Documentation 8.0

ZABBIX

09.04.2026

Contents

Podręcznik użytkownika **6**

Witamy w dokumentacji Zabbix **6**

Rozpocznij pracę z Zabbix . . . 6
Zabbix Cloud . . . 6
Centrum dewelopera . . . 6
Społeczność i inne zasoby . . . 6
1 Instalacja i pierwsze kroki . . . 6
1 Instalacja interfejsu webowego . . . 7
2 Przewodniki szybkiego startu . . . 13
3 Instalacja: dodatkowe przewodniki . . . 33
4 Aktualizacja . . . 72
5 Uwagi dotyczące aktualizacji do Zabbix 8.0 . . . 87
Wymagania . . . 89
Znane problemy . . . 98
2 Co nowego w Zabbix 8.0 . . . 106
Szablony . . . 107
Pozycje . . . 108
Wtyczki . . . 108
Wykrywanie niskiego poziomu . . . 109
Procesy . . . 109
Uwierzytelnianie . . . 110
Widżety . . . 110
Frontend . . . 111
Dokumentacja . . . 112
Co nowego w Zabbix 8.0.x . . . 112
3 Urządzenie Zabbix . . . 112
4 Procesy Zabbix . . . 116
1 Server . . . 116
2 Agent . . . 125
3 Agent 2 . . . 128
4 Proxy . . . 137
5 Java gateway . . . 142
6 Sender . . . 146
7 Get . . . 146
8 JS . . . 147
9 Usługa sieciowa . . . 148
5 Konfiguracja . . . 149
1 Hosty i grupy hostów . . . 159
2 Pozycje . . . 177
3 Wykrywanie problemów za pomocą wyzwalaczy . . . 391
4 Zdarzenia . . . 441
5 Korelacja zdarzeń . . . 445
6 Tagowanie . . . 452
7 Wizualizacja . . . 455
8 Szablony i grupy szablonów . . . 481
9 Szablony dostępne od razu . . . 481
10 Powiadomienia o zdarzeniach . . . 495
11 Makra . . . 544
12 Użytkownicy i grupy użytkowników . . . 558
13 Przechowywanie sekretów . . . 567

14 Zaplanowane raporty . . . 574
15 Eksport danych . . . 578
6 Monitorowanie usług . . . 584
1 Drzewo usług . . . 585
2 SLA . . . 589
3 Przykład konfiguracji . . . 590
7 Monitorowanie WWW . . . 594
1 Pozycje monitorowania WWW . . . 603
2 Scenariusz z życia wzięty . . . 604
8 Monitorowanie maszyn wirtualnych . . . 611
1 Klucze pozycji monitorowania VMware . . . 613
2 Kluczowe pola wykrywania maszyn wirtualnych . . . 631
3 przykłady JSON dla pozycji VMware . . . 635
4 Przykład konfiguracji monitorowania VMware . . . 640
9 Konserwacja . . . 645
10 Wyrażenia regularne . . . 650
11 Potwierdzanie problemu . . . 656
1 Tłumienie problemów . . . 658
12 Eksport/import konfiguracji . . . 659
1 Grupy szablonów . . . 660
2 Grupy hostów . . . 661
4 Hosty . . . 678
5 Mapy sieciowe . . . 694
6 Typy mediów . . . 703
13 Wykrywanie . . . 709
1 Wykrywanie sieci . . . 710
2 Autorejestracja agenta aktywnego . . . 718
3 Odkrywanie niskiego poziomu . . . 722
14 Monitorowanie rozproszone . . . 776
1 Proxy . . . 777
15 Szyfrowanie . . . 785
1 Korzystanie z certyfikatów . . . 792
2 Używanie kluczy współdzielonych z wyprzedzeniem . . . 799
3 Rozwiązywanie problemów . . . 802
16 Interfejs webowy . . . 804
1 Menu . . . 805
2 Sekcje frontend . . . 812
3 Ustawienia użytkownika . . . 1067
4 Wyszukiwanie globalne . . . 1072
5 Tryb konserwacji frontendu . . . 1074
6 Parametry strony . . . 1075
7 Definicje . . . 1078
8 Tworzenie własnego motywu . . . 1078
9 Tryb debugowania . . . 1079
10 Ciasteczka używane przez Zabbix . . . 1080
11 Strefy czasowe . . . 1081
12 Resetowanie hasła . . . 1082
13 Okres czasu i selektory hostów . . . 1082
17 Najlepsze praktyki . . . 1084
1 Najlepsze praktyki bezpieczeństwa . . . 1084
2 Najlepsze praktyki konfiguracji . . . 1092
18 API . . . 1094
Odniesienie do metody . . . 1098
Dodatek 1. Komentarz referencyjny . . . 1920
Załącznik 2. Zmiany od 7.4 do 8.0 . . . 1926
Załącznik 3. Zmiany w wersji 8.0 . . . 1928
19 Rozszerzenia . . . 1928
1 Moduły ładowalne . . . 1930
3 Moduły frontend . . . 1939
20 Aneksy . . . 1940
1 Instalacja i konfiguracja . . . 1940
2 Konfiguracja procesów . . . 2000
3 Protokoły . . . 2088

4 Pozycje . . . 2113
5 Obsługiwane funkcje . . . 2149
6 Makra . . . 2150
7 Symbole jednostek . . . 2184
8 Składnia okresu czasu . . . 2186
9 Wykonywanie poleceń . . . 2187
10 Zgodność wersji . . . 2188
12 Biblioteka dynamiczna Zabbix sender dla systemu Windows . . . 2189
13 Aktualizacja monitorowania usług . . . 2189
14 Inne problemy . . . 2190
16 Przykłady znaków ucieczki . . . 2191
21 Przewodniki szybkiego odniesienia . . . 2192
Przegląd . . . 2193
1. Monitor Linux with Zabbix agent . . . 2193
2 Monitorowanie systemu Windows za pomocą agent Zabbix . . . 2196
3. Monitor Apache via HTTP . . . 2200
4. Monitor MySQL with Zabbix agent 2 . . . 2204
5 Monitoruj VMware za pomocą Zabbix . . . 2212
6 Monitoruj ruch sieciowy za pomocą Zabbix . . . 2216
7 Monitoruj ruch sieciowy za pomocą aktywnych kontroli . . . 2219
8 Monitorowanie stron internetowych za pomocą pozycji przeglądarki . . . 2222
9 Monitorowanie certyfikatów stron internetowych za pomocą agent Zabbix 2 (pasywnie) . . . 2227
10 Monitorowanie przełącznika sieciowego lub routera za pomocą Zabbix . . . 2231
11 Monitorowanie dziennika zdarzeń Windows przy użyciu aktywnych kontroli . . . 2238
Czym jest Zabbix . . . 2242

Zabbix Cloud **2246**

Zabbix Cloud **2246**
Konfiguracja i zarządzanie Zabbix Cloud . . . 2246
Dowiedz się więcej o Zabbix Cloud . . . 2247
Wdróż Zabbix w chmurze . . . 2247
Konfiguracja węzła . . . 2251
Przegląd . . . 2251
Karta Przegląd . . . 2252
Karta filtrów dostępu . . . 2253
Karta Szyfrowanie . . . 2254
Karta Kopie zapasowe . . . 2255
Karta Historia . . . 2255
Karta Konserwacja . . . 2256
Karta Upgrade . . . 2257
Dodawanie użytkowników . . . 2259
Wprowadzenie . . . 2259
Dodawanie użytkowników do organizacji . . . 2259
Dodawanie użytkowników do węzłów . . . 2260
Kluczowe różnice w Zabbix Cloud . . . 2261

Centrum dewelopera **2263**

Centrum deweloperskie **2263**
Twórz na Zabbix . . . 2263
Pluginy . . . 2263
Interfejsy wtyczek . . . 2269
Biblioteka Python dla Zabbix . . . 2272
Instalacja . . . 2272
Przewodnik szybkiego startu . . . 2272
Korzystanie z API Zabbix . . . 2276
Zbieranie danych z agenta Zabbix . . . 2279
Wysyłanie danych do serwera lub proxy Zabbix . . . 2280
Rejestrowanie debugowania . . . 2284
Moduły . . . 2284
Struktura plików modułu . . . 2285
Widżety . . . 2292
Poradniki . . . 2301

Przykłady . . . 2327
Zmiany w tworzeniu rozszerzeń . . . 2327

Strony podręcznika Zabbix **2328**
zabbix_agent2 . . . 2328
NAZWA . . . 2328
SKŁADNIA . . . 2328
OPIS . . . 2328
OPCJE . . . 2328
PLIKI . . . 2329
ZOBACZ TAKŻE . . . 2329
Indeks . . . 2329
zabbix_agentd . . . 2330
Nazwa . . . 2330
SKŁADNIA . . . 2330
OPIS . . . 2330
OPCJE . . . 2330
PLIKI . . . 2331
ZOBACZ TAKŻE . . . 2331
Indeks . . . 2331
zabbix_get . . . 2331
NAME . . . 2332
SKŁADNIA . . . 2332
OPIS . . . 2332
OPCJE . . . 2332
PRZYKŁADY . . . 2333
ZOBACZ TAKŻE . . . 2333
Indeks . . . 2333
zabbix_js . . . 2334
NAZWA . . . 2334
SKŁADNIA . . . 2334
OPIS . . . 2334
OPCJE . . . 2334
PRZYKŁADY . . . 2334
ZOBACZ TAKŻE . . . 2334
Indeks . . . 2335
zabbix_proxy . . . 2335
NAZWA . . . 2335
SKŁADNIA . . . 2335
OPIS . . . 2335
OPCJE . . . 2335
PLIKI . . . 2336
ZOBACZ TAKŻE . . . 2336
Indeks . . . 2336
zabbix_sender . . . 2337
NAME . . . 2337
SKŁADNIA . . . 2337
DESCRIPTION . . . 2337
OPCJE . . . 2338
KOD POWROTU . . . 2340
PRZYKŁADY . . . 2340
ZOBACZ TAKŻE . . . 2341
Indeks . . . 2341
zabbix_server . . . 2341
NAME . . . 2341
SKŁADNIA . . . 2341
OPIS . . . 2341
OPCJE . . . 2341
PLIKI . . . 2343
ZOBACZ TAKŻE . . . 2343
Indeks . . . 2343
zabbix_web_service . . . 2343
NAZWA . . . 2344

SKŁADNIA 2344
OPIS 2344
OPCJE 2344
PLIKI 2344
ZOBACZ TAKŻE 2344
Indeks 2344

Informacja o prawach autorskich **2344**

Podręcznik użytkownika

Witamy w dokumentacji Zabbix

Twoje podstawowe źródło informacji do pracy z monitoringiem Zabbix — od podstawowych wdrożeń po zaawansowane konfiguracje. Ten podręcznik obejmuje wszystko, co jest potrzebne do instalacji, konfiguracji i obsługi Zabbix.

Co nowego w Zabbix 8.0

Rozpocznij pracę z Zabbix

Instalacja Instrukcje krok po kroku dotyczące instalacji Zabbix na wybranej platformie, obejmujące różne systemy operacyjne i konfiguracje baz danych.

Wymagania Lista obsługiwanych platform i wymagań wstępnych dotyczących oprogramowania, która pomoże Ci przygotować środowisko do pomyślnego wdrożenia Zabbix.

Przewodniki szybkiego startu Zwięzłe instrukcje krok po kroku, zorientowane na wykonanie konkretnych zadań, które przeprowadzą Cię przez podstawy — od pierwszych kroków konfiguracji po otrzymanie pierwszego alertu o problemie.

Zabbix Cloud

Rozpocznij korzystanie z Zabbix Cloud Instrukcje krok po kroku, które pomogą szybko uruchomić instancję Zabbix Cloud, w tym przeprowadzić wstępną konfigurację i podłączyć monitorowane urządzenia.

Zabbix Cloud a on-premises Porównaj różnice w zarządzaniu, skalowalności i utrzymaniu między tymi dwoma wdrożeniami i dowiedz się, które z nich może najpłynniej wspierać Twój przepływ pracy.

Poznaj Zabbix Cloud Zapoznaj się z przeglądem Zabbix Cloud, w tym z jego kluczowymi funkcjami, korzyściami oraz tym, co obejmuje subskrypcja. Odpowiedzi na często zadawane pytania dotyczące konfiguracji i użytkowania można znaleźć w FAQ.

Centrum dewelopera

Moduły frontend Przewodniki i materiały referencyjne dotyczące tworzenia niestandardowych modułów, które rozszerzają lub modyfikują frontend Zabbix, aby dostosować go do konkretnych przypadków użycia.

Widgety Omówienie struktury i logiki widgetów wraz z instrukcjami tworzenia niestandardowych elementów pulpitu dostosowanych do Twoich potrzeb.

Wtyczki Przegląd sposobu tworzenia i zarządzania wtyczkami Zabbix w celu rozszerzenia funkcjonalności lub integracji z systemami zewnętrznymi.

Społeczność i inne zasoby

Fora Zabbix Miejsce do wymiany pomysłów, znajdowania rozwiązań i dzielenia się doświadczeniami na wszystkich poziomach zaawansowania w Zabbix.

Blog Zabbix Aktualności, samouczki i studia przypadków przygotowane przez zespół Zabbix oraz współtwórców społeczności.

Filmy instruktażowe Biblioteka filmów zawierająca demonstracje, dyskusje i wskazówki, które pomogą Ci w pełni wykorzystać możliwości Zabbix.

1 Instalacja i pierwsze kroki

Aby skonfigurować Zabbix od podstaw, wykonaj następujące kroki:

1. Upewnij się, że wymagane oprogramowanie jest zainstalowane i uruchomione.
2. Zainstaluj Zabbix.
3. Zainstaluj interfejs webowy Zabbix.
4. Rozpocznij monitorowanie.

Poniżej znajdują się bardziej szczegółowe informacje dotyczące każdego kroku.

Wymagane oprogramowanie Zabbix dobrze współpracuje z następującym oprogramowaniem (często nazywanym stosem LAMP):

- **System operacyjny Linux:** Ubuntu, Debian, CentOS lub inne
- **Serwer WWW:** Apache lub NGINX
- **Serwer bazy danych:** MySQL/MariaDB lub PostgreSQL
- **PHP**

W większości nowoczesnych systemów Linux PHP może być już zainstalowany. W takim przypadku może być konieczne jedynie skonfigurowanie serwera bazy danych i serwera WWW.

Aby uzyskać bardziej szczegółowe informacje, takie jak obsługiwane wersje oprogramowania, zobacz Wymagane oprogramowanie.

Zainstaluj Zabbix **Najłatwiejszym** sposobem instalacji Zabbix jest użycie **pakietów dystrybucyjnych**. Pakiety instalują drobne zależności programowe.

Dokładne instrukcje instalacji, dostosowane do Twojego systemu operacyjnego, są dostępne na **stronie internetowej Zabbix**.

Wybierz swoją platformę i postępuj zgodnie z podanymi instrukcjami. Na początek zaleca się zainstalowanie serwera Zabbix, agenta Zabbix 2 oraz frontendu (interfejsu webowego). Później możesz dodać proxy Zabbix i kolejne agenty.

Częścią procesu instalacji jest utworzenie bazy danych (do przechowywania danych konfiguracyjnych i historycznych) oraz zaimportowanie do niej danych początkowych.

Zainstaluj interfejs webowy Zabbix Wykonaj kroki **kreatora instalacji** interfejsu webowego.

Zostaniesz poproszony o podanie hasła do bazy danych (utworzonego w poprzednim kroku), aby frontend mógł komunikować się z bazą danych.

Rozpocznij monitorowanie Zaloguj się do interfejsu webowego Zabbix.

Skorzystaj z **przewodników szybkiego startu**, aby rozpocząć monitorowanie popularnych zasobów (Linux, Apache, MySQL lub innych). Te krótkie przewodniki wyjaśniają, z którymi szablonami należy pracować, aby rozpocząć monitorowanie popularnych zasobów.

Możesz zacząć od przewodnika szybkiego startu dotyczącego monitorowania serwera Linux.

1 Instalacja interfejsu webowego

Ta sekcja zawiera instrukcje krok po kroku dotyczące instalacji interfejsu webowego Zabbix. Wykonaj te kroki po zainstalowaniu backendu Zabbix — serwera Zabbix, agenta i bazy danych.

Frontend Zabbix jest napisany w PHP, dlatego do jego uruchomienia wymagany jest serwer WWW obsługujący PHP.

> **Note:**
> Więcej informacji na temat konfiguracji SSL dla frontend Zabbix można znaleźć, zapoznając się z tymi najlepszymi praktykami.

Ekran powitalny

Otwórz adres URL frontendu Zabbix w przeglądarce. Jeśli Zabbix został zainstalowany z pakietów, adres URL to:

- dla Apache: `http://<server_ip_or_name>/zabbix`
- dla Nginx: `http://<server_ip_or_name>`

Powinien zostać wyświetlony pierwszy ekran kreatora instalacji frontendu.

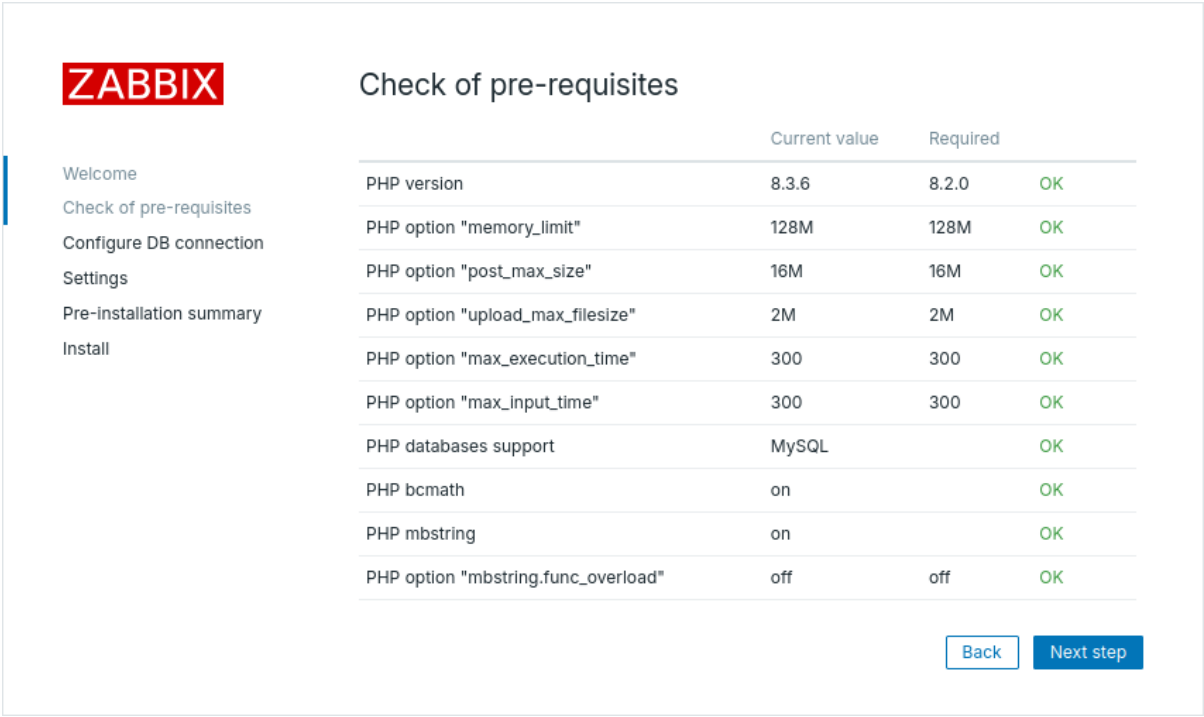
Użyj listy rozwijanej *Default language*, aby zmienić domyślny język systemu i kontynuować proces instalacji w wybranym języku (opcjonalnie). Więcej informacji znajduje się w sekcji Instalacja dodatkowych języków frontendu.

Pamiętaj, że ustawienie języka na *English (en_US)* spowoduje również włączenie amerykańskiego formatu czasu/daty we frontendcie.



Sprawdzenie wymagań wstępnych

Upewnij się, że wszystkie obowiązkowe wymagania wstępne Zabbix frontend są spełnione.



Wymaganie wstępne	Wartość minimalna	Opis
Wersja PHP	8.2.0	
Opcja PHP "memory_limit"	128MB	W php.ini: memory_limit = 128M
Opcja PHP "post_max_size"	16MB	W php.ini: post_max_size = 16M
Opcja PHP "upload_max_filesize"	2MB	W php.ini: upload_max_filesize = 2M
Opcja PHP "max_execution_time"	300 sekund	W php.ini: max_execution_time = 300 (dozwolone są również wartości 0 i -1)
Opcja PHP "max_input_time"	300 sekund	W php.ini: max_input_time = 300 (dozwolone są również wartości 0 i -1)

Wymaganie wstępne	Wartość minimalna	Opis
Obsługa baz danych PHP	Jedna z: MySQL, PostgreSQL	Listę wszystkich obowiązkowych i opcjonalnych rozszerzeń PHP można znaleźć w sekcji Wymagania. Należy pamiętać, że niespełnione opcjonalne wymagania wstępne są wyświetlane z czerwonym statusem *Ostrzeżenie*, a proces konfiguracji może być kontynuowany, nawet jeśli nie są spełnione.
PHP bcmath	musi być włączone	
PHP mbstring	musi być włączone	
Opcja PHP "mbstring.func_overload"	musi być wyłączona	W php.ini: mbstring.func_overload = 0
Opcja PHP "session.auto_start"	musi być wyłączona	W php.ini: session.auto_start = 0
Opcja PHP "arg_separator.output"	&	W php.ini: arg_separator.output = "&" (dozwolona jest również wartość "&")

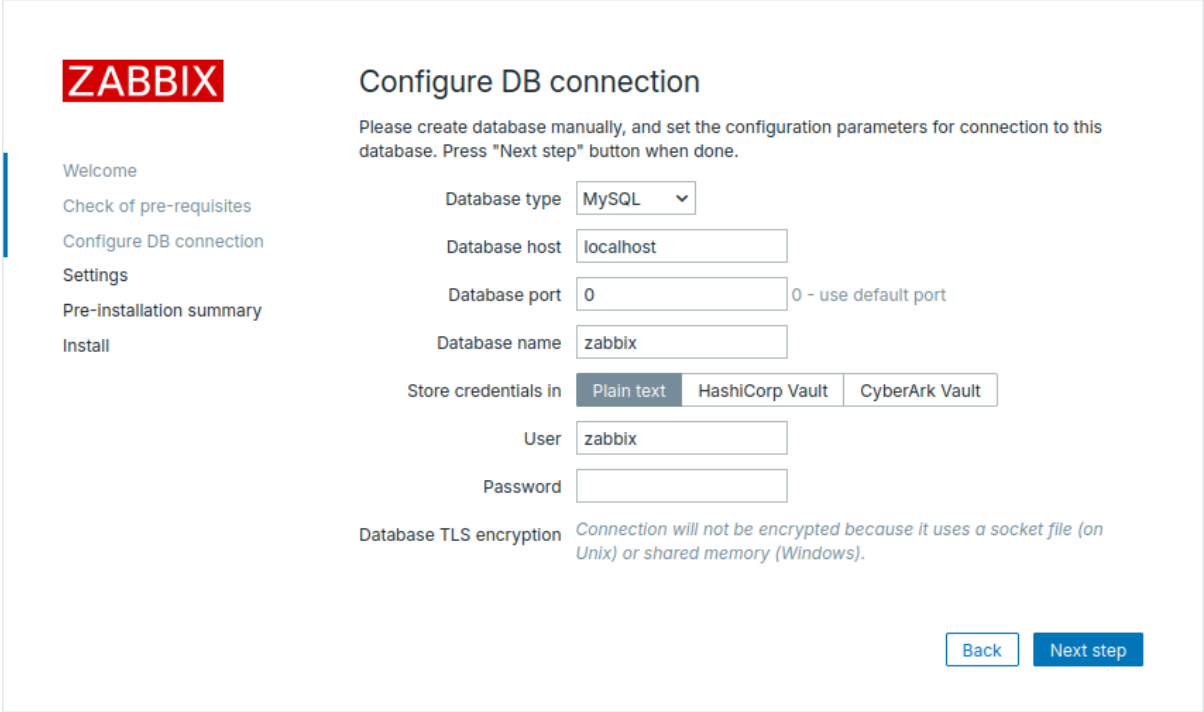
Attention:
Jeśli użytkownik Apache lub grupa użytkowników Apache wymaga zmiany, zweryfikuj uprawnienia do folderu sesji; w przeciwnym razie konfiguracja Zabbix może nie móc być kontynuowana.

Skonfiguruj połączenie z bazą danych

Wprowadź szczegóły połączenia z bazą danych. Baza danych Zabbix musi być już utworzona.

W przypadku MySQL wpisanie `localhost` lub pozostawienie pola *Database host* pustego powoduje połączenie przez domyślne gniazdo Unix. Formularz konfiguracji nie udostępnia osobnego pola *Database socket*, dlatego aby użyć niestandardowego gniazda, skonfiguruj je w ustawieniach serwera Zabbix (na przykład za pomocą `DBSocket=` w pliku zabbix_server.conf). Dzięki temu frontend pozostaje zgodny z ustawieniami połączenia serwer-baza danych.

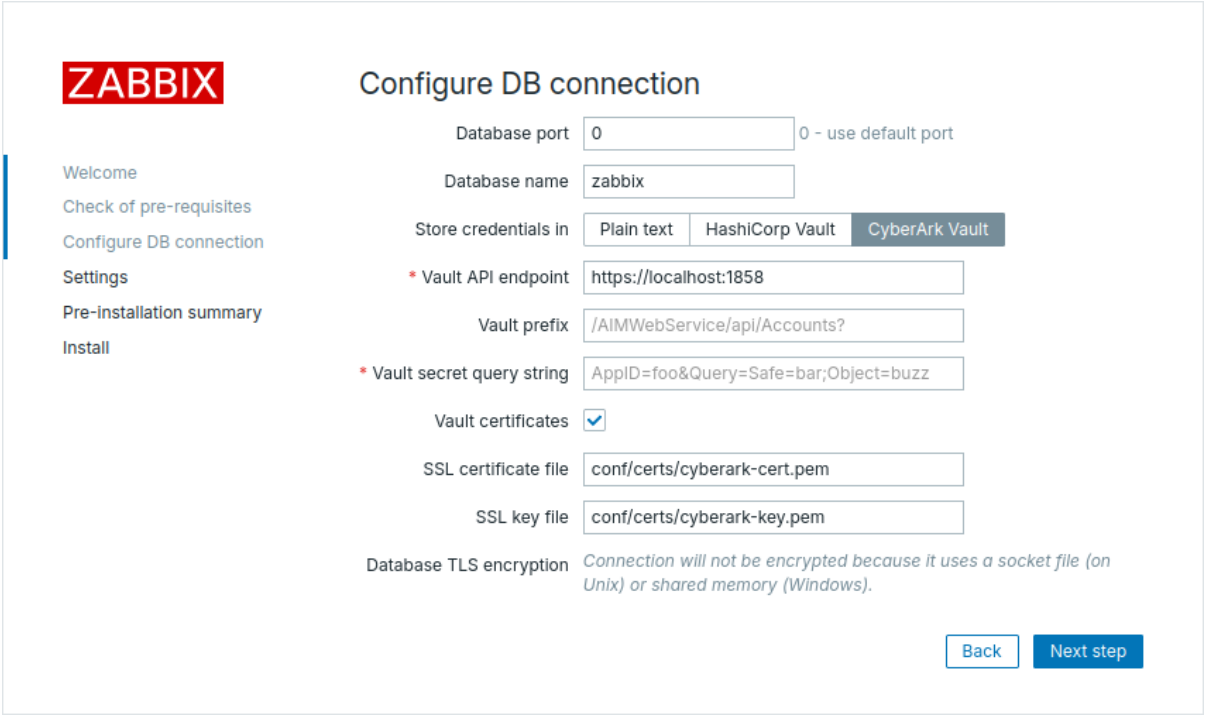
W przypadku PostgreSQL, jeśli pole *Database host* pozostanie puste, użyte zostanie domyślne gniazdo domeny Unix. Jeśli zostanie podana ścieżka do gniazda (na przykład `/var/run/pgbouncer`), zamiast tego użyte zostanie to gniazdo domeny Unix.



Jeśli zaznaczona jest opcja *Database TLS encryption*, w formularzu pojawią się dodatkowe pola do konfiguracji połączenia TLS z bazą danych (tylko MySQL lub PostgreSQL).

Jeśli *Store credentials in* jest ustawione na HashiCorp Vault lub CyberArk Vault, dostępne staną się dodatkowe parametry:

- dla HashiCorp Vault: punkt końcowy API Vault, prefiks skarbca, ścieżka sekretu oraz token uwierzytelniający;
- dla CyberArk Vault: punkt końcowy API Vault, prefiks skarbca, ciąg zapytania sekretu oraz certyfikaty. Po zaznaczeniu pola *Vault certificates* pojawią się dwa nowe pola do określenia ścieżek do pliku certyfikatu SSL i pliku klucza SSL.

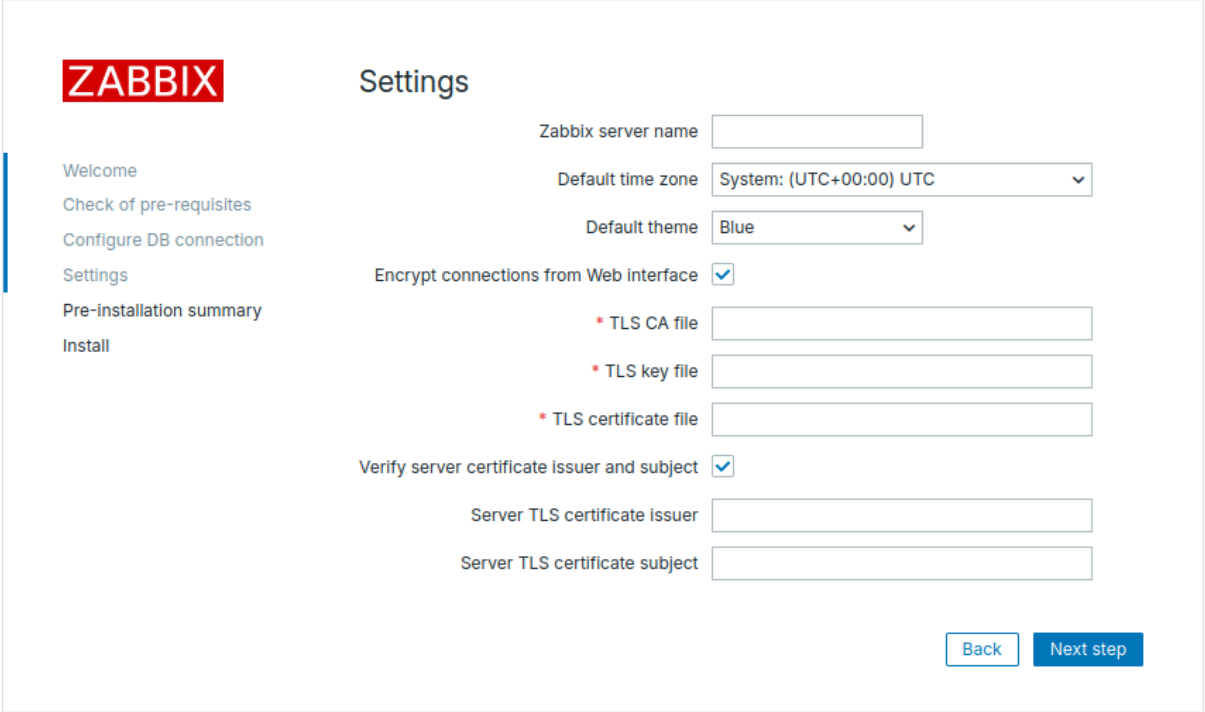


Ustawienia

Wprowadzenie nazwy serwera Zabbix jest opcjonalne, jednak jeśli zostanie podana, będzie wyświetlana na pasku menu i w tytułach stron.

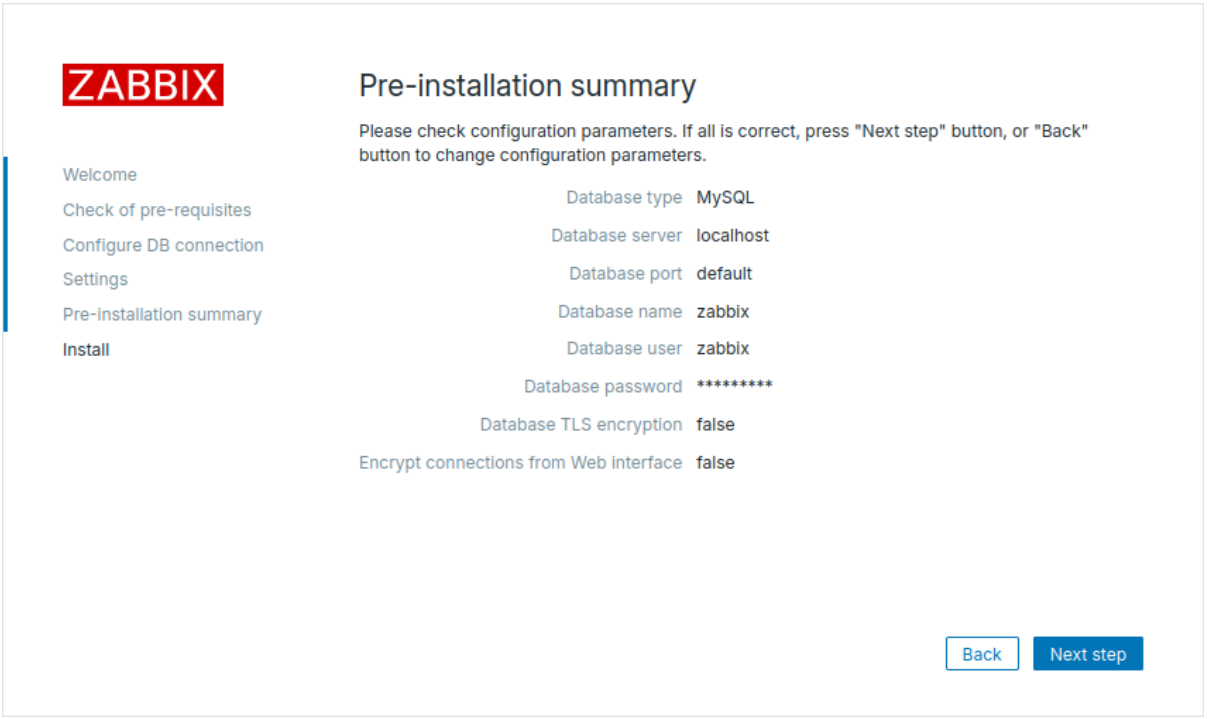
Ustaw domyślną strefę czasową i motyw dla frontend.

Jeśli zaznaczona jest opcja *Encrypt connections from Web interface*, w formularzu pojawią się dodatkowe pola do konfigurowania połączenia TLS między serwerem Zabbix a frontend.

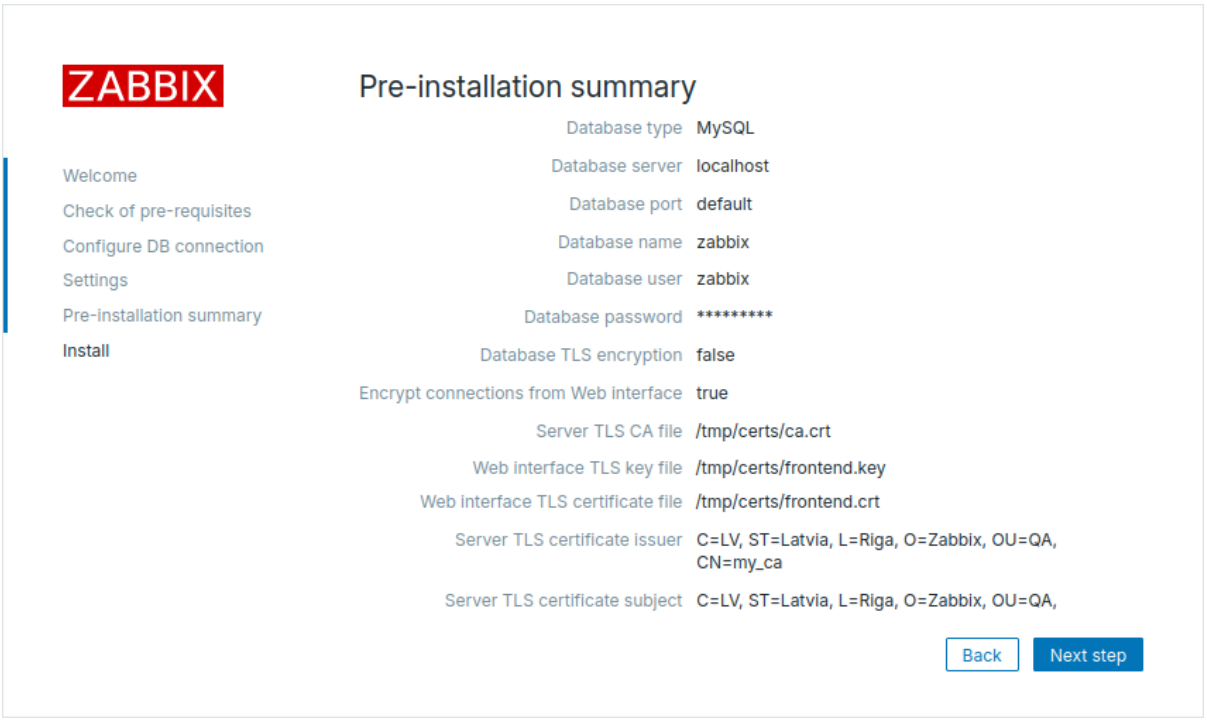


Podsumowanie przed instalacją

Przejrzyj podsumowanie ustawień.

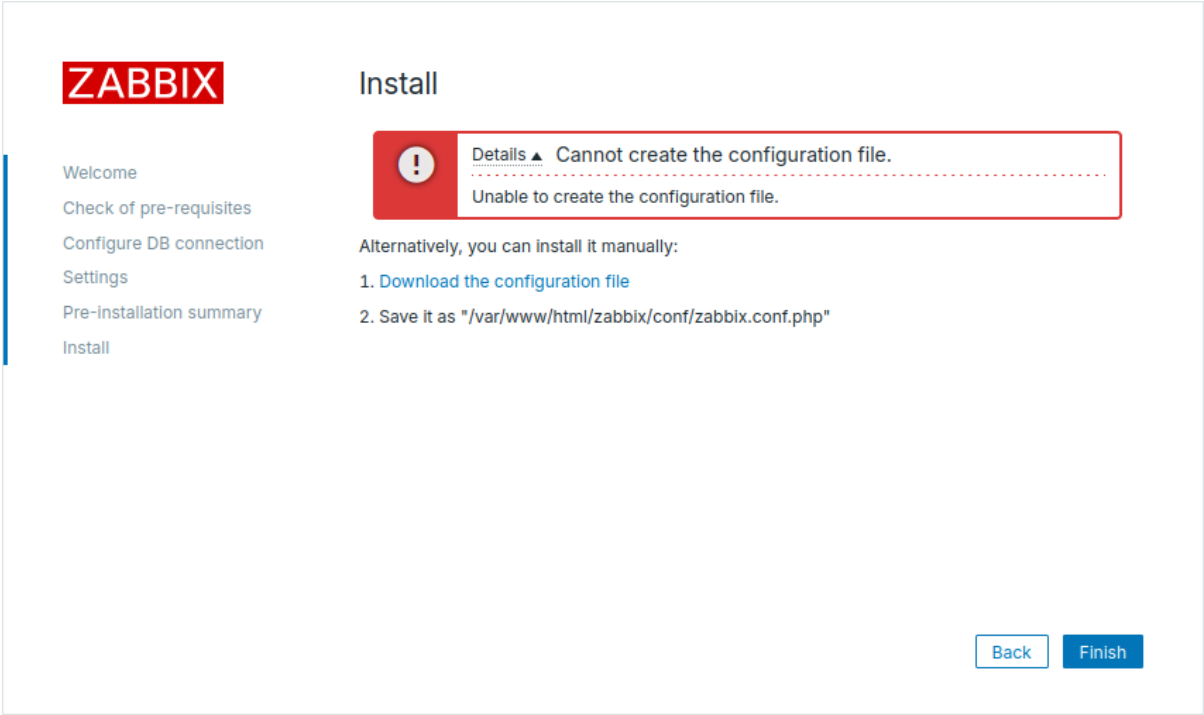


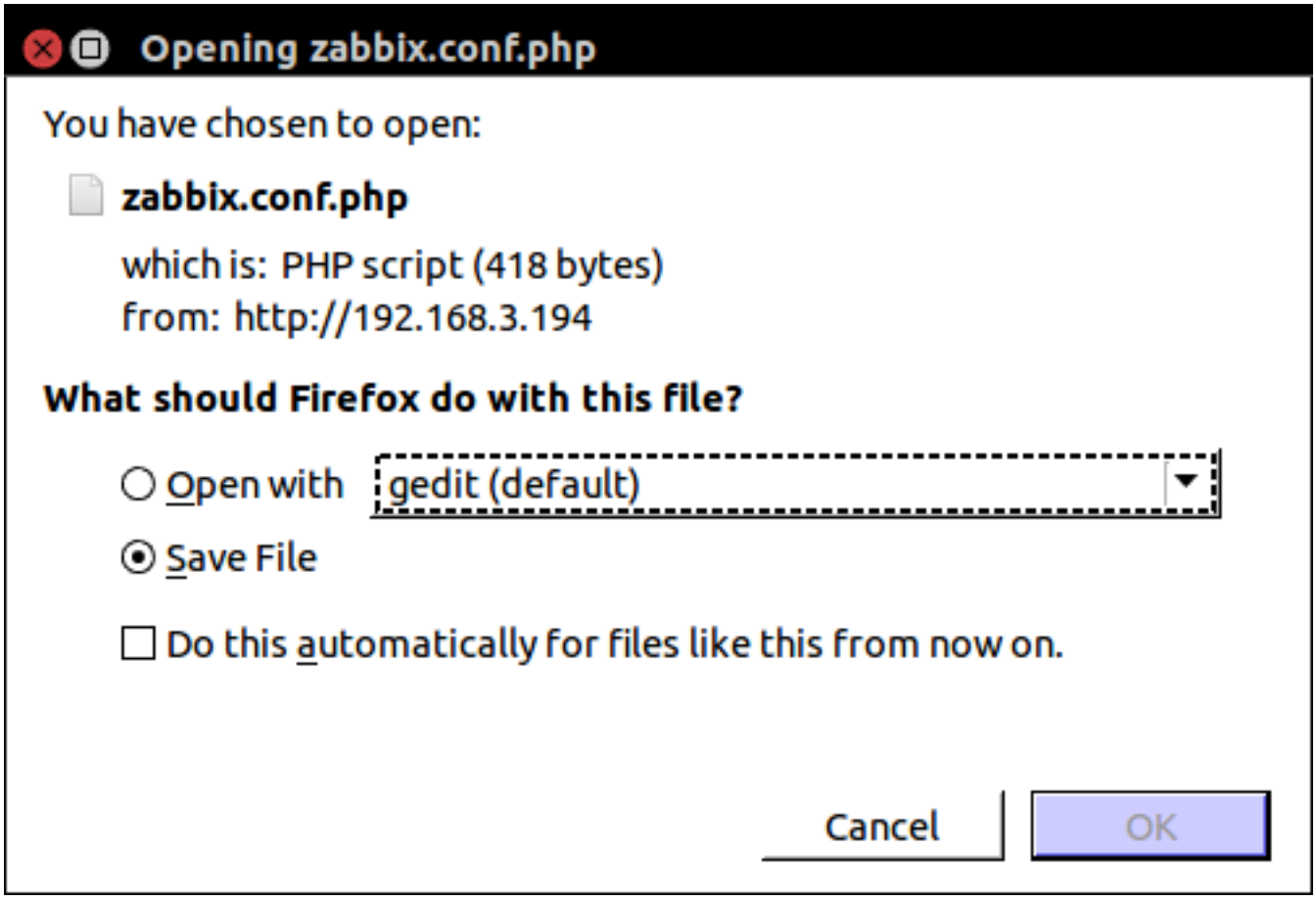
Podstrona wyświetli dane, jeśli konfiguracja TLS została dodana.



Instalacja

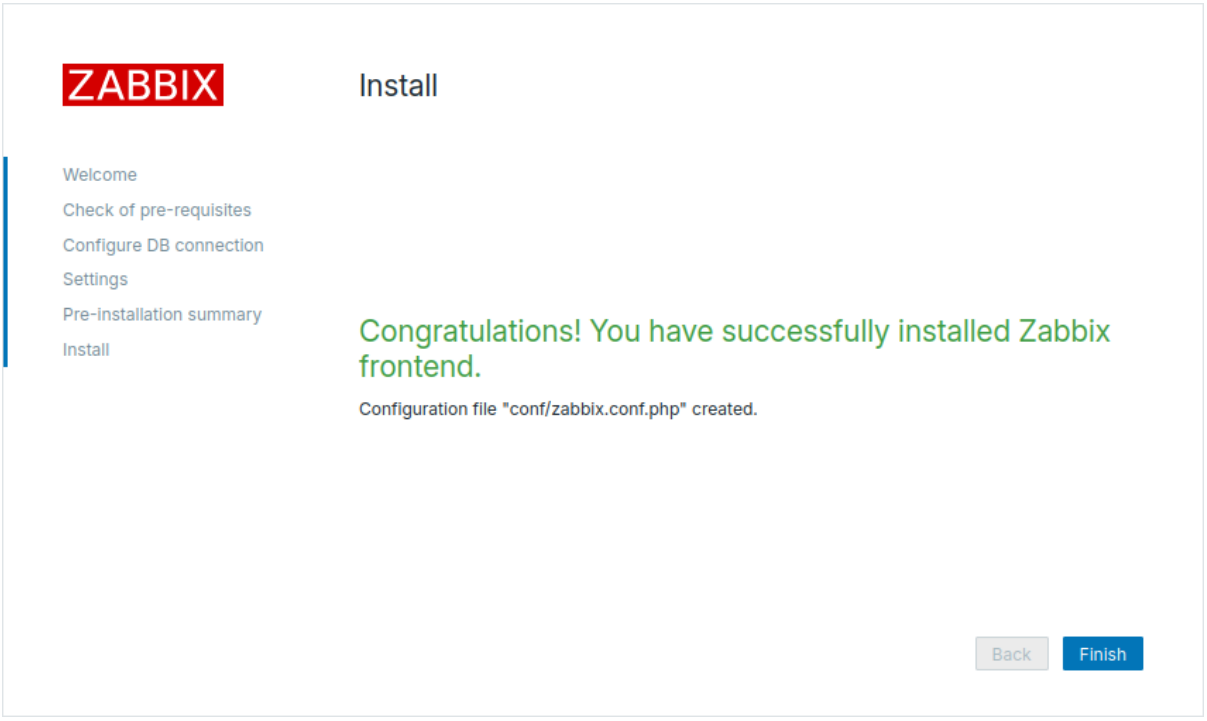
Jeśli instalujesz Zabbix ze źródeł, pobierz plik konfiguracyjny i umieść go w katalogu conf/ w podkatalogu dokumentów HTML serwera WWW, do którego skopiowano pliki PHP Zabbix.





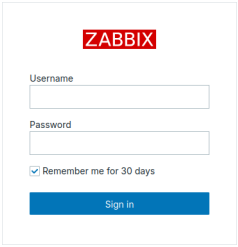
Note:
Jeśli użytkownik serwera WWW ma uprawnienia do zapisu w katalogu conf/, plik konfiguracyjny zostanie zapisany automatycznie i będzie można od razu przejść do następnego kroku.

Zakończ instalację.



Logowanie

Frontend Zabbix jest gotowy! Domyślna nazwa użytkownika to **Admin**, hasło **zabbix**.



Przejdź do przewodnika monitorowania Linuxa.

2 Przewodniki szybkiego startu

Po zainstalowaniu Zabbix i jego interfejsu webowego nadszedł czas, aby rozpocząć monitorowanie.

Skorzystaj z tych krótkich przewodników, aby rozpocząć monitorowanie popularnych zasobów:

- Monitorowanie serwera Linux
- Monitorowanie serwera WWW Apache
- Monitorowanie serwera MySQL

Przewodniki szybkiego startu koncentrują się na użyciu oficjalnych szablonów Zabbix do monitorowania. Szablon to wstępnie skonfigurowany zestaw elementów monitorowania. Szablon umożliwia skalowanie monitorowania — możesz przetestować szablon na pojedynczym monitorowanym obiekcie (urządzeniu, aplikacji itp.), dostosować go, a następnie zastosować do wielu podobnych obiektów monitorowania.

Chociaż szablony dobrze nadają się do monitorowania od razu po wdrożeniu, możesz także chcieć dostosować ich elementy.

Aby lepiej zrozumieć podstawowe elementy składające się na szablon, zapoznaj się z sekcją Podstawowa konfiguracja.

Podstawowa konfiguracja

Te przewodniki przedstawiają podstawowe elementy konfiguracji Zabbix:

- Logowanie i konfiguracja użytkownika
- Nowy host
- Nowa pozycja
- Nowy wyzwalacz

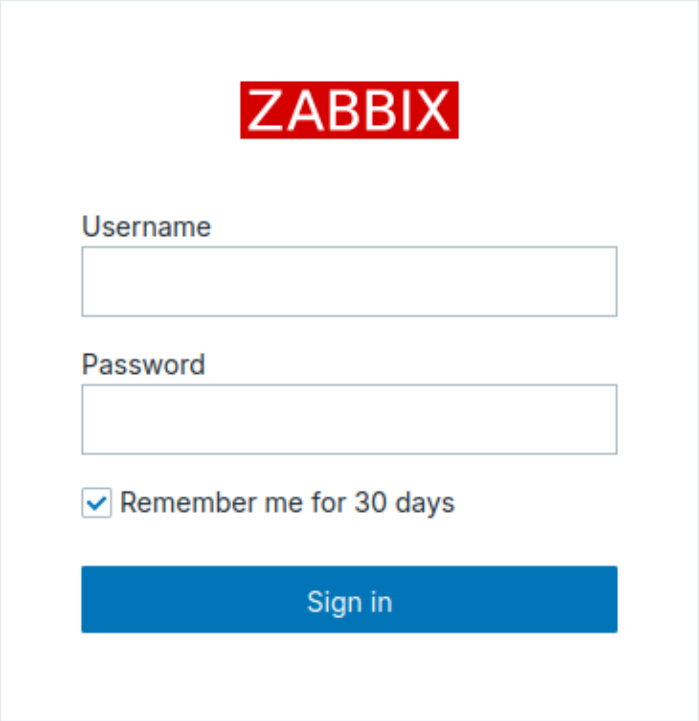
- Otrzymywanie powiadomień o problemach
- Nowy szablon

1 Logowanie i konfiguracja użytkownika

Przegląd

W tej sekcji dowiesz się, jak zalogować się i skonfigurować użytkownika systemowego w Zabbix.

Logowanie



To jest ekran powitalny Zabbix. Wprowadź nazwę użytkownika **Admin** oraz hasło **zabbix**, aby zalogować się jako superużytkownik Zabbix. Zostanie przyznany dostęp do wszystkich sekcji menu.

Ze względów bezpieczeństwa zdecydowanie zaleca się zmianę domyślnego hasła dla konta Admin natychmiast po pierwszym logowaniu.

Trwałe logowanie

Aby pozostać zalogowanym przez maksymalnie 30 dni, zaznacz opcję *Zapamiętaj na 30 dni* przed kliknięciem *Zaloguj się*.

Opcja *Zapamiętaj na 30 dni* włączona:

- Twoja sesja pozostaje aktywna przez 30 dni.
- Ustawienie *Auto-logout* jest nadpisywane, dzięki czemu pozostajesz zalogowany do końca tego okresu.
- Przy kolejnych wizytach w ciągu 30 dni zostaniesz zalogowany automatycznie bez ponownego wprowadzania danych logowania.

Opcja *Zapamiętaj na 30 dni* wyłączona:

- Wszelkie wcześniej włączone automatyczne logowanie zostaje wyczyszczone.
- Sesja wygaśnie zgodnie ze skonfigurowanym interwałem *Auto-logout*.

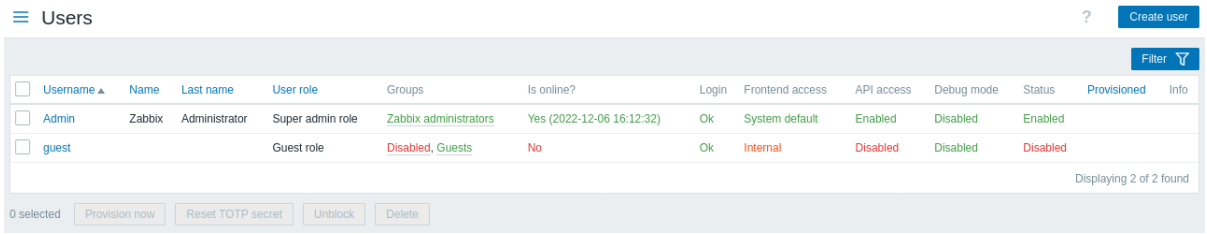
Ochrona przed atakami brute force

W przypadku pięciu kolejnych nieudanych prób logowania interfejs Zabbix zostanie wstrzymany na 30 sekund, aby zapobiec atakom brute force i słownikowym.

Adres IP nieudanej próby logowania zostanie wyświetlony po pomyślnym zalogowaniu.

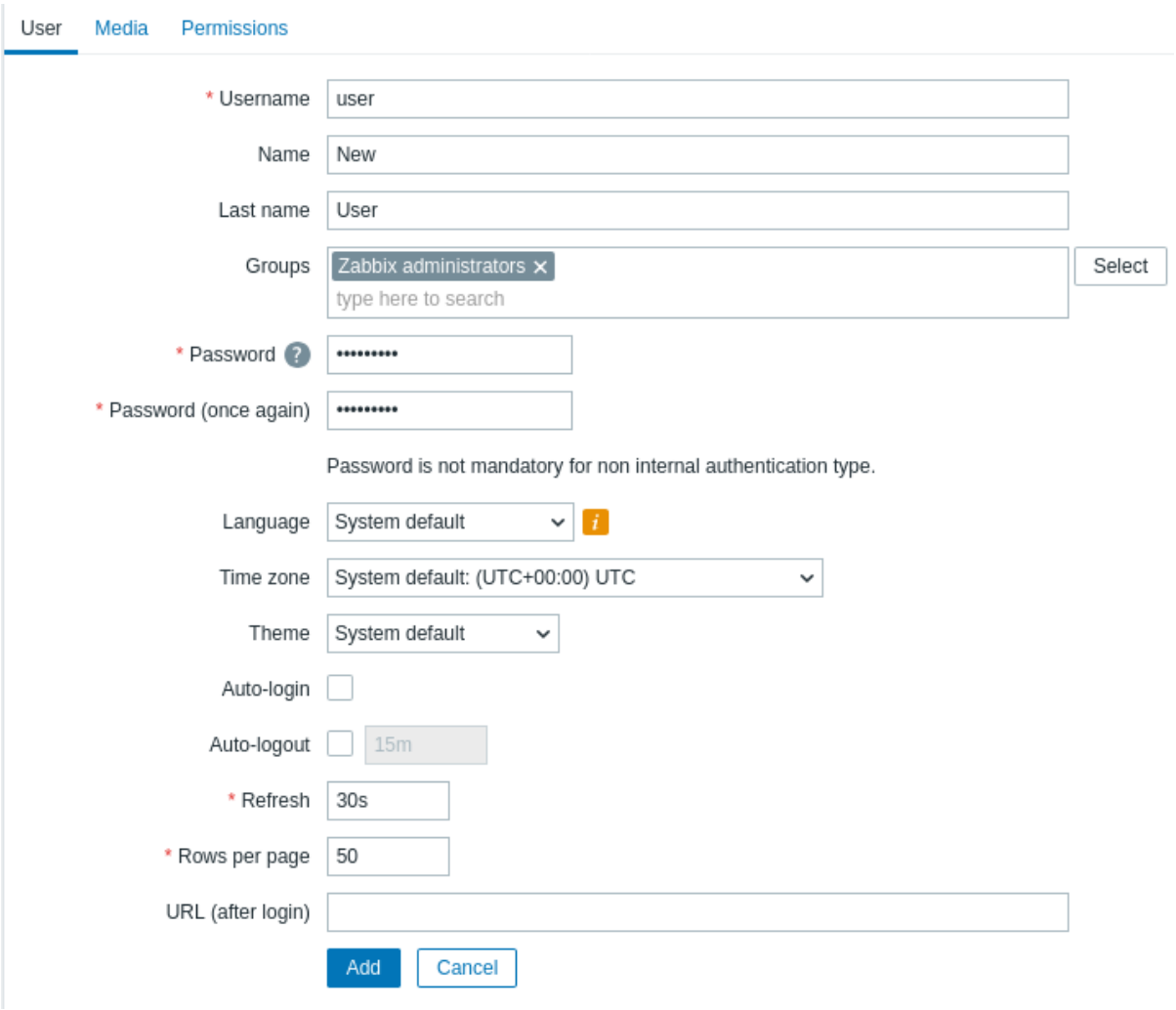
Dodawanie użytkownika

Aby wyświetlić informacje o użytkownikach, przejdź do *Users* > *Users* w pionowym menu paska bocznego.



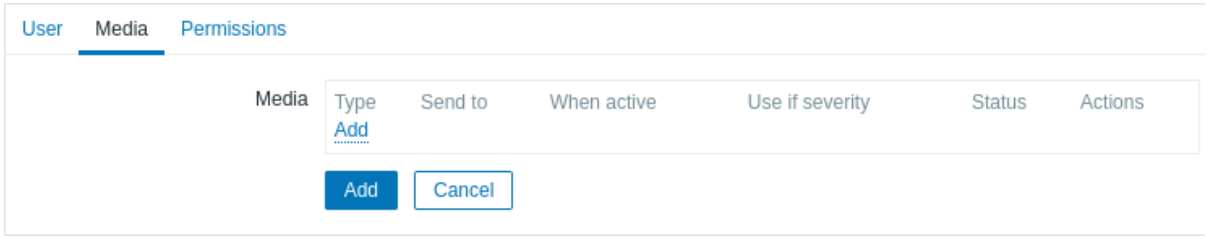
Aby dodać nowego użytkownika, wybierz *Create user* w prawym górnym rogu.

W formularzu nowego użytkownika pamiętaj, aby dodać użytkownika do jednej z istniejących grup użytkowników, na przykład „Zabbix administrators”.



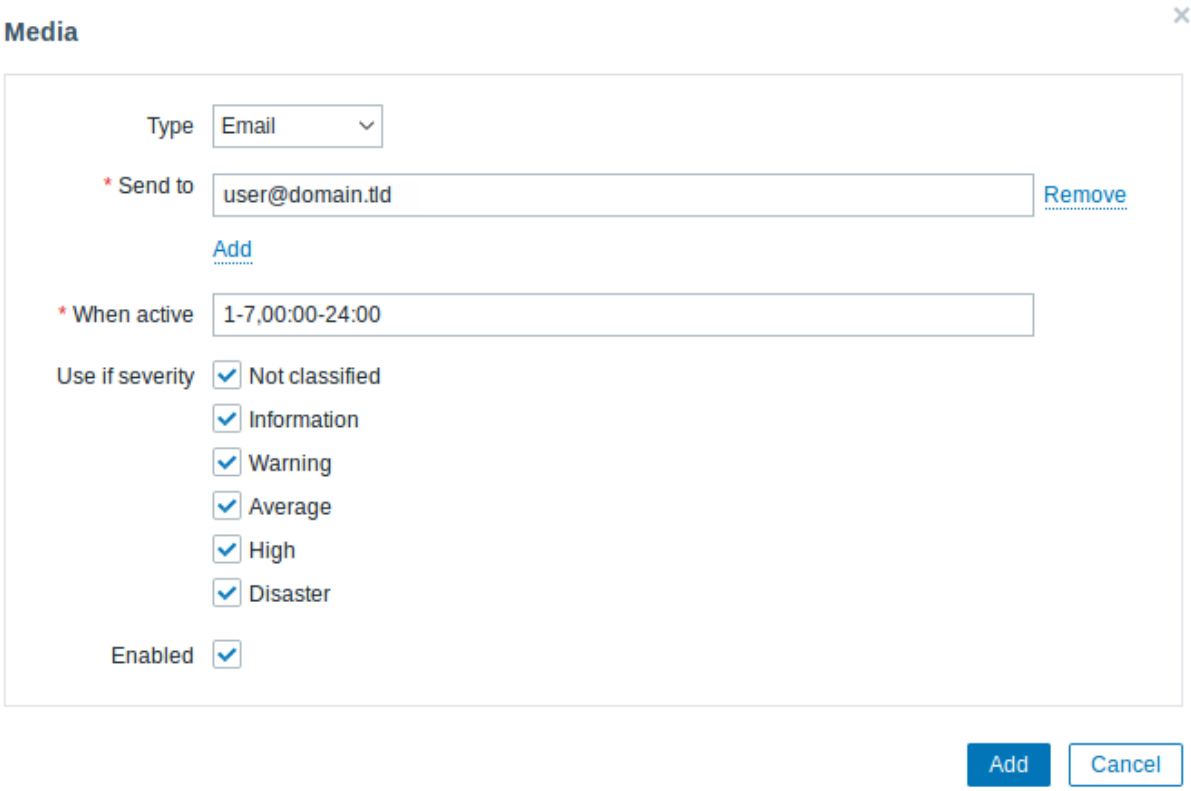
Wszystkie obowiązkowe pola wejściowe są oznaczone czerwoną gwiazdką. Szczegółowe informacje o polach wejściowych w tym formularzu konfiguracji można znaleźć na stronie Ustawienia użytkownika.

Domyślnie nowi użytkownicy nie mają zdefiniowanych żadnych mediów (metod dostarczania powiadomień). Aby je utworzyć, przejdź do zakładki „Media” i kliknij *Add*.



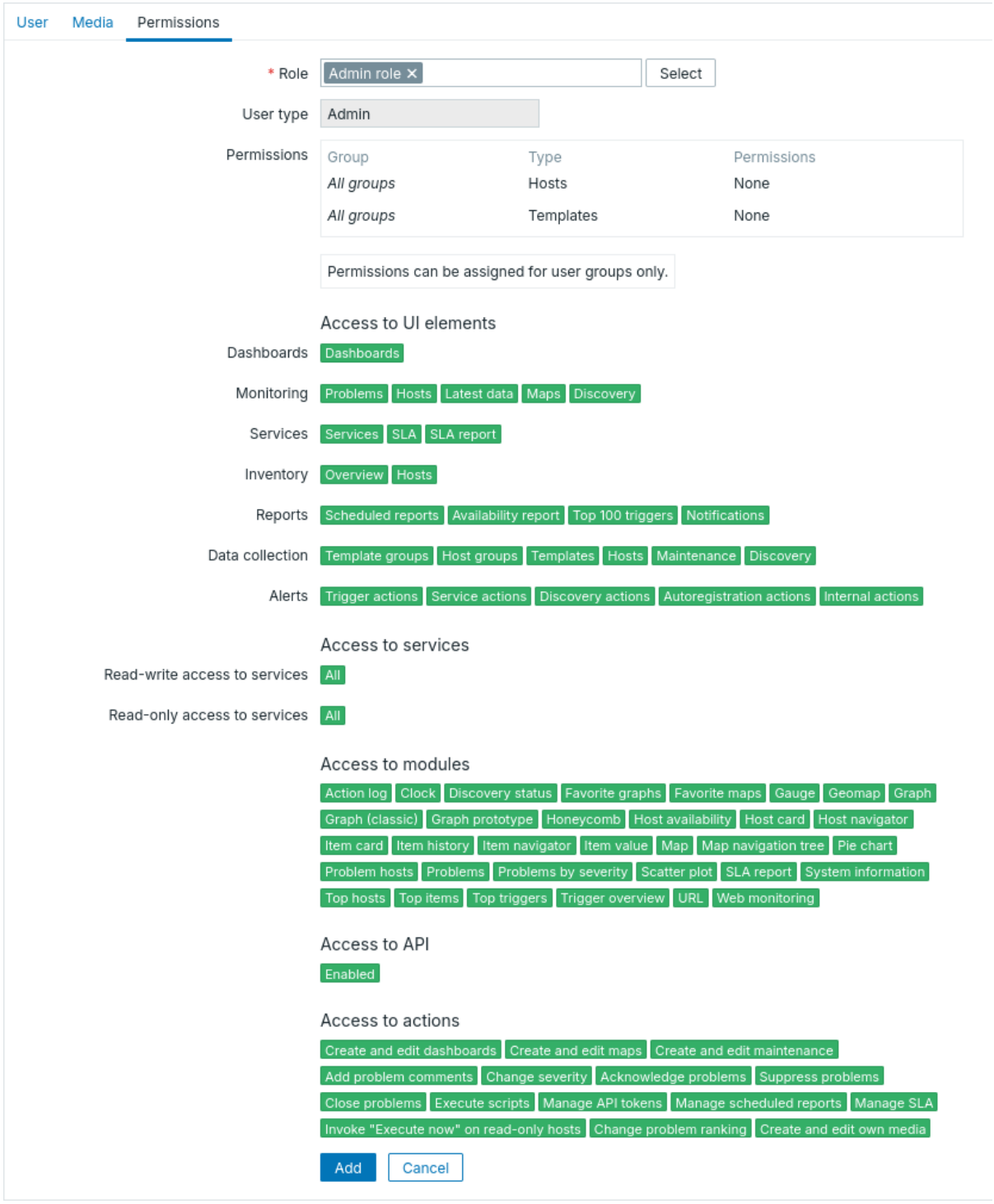
W wyskakującym oknie wprowadź adres e-mail użytkownika.

Możesz określić przedział czasu, w którym medium będzie aktywne (opis formatu znajduje się na stronie Specyfikacja przedziału czasu). Domyślnie medium jest zawsze aktywne. Możesz także dostosować poziomy ważności wyzwalacza, dla których medium będzie aktywne, ale na razie pozostaw wszystkie włączone.



Kliknij *Add*, aby zapisać medium, a następnie przejdź do zakładki Uprawnienia.

Zakładka Uprawnienia zawiera obowiązkowe pole *Role*. Rola określa, które elementy frontend użytkownik może wyświetlać i jakie działania może wykonywać. Naciśnij Select i wybierz jedną z ról z listy. Na przykład wybierz *Admin role*, aby zezwolić na dostęp do wszystkich sekcji frontend Zabbix z wyjątkiem Administracji. Później możesz zmodyfikować uprawnienia lub utworzyć więcej ról użytkowników. Po wybraniu roli uprawnienia pojawią się w tej samej zakładce:

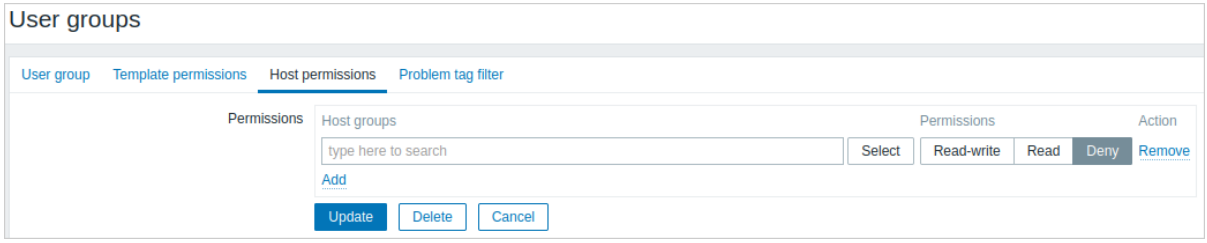


Kliknij *Add* w formularzu właściwości użytkownika, aby zapisać użytkownika. Nowy użytkownik pojawi się na liście użytkowników.



Dodawanie uprawnień

Domyślnie nowy użytkownik nie ma żadnych uprawnień dostępu do hostów i szablonów. Aby nadać użytkownikowi uprawnienia, kliknij grupę użytkownika w kolumnie *Groups* (w tym przypadku — „Zabbix administrators"). W formularzu właściwości *User groups* przejdź do zakładki *Host permissions*, aby przypisać uprawnienia do grup hostów. Kliknij Add, aby wyświetlić pole wyboru grupy hostów:



Następnie kliknij *Select* obok pola, aby zobaczyć listę grup hostów. Ten użytkownik ma mieć dostęp tylko do odczytu do grupy *Linux servers*, więc zaznacz odpowiednie pole wyboru na liście i kliknij *Select*, aby potwierdzić wybór.



Kliknij przycisk *Read*, aby ustawić poziom uprawnień, a następnie *Update*, aby zapisać zmiany wprowadzone w konfiguracji grupy użytkowników.

Aby nadać uprawnienia do szablonów, należy przejść do zakładki *Template permissions* i określić grupy szablonów. Kroki są identyczne jak przy przypisywaniu uprawnień do grup hostów. Przegląd szablonów jest dostępny w sekcji New template tego przewodnika Quickstart.

Attention:
W Zabbix prawa dostępu do hostów i szablonów są przypisywane do grup użytkowników, a nie do poszczególnych użytkowników.

Gotowe! Możesz spróbować zalogować się przy użyciu danych logowania nowego użytkownika.

2 Nowy host

Przegląd

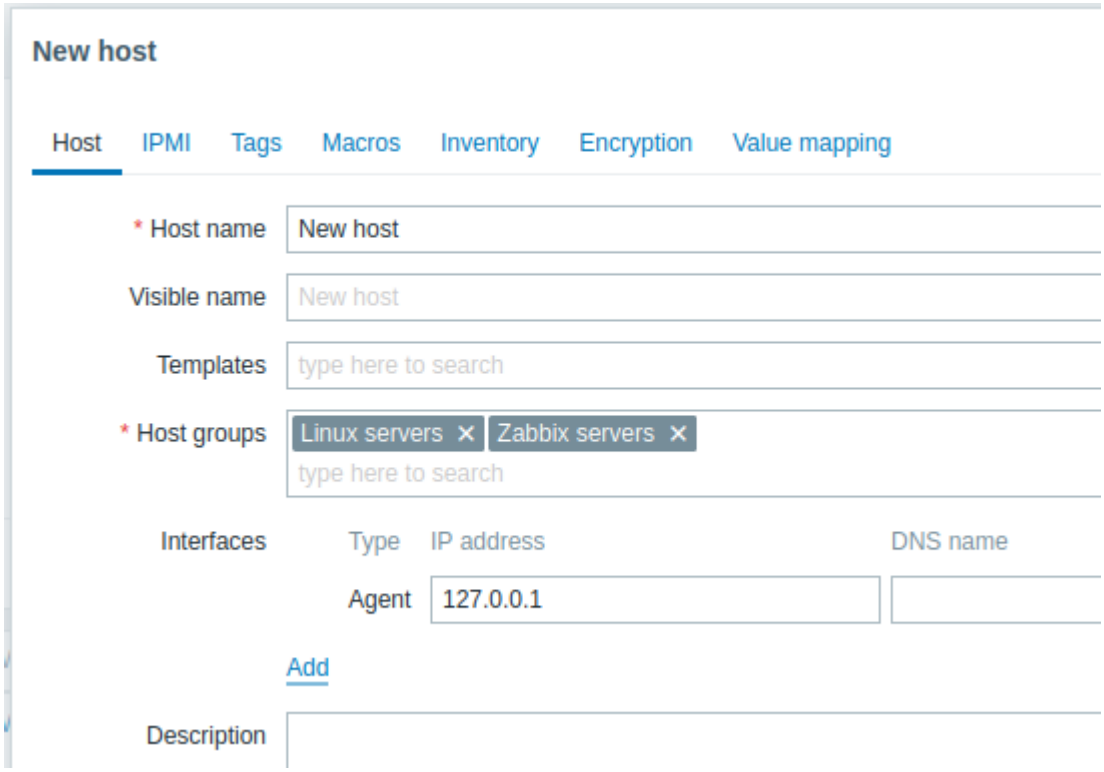
W tej sekcji dowiesz się, jak skonfigurować nowy host.

Host w Zabbix to element sieci (fizyczny, wirtualny), który chcesz monitorować. Definicja tego, czym może być „host” w Zabbix, jest dość elastyczna. Może to być fizyczny serwer, przełącznik sieciowy, maszyna wirtualna lub jakaś aplikacja.

Dodawanie hosta

Informacje o skonfigurowanych hostach w Zabbix są dostępne w sekcjach menu *Data collection* > *Hosts* oraz *Monitoring* > *Hosts*. Jeden predefiniowany host o nazwie „Zabbix server” już istnieje, ale chcemy nauczyć się dodawać kolejny.

Aby dodać nowy host, kliknij *Create host*. Zostanie otwarty formularz konfiguracji hosta.



Wszystkie obowiązkowe pola wejściowe są oznaczone czerwoną gwiazdką.

Minimalny zakres danych, które należy tutaj wprowadzić, to:

Host name

- Wprowadź nazwę hosta. Dozwolone są znaki alfanumeryczne, spacje, kropki, myślniki oraz podkreślenia.

Host groups

- Wybierz jedną lub kilka istniejących grup, klikając przycisk *Select*, albo wprowadź nazwę nieistniejącej grupy, aby utworzyć nową grupę.

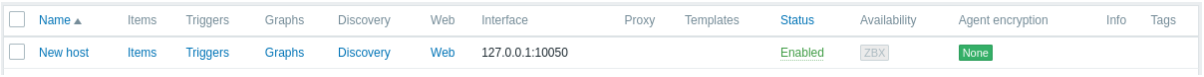
Note:
Wszystkie uprawnienia dostępu są przypisywane do grup hostów, a nie do poszczególnych hostów. Dlatego host musi należeć do co najmniej jednej grupy.

Interfaces: IP address

- Chociaż technicznie nie jest to pole wymagane, interfejs hosta jest niezbędny do zbierania niektórych metryk. Aby używać pasywnych kontroli Zabbix agent, podaj w tym polu adres IP lub DNS agenta. Pamiętaj, że w pliku konfiguracyjnym Zabbix agent należy również określić adres IP lub DNS serwera Zabbix w dyrektywie 'Server'. Jeśli Zabbix agent i serwer Zabbix są zainstalowane na tej samej maszynie, musisz podać ten sam adres IP/DNS w obu miejscach.

Inne opcje można pozostawić bez zmian, używając ich wartości domyślnych.

Po zakończeniu kliknij *Add*. Nowy host powinien być widoczny na liście hostów.



Kolumna Availability zawiera wskaźniki dostępności hosta dla każdego interfejsu. Zdefiniowaliśmy interfejs Zabbix agent, więc możemy użyć ikony dostępności agenta (z napisem „ZBX"), aby określić dostępność hosta:

- ZBX - status hosta nie został jeszcze ustalony; nie wykonano jeszcze żadnej kontroli metryki
- ZBX - host jest dostępny, kontrola metryki zakończyła się powodzeniem
- ZBX - host jest niedostępny, kontrola metryki zakończyła się niepowodzeniem (najedź kursorem myszy na ikonę, aby zobaczyć komunikat o błędzie). Może występować problem z komunikacją, prawdopodobnie spowodowany nieprawidłowymi poświadczeniami interfejsu. Sprawdź, czy serwer Zabbix jest uruchomiony, a następnie spróbuj również odświeżyć stronę później.

3 Nowa pozycja

Przegląd

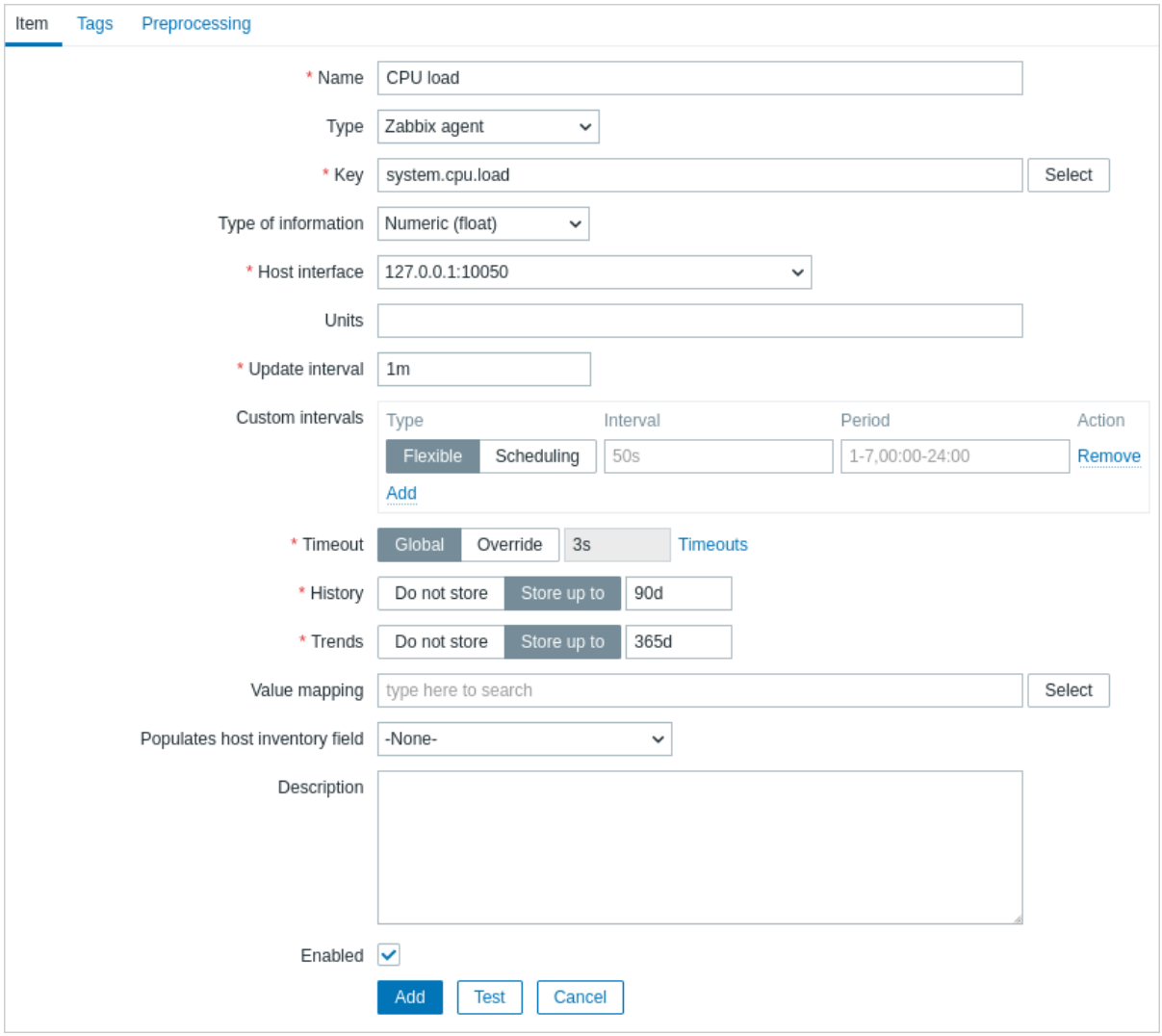
W tej sekcji dowiesz się, jak skonfigurować pozycję.

Pozycje stanowią podstawę zbierania danych w Zabbix. Bez pozycji nie ma danych — ponieważ tylko pozycja definiuje pojedynczą metrykę lub określa, jaki rodzaj danych należy zbierać z hosta.

Dodawanie pozycji

Wszystkie pozycje są pogrupowane wokół hostów. Dlatego, aby skonfigurować przykładową pozycję, przechodzimy do *Data collection* > *Hosts* i znajdujemy utworzony przez nas „New host”.

Kliknij łącze *Items* w wierszu „New host”, a następnie kliknij *Create item*. Zostanie otwarty formularz konfiguracji pozycji.



Wszystkie obowiązkowe pola wejściowe są oznaczone czerwoną gwiazdką.

Dla naszej przykładowej pozycji należy wprowadzić następujące podstawowe informacje:

Name

- Wprowadź wartość *CPU load*. Będzie to nazwa pozycji wyświetlana na listach i w innych miejscach.

Key

- Ręcznie wprowadź wartość *system.cpu.load*. Jest to techniczna nazwa pozycji, która identyfikuje typ informacji, jakie będą zbierane. Ten konkretny klucz jest tylko jednym ze wstępnie zdefiniowanych kluczy dostarczanych z Zabbix agent.

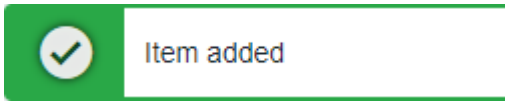
Type of information

- Ten atrybut określa format oczekiwanych danych. Dla klucza *system.cpu.load* to pole zostanie automatycznie ustawione na *Numeric (float)*.

Note:
Możesz także zmniejszyć liczbę dni przechowywania historii pozycji do 7 lub 14. Jest to dobra praktyka, która odciąża bazę danych od przechowywania dużej liczby wartości historycznych.

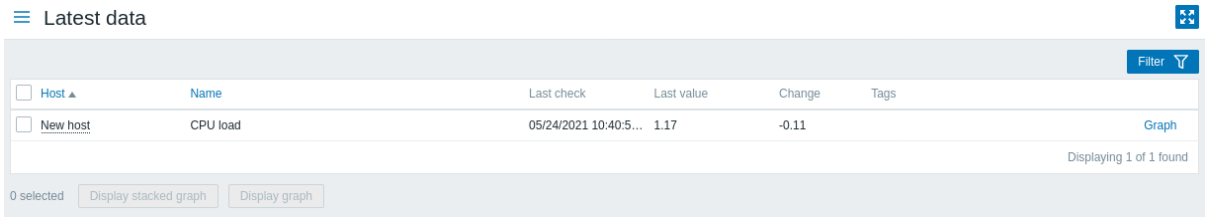
Inne opcje można pozostawić bez zmian, używając ich wartości domyślnych.

Po zakończeniu kliknij *Add*. Nowa pozycja powinna pojawić się na liście pozycji i powinien zostać wyświetlony komunikat o powodzeniu.



Przeglądanie danych

Po zdefiniowaniu pozycji możesz chcieć sprawdzić, czy rzeczywiście zbiera dane. W tym celu przejdź do *Monitoring* > *Latest data*, wybierz 'New host' w filtrze i kliknij *Apply*.



Warto jednak pamiętać, że pojawienie się pierwszych danych może zająć do 60 sekund. Domyślnie właśnie z taką częstotliwością serwer odczytuje zmiany w konfiguracji i wykrywa nowe pozycje do wykonania.

Jeśli w kolumnie 'Change' nie widzisz żadnej wartości, być może do tej pory odebrano tylko jedną wartość. Poczekaj 30 sekund, aż nadejdzie kolejna wartość.

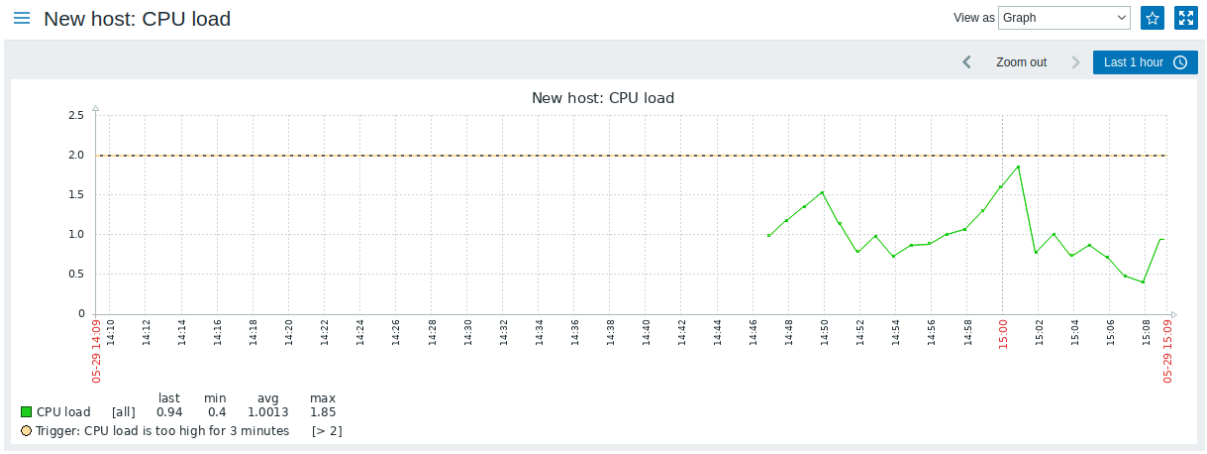
Jeśli nie widzisz informacji o pozycji tak jak na zrzucie ekranu, upewnij się, że:

- pola 'Key' i 'Type of information' w pozycji zostały wypełnione dokładnie tak, jak na zrzucie ekranu;
- zarówno agent, jak i serwer są uruchomione;
- status hosta to 'Monitored', a ikona jego dostępności jest zielona;
- host wybrany w filtrze hostów jest prawidłowy;
- pozycja jest włączona.

Wykresy

Gdy pozycja działa już od pewnego czasu, być może nadszedł moment, aby zobaczyć coś wizualnego. Proste wykresy są dostępne dla każdej monitorowanej numerycznej pozycji bez żadnej dodatkowej konfiguracji. Wykresy te są generowane w czasie działania.

Aby wyświetlić wykres, przejdź do *Monitoring* > *Latest data* i kliknij odnośnik „Graph" obok pozycji.



4 Nowy wyzwalacz

Przegląd

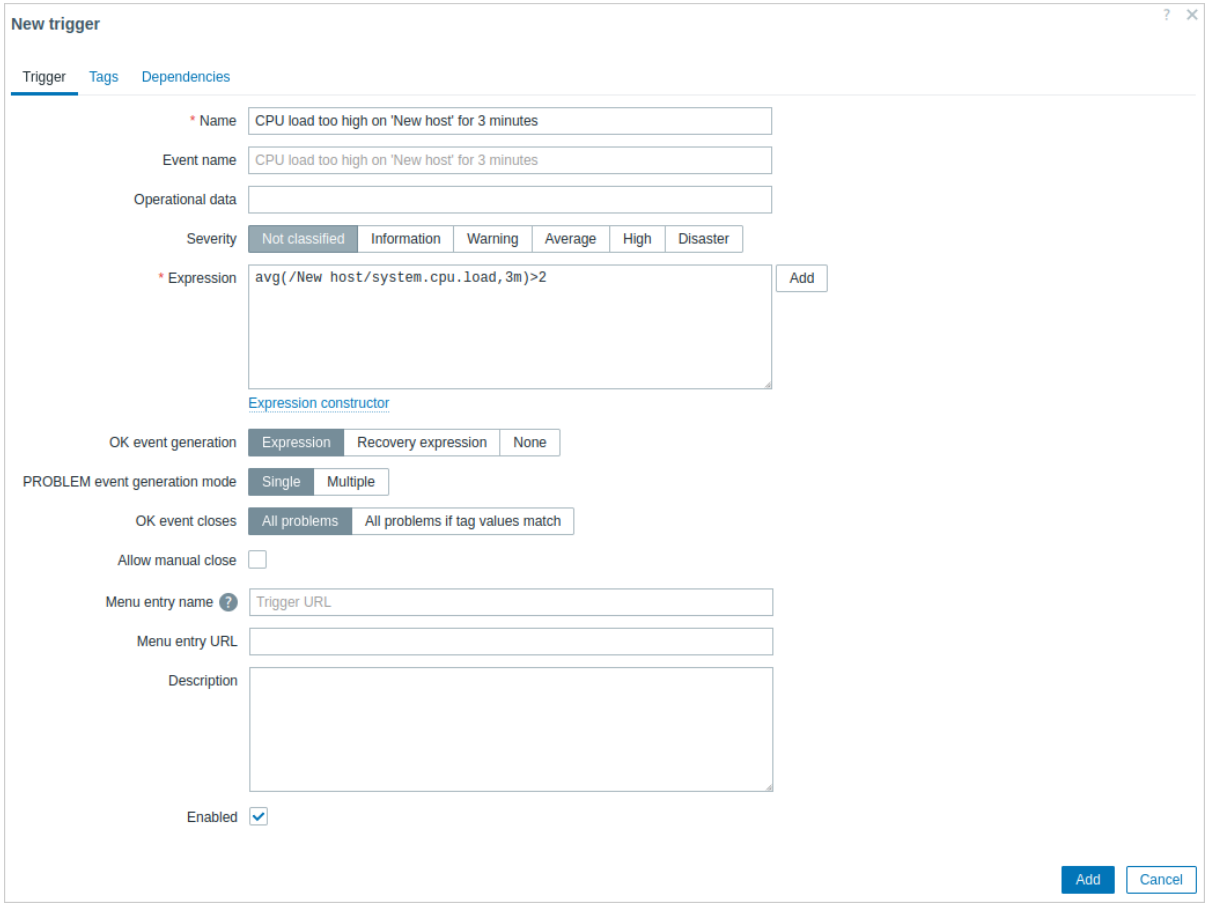
W tej sekcji dowiesz się, jak skonfigurować wyzwalacz.

Pozycje jedynie zbierają dane. Aby automatycznie oceniać napływające dane, musimy zdefiniować wyzwalacze. Wyzwalacz zawiera wyrażenie, które określa próg akceptowalnego poziomu danych.

Jeśli ten poziom zostanie przekroczony przez napływające dane, wyzwalacz „uruchomi się" lub przejdzie do stanu „Problem" — wskazując, że wydarzyło się coś, co może wymagać uwagi. Gdy poziom ponownie będzie akceptowalny, wyzwalacz wróci do stanu „Ok".

Dodawanie wyzwalacza

Aby skonfigurować wyzwalacz dla naszej pozycji, przejdź do *Data collection* > *Hosts*. Kliknij łącze *Triggers* w wierszu „New host", a następnie kliknij *Create trigger*. Zostanie otwarty formularz konfiguracji wyzwalacza.



W przypadku naszego wyzwalacza należy tutaj wprowadzić następujące podstawowe informacje:

Nazwa

- Wprowadź *CPU load too high on 'New host' for 3 minutes* jako wartość. Będzie to nazwa wyzwalacza wyświetlana na listach i w innych miejscach.

Wyrażenie

- Wprowadź: avg(/New host/system.cpu.load,3m)>2

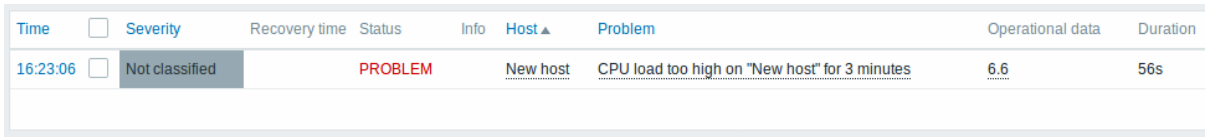
Jest to wyrażenie wyzwalacza. Upewnij się, że wyrażenie zostało wprowadzone poprawnie, aż do ostatniego znaku. Klucz pozycji (system.cpu.load) jest tutaj używany do odwołania się do pozycji. To konkretne wyrażenie zasadniczo oznacza, że próg problemu zostaje przekroczony, gdy średnia wartość obciążenia CPU z 3 minut jest większa niż 2. Więcej informacji można znaleźć w sekcji składnia wyrażeń wyzwalaczy.

Po zakończeniu kliknij *Add*. Nowy wyzwalacz powinien pojawić się na liście wyzwalaczy.

Wyświetlanie stanu wyzwalacza

Po zdefiniowaniu wyzwalacza możesz chcieć sprawdzić jego stan.

Jeśli obciążenie CPU przekroczyło poziom progu zdefiniowany w wyzwalaczu, problem będzie wyświetlany w *Monitoring* > *Problems*.



Miganie w kolumnie statusu wskazuje na niedawną zmianę stanu wyzwalacza, która nastąpiła w ciągu ostatnich 30 minut.

5 Otrzymywanie powiadomienia o problemie

Przegląd

W tej sekcji dowiesz się, jak skonfigurować alerty w formie powiadomień w Zabbix.

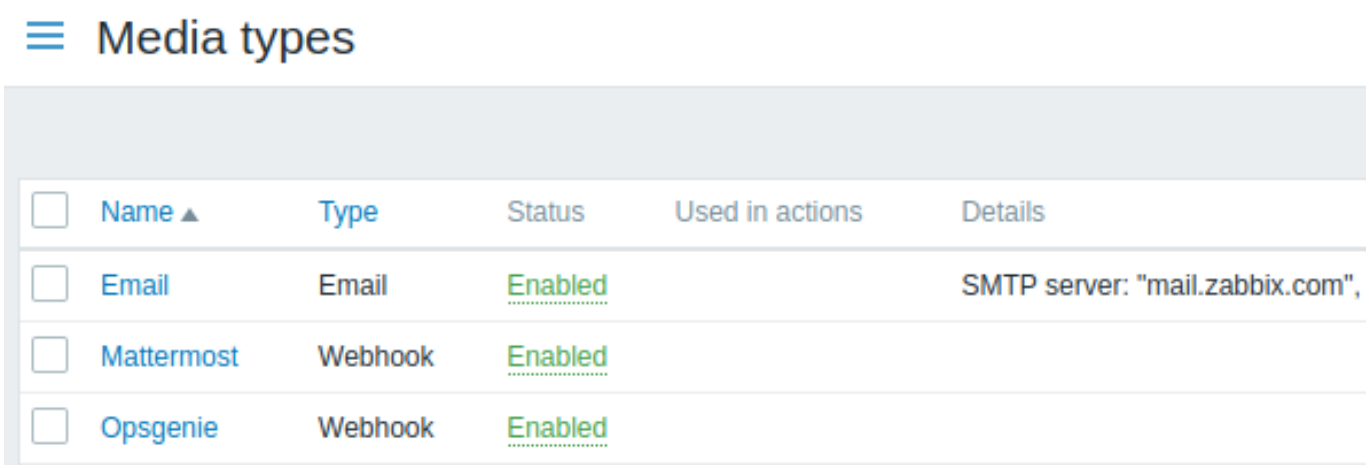
Gdy pozycje zbierają dane, a wyzwalacze są zaprojektowane tak, aby „uruchamiać się" w sytuacjach problemowych, przydatne jest również posiadanie mechanizmu alertowania, który będzie informował o ważnych zdarzeniach, nawet gdy frontend Zabbix nie jest aktywnie sprawdzany.

Temu właśnie służą powiadomienia. Ponieważ e-mail jest najpopularniejszą metodą dostarczania powiadomień o problemach, nauczymy się, jak skonfigurować powiadomienie e-mail.

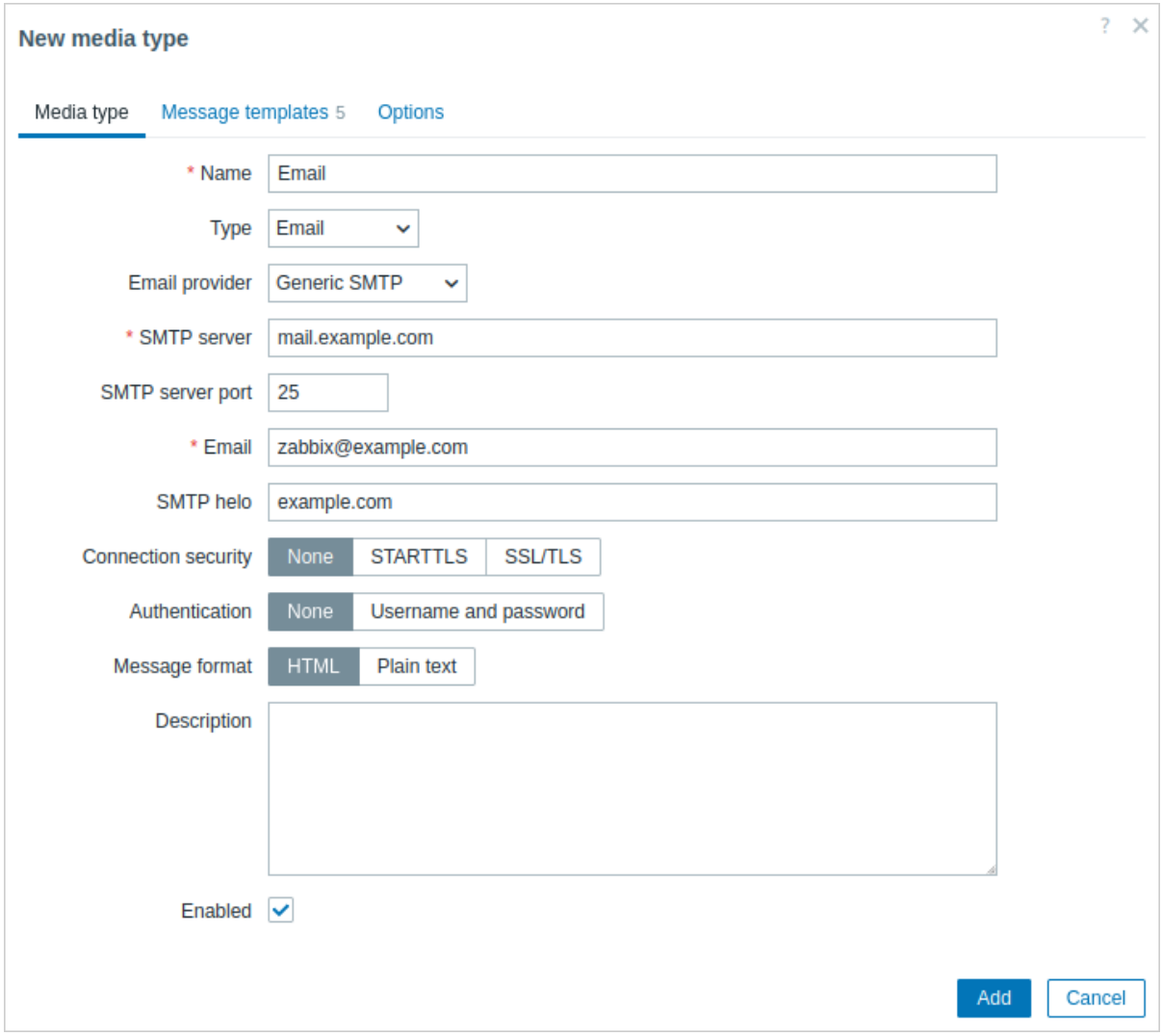
Ustawienia e-mail

Początkowo w Zabbix dostępnych jest kilka predefiniowanych metod dostarczania powiadomień. Email jest jedną z nich.

Aby skonfigurować ustawienia e-mail, przejdź do *Alerts* > *Media types* i kliknij *Email* na liście predefiniowanych typów mediów.



Otworzy się formularz konfiguracji ustawień e-mail.



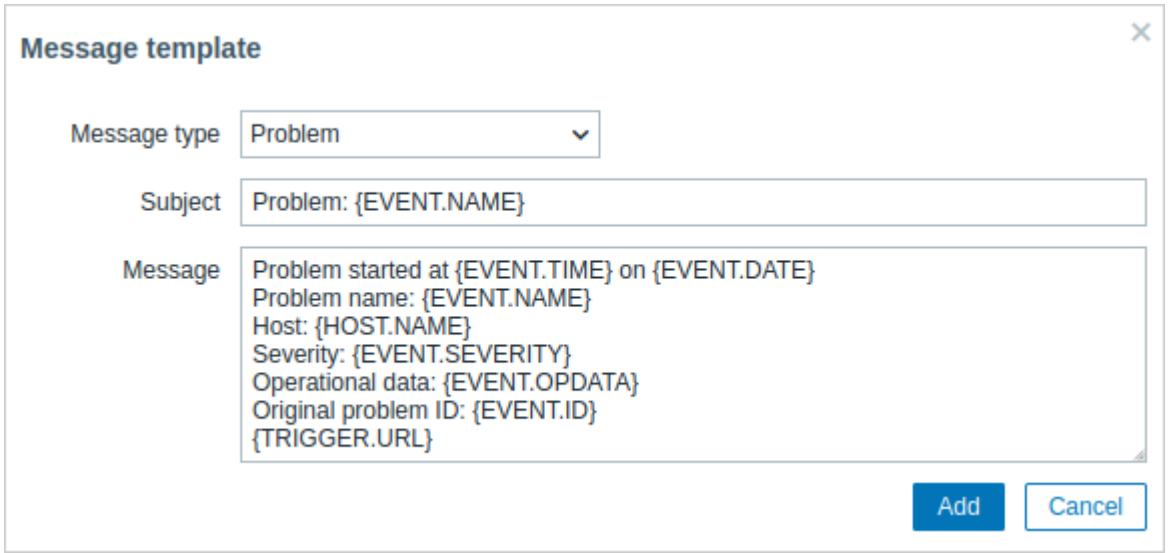
Wszystkie wymagane pola wejściowe są oznaczone czerwoną gwiazdką.

Na karcie *Media type* ustaw wartości *SMTP server*, *SMTP helo* oraz *Email* odpowiednio do swojego środowiska.

Note:
Wartość w polu *Email* będzie używana jako adres „From" dla powiadomień wysyłanych z Zabbix.

Następnie należy zdefiniować treść wiadomości o problemie. Treść jest definiowana za pomocą szablonu wiadomości, konfigurowanego na karcie *Message templates*.

Kliknij *Add*, aby utworzyć szablon wiadomości, i wybierz *Problem* jako typ wiadomości.

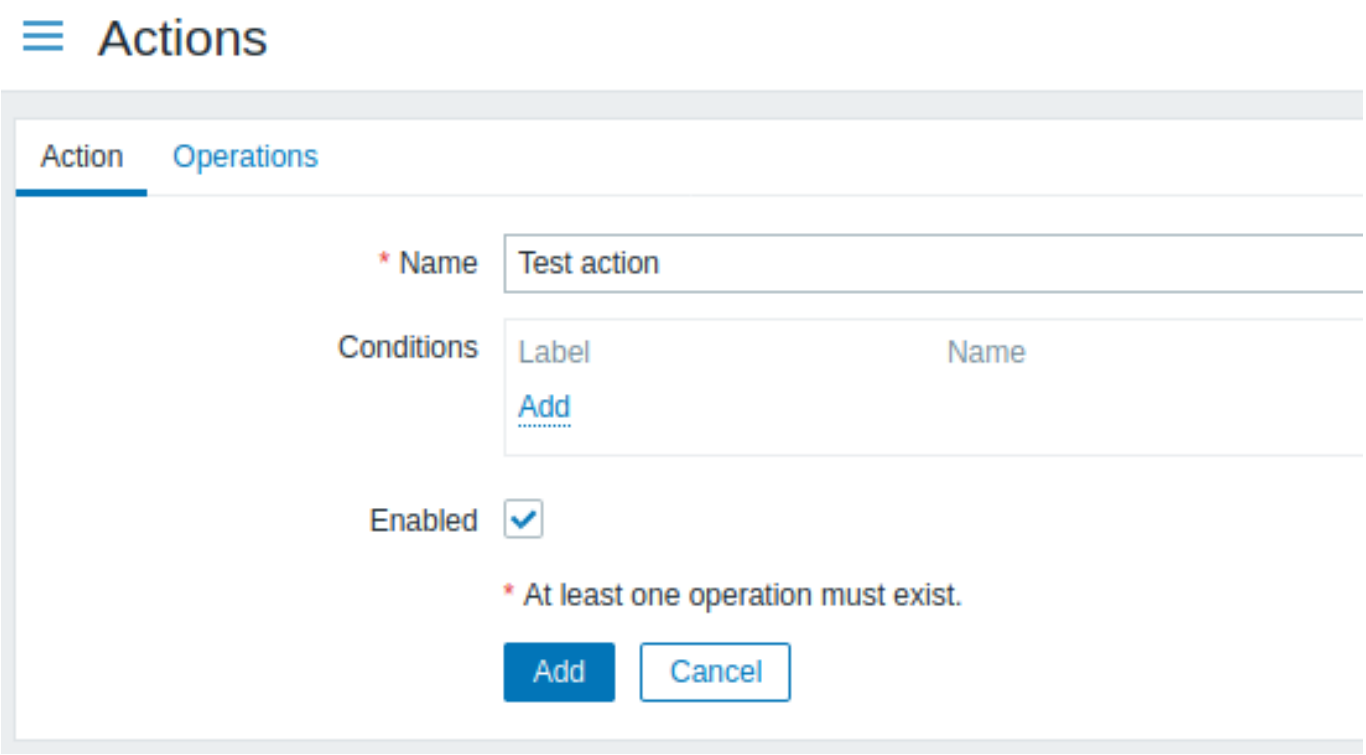


Po zakończeniu kliknij *Add* i zapisz formularz.

Teraz masz skonfigurowany *Email* jako działający typ mediów. Typ mediów musi być również powiązany z użytkownikami przez zdefiniowanie konkretnych adresów dostarczania (tak jak zrobiliśmy to podczas konfigurowania nowego użytkownika), w przeciwnym razie nie będzie używany.

Nowa akcja

Dostarczanie powiadomień jest jedną z rzeczy, które akcje wykonują w Zabbix. Dlatego, aby skonfigurować powiadomienie, przejdź do *Alerty* > *Akcje* > *Akcje wyzwalaczy* i kliknij *Utwórz akcję*.

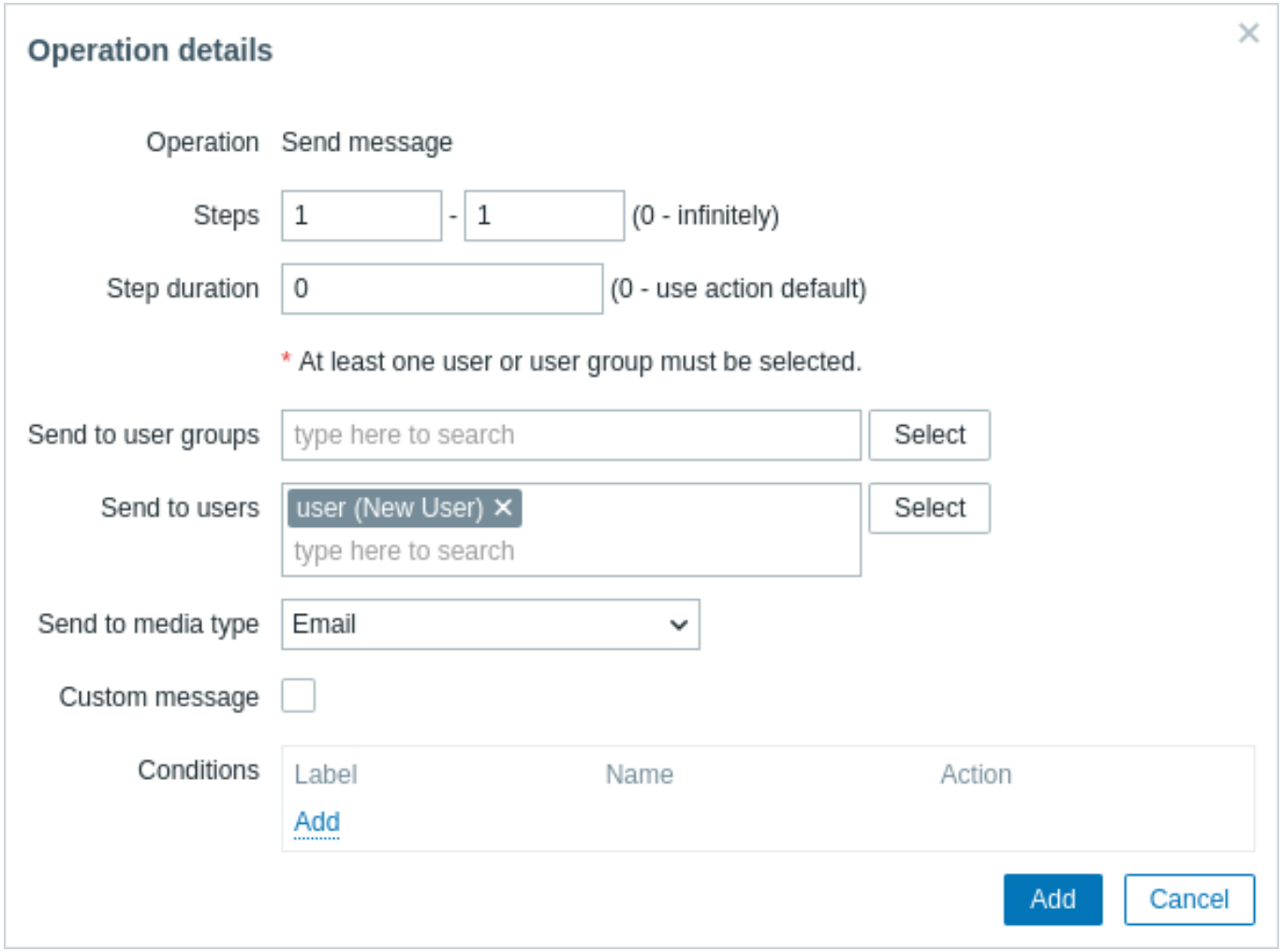


Wszystkie obowiązkowe pola wejściowe są oznaczone czerwoną gwiazdką.

W tym formularzu wprowadź nazwę akcji.

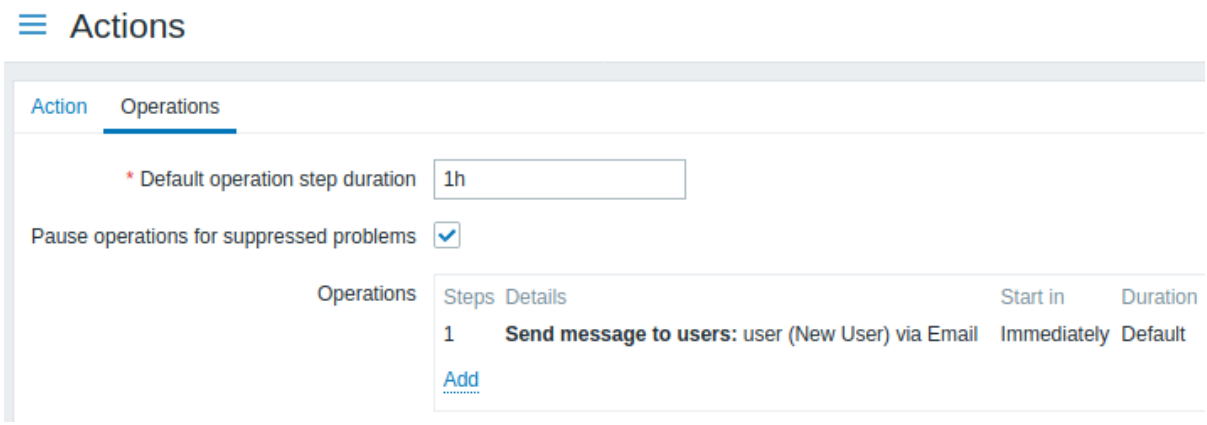
W najprostszym przypadku, jeśli nie dodamy żadnych bardziej szczegółowych warunków, akcja zostanie wykonana przy każdej zmianie wyzwalacza ze stanu „Ok" na „Problem".

Nadal musimy określić, co akcja ma zrobić — i robi się to na karcie *Operacje*. Kliknij *Dodaj* w bloku *Operacje*, co otworzy nowy formularz operacji.



Wszystkie obowiązkowe pola wejściowe są oznaczone czerwoną gwiazdką.

Tutaj kliknij *Wybierz* w bloku *Wyślij do użytkowników* i wybierz użytkownika („user"), którego zdefiniowaliśmy. Wybierz „Email" jako wartość pola *Wyślij do typu mediów*. Po wykonaniu tej czynności kliknij *Dodaj*, a operacja powinna zostać dodana:



To wszystko w przypadku prostej konfiguracji akcji, więc kliknij *Dodaj* w formularzu akcji.

Otrzymywanie powiadomienia

Teraz, gdy skonfigurowano dostarczanie powiadomień, dobrze byłoby faktycznie jakieś otrzymać. Aby w tym pomóc, możemy celowo zwiększyć obciążenie naszego hosta — tak, aby nasz wyzwalacz „uruchomił się" i abyśmy otrzymali powiadomienie o problemie.

Otwórz konsolę na swoim hoście i uruchom:

```
cat /dev/urandom | md5sum
```

Możesz uruchomić jeden lub kilka takich procesów.

Teraz przejdź do *Monitoring* > *Latest data* i zobacz, jak wzrosły wartości „CPU Load". Pamiętaj, że aby nasz wyzwalacz „uruchomił się", wartość „CPU Load" musi przez 3 kolejne minuty przekraczać „2". Gdy tak się stanie:

- w *Monitoring* > *Problems* powinien być widoczny wyzwalacz z migającym stanem `Problem`;
- powinieneś otrzymać powiadomienie o problemie na swój adres e-mail.

Attention:
Jeśli powiadomienia nie działają:
- sprawdź ponownie, czy zarówno ustawienia e-mail, jak i akcja zostały poprawnie skonfigurowane
- upewnij się, że utworzony użytkownik ma co najmniej uprawnienia do odczytu dla hosta, który wygenerował zdarzenie, zgodnie z opisem w kroku *Adding user*. Użytkownik, jako członek grupy użytkowników „Zabbix administrators", musi mieć co najmniej dostęp do odczytu do grupy hostów „Linux servers", do której należy nasz host.
- Dodatkowo możesz sprawdzić dziennik akcji, przechodząc do *Reports* > *Action log*.

6 Nowy szablon

Przegląd

W tej sekcji dowiesz się, jak skonfigurować szablon.

Wcześniej omówiliśmy, jak skonfigurować pozycję, wyzwalacz oraz jak otrzymywać powiadomienia o problemach dla hosta.

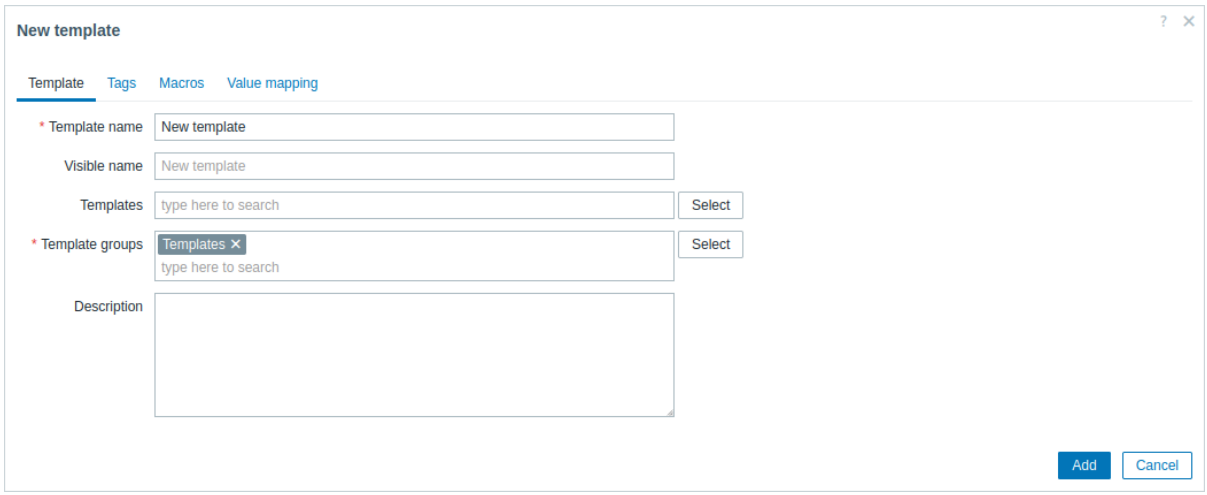
Chociaż wszystkie te kroki same w sobie oferują dużą elastyczność, może się wydawać, że jest ich zbyt wiele, jeśli trzeba je wykonać na przykład dla tysiąca hostów. Przydałaby się pewna automatyzacja.

W tym miejscu z pomocą przychodzą szablony. Szablony umożliwiają grupowanie przydatnych pozycji, wyzwalaczy i innych elementów, tak aby można je było wielokrotnie wykorzystywać przez zastosowanie ich do hostów w jednym kroku.

Gdy szablon jest podłączony do hosta, host dziedziczy wszystkie elementy szablonu. Oznacza to, że w praktyce można bardzo szybko zastosować wcześniej przygotowany zestaw kontroli.

Dodawanie szablonu

Aby rozpocząć pracę z szablonami, musimy najpierw utworzyć szablon. W tym celu w *Data collection* > *Templates* kliknij *Create template*. Spowoduje to wyświetlenie formularza konfiguracji szablonu.



Wszystkie obowiązkowe pola wejściowe są oznaczone czerwoną gwiazdką.

Wymagane parametry, które należy tutaj wprowadzić, to:

Nazwa szablonu

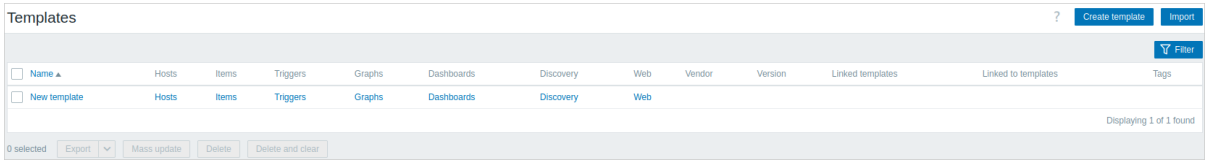
- Wprowadź nazwę szablonu. Dozwolone są znaki alfanumeryczne, spacje i podkreślenia.

Grupy szablonów

- Wybierz jedną lub kilka grup, klikając przycisk *Select*. Szablon musi należeć do grupy.

Note:
Uprawnienia dostępu do grup szablonów są przypisywane w konfiguracji grupy użytkowników na karcie **Template permissions** w taki sam sposób jak uprawnienia do hostów. Wszystkie uprawnienia dostępu są przypisywane do grup, a nie do poszczególnych szablonów, dlatego uwzględnienie szablonu w co najmniej jednej grupie jest obowiązkowe.

Po zakończeniu kliknij *Add*. Twój nowy szablon powinien być widoczny na liście szablonów. Możesz także użyć filtra, aby znaleźć swój szablon.



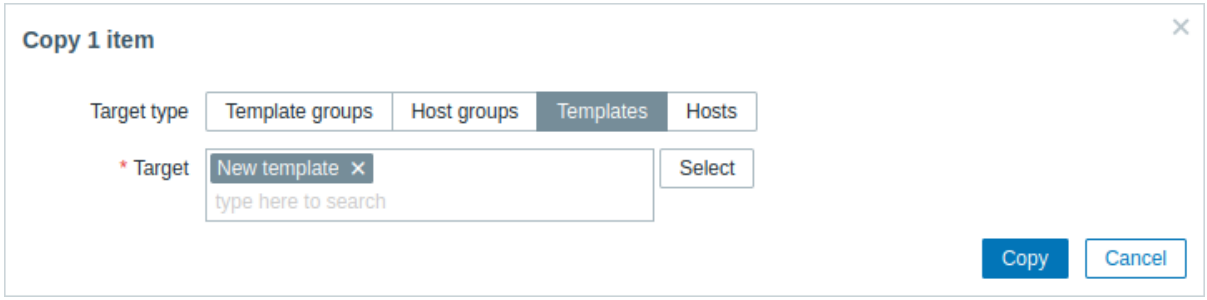
Jak widać, szablon jest na liście, ale nic jeszcze nie zawiera — nie ma w nim pozycji, wyzwalaczy ani innych elementów.

Dodawanie pozycji do szablonu

Aby dodać pozycję do szablonu, otwórz listę pozycji dla „New host”, przechodząc do *Data collection* → *Hosts* i klikając *Items* obok „New host”.

Następnie:

- Zaznacz pole wyboru przy pozycji „CPU Load” na liście.
- Kliknij *Copy* pod listą.
- Wybierz kartę *Templates*.
- Wybierz szablon, do którego chcesz skopiować pozycję.



Wszystkie wymagane pola wejściowe są oznaczone czerwoną gwiazdką.

- Kliknij *Copy*.

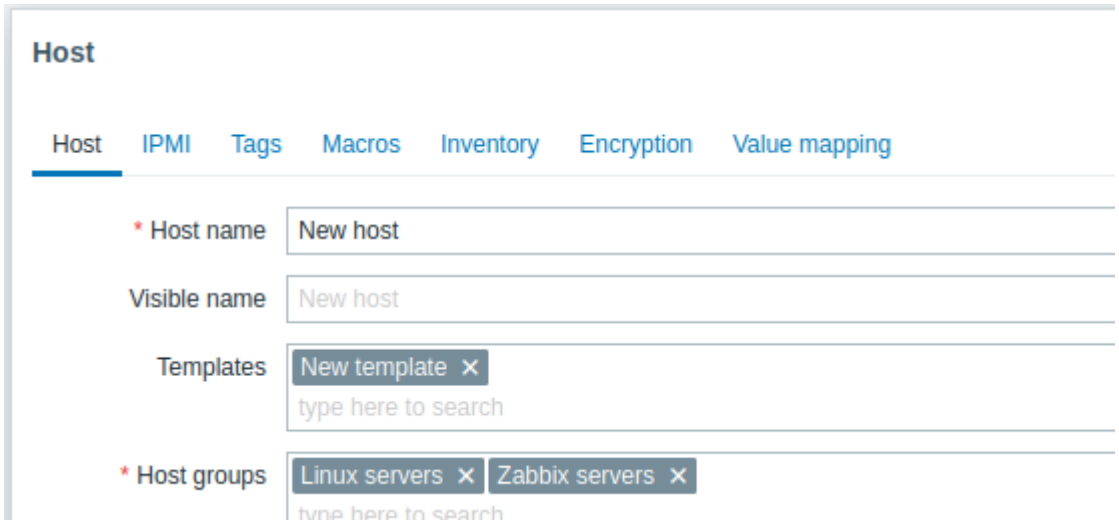
Jeśli teraz przejdziesz do *Data collection* > *Templates*, „New template” powinien zawierać jedną nową pozycję.

Na razie poprzestaniemy tylko na jednej pozycji, ale w podobny sposób możesz dodać do szablonu dowolne inne pozycje, wyzwalacze lub inne elementy, aż stanie się on dość kompletnym zestawem elementów do danego celu (monitorowanie systemu operacyjnego, monitorowanie pojedynczej aplikacji).

Podłączanie szablonu do hosta

Gdy szablon jest już gotowy, pozostaje tylko dodać go do hosta. W tym celu przejdź do *Data collection* > *Hosts*, kliknij „New host”, aby otworzyć formularz konfiguracji, i znajdź pole **Templates**.

Zacznij wpisywać *New template* w polu *Templates*. Nazwa szablonu, który utworzyliśmy, powinna pojawić się na liście rozwijanej. Przewiń w dół, aby ją wybrać. Zobacz, że pojawi się ona w polu *Templates*.



Kliknij *Update* w formularzu, aby zapisać zmiany. Szablon jest teraz dodany do hosta wraz ze wszystkimi encjami, które zawiera.

W ten sposób można go zastosować również do dowolnego innego hosta. Wszelkie zmiany w pozycjach, wyzwalaczach i innych encjach na poziomie szablonu będą propagowane do hostów, do których szablon jest podłączony.

Podłączanie predefiniowanych szablonów do hostów

Jak zapewne zauważyłeś, Zabbix jest dostarczany z zestawem predefiniowanych szablonów dla różnych systemów operacyjnych, urządzeń i aplikacji. Aby bardzo szybko rozpocząć monitorowanie, możesz podłączyć odpowiedni z nich do hosta, ale pamiętaj, że te szablony wymagają dostrojenia do Twojego środowiska. Niektóre kontrole mogą nie być potrzebne, a interwały odpytywania mogą być zdecydowanie zbyt częste.

Dostępne są również bardziej szczegółowe informacje o szablonach.

Monitorowanie serwera WWW Apache

Aby rozpocząć monitorowanie serwera WWW Apache, wykonaj następujące kroki:

1. Upewnij się, że masz dostęp do statystyk Apache.
2. Zastosuj szablon monitorowania Apache.
3. Sprawdź najnowsze dane.

Aby skorzystać z tego przewodnika, musisz mieć zainstalowany serwer Zabbix oraz interfejs WWW installed. Musisz być zalogowany do Zabbix jako domyślny użytkownik *Admin*.

Dostęp do statystyk Apache

Celem tego kroku jest upewnienie się, że statystyki serwera WWW Apache mogą być odczytywane przez Zabbix.

W Apache informacje w czasie rzeczywistym o wydajności i aktywności serwera są udostępniane przez wbudowany moduł `mod_status`. Po jego włączeniu tworzona jest dostępna przez WWW strona (zwykle pod adresem `/server-status`) wyświetlająca dane o wydajności i aktywności.

Aby sprawdzić, czy `mod_status` jest włączony dla serwera WWW Apache, uruchom:

W Debian/Ubuntu	W systemach opartych na RHEL
`apache2ctl -M | grep status`	`httpd -M | grep status`

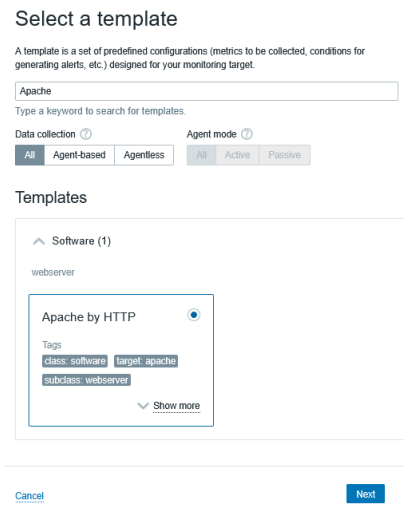
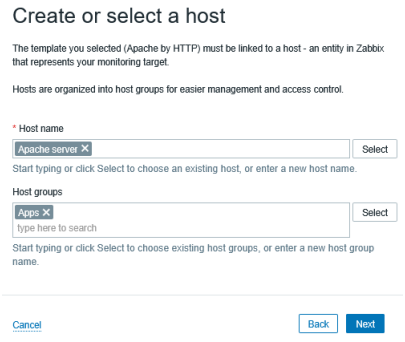
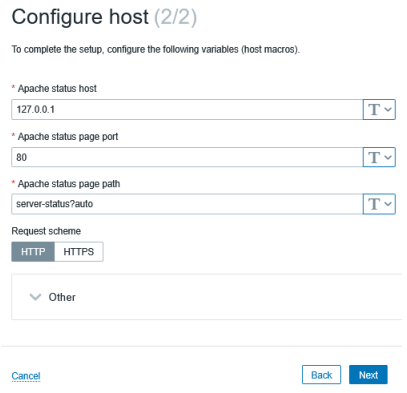
Jeśli w danych wyjściowych widzisz "`status_module (shared)`", oznacza to, że moduł statusu jest już włączony. Jeśli nie, musisz włączyć moduł statusu.

Zastosowanie szablonu monitorowania Apache

W Zabbix ten szablon jest gotowy do użycia. Zawiera wstępnie skonfigurowane elementy gotowe do zbierania danych, wizualizacji i analizy.

Aby zastosować szablon, uruchom Kreator hosta (w *Zbieranie danych* > *Hosty*):

- **Wybierz szablon** („Apache by HTTP")
- Utwórz host Apache i dodaj dla niego grupę. Ten wirtualny host będzie zawierał dane związane z Apache.
- Skonfiguruj host. Co ważne, wprowadź adres serwera WWW Apache (127.0.0.1 na maszynie lokalnej, adres IP na maszynie zdalnej).

Krok 1	Krok 2	Krok 3
		
Wybór szablonu.	Tworzenie hosta/grupy hostów.	Konfigurowanie hosta.

Pozostałe ustawienia możesz pozostawić domyślne.

Aby ukończyć pracę z Kreatorem hosta, kliknij *Create* i *Finish*.

Zobacz najnowsze dane

Latest data

Host	Name ▲	Last check	Last value	Change	Tags
Apache server	Bytes per second	21s	2.37 KBps		component: network
Apache server	Get status	21s	{"Date":"Mon, 24 Nov …		component: raw
Apache server	Requests per second	21s	0.5501		component: network
Apache server	Service ping	1m 19s	Up (1)		component: application
Apache server	Service response time	20s	0.11ms	-0.026ms	component: application
Apache server	Total bytes	21s	2.5 MB	+142 KB	component: network
Apache server	Total requests	21s	580	+33	component: network
Apache server	Total workers busy	21s	2		component: system
Apache server	Total workers idle	21s	8		component: system
Apache server	Uptime	21s	00:31:21	+00:01:00	component: system
Apache server	Version	1m 21s	Apache/2.4.58 (Ubuntu)		component: system

Gratulacje, monitorowanie serwera WWW Apache zostało uruchomione!

Zabbix udostępnia opcje wizualizacji i wysyła alerty, jeśli pojawią się jakiekolwiek problemy. Aby skonfigurować alerty e-mail, zobacz Otrzymywanie powiadomień o problemach.

Monitorowanie serwera Linux

Aby rozpocząć monitorowanie serwera Linux, wykonaj następujące kroki:

1. Zastosuj szablon monitorowania Linux.
2. Zainstaluj agent Zabbix na serwerze.
3. Sprawdź najnowsze dane.

Aby rozpocząć monitorowanie zdalnego serwera Linux, musisz znać jego adres IP oraz adres IP serwera Zabbix.

Do monitorowania serwera Linux zostanie użyty agent Zabbix. Instrukcje instalacji agent zostaną podane w dalszej części procesu.

Aby skorzystać z tego przewodnika, musisz mieć zainstalowany serwer Zabbix oraz interfejs webowy installed. Musisz być zalogowany do Zabbix jako domyślny użytkownik *Admin*.

Zastosowanie szablonu monitorowania Linuxa

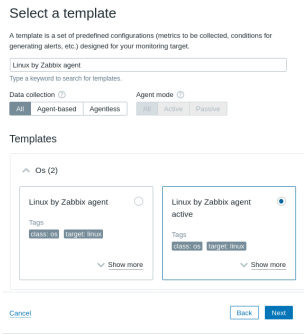
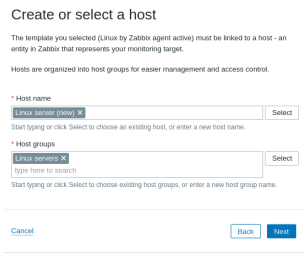
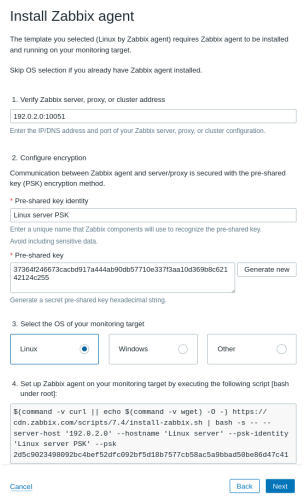
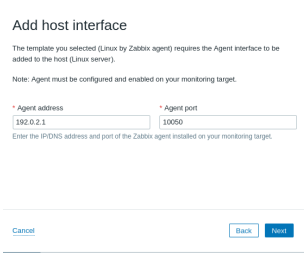
W Zabbix ten szablon jest gotowy do użycia. Zawiera wstępnie skonfigurowane elementy gotowe do zbierania danych, wizualizacji i analizy.

Aby zastosować szablon, uruchom Kreator hosta (w *Zbieranie danych* > *Hosty*):

- **Wybierz szablon** („Linux by Zabbix agent active")
- Utwórz host dla serwera Linux i dodaj dla niego grupę. Ten wirtualny host będzie zawierał wszystkie dane związane z monitorowaniem serwera Linux.
- Skonfiguruj i zainstaluj agent. Aby zainstalować agent, wykonaj na serwerze Linux podane polecenie. Spowoduje to instalację agent oraz skonfigurowanie szyfrowanego połączenia agent z serwer Zabbix.

Jeśli agent jest już zainstalowany, możesz pominąć ten krok (kliknij *Dalej*). Zostaniesz jednak poproszony o podanie tożsamości klucza współdzielonego oraz samego klucza współdzielonego w celu połączenia z agent.

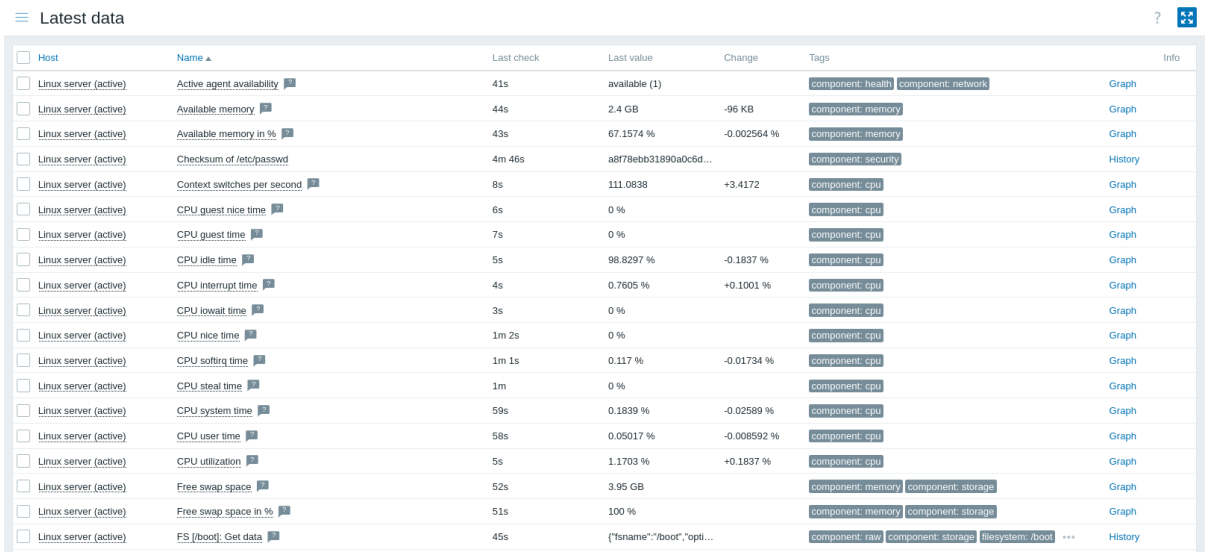
- Zakończ konfigurację hosta. Wprowadź adres IP i port agenta (serwera Linux).

Krok 1	Krok 2	Krok 3	Krok 4
			
Wybór szablonu.	Tworzenie hosta/grupy hostów.	Konfigurowanie i instalowanie agent na hoście.	Dodawanie adresu IP/portu serwera Linux jako interfejsu agenta.

Pozostałe ustawienia możesz pozostawić domyślne.

Aby zakończyć pracę z Kreatorem hosta, kliknij *Utwórz* i *Zakończ*.

Zobacz najnowsze dane



Gratulacje, monitorowanie serwera Linux zostało uruchomione!

Zabbix udostępnia opcje wizualizacji i wysyła alerty, jeśli pojawią się jakiekolwiek problemy. Aby skonfigurować alerty e-mail, zobacz Otrzymywanie powiadomień o problemach.

Monitorowanie serwera MySQL

Aby rozpocząć monitorowanie serwera MySQL, wykonaj następujące kroki:

1. Utwórz użytkownika MySQL z ograniczonymi uprawnieniami.
2. Zastosuj szablon monitorowania MySQL.
3. Sprawdź najnowsze dane.

Aby rozpocząć monitorowanie serwera MySQL, musisz znać jego DSN oraz adres IP serwera Zabbix.

Do monitorowania serwera MySQL zostanie użyty agent Zabbix. Instrukcje instalacji agent zostaną podane w dalszej części procesu.

Aby skorzystać z tego przewodnika, musisz mieć zainstalowany serwer Zabbix oraz interfejs web. Musisz być zalogowany do Zabbix jako domyślny użytkownik *Admin*.

Utwórz użytkownika MySQL z ograniczonymi uprawnieniami

Zaleca się utworzenie użytkownika MySQL z uprawnieniami ograniczonymi wyłącznie do tych potrzebnych do monitorowania MySQL.

```
mysql> CREATE USER 'zbx_monitor'@'%' IDENTIFIED BY '<password>';
mysql> GRANT REPLICATION CLIENT,PROCESS,SHOW DATABASES,SHOW VIEW ON *.* TO 'zbx_monitor'@'%';
```

Zastosowanie szablonu monitorowania MySQL

W Zabbix ten szablon jest gotowy do użycia. Zawiera wstępnie skonfigurowane elementy gotowe do zbierania danych, wizualizacji i analizy.

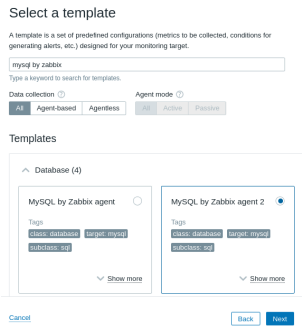
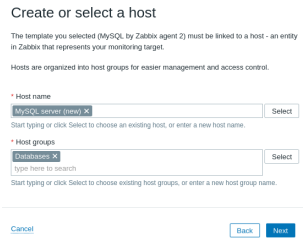
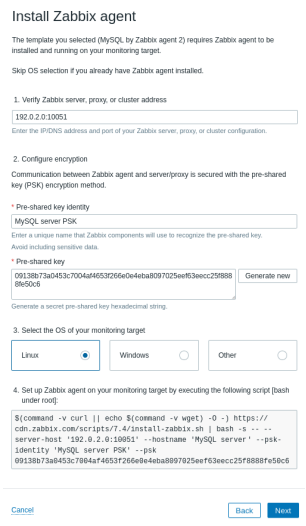
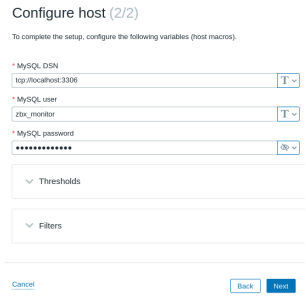
Aby zastosować szablon, uruchom Kreator hosta (w *Zbieranie danych* > *Hosty*):

- **Wybierz szablon** („MySQL by Zabbix agent 2”)
- Utwórz host serwera MySQL i dodaj dla niego grupę. Ten wirtualny host będzie zawierał wszystkie dane związane z monitorowaniem serwera MySQL.
- Skonfiguruj i zainstaluj agent 2 (Zabbix agent 2 zapewnia monitorowanie MySQL od razu po instalacji).

Aby zainstalować agent, wykonaj podane polecenie na maszynie hostującej serwer MySQL. Spowoduje to instalację agenta oraz skonfigurowanie połączenia agenta z serwerem Zabbix z użyciem szyfrowania.

Jeśli agent 2 jest już zainstalowany, możesz pominąć ten krok (kliknij *Dalej*). Zostaniesz jednak poproszony o podanie tożsamości klucza współdzielonego oraz klucza współdzielonego w celu połączenia z agentem.

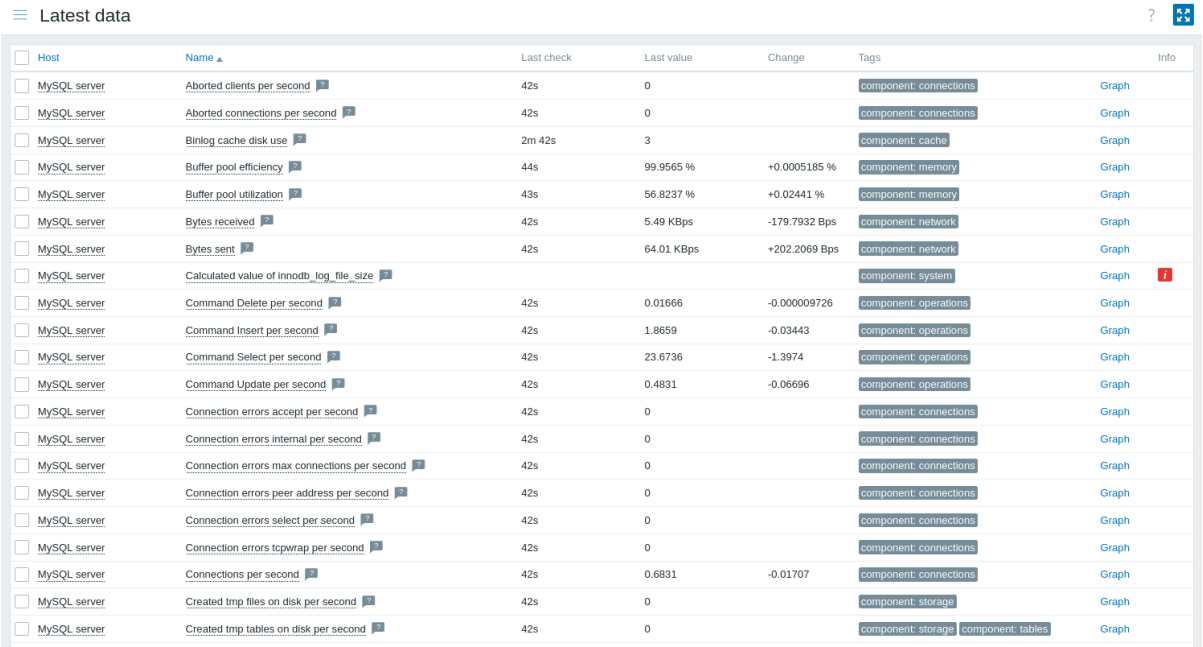
- Zakończ konfigurację hosta. Co ważne, zostaniesz poproszony o podanie DSN serwera MySQL, użytkownika MySQL i hasła. Podaj użytkownika `zbx_monitor` z hasłem, które zostało utworzone.

Krok 1	Krok 2	Krok 3	Krok 4
			
Wybór szablonu.	Tworzenie hosta/grupy hostów.	Konfigurowanie i instalowanie agenta na hoście.	Dodawanie DNS serwera MySQL, użytkownika i hasła.

Pozostałe ustawienia możesz pozostawić domyślne.

Aby ukończyć Kreator hosta, kliknij *Utwórz* i *Zakończ*.

Zobacz najnowsze dane



Gratulacje, monitorowanie serwera MySQL zostało uruchomione!

Zabbix udostępnia opcje wizualizacji i wysyła alerty, jeśli pojawią się jakiekolwiek problemy. Aby skonfigurować alerty e-mail, zobacz Otrzymywanie powiadomień o problemach.

3 Instalacja: dodatkowe przewodniki

Jeśli szukasz najprostszego sposobu instalacji Zabbix, zobacz Instalacja i pierwsze kroki.

Poniższe przewodniki opisują **dodatkowe** lub specyficzne dla systemu sposoby instalacji Zabbix lub jego komponentów:

- Instalacja z kontenerów
- Instalacja ze źródeł
- Uwagi dotyczące instalacji z pakietów
- Instalacja agenta Zabbix z pakietu Windows MSI
- Kompilacja agenta Zabbix 2 w systemie Windows
- Kompilacja agenta Zabbix w systemie Windows
- Instalacja agenta w systemie macOS z pakietu PKG
- Kompilacja agenta Zabbix w systemie macOS
- Urządzenie Zabbix

Instalacja z kontenerów

Przegląd

Ta sekcja opisuje, jak wdrożyć Zabbix za pomocą Docker lub Docker Compose.

Zabbix oficjalnie udostępnia:

- Oddzielne obrazy Docker dla każdego komponentu Zabbix, umożliwiające ich uruchamianie jako przenośnych i samowystarczalnych kontenerów.
- Pliki Compose do definiowania i uruchamiania wielokontenerowych komponentów Zabbix w Docker.

Attention:
Od wersji Zabbix 6.0 deterministyczne wyzwalacze muszą być tworzone podczas instalacji. Jeśli dla MySQL/MariaDB włączone jest logowanie binarne, wymaga to uprawnień superusera lub ustawienia zmiennej/parametru konfiguracyjnego *log_bin_trust_function_creators = 1*. Instrukcje dotyczące ustawienia tej zmiennej można znaleźć w sekcji Database creation scripts.
Należy pamiętać, że w przypadku wykonania z konsoli zmienna zostanie ustawiona tylko tymczasowo i zostanie utracona po ponownym uruchomieniu Docker. W takim przypadku pozostaw usługę SQL uruchomioną, zatrzymaj tylko usługę zabbix-server, wykonując polecenia 'docker compose down zabbix-server', a następnie 'docker compose up -d zabbix-server'.
Alternatywnie można ustawić tę zmienną w pliku konfiguracyjnym.

Pliki źródłowe

Pliki źródłowe Dockerfile są przechowywane w oficjalnym repozytorium Zabbix na GitHubie, gdzie można śledzić najnowsze zmiany w plikach lub sforkować projekt, aby tworzyć własne obrazy.

Docker

Zabbix udostępnia obrazy oparte na różnych bazowych obrazach systemów operacyjnych. Aby uzyskać listę obsługiwanych bazowych obrazów systemów operacyjnych dla określonego komponentu Zabbix, zobacz opis komponentu w Docker Hub. Wszystkie obrazy Zabbix są skonfigurowane tak, aby przebudowywać najnowsze obrazy, jeśli obrazy bazowe zostaną zaktualizowane.

Instalacja

Aby pobrać obraz komponentu Zabbix, uruchom:

```
docker pull zabbix/zabbix-server-mysql
```

Zastąp `zabbix/zabbix-server-mysql` nazwą wymaganego repozytorium dockera.

To polecenie pobierze najnowszą stabilną wersję komponentu Zabbix opartą na systemie operacyjnym Alpine Linux. Możesz dodać tagi do nazwy repozytorium, aby uzyskać obraz oparty na innym systemie operacyjnym lub obraz określonej głównej albo pobocznej wersji Zabbix.

W Docker Hub dostępne są następujące repozytoria:

Komponent		Repozytorium Docker
Zabbix agent		zabbix/zabbix-agent
Zabbix server		
	z obsługą MySQL	zabbix/zabbix-server-mysql
	z obsługą PostgreSQL	zabbix/zabbix-server-pgsql
Interfejs webowy Zabbix		
	oparty na serwerze WWW Apache2 z obsługą MySQL	zabbix/zabbix-web-apache-mysql
	oparty na serwerze WWW Apache2 z obsługą PostgreSQL	zabbix/zabbix-web-apache-pgsql
	oparty na serwerze WWW Nginx z obsługą MySQL	zabbix/zabbix-web-nginx-mysql
	oparty na serwerze WWW Nginx z obsługą PostgreSQL	zabbix/zabbix-web-nginx-pgsql
Zabbix proxy		
	z obsługą SQLite3	zabbix/zabbix-proxy-sqlite3
	z obsługą MySQL	zabbix/zabbix-proxy-mysql
Zabbix Java gateway		zabbix/zabbix-java-gateway

Note:
Obsługa pułapek SNMP jest udostępniana w osobnym repozytorium zabbix/zabbix-snmptraps. Może ono zostać połączone z Zabbix serwer i Zabbix proxy.

Tagi

Oficjalne obrazy komponentów Zabbix mogą zawierać następujące tagi:

Tag	Opis	Przykład
latest	Najnowsza stabilna wersja komponentu Zabbix oparta na obrazie Alpine Linux.	zabbix-agent:latest
<OS>-trunk	Najnowsza kompilacja nightly wersji Zabbix, która jest obecnie rozwijana dla określonego systemu operacyjnego. **<OS>** - bazowy system operacyjny. Obsługiwane wartości: *alpine* - Alpine Linux; *ltsc2019* - Windows 10 LTSC 2019 (tylko agent); *ol* - Oracle Linux; *ltsc2022* - Windows 11 LTSC 2022 (tylko agent); *ubuntu* - Ubuntu	zabbix-agent:ubuntu-trunk
<OS>-latest	Najnowsza stabilna wersja komponentu Zabbix dla określonego systemu operacyjnego. **<OS>** - bazowy system operacyjny. Obsługiwane wartości: *alpine* - Alpine Linux; *ltsc2019* - Windows 10 LTSC 2019 (tylko agent); *ol* - Oracle Linux; *ltsc2022* - Windows 11 LTSC 2022 (tylko agent); *ubuntu* - Ubuntu	zabbix-agent:ol-latest
<OS>-X.X-latest	Najnowsza wersja podrzędna komponentu Zabbix dla określonej wersji głównej i systemu operacyjnego. **<OS>** - bazowy system operacyjny. Obsługiwane wartości: *alpine* - Alpine Linux; *ltsc2019* - Windows 10 LTSC 2019 (tylko agent); *ol* - Oracle Linux; *ltsc2022* - Windows 11 LTSC 2022 (tylko agent); *ubuntu* - Ubuntu **X.X** - główna wersja Zabbix (tj. *6.0*, *7.4*, *8.0*).	zabbix-agent:alpine-8.0-latest
<OS>-X.X.*	Określona wersja podrzędna komponentu Zabbix dla określonej wersji głównej i systemu operacyjnego. **<OS>** - bazowy system operacyjny. Obsługiwane wartości: *alpine* - Alpine Linux; *ltsc2019* - Windows 10 LTSC 2019 (tylko agent); *ol* - Oracle Linux; *ltsc2022* - Windows 11 LTSC 2022 (tylko agent); *ubuntu* - Ubuntu **X.X** - główna wersja Zabbix (tj. *6.0*, *7.4*, *8.0*). * - wersja podrzędna Zabbix	zabbix-agent:alpine-8.0.1

Konfiguracja początkowa

Po pobraniu obrazów uruchom kontenery, wykonując polecenie `docker run`, a następnie podając dodatkowe argumenty określające wymagane zmienne środowiskowe i/lub punkty montowania. Poniżej przedstawiono kilka przykładów konfiguracji.

Note:
Aby umożliwić komunikację między komponentami Zabbix, niektóre porty, takie jak 10051/TCP dla serwera Zabbix (trapper), 10050/TCP dla agenta Zabbix, 162/UDP dla pułapek SNMP oraz 80/TCP dla interfejsu webowego Zabbix, będą udostępnione na maszynie hosta. Pełna lista domyślnych portów używanych przez komponenty Zabbix jest dostępna na stronie Wymagania. W przypadku serwera Zabbix i agenta domyślny port można zmienić, ustawiając zmienną środowiskową ZBX_LISTENPORT environment variable.

Zmienne środowiskowe

Wszystkie obrazy komponentów Zabbix udostępniają zmienne środowiskowe do sterowania konfiguracją. Obsługiwane zmienne środowiskowe są wymienione w repozytorium komponentu.

Te zmienne środowiskowe są odpowiednikami opcji z plików konfiguracyjnych Zabbix, ale mają inną metodę nazewnictwa. Na przykład `ZBX_LOGSLOWQUERIES` jest odpowiednikiem `LogSlowQueries` z plików konfiguracyjnych Zabbix serwer lub Zabbix proxy.

Attention:
Niektórych opcji konfiguracyjnych (np. `PIDFile` i `LogType`) nie można zmienić.

Następujące zmienne środowiskowe są specyficzne dla komponentów Docker i nie występują w plikach konfiguracyjnych Zabbix:

Variable	Components	Default value	Description
`DB_SERVER_HOST`	Serwer Proxy Interfejs webowy	`mysql-server` dla MYSQL `postgres-server` dla PostgreSQL	Nazwa IP lub DNS serwera MySQL lub PostgreSQL.
`DB_SERVER_PORT`	Serwer Proxy Interfejs webowy	3306 dla MYSQL 5432 dla PostgreSQL	Port serwera MySQL lub PostgreSQL.
`MYSQL_USER`	Serwer Proxy Interfejs webowy	`zabbix`	Użytkownik bazy danych MySQL.
`MYSQL_PASSWORD`	Serwer Proxy Interfejs webowy	`zabbix`	Hasło bazy danych MySQL.
`MYSQL_DATABASE`	Serwer Proxy Interfejs webowy	`zabbix` dla serwera Zabbix `zabbix_proxy` dla proxy Zabbix	Nazwa bazy danych Zabbix.
`POSTGRES_USER`	Serwer Interfejs webowy	`zabbix`	Użytkownik bazy danych PostgreSQL.
`POSTGRES_PASSWORD`	Serwer Interfejs webowy	`zabbix`	Hasło bazy danych PostgreSQL.
`POSTGRES_DB`	Serwer Interfejs webowy	`zabbix` dla serwera Zabbix `zabbix_proxy` dla proxy Zabbix	Nazwa bazy danych Zabbix.
`PHP_TZ`	Interfejs webowy	`Europe/Riga`	Strefa czasowa w formacie PHP. Pełna lista obsługiwanych stref czasowych jest dostępna na php.net.
`ZBX_SERVER_NAME`	Interfejs webowy	`Zabbix Docker`	Widoczna nazwa instalacji Zabbix pod logo Zabbix w pionowym menu interfejsu webowego.
`ZBX_JAVAGATEWAY_ENABLE`	Serwer Proxy	`false`	Włącza komunikację z Zabbix Java gateway w celu zbierania kontroli związanych z Javą.
`ZBX_ENABLE_SNMP_TRAPS`	Serwer Proxy	`false`	Włącza funkcję pułapek SNMP. Wymaga instancji **zabbix-snmptraps** oraz współdzielonego woluminu */var/lib/zabbix/snmptraps* dla serwera Zabbix lub proxy Zabbix.

Woluminy

Obrazy umożliwiają montowanie woluminów przy użyciu następujących punktów montowania:

Wolumin	Opis
Zabbix agent	
/etc/zabbix/zabbix_agentd	Wolumin umożliwia dołączanie plików **.conf* oraz rozszerzanie Zabbix agent przy użyciu funkcji `UserParameter`
/var/lib/zabbix/modules	Wolumin umożliwia ładowanie dodatkowych modułów oraz rozszerzanie Zabbix agent przy użyciu funkcji LoadModule
/var/lib/zabbix/enc	Wolumin służy do przechowywania plików związanych z TLS. Nazwy tych plików są określane przy użyciu zmiennych środowiskowych `ZBX_TLSCAFILE`, `ZBX_TLSCRLFILE`, `ZBX_TLSKEY_FILE` oraz `ZBX_TLSPSKFILE`
Zabbix server	
/usr/lib/zabbix/alertscripts	Wolumin jest używany dla niestandardowych skryptów alertów. Jest to parametr `AlertScriptsPath` w zabbix_server.conf
/usr/lib/zabbix/externalscripts	Wolumin jest używany przez kontrole zewnętrzne. Jest to parametr `ExternalScripts` w zabbix_server.conf
/var/lib/zabbix/modules	Wolumin umożliwia ładowanie dodatkowych modułów oraz rozszerzanie Zabbix serwer przy użyciu funkcji LoadModule
/var/lib/zabbix/enc	Wolumin służy do przechowywania plików związanych z TLS. Nazwy tych plików są określane przy użyciu zmiennych środowiskowych `ZBX_TLSCAFILE`, `ZBX_TLSCRLFILE`, `ZBX_TLSKEY_FILE` oraz `ZBX_TLSPSKFILE`
/var/lib/zabbix/ssl/certs	Wolumin jest używany jako lokalizacja plików certyfikatów klienta SSL do uwierzytelniania klienta. Jest to parametr `SSLCertLocation` w zabbix_server.conf
/var/lib/zabbix/ssl/keys	Wolumin jest używany jako lokalizacja plików kluczy prywatnych SSL do uwierzytelniania klienta. Jest to parametr `SSLKeyLocation` w zabbix_server.conf
/var/lib/zabbix/ssl/ssl_ca	Wolumin jest używany jako lokalizacja plików urzędu certyfikacji (CA) do weryfikacji certyfikatu serwera SSL. Jest to parametr `SSLCALocation` w zabbix_server.conf
/var/lib/zabbix/snmptraps	Wolumin jest używany jako lokalizacja pliku snmptraps.log. Może być współdzielony przez kontener zabbix-snmptraps i dziedziczony przy użyciu opcji Docker volumes_from podczas tworzenia nowej instancji Zabbix serwer. Funkcję przetwarzania pułapek SNMP można włączyć przy użyciu współdzielonego woluminu i ustawieniu zmiennej środowiskowej `ZBX_ENABLE_SNMP_TRAPS` na 'true'
/var/lib/zabbix/mibs	Wolumin umożliwia dodawanie nowych plików MIB. Nie obsługuje podkatalogów, wszystkie pliki MIB muszą być umieszczone w `/var/lib/zabbix/mibs`
Zabbix proxy	
/usr/lib/zabbix/externalscripts	Wolumin jest używany przez kontrole zewnętrzne. Jest to parametr `ExternalScripts` w zabbix_proxy.conf
/var/lib/zabbix/db_data	Wolumin umożliwia przechowywanie plików bazy danych na urządzeniach zewnętrznych. Obsługiwane tylko dla Zabbix proxy z SQLite3
/var/lib/zabbix/modules	Wolumin umożliwia ładowanie dodatkowych modułów oraz rozszerzanie Zabbix serwer przy użyciu funkcji LoadModule
/var/lib/zabbix/enc	Wolumin służy do przechowywania plików związanych z TLS. Nazwy tych plików są określane przy użyciu zmiennych środowiskowych `ZBX_TLSCAFILE`, `ZBX_TLSCRLFILE`, `ZBX_TLSKEY_FILE` oraz `ZBX_TLSPSKFILE`
/var/lib/zabbix/ssl/certs	Wolumin jest używany jako lokalizacja plików certyfikatów klienta SSL do uwierzytelniania klienta. Jest to parametr `SSLCertLocation` w zabbix_proxy.conf
/var/lib/zabbix/ssl/keys	Wolumin jest używany jako lokalizacja plików kluczy prywatnych SSL do uwierzytelniania klienta. Jest to parametr `SSLKeyLocation` w zabbix_proxy.conf
/var/lib/zabbix/ssl/ssl_ca	Wolumin jest używany jako lokalizacja plików urzędu certyfikacji (CA) do weryfikacji certyfikatu serwera SSL. Jest to parametr `SSLCALocation` w zabbix_proxy.conf
/var/lib/zabbix/snmptraps	Wolumin jest używany jako lokalizacja pliku snmptraps.log. Może być współdzielony przez kontener zabbix-snmptraps i dziedziczony przy użyciu opcji Docker volumes_from podczas tworzenia nowej instancji Zabbix serwer. Funkcję przetwarzania pułapek SNMP można włączyć przy użyciu współdzielonego woluminu i ustawieniu zmiennej środowiskowej `ZBX_ENABLE_SNMP_TRAPS` na 'true'
/var/lib/zabbix/mibs	Wolumin umożliwia dodawanie nowych plików MIB. Nie obsługuje podkatalogów, wszystkie pliki MIB muszą być umieszczone w `/var/lib/zabbix/mibs`

Wolumin	Opis
Interfejs webowy Zabbix oparty na serwerze Apache2	
/etc/ssl/apache2	Wolumin umożliwia włączenie HTTPS dla interfejsu webowego Zabbix. Wolumin musi zawierać dwa pliki `ssl.crt` oraz `ssl.key` przygotowane dla połączeń SSL Apache2
Interfejs webowy Zabbix oparty na serwerze Nginx	
/etc/ssl/nginx	Wolumin umożliwia włączenie HTTPS dla interfejsu webowego Zabbix. Wolumin musi zawierać dwa pliki `ssl.crt`, `ssl.key` oraz `dhparam.pem` przygotowane dla połączeń SSL Nginx
Zabbix snmptraps	
/var/lib/zabbix/snmptraps	Wolumin zawiera plik dziennika `snmptraps.log` z odebranymi pułapkami SNMP
/var/lib/zabbix/mibs	Wolumin umożliwia dodawanie nowych plików MIB. Nie obsługuje podkatalogów, wszystkie pliki MIB muszą być umieszczone w `/var/lib/zabbix/mibs`

Aby uzyskać dodatkowe informacje, zobacz oficjalne repozytoria Zabbix w Docker Hub.

Przykłady

Przykład 1

Ten przykład pokazuje, jak uruchomić serwer Zabbix z obsługą bazy danych MySQL, interfejs webowy Zabbix oparty na serwerze webowym Nginx oraz Zabbix Java gateway.

1. Utwórz sieć przeznaczoną dla kontenerów komponentów Zabbix:

```
docker network create --subnet 172.20.0.0/16 --ip-range 172.20.240.0/20 zabbix-net
```

2. Uruchom pustą instancję serwera MySQL:

```
docker run --name mysql-server -t \
    -e MYSQL_DATABASE="zabbix" \
    -e MYSQL_USER="zabbix" \
    -e MYSQL_PASSWORD="zabbix_pwd" \
    -e MYSQL_ROOT_PASSWORD="root_pwd" \
    --network=zabbix-net \
    --restart unless-stopped \
    -d mysql:8.4-oracle \
    --character-set-server=utf8 --collation-server=utf8_bin \
    --default-authentication-plugin=caching_sha2_password
```

3. Uruchom instancję Zabbix Java gateway:

```
docker run --name zabbix-java-gateway -t \
    --network=zabbix-net \
```

```
    --restart unless-stopped \
    -d zabbix/zabbix-java-gateway:alpine-8.0-latest
```

4. Uruchom instancję serwera Zabbix i połącz ją z utworzoną instancją serwera MySQL:

```
docker run --name zabbix-server-mysql -t \
    -e DB_SERVER_HOST="mysql-server" \
    -e MYSQL_DATABASE="zabbix" \
    -e MYSQL_USER="zabbix" \
    -e MYSQL_PASSWORD="zabbix_pwd" \
    -e MYSQL_ROOT_PASSWORD="root_pwd" \
    -e ZBX_JAVAGATEWAY="zabbix-java-gateway" \
    --network=zabbix-net \
    -p 10051:10051 \
    --restart unless-stopped \
    -d zabbix/zabbix-server-mysql:alpine-8.0-latest
```

5. Uruchom interfejs webowy Zabbix i połącz tę instancję z utworzonymi instancjami serwera MySQL i serwera Zabbix:

```
docker run --name zabbix-web-nginx-mysql -t \
    -e ZBX_SERVER_HOST="zabbix-server-mysql" \
    -e DB_SERVER_HOST="mysql-server" \
    -e MYSQL_DATABASE="zabbix" \
    -e MYSQL_USER="zabbix" \
    -e MYSQL_PASSWORD="zabbix_pwd" \
    -e MYSQL_ROOT_PASSWORD="root_pwd" \
    --network=zabbix-net \
    -p 80:8080 \
    --restart unless-stopped \
    -d zabbix/zabbix-web-nginx-mysql:alpine-8.0-latest
```

Przykład 2

Ten przykład pokazuje, jak uruchomić serwer Zabbix z obsługą bazy danych PostgreSQL, interfejs webowy Zabbix oparty na serwerze webowym Nginx oraz funkcję pułapek SNMP.

1. Utwórz sieć przeznaczoną dla kontenerów komponentów Zabbix:

```
docker network create --subnet 172.20.0.0/16 --ip-range 172.20.240.0/20 zabbix-net
```

2. Uruchom pustą instancję serwera PostgreSQL:

```
docker run --name postgres-server -t \
      -e POSTGRES_USER="zabbix" \
      -e POSTGRES_PASSWORD="zabbix_pwd" \
      -e POSTGRES_DB="zabbix" \
      --network=zabbix-net \
      --restart unless-stopped \
      -d postgres:latest
```

3. Uruchom instancję Zabbix snmptraps:

```
docker run --name zabbix-snmptraps -t \
    -v /zbx_instance/snmptraps:/var/lib/zabbix/snmptraps:rw \
    -v /var/lib/zabbix/mibs:/usr/share/snmp/mibs:ro \
    --network=zabbix-net \
    -p 162:1162/udp \
    --restart unless-stopped \
    -d zabbix/zabbix-snmptraps:alpine-8.0-latest
```

4. Uruchom instancję serwera Zabbix i połącz ją z utworzoną instancją serwera PostgreSQL:

```
docker run --name zabbix-server-pgsql -t \
    -e DB_SERVER_HOST="postgres-server" \
    -e POSTGRES_USER="zabbix" \
    -e POSTGRES_PASSWORD="zabbix_pwd" \
    -e POSTGRES_DB="zabbix" \
    -e ZBX_ENABLE_SNMP_TRAPS="true" \
```

```
    --network=zabbix-net \
    -p 10051:10051 \
    --volumes-from zabbix-snmptraps \
    --restart unless-stopped \
    -d zabbix/zabbix-server-pgsql:alpine-8.0-latest
```

5. Uruchom interfejs webowy Zabbix i połącz tę instancję z utworzonymi instancjami serwera PostgreSQL i serwera Zabbix:

```
docker run --name zabbix-web-nginx-pgsql -t \
    -e ZBX_SERVER_HOST="zabbix-server-pgsql" \
    -e DB_SERVER_HOST="postgres-server" \
    -e POSTGRES_USER="zabbix" \
    -e POSTGRES_PASSWORD="zabbix_pwd" \
    -e POSTGRES_DB="zabbix" \
    --network=zabbix-net \
    -p 443:8443 \
    -p 80:8080 \
    -v /etc/ssl/nginx:/etc/ssl/nginx:ro \
    --restart unless-stopped \
    -d zabbix/zabbix-web-nginx-pgsql:alpine-8.0-latest
```

Przykład 3

Ten przykład pokazuje, jak uruchomić serwer Zabbix z obsługą bazy danych MySQL, interfejs webowy Zabbix oparty na serwerze webowym Nginx oraz Zabbix Java gateway przy użyciu podman w systemie Red Hat 8.

1. Utwórz nowy pod o nazwie zabbix i udostępnionych portach (interfejs webowy, trapper serwera Zabbix):

```
podman pod create --name zabbix -p 80:8080 -p 10051:10051
```

2. (opcjonalnie) Uruchom kontener Zabbix agent w podzie zabbix:

```
podman run --name zabbix-agent \
  -e ZBX_SERVER_HOST="127.0.0.1,localhost" \
  --restart=always \
  --pod=zabbix \
  -d registry.connect.redhat.com/zabbix/zabbix-agent-74:latest
```

3. Utwórz katalog ./mysql/ na hoście i uruchom serwer Oracle MySQL 8.4:

```
podman run --name mysql-server -t \
    -e MYSQL_DATABASE="zabbix" \
    -e MYSQL_USER="zabbix" \
    -e MYSQL_PASSWORD="zabbix_pwd" \
    -e MYSQL_ROOT_PASSWORD="root_pwd" \
    -v ./mysql/:/var/lib/mysql/:Z \
    --restart=always \
    --pod=zabbix \
    -d mysql:8.4 \
    --character-set-server=utf8 --collation-server=utf8_bin \
    --default-authentication-plugin=caching_sha2_password
```

4. Uruchom kontener serwera Zabbix:

```
podman run --name zabbix-server-mysql -t \
                -e DB_SERVER_HOST="127.0.0.1" \
                -e MYSQL_DATABASE="zabbix" \
                -e MYSQL_USER="zabbix" \
                -e MYSQL_PASSWORD="zabbix_pwd" \
                -e MYSQL_ROOT_PASSWORD="root_pwd" \
                -e ZBX_JAVAGATEWAY="127.0.0.1" \
                --restart=always \
                --pod=zabbix \
                -d registry.connect.redhat.com/zabbix/zabbix-server-mysql-74
```

5. Uruchom kontener Zabbix Java Gateway:

```
podman run --name zabbix-java-gateway -t \
    --restart=always \
    --pod=zabbix \
    -d registry.connect.redhat.com/zabbix/zabbix-java-gateway-74
```

6. Uruchom kontener interfejsu webowego Zabbix:

```
podman run --name zabbix-web-mysql -t \
                -e ZBX_SERVER_HOST="127.0.0.1" \
                -e DB_SERVER_HOST="127.0.0.1" \
                -e MYSQL_DATABASE="zabbix" \
                -e MYSQL_USER="zabbix" \
                -e MYSQL_PASSWORD="zabbix_pwd" \
                -e MYSQL_ROOT_PASSWORD="root_pwd" \
                --restart=always \
                --pod=zabbix \
                -d registry.connect.redhat.com/zabbix/zabbix-web-mysql-74
```

Note:
Pod `zabbix` udostępnia port 80/TCP (HTTP) na maszynie hosta z portu 8080/TCP kontenera `zabbix-web-mysql`.

Docker Compose

Alternatywnie Zabbix można zainstalować przy użyciu wtyczki Docker Compose. Pliki Compose do definiowania i uruchamiania wielokontenerowych komponentów Zabbix są dostępne w oficjalnym repozytorium Zabbix Docker w serwisie GitHub.

Attention:
Oficjalne pliki Compose Zabbix obsługują wersję 3 Docker Compose.

Te pliki Compose zostały dodane jako przykłady; są rozbudowane. Na przykład zawierają proxy z obsługą zarówno MySQL, jak i SQLite3.

Aby uzyskać pliki Docker Compose udostępniane przez Zabbix, sklonuj repozytorium:

```
git clone https://github.com/zabbix/zabbix-docker.git
```

Przełącz się na wymaganą wersję:

```
git checkout 8.0
```

Skonfiguruj pliki Compose oraz utwórz i uruchom kontenery:

```
docker compose -f ./docker-compose_v3_alpine_mysql_latest.yaml up
```

Zastąp `docker-compose_v3_alpine_mysql_latest.yaml` w powyższym poleceniu wymaganym plikiem konfiguracyjnym.

Dostępne są następujące opcje:

Nazwa pliku	Opis
`docker-compose_v3_alpine_mysql_latest.yaml`	Plik Compose instaluje najnowszą wersję komponentów Zabbix 8.0 w systemie Alpine Linux z obsługą bazy danych MySQL.
`docker-compose_v3_alpine_mysql_local.yaml`	Plik Compose buduje najnowszą wersję Zabbix 8.0 i uruchamia komponenty Zabbix w systemie Alpine Linux z obsługą bazy danych MySQL.
`docker-compose_v3_alpine_pgsql_latest.yaml`	Plik Compose instaluje najnowszą wersję komponentów Zabbix 8.0 w systemie Alpine Linux z obsługą bazy danych PostgreSQL.
`docker-compose_v3_alpine_pgsql_local.yaml`	Plik Compose buduje najnowszą wersję Zabbix 8.0 i uruchamia komponenty Zabbix w systemie Alpine Linux z obsługą bazy danych PostgreSQL.
`docker-compose_v3_ol_mysql_latest.yaml`	Plik Compose instaluje najnowszą wersję komponentów Zabbix 8.0 w systemie Oracle Linux z obsługą bazy danych MySQL.
`docker-compose_v3_ol_mysql_local.yaml`	Plik Compose buduje najnowszą wersję Zabbix 8.0 i uruchamia komponenty Zabbix w systemie Oracle Linux z obsługą bazy danych MySQL.
`docker-compose_v3_ol_pgsql_latest.yaml`	Plik Compose instaluje najnowszą wersję komponentów Zabbix 8.0 w systemie Oracle Linux z obsługą bazy danych PostgreSQL.
`docker-compose_v3_ol_pgsql_local.yaml`	Plik Compose buduje najnowszą wersję Zabbix 8.0 i uruchamia komponenty Zabbix w systemie Oracle Linux z obsługą bazy danych PostgreSQL.

Nazwa pliku	Opis
docker-compose_v3_ubuntu_mysql_latest.yaml	Plik Compose do instalacji najnowszą wersję komponentów Zabbix 8.0 w systemie Ubuntu 24.04 (noble) z obsługą bazy danych MySQL.
docker-compose_v3_ubuntu_mysql_local.yaml	Plik Compose do lokalnego budowania i uruchamia najnowszą wersję Zabbix 8.0 i uruchamia komponenty Zabbix w systemie Ubuntu 24.04 (noble) z obsługą bazy danych MySQL.
docker-compose_v3_ubuntu_pgsql_latest.yaml	Plik Compose do instalacji najnowszą wersję komponentów Zabbix 8.0 w systemie Ubuntu 24.04 (noble) z obsługą bazy danych PostgreSQL.
docker-compose_v3_ubuntu_pgsql_local.yaml	Plik Compose do lokalnego budowania i uruchamia najnowszą wersję Zabbix 8.0 i uruchamia komponenty Zabbix w systemie Ubuntu 24.04 (noble) z obsługą bazy danych PostgreSQL.

Pamięć masowa

Pliki Compose są skonfigurowane tak, aby obsługiwać lokalną pamięć masową na maszynie hosta. Docker Compose utworzy katalog `zbx_env` w folderze z plikiem compose podczas uruchamiania komponentów Zabbix przy użyciu pliku compose. Katalog będzie zawierał tę samą strukturę, jak opisano w sekcji Volumes, oraz katalog do przechowywania bazy danych.

Dostępne są również wolumeny w trybie tylko do odczytu dla plików `/etc/localtime` i `/etc/timezone`.

Zmienne środowiskowe

Pliki zmiennych mają następującą strukturę nazewnictwa: `.env_<typ komponentu>` i znajdują się w katalogu *env_vars*. Szczegółowe informacje o nazewnictwie zmiennych i dostępnych opcjach wyboru można znaleźć w sekcji zmienne środowiskowe.

Przykłady

Przykład 1

```
git checkout 8.0
docker compose -f ./docker-compose_v3_alpine_mysql_latest.yaml up -d
```

Polecenie pobierze najnowsze obrazy Zabbix 8.0 dla każdego komponentu Zabbix i uruchomi je w trybie odłączonym.

> **Attention:**
> Nie zapomnij pobrać plików `.env_<type of component>` z oficjalnego repozytorium Zabbix na github.com wraz z plikami compose.

Przykład 2

```
git checkout 8.0
docker compose -f ./docker-compose_v3_ubuntu_mysql_local.yaml up -d
```

Polecenie pobierze obraz bazowy Ubuntu 24.04 (noble), a następnie zbuduje lokalnie komponenty Zabbix 8.0 i uruchomi je w trybie odłączonym.

Instalacja ze źródeł

Najnowszą wersję Zabbix można uzyskać, kompilując ją ze źródeł. Zobacz także Pobieranie kodu źródłowego Zabbix.

Tutaj znajduje się samouczek krok po kroku dotyczący instalacji Zabbix ze źródeł.

Instalowanie demonów Zabbix

1 Pobierz archiwum źródłowe

Przejdź do strony pobierania Zabbix i pobierz archiwum źródłowe. Po pobraniu rozpakuj źródła, uruchamiając:

```
tar -zxvf zabbix-8.0.0.tar.gz
```

> **Note:**
> Wprowadź w poleceniu prawidłową wersję Zabbix. Musi ona odpowiadać nazwie pobranego archiwum.

2 Utwórz konto użytkownika

Wszystkie procesy demonów Zabbix działają pod nieuprzywilejowanymi użytkownikami systemowymi. Jeśli demon Zabbix zostanie uruchomiony z nieuprzywilejowanego konta użytkownika, będzie nadal działał jako ten użytkownik.

W domyślnej konfiguracji, jeśli demon zostanie uruchomiony jako `root`, przełączy się na konto użytkownika `zabbix`, które musi istnieć. Aby utworzyć użytkownika systemowego `zabbix` i grupę, uruchom poniższe polecenia.

System oparty na RedHat:

```
groupadd --system zabbix
useradd --system -g zabbix -d /usr/lib/zabbix -s /sbin/nologin -c "Zabbix Monitoring System" zabbix
```

System oparty na Debianie:

```
addgroup --system --quiet zabbix
adduser --quiet --system --disabled-login --ingroup zabbix --home /var/lib/zabbix --no-create-home zabbix
```

Nie ma potrzeby tworzenia osobnego konta użytkownika dla frontend Zabbix.

Zalecenie dotyczące bezpieczeństwa

Jeśli Zabbix serwer i agent działają na tej samej maszynie, zaleca się uruchamianie ich pod **oddzielnymi kontami użytkowników**. Uruchamianie obu pod tym samym użytkownikiem pozwala agentowi uzyskać dostęp do pliku konfiguracyjnego serwera, co może ujawnić poufne informacje — takie jak hasło do bazy danych — każdemu użytkownikowi z uprawnieniami administratora w Zabbix.

> **Attention:**
> Uruchamianie Zabbix jako `root`, `bin` lub dowolnego innego konta ze specjalnymi uprawnieniami stanowi zagrożenie bezpieczeństwa.

Katalog domowy (opcjonalnie)

Procesy Zabbix nie wymagają katalogu domowego, dlatego jego tworzenie zasadniczo nie jest zalecane. Jeśli jednak potrzebujesz funkcjonalności wymagającej katalogu domowego (na przykład przechowywania poświadczeń MySQL w $HOME/.my.cnf), możesz go utworzyć za pomocą poniższych poleceń.

W systemach opartych na RedHat uruchom:

```
mkdir -m u=rwx,g=rwx,o= -p /usr/lib/zabbix
chown zabbix:zabbix /usr/lib/zabbix
```

W systemach opartych na Debianie uruchom:

```
mkdir -m u=rwx,g=rwx,o= -p /var/lib/zabbix
chown zabbix:zabbix /var/lib/zabbix
```

3 Tworzenie bazy danych Zabbix

Dla demonów Zabbix serwer i proxy, a także dla frontendu Zabbix, wymagana jest baza danych. Nie jest ona potrzebna do uruchomienia Zabbix agent.

Dostępne są skrypty SQL do utworzenia schematu bazy danych i wstawienia zestawu danych. Baza danych proxy Zabbix wymaga tylko schematu, natomiast baza danych serwera Zabbix wymaga oprócz schematu również zestawu danych.

Po utworzeniu bazy danych Zabbix przejdź do kolejnych kroków kompilacji Zabbix.

4 Konfiguracja źródeł

Do budowania Zabbix serwer, Zabbix proxy lub Zabbix agent wymagany jest standard C99 z rozszerzeniami GNU. Tę wersję można jawnie określić, ustawiając CFLAGS=”-std=gnu99”:

```
export CFLAGS="-std=gnu99"
```

> **Note:**
> W przypadku instalacji z repozytorium Git Zabbix należy najpierw uruchomić:
>
> ```
> ./bootstrap.sh
> ```

Podczas konfigurowania źródeł dla Zabbix serwer lub proxy należy określić typ bazy danych, który ma zostać użyty. W danym momencie z procesem serwer lub proxy może być skompilowany tylko jeden typ bazy danych.

Aby zobaczyć wszystkie obsługiwane opcje konfiguracji, w rozpakowanym katalogu ze źródłami Zabbix uruchom:

```
./configure --help
```

Aby skonfigurować źródła dla Zabbix serwer i agent, możesz uruchomić na przykład:

```
./configure --enable-server --enable-agent --with-mysql --enable-ipv6 --with-net-snmp --with-libcurl --wit
```

Aby skonfigurować źródła dla Zabbix serwer (z PostgreSQL itp.), możesz uruchomić:

```
./configure --enable-server --with-postgresql --with-net-snmp
```

Aby skonfigurować źródła dla Zabbix proxy (z SQLite itp.), możesz uruchomić:

```
./configure --prefix=/usr --enable-proxy --with-net-snmp --with-sqlite3 --with-ssh2
```

Aby skonfigurować źródła dla Zabbix agent, możesz uruchomić:

```
./configure --enable-agent
```

lub, dla Zabbix agent 2:

```
./configure --enable-agent2
```

Note:
Aby zbudować Zabbix agent 2, musi być zainstalowana obsługiwana wersja Go.

Uwagi dotyczące opcji kompilacji:

- `--enable-agent` - kompiluje Zabbix agent, a także narzędzia wiersza poleceń Zabbix get i Zabbix sender.
- `--with-libcurl` - wymagane do monitorowania maszyn wirtualnych, uwierzytelniania SMTP oraz pozycji Zabbix agent `web.page.*`. Zobacz także: Wymagania (libcurl).
- `--with-libxml2` - wymagane do monitorowania maszyn wirtualnych.
- `--with-libpcre2[=DIR]` - Zabbix zawsze kompiluje się z biblioteką PCRE2; ta opcja pozwala jedynie określić niestandardową ścieżkę instalacji PCRE2.
- `--with-mysql=/path/to/mysql_config` - określa ścieżkę do konfiguracji konkretnej biblioteki klienckiej MySQL. Przydatne, gdy zainstalowanych jest wiele wersji MySQL lub MariaDB.
- `--enable-static` - statycznie linkuje biblioteki (nieobsługiwane w systemie Solaris). Użyj tej opcji, jeśli planujesz dystrybuować skompilowane pliki binarne do systemów bez wymaganych bibliotek. Nie jest zalecana podczas budowania Zabbix serwer. Aby zbudować serwer statycznie, wymagana jest statyczna wersja każdej biblioteki zewnętrznej. Skrypt configure nie sprawdza tego automatycznie.
- `--with-stacksize=<value>` - ustawia rozmiar stosu na wątek w kilobajtach (np. `--with-stacksize=512`). Możesz zwiększyć tę wartość, jeśli Zabbix ulega awarii lub zawiesza się z powodu przepełnienia stosu (np. podczas preprocessingu w systemach z niskimi domyślnymi limitami stosu wątków).

Attention:
Jeśli `./configure` zakończy się niepowodzeniem z powodu brakujących bibliotek lub innych problemów, sprawdź plik `config.log`, aby uzyskać szczegółowe informacje o błędzie.
Na przykład, jeśli brakuje `libssl`, bezpośredni komunikat o błędzie może być mylący:

```
checking for main in -lmysqlclient... no
configure: error: Not found mysqlclient library
```

W takim przypadku `config.log` ujawnia rzeczywistą przyczynę:

```
/usr/bin/ld: cannot find -lssl
/usr/bin/ld: cannot find -lcrypto
```

Zobacz także:

- Kompilowanie Zabbix z obsługą szyfrowania
- Znane problemy z kompilacją

5 Skompiluj i zainstaluj wszystko

Note:
Jeśli instalujesz z repozytorium Git Zabbix, należy najpierw uruchomić:

```
$ make dbschema
```

```
make install
```

Ten krok należy uruchomić jako użytkownik z wystarczającymi uprawnieniami (zwykle 'root' lub przy użyciu sudo).

Uruchomienie `make install` domyślnie zainstaluje pliki binarne demonów (zabbix_server, zabbix_agentd, zabbix_proxy) w /usr/local/sbin oraz pliki binarne klienta (zabbix_get, zabbix_sender) w /usr/local/bin.

Note:
Aby określić inną lokalizację niż /usr/local, użyj klucza --prefix w poprzednim kroku konfiguracji źródeł, na przykład --prefix=/home/zabbix. W takim przypadku pliki binarne demonów zostaną zainstalowane w <prefix>/sbin, a narzędzia w <prefix>/bin. Strony podręcznika man zostaną zainstalowane w <prefix>/share.

6 Przejrzyj i edytuj pliki konfiguracyjne

- edytuj plik konfiguracyjny agenta Zabbix **/usr/local/etc/zabbix_agentd.conf**

Musisz skonfigurować ten plik dla każdego hosta z zainstalowanym zabbix_agentd.

W pliku musisz podać **adres IP** serwera Zabbix. Połączenia z innych hostów będą odrzucane.

- edytuj plik konfiguracyjny serwera Zabbix **/usr/local/etc/zabbix_server.conf**

Musisz podać nazwę bazy danych, użytkownika i hasło (jeśli są używane).

Pozostałe parametry w przypadku małej instalacji (do dziesięciu monitorowanych hostów) mogą pozostać z wartościami domyślnymi. Jeśli jednak chcesz zmaksymalizować wydajność serwera Zabbix (lub proxy), powinieneś zmienić parametry domyślne.

- jeśli zainstalowano proxy Zabbix, edytuj plik konfiguracyjny proxy **/usr/local/etc/zabbix_proxy.conf**

Musisz podać adres IP serwera i nazwę hosta proxy (musi być znana serwerowi), a także nazwę bazy danych, użytkownika i hasło (jeśli są używane).

> **Note:**
> W przypadku SQLite należy podać pełną ścieżkę do pliku bazy danych; użytkownik i hasło bazy danych nie są wymagane.

7 Uruchom demony

Uruchom zabbix_server po stronie serwera.

```
zabbix_server
```

> **Note:**
> Upewnij się, że system pozwala na przydzielenie 36 MB (lub nieco więcej) pamięci współdzielonej, w przeciwnym razie serwer może się nie uruchomić i w pliku dziennika serwera zobaczysz „Cannot allocate shared memory for <type of cache>.”. Może się to zdarzyć w systemach FreeBSD i Solaris 8.

Uruchom zabbix_agentd na wszystkich monitorowanych maszynach.

```
zabbix_agentd
```

> **Note:**
> Upewnij się, że system pozwala na przydzielenie 2 MB pamięci współdzielonej, w przeciwnym razie agent może się nie uruchomić i w pliku dziennika agenta zobaczysz „Cannot allocate shared memory for collector.”. Może się to zdarzyć w systemie Solaris 8.

Jeśli zainstalowano Zabbix proxy, uruchom zabbix_proxy.

```
zabbix_proxy
```

Instalacja interfejsu webowego Zabbix

Kopiowanie plików PHP

Frontend Zabbix jest napisany w PHP, dlatego do jego uruchomienia wymagany jest serwer WWW obsługujący PHP. Instalacja polega po prostu na skopiowaniu plików PHP z katalogu ui do katalogu dokumentów HTML serwera WWW.

Typowe lokalizacje katalogów dokumentów HTML dla serwerów WWW Apache obejmują:

- /usr/local/apache2/htdocs (domyślny katalog przy instalacji Apache ze źródeł)
- /srv/www/htdocs (OpenSUSE, SLES)
- /var/www/html (Debian, Ubuntu, Fedora, RHEL)

Zaleca się użycie podkatalogu zamiast głównego katalogu HTML. Aby utworzyć podkatalog i skopiować do niego pliki frontend Zabbix, wykonaj następujące polecenia, zastępując <htdocs> rzeczywistym katalogiem:

```
mkdir <htdocs>/zabbix
cd ui
cp -a . <htdocs>/zabbix
```

Jeśli planujesz używać innego języka niż angielski, zobacz Instalacja dodatkowych języków frontend, aby uzyskać instrukcje.

Instalacja frontend

Aby uzyskać informacje o kreatorze instalacji frontend Zabbix, zobacz stronę Instalacja interfejsu webowego.

Instalacja ładowalnych wtyczek Zabbix agent 2

Instalacja ładowalnych wtyczek Zabbix agent 2 jest wymagana tylko wtedy, gdy chcesz monitorować cele nieobsługiwane przez wbudowane wtyczki (np. serwery lub klastry MongoDB, PostgreSQL i jego forków itp.). Zobacz pełną listę ładowalnych wtyczek oraz wbudowanych wtyczek.

Attention:
Przed zainstalowaniem wtyczki sprawdź jej plik README. Może on zawierać szczegółowe wymagania i instrukcje instalacji.

Aby zainstalować ze źródeł, najpierw pobierz i rozpakuj archiwum źródłowe ładowalnej wtyczki.

Aby skompilować wtyczkę, przejdź do rozpakowanego katalogu wtyczki i uruchom `make`:

```
make
```

Note:
Aby zbudować ładowalne wtyczki Zabbix agent 2, musi być zainstalowana obsługiwana wersja Go.

Plik wykonywalny wtyczki może zostać umieszczony w dowolnym miejscu, o ile może zostać załadowany przez Zabbix agent 2. Ścieżkę do pliku binarnego wtyczki należy określić w pliku konfiguracyjnym wtyczki, np. w pliku postgresql.conf dla wtyczki PostgreSQL:

```
Plugins.PostgreSQL.System.Path=/path/to/executable/zabbix-agent2-plugin-postgresql
```

Ścieżka do pliku konfiguracyjnego wtyczki musi zostać określona w parametrze Include pliku konfiguracyjnego Zabbix agent 2:

```
Include=/path/to/plugin/configuration/file/postgresql.conf
```

Przejdź do sekcji konfiguracja, aby uzyskać więcej informacji o konfigurowaniu wtyczek.

Ładowalne wtyczki dostarczane przez Zabbix używają prostych plików makefile z następującymi celami kompilacji:

- `make` - zbudowanie wtyczki
- `make clean` - usunięcie wszystkich plików utworzonych podczas budowania wtyczki
- `make check` - uruchomienie autotestów (wymaga rzeczywistego celu monitorowania, np. bazy danych PostgreSQL)
- `make style` - sprawdzenie stylu kodu Go za pomocą `golangci-lint`
- `make format` - formatowanie kodu Go za pomocą `go fmt`
- `make dist` - utworzenie archiwum źródłowego zawierającego wszystkie zależności

Instalacja Java gateway

Instalacja Java gateway jest wymagana tylko wtedy, gdy chcesz monitorować aplikacje JMX. Java gateway jest lekki i nie wymaga bazy danych.

Aby zainstalować ze źródeł, najpierw pobierz i rozpakuj archiwum źródłowe.

Aby skompilować Java gateway, uruchom skrypt `./configure` z opcją `--enable-java`. Zaleca się podanie opcji `--prefix`, aby wskazać ścieżkę instalacji inną niż domyślna /usr/local, ponieważ instalacja Java gateway utworzy całe drzewo katalogów, a nie tylko pojedynczy plik wykonywalny.

```
./configure --enable-java --prefix=$PREFIX
```

Aby skompilować i spakować Java gateway do pliku JAR, uruchom `make`. Zwróć uwagę, że na tym etapie będziesz potrzebować plików wykonywalnych `javac` i `jar` dostępnych w swojej ścieżce.

```
make
```

Teraz masz plik zabbix-java-gateway-$VERSION.jar w src/zabbix_java/bin. Jeśli odpowiada Ci uruchamianie Java gateway z katalogu src/zabbix_java w katalogu dystrybucji, możesz przejść do instrukcji dotyczących konfiguracji i uruchamiania Java gateway. W przeciwnym razie upewnij się, że masz wystarczające uprawnienia, i uruchom `make install`.

```
make install
```

Przejdź do konfiguracji, aby uzyskać więcej informacji na temat konfigurowania i uruchamiania Java gateway.

Instalacja usługi internetowej Zabbix

Instalacja usługi internetowej Zabbix jest wymagana tylko wtedy, gdy chcesz używać raportów harmonogramowanych.

Aby zainstalować ze źródeł, najpierw pobierz i rozpakuj archiwum źródłowe.

Aby skompilować usługę internetową Zabbix, uruchom skrypt `./configure` z opcją `--enable-webservice`.

Note:
Aby zbudować usługę internetową Zabbix, musi być zainstalowana obsługiwana wersja Go.

Uruchom zabbix_web_service na maszynie, na której usługa internetowa jest zainstalowana:

```
zabbix_web_service
```

Przejdź do sekcji konfiguracji, aby uzyskać więcej informacji o konfigurowaniu generowania raportów harmonogramowanych.

Pobieranie kodu źródłowego Zabbix

Istnieje kilka sposobów pobrania kodu źródłowego Zabbix:

- Możesz pobrać wydane stabilne wersje z oficjalnej strony internetowej Zabbix
- Możesz pobrać kompilacje nightly ze strony dla deweloperów w oficjalnym serwisie Zabbix
- Możesz pobrać najnowszą wersję rozwojową z repozytorium kodu źródłowego Git:
  - Główna lokalizacja pełnego repozytorium znajduje się pod adresem https://git.zabbix.com/scm/zbx/zabbix.git
  - Gałąź master oraz obsługiwane wydania są również mirrorowane w Github pod adresem https://github.com/zabbix/zabbix

Aby sklonować repozytorium, musi być zainstalowany klient Git. Oficjalny pakiet klienta Git uruchamianego z wiersza poleceń jest w dystrybucjach zwykle nazywany **git**. Aby go zainstalować, na przykład w Debian/Ubuntu, uruchom:

```
sudo apt-get update
sudo apt-get install git
```

Aby pobrać cały kod źródłowy Zabbix, przejdź do katalogu, w którym chcesz umieścić kod, i wykonaj:

```
git clone https://git.zabbix.com/scm/zbx/zabbix.git
```

Problemy z kompilacją

Są to znane problemy dotyczące kompilacji Zabbix ze źródeł. We wszystkich pozostałych przypadkach zobacz stronę Znane problemy.

Biblioteka w niestandardowej lokalizacji

Zabbix umożliwia wskazanie biblioteki znajdującej się w niestandardowej lokalizacji. W poniższym przykładzie Zabbix uruchomi `curl-config` z podanej niestandardowej lokalizacji i użyje jego danych wyjściowych do określenia właściwej biblioteki libcurl.

```
$ ./configure --enable-server --with-mysql --with-libcurl=/usr/local/bin/curl-config
```

To zadziała, jeśli jest to jedyna biblioteka libcurl zainstalowana w systemie, ale może nie zadziałać, jeśli inna biblioteka libcurl jest zainstalowana w standardowej lokalizacji (na przykład przez menedżera pakietów). Taka sytuacja występuje wtedy, gdy dla Zabbix potrzebna jest nowsza wersja biblioteki, a starsza dla innych aplikacji.

Dlatego wskazanie komponentu w niestandardowej lokalizacji nie zawsze będzie działać, jeśli ten sam komponent istnieje również w standardowej lokalizacji.

Na przykład, jeśli używasz nowszej biblioteki libcurl zainstalowanej w `/usr/local`, podczas gdy pakiet libcurl nadal jest zainstalowany, Zabbix może wybrać niewłaściwą bibliotekę i kompilacja zakończy się niepowodzeniem:

```
usr/bin/ld: ../../src/libs/zbxhttp/libzbxhttp.a(http.o): in function 'zbx_http_convert_to_utf8':
/tmp/zabbix-master/src/libs/zbxhttp/http.c:957: undefined reference to 'curl_easy_header'
collect2: error: ld returned 1 exit status
```

Tutaj funkcja `curl_easy_header()` nie jest dostępna w starszej bibliotece `/usr/lib/x86_64-linux-gnu/libcurl.so`, ale jest dostępna w nowszej `/usr/local/lib/libcurl.so`.

Problem wynika z kolejności flag linkera, a jednym z rozwiązań jest podanie pełnej ścieżki do biblioteki w zmiennej LDFLAGS:

```
$ LDFLAGS="-Wl,--no-as-needed /usr/local/lib/libcurl.so" ./configure --enable-server --with-mysql --with-l
```

Zwróć uwagę na opcję `-Wl,--no-as-needed`, która może być wymagana w niektórych systemach (zobacz także: domyślne opcje linkowania w systemach opartych na Debianie).

Zbyt mały rozmiar stosu w niektórych systemach

Jeśli Zabbix ulega awarii lub zawiesza się z powodu przepełnienia stosu, możesz zwiększyć rozmiar stosu na wątek za pomocą opcji `--with-stacksize` podczas konfigurowania źródeł. Ten problem może występować w systemach z niskimi domyślnymi limitami rozmiaru stosu wątków, szczególnie podczas preprocessingu, gdy tworzonych jest wiele wątków.

Poniższy przykład ustawia rozmiar stosu na 512 KB na wątek:

```
./configure --enable-server --with-mysql --with-stacksize=512
```

Możesz sprawdzić limity rozmiaru stosu wątków w systemie w czasie działania za pomocą polecenia `ulimit -s` w systemach opartych na Linuksie.

Uwagi dotyczące instalacji z pakietów

Przegląd

Oficjalne pakiety **przedpremierowe** Zabbix 8.0 są dostępne na stronie internetowej Zabbix.

Wybierz swój system operacyjny i komponent Zabbix, aby wygenerować instrukcje instalacji odpowiednie dla Twojego środowiska. Zobacz także uwagi dotyczące instalacji pakietów na tej stronie, aby uzyskać ważne dodatkowe informacje, a także sekcję Instalacja i konfiguracja.

Pakiety są dostępne dla następujących dystrybucji Linuksa:

- Red Hat Enterprise Linux i jego pochodne: AlmaLinux, Amazon Linux 2023, CentOS Stream, CentOS 7, Oracle Linux, Rocky Linux
- Debian, Ubuntu, Raspberry Pi OS, Raspbian
- SUSE Linux Enterprise Server, openSUSE Leap

Attention:
Niektóre dystrybucje systemów operacyjnych (w szczególności dystrybucje oparte na Debianie) udostępniają własne pakiety Zabbix. Pakiety te **nie** są wspierane przez Zabbix i mogą być nieaktualne lub nie zawierać najnowszych funkcji oraz poprawek błędów. Zaleca się używanie wyłącznie oficjalnych pakietów z Oficjalnego repozytorium Zabbix. Jeśli wcześniej zainstalowano Zabbix z repozytorium systemu operacyjnego, zobacz kroki dotyczące aktualizacji pakietów Zabbix z repozytoriów systemu operacyjnego.

Pakiety obsługują bazy danych MySQL/PostgreSQL oraz serwer WWW Apache/Nginx. Należy pamiętać, że serwer Zabbix i proxy nie mogą współdzielić tej samej bazy danych; jeśli oba są zainstalowane na tym samym hoście, użyj różnych nazw baz danych.

W razie potrzeby oddzielne pakiety dla Zabbix agent/agent 2, Zabbix get i Zabbix sender są dostępne w Oficjalnym repozytorium Zabbix.

Zabbix udostępnia również wstępnie skompilowane pliki binarne Zabbix agent dla systemów operacyjnych innych niż Linux; zobacz:

- Instalacja agenta w systemie Windows z pakietu MSI
- Instalacja agenta w systemie macOS z pakietu PKG
- Starsze pliki binarne (dla starszych/mniej popularnych systemów, takich jak HP-UX, NetBSD, Tru64 i starsze wersje SLES)

Uwagi dotyczące instalacji pakietów

Poniższe uwagi dotyczą wszystkich systemów:

- W przypadku korzystania z PostgreSQL, ustawienie `DBHost=localhost` (lub adresu IP) w konfiguracji Zabbix serwer/proxy powoduje, że PostgreSQL używa gniazda sieciowego zamiast lokalnego gniazda UNIX; powiązane instrukcje konfiguracji znajdują się w sekcji Konfiguracja SELinux.
- W przypadku korzystania z TimescaleDB, zobacz dodatkowe informacje w sekcji Konfiguracja TimescaleDB.
- W przypadku instalacji Zabbix Java gateway (do monitorowania aplikacji JMX), zobacz dodatkowe instrukcje konfiguracji dla systemów opartych na RHEL i systemów opartych na Debianie.
- Aby uruchamiać Zabbix agent jako root, zobacz Uruchamianie agent jako root.

Poniższe uwagi dotyczą RHEL i jego pochodnych:

- Jeśli włączono repozytorium EPEL dla EL9, które również udostępnia pakiety Zabbix, musi ono zostać wykluczone z rozwiązywania pakietów przed instalacją oficjalnych pakietów Zabbix; zobacz Przypadkowa instalacja pakietów Zabbix z EPEL.
- Aby instalować pakiety Zabbix w środowiskach Red Hat UBI, zobacz Pakiety Zabbix dla RHEL w środowiskach Red Hat UBI.
- W przypadku korzystania z pozycji ICMP ping, pakiety dla `fping` są również dostępne w Oficjalnym repozytorium Zabbix.

Konfiguracja SELinux

Zabbix używa komunikacji międzyprocesowej opartej na gniazdach. W systemach, w których Security-Enhanced Linux (SELinux) jest włączony, może być konieczne dodanie reguł SELinux, aby umożliwić Zabbix tworzenie/używanie gniazd domeny UNIX w katalogu SocketDir. Pliki gniazd są używane przez Zabbix serwer (alerter, preprocessing, IPMI) oraz Zabbix proxy (IPMI) i są obecne podczas działania procesu.

Jeśli SELinux jest włączony w trybie enforcing, wykonaj następujące polecenia, aby włączyć komunikację między Zabbix frontend a serwerem:

Dla RHEL 7 (i nowszych), AlmaLinux, CentOS Stream, Oracle Linux, Rocky Linux 8 (i nowszych):

```
setsebool -P httpd_can_connect_zabbix on
```

Jeśli dostęp do bazy danych odbywa się przez sieć (w tym `localhost` dla PostgreSQL), zezwól również Zabbix frontend na łączenie się z bazą danych:

```
setsebool -P httpd_can_network_connect_db on
```

Dla RHEL wcześniejszych niż 7:

```
setsebool -P httpd_can_network_connect on
setsebool -P zabbix_can_network on
```

Po zastosowaniu ustawień SELinux uruchom ponownie Apache:

```
systemctl restart httpd
```

Opcjonalnie możesz zainstalować predefiniowany pakiet `zabbix-selinux-policy` z Oficjalnego repozytorium Zabbix. Pakiet ten jest udostępniany dla wszystkich wspieranych wersji systemów operacyjnych, aby uprościć wdrożenie Zabbix i zapobiec wyłączaniu SELinux przez użytkowników z powodu złożoności konfiguracji.

> **Attention:**
> Dla maksymalnego bezpieczeństwa zaleca się ustawienie niestandardowych ustawień SELinux.

Pakiet `zabbix-selinux-policy` zawiera podstawową politykę SELinux, umożliwiającą Zabbix tworzenie i używanie gniazd oraz włączającą połączenie HTTPd z PostgreSQL (używanym przez frontend).

Plik źródłowy `zabbix_policy.te` zawiera następujące reguły:

```
module zabbix_policy 1.2;

require {
    type zabbix_t;
    type zabbix_port_t;
    type zabbix_var_run_t;
    type postgresql_port_t;
    type httpd_t;
    class tcp_socket name_connect;
    class sock_file { create unlink };
    class unix_stream_socket connectto;
}

####============= zabbix_t ==============
allow zabbix_t self:unix_stream_socket connectto;
allow zabbix_t zabbix_port_t:tcp_socket name_connect;
allow zabbix_t zabbix_var_run_t:sock_file create;
allow zabbix_t zabbix_var_run_t:sock_file unlink;
allow httpd_t zabbix_port_t:tcp_socket name_connect;

####============= httpd_t ==============
allow httpd_t postgresql_port_t:tcp_socket name_connect;
```

Pakiety debuginfo

Pakiety debuginfo zawierają symbole debugowania dla plików binarnych Zabbix. Nie są wymagane do normalnej instalacji ani działania, ale są przydatne przy zaawansowanym rozwiązywaniu problemów.

Aby włączyć repozytorium `zabbix-debuginfo`:

- W systemie RHEL 7 edytuj plik `/etc/yum.repos.d/zabbix.repo` i ustaw `enabled=1` dla sekcji `zabbix-debuginfo`:

```
[zabbix-debuginfo]
name=Zabbix Official Repository debuginfo - $basearch
baseurl=http://repo.zabbix.com/zabbix/8.0/stable/rhel/7/$basearch/debuginfo/
enabled=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-ZABBIX-A14FE591
gpgcheck=1
```

- W systemie SUSE edytuj plik `/etc/zypp/repos.d/zabbix.repo` i ustaw `enabled=1` dla sekcji `zabbix-debuginfo`:

```
[zabbix-debuginfo]
name=Zabbix Official Repository debuginfo
type=rpm-md
baseurl=https://repo.zabbix.com/zabbix/8.0/stable/sles/15/x86_64/debuginfo/
gpgcheck=1
gpgkey=https://repo.zabbix.com/zabbix/8.0/stable/sles/15/x86_64/debuginfo/repodata/repomd.xml.key
enabled=0
update=1
```

Po włączeniu zainstaluj pakiety:

- W systemie RHEL zainstaluj pojedynczy pakiet z informacjami debugowania dla wszystkich komponentów Zabbix:

```
dnf install zabbix-debuginfo
```

- W systemie SUSE zainstaluj pakiety debuginfo specyficzne dla komponentów:

```
zypper install zabbix-<component>-debuginfo
```

Włączanie repozytoriów niestabilnych wydań

Poniższe instrukcje dotyczą włączania repozytoriów niestabilnych wydań Zabbix (domyślnie wyłączonych), używanych dla kandydatów do wydań pomniejszych wersji Zabbix.

Najpierw zainstaluj lub zaktualizuj pakiet zabbix-release do najnowszej wersji. Aby włączyć pakiety rc w swoim systemie, wykonaj następujące czynności:

Red Hat Enterprise Linux

Otwórz plik `/etc/yum.repos.d/zabbix.repo` i ustaw `enabled=1` dla repozytorium `zabbix-unstable`.

```
[zabbix-unstable]
name=Zabbix Official Repository (unstable) - $basearch
baseurl=https://repo.zabbix.com/zabbix/8.0/unstable/rhel/8/$basearch/
enabled=1
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-ZABBIX-A14FE591
```

Debian/Ubuntu

Otwórz plik `/etc/apt/sources.list.d/zabbix.list` i odkomentuj „niestabilne repozytorium Zabbix”.

```
#### Zabbix unstable repository
deb https://repo.zabbix.com/zabbix/8.0/unstable/debian bullseye main
deb-src https://repo.zabbix.com/zabbix/8.0/unstable/debian bullseye main
```

SUSE

Otwórz plik `/etc/zypp/repos.d/zabbix.repo` i ustaw `enabled=1` dla repozytorium `zabbix-unstable`.

```
[zabbix-unstable]
name=Zabbix Official Repository
type=rpm-md
baseurl=https://repo.zabbix.com/zabbix/8.0/unstable/sles/15/x86_64/
gpgcheck=1
gpgkey=https://repo.zabbix.com/zabbix/8.0/unstable/sles/15/x86_64/repodata/repomd.xml.key
enabled=1
update=1
```

Instalacja agenta Windows z pakietu MSI

Przegląd

Zabbix agent można zainstalować w systemie Windows przy użyciu 32-bitowych lub 64-bitowych pakietów instalatora MSI, dostępnych do pobrania.

Minimalne wymagania systemu operacyjnego dla instalacji MSI to:

- **Dla Zabbix agent:** Windows XP (64-bit) lub Windows Server 2003

- **Dla Zabbix agent 2:** Windows 10 (32-bit) lub Windows Server 2016

Pakietów 32-bitowych nie można instalować w systemach 64-bitowych.

Pakiety zawierają:

- obsługę TLS (konfiguracja TLS jest opcjonalna)
- narzędzia Zabbix get i Zabbix sender (mogą być instalowane razem z Zabbix agent/agent 2 lub osobno)

Attention:
Pakiety Zabbix agent 2 nie zawierają ładowalnych wtyczek (MongoDB, PostgreSQL, MSSQL), które należy pobrać i zainstalować osobno.

Instalację można przeprowadzić przy użyciu kreatora instalacji lub wiersza poleceń.

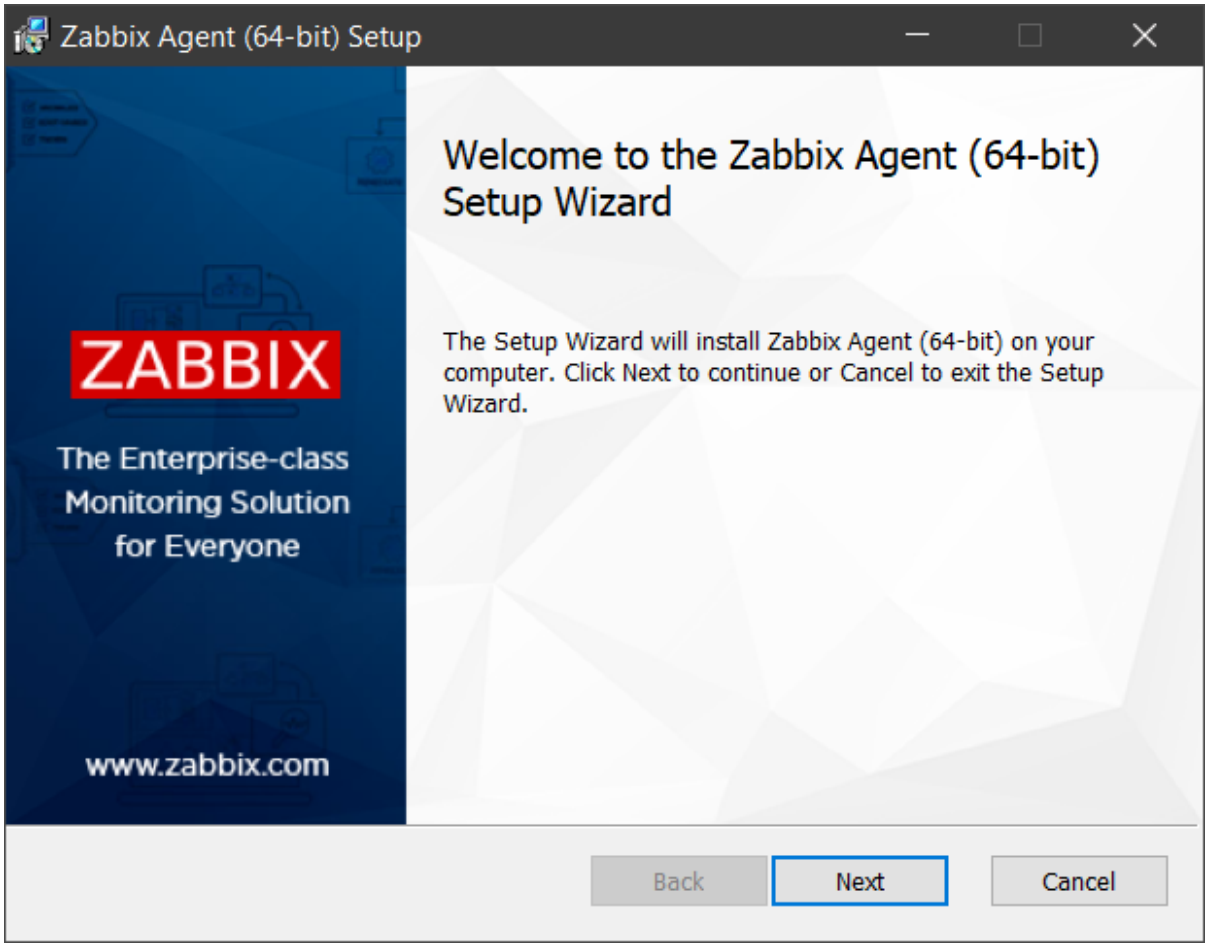
Chociaż instalacja przy użyciu pakietów MSI jest w pełni obsługiwana, zaleca się zainstalowanie co najmniej Microsoft .NET Framework 2, aby zapewnić prawidłową obsługę błędów.

Attention:
Zaleca się użycie domyślnej lokalizacji instalacji oferowanej przez instalator. Użycie niestandardowej lokalizacji bez wymaganych uprawnień może obniżyć bezpieczeństwo instalacji.

Instalacja za pomocą kreatora konfiguracji

Poniższe kroki instalacji dotyczą zarówno Zabbix agent, jak i Zabbix agent 2.

1. Kliknij dwukrotnie pobrany plik MSI, aby rozpocząć instalację:

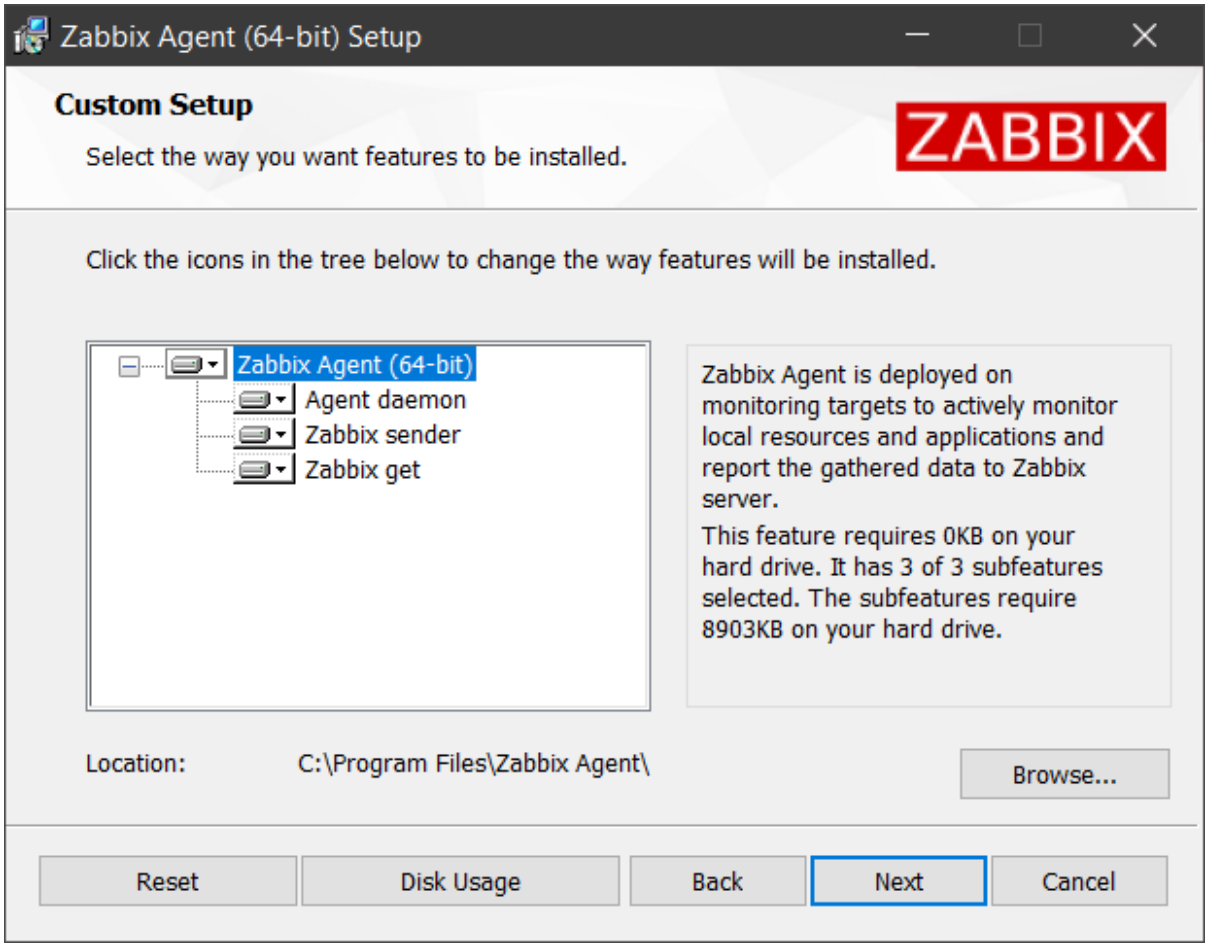


2. Zaakceptuj umowę licencyjną użytkownika końcowego:



3. Wybierz komponenty Zabbix (Agent daemon, Zabbix sender, Zabbix get), które mają zostać zainstalowane:

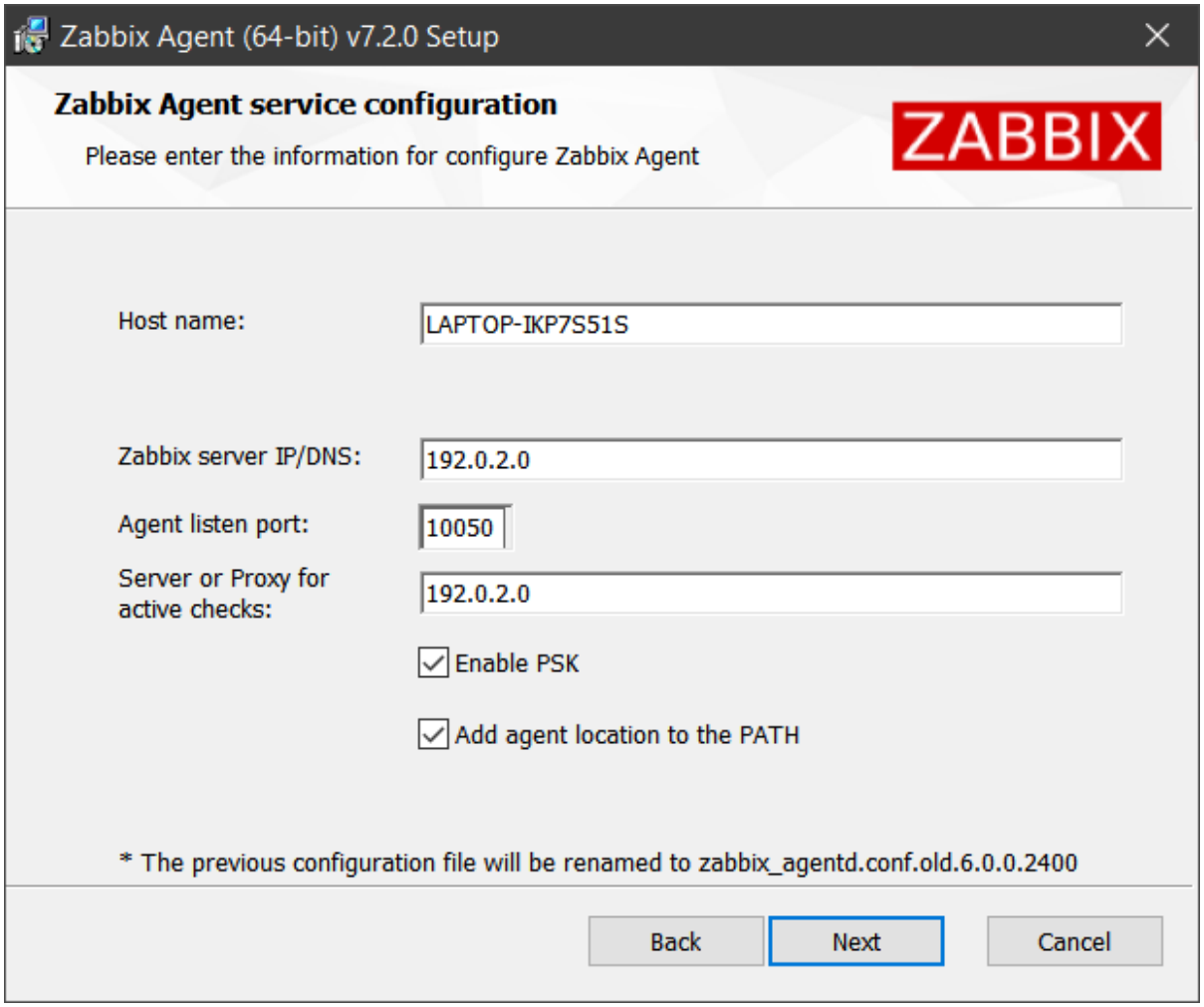
Attention:
Zaleca się użycie domyślnej lokalizacji instalacji podanej przez instalator. Użycie niestandardowej lokalizacji bez wymaganych uprawnień może zagrozić bezpieczeństwu instalacji.



4. Skonfiguruj następujące parametry. Ich wartości zostaną ustawione w pliku konfiguracyjnym Zabbix agent:

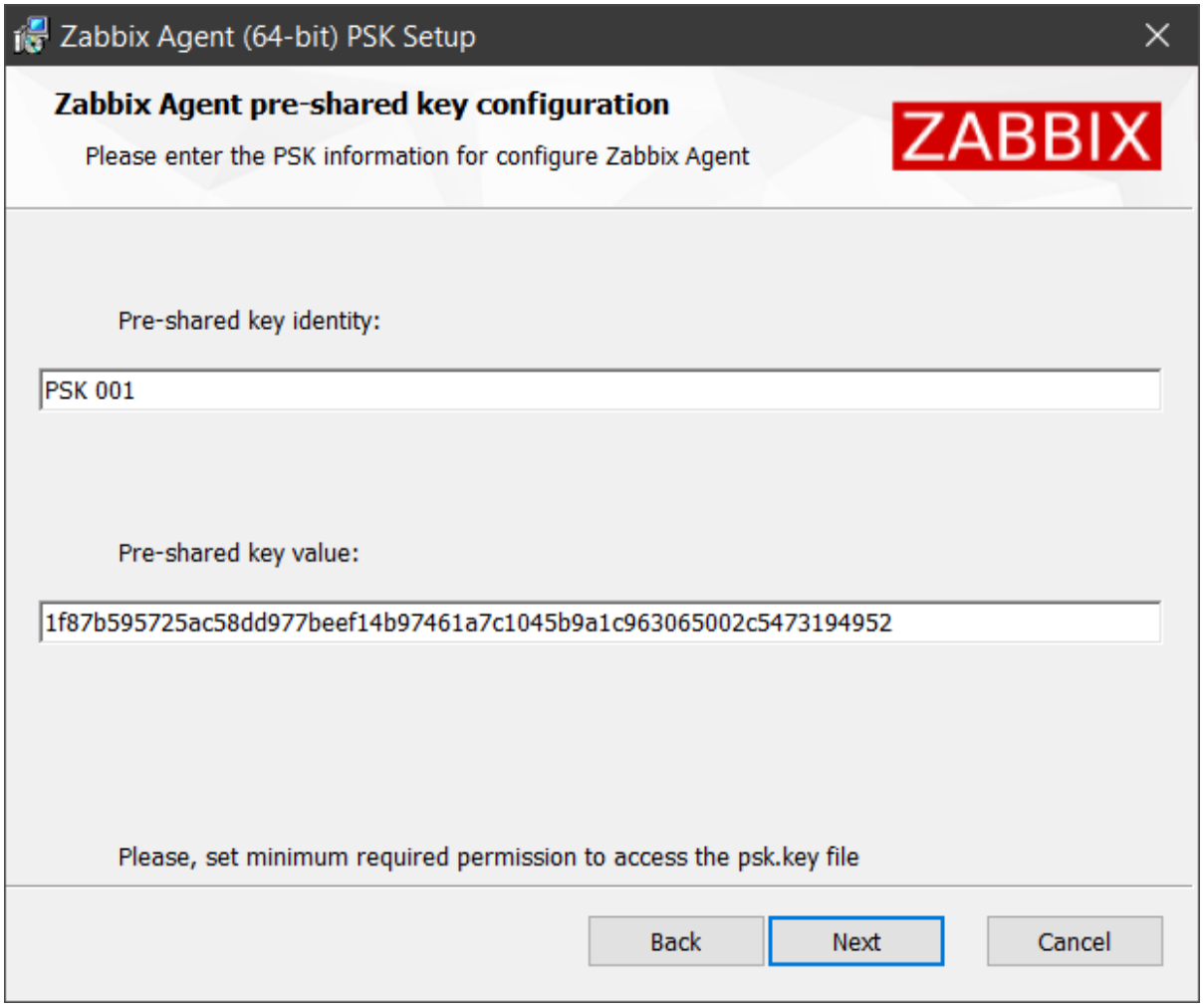
Parameter	Description
Host name	Nazwa hosta maszyny, na której instalowany jest Zabbix agent. Ustawia parametr Hostname.
Zabbix server IP/DNS	Lista adresów IP oddzielonych przecinkami, opcjonalnie w notacji CIDR, lub nazw DNS serwerów Zabbix albo proxy Zabbix. Ten parametr jest **obowiązkowy**. Ustawia parametr Server.
Agent listen port	agent będzie nasłuchiwał na tym porcie połączeń z serwera. Ustawia parametr ListenPort.
Server or Proxy for active checks	Adres serwera/proxy Zabbix lub konfiguracja klastra, z którego mają być pobierane active checks. Adres serwera/proxy to adres IP lub nazwa DNS oraz opcjonalny port oddzielony dwukropkiem. Ustawia parametr ServerActive.
Enable PSK	Zaznacz pole wyboru, aby włączyć obsługę TLS przy użyciu kluczy współdzielonych. Ustawia parametry TLSConnect i TLSAccept na psk.
Add agent location to the PATH	Zaznacz pole wyboru, aby dodać lokalizację Zabbix agent do systemowej zmiennej PATH.

Note:
Jeśli zostanie wykryty istniejący Zabbix agent, zostaną wyświetlone wartości parametrów z jego pliku konfiguracyjnego. Dodatkowo istniejący plik konfiguracyjny zostanie podczas instalacji przemianowany, a następnie zostanie utworzony nowy plik konfiguracyjny.



5. Skonfiguruj parametry PSK, jeśli w poprzednim kroku zaznaczono pole wyboru *Enable PSK*. Te parametry również zostaną ustawione w pliku konfiguracyjnym Zabbix agent:

Parameter	Description
Pre-shared key identity	Ciąg identyfikatora klucza współdzielonego. Ustawia parametr TLSPSKIdentity.
Pre-shared key value	Wartość ciągu klucza współdzielonego. Tworzy plik psk.key zawierający klucz i ustawia parametr TLSPSKFile na lokalizację klucza (domyślnie: `C:\Program Files\Zabbix Agent\psk.key`). **Zaleca się** ograniczenie dostępu do pliku klucza współdzielonego przez dostosowanie ustawień zabezpieczeń pliku tak, aby tylko Zabbix agent (lub użytkownik uruchamiający agent) mógł go odczytać.

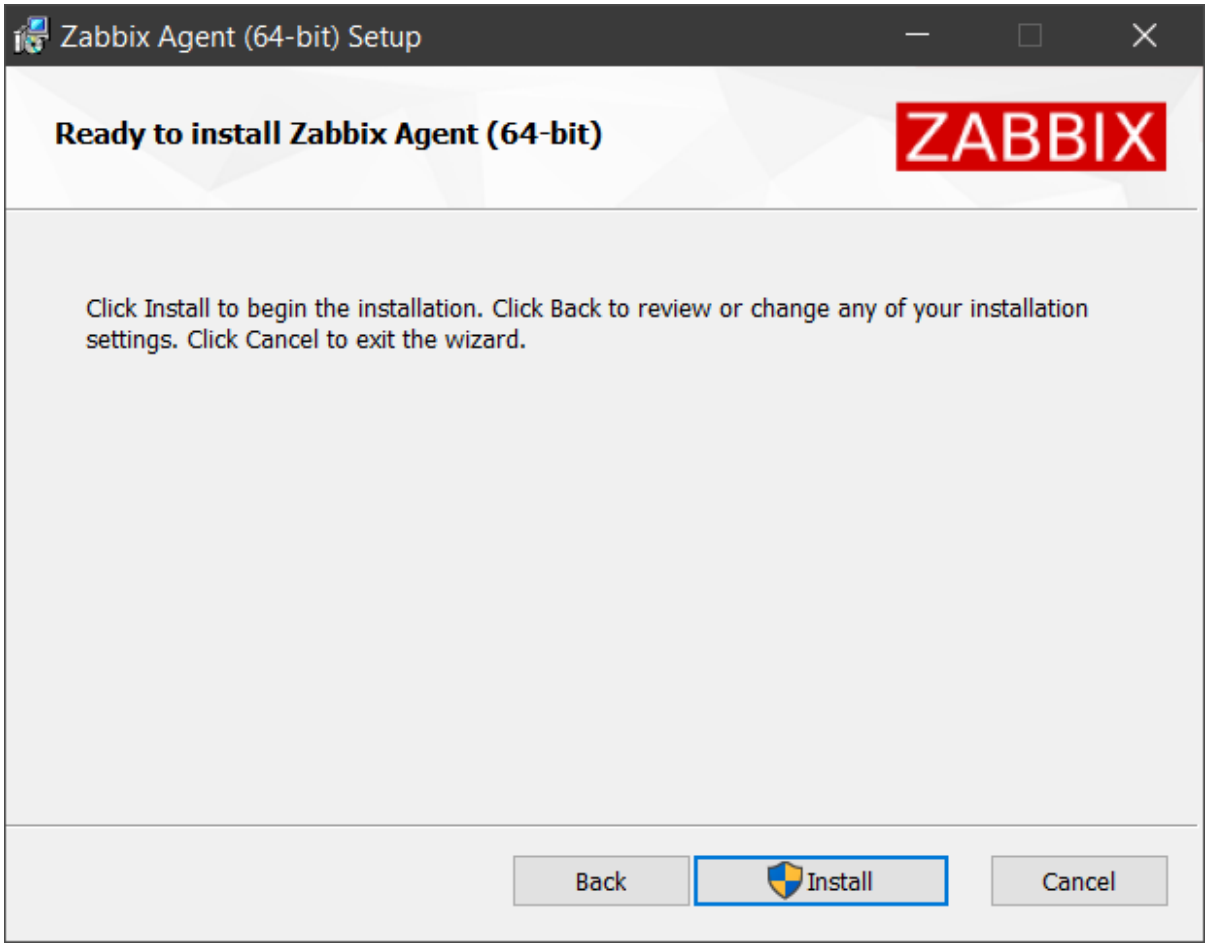


6. Kliknij *Install*, aby rozpocząć instalację.

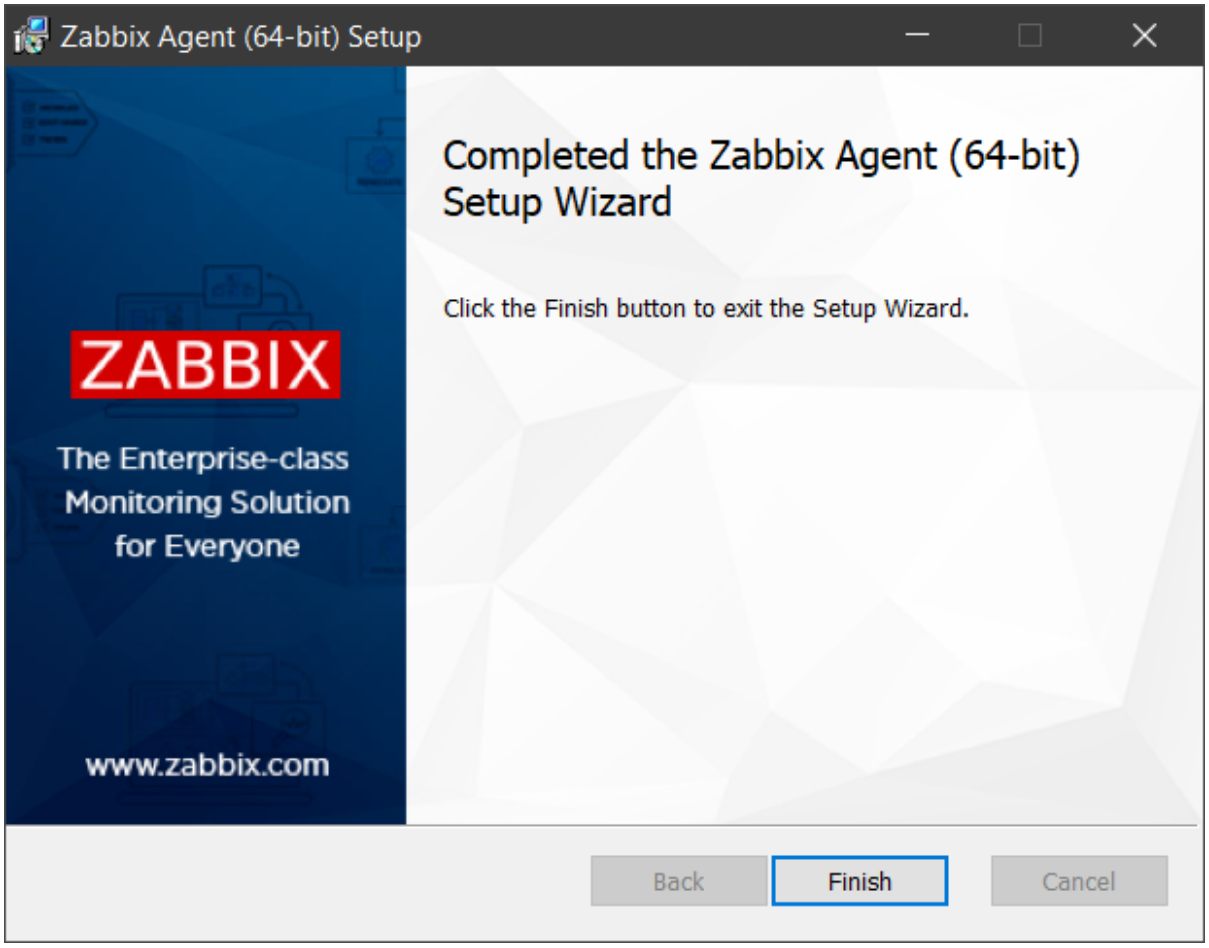
Wszystkie wybrane komponenty Zabbix oraz plik konfiguracyjny Zabbix agent zostaną zainstalowane w określonej lokalizacji (domyślnie: `C:\Program Files\Zabbix Agent`). To samo dotyczy Zabbix agent 2, z tym wyjątkiem, że dodatkowe pliki konfiguracyjne dla jego wbudowanych wtyczek zostaną zainstalowane w podfolderze `zabbix_agent2.d\plugins.d`.

Dodatkowo plik zabbix_agentd.exe (lub zabbix_agent2.exe) zostanie skonfigurowany jako usługa Windows z opóźnionym automatycznym uruchamianiem (lub automatycznym uruchamianiem w wersjach Windows wcześniejszych niż Windows Vista/Server 2008).

Jeśli podczas instalacji działa inna wersja Zabbix agent, pojawi się monit z wyborem: zamknąć aplikację i spróbować uruchomić ją ponownie albo pozostawić ją otwartą, co będzie wymagało ponownego uruchomienia systemu.



7. Kliknij przycisk *Finish*, aby zamknąć kreatora konfiguracji.



Instalacja z wiersza poleceń

Agent Zabbix można zainstalować z wiersza poleceń, uruchamiając instalator MSI za pomocą msiexec. Na przykład:

```
msiexec.exe /l*v "C:\package.log" /i "C:\zabbix_agent-8.0.0-windows-amd64-openssl.msi" /qn+ SERVER=192.0.2
```

Ta metoda umożliwia instalacje nienadzorowane oraz niestandardową konfigurację przy użyciu parametrów.

Obsługiwane parametry

Pakiety instalatora MSI Zabbix agent obsługują następujące parametry zarówno dla Zabbix agent, jak i Zabbix agent 2.

Note:
Parametry Zabbix agent/agent2 są ustawiane w pliku konfiguracyjnym podczas instalacji. Kliknij nazwę parametru, aby wyświetlić jego szczegółowy opis oraz przykłady konfiguracji na stronie Zabbix agent (Windows). W przypadku Zabbix agent 2 zobacz stronę Zabbix agent 2 (Windows).

Parameter	Description
ADDDEFAULT	Lista komponentów rozdzielonych przecinkami do zainstalowania w ich domyślnej konfiguracji. Więcej informacji znajduje się w właściwości ADDDEFAULT. Możliwe wartości: `AgentProgram`, `GetProgram`, `SenderProgram`, `ALL` Przykład: `ADDDEFAULT=AgentProgram,GetProgram`
ADDLOCAL	Lista komponentów rozdzielonych przecinkami do zainstalowania lokalnie. Więcej informacji znajduje się w właściwości ADDLOCAL. Możliwe wartości: `AgentProgram`, `GetProgram`, `SenderProgram`, `ALL` Przykład: `ADDLOCAL=AgentProgram,SenderProgram`
ALLOWDENYKEY	Lista parametrów AllowKey lub DenyKey rozdzielonych średnikami służących do ograniczania kontroli Zabbix agent. W razie potrzeby użyj ukośnika odwrotnego, aby poprzedzić separator znakiem ucieczki (`\;`). Ustawia parametry AllowKey i DenyKey w pliku konfiguracyjnym agenta. Przykład: `ALLOWDENYKEY="AllowKey=system.run[more C:\Windows\System32\drivers\etc\hosts\\; echo 'File read complete'];DenyKey=system.run[*]"`
CONF	Pełna ścieżka do szablon pliku konfiguracyjnego dla Zabbix agent. Podczas instalacji plik ten stanie się plikiem konfiguracyjnym agenta. Plik musi zawierać co najmniej parametry Server i LogFile. Przykład: `CONF="C:\full\path\to\example.conf"`
DONOTSTART	Użyj `DONOTSTART=1`, aby uniemożliwić instalatorowi MSI uruchomienie usługi Zabbix agent.
ENABLEPATH	Użyj `ENABLEPATH=1`, aby dodać lokalizację Zabbix agent do systemowej zmiennej PATH.
ENABLEPERSISTENTBUFFER	Tylko Zabbix agent 2. Włącza użycie lokalnej trwałej pamięci masowej dla aktywnych pozycji.
HOSTINTERFACE	Opcjonalny parametr definiujący interfejs hosta.
HOSTMETADATA	Opcjonalny parametr definiujący metadane hosta.
HOSTMETADATAITEM	Opcjonalny parametr definiujący pozycja używaną do pobierania metadanych hosta.
HOSTNAME	Opcjonalny parametr definiujący nazwę hosta.
HOSTNAMEITEM	Opcjonalny parametr definiujący pozycja używaną do pobierania nazwy hosta.
INCLUDE	Lista pojedynczych plików lub wszystkich plików w katalogu, rozdzielonych średnikami, które mają zostać dołączone do pliku konfiguracyjnego Zabbix agent.
INSTALLFOLDER	Pełna ścieżka do folderu, w którym zostaną zainstalowane komponenty Zabbix oraz plik konfiguracyjny Zabbix agent. W przypadku Zabbix agent 2 dodatkowe pliki konfiguracyjne dla wbudowanych wtyczek zostaną zainstalowane w podfolderze `zabbix_agent2.d\plugins.d`. Przykład: `INSTALLFOLDER="C:\Program Files\Zabbix Agent"`
LISTENIP	Lista adresów IP rozdzielonych przecinkami, na których agent powinien nasłuchiwać.
LISTENPORT	Agent będzie nasłuchiwał na tym porcie połączeń z serwer.
LOGFILE	Nazwa pliku dziennika Zabbix agent.
LOGTYPE	Typ wyjścia dziennika.
NONMSICONFNAME	Pełna ścieżka do niestandardowego pliku konfiguracyjnego dla Zabbix agent. Podczas instalacji wszelkie prawidłowe parametry konfiguracji agenta obecne w tym pliku (ograniczone do tych wymienionych w tej tabeli) zostaną zapisane w nowo utworzonym pliku konfiguracyjnym agenta. Plik musi zawierać co najmniej parametr Server. Przykład: `NONMSICONFNAME="C:\full\path\to\example.conf"`
PERSISTENTBUFFERFILE	Tylko Zabbix agent 2. Plik, w którym Zabbix agent 2 powinien przechowywać bazę danych SQLite.
PERSISTENTBUFFERPERIOD	Tylko Zabbix agent 2. Okres, przez który dane powinny być przechowywane, gdy nie ma połączenia z serwer lub proxy.
SERVER	Lista adresów IP rozdzielonych przecinkami, opcjonalnie w notacji CIDR, lub nazw DNS serwerów Zabbix albo proxy Zabbix. Ten parametr jest **obowiązkowy**, z wyjątkiem sytuacji, gdy STARTAGENTS jest ustawione na 0.

Parameter	Description
SERVERACTIVE	Adres Zabbix serwer/proxy lub konfiguracja klastra, z którego mają być pobierane aktywne kontrole.
SKIP	Użyj `SKIP=fw`, aby uniemożliwić instalatorowi MSI dodanie reguły wyjątku Zapory systemu Windows dla Zabbix agent.
SOURCEIP	Źródłowy adres IP dla połączeń wychodzących do Zabbix serwer lub Zabbix proxy albo do nawiązywania połączeń podczas wykonywania niektórych pozycji (web.page.get, net.tcp.port itd.).
STARTAGENTS	Liczba wstępnie utworzonych instancji zabbix_agentd przetwarzających kontrole pasywne. Jeśli ustawione na 0, kontrole pasywne są wyłączone, a agent nie będzie nasłuchiwał na żadnym porcie TCP.
STARTUPTYPE	Typ uruchamiania usługi Zabbix agent. Możliwe wartości: **automatic** - uruchom usługę automatycznie podczas startu systemu Windows; **delayed** - *(domyślnie)* opóźnij uruchomienie usługi do momentu zakończenia uruchamiania usług startowanych automatycznie (dostępne w systemach Windows Vista/Server 2008 i nowszych); **manual** - uruchom usługę ręcznie (przez użytkownika lub aplikację); **disabled** - wyłącz usługę, aby nie mogła zostać uruchomiona przez użytkownika lub aplikację. Przykład: `STARTUPTYPE=disabled`
STATUSPORT	Tylko Zabbix agent 2. Jeśli ustawione, agent będzie nasłuchiwał na tym porcie żądań statusu HTTP (http://localhost:<port>/status).
TIMEOUT	Określa, jak długo czekać (w sekundach) na ustanowienie połączenia i wymianę danych z Zabbix proxy lub serwer.
TLSACCEPT	Przychodzące połączenia do zaakceptowania (używane dla kontroli pasywnych). Jeśli ustawione na `psk`, wówczas TLSCONNECT również zostanie ustawione na `psk` (o ile nie określono inaczej).
TLSCAFILE	Pełna ścieżka do pliku zawierającego certyfikaty głównych urzędów certyfikacji (CA) do weryfikacji certyfikatu strony zdalnej.
TLSCERTFILE	Pełna ścieżka do pliku zawierającego certyfikat agenta lub łańcuch certyfikatów.
TLSCONNECT	Sposób, w jaki agent powinien łączyć się z Zabbix serwer lub proxy (używane dla kontroli aktywnych). Jeśli ustawione na `psk`, wówczas TLSACCEPT również zostanie ustawione na `psk` (o ile nie określono inaczej).
TLSCRLFILE	Pełna ścieżka do pliku zawierającego unieważnione certyfikaty.
TLSKEYFILE	Pełna ścieżka do pliku zawierającego klucz prywatny Zabbix agent.
TLSPSKFILE	Pełna ścieżka do pliku zawierającego klucz współdzielony Zabbix agent. Jeśli ustawione są zarówno TLSPSKFILE, jak i TLSPSKVALUE, wartość TLSPSKVALUE zostanie zapisana do pliku określonego w TLSPSKFILE. **Zaleca się** ograniczenie dostępu do pliku z kluczem współdzielonym przez dostosowanie ustawień zabezpieczeń pliku tak, aby tylko Zabbix agent (lub użytkownik uruchamiający agenta) mógł go odczytać.
TLSPSKIDENTITY	Ciąg tożsamości klucza współdzielonego.
TLSPSKVALUE	Wartość ciągu klucza współdzielonego. Jeśli ustawione są zarówno TLSPSKFILE, jak i TLSPSKVALUE, wartość TLSPSKVALUE zostanie zapisana do pliku określonego w TLSPSKFILE. Przykład: `TLSPSKVALUE=1f87b595725ac58dd977beef14b97461a7c1045b9a1c963065002c5473194952`
TLSSERVERCERTISSUER	Dozwolony wystawca certyfikatu serwer (proxy).
TLSSERVERCERTSUBJECT	Dozwolony podmiot certyfikatu serwer (proxy).
UNSAFEUSERPARAMETERS	Zezwala na przekazywanie wszystkich znaków w argumentach do parametrów zdefiniowanych przez użytkownika.

Przykłady

Poniższy przykład instaluje agent Zabbix z niestandardową konfiguracją. Włącza również obsługę TLS przy użyciu kluczy współdzielonych.

```
mkdir "C:\Program Files\Zabbix Agent" 2>nul
msiexec.exe /l*v "C:\package.log" /i "C:\zabbix_agent-8.0.0-windows-amd64-openssl.msi" /qn+^
 SERVER=192.0.2.0^
 INSTALLFOLDER="C:\Program Files\Zabbix Agent"^
 HOSTNAME=LAPTOP-IKP7S51S^
 TLSACCEPT=psk^
 TLSCONNECT=psk^
 TLSPSKIDENTITY="PSK 001"^
 TLSPSKFILE="C:\Program Files\Zabbix Agent\psk.key"^
 TLSPSKVALUE=1f87b595725ac58dd977beef14b97461a7c1045b9a1c963065002c5473194952^
 ENABLEPATH=1^
```

```
ALLOWDENYKEY="AllowKey=system.run[type C:\Windows\System32\drivers\etc\hosts];DenyKey=system.run[*]"
```

Kolejny przykład instaluje nowszą wersję agent Zabbix i używa **pliku konfiguracyjnego szablonu** (`CONF="C:\agent-template.conf"`). Podczas instalacji plik ten stanie się plikiem konfiguracyjnym agent. Aby dziedziczyć parametry ze starego pliku konfiguracyjnego, użyj symboli zastępczych parametrów (np. `[AllowDenyKey]`).

```
msiexec.exe /l*v "C:\package.log" /i "C:\zabbix_agent-8.0.1-windows-amd64-openssl.msi" /qn+ NONMSICONFNAME

#### przykład agent-template.conf:
LogFile=[LogFile]
[AllowDenyKey]
Server=192.0.2.8
Hostname=DESKTOP-X9F4A2B
[Include]
[TLSConnect]
[TLSAccept]
[TLSPSKIdentity]
[TLSPSKFile]
```

Alternatywnie możesz użyć **niestandardowego pliku konfiguracyjnego** (`NONMSICONFNAME="C:\agent-custom.conf"`). Podczas instalacji wszystkie prawidłowe parametry konfiguracyjne agent obecne w tym pliku (ograniczone do tych wymienionych w powyższej tabeli) zostaną zapisane w nowo utworzonym pliku konfiguracyjnym agent. Aby zachować istniejącą konfigurację agent, zdefiniuj parametry, które mają zostać zachowane.

```
msiexec.exe /l*v "C:\package.log" /i "C:\zabbix_agent-8.0.1-windows-amd64-openssl.msi" /qn+ NONMSICONFNAME

#### przykład agent-custom.conf:
Server=192.0.2.8
Hostname=DESKTOP-X9F4A2B
```

Ładowalne pluginy Zabbix agent 2

Ładowalne pluginy Zabbix agent 2 można zainstalować w systemie Windows przy użyciu 64-bitowych pakietów instalatora MSI, dostępnych do pobrania.

Minimalne wymagania systemowe dla instalacji MSI to Windows 10 (64-bit) lub Windows Server 2016.

> **Attention:**
> Przed zainstalowaniem pluginu sprawdź jego plik README. Może on zawierać szczegółowe wymagania oraz instrukcje instalacji.

Podobnie jak w przypadku Zabbix agent/agent2, ładowalne pluginy można instalować za pomocą kreatora instalacji lub z wiersza poleceń.

Instalacja za pomocą kreatora konfiguracji

1. Kliknij dwukrotnie pobrany plik MSI, aby rozpocząć instalację.
2. Zaakceptuj umowę licencyjną użytkownika końcowego.
3. Wybierz ładowalne wtyczki Zabbix agent 2 do zainstalowania.

> **Attention:**
> Zaleca się użycie domyślnej lokalizacji instalacji udostępnionej przez instalator. Użycie niestandardowej lokalizacji bez wymaganych uprawnień może zagrozić bezpieczeństwu instalacji.

4. Kliknij *Install*, aby rozpocząć instalację.

Wszystkie wybrane ładowalne wtyczki Zabbix agent 2 zostaną zainstalowane w określonej lokalizacji (domyślnie: `C:\Program Files\Zabbix Agent 2`), a ich pliki konfiguracyjne zostaną zainstalowane w podfolderze `zabbix_agent2.d`.

5. Kliknij przycisk *Finish*, aby zamknąć kreatora konfiguracji.

Instalacja z wiersza poleceń

Ładowalne pluginy Zabbix agent 2 można zainstalować z wiersza poleceń, uruchamiając instalator MSI za pomocą msiexec. Na przykład:

```
msiexec.exe /l*v "C:\package.log" /i "C:\zabbix_agent2_plugins-8.0.0-windows-amd64.msi" /qn+
```

Pakiety instalatora MSI dla ładowalnych pluginów Zabbix agent 2 obsługują następujące parametry.

Parameter	Description
ADDDEFAULT	Lista komponentów rozdzielonych przecinkami, które mają zostać zainstalowane w swojej domyślnej konfiguracji. Więcej informacji można znaleźć w właściwości ADDDEFAULT. Możliwe wartości: `ALL`, `CephPlugin`, `EmberplusPlugin`, `MongodbPlugin`, `MssqlPlugin`, `NvidiagpuPlugin`, `PostgresqlPlugin` Przykład: `ADDDEFAULT=MongodbPlugin,PostgresqlPlugin`
ADDLOCAL	Lista komponentów rozdzielonych przecinkami, które mają zostać zainstalowane lokalnie. Więcej informacji można znaleźć w właściwości ADDLOCAL. Możliwe wartości: `ALL`, `CephPlugin`, `EmberplusPlugin`, `MongodbPlugin`, `MssqlPlugin`, `NvidiagpuPlugin`, `PostgresqlPlugin` Przykład: `ADDLOCAL=MongodbPlugin,MssqlPlugin`
INSTALLFOLDER	Pełna ścieżka do folderu, w którym zostaną zainstalowane komponenty Zabbix, a ich pliki konfiguracyjne zostaną zainstalowane w podfolderze `zabbix_agent2.d`. Przykład: `INSTALLFOLDER="C:\Program Files\Zabbix Agent 2"`

Budowanie Zabbix agent 2 w systemie Windows

Przegląd

Ta strona pokazuje, jak zbudować Zabbix agent 2 ze źródeł w systemie Windows 10 (64-bitowym lub 32-bitowym).

Zarówno wersje 32-bitowe, jak i 64-bitowe można zbudować na platformie 64-bitowej, ale na platformie 32-bitowej można zbudować tylko wersję 32-bitową.

Budowanie Zabbix agent 2 wymaga:

- narzędzi build MinGW
- języka programowania Go
- OpenSSL (dla funkcji szyfrowania w Zabbix)
- PCRE2 (Perl Compatible Regular Expressions; dla funkcji dopasowywania wzorców wyrażeń regularnych w Zabbix)

Możesz zbudować Zabbix agent 2, korzystając z jednej z następujących metod:

- Użycie vcpkg — zautomatyzowane podejście, które upraszcza zarządzanie zależnościami przy użyciu menedżera pakietów C++.
- Budowanie ręczne — ręczne podejście wymagające zainstalowania wszystkich zależności przed kompilacją agent.

Attention:
Przed rozpoczęciem procesu budowania pamiętaj o następujących kwestiach:

- Do wykonywania poleceń używaj Wiersza polecenia uruchomionego przez użytkownika z wystarczającymi uprawnieniami do zapisu w chronionych folderach. Jednak podczas instalacji OpenSSL i PCRE2 używaj terminala MSYS2.
- Zaleca się utworzenie katalogu roboczego `C:\Zabbix` dla wszystkich plików źródłowych i folderów build. Jednak skompilowane komponenty powinny być instalowane w `C:\Zabbix\x64` (lub `C:\Zabbix\x86` dla buildów 32-bitowych).

Budowanie Zabbix agent 2 przy użyciu vcpkg

Ta sekcja zawiera instrukcje dotyczące budowania Zabbix agent przy użyciu vcpkg, menedżera pakietów, który upraszcza zarządzanie zależnościami i integrację z projektami C++.

1. Pobierz i zainstaluj Build Tools for Visual Studio 2022. Podczas instalacji upewnij się, że wybrano obciążenie *Desktop development with C++*, które zawiera menedżer pakietów vcpkg.

2. Pobierz i zainstaluj Go (dostępny jako instalator MSI). Podczas instalacji upewnij się, że jako folder instalacyjny wskazano `C:\Zabbix\Go`.

3. Pobierz dystrybucję MinGW, która używa biblioteki uruchomieniowej Microsoft Visual C; na przykład:

- Dla kompilacji 64-bitowych: `x86_64-15.1.0-release-win32-seh-msvcrt-rt_v12-rev0.7z`
- Dla kompilacji 32-bitowych: `i686-15.1.0-release-win32-dwarf-msvcrt-rt_v12-rev0.7z`

Następnie rozpakuj ją do `C:\Zabbix\mingw64` (lub `C:\Zabbix\mingw32` dla kompilacji 32-bitowych).

4. Zainicjuj vcpkg i zainstaluj zależności wymagane do budowania Zabbix agent 2 (pamiętaj, że może to zająć trochę czasu):

```
cd C:\Zabbix

set PATH=%PATH%;"C:\Program Files (x86)\Microsoft Visual Studio\2022\BuildTools\VC\vcpkg"
vcpkg new --application
vcpkg add port pcre2
vcpkg add port libiconv
vcpkg add port openssl

#### For 64-bit builds:
set PATH=C:\Zabbix\mingw64\bin;%PATH%
vcpkg install --triplet x64-mingw-static --x-install-root=x64

#### For 32-bit builds:
set PATH=C:\Zabbix\mingw32\bin;%PATH%
vcpkg install --triplet x86-mingw-static --x-install-root=x86
```

5. Pobierz archiwum kodu źródłowego Zabbix i rozpakuj je do `C:\Zabbix\zabbix-8.0.0`.

6. Przejdź do katalogu budowania Zabbix (`C:\Zabbix\zabbix-8.0.0\build\mingw`) i utwórz następujący skrypt `build.bat`:

- Dla kompilacji 64-bitowych:

```
:: Add MinGW and Go to the system `PATH` variable for the current session:
set PATH=C:\Zabbix\mingw64\bin;%PATH%
set PATH=C:\Zabbix\Go\bin;%PATH%

:: Set vcpkg installation path:
set vcpkg="C:\Zabbix\x64\x64-mingw-static"

:: Set linker flags for Crypt32 library:
SET CGO_LDFLAGS="-lCrypt32"

:: Run the build process:
mingw32-make GOFLAGS="-buildvcs=false" ARCH=AMD64 ^
    PCRE2="%vcpkg%" ^
    OPENSSL="%vcpkg%" ^
    all
```

- Dla kompilacji 32-bitowych:

```
:: Add MinGW and Go to the system `PATH` variable for the current session:
set PATH=C:\Zabbix\mingw32\bin;%PATH%
set PATH=C:\Zabbix\Go\bin;%PATH%

:: Set vcpkg installation path:
set vcpkg="C:\Zabbix\x86\x86-mingw-static"

:: Set linker flags for Crypt32 library:
SET CGO_LDFLAGS="-lCrypt32"

:: Run the build process:
mingw32-make GOFLAGS="-buildvcs=false" ARCH=x86 ^
    PCRE2="%vcpkg%" ^
    OPENSSL="%vcpkg%" ^
    all
```

7. Skompiluj Zabbix agent 2, uruchamiając skrypt:

```
build.bat
```

Po kompilacji plik binarny Zabbix agent 2 będzie znajdować się w `C:\Zabbix\zabbix-8.0.0\bin\win64` (dla kompilacji 64-bitowych) lub `C:\Zabbix\zabbix-8.0.0\bin\win32` (dla kompilacji 32-bitowych). Pliki konfiguracyjne Zabbix agent 2 znajdują się w `C:\Zabbix\zabbix-8.0.0\src\go\conf`.

Aby uruchomić agent, skopiuj `zabbix_agent2.exe` oraz jego pliki konfiguracyjne do dedykowanego folderu (np. `C:\Zabbix\agent2`), a następnie uruchom agent:

```
mkdir C:\Zabbix\agent2

#### For 64-bit builds:
copy C:\Zabbix\zabbix-8.0.0\bin\win64\zabbix_agent2.exe C:\Zabbix\agent2\

#### For 32-bit builds:
copy C:\Zabbix\zabbix-8.0.0\bin\win32\zabbix_agent2.exe C:\Zabbix\agent2\

copy C:\Zabbix\zabbix-8.0.0\src\go\conf\zabbix_agent2.win.conf C:\Zabbix\agent2\
xcopy /E /I C:\Zabbix\zabbix-8.0.0\src\go\conf\zabbix_agent2.d C:\Zabbix\agent2\zabbix_agent2.d\

C:\Zabbix\agent2\zabbix_agent2.exe -c C:\Zabbix\agent2\zabbix_agent2.win.conf
```

W razie potrzeby kontynuuj, kompilując wtyczki ładowalne dla Zabbix agent 2.

Kompilowanie ładowalnych wtyczek Zabbix agent 2

1. Pobierz kod źródłowy wtyczki Zabbix zgodny z wersją Zabbix agent 2 (np. `zabbix-agent2-plugin-postgresql-8.0.0.tar.gz`) i rozpakuj go do `C:\Zabbix`.

> **Attention:**
> Przed zainstalowaniem wtyczki sprawdź jej plik README. Może on zawierać szczegółowe wymagania i instrukcje instalacji.

2. Przejdź do katalogu rozpakowanej wtyczki i skompiluj wtyczkę:

```
cd C:\Zabbix\zabbix-agent2-plugin-ember-plus-8.0.0

#### Dla kompilacji 64-bitowych:
mingw32-make ARCH=AMD64

#### Dla kompilacji 32-bitowych:
mingw32-make ARCH=x86
```

Po kompilacji plik binarny wtyczki Zabbix agent 2 oraz jego plik konfiguracyjny będą znajdować się w tym samym katalogu wtyczki.

Plik wykonywalny wtyczki można umieścić w dowolnym miejscu, o ile może zostać załadowany przez Zabbix agent 2. Ścieżkę do pliku binarnego wtyczki należy określić w pliku konfiguracyjnym wtyczki, np. w pliku postgresql.conf dla wtyczki PostgreSQL:

```
Plugins.PostgreSQL.System.Path=/path/to/executable/zabbix-agent2-plugin-postgresql
```

Ścieżkę do pliku konfiguracyjnego wtyczki należy określić w parametrze Include pliku konfiguracyjnego Zabbix agent 2:

```
Include=/path/to/plugin/configuration/file/postgresql.conf
```

Przejdź do sekcji konfiguracja, aby uzyskać więcej informacji o konfigurowaniu wtyczek.

Ręczne budowanie Zabbix agent 2

> **Attention:**
> Ta metoda budowania Zabbix agent 2 jest odpowiednia dla użytkowników, którzy wymagają pełnej kontroli nad środowiskiem budowania lub działają w ograniczonym środowisku, w którym użycie vcpkg nie jest możliwe.

Ta sekcja zawiera instrukcje dotyczące ręcznego budowania Zabbix agent 2, co obejmuje instalację wymaganych narzędzi do budowania i zależności, a następnie kompilację agenta.

Konfigurowanie narzędzi do budowania

1. Pobierz i zainstaluj MSYS2 (dostępny jako instalator MSI). Podczas instalacji upewnij się, że jako folder instalacyjny podano `C:\Zabbix\msys64`.

2. Pobierz i zainstaluj Go (dostępny jako instalator MSI; zobacz obecnie obsługiwane wersje Go). Podczas instalacji upewnij się, że jako folder instalacyjny podano `C:\Zabbix\Go`.

3. Pobierz dystrybucję MinGW, która korzysta z biblioteki uruchomieniowej Microsoft Visual C; na przykład:

- Dla kompilacji 64-bitowych: `x86_64-15.1.0-release-win32-seh-msvcrt-rt_v12-rev0.7z`
- Dla kompilacji 32-bitowych: `i686-15.1.0-release-win32-dwarf-msvcrt-rt_v12-rev0.7z`

Następnie rozpakuj ją do `C:\Zabbix\mingw64` (lub `C:\Zabbix\mingw32` dla kompilacji 32-bitowych).

Instalacja OpenSSL

> **Note:**
> Aby skompilować agent Zabbix bez obsługi TLS, przejdź do sekcji Installing PCRE2.

1. Otwórz terminal MSYS2 MSYS z uprawnieniami administratora i uruchom następujące polecenia:

```
pacman -S perl-Locale-Maketext-Simple
pacman -S nasm
pacman -S make
pacman -S cmake
```

2. Pobierz archiwum źródłowe OpenSSL i rozpakuj je do `C:\Zabbix\openssl-3.5.0`.

3. Przejdź do rozpakowanego katalogu OpenSSL i utwórz następujący skrypt `build.sh`:

- Dla kompilacji 64-bitowych:

```
####!/usr/bin/env bash

export PATH="/c/Zabbix/mingw64/bin:$PATH"
export d="/c/Zabbix/x64/OpenSSL-Win64-350-static"

perl Configure mingw64 no-shared no-capieng no-winstore no-srp no-gost no-dgram no-dtls1-method no-dtls1_2

make
make install
```

- Dla kompilacji 32-bitowych:

```
####!/usr/bin/env bash

export PATH="/c/Zabbix/mingw32/bin:$PATH"
export d="/c/Zabbix/x86/OpenSSL-Win64-350-static"

perl Configure mingw no-shared no-capieng no-winstore no-srp no-gost no-dgram no-dtls1-method no-dtls1_2-m

make
make install
```

> **Attention:**
> Upewnij się, że użytkownicy niebędący administratorami nie mają uprawnień do zapisu w katalogu `C:\Zabbix\x64\OpenSSL-Win64-350-static`. W przeciwnym razie agent będzie ładować ustawienia SSL ze ścieżki, którą mogą modyfikować użytkownicy bez uprawnień, co stwarza potencjalną lukę bezpieczeństwa.

- Opcja `no-shared` powoduje, że statyczne biblioteki OpenSSL libcrypto.lib i libssl.lib są samowystarczalne, dzięki czemu pliki binarne Zabbix zawierają OpenSSL bez potrzeby używania zewnętrznych bibliotek DLL. Oznacza to, że pliki binarne Zabbix można kopiować na inne komputery z systemem Windows bez bibliotek OpenSSL; jednak po wydaniu nowej wersji OpenSSL zawierającej poprawki błędów agent Zabbix będzie wymagał ponownej kompilacji.
- Bez opcji `no-shared` Zabbix korzysta z bibliotek DLL OpenSSL w czasie działania. Oznacza to, że aktualizacje OpenSSL mogą nie wymagać ponownej kompilacji agent Zabbix; jednak podczas kopiowania go na inne komputery należy również skopiować biblioteki DLL OpenSSL.

Aby uzyskać więcej informacji o innych opcjach konfiguracji OpenSSL, zobacz dokumentację OpenSSL.

4. Skonfiguruj i zainstaluj OpenSSL, wykonując skrypt (pamiętaj, że może to zająć trochę czasu):

```
cd /c/Zabbix/openssl-3.5.0
./build.sh
```

Instalacja PCRE2

1. Pobierz archiwum źródłowe PCRE2 i rozpakuj je do `C:\Zabbix\pcre2-10.45`.

2. Otwórz terminal MSYS2 MSYS z uprawnieniami administratora. Następnie utwórz katalog `build` w rozpakowanym katalogu PCRE2 i przejdź do niego:

```
mkdir /c/Zabbix/pcre2-10.45/build
cd /c/Zabbix/pcre2-10.45/build
```

3. Skonfiguruj PCRE2:

```
#### Dla kompilacji 64-bitowych:
export PATH="/c/Zabbix/mingw64/bin:$PATH"
cmake -DCMAKE_C_COMPILER=gcc -DCMAKE_C_FLAGS="-O2 -g" -DCMAKE_INSTALL_PREFIX="/c/Zabbix/x64/PCRE2" ..

#### Dla kompilacji 32-bitowych:
export PATH="/c/Zabbix/mingw32/bin:$PATH"
cmake -DCMAKE_C_COMPILER=gcc -DCMAKE_C_FLAGS="-m32 -O2 -g" -DCMAKE_EXE_LINKER_FLAGS="-Wl,-mi386pe" -DCMAKE
```

Note:
Jeśli wystąpią jakiekolwiek błędy, zaleca się usunięcie pamięci podręcznej CMake przed ponowną próbą przeprowadzenia procesu budowania CMake. Pamięć podręczna (`CMakeCachecache.txt`) może znajdować się w katalogu build rozpakowanego katalogu PCRE2.

4. Zainstaluj PCRE2:

```
make install
```

Kompilacja Zabbix agent 2

1. Pobierz archiwum kodu źródłowego Zabbix i rozpakuj je do `C:\Zabbix\zabbix-8.0.0`.

Jeśli musisz wygenerować archiwum kodu źródłowego z surowego repozytorium źródeł (np. aby zastosować własne poprawki lub zbudować z najnowszego kodu źródłowego), uruchom następujące polecenia na komputerze z systemem **Linux** z zainstalowanym Go (wymaganym do konfiguracji Zabbix agent 2):

```
git clone https://git.zabbix.com/scm/zbx/zabbix.git
cd zabbix
./bootstrap.sh
./configure --enable-agent2 --enable-ipv6 --prefix=`pwd`
make dist
```

Spowoduje to utworzenie archiwum kodu źródłowego, które następnie można skopiować na komputer z systemem Windows.

2. Otwórz Wiersz polecenia z uprawnieniami administratora. Następnie przejdź do katalogu kompilacji Zabbix i skompiluj agent Zabbix; pamiętaj, aby poprawnie określić katalogi, w których zainstalowano OpenSSL i PCRE2:

- Dla kompilacji 64-bitowych:

```
cd C:\Zabbix\zabbix-8.0.0\build\mingw
set PATH=C:\Zabbix\mingw64\bin;%PATH%
mklink /D C:\Zabbix\x64\OpenSSL-Win64-350-static\lib C:\Zabbix\x64\OpenSSL-Win64-350-static\lib64

#### With TLS support:
mingw32-make ARCH=AMD64 PCRE2="C:\Zabbix\x64\PCRE2" OPENSSL="C:\Zabbix\x64\OpenSSL-Win64-350-static"

#### Without TLS support:
mingw32-make ARCH=AMD64 PCRE2="C:\Zabbix\x64\PCRE2"
```

- Dla kompilacji 32-bitowych:

```
cd C:\Zabbix\zabbix-8.0.0\build\mingw
set PATH=C:\Zabbix\mingw32\bin;%PATH%

#### With TLS support:
mingw32-make ARCH=x86 PCRE2="C:\Zabbix\x86\PCRE2" OPENSSL="C:\Zabbix\x86\OpenSSL-Win64-350-static"

#### Without TLS support:
mingw32-make ARCH=x86 PCRE2="C:\Zabbix\x86\PCRE2"
```

Po zakończeniu kompilacji plik binarny Zabbix agent 2 będzie znajdować się w `C:\Zabbix\zabbix-8.0.0\bin\win64` (lub `C:\Zabbix\zabbix-8.0.0\bin\win32` dla kompilacji 32-bitowych). Pliki konfiguracyjne Zabbix agent 2 znajdują się w `C:\Zabbix\zabbix-8.0.0\src\go\conf`.

Aby uruchomić agent, skopiuj plik binarny `zabbix_agent2.exe` oraz jego pliki konfiguracyjne do dedykowanego folderu (np. `C:\Zabbix\agent2`), a następnie uruchom agent:

```
mkdir C:\Zabbix\agent2
copy C:\Zabbix\zabbix-8.0.0\bin\win64\zabbix_agent2.exe C:\Zabbix\agent2\
copy C:\Zabbix\zabbix-8.0.0\src\go\conf\zabbix_agent2.win.conf C:\Zabbix\agent2\
xcopy /E /I C:\Zabbix\zabbix-8.0.0\src\go\conf\zabbix_agent2.d C:\Zabbix\agent2\zabbix_agent2.d\

C:\Zabbix\agent2\zabbix_agent2.exe -c C:\Zabbix\agent2\zabbix_agent2.win.conf
```

W razie potrzeby przejdź dalej do sekcji kompilacja ładowalnych wtyczek Zabbix agent 2.

Building Zabbix agent on Windows

Przegląd

Ta strona pokazuje, jak zbudować Zabbix agent ze źródeł w systemie Windows 10 (64-bit).

Te instrukcje dotyczą wersji Windows, które obsługują Visual Studio 2022.

Budowanie Zabbix agent wymaga:

- kompilatora C (dołączonego do Build Tools for Visual Studio 2022)
- OpenSSL (dla funkcji szyfrowania w Zabbix)
- PCRE2 (Perl Compatible Regular Expressions; dla funkcji dopasowywania wzorców wyrażeń regularnych w Zabbix)

Możesz zbudować Zabbix agent, korzystając z jednej z następujących metod:

- Korzystanie z vcpkg — zautomatyzowane podejście, które upraszcza zarządzanie zależnościami przy użyciu menedżera pakietów C++.
- Budowanie ręczne — ręczne podejście, które wymaga zainstalowania wszystkich zależności przed skompilowaniem agent.
- W zależności od potrzeb monitorowania mogą być wymagane dodatkowe biblioteki. Więcej informacji można znaleźć w sekcji Wymagania.

Attention:
Przed rozpoczęciem procesu budowania pamiętaj o następujących kwestiach:

- Do wykonywania poleceń używaj x64 Native Tools Command Prompt (dołączonego do Build Tools for Visual Studio 2022), uruchomionego przez użytkownika z wystarczającymi uprawnieniami do zapisu w chronionych folderach.
- Zaleca się utworzenie katalogu roboczego `C:\Zabbix` dla wszystkich plików źródłowych i folderów budowania. Jednak skompilowane komponenty powinny być instalowane w `C:\Program Files\Zabbix\x64`.

Budowanie Zabbix agent przy użyciu vcpkg

Ta sekcja zawiera instrukcje dotyczące budowania Zabbix agent przy użyciu vcpkg, menedżera pakietów, który upraszcza zarządzanie zależnościami i integrację z projektami C++.

1. Pobierz i zainstaluj Build Tools for Visual Studio 2022. Podczas instalacji upewnij się, że wybrano obciążenie *Desktop development with C++*, które zawiera narzędzia wymagane do budowania agent przy użyciu vcpkg:

- kompilator C (Microsoft Visual C++)
- narzędzie wiersza poleceń NMake
- menedżer pakietów vcpkg
- x64 Native Tools Command Prompt

2. Zainicjuj vcpkg i zainstaluj zależności wymagane do budowania Zabbix agent (pamiętaj, że może to zająć trochę czasu):

```
cd C:\Zabbix
vcpkg new --application
vcpkg add port pcre2
vcpkg add port openssl
vcpkg install --triplet x64-windows-static --x-install-root="C:\Program Files\Zabbix\x64"
```

3. Pobierz archiwum kodu źródłowego Zabbix i rozpakuj je do `C:\Zabbix\zabbix-8.0.0`.

4. Przejdź do katalogu budowania Zabbix (`C:\Zabbix\zabbix-8.0.0\build\win32\project`) i utwórz następujący skrypt `build.bat`; upewnij się, że poprawnie określono katalogi, w których zainstalowano OpenSSL i PCRE2:

```
:: Set vcpkg installation path:
set vcpkg=C:\Program Files\Zabbix\x64\x64-windows-static
```

```
:: Run the build process:
nmake -f Makefile CPU=AMD64 ^
    PCRE2INCDIR="%vcpkg%\include" ^
    PCRE2LIBDIR="%vcpkg%\lib" ^
    TLS=openssl ^
    TLSINCDIR="%vcpkg%\include" ^
    TLSLIBDIR="%vcpkg%\lib" ^
    LIBS="$(LIBS) Crypt32.lib" ^
    all
```

5. Skompiluj Zabbix agent, uruchamiając skrypt:

```
build.bat
```

Po kompilacji pliki binarne komponentów Zabbix będą znajdować się w `C:\Zabbix\zabbix-8.0.0\bin\win64`. Plik konfiguracyjny Zabbix agent znajduje się w `C:\Zabbix\zabbix-8.0.0\conf`.

Aby uruchomić agent, skopiuj `zabbix_agent.exe` oraz jego plik konfiguracyjny do dedykowanego folderu (na przykład `C:\Zabbix\agent`), a następnie uruchom agent:

```
mkdir C:\Zabbix\agent
copy C:\Zabbix\zabbix-8.0.0\bin\win64\zabbix_agent.exe C:\Zabbix\agent\
copy C:\Zabbix\zabbix-8.0.0\conf\zabbix_agent.win.conf C:\Zabbix\agent\

C:\Zabbix\agent\zabbix_agent.exe -c C:\Zabbix\agent\zabbix_agent.win.conf
```

Ręczne budowanie Zabbix agent

Attention:
Ta metoda budowania Zabbix agent jest odpowiednia dla użytkowników, którzy wymagają pełnej kontroli nad środowiskiem budowania lub znajdują się w środowisku z ograniczeniami, gdzie użycie vcpkg nie jest możliwe.

Ta sekcja zawiera instrukcje dotyczące ręcznego budowania Zabbix agent, co obejmuje instalację wymaganych narzędzi do budowania i zależności (Perl, OpenSSL, PCRE2), a następnie kompilację agent.

Instalacja narzędzi kompilacyjnych

1. Pobierz i zainstaluj Build Tools for Visual Studio 2022. Podczas instalacji upewnij się, że wybrano obciążenie *Desktop development with C++*, które zawiera narzędzia wymagane do ręcznego zbudowania agenta:

- kompilator C (Microsoft Visual C++)
- narzędzie wiersza poleceń NMake
- x64 Native Tools Command Prompt

Instalacja OpenSSL

Note:
Aby skompilować Zabbix agent bez obsługi TLS, przejdź do sekcji Installing PCRE2.

1. Pobierz i zainstaluj Strawberry Perl (dostępny jako instalator MSI). Podczas instalacji upewnij się, że jako folder instalacyjny wskazano `C:\Zabbix\Strawberry`.

2. Zainstaluj moduł Perl `Text::Template`:

```
cpanm Text::Template
```

3. Sprawdź, czy Netwide Assembler (NASM; wymagany do kompilacji OpenSSL) został skompilowany podczas instalacji Strawberry Perl:

```
nasm -v
#### NASM version 2.16.01 compiled on May  3 2024
```

Jeśli NASM nie został skompilowany, zainstaluj go ręcznie. Więcej informacji znajdziesz w dokumentacji NASM.

4. Pobierz archiwum źródłowe OpenSSL i rozpakuj je do `C:\Zabbix\openssl-3.5.0`.

5. Przejdź do rozpakowanego katalogu i skonfiguruj OpenSSL, na przykład:

```
cd C:\Zabbix\openssl-3.5.0
perl Configure VC-WIN64A no-shared no-capieng no-winstore no-srp no-gost no-dgram no-dtls1-method no-dtls1
```

Attention:
Jeśli podczas kompilacji Zabbix agent w systemie Windows wybierzesz niestandardowy katalog dla OpenSSL (na przykład `C:\zabbix` lub `C:\openssl-64bit`), upewnij się, że odebrano uprawnienia do zapisu w tym katalogu użytkownikom niebędącym administratorami. W przeciwnym razie agent będzie ładować ustawienia SSL ze ścieżki, którą mogą modyfikować użytkownicy bez uprawnień, co stwarza potencjalną lukę bezpieczeństwa.

- Opcja `no-shared` powoduje, że biblioteki statyczne OpenSSL libcrypto.lib i libssl.lib są samowystarczalne, dzięki czemu pliki binarne Zabbix zawierają OpenSSL bez potrzeby używania zewnętrznych bibliotek DLL. Oznacza to, że pliki binarne Zabbix można kopiować na inne komputery z systemem Windows bez bibliotek OpenSSL; jednak po wydaniu nowej wersji OpenSSL zawierającej poprawki błędów konieczna będzie ponowna kompilacja Zabbix agent.
- Bez opcji `no-shared` Zabbix korzysta z bibliotek DLL OpenSSL w czasie działania. Oznacza to, że aktualizacje OpenSSL mogą nie wymagać ponownej kompilacji Zabbix agent; jednak podczas kopiowania go na inne komputery należy również skopiować biblioteki DLL OpenSSL.

Więcej informacji o innych opcjach konfiguracji OpenSSL znajdziesz w dokumentacji OpenSSL.

6. Skompiluj OpenSSL i uruchom testy (pamiętaj, że może to zająć trochę czasu):

Attention:
Uruchamiaj testy bez uprawnień administracyjnych; w przeciwnym razie może to prowadzić do nieoczekiwanych wyników lub zagrożeń bezpieczeństwa. Jeśli niektóre testy zakończą się niepowodzeniem, zapoznaj się z dokumentacją OpenSSL, aby rozwiązać problem.

```
nmake
nmake test
...
All tests successful.
Files=325, Tests=3101, 822 wallclock secs ( 4.81 usr +  0.81 sys =  5.62 CPU)
Result: PASS
```

7. Zainstaluj OpenSSL:

```
nmake install
```

Aby zainstalować tylko komponenty programowe (biblioteki, pliki nagłówkowe, ale bez dokumentacji), możesz użyć `nmake install_sw`.

Instalacja PCRE2

1. Pobierz i zainstaluj CMake (dostępny jako instalator MSI). Podczas instalacji upewnij się, że jako folder instalacyjny wskazano `C:\Zabbix\CMake`, oraz wybierz opcję *Add CMake to the PATH environment variable*.

2. Pobierz archiwum kodu źródłowego PCRE2 i rozpakuj je do `C:\Zabbix\pcre2-10.45`.

3. Utwórz katalog `build` w rozpakowanym katalogu PCRE2 i przejdź do niego:

```
mkdir C:\Zabbix\pcre2-10.45\build
cd C:\Zabbix\pcre2-10.45\build
```

4. Skonfiguruj PCRE2:

```
cmake -G "NMake Makefiles" -DPCRE_SUPPORT_UNICODE_PROPERTIES=ON -DCMAKE_BUILD_TYPE=Release -DCMAKE_INSTALL
```

Note:
Jeśli wystąpią jakiekolwiek błędy, zaleca się usunięcie pamięci podręcznej CMake przed ponowną próbą przeprowadzenia procesu budowania CMake. Pamięć podręczna (`CMakeCachecache.txt`) znajduje się w katalogu build rozpakowanego katalogu PCRE2.

5. Zbuduj PCRE2 za pomocą NMake:

```
nmake
```

6. Zainstaluj PCRE2:

```
cmake --install .
```

Kompilowanie Zabbix agent

1. Pobierz archiwum kodu źródłowego Zabbix i rozpakuj je do `C:\Zabbix\zabbix-8.0.0`.

Jeśli chcesz wygenerować archiwum kodu źródłowego z surowego repozytorium źródeł (np. aby zastosować własne poprawki lub zbudować z najnowszego kodu źródłowego), uruchom następujące polecenia na komputerze z systemem **Linux**:

```
git clone https://git.zabbix.com/scm/zbx/zabbix.git
cd zabbix
./bootstrap.sh
./configure --enable-agent --enable-ipv6 --prefix=`pwd`
make dist
```

Spowoduje to utworzenie archiwum kodu źródłowego, które następnie można skopiować na komputer z systemem Windows.

2. Przejdź do katalogu kompilacji Zabbix i skompiluj Zabbix agent (lub inne komponenty); upewnij się, że poprawnie określono katalogi, w których zainstalowano OpenSSL i PCRE2:

```
cd C:\Zabbix\zabbix-8.0.0\build\win32\project

#### Z obsługą TLS:
nmake /K -f Makefile_agent PCRE2INCDIR="C:\Program Files\Zabbix\x64\PCRE2\include" PCRE2LIBDIR="C:\Program
nmake /K -f Makefile_get PCRE2INCDIR="C:\Program Files\Zabbix\x64\PCRE2\include" PCRE2LIBDIR="C:\Program F
nmake /K -f Makefile_sender PCRE2INCDIR="C:\Program Files\Zabbix\x64\PCRE2\include" PCRE2LIBDIR="C:\Progra

#### Bez obsługi TLS:
nmake /K -f Makefile_agent PCRE2INCDIR="C:\Program Files\Zabbix\x64\PCRE2\include" PCRE2LIBDIR="C:\Program
nmake /K -f Makefile_get PCRE2INCDIR="C:\Program Files\Zabbix\x64\PCRE2\include" PCRE2LIBDIR="C:\Program F
nmake /K -f Makefile_sender PCRE2INCDIR="C:\Program Files\Zabbix\x64\PCRE2\include" PCRE2LIBDIR="C:\Progra
```

Po kompilacji pliki binarne komponentów Zabbix będą znajdować się w `C:\Zabbix\zabbix-8.0.0\bin\win64`. Plik konfiguracyjny Zabbix agent znajduje się w `C:\Zabbix\zabbix-8.0.0\conf`.

Aby uruchomić agent, skopiuj `zabbix_agent.exe` oraz jego plik konfiguracyjny do dedykowanego folderu (np. `C:\Zabbix\agent`), a następnie uruchom agent:

```
mkdir C:\Zabbix\agent
copy C:\Zabbix\zabbix-8.0.0\bin\win64\zabbix_agentd.exe C:\Zabbix\agent\
copy C:\Zabbix\zabbix-8.0.0\conf\zabbix_agentd.win.conf C:\Zabbix\agent\

C:\Zabbix\agent\zabbix_agentd.exe -c C:\Zabbix\agent\zabbix_agentd.win.conf -f
```

Instalacja agent na macOS z pakietu PKG

Przegląd

Agent Zabbix można zainstalować w systemie macOS za pomocą pakietów instalatora PKG, dostępnych do pobrania.

Pakiety agenta Zabbix są dostępne z szyfrowaniem lub bez niego.

Instalacja agent

Agent można zainstalować za pomocą graficznego interfejsu użytkownika lub z wiersza poleceń, na przykład:

```
sudo installer -pkg zabbix_agent-8.0.0-macos-arm64-openssl.pkg -target /
```

Upewnij się, że w poleceniu używasz poprawnej wersji pakietu Zabbix. Musi ona odpowiadać nazwie pobranego pakietu.

Uruchamianie agent

Agent uruchomi się automatycznie po instalacji lub restarcie.

W razie potrzeby możesz edytować plik konfiguracyjny `/usr/local/etc/zabbix/zabbix_agentd.conf`.

Aby uruchomić agent ręcznie, możesz wykonać:

```
sudo launchctl start com.zabbix.zabbix_agentd
```

Aby zatrzymać agent ręcznie:

```
sudo launchctl stop com.zabbix.zabbix_agentd
```

Podczas aktualizacji istniejący plik konfiguracyjny nie jest nadpisywany. Zamiast tego tworzony jest nowy plik `zabbix_agentd.conf.NEW`, który służy do przeglądu i aktualizacji istniejącego pliku konfiguracyjnego, jeśli to konieczne. Pamiętaj, aby po ręcznych zmianach w pliku konfiguracyjnym ponownie uruchomić agent.

Rozwiązywanie problemów i usuwanie agent

W tej sekcji wymieniono kilka przydatnych poleceń, których można użyć do rozwiązywania problemów i usuwania instalacji Zabbix agent.

Sprawdź, czy Zabbix agent jest uruchomiony:

```
ps aux | grep zabbix_agentd
```

Sprawdź, czy Zabbix agent został zainstalowany z pakietów:

```
pkgutil --pkgs | grep zabbix
com.zabbix.pkg.ZabbixAgent
```

Sprawdź pliki, które zostały zainstalowane z pakietu instalacyjnego (zwróć uwagę, że początkowy znak / nie jest wyświetlany w tym widoku):

```
pkgutil --only-files --files com.zabbix.pkg.ZabbixAgent
Library/LaunchDaemons/com.zabbix.zabbix_agentd.plist
usr/local/bin/zabbix_get
usr/local/bin/zabbix_sender
usr/local/etc/zabbix/zabbix_agentd/userparameter_examples.conf.NEW
usr/local/etc/zabbix/zabbix_agentd/userparameter_mysql.conf.NEW
usr/local/etc/zabbix/zabbix_agentd.conf.NEW
usr/local/sbin/zabbix_agentd
```

Zatrzymaj Zabbix agent, jeśli został uruchomiony za pomocą `launchctl`:

```
sudo launchctl unload /Library/LaunchDaemons/com.zabbix.zabbix_agentd.plist
```

Usuń pliki (w tym konfigurację i logi), które zostały zainstalowane przez pakiet instalacyjny:

```
sudo rm -f /Library/LaunchDaemons/com.zabbix.zabbix_agentd.plist
sudo rm -f /usr/local/sbin/zabbix_agentd
sudo rm -f /usr/local/bin/zabbix_get
sudo rm -f /usr/local/bin/zabbix_sender
sudo rm -rf /usr/local/etc/zabbix
sudo rm -rf /var/log/zabbix
```

Usuń informację o tym, że Zabbix agent został zainstalowany:

```
sudo pkgutil --forget com.zabbix.pkg.ZabbixAgent
```

Building Zabbix agent on macOS

Przegląd

Ta sekcja pokazuje, jak zbudować binaria agenta Zabbix dla systemu macOS ze źródeł, z obsługą TLS lub bez niej.

Wymagania wstępne

Będziesz potrzebować narzędzi deweloperskich wiersza poleceń (Xcode nie jest wymagany), Automake, pkg-config oraz PCRE (v8.x) lub PCRE2 (v10.x). Jeśli chcesz zbudować pliki binarne agent z obsługą TLS, będziesz także potrzebować OpenSSL lub GnuTLS.

Aby zainstalować Automake i pkg-config, będziesz potrzebować menedżera pakietów Homebrew ze strony https://brew.sh/. Aby go zainstalować, otwórz terminal i uruchom następujące polecenie:

```
/usr/bin/ruby -e "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/master/install)"
```

Następnie zainstaluj Automake i pkg-config:

```
brew install automake
brew install pkg-config
```

Przygotowanie bibliotek PCRE, OpenSSL i GnuTLS zależy od sposobu, w jaki będą one linkowane z agent.

Jeśli zamierzasz uruchamiać pliki binarne agent na komputerze z macOS, który ma już te biblioteki, możesz użyć wstępnie skompilowanych bibliotek dostarczanych przez Homebrew. Zwykle są to komputery z macOS, na których Homebrew jest używany do budowania plików binarnych agent Zabbix lub do innych celów.

Jeśli pliki binarne agent będą używane na komputerach z macOS, które nie mają współdzielonej wersji bibliotek, powinieneś skompilować biblioteki statyczne ze źródeł i połączyć z nimi agent Zabbix.

Budowanie plików binarnych agent z bibliotekami współdzielonymi

Zainstaluj PCRE2 (w razie potrzeby zastąp *pcre2* przez *pcre* w poniższych poleceniach):

```
brew install pcre2
```

Podczas budowania z TLS zainstaluj OpenSSL i/lub GnuTLS:

```
brew install openssl
brew install gnutls
```

Pobierz kod źródłowy Zabbix:

```
git clone https://git.zabbix.com/scm/zbx/zabbix.git
```

Zbuduj agent bez TLS:

```
cd zabbix
./bootstrap.sh
./configure --sysconfdir=/usr/local/etc/zabbix --enable-agent --enable-ipv6
make
make install
```

Zbuduj agent z OpenSSL:

```
cd zabbix
./bootstrap.sh
./configure --sysconfdir=/usr/local/etc/zabbix --enable-agent --enable-ipv6 --with-openssl=/usr/local/opt/
make
make install
```

Zbuduj agent z GnuTLS:

```
cd zabbix-source/
./bootstrap.sh
./configure --sysconfdir=/usr/local/etc/zabbix --enable-agent --enable-ipv6 --with-gnutls=/usr/local/opt/g
make
make install
```

Budowanie plików binarnych agent z bibliotekami statycznymi bez TLS

Załóżmy, że statyczne biblioteki PCRE zostaną zainstalowane w `$HOME/static-libs`. Użyjemy PCRE2 10.39.

```
PCRE_PREFIX="$HOME/static-libs/pcre2-10.39"
```

Pobierz i zbuduj PCRE z obsługą właściwości Unicode:

```
mkdir static-libs-source
cd static-libs-source
curl --remote-name https://github.com/PhilipHazel/pcre2/releases/download/pcre2-10.39/pcre2-10.39.tar.gz
tar xf pcre2-10.39.tar.gz
cd pcre2-10.39
./configure --prefix="$PCRE_PREFIX" --disable-shared --enable-static --enable-unicode-properties
make
make check
make install
```

Pobierz kod źródłowy Zabbix i zbuduj agent:

```
git clone https://git.zabbix.com/scm/zbx/zabbix.git
cd zabbix
./bootstrap.sh
./configure --sysconfdir=/usr/local/etc/zabbix --enable-agent --enable-ipv6 --with-libpcre2="$PCRE_PREFIX"
make
make install
```

Budowanie plików binarnych agent z bibliotekami statycznymi przy użyciu OpenSSL

Podczas budowania OpenSSL zaleca się uruchomienie `make test` po pomyślnym zakończeniu kompilacji. Nawet jeśli kompilacja zakończyła się sukcesem, testy czasami kończą się niepowodzeniem. W takim przypadku należy zbadać problemy i je rozwiązać przed kontynuowaniem.

Załóżmy, że statyczne biblioteki PCRE i OpenSSL zostaną zainstalowane w `$HOME/static-libs`. Użyjemy PCRE2 10.39 oraz OpenSSL 1.1.1a.

```
PCRE_PREFIX="$HOME/static-libs/pcre2-10.39"
OPENSSL_PREFIX="$HOME/static-libs/openssl-1.1.1a"
```

Zbudujmy biblioteki statyczne w `static-libs-source`:

```
mkdir static-libs-source
cd static-libs-source
```

Pobierz i zbuduj PCRE z obsługą właściwości Unicode:

```
curl --remote-name https://github.com/PhilipHazel/pcre2/releases/download/pcre2-10.39/pcre2-10.39.tar.gz
tar xf pcre2-10.39.tar.gz
cd pcre2-10.39
./configure --prefix="$PCRE_PREFIX" --disable-shared --enable-static --enable-unicode-properties
make
make check
make install
cd ..
```

Pobierz i zbuduj OpenSSL:

```
curl --remote-name https://www.openssl.org/source/openssl-1.1.1a.tar.gz
tar xf openssl-1.1.1a.tar.gz
cd openssl-1.1.1a
./Configure --prefix="$OPENSSL_PREFIX" --openssldir="$OPENSSL_PREFIX" --api=1.1.0 no-shared no-capieng no-
make
make test
make install_sw
cd ..
```

Pobierz kod źródłowy Zabbix i zbuduj agent:

```
git clone https://git.zabbix.com/scm/zbx/zabbix.git
cd zabbix
./bootstrap.sh
./configure --sysconfdir=/usr/local/etc/zabbix --enable-agent --enable-ipv6 --with-libpcre2="$PCRE_PREFIX"
make
make install
```

Budowanie plików binarnych agent z bibliotekami statycznymi przy użyciu GnuTLS

GnuTLS zależy od backendu kryptograficznego Nettle oraz biblioteki arytmetycznej GMP. Zamiast używać pełnej biblioteki GMP, ten przewodnik wykorzystuje mini-gmp, które jest dołączone do Nettle.

Podczas budowania GnuTLS i Nettle zaleca się uruchomienie `make check` po pomyślnym zakończeniu kompilacji. Nawet jeśli kompilacja zakończyła się powodzeniem, testy czasami kończą się niepowodzeniem. W takim przypadku należy zbadać problemy i rozwiązać je przed kontynuowaniem.

Załóżmy, że statyczne biblioteki PCRE, Nettle i GnuTLS zostaną zainstalowane w `$HOME/static-libs`. Użyjemy PCRE2 10.39, Nettle 3.4.1 oraz GnuTLS 3.6.5.

```
PCRE_PREFIX="$HOME/static-libs/pcre2-10.39"
NETTLE_PREFIX="$HOME/static-libs/nettle-3.4.1"
GNUTLS_PREFIX="$HOME/static-libs/gnutls-3.6.5"
```

Zbudujmy biblioteki statyczne w `static-libs-source`:

```
mkdir static-libs-source
cd static-libs-source
```

Pobierz i zbuduj Nettle:

```
curl --remote-name https://ftp.gnu.org/gnu/nettle/nettle-3.4.1.tar.gz
tar xf nettle-3.4.1.tar.gz
cd nettle-3.4.1
./configure --prefix="$NETTLE_PREFIX" --enable-static --disable-shared --disable-documentation --disable-a
make
make check
make install
cd ..
```

Pobierz i zbuduj GnuTLS:

```
curl --remote-name https://www.gnupg.org/ftp/gcrypt/gnutls/v3.6/gnutls-3.6.5.tar.xz
tar xf gnutls-3.6.5.tar.xz
cd gnutls-3.6.5
PKG_CONFIG_PATH="$NETTLE_PREFIX/lib/pkgconfig" ./configure --prefix="$GNUTLS_PREFIX" --enable-static --dis
make
make check
make install
cd ..
```

Pobierz kod źródłowy Zabbix i zbuduj agent:

```
git clone https://git.zabbix.com/scm/zbx/zabbix.git
cd zabbix
./bootstrap.sh
CFLAGS="-Wno-unused-command-line-argument -framework Foundation -framework Security" \
> LIBS="-lgnutls -lhogweed -lnettle" \
> LDFLAGS="-L$GNUTLS_PREFIX/lib -L$NETTLE_PREFIX/lib" \
> ./configure --sysconfdir=/usr/local/etc/zabbix --enable-agent --enable-ipv6 --with-libpcre2="$PCRE_PREFI
make
make install
```

4 Aktualizacja

Przed aktualizacją zdecydowanie zaleca się zapoznanie ze wszystkimi odpowiednimi uwagami dotyczącymi aktualizacji.

Przydatne będzie również sprawdzenie, które komponenty należy zaktualizować.

Przegląd

Instrukcje aktualizacji krok po kroku są dostępne dla::

- Red Hat Enterprise Linux (przy użyciu pakietów)
- Debian/Ubuntu (przy użyciu pakietów)
- Aktualizacja przy użyciu kontenerów
- Aktualizacja przy użyciu źródeł

Powiązane instrukcje:

- W przypadku serwerów w klastrze wysokiej dostępności (HA) zobacz Aktualizacja klastra HA
- W przypadku bazy danych TimescaleDB zobacz Aktualizacja schematu TimescaleDB

Komponenty do aktualizacji

Aktualizacja agentów Zabbix jest zalecana, ale nie jest obowiązkowa.

Aktualizacja proxy Zabbix jest zdecydowanie zalecana. Serwer Zabbix w pełni obsługuje proxy w tej samej głównej wersji co serwer. Serwer Zabbix obsługuje również proxy, które są **nie starsze** niż poprzednie wydanie LTS serwera Zabbix, ale z ograniczoną funkcjonalnością (zbieranie danych, wykonywanie zdalnych poleceń, natychmiastowe sprawdzanie wartości pozycji). Aktualizacja konfiguracji jest również wyłączona, a nieaktualne proxy będą działać tylko ze starą konfiguracją.

> **Attention:**
> Proxy starsze niż poprzednie wydanie LTS serwera Zabbix lub nowsze niż główna wersja serwera Zabbix nie są obsługiwane. Serwer Zabbix będzie ignorował dane z nieobsługiwanych proxy, a cała komunikacja z serwerem Zabbix zakończy się niepowodzeniem z ostrzeżeniem. Więcej informacji można znaleźć w sekcji Version compatibility.

Aby zminimalizować przestoje i utratę danych podczas aktualizacji, zaleca się zatrzymanie, zaktualizowanie i uruchomienie serwera Zabbix, a następnie zatrzymywanie, aktualizowanie i uruchamianie proxy kolejno, jeden po drugim. Podczas przestoju serwera działające proxy będą kontynuować zbieranie danych. Gdy serwer zostanie ponownie uruchomiony i będzie działał, nieaktualne proxy wyślą dane do nowszego serwera (konfiguracja proxy nie zostanie jednak zaktualizowana) i pozostaną częściowo funkcjonalne. Wszelkie powiadomienia o problemach podczas przestoju serwera Zabbix zostaną wygenerowane dopiero po uruchomieniu zaktualizowanego serwera.

Jeśli Zabbix proxy jest uruchamiany po raz pierwszy i brakuje pliku bazy danych SQLite, proxy utworzy go automatycznie.

Uwaga: jeśli Zabbix proxy używa SQLite3 i podczas uruchamiania wykryje, że wersja istniejącego pliku bazy danych jest starsza niż wymagana, **automatycznie usunie plik bazy danych** i utworzy nowy. W związku z tym dane historii przechowywane w pliku

bazy danych SQLite zostaną utracone. Jeśli wersja Zabbix proxy jest starsza niż wersja pliku bazy danych, Zabbix zapisze błąd w logu i zakończy działanie.

W zależności od rozmiaru bazy danych aktualizacja bazy danych do wersji 8.0 może zająć dużo czasu.

Uwagi dotyczące aktualizacji

Bezpośrednia aktualizacja do Zabbix 8.0.x jest obsługiwana z wersji **2.0**.x. W przypadku aktualizacji ze wcześniejszych wersji należy zapoznać się z dokumentacją Zabbix dla wersji 2.0 i wcześniejszych.

Note:
Należy pamiętać, że po aktualizacji niektóre integracje oprogramowania firm trzecich w Zabbix mogą zostać objęte wpływem, jeśli zewnętrzne oprogramowanie nie jest zgodne ze zaktualizowaną wersją Zabbix.

Dostępne są następujące uwagi dotyczące aktualizacji:

Aktualizacja z wersji	Przeczytaj pełne uwagi dotyczące aktualizacji	Najważniejsze zmiany między wersjami
7.4.x	Dla: Zabbix 8.0	Podniesiono minimalne wymagane wersje bazy danych. Podniesiono minimalną wymaganą wersję PHP z 8.0.0 do 8.2.0. Znak % został dodany do listy `UnsafeUserParameters` dla Zabbix agent i Zabbix agent 2.
7.2.x	Dla: Zabbix 7.4 Zabbix 8.0	Usunięto obsługę biblioteki PCRE.
7.0.x	Dla: Zabbix 7.2 Zabbix 7.4 Zabbix 8.0	Usunięto obsługę Oracle DB.
6.4.x	Dla: Zabbix 7.0 Zabbix 7.2 Zabbix 7.4 Zabbix 8.0	Podniesiono minimalną wymaganą wersję PHP z 7.4.0 do 8.0.0. Asynchroniczne pollery dla kontroli agent, HTTP agent i SNMP walk[oid]. Oddzielna tabela bazy danych dla proxy. Zmieniono domyślną lokalizację pliku konfiguracyjnego agenta dla systemu Windows. Oracle DB oznaczono jako przestarzałe. Usunięto stary typ wartości numerycznej (float).
6.2.x	Dla: Zabbix 6.4 Zabbix 7.0 Zabbix 7.2 Zabbix 7.4 Zabbix 8.0	Podniesiono minimalną wymaganą wersję MySQL z 8.0.0 do 8.0.30. Biblioteka `libevent_pthreads` jest wymagana dla Zabbix serwer/proxy. Przy pierwszym uruchomieniu po aktualizacji Zabbix proxy z SQLite3 automatycznie usuwa starą wersję bazy danych (wraz z całą historią) i tworzy nową.
6.0.x LTS	Dla: Zabbix 6.2 Zabbix 6.4 Zabbix 7.0 Zabbix 7.2 Zabbix 7.4 Zabbix 8.0	Podniesiono minimalną wymaganą wersję PHP z 7.2.5 do 7.4.0. Monitorowanie usług zostało znacząco przebudowane. Deterministyczne wyzwalacze muszą zostać utworzone podczas aktualizacji. Jeśli dla MySQL/MariaDB włączone jest logowanie binarne, wymaga to uprawnień superusera lub ustawienia zmiennej/parametru konfiguracyjnego *log_bin_trust_function_creators = 1*. Instrukcje ustawienia tej zmiennej znajdują się w sekcji Database creation scripts.
5.4.x	Dla: Zabbix 6.0 Zabbix 6.2 Zabbix 6.4 Zabbix 7.0 Zabbix 7.2 Zabbix 7.4 Zabbix 8.0	Podniesiono minimalne wymagane wersje bazy danych. Serwer/proxy nie uruchomi się, jeśli baza danych jest przestarzała. Utracono rekordy dziennika audytu z powodu zmiany struktury bazy danych.

Aktualizacja z wersji	Przeczytaj pełne uwagi dotyczące aktualizacji	Najważniejsze zmiany między wersjami
5.2.x	Dla: Zabbix 5.4 Zabbix 6.0 Zabbix 6.2 Zabbix 6.4 Zabbix 7.0 Zabbix 7.2 Zabbix 7.4 Zabbix 8.0	Podniesiono minimalne wymagane wersje bazy danych. Agregowane pozycja zostały usunięte jako osobny typ.
5.0.x LTS	Dla: Zabbix 5.2 Zabbix 5.4 Zabbix 6.0 Zabbix 6.2 Zabbix 6.4 Zabbix 7.0 Zabbix 7.2 Zabbix 7.4 Zabbix 8.0	Podniesiono minimalną wymaganą wersję PHP z 7.2.0 do 7.2.5. Algorytm haszowania haseł został zmieniony z MD5 na bcrypt.
4.4.x	Dla: Zabbix 5.0 Zabbix 5.2 Zabbix 5.4 Zabbix 6.0 Zabbix 6.2 Zabbix 6.4 Zabbix 7.0 Zabbix 7.2 Zabbix 7.4 Zabbix 8.0	Usunięto obsługę IBM DB2. Podniesiono minimalną wymaganą wersję PHP z 5.4.0 do 7.2.0. Podniesiono minimalne wymagane wersje bazy danych. Zmieniono katalog plików PHP Zabbix.
4.2.x	Dla: Zabbix 4.4 Zabbix 5.0 Zabbix 5.2 Zabbix 5.4 Zabbix 6.0 Zabbix 6.2 Zabbix 6.4 Zabbix 7.0 Zabbix 7.2 Zabbix 7.4 Zabbix 8.0	Usunięto typy mediów Jabber i Ez Texting.
4.0.x LTS	Dla: Zabbix 4.2 Zabbix 4.4 Zabbix 5.0 Zabbix 5.2 Zabbix 5.4 Zabbix 6.0 Zabbix 6.2 Zabbix 6.4 Zabbix 7.0 Zabbix 7.2 Zabbix 7.4 Zabbix 8.0	Starsze proxy nie mogą już raportować danych do zaktualizowanego serwera. Nowsze agenty nie będą już mogły współpracować ze starszym serwerem Zabbix.

Aktualizacja z wersji	Przeczytaj pełne uwagi dotyczące aktualizacji	Najważniejsze zmiany między wersjami
3.4.x	Dla: Zabbix 4.0 Zabbix 4.2 Zabbix 4.4 Zabbix 5.0 Zabbix 5.2 Zabbix 5.4 Zabbix 6.0 Zabbix 6.2 Zabbix 6.4 Zabbix 7.0 Zabbix 7.2 Zabbix 7.4 Zabbix 8.0	Biblioteki `libpthread` i `zlib` są teraz obowiązkowe. Usunięto obsługę protokołu zwykłego tekstu, a nagłówek jest obowiązkowy. Agenty Zabbix w wersji wcześniejszej niż 1.4 nie są już obsługiwane. Parametr Server w konfiguracji pasywnego proxy jest teraz obowiązkowy.
3.2.x	Dla: Zabbix 3.4 Zabbix 4.0 Zabbix 4.2 Zabbix 4.4 Zabbix 5.0 Zabbix 5.2 Zabbix 5.4 Zabbix 6.0 Zabbix 6.2 Zabbix 6.4 Zabbix 7.0 Zabbix 7.2 Zabbix 7.4 Zabbix 8.0	Usunięto obsługę SQLite jako bazy danych backendowej dla Zabbix serwer/frontend. Zamiast rozszerzonych wyrażeń regularnych POSIX obsługiwane są Perl Compatible Regular Expressions (PCRE). Biblioteki `libpcre` i `libevent` są obowiązkowe dla Zabbix serwer. Dodano sprawdzanie kodów wyjścia dla parametrów użytkownika, zdalnych poleceń i pozycja system.run[] bez flagi `nowait`, a także dla skryptów wykonywanych przez Zabbix serwer. Aby obsługiwać nową funkcjonalność, Zabbix Java gateway musi zostać zaktualizowany.
3.0.x LTS	Dla: Zabbix 3.2 Zabbix 3.4 Zabbix 4.0 Zabbix 4.2 Zabbix 4.4 Zabbix 5.0 Zabbix 5.2 Zabbix 5.4 Zabbix 6.0 Zabbix 6.2 Zabbix 6.4 Zabbix 7.0 Zabbix 7.2 Zabbix 7.4 Zabbix 8.0	Aktualizacja bazy danych może być powolna, w zależności od rozmiaru tabeli historii.

Aktualizacja z wersji	Przeczytaj pełne uwagi dotyczące aktualizacji	Najważniejsze zmiany między wersjami
2.4.x	Dla: Zabbix 3.0 Zabbix 3.2 Zabbix 3.4 Zabbix 4.0 Zabbix 4.2 Zabbix 4.4 Zabbix 5.0 Zabbix 5.2 Zabbix 5.4 Zabbix 6.0 Zabbix 6.2 Zabbix 6.4 Zabbix 7.0 Zabbix 7.2 Zabbix 7.4 Zabbix 8.0	Podniesiono minimalną wymaganą wersję PHP z 5.3.0 do 5.4.0. Należy określić parametr agenta LogFile.
2.2.x LTS	Dla: Zabbix 2.4 Zabbix 3.0 Zabbix 3.2 Zabbix 3.4 Zabbix 4.0 Zabbix 4.2 Zabbix 4.4 Zabbix 5.0 Zabbix 5.2 Zabbix 5.4 Zabbix 6.0 Zabbix 6.2 Zabbix 6.4 Zabbix 7.0 Zabbix 7.2 Zabbix 7.4 Zabbix 8.0	Usunięto rozproszone monitorowanie oparte na węzłach.
2.0.x	Dla: Zabbix 2.2 Zabbix 2.4 Zabbix 3.0 Zabbix 3.2 Zabbix 3.4 Zabbix 4.0 Zabbix 4.2 Zabbix 4.4 Zabbix 5.0 Zabbix 5.2 Zabbix 5.4 Zabbix 6.0 Zabbix 6.2 Zabbix 6.4 Zabbix 7.0 Zabbix 7.2 Zabbix 7.4 Zabbix 8.0	Podniesiono minimalną wymaganą wersję PHP z 5.1.6 do 5.3.0. Do poprawnego działania serwera wymagana jest baza danych MySQL rozróżniająca wielkość liter; aby Zabbix serwer działał poprawnie z bazą danych MySQL, wymagane są zestaw znaków utf8 i porównywanie utf8_bin. Zobacz database creation scripts. Wymagane jest rozszerzenie PHP `mysqli` zamiast `mysql`.

Upgrade from packages

Przegląd

Ta sekcja zawiera kroki wymagane do pomyślnego uaktualnienia przy użyciu oficjalnych pakietów RPM i DEB dostarczanych przez

Zabbix dla:

- Red Hat Enterprise Linux
- Debian/Ubuntu

Pakiety Zabbix z repozytoriów systemu operacyjnego

Niektóre dystrybucje systemów operacyjnych (w szczególności dystrybucje oparte na Debianie) udostępniają własne pakiety Zabbix. Pakiety te **nie są wspierane przez Zabbix** i mogą być nieaktualne lub nie zawierać najnowszych funkcji oraz poprawek błędów. Zaleca się korzystanie wyłącznie z oficjalnych pakietów z Oficjalnego Repozytorium Zabbix.

Jeśli przeprowadzasz aktualizację z pakietów dostarczanych przez dystrybucje systemu operacyjnego (lub były one zainstalowane w pewnym momencie), wykonaj poniższą procedurę, aby przejść na oficjalne pakiety Zabbix:

1. Odinstaluj stare pakiety.
2. Sprawdź, czy po starej instalacji nie pozostały żadne pliki, i usuń je.
3. Zainstaluj oficjalne pakiety Zabbix zgodnie z instrukcjami instalacji udostępnionymi przez Zabbix.

Nie wykonuj bezpośredniej aktualizacji, ponieważ może to spowodować uszkodzenie instalacji.

Debian/Ubuntu

Przegląd

Ta sekcja zawiera instrukcje dotyczące aktualizacji z Zabbix **7.4.x** do najnowszej wersji Zabbix **8.0.x** przy użyciu oficjalnych pakietów Zabbix dla Debiana/Ubuntu.

> **Warning:**
> Przed aktualizacją zapoznaj się z odpowiednimi uwagami dotyczącymi aktualizacji i upewnij się, że Twój system spełnia wymagania dla Zabbix 8.0.

> **Note:**
> Rozważ uruchomienie dwóch równoległych sesji SSH podczas aktualizacji: jednej do wykonywania kroków aktualizacji, a drugiej do monitorowania logów serwera/proxy. Na przykład w drugiej sesji uruchom `tail -f zabbix_server.log` lub `tail -f zabbix_proxy.log`, aby wyświetlać najnowsze wpisy logów i możliwe błędy w czasie rzeczywistym. Może to mieć kluczowe znaczenie w środowiskach produkcyjnych.

Instrukcje dotyczące aktualizacji między wersjami podrzędnymi Zabbix 8.0.x (na przykład z 8.0.1 do 8.0.3) znajdują się w sekcji Aktualizacja między wersjami podrzędnymi.

Procedura aktualizacji

1 Zatrzymaj procesy Zabbix

Zatrzymaj serwer Zabbix, aby upewnić się, że do bazy danych nie są wstawiane żadne nowe dane:

```
systemctl stop zabbix-server
```

Jeśli aktualizujesz Zabbix proxy, agent lub agent 2, zatrzymaj również te komponenty:

```
systemctl stop zabbix-proxy
systemctl stop zabbix-agent
systemctl stop zabbix-agent2
```

2 Utwórz kopię zapasową bazy danych Zabbix

Utwórz kopię zapasową istniejącej bazy danych Zabbix, aby zabezpieczyć się przed niepowodzeniem aktualizacji (na przykład z powodu braku miejsca na dysku, utraty zasilania lub nieoczekiwanych problemów).

3 Utwórz kopię zapasową plików konfiguracyjnych Zabbix, plików PHP i plików binarnych Zabbix

Utwórz kopię zapasową istniejących plików konfiguracyjnych Zabbix, plików PHP i plików binarnych Zabbix.

W przypadku plików konfiguracyjnych uruchom:

```
mkdir /opt/zabbix-backup/
cp /etc/zabbix/zabbix_server.conf /opt/zabbix-backup/
cp /etc/apache2/conf-enabled/zabbix.conf /opt/zabbix-backup/
```

W przypadku plików PHP i plików binarnych Zabbix uruchom:

```
cp -R /usr/share/zabbix/ /opt/zabbix-backup/
cp -R /usr/share/zabbix-* /opt/zabbix-backup/
```

4 Aktualizacja pakietu konfiguracji repozytorium

Przed przystąpieniem do aktualizacji odinstaluj bieżący pakiet repozytorium Zabbix:

```
rm -Rf /etc/apt/sources.list.d/zabbix.list
```

Może być również konieczne ręczne usunięcie starych pakietów Zabbix z katalogu roboczego (np. `rm zabbix-release_latest+debian12_` przed pobraniem nowego, aby zapobiec ponownemu użyciu nieaktualnej wersji przez menedżera pakietów podczas procesu aktualizacji.

Następnie zainstaluj najnowszy pakiet konfiguracji repozytorium, aby zapewnić zgodność z najnowszymi pakietami oraz uwzględnić ostatnie poprawki bezpieczeństwa i poprawki błędów.

W systemie **Debian 12** uruchom:

```
wget https://repo.zabbix.com/zabbix/8.0/release/debian/pool/main/z/zabbix-release/zabbix-release_latest+de
dpkg -i zabbix-release_latest+debian12_all.deb
```

Note:
W przypadku starszych wersji Debiana zastąp powyższy link właściwym linkiem z repozytorium Zabbix. Należy jednak pamiętać, że pakiety dla tych wersji mogą nie zawierać wszystkich komponentów Zabbix, a aby zaktualizować te komponenty z pakietów, rozważ aktualizację systemu operacyjnego. Listę dołączonych komponentów można znaleźć w sekcji Pakiety Zabbix.

W systemie **Ubuntu 24.04** uruchom:

```
wget https://repo.zabbix.com/zabbix/8.0/release/ubuntu/pool/main/z/zabbix-release/zabbix-release_latest+ub
dpkg -i zabbix-release_latest+ubuntu24.04_all.deb
```

W systemie **Ubuntu 22.04** uruchom:

```
wget https://repo.zabbix.com/zabbix/8.0/release/ubuntu/pool/main/z/zabbix-release/zabbix-release_latest+ub
dpkg -i zabbix-release_latest+ubuntu22.04_all.deb
```

Note:
W przypadku starszych wersji Ubuntu zastąp powyższy link właściwym linkiem z repozytorium Zabbix. Należy jednak pamiętać, że pakiety dla tych wersji mogą nie zawierać wszystkich komponentów Zabbix, a aby zaktualizować te komponenty z pakietów, rozważ aktualizację systemu operacyjnego. Listę dołączonych komponentów można znaleźć w sekcji Pakiety Zabbix.

Możesz zobaczyć monit dotyczący konfiguracji repozytorium Zabbix:

```
Configuration file '/etc/apt/sources.list.d/zabbix.list'
==> Deleted (by you or by a script) since installation.
==> Package distributor has shipped an updated version.
What would you like to do about it ?  Your options are:
Y or I  : install the package maintainer's version
N or O  : keep your currently-installed version
D       : show the differences between the versions
Z       : start a shell to examine the situation
The default action is to keep your current version.
*** zabbix.list (Y/I/N/O/D/Z) [default=N] ?
```

Wprowadź `Y` (lub `I`), aby zainstalować wersję konfiguracji repozytorium Zabbix dostarczoną przez opiekuna pakietu.

Następnie zaktualizuj informacje o repozytorium:

```
apt update
```

5 Aktualizacja komponentów Zabbix

Aby zaktualizować komponenty Zabbix, uruchom:

```
apt install --only-upgrade zabbix-server-mysql zabbix-frontend-php zabbix-agent
```

- Jeśli używasz PostgreSQL, zastąp `mysql` przez `pgsql` w poleceniu.

- Jeśli aktualizujesz proxy, zastąp `server` przez `proxy` w poleceniu.
- Jeśli aktualizujesz Zabbix agent 2, zastąp `zabbix-agent` przez `zabbix-agent2 zabbix-agent2-plugin-*` w poleceniu.

Attention:
Aktualizacja Zabbix agent 2 za pomocą polecenia `apt install zabbix-agent2` może prowadzić do błędu. Aby uzyskać więcej informacji, zobacz *Znane problemy*.

Może zostać wyświetlony monit dotyczący konfiguracji serwera Zabbix (lub proxy):

```
Configuration file '/etc/zabbix/zabbix_server.conf'
==> Modified (by you or by a script) since installation.
==> Package distributor has shipped an updated version.
What would you like to do about it ?  Your options are:
Y or I  : install the package maintainer's version
N or O  : keep your currently-installed version
D       : show the differences between the versions
Z       : start a shell to examine the situation
The default action is to keep your current version.
*** zabbix_server.conf (Y/I/N/O/D/Z) [default=N] ?
```

Wybierz opcję, która najlepiej pasuje do Twojej sytuacji. Na przykład wpisz `D`, aby porównać bieżącą i nową konfigurację, a następnie zdecyduj, czy chcesz zainstalować wersję dostarczoną przez opiekuna pakietu (`Y` lub `I`).

Następnie, aby zaktualizować frontend Zabbix z Apache i ponownie uruchomić Apache, wykonaj:

```
apt install zabbix-apache-conf
systemctl restart apache2
```

6 Przejrzyj parametry konfiguracji komponentu

Przejrzyj odpowiednie uwagi dotyczące aktualizacji, aby sprawdzić, czy konieczne są jakiekolwiek zmiany parametrów konfiguracji.

Informacje o nowych opcjonalnych parametrach można znaleźć na stronie Co nowego.

7 Uruchom procesy Zabbix

Uruchom zaktualizowane komponenty Zabbix:

```
systemctl start zabbix-server
systemctl start zabbix-proxy
systemctl start zabbix-agent
systemctl start zabbix-agent2
```

8 Wyczyść pliki cookie i pamięć podręczną przeglądarki internetowej

Po aktualizacji może być konieczne wyczyszczenie plików cookie i pamięci podręcznej przeglądarki internetowej, aby interfejs webowy Zabbix działał prawidłowo.

Aktualizacja między wersjami minor

Możliwa jest aktualizacja między wersjami minor Zabbix 8.0.x (na przykład z 8.0.1 do 8.0.3).

Najpierw zaktualizuj informacje o repozytorium:

```
apt update
```

Następnie, aby zaktualizować wszystkie komponenty Zabbix, uruchom:

```
apt install --only-upgrade 'zabbix*'
```

- Aby zaktualizować tylko serwer Zabbix, zastąp w poleceniu `'zabbix*'` przez `'zabbix-server*'`.
- Aby zaktualizować tylko proxy Zabbix, zastąp w poleceniu `'zabbix*'` przez `'zabbix-proxy*'`.
- Aby zaktualizować tylko agent Zabbix, zastąp w poleceniu `'zabbix*'` przez `'zabbix-agent*'`.
- Aby zaktualizować tylko agent 2 Zabbix, zastąp w poleceniu `'zabbix*'` przez `'zabbix-agent2*'`.

Red Hat Enterprise Linux

Przegląd

Ta sekcja zawiera instrukcje dotyczące aktualizacji z Zabbix **7.4.x** do najnowszej wersji Zabbix **8.0.x** przy użyciu oficjalnych pakietów Zabbix dla Red Hat Enterprise Linux lub jego pochodnych — AlmaLinux, CentOS Stream, Oracle Linux i Rocky Linux.

Warning:
Przed aktualizacją zapoznaj się z odpowiednimi uwagami dotyczącymi aktualizacji i upewnij się, że Twój system spełnia wymagania dla Zabbix 8.0.

Note:
Rozważ uruchomienie dwóch równoległych sesji SSH podczas aktualizacji: jednej do wykonywania kroków aktualizacji, a drugiej do monitorowania logów serwera/proxy. Na przykład uruchom `tail -f zabbix_server.log` lub `tail -f zabbix_proxy.log` w drugiej sesji, aby wyświetlać najnowsze wpisy logów i ewentualne błędy w czasie rzeczywistym. Może to mieć kluczowe znaczenie w przypadku instancji produkcyjnych.

Instrukcje dotyczące aktualizacji między wersjami podrzędnymi Zabbix 8.0.x (na przykład z 8.0.1 do 8.0.3) znajdują się w sekcji Aktualizacja między wersjami podrzędnymi.

Procedura aktualizacji

1 Zatrzymaj procesy Zabbix

Zatrzymaj serwer Zabbix, aby upewnić się, że żadne nowe dane nie są wstawiane do bazy danych:

```
systemctl stop zabbix-server
```

Jeśli aktualizujesz Zabbix proxy, agent lub agent 2, zatrzymaj również te komponenty:

```
systemctl stop zabbix-proxy
systemctl stop zabbix-agent
systemctl stop zabbix-agent2
```

2 Utwórz kopię zapasową bazy danych Zabbix

Utwórz kopię zapasową istniejącej bazy danych Zabbix, aby zabezpieczyć się przed niepowodzeniem aktualizacji (na przykład z powodu problemów z miejscem na dysku, utraty zasilania lub nieoczekiwanych problemów).

3 Utwórz kopię zapasową plików konfiguracyjnych Zabbix, plików PHP i plików binarnych Zabbix

Utwórz kopię zapasową istniejących plików konfiguracyjnych Zabbix, plików PHP i plików binarnych Zabbix.

Dla plików konfiguracyjnych uruchom:

```
mkdir /opt/zabbix-backup/
cp /etc/zabbix/zabbix_server.conf /opt/zabbix-backup/
cp /etc/httpd/conf.d/zabbix.conf  /opt/zabbix-backup/
```

Dla plików PHP i plików binarnych Zabbix uruchom:

```
cp -R /usr/share/zabbix/ /opt/zabbix-backup/
cp -R /usr/share/zabbix-* /opt/zabbix-backup/
```

4 Aktualizacja pakietu konfiguracji repozytorium

Przed przystąpieniem do aktualizacji zaktualizuj bieżący pakiet repozytorium do najnowszej wersji, aby zapewnić zgodność z najnowszymi pakietami oraz uwzględnić ostatnie poprawki bezpieczeństwa i poprawki błędów.

W systemie **RHEL 10** uruchom:

```
rpm -Uvh https://repo.zabbix.com/zabbix/8.0/release/rhel/10/noarch/zabbix-release-latest.el10.noarch.rpm
```

W systemie **RHEL 9** uruchom:

```
rpm -Uvh https://repo.zabbix.com/zabbix/8.0/release/rhel/9/noarch/zabbix-release-latest.el9.noarch.rpm
```

Note:
W przypadku starszych wersji RHEL lub systemów pochodnych zastąp powyższy link właściwym linkiem z repozytorium Zabbix. Należy jednak pamiętać, że pakiety dla tych wersji mogą nie zawierać wszystkich komponentów Zabbix, a aby zaktualizować te komponenty z pakietów, rozważ aktualizację systemu operacyjnego. Listę uwzględnionych komponentów można znaleźć w sekcji Pakiety Zabbix.

Następnie wyczyść pamięć podręczną menedżera pakietów dnf (w tym nagłówki, metadane i pliki pakietów pobrane podczas poprzednich instalacji lub aktualizacji):

```
dnf clean all
```

Przy następnej operacji dnf pobierze świeże metadane z repozytoriów, ponieważ stare metadane zostały usunięte.

Zobacz także: Znane problemy dotyczące aktualizacji pakietu konfiguracji repozytorium w systemie RHEL.

5 Aktualizacja komponentów Zabbix

Aby zaktualizować komponenty Zabbix, uruchom:

```
dnf install zabbix-server-mysql zabbix-web-mysql zabbix-agent
```

- Jeśli używasz PostgreSQL, w poleceniu zastąp mysql przez pgsql.
- Jeśli aktualizujesz proxy, w poleceniu zastąp server przez proxy.
- Jeśli aktualizujesz agent 2, zastąp zabbix-agent przez zabbix-agent2 zabbix-agent2-plugin-* w poleceniu.

Attention:
Aktualizacja Zabbix agent 2 za pomocą polecenia dnf install zabbix-agent2 może prowadzić do błędu. Więcej informacji znajdziesz w *Znane problemy*.

Następnie, aby zaktualizować frontend Zabbix z Apache i ponownie uruchomić Apache, wykonaj:

```
dnf install zabbix-apache-conf
systemctl restart httpd
```

6 Przejrzyj parametry konfiguracji komponentów

Przejrzyj odpowiednie uwagi dotyczące aktualizacji, aby sprawdzić, czy konieczne są jakiekolwiek zmiany parametrów konfiguracji.

Informacje o nowych opcjonalnych parametrach można znaleźć na stronie Co nowego.

7 Uruchom procesy Zabbix

Uruchom zaktualizowane komponenty Zabbix:

```
systemctl start zabbix-server
systemctl start zabbix-proxy
systemctl start zabbix-agent
systemctl start zabbix-agent2
```

8 Wyczyść pliki cookie i pamięć podręczną przeglądarki internetowej

Po aktualizacji może być konieczne wyczyszczenie plików cookie i pamięci podręcznej przeglądarki internetowej, aby interfejs webowy Zabbix działał prawidłowo.

Aktualizacja między wersjami pobocznymi

Możliwa jest aktualizacja między wersjami pobocznymi Zabbix 8.0.x (na przykład z 8.0.1 do 8.0.3).

Aby zaktualizować wszystkie komponenty Zabbix, uruchom:

```
dnf upgrade 'zabbix-*'
```

- Aby zaktualizować tylko serwer Zabbix, zastąp w poleceniu 'zabbix-*' przez 'zabbix-server-*'.
- Aby zaktualizować tylko proxy Zabbix, zastąp w poleceniu 'zabbix-*' przez 'zabbix-proxy-*'.
- Aby zaktualizować tylko agent Zabbix, zastąp w poleceniu 'zabbix-*' przez 'zabbix-agent-*'.
- Aby zaktualizować tylko Zabbix agent 2, zastąp w poleceniu 'zabbix-*' przez 'zabbix-agent2-*'.

Problemy podczas aktualizacji

Związane z sekwencjami ucieczki Przekroczony limit znaków dla parametrów funkcji po aktualizacji

W Zabbix 7.0 dodano prawidłowe stosowanie znaków ucieczki dla ukośników odwrotnych w parametrach tekstowych funkcji historii.

Ponieważ podczas aktualizacji z wersji Zabbix starszych niż 7.0 dodawane są dodatkowe ukośniki odwrotne, prowadzi to do wydłużenia parametrów, co może skutkować uszkodzeniem funkcji wyzwalaczy, jeśli długość parametru przekroczy maksymalny rozmiar danych wynoszący 255 znaków.

Aby zilustrować, jakie problemy mogą wystąpić podczas aktualizacji bazy danych, jaki mają wpływ oraz jak je rozpoznać i naprawić, rozważmy przykładową konfigurację z 3 pozycjami i 2 wyzwalaczami.

Konfiguracja

1. Wersja Zabbix 6.0.
2. Plik `/tmp/ONE`, który zawiera 114 ukośników odwrotnych, z literą „a” na końcu:

```
\\\
```

2. Aktualizacja bazy danych **kończy się**, a serwer Zabbix nadal działa.
3. Calc_228 nadal zwraca 1, podczas gdy Calc_232 zwraca 0.
4. Wyzwalacze zostały zaktualizowane w następujący sposób:

Trig_228:

```
find(/Zabbix server/vfs.file.contents[/tmp/ONE],1m:now,"regexp","\\\
```

Attention:
Przed rozpoczęciem uaktualnienia należy sprawdzić, czy użytkownicy mają niezbędne uprawnienia do bazy danych na potrzeby uaktualnienia.

W przypadku uaktualnienia z Zabbix 6.0 lub starszego podczas uaktualnienia konieczne będzie utworzenie deterministycznych wyzwalaczy. Jeśli dla MySQL/MariaDB włączone jest logowanie binarne, wymaga to uprawnień superusera lub ustawienia zmiennej/parametru konfiguracyjnego *log_bin_trust_function_creators = 1*. Instrukcje dotyczące ustawienia tej zmiennej znajdują się w sekcji Database creation scripts.
Należy pamiętać, że w przypadku wykonania z konsoli zmienna zostanie ustawiona tylko tymczasowo i zostanie utracona po ponownym uruchomieniu Dockera. W takim przypadku należy pozostawić usługę SQL uruchomioną, zatrzymać tylko usługę zabbix-server, uruchamiając `docker compose down zabbix-server`, a następnie `docker compose up -d zabbix-server`.
Alternatywnie można ustawić tę zmienną w pliku konfiguracyjnym.

W zależności od rozmiaru bazy danych uaktualnienie do wersji 8.0 może zająć dość dużo czasu.

Aktualizacja obrazu Zabbix

Poniższe kroki można wykorzystać do aktualizacji dowolnego komponentu Zabbix. Zastąp `zabbix-server-mysql` nazwą obrazu wymaganego komponentu.

1. Sprawdź bieżącą wersję obrazu:

```
docker inspect -f '{{ .Config.Image }}' zabbix-server-mysql
```

2. Pobierz żądaną wersję obrazu, na przykład:

```
docker pull zabbix/zabbix-server-mysql:alpine-8.0-latest
```

`zabbix/zabbix-server-mysql:alpine-8.0-latest` pobierze najnowszą wydaną pomocniczą wersję Zabbix serwer 8.0 z obsługą MySQL opartą na Alpine Linux. Zastąp ją nazwą repozytorium Docker i kombinacją tagów, których potrzebujesz. Listę dostępnych opcji znajdziesz w Instalacja z kontenerów.

3. Zatrzymaj kontener:

```
docker stop zabbix-server-mysql
```

4. Usuń kontener:

```
docker rm zabbix-server-mysql
```

5. Uruchom zaktualizowany kontener, wykonując polecenie `docker run`, a następnie podając dodatkowe argumenty określające wymagane zmienne środowiskowe i/lub punkty montowania.

Przykłady konfiguracji

Zabbix serwer z MySQL:

```
docker run --name zabbix-server-mysql -t \
    -e DB_SERVER_HOST="mysql-server" \
    -e MYSQL_DATABASE="zabbix" \
    -e MYSQL_USER="zabbix" \
    -e MYSQL_PASSWORD="zabbix_pwd" \
    -e MYSQL_ROOT_PASSWORD="root_pwd" \
    -e ZBX_JAVAGATEWAY="zabbix-java-gateway" \
    --network=zabbix-net \
    -p 10051:10051 \
    --restart unless-stopped \
    -d zabbix/zabbix-server-mysql:alpine-8.0-latest
```

Zabbix serwer z PostgreSQL:

```
docker run --name zabbix-server-pgsql -t \
    -e DB_SERVER_HOST="postgres-server" \
    -e POSTGRES_USER="zabbix" \
    -e POSTGRES_PASSWORD="zabbix_pwd" \
    -e POSTGRES_DB="zabbix" \
    -e ZBX_ENABLE_SNMP_TRAPS="true" \
    --network=zabbix-net \
```

```
    -p 10051:10051 \
    --volumes-from zabbix-snmptraps \
    --restart unless-stopped \
    -d zabbix/zabbix-server-pgsql:alpine-8.0-latest
```

Serwer MySQL:

```
docker run --name mysql-server -t \
    -e MYSQL_DATABASE="zabbix" \
    -e MYSQL_USER="zabbix" \
    -e MYSQL_PASSWORD="zabbix_pwd" \
    -e MYSQL_ROOT_PASSWORD="root_pwd" \
    --network=zabbix-net \
    --restart unless-stopped \
    -d mysql:8.4-oracle \
    --character-set-server=utf8mb4--collation-server=utf8mb4_bin \
```

Więcej przykładów konfiguracji, w tym przykładów dla innych komponentów Zabbix, jest dostępnych na stronie Instalacja z kontenerów.

6. Zweryfikuj aktualizację:

```
docker logs -f zabbix-server-mysql
```

Pliki compose

Postępuj zgodnie z instrukcjami aktualizacji w tej sekcji, jeśli zainstalowano Zabbix przy użyciu pliku compose.

1. Sprawdź bieżącą wersję obrazu:

```
docker inspect -f '{{ .Config.Image }}' zabbix-server-mysql
```

2. Pobierz najnowsze aktualizacje z repozytorium GitHub i przełącz się na wymaganą gałąź:

```
git pull
git checkout 8.0
```

3. Uruchom komponenty Zabbix przy użyciu nowego pliku compose:

```
docker-compose -f ./docker-compose_v3_alpine_mysql_latest.yaml up -d
```

4. Zweryfikuj aktualizację:

```
docker logs -f zabbix-server-mysql
```

Więcej szczegółów, w tym listy obsługiwanych zmiennych środowiskowych i punktów montowania woluminów, znajduje się w sekcji Instalacja z kontenerów.

Upgrade from sources

Przegląd

Ta sekcja zawiera kroki wymagane do pomyślnego upgrade z Zabbix **7.4**.x do Zabbix **8.0**.x przy użyciu oficjalnych źródeł Zabbix.

> **Warning:**
> Przed upgrade upewnij się, że przeczytałeś odpowiednie **uwagi dotyczące upgrade**!

Możesz także chcieć zapoznać się z wymaganiami dla wersji 8.0.

> **Note:**
> Podczas upgrade przydatne może być uruchomienie dwóch równoległych sesji SSH: w jednej wykonywanie kroków upgrade, a w drugiej monitorowanie logów serwera/proxy. Na przykład uruchom `tail -f zabbix_server.log` lub `tail -f zabbix_proxy.log` w drugiej sesji SSH, aby na bieżąco widzieć najnowsze wpisy w pliku logu oraz ewentualne błędy w czasie rzeczywistym. Może to mieć kluczowe znaczenie dla środowisk produkcyjnych.

Proces aktualizacji serwera

1 Zatrzymaj serwer

Zatrzymaj serwer Zabbix, aby upewnić się, że do bazy danych nie są wstawiane żadne nowe dane.

2 Utwórz kopię zapasową istniejącej bazy danych Zabbix

To bardzo ważny krok. Upewnij się, że masz kopię zapasową swojej bazy danych. Pomoże ona, jeśli procedura aktualizacji zakończy się niepowodzeniem (brak miejsca na dysku, zanik zasilania, jakikolwiek nieoczekiwany problem).

3 Utwórz kopię zapasową plików konfiguracyjnych, plików PHP i plików binarnych Zabbix

Utwórz kopię zapasową plików binarnych Zabbix, plików konfiguracyjnych oraz katalogu plików PHP.

4 Instalacja nowych plików binarnych serwera

Skorzystaj z tych instrukcji aby skompilować serwer Zabbix ze źródeł.

5 Przejrzyj parametry konfiguracji serwera

Upewnij się, że zapoznałeś się z uwagami dotyczącymi aktualizacji, aby sprawdzić, czy wymagane są jakiekolwiek zmiany parametrów konfiguracji.

Informacje o nowych opcjonalnych parametrach znajdziesz na stronie Co nowego.

6 Uruchom nowe pliki binarne Zabbix

Uruchom nowe pliki binarne. Sprawdź pliki dziennika, aby zobaczyć, czy pliki binarne zostały uruchomione pomyślnie.

serwer Zabbix automatycznie zaktualizuje bazę danych. Podczas uruchamiania serwer Zabbix zgłasza bieżące (obowiązkową i opcjonalną) oraz wymaganą wersję bazy danych. Jeśli bieżąca wersja obowiązkowa jest starsza niż wymagana wersja, serwer Zabbix automatycznie wykona wymagane poprawki aktualizacji bazy danych. Rozpoczęcie i poziom postępu (procentowy) aktualizacji bazy danych są zapisywane w pliku dziennika serwera Zabbix. Po zakończeniu aktualizacji do pliku dziennika zostaje zapisany komunikat „database upgrade fully completed". Jeśli którakolwiek z poprawek aktualizacji zakończy się niepowodzeniem, serwer Zabbix nie uruchomi się. serwer Zabbix nie uruchomi się również, jeśli bieżąca obowiązkowa wersja bazy danych jest nowsza niż wymagana. serwer Zabbix uruchomi się tylko wtedy, gdy bieżąca obowiązkowa wersja bazy danych odpowiada wymaganej obowiązkowej wersji.

```
8673:20161117:104750.259 current database version (mandatory/optional): 03040000/03040000
8673:20161117:104750.259 required mandatory version: 03040000
```

Przed uruchomieniem serwera:

- Upewnij się, że użytkownik bazy danych ma wystarczające uprawnienia (create table, drop table, create index, drop index)
- Upewnij się, że masz wystarczającą ilość wolnego miejsca na dysku.

7 Instalacja nowego interfejsu webowego Zabbix

Minimalna wymagana wersja PHP to 8.2.0. W razie potrzeby zaktualizuj ją i postępuj zgodnie z instrukcjami instalacji.

8 Wyczyść pliki cookie i pamięć podręczną przeglądarki internetowej

Po aktualizacji może być konieczne wyczyszczenie plików cookie i pamięci podręcznej przeglądarki internetowej, aby interfejs webowy Zabbix działał prawidłowo.

Proces aktualizacji proxy

1 Zatrzymaj proxy

Zatrzymaj Zabbix proxy.

2 Utwórz kopię zapasową plików konfiguracyjnych i plików binarnych Zabbix proxy

Utwórz kopię zapasową pliku binarnego Zabbix proxy oraz pliku konfiguracyjnego.

3 Instalacja nowych plików binarnych proxy

Użyj tych instrukcji, aby skompilować proxy Zabbix ze źródeł.

4 Przejrzyj parametry konfiguracji proxy

Upewnij się, że zapoznałeś się z uwagami dotyczącymi aktualizacji, aby sprawdzić, czy wymagane są jakiekolwiek zmiany parametrów konfiguracji.

Informacje o nowych opcjonalnych parametrach znajdziesz na stronie Co nowego.

5 Uruchom nowy Zabbix proxy

Uruchom nowy Zabbix proxy. Sprawdź pliki dziennika, aby zobaczyć, czy proxy uruchomił się pomyślnie.

Zabbix proxy automatycznie zaktualizuje bazę danych. Aktualizacja bazy danych przebiega podobnie jak podczas uruchamiania Zabbix server.

Proces aktualizacji agenta

> **Attention:**
> Aktualizacja agentów nie jest obowiązkowa. Należy zaktualizować agenty tylko wtedy, gdy jest to wymagane do uzyskania dostępu do nowych funkcji.

Procedura aktualizacji opisana w tej sekcji może być używana do aktualizacji zarówno agenta Zabbix, jak i agenta Zabbix 2.

1 Zatrzymaj agent

Zatrzymaj agent Zabbix.

2 Utwórz kopię zapasową plików konfiguracyjnych i plików binarnych agenta Zabbix

Utwórz kopię zapasową pliku binarnego agenta Zabbix oraz pliku konfiguracyjnego.

3 Zainstaluj nowe pliki binarne agenta

Skorzystaj z tych instrukcji, aby skompilować agent Zabbix ze źródeł.

Alternatywnie możesz pobrać wstępnie skompilowane agenty Zabbix ze strony pobierania Zabbix.

4 Przejrzyj parametry konfiguracji agent

Upewnij się, że zapoznałeś się z uwagami dotyczącymi aktualizacji, aby sprawdzić, czy wymagane są jakiekolwiek zmiany parametrów konfiguracji.

Informacje o nowych opcjonalnych parametrach można znaleźć na stronie Co nowego.

5 Uruchom nowy agent Zabbix

Uruchom nowy agent Zabbix. Sprawdź pliki dziennika, aby zobaczyć, czy agent został uruchomiony pomyślnie.

Aktualizacja między wersjami pobocznymi

Podczas aktualizacji między wersjami pobocznymi 8.0.x (na przykład z 8.0.1 do 8.0.3) wymagane jest wykonanie tych samych działań dla serwer/proxy/agent jak podczas aktualizacji między wersjami głównymi. Jedyna różnica polega na tym, że podczas aktualizacji między wersjami pobocznymi nie są wprowadzane żadne zmiany w bazie danych.

5 Uwagi dotyczące aktualizacji do Zabbix 8.0

Te uwagi dotyczą aktualizacji z Zabbix 7.4.x do Zabbix 8.0.0.

Wszystkie uwagi są pogrupowane w następujące kategorie:

- **Zmiany niekompatybilne** - zmiany, które mogą spowodować problemy w istniejących instalacjach, oraz inne krytyczne informacje związane z procesem aktualizacji
- **Inne** - wszystkie pozostałe informacje opisujące zmiany w funkcjonalności Zabbix

Zobacz także:

- Procedura aktualizacji zawierająca wszystkie istotne informacje o aktualizacji z wersji wcześniejszych niż Zabbix 8.0.0;
- Aktualizacja klastra HA zawierająca instrukcje dotyczące aktualizacji serwerów w klastrze **high-availability** (HA).

Przełomowe zmiany Wersje baz danych

Minimalne wymagane wersje baz danych zostały podniesione:

- MySQL/Percona: 8.0.30 → 8.4.0
- MariaDB: 10.5.00 → 10.11.00
- PostgreSQL: 13.0 → 15.0
- TimescaleDB: 2.13.0 → 2.20.0

Wtyczki

Wtyczka Ceph dla Zabbix agent 2 jest teraz ładowalną wtyczką i wymaga dodatkowych kroków instalacyjnych. Szczegółowe informacje można znaleźć w pliku readme wtyczki Ceph.

Schemat `tcp://` jest przestarzały we wtyczce MongoDB, ale pozostaje zachowany ze względu na zgodność wsteczną z istniejącymi konfiguracjami.

Minimalna wymagana wersja PHP

Minimalna wymagana wersja PHP została podniesiona z 8.0.0 do 8.2.0.

Rozszerzona lista UnsafeUserParameters

Znak % został dodany do listy `UnsafeUserParameters` dla Zabbix agent oraz Zabbix agent 2.

Inne Wycofane makra usunięte

Obsługa następujących wbudowanych makr została teraz usunięta:

Usunięte	Użyj zamiast tego
{ACK.DATE}	{EVENT.UPDATE.DATE}
{ACK.MESSAGE}	{EVENT.UPDATE.MESSAGE}
{ACK.TIME}	{EVENT.UPDATE.TIME}
{EVENT.ACK.HISTORY}	{EVENT.UPDATE.HISTORY}
{HOSTNAME<1-9>}	{HOST.HOST}
{IPADDRESS<1-9>}	{HOST.IP}
{PROFILE.*}	{INVENTORY.*}
{TRIGGER.COMMENT}	{TRIGGER.DESCRIPTION}
{TRIGGER.KEY}	{ITEM.KEY}
{STATUS}	{TRIGGER.STATUS}
{USER.ALIAS}	{USER.USERNAME}

Usunięto walidację JSON i XML z pozycji HTTP agent

Walidacja JSON i XML została usunięta z pola *Treść żądania* w pozycjach HTTP agent. Pole nie sprawdza już, czy wartość jest prawidłowym XML lub JSON, a wybranie *Dane XML* jako *Typ treści żądania* nie wymaga już biblioteki libxml2.

Ukryte wyłączone linki w monitorowanych hostach

Wyłączone linki *Graphs*, *Dashboards* i *Web* nie są już wyświetlane na liście monitorowanych hostów.

Typ danych JSON

Zabbix obsługuje teraz JSON jako typ danych dla wartości pozycji. Jeśli używasz TimescaleDB, nowa hypertabela `history_json` (używana do przechowywania wartości JSON) musi zostać skonfigurowana ręcznie. Jeśli używasz Elasticsearch, domyślna wartość parametru konfiguracyjnego serwera Zabbix `HistoryStorageTypes` obejmuje teraz `json`.

Usunięto przycisk opcji w formularzu nowego filtra tagów

Przycisk opcji, który wymagał wyboru między *Wszystkie tagi* a *Lista tagów* podczas tworzenia nowego filtra tagów, został usunięty.

Wartości pozycji wyświetlane jako HTML przy użyciu iframe'ów

Dane pozycji w widżecie Historia pozycji, gdy są wyświetlane jako tekst sformatowany w HTML, są teraz izolowane w iframe'ach.

Template compatibility with Host Wizard

All out-of-the-box templates are now compatible with the Host Wizard. To upgrade them, see Template upgrade.

Uwagi dotyczące aktualizacji dla Zabbix 8.0.x

Ta strona zawiera zbiorcze uwagi dotyczące aktualizacji dla wydań minor głównej wersji Zabbix.

Zobacz także uwagi dotyczące aktualizacji dla głównej wersji.

Uwagi dotyczące aktualizacji dla wersji 8.0.1 Ta wersja nie została jeszcze wydana.

Zmiany w szablonach

Ta strona zawiera listę wszystkich zmian w standardowych szablonach dostarczanych z Zabbix.

Podczas aktualizacji Zabbix istniejące szablony nie są aktualizowane automatycznie, aby uniknąć nadpisania niestandardowych modyfikacji. Aby zaktualizować szablony lub dodać nowe, zobacz Aktualizacja szablonów.

> **Note:**
> Informujemy, że od Zabbix 6.0 wszystkie szablony mają zaktualizowany format, co może mieć wpływ na import szablonów sprzed wersji 6.0. Więcej informacji można znaleźć w sekcji Zmiany w szablonach w wersji 6.0.

Zmiany w 8.0.0

Wymagania

Sprzęt

Pamięć

Zabbix wymaga zarówno pamięci fizycznej, jak i pamięci dyskowej. Wymagana ilość pamięci dyskowej zależy oczywiście od liczby hostów i parametrów, które są monitorowane. Jeśli planujesz przechowywać długą historię monitorowanych parametrów, powinieneś przewidzieć co najmniej kilka gigabajtów, aby mieć wystarczająco dużo miejsca na zapisanie historii w bazie danych. Każdy proces demona Zabbix wymaga kilku połączeń z serwerem bazy danych. Ilość pamięci przydzielonej dla połączenia zależy od konfiguracji silnika bazy danych.

> **Note:**
> Im więcej masz pamięci fizycznej, tym szybciej działa baza danych (a tym samym Zabbix).

CPU

Zabbix, a w szczególności baza danych Zabbix, może wymagać znacznych zasobów CPU w zależności od liczby monitorowanych parametrów i wybranego silnika bazy danych.

Inny sprzęt

Port komunikacji szeregowej oraz szeregowy modem GSM są wymagane do korzystania z obsługi powiadomień SMS w Zabbix. Konwerter USB-do-portu-szeregowego również będzie działać.

Przykłady konfiguracji sprzętowej

Tabela przedstawia przykłady konfiguracji sprzętowej przy założeniu platformy **Linux/BSD/Unix**.

Są to przykłady rozmiaru i konfiguracji sprzętowej na początek. Każda instalacja Zabbix jest unikalna. Przed wdrożeniem instalacji Zabbix do środowiska produkcyjnego należy koniecznie przeprowadzić testy wydajności systemu Zabbix w środowisku testowym lub deweloperskim, aby w pełni zrozumieć swoje wymagania.

Rozmiar instalacji	Monitorowane metryki[1]	Rdzenie CPU/vCPU	Pamięć (GiB)	Baza danych	Amazon EC2[2]
Mała	1 000	2	8	MySQL Server, Percona Server, MariaDB Server, PostgreSQL	m6i.large/m6g.large
Średnia	10 000	4	16	MySQL Server, Percona Server, MariaDB Server, PostgreSQL	m6i.xlarge/m6g.xlarge
Duża	100 000	16	64	MySQL Server, Percona Server, MariaDB Server, PostgreSQL	m6i.4xlarge/m6g.4xlarge
Bardzo duża	1 000 000	32	96	MySQL Server, Percona Server, MariaDB Server, PostgreSQL	m6i.8xlarge/m6g.8xlarge

[1] 1 metryka = 1 pozycja + 1 wyzwalacz + 1 wykres
 [2] Przykład z użyciem instancji Amazon EC2 ogólnego przeznaczenia, z architekturą ARM64 lub x86_64; podczas oceny i testowania instalacji Zabbix, przed wdrożeniem do środowiska produkcyjnego, należy wybrać odpowiedni typ instancji, taki jak zoptymalizowany pod kątem mocy obliczeniowej/pamięci/pamięci masowej.

> **Note:**
> Rzeczywista konfiguracja w dużym stopniu zależy od liczby aktywnych pozycji i częstotliwości odświeżania (szczegóły znajdują się w sekcji rozmiar bazy danych na tej stronie). W przypadku dużych instalacji zdecydowanie zaleca się uruchamianie bazy danych na oddzielnym serwerze.

Obsługiwane platformy

Ze względu na wymagania bezpieczeństwa oraz krytyczny charakter serwera monitoringu, UNIX jest jedynym systemem operacyjnym, który może stale zapewniać wymaganą wydajność, odporność na awarie i niezawodność. Zabbix działa na wiodących na rynku wersjach systemów.

Komponenty Zabbix są dostępne i przetestowane dla następujących platform:

Platforma	Serwer	Agent	Agent 2	Uwagi
Linux	x	x	x	
Windows	-	x	x	Agent Zabbix jest obsługiwany we wszystkich desktopowych i serwerowych wersjach systemu od Windows XP (64-bit)/Server 2003. Agent Zabbix 2 jest obsługiwany we wszystkich desktopowych i serwerowych wersjach systemu od Windows 10 (32-bit)/Server 2016, ponieważ jest kompilowany wyłącznie przy użyciu obsługiwanej wersji Go, aby zapobiec krytycznym lukom bezpieczeństwa. Od Go 1.21 minimalne wymagane wersje Windows zostały podniesione, co sprawia, że Windows 10/Server 2016 jest minimalną wersją dla agenta Zabbix 2.
macOS	x	x	-	
IBM AIX	x	x	-	Agent Zabbix nie działa na platformach AIX w wersjach niższych niż 6.1 TL07 / 7.1 TL01.
FreeBSD	x	x	-	
OpenBSD	x	x	-	
Solaris	x	x	-	
NetBSD	x	x	-	
HP-UX	x	x	-	

Note:
Serwer/agent Zabbix może działać na innych systemach operacyjnych typu Unix.

Attention:
Zabbix wyłącza zrzuty core, jeśli został skompilowany z obsługą szyfrowania, i nie uruchamia się, jeśli system nie pozwala na wyłączenie zrzutów core.

Wymagane oprogramowanie

Zabbix jest oparty na nowoczesnych serwerach WWW, wiodących silnikach baz danych oraz języku skryptowym PHP.

Zewnętrzne oprogramowanie otaczające innych producentów

Jeśli określono jako obowiązkowe, wymagane oprogramowanie/biblioteka jest bezwzględnie konieczne. Opcjonalne składniki są potrzebne do obsługi niektórych określonych funkcji.

Oprogramowanie	Status obowiązkowości	Obsługiwane wersje	Uwagi
MySQL/Percona	Jedno z	8.4.0-9.5.X	Wymagane, jeśli MySQL (lub Percona) jest używane jako baza danych backendowa Zabbix. Wymagany jest silnik InnoDB. Zalecamy użycie biblioteki C API (libmysqlclient) do budowania serwera/proxy.

Oprogramowanie	Status obow-iązkowości	Obsługiwane wersje	Uwagi
MariaDB		10.11.00-12.0.X	Wymagany jest silnik InnoDB. Zalecana wersja to 11.4. Zalecamy użycie biblioteki MariaDB Connector/C do budowania serwera/proxy. Zobacz także: Possible deadlocks with MariaDB oraz Access to UI elements with MariaDB 10.5.1–10.5.9.
PostgreSQL		15.0-18.X	Wymagane, jeśli PostgreSQL jest używany jako baza danych backendowa Zabbix. W zależności od rozmiaru instalacji może być konieczne zwiększenie właściwości konfiguracyjnej PostgreSQL *work_mem* (domyślną wartością jest 4MB), tak aby ilość pamięci używanej przez bazę danych dla konkretnej operacji była wystarczająca, a wykonywanie zapytań nie zajmowało zbyt dużo czasu.
TimescaleDB for PostgreSQL		2.20.X-2.25.X	Wymagane, jeśli TimescaleDB jest używane jako rozszerzenie bazy danych PostgreSQL. Upewnij się, że instalujesz TimescaleDB Community Edition, która obsługuje kompresję. Należy pamiętać, że PostgreSQL 15 jest obsługiwany od TimescaleDB 2.10. Możesz także zapoznać się z TimescaleDB documentation, aby uzyskać szczegółowe informacje dotyczące zgodności wersji PostgreSQL i TimescaleDB.
SQLite	Opcjonalne	3.3.5-3.34.X	SQLite jest obsługiwane tylko z proxy Zabbix. Wymagane, jeśli SQLite jest używane jako baza danych proxy Zabbix.
Elasticsearch		7.X	Elasticsearch jest obsługiwany tylko z serwerami Zabbix, wyłącznie do przechowywania danych historycznych. Obsługa Elasticsearch jest obecnie eksperymentalna. Zobacz także wymagane oprogramowanie dla server/proxy.
smartmontools		7.1 lub nowsza	Wymagane dla Zabbix agent 2.
who			Wymagane dla wtyczki zliczania użytkowników.
dpkg			Wymagane dla wtyczki system.sw.packages.
pkgtool			Wymagane dla wtyczki system.sw.packages.
rpm			Wymagane dla wtyczki system.sw.packages.
pacman			Wymagane dla wtyczki system.sw.packages.
q applets			`qlist` i `qsize`, jako część q applets, są wymagane dla wtyczki system.sw.packages w Gentoo Linux.

Note:
Chociaż Zabbix może działać z bazami danych dostępnymi w systemach operacyjnych, dla uzyskania najlepszych rezultatów zalecamy używanie baz danych zainstalowanych z oficjalnych repozytoriów producentów baz danych.

Frontend

Minimalna obsługiwana szerokość ekranu dla frontend Zabbix wynosi 1200 px.

Jeśli oprogramowanie/biblioteka jest oznaczone jako obowiązkowe, oznacza to, że jest bezwzględnie wymagane. Elementy opcjonalne są potrzebne do obsługi niektórych określonych funkcji.

Oprogramowanie	Status obow-iązkowości	Obsługiwane wersje	Uwagi
PHP	Tak	8.2.0 - 8.4.X	
Apache	Jedno z	2.4 lub nowsza	

Oprogramowanie	Status obowiązkowości	Obsługiwane wersje	Uwagi
Nginx		1.20 lub nowsza	
MySQL	Jedno z	Zobacz Zewnętrzne oprogramowanie innych producentów	
PostgreSQL			
Rozszerzenia PHP			
mysqli	Tak		Wymagane, jeśli MySQL jest używany jako baza danych backend Zabbix.
pgsql			Wymagane, jeśli PostgreSQL jest używany jako baza danych backend Zabbix.
bcmath			php-bcmath (*--enable-bcmath*)
mbstring			php-mbstring (*--enable-mbstring*)
sockets			php-net-socket (*--enable-sockets*); wymagane do obsługi skryptów użytkownika.
gd		2.0.28 lub nowsza	php-gd (jeśli dostarczane jako osobny pakiet przez dystrybutora); rozszerzenie PHP GD musi obsługiwać obrazy PNG (*--with-png-dir*), obrazy JPEG (*--with-jpeg-dir*) oraz FreeType 2 (*--with-freetype-dir*). Wersja 2.3.0 lub nowsza może być wymagana, aby uniknąć możliwego nakładania się tekstu na wykresach w przypadku niektórych języków frontend.
libxml		2.6.15 lub nowsza	php-xml (jeśli dostarczane jako osobny pakiet przez dystrybutora)
xmlwriter			php-xmlwriter (jeśli dostarczane jako osobny pakiet przez dystrybutora)
xmlreader			php-xmlreader (jeśli dostarczane jako osobny pakiet przez dystrybutora)
ctype			php-ctype (*--enable-ctype*)
session			php-session (jeśli dostarczane jako osobny pakiet przez dystrybutora)
ldap	Nie		php-ldap; wymagane do uwierzytelniania LDAP.
openssl			php-openssl; wymagane do uwierzytelniania SAML.
gettext			php-gettext (*--with-gettext*); wymagane do tłumaczeń.
cURL		7.19.4 lub nowsza	php-curl; wymagane dla Duo Universal Prompt MFA oraz uwierzytelniania SMTP.

Biblioteki frontend innych producentów dostarczane z Zabbix:

Biblioteka	Status obowiązkowości	Dostarczana wersja	Uwagi
jQuery JavaScript Library	Tak	3.6.0	Biblioteka JavaScript upraszczająca proces tworzenia aplikacji działających w różnych przeglądarkach.
jQuery UI		1.12.1	Zestaw interakcji interfejsu użytkownika, efektów, widżetów i motywów zbudowanych na bazie jQuery.
SAML PHP Toolkit		4.3.1	Zestaw narzędzi PHP, który dodaje obsługę uwierzytelniania SAML 2.0, umożliwiając logowanie do Zabbix.
Symfony Yaml Component		5.1.0	Dodaje obsługę eksportu i importu elementów konfiguracji Zabbix w formacie YAML.

Note:
Zabbix może działać również z wcześniejszymi wersjami Apache, MySQL i PostgreSQL.

Attention:
W przypadku używania czcionek innych niż domyślna DejaVu może być wymagana funkcja PHP imagerotate. Jeśli jej brakuje, czcionki te mogą być renderowane niepoprawnie podczas wyświetlania wykresu. Ta funkcja jest dostępna tylko wtedy, gdy PHP zostało skompilowane z dołączonym GD, co nie ma miejsca w Debianie i innych dystrybucjach.

Biblioteki innych producentów używane do pisania i debugowania kodu frontend Zabbix:

Biblioteka	Status obowiązkowości	Wersja minimalna	Opis
Composer	Nie	2.4.1	Menedżer pakietów dla PHP na poziomie aplikacji, który zapewnia standardowy format zarządzania zależnościami oprogramowania PHP i wymaganymi bibliotekami.
PHPUnit		8.5.29	Framework do testów jednostkowych PHP służący do testowania frontend Zabbix.
SASS		3.4.22	Język skryptowy preprocesora, który jest interpretowany i kompilowany do kaskadowych arkuszy stylów (CSS).

Przeglądarka internetowa po stronie klienta

Pliki cookie i JavaScript muszą być włączone.

Obsługiwane są najnowsze stabilne wersje Google Chrome, Mozilla Firefox, Microsoft Edge, Apple Safari i Opera.

Warning:
Stosowana jest polityka same-origin dla IFrame, co oznacza, że Zabbix nie może być osadzony w ramkach w innej domenie.

 Jednak strony osadzone w ramce Zabbix będą miały dostęp do frontend Zabbix (przez JavaScript), jeśli strona osadzona w ramce i frontend Zabbix znajdują się w tej samej domenie. Strona taka jak `http://secure-zabbix.com/cms/page.html`, jeśli zostanie umieszczona na pulpitach w `http://secure-zabbix.com/zabbix/`, będzie miała pełny dostęp JS do Zabbix.

Serwer/proxy

Jeśli oznaczono jako obowiązkowe, wymagane oprogramowanie/biblioteka są bezwzględnie niezbędne. Opcjonalne są potrzebne do obsługi niektórych określonych funkcji.

Wymaganie	Status obowiązkowości	Opis
libpcre2	Tak	Biblioteka PCRE2 jest wymagana do obsługi Perl Compatible Regular Expression (PCRE). Obsługiwana jest PCRE2 v10.x.
libevent		Wymagana do komunikacji międzyprocesowej. Wersja 2.0.10 lub nowsza.
libevent-pthreads		Wymagana do komunikacji międzyprocesowej.
libpthread		Wymagana do obsługi mutexów i blokad odczytu-zapisu (może być częścią libc).
libresolv		Wymagana do rozwiązywania nazw DNS (może być częścią libc).
libiconv		Wymagana do kodowania/konwersji formatu tekstu (może być częścią libc). Obowiązkowa dla serwera Zabbix w systemie Linux.
libz		Wymagana do obsługi kompresji.
libm		Biblioteka matematyczna. Wymagana tylko przez serwer Zabbix.
libmysqlclient	Jedna z	Wymagana, jeśli używany jest MySQL.
libmariadb		Wymagana, jeśli używany jest MariaDB.
libpq5		Wymagana, jeśli używany jest PostgreSQL; wersja *libpq5* musi być zgodna z wersją używanej bazy danych PostgreSQL lub wyższa od niej.
libsqlite3		Wymagana, jeśli używany jest SQLite. Wymagana tylko dla Zabbix proxy.
libOpenIPMI	Nie	Wymagana do obsługi IPMI. Wymagana tylko przez serwer Zabbix.
libssh2 lub *libssh*		Wymagana do kontroli SSH. Wersja 1.8.0 lub nowsza (libssh2); 0.9.0 lub nowsza (libssh).

Wymaganie	Status obowiązkowości	Opis
libcurl		Wymagana dla następujących funkcji: - pozycji monitorowania WWW, monitorowania VMware oraz HTTP agent (dla wszystkich: wersja 7.19.1 lub nowsza); - pozycji Zabbix agent web.page.* (wersja 7.19.1 lub nowsza; zobacz także wymagania agent); - uwierzytelniania SMTP (Basic: wersja 7.20.0 lub nowsza; OAuth: wersja 7.33 lub nowsza; zobacz także wymagania frontend); - Elasticsearch (wersja 7.28.0 lub nowsza). Zalecana jest wersja 7.28.0 lub nowsza dla wszystkich funkcji. Aby używać rozszerzonych funkcji cURL dla pozycji `web.page.*`, uruchom ponownie serwer/proxy Zabbix. Do uwierzytelniania SMTP używaj pakietu `libcurl-full` w czasie działania.
libxml2		Wymagana do monitorowania VMware oraz preprocessingu XML XPath.
net-snmp		Wymagana do obsługi SNMP. Wersja 5.3.0 lub nowsza. Obsługa silnych protokołów szyfrowania (AES192/AES192C, AES256/AES256C) jest dostępna od biblioteki net-snmp 5.8; w systemach opartych na RHEL 8+ zaleca się używanie net-snmp 5.8.15 lub nowszej.
libunixodbc		Wymagana do monitorowania baz danych.
libgnutls lub *libopenssl*		Wymagana przy używaniu szyfrowania. Minimalne wersje: *libgnutls* - 3.1.18, *libopenssl* - 1.0.1
libldap		Wymagana do obsługi LDAP.
fping		Wymagana dla pozycji ICMP ping.
c-ares		Wymagana do asynchronicznego rozwiązywania nazw DNS, jeśli Zabbix jest skonfigurowany z opcją `--with-ares`. W przeciwnym razie użyta zostanie *libevent*. Minimalna wersja: 1.16.0. Buforowanie zapytań DNS (pamięć podręczna zapytań domyślnie włączona) wymaga c-ares 1.26.0 lub nowszej.

Agent

Wymaganie	Status obowiązkowy	Opis
libpcre2	Tak	Biblioteka PCRE2 jest wymagana do obsługi Perl Compatible Regular Expression (PCRE). Obsługiwana jest PCRE2 v10.x. Wymagana do monitorowania logów. Wymagana również w systemie Windows.
libpthread		Wymagana do obsługi mutexów oraz blokad odczytu-zapisu (może być częścią libc). Niewymagana w systemie Windows.
libresolv		Wymagana do rozwiązywania nazw DNS (może być częścią libc). Niewymagana w systemie Windows.
libiconv		Wymagana do kodowania/konwersji formatu tekstu do UTF-8 w pozycjach logów, zawartości plików, file regex oraz regmatch (może być częścią libc). Niewymagana w systemie Windows.
libgnutls lub *libopenssl*	Nie	Wymagane w przypadku korzystania z szyfrowania. Minimalne wersje: *libgnutls* - 3.1.18, *libopenssl* - 1.0.1 W systemie Microsoft Windows wymagany jest OpenSSL 1.1.1 lub nowszy.
libldap		Wymagana, jeśli używany jest LDAP. Nieobsługiwana w systemie Windows.
libcurl		Wymagana do rozszerzonej obsługi pozycji web.page.* w Zabbix agent. Bez libcurl dostępna jest podstawowa funkcjonalność (np. web.page.get[http://example.com]). Z libcurl agent obsługuje dodatkowe funkcje, takie jak adresy URL HTTP z poświadczeniami (np. http://user:password@example.com) oraz adresy URL HTTPS. Wymagana jest wersja 7.19.1 lub nowsza (zalecana jest wersja 7.28.0 lub nowsza). Aby używać rozszerzonych funkcji cURL, uruchom ponownie Zabbix agent.
libmodbus		Wymagana tylko w przypadku korzystania z monitorowania Modbus. Wersja 3.0 lub nowsza.

Agent 2

Wymaganie	Status obow-iązkowy	Opis
Go	Tak	Wymagane do budowania Zabbix agent 2 i jego wtyczek ze źródeł. Obsługiwane jest Go 1.24.10 lub nowsze. Instrukcje instalacji znajdują się na go.dev. Biblioteki Go używane przez Zabbix agent 2 i jego wtyczki są wymienione w repozytorium Git Zabbix (biblioteki oznaczone w repozytorium jako `indirect` są zależnościami innych wymaganych bibliotek): - Zabbix agent 2 - Obsługa wtyczek - PostgreSQL - MongoDB - MSSQL - Ember+ - NVIDIA GPU - Przykładowa wtyczka
libpcre2	Tak	Biblioteka PCRE2 jest wymagana do obsługi wyrażeń regularnych zgodnych z Perlem (PCRE). Obsługiwane jest PCRE2 v10.x. Wymagane do monitorowania logów. Wymagane również w systemie Windows.
libopenssl	Nie	Wymagane przy używaniu szyfrowania. Na platformach UNIX wymagany jest OpenSSL 1.0.1 lub nowszy. Biblioteka OpenSSL musi mieć włączoną obsługę PSK. LibreSSL nie jest obsługiwany. W systemach Microsoft Windows wymagany jest OpenSSL 1.1.1 lub nowszy.

Usługa web

Najnowsza stabilna wersja Google Chrome jest obsługiwana do generowania zaplanowanych raportów przy użyciu usługi web Zabbix.

Wymagana wersja Go do budowania usługi web jest taka sama jak ta używana dla Zabbix agent 2.

Java gateway

Jeśli Zabbix został pozyskany z repozytorium kodu źródłowego lub z archiwum, wszystkie niezbędne zależności są już zawarte w drzewie źródeł.

Jeśli Zabbix został pozyskany z pakietu dostarczanego przez dystrybucję, wszystkie niezbędne zależności są już zapewniane przez system pakietów.

W obu powyższych przypadkach oprogramowanie jest gotowe do użycia i nie są wymagane żadne dodatkowe pliki do pobrania.

Jeśli jednak chcesz dostarczyć własne wersje tych zależności (na przykład podczas przygotowywania pakietu dla jakiejś dystrybucji Linuksa), poniżej znajduje się lista wersji bibliotek, z którymi Java gateway działa poprawnie. Zabbix może również działać z innymi wersjami tych bibliotek.

Poniższa tabela zawiera listę plików JAR, które są obecnie dołączane do Java gateway w oryginalnym kodzie:

Library	Mandatory status	Bundled version	Comments
android-json	Tak	4.3r1	JSON (JavaScript Object Notation) to lekki format wymiany danych. Jest to zgodna z org.json implementacja Androida wyodrębniona z Android SDK.
logback-classic		1.5.16	
logback-core		1.5.16	
slf4j-api		2.0.16	

Java gateway można zbudować przy użyciu zarówno Oracle Java, jak i otwartego OpenJDK (wersja 1.6 lub nowsza). Pakiety dostarczane przez Zabbix są kompilowane przy użyciu OpenJDK. Poniższa tabela zawiera listę pakietów OpenJDK używanych do budowania pakietów Zabbix dla poszczególnych dystrybucji:

Distribution	OpenJDK package
AlmaLinux 9	`java-11-openjdk-devel` (amd64: 11.0.19.0.7-4; arm64: 11.0.20.0.8-3)
AlmaLinux 8	`java-1.8.0-openjdk-devel` (amd64: 1.8.0.332.b09-2; arm64: 1.8.0.382.b05-2)
Amazon Linux 2023	`java-22-amazon-corretto-devel` (amd64, arm64: 22.0.2+9-1)
CentOS Stream 9	`java-11-openjdk-devel` (amd64, arm64: 11.0.18.0.10-3)
CentOS Stream 8	`java-1.8.0-openjdk-devel` (amd64, arm64: 1.8.0.362.b08-3)
CentOS 7	`java-1.8.0-openjdk-devel` (amd64: 1.8.0.282.b08-1)
Debian 12	`default-jdk-headless` (amd64, arm64: 2:1.17-74)
Debian 11	`default-jdk-headless` (amd64: 2:1.11-72)
OpenSUSE Leap 15	`java-17-openjdk-devel` (amd64: 17.0.5.0-150400.3.9.3; arm64: 17.0.8.0-150400.3.27.1)
Oracle Linux 9	`java-11-openjdk-devel` (amd64: 11.0.19.0.7-4.0.1; arm64: 11.0.20.0.8-2.0.1)
Oracle Linux 8	`java-1.8.0-openjdk-devel` (amd64: 1.8.0.372.b07-4.0.1); `java-11-openjdk-devel` (arm64: 11.0.20.0.8-3.0.1)
Oracle Linux 7	`java-1.8.0-openjdk-devel` (amd64: 1.8.0.282.b08-1)
Raspberry Pi OS 12	`default-jdk-headless` (arm64, armhf: 2:1.17-74)
Raspberry Pi OS 11	`default-jdk-headless` (arm64: 2:1.11-72; armhf: 2:1.11-72+b4)
RHEL 9	`java-11-openjdk-devel` (amd64: 11.0.19.0.7-4; arm64: 11.0.20.0.8-3)
RHEL 8	`java-1.8.0-openjdk-devel` (amd64: 1.8.0.372.b07-4; arm64: 1.8.0.382.b05-2)
RHEL 7	`java-1.8.0-openjdk-devel` (amd64: 1.8.0.282.b08-1)
Rocky Linux 9	`java-11-openjdk-devel` (amd64: 11.0.19.0.7-4; arm64: 11.0.20.0.8-3)
Rocky Linux 8	`java-1.8.0-openjdk-devel` (amd64: 1.8.0.372.b07-4; arm64: 1.8.0.382.b05-2)
SLES 15	`java-17-openjdk-devel` (amd64: 17.0.5.0-150400.3.9.3; arm64: 17.0.8.0-150400.3.27.1)
Ubuntu 24.04	`default-jdk-headless` (amd64, arm64: 2:1.21-75+exp1)
Ubuntu 22.04	`default-jdk-headless` (amd64, arm64: 2:1.11-72build2)
Ubuntu 20.04	`default-jdk-headless` (amd64, arm64: 2:1.11-72)

Domyślne numery portów

Poniższa lista otwartych portów dla poszczególnych komponentów ma zastosowanie do konfiguracji domyślnej:

Komponent Zabbix	Numer portu	Protokół	Typ połączenia
Zabbix agent	10050	TCP	na żądanie
Zabbix agent 2	10050	TCP	na żądanie
Zabbix serwer	10051	TCP	na żądanie
Zabbix proxy	10051	TCP	na żądanie
Zabbix Java gateway	10052	TCP	na żądanie
Usługa internetowa Zabbix	10053	TCP	na żądanie
Zabbix frontend	80	HTTP	na żądanie
	443	HTTPS	na żądanie
Zabbix trapper	10051	TCP	na żądanie

Note:
Numery portów powinny być otwarte w zaporze sieciowej, aby umożliwić komunikację Zabbix. Wychodzące połączenia TCP zwykle nie wymagają jawnych ustawień zapory sieciowej.

Rozmiar bazy danych

Dane konfiguracyjne Zabbix wymagają stałej ilości miejsca na dysku i nie zwiększają się znacząco.

Rozmiar bazy danych Zabbix zależy głównie od następujących zmiennych, które określają ilość przechowywanych danych historycznych:

- Liczba przetwarzanych wartości na sekundę

Jest to średnia liczba nowych wartości, które serwer Zabbix otrzymuje co sekundę. Na przykład, jeśli mamy 3000 pozycji do monitorowania z interwałem odświeżania 60 sekund, liczba wartości na sekundę jest obliczana jako 3000/60 = **50**.

Oznacza to, że co sekundę do bazy danych Zabbix dodawanych jest 50 nowych wartości.

- Ustawienia housekeepera dla historii

Zabbix przechowuje wartości przez stały okres czasu, zwykle kilka tygodni lub miesięcy. Każda nowa wartość wymaga określonej ilości miejsca na dysku na dane i indeks.

Jeśli więc chcemy przechowywać historię przez 30 dni i otrzymujemy 50 wartości na sekundę, całkowita liczba wartości wyniesie około (**30***24*3600)* **50** = 129.600.000, czyli około 130 mln wartości.

W zależności od używanego silnika bazy danych oraz typu otrzymywanych wartości (liczby zmiennoprzecinkowe, liczby całkowite, ciągi znaków, pliki logów itp.), ilość miejsca na dysku potrzebna do przechowywania pojedynczej wartości może wynosić od 40 bajtów do setek bajtów. Zwykle dla numerycznych pozycji jest to około 90 bajtów na wartość[2]. W naszym przypadku oznacza to, że 130 mln wartości będzie wymagać 130 mln * 90 bajtów = **10.9GB** miejsca na dysku.

Note:
Rozmiaru wartości tekstowych/logów dla pozycji nie da się dokładnie przewidzieć, ale można przyjąć około 500 bajtów na wartość.

- Ustawienie housekeepera dla trendów

Zabbix przechowuje 1-godzinny zestaw wartości maks./min./śr./liczba dla każdej pozycji w tabeli **trends**. Dane te są używane do analizy trendów i wykresów długookresowych. Okres jednej godziny nie może być dostosowany.

Baza danych Zabbix, w zależności od typu bazy danych, wymaga około 90 bajtów dla każdego takiego zestawu. Załóżmy, że chcemy przechowywać dane trendów przez 5 lat. Wartości dla 3000 pozycji będą wymagać 3000*24*365* **90** = **2.2GB** rocznie, czyli **11GB** przez 5 lat.

- Ustawienia housekeepera dla zdarzeń

Każde zdarzenie Zabbix wymaga około 250 bajtów miejsca na dysku[1]. Trudno oszacować liczbę zdarzeń generowanych codziennie przez Zabbix. W najgorszym przypadku można założyć, że Zabbix generuje jedno zdarzenie na sekundę.

Dla każdego odzyskanego zdarzenia tworzony jest rekord event_recovery. Zwykle większość zdarzeń zostanie odzyskana, więc można założyć jeden rekord event_recovery na zdarzenie. Oznacza to dodatkowe 80 bajtów na zdarzenie.

Opcjonalnie zdarzenia mogą mieć tagi, przy czym każdy rekord tagu wymaga około 100 bajtów miejsca na dysku[1]. Liczba tagów na zdarzenie (#tags) zależy od konfiguracji. Każde zdarzenie będzie więc wymagać dodatkowo #tags * 100 bajtów miejsca na dysku.

Oznacza to, że jeśli chcemy przechowywać zdarzenia przez 3 lata, będzie to wymagać 3*365*24*3600* (250+80+#tags*100) = **~30GB**+#tags*100B miejsca na dysku[2].

Note:
[1] Więcej w przypadku nazw zdarzeń, tagów i wartości zawierających znaki spoza ASCII.
 [2] Przybliżenia rozmiaru opierają się na MySQL i mogą się różnić w przypadku innych baz danych.

Tabela zawiera wzory, które można wykorzystać do obliczenia ilości miejsca na dysku wymaganego przez system Zabbix:

Parametr	Wzór na wymagane miejsce na dysku (w bajtach)
Konfiguracja Zabbix	Stały rozmiar. Zwykle 10MB lub mniej.
Historia	days*(items/refresh rate)*24*3600*bytes items : liczba pozycji days : liczba dni przechowywania historii refresh rate : średni interwał odświeżania pozycji bytes : liczba bajtów wymagana do przechowywania pojedynczej wartości, zależy od silnika bazy danych, zwykle ~90 bajtów.
Trendy	days*(items/3600)*24*3600*bytes items : liczba pozycji days : liczba dni przechowywania historii bytes : liczba bajtów wymagana do przechowywania pojedynczego trendu, zależy od silnika bazy danych, zwykle ~90 bajtów.
Zdarzenia	days*events*24*3600*bytes events : liczba zdarzeń na sekundę. Jedno (1) zdarzenie na sekundę w najgorszym przypadku. days : liczba dni przechowywania historii bytes : liczba bajtów wymagana do przechowywania pojedynczego zdarzenia, zależy od silnika bazy danych, zwykle ~330 + średnia liczba tagów na zdarzenie * 100 bajtów.

Całkowite wymagane miejsce na dysku można więc obliczyć jako:

Konfiguracja + Historia + Trendy + Zdarzenia

Miejsce na dysku NIE zostanie wykorzystane natychmiast po instalacji Zabbix. Rozmiar bazy danych będzie rósł, a następnie w pewnym momencie przestanie się zwiększać, w zależności od ustawień housekeepera.

Synchronizacja czasu

Bardzo ważne jest, aby na serwerze, na którym działa Zabbix, czas systemowy był precyzyjnie ustawiony. ntpd to najpopularniejszy demon synchronizujący czas hosta z czasem innych maszyn. Zdecydowanie zaleca się utrzymywanie zsynchronizowanego czasu systemowego na wszystkich systemach, na których działają komponenty Zabbix.

Wymagania sieciowe

Poniższa lista otwartych portów dla poszczególnych komponentów ma zastosowanie do konfiguracji domyślnej.

Components	Port
Frontend	http na 80, https na 443
Server	10051 (do użycia z aktywnym proxy/agentami)
Active Proxy	10051
Passive Proxy	10051
Agent2	10050
Trapper	
JavaGateway	10052
WebService	10053

Note:
Numery portów powinny być otwarte w zaporze sieciowej, aby umożliwić zewnętrzną komunikację z Zabbix. Wychodzące połączenia TCP zwykle nie wymagają jawnych ustawień zapory sieciowej.

Znane problemy

Zobacz także: Problemy z kompilacją.

Aktualizacja

Ustawienie trybu SQL dla pomyślnej aktualizacji

Ustawienie `sql_mode` w MySQL/MariaDB musi mieć ustawiony tryb "STRICT_TRANS_TABLES". Jeśli go brakuje, aktualizacja bazy danych Zabbix zakończy się niepowodzeniem (zobacz także ZBX-19435).

Aktualizacja z MariaDB 10.2.1 i wcześniejszą

Aktualizacja Zabbix może się nie powieść, jeśli tabele bazy danych zostały utworzone przy użyciu MariaDB 10.2.1 lub wcześniejszej, ponieważ w tych wersjach domyślny format wiersza to compact. Można to naprawić, zmieniając format wiersza na dynamic (zobacz także ZBX-17690).

Szablony

Zgodność szablonów w środowiskach dual-stack (IPv4/IPv6)

W środowiskach dual-stack (systemach skonfigurowanych do obsługi zarówno IPv4, jak i IPv6) nazwa hosta `localhost` zwykle jest rozwiązywana zarówno do adresów IPv4, jak i IPv6. Ze względu na częste priorytetyzowanie IPv6 względem IPv4 przez wiele systemów operacyjnych i resolverów DNS, szablony Zabbix mogą nie działać poprawnie, jeśli monitorowana usługa jest skonfigurowana do nasłuchiwania wyłącznie na IPv4.

Usługi, które nie są skonfigurowane do nasłuchiwania na adresach IPv6, mogą stać się niedostępne, co prowadzi do niepowodzeń monitorowania. Użytkownicy mogą poprawnie skonfigurować dostęp dla IPv4, a mimo to nadal napotykać problemy z łącznością z powodu domyślnego zachowania polegającego na priorytetyzowaniu IPv6.

Obejściem tego problemu jest upewnienie się, że usługi (Nginx, Apache, PostgreSQL itp.) są skonfigurowane do nasłuchiwania zarówno na adresach IPv4, jak i IPv6, a serwer/agent Zabbix ma dozwolony dostęp przez IPv6. Dodatkowo w szablonach i konfiguracjach Zabbix należy jawnie używać `localhost` zamiast `127.0.0.1`, aby zapewnić zgodność zarówno z IPv4, jak i IPv6.

Na przykład, podczas monitorowania PostgreSQL za pomocą szablonu PostgreSQL by Zabbix agent 2, może być konieczna edycja pliku `pg_hba.conf`, aby zezwolić na połączenia dla użytkownika `zbx_monitor`. Jeśli środowisko dual-stack nadaje priorytet

IPv6 (system rozwiązuje localhost do `::1`) i skonfigurujesz `localhost`, ale dodasz tylko wpis IPv4 (`127.0.0.1/32`), połączenie zakończy się niepowodzeniem, ponieważ nie ma pasującego wpisu IPv6.

Poniższy przykład pliku `pg_hba.conf` zapewnia, że użytkownik `zbx_monitor` może łączyć się z dowolną bazą danych z lokalnej maszyny przy użyciu zarówno adresów IPv4, jak i IPv6, z różnymi metodami uwierzytelniania:

```
### TYPE     DATABASE     USER            ADDRESS          METHOD
  host     all          zbx_monitor     localhost        trust
  host     all          zbx_monitor     127.0.0.1/32     md5
  host     all          zbx_monitor     ::1/128          scram-sha-256
```

W razie potrzeby można również użyć bezpośrednio adresu IPv4 (`127.0.0.1`) podczas konfigurowania makra szablonu PostgreSQL by Zabbix agent 2 dla ciągu połączenia.

Przypadkowa instalacja pakietów Zabbix z EPEL

Jeśli repozytorium EPEL jest zainstalowane i włączone, instalacja pakietów Zabbix może spowodować pobranie wersji z EPEL zamiast oficjalnych pakietów Zabbix. Aby rozwiązać ten problem:

1. Usuń wszystkie pakiety Zabbix zainstalowane z EPEL:

```
dnf remove zabbix-server-mysql
```

2. Wyklucz pakiety Zabbix z EPEL, dodając następujący wiersz do pliku `/etc/yum.repos.d/epel.repo`:

```
[epel]
...
excludepkgs=zabbix*
```

3. Zainstaluj ponownie oficjalny pakiet serwera Zabbix:

```
dnf install zabbix-server-mysql
```

Podczas instalacji oficjalne pakiety Zabbix zawierają słowo `release` w ciągu wersji (na przykład `7.0.0-release1.el8`), co odróżnia je od pakietów EPEL.

Pakiety Zabbix dla RHEL w środowiskach Red Hat UBI

Podczas instalacji Zabbix z pakietów Red Hat Enterprise Linux w środowiskach Red Hat Universal Base Image należy zapewnić dostęp do wymaganych repozytoriów i zależności. Pakiety Zabbix zależą od bibliotek `libOpenIPMI.so` i `libOpenIPMIposix.so`, które nie są dostarczane przez żaden pakiet w domyślnych repozytoriach menedżera pakietów włączonych w systemach UBI, co spowoduje niepowodzenie instalacji.

Biblioteki `libOpenIPMI.so` i `libOpenIPMIposix.so` są dostępne w pakiecie `OpenIPMI-libs`, który jest udostępniany przez repozytorium `redhat-#-for-<arch>-appstream-rpms`. Dostęp do tego repozytorium jest regulowany przez subskrypcje, które w przypadku środowisk UBI są propagowane przez montowanie katalogów konfiguracji repozytoriów i sekretów hosta RHEL do przestrzeni nazw systemu plików kontenera.

Aby uzyskać więcej informacji, zobacz ZBX-24291.

Wygasły klucz podpisujący dla pakietów RHEL

Podczas aktualizacji Zabbix w systemie Red Hat Enterprise Linux lub jego pochodnych możesz napotkać problem z wygasłym kluczem podpisującym pakiety w repozytorium Zabbix. Gdy klucz podpisujący wygaśnie, próby weryfikacji podpisów pakietów zakończą się błędem wskazującym, że certyfikat lub klucz nie jest już ważny. Na przykład:

```
error: Verifying a signature using certificate D9AA84C2B617479C6E4FCF4D19F2475308EFA7DD (Zabbix LLC (Jul 2
  1. Certificate 19F2475308EFA7DD invalid: certificate is not alive
      because: The primary key is not live
      because: Expired on 2024-07-04T11:41:23Z
  2. Key 19F2475308EFA7DD invalid: key is not alive
      because: The primary key is not live
      because: Expired on 2024-07-04T11:41:23Z
```

Aby rozwiązać taki problem, ręcznie zainstaluj ponownie najnowszy pakiet `zabbix-release` dla konkretnego wariantu RHEL (zastąp poniższy link właściwym linkiem z repozytorium Zabbix).

Na przykład w systemie **RHEL 10** uruchom:

```
rpm -Uvh https://repo.zabbix.com/zabbix/8.0/release/rhel/10/noarch/zabbix-release-latest.el10.noarch.rpm
```

Następnie zaktualizuj informacje o repozytorium:

```
dnf update
```

Więcej informacji znajdziesz w ZBX-24761.

Timescale DB: wysokie użycie pamięci przy dużej liczbie partycji

Wersje PostgreSQL 9.6-12 zużywają zbyt dużo pamięci podczas aktualizacji tabel z dużą liczbą partycji. Problem ten ujawnia się, gdy Zabbix aktualizuje trendy w systemach z TimescaleDB, jeśli trendy są podzielone na relatywnie małe fragmenty (np. 1 dzień). Prowadzi to do obecności setek fragmentów w tabelach trendów przy domyślnych ustawieniach housekeeping — jest to sytuacja, w której PostgreSQL może najprawdopodobniej wyczerpać pamięć.

Problem został rozwiązany od Zabbix 5.0.1 dla nowych instalacji z TimescaleDB, ale jeśli TimescaleDB skonfigurowano z Zabbix wcześniej, zapoznaj się z ZBX-16347, aby sprawdzić uwagi dotyczące migracji.

Timescale DB 2.5.0: polityka kompresji może zakończyć się niepowodzeniem w tabelach zawierających liczby całkowite

Problem ten występuje podczas używania TimescaleDB 2.5.0/2.5.1. Został on rozwiązany od TimescaleDB 2.5.2.

Aby uzyskać więcej informacji, zobacz TimescaleDB Issue #3773.

Połączenie TLS z bazą danych przy użyciu MariaDB

Połączenie TLS z bazą danych nie jest obsługiwane z opcją 'verify_ca' dla parametru DBTLSConnect, jeśli używana jest MariaDB.

Możliwe zakleszczenia z MySQL/MariaDB

Podczas pracy pod dużym obciążeniem, gdy zaangażowany jest więcej niż jeden worker LLD, może dojść do zakleszczenia spowodowanego błędem InnoDB związanym ze strategią blokowania wierszy (zobacz błąd upstream). Błąd został naprawiony w MySQL od wersji 8.0.29, ale nie w MariaDB. Więcej informacji można znaleźć w ZBX-21506.

Globalna korelacja zdarzeń

Zdarzenia mogą nie zostać skorelowane poprawnie, jeśli odstęp czasu między pierwszym a drugim zdarzeniem jest bardzo mały, tj. pół sekundy lub mniej.

NetBSD 8.0 i nowsze

Różne procesy Zabbix mogą losowo ulegać awarii podczas uruchamiania w wersjach NetBSD 8.X i 9.X. Jest to spowodowane zbyt małym domyślnym rozmiarem stosu (4 MB), który należy zwiększyć, uruchamiając:

```
ulimit -s 10240
```

Aby uzyskać więcej informacji, zobacz powiązane zgłoszenie problemu: ZBX-18275.

Ograniczenia wyrażeń regularnych w Zabbix agent 2

Zabbix agent 2 nie obsługuje asercji lookahead i lookbehind w wyrażeniach regularnych ze względu na ograniczenia standardowej biblioteki Go regexp.

Kontrole IPMI

Kontrole IPMI nie będą działać ze standardowym pakietem biblioteki OpenIPMI w Debianie wcześniejszym niż 9 (stretch) oraz Ubuntu wcześniejszym niż 16.04 (xenial). Aby to naprawić, należy ponownie skompilować bibliotekę OpenIPMI z włączoną obsługą OpenSSL, jak omówiono w ZBX-6139.

IPMI — niezaufane hosty mogą powodować awarię OpenIPMI

W bibliotece OpenIPMI używanej przez Zabbix do odpytywania danych IPMI występuje błąd, który może zostać wywołany przez specjalnie spreparowane odpowiedzi z niezaufanego urządzenia.
Niezaufane urządzenie IPMI może wysyłać spreparowane dane, które powodują awarię biblioteki OpenIPMI, co z kolei może doprowadzić do zakończenia procesu serwera Zabbix wykonującego odpytywanie IPMI.

Kontrole SSH

- Niektóre dystrybucje Linuksa, takie jak Debian i Ubuntu, nie obsługują zaszyfrowanych kluczy prywatnych (z hasłem) w przypadku, gdy biblioteka libssh2 jest zainstalowana z pakietów. Więcej informacji znajduje się w ZBX-4850.
- W przypadku używania libssh 0.9.x w niektórych dystrybucjach Linuksa z OpenSSH 8, kontrole SSH mogą sporadycznie zgłaszać błąd „Cannot read data from SSH server". Jest to spowodowane problemem w libssh (bardziej szczegółowy raport). Oczekuje się, że błąd został naprawiony w stabilnym wydaniu libssh 0.9.5. Szczegóły znajdują się także w ZBX-17756.
- Użycie znaku potoku „|" w skrypcie SSH może prowadzić do błędu „Cannot read data from SSH server". W takim przypadku zaleca się aktualizację wersji biblioteki libssh. Szczegóły znajdują się także w ZBX-21337.

Kontrole ODBC

- Sterownik MySQL unixODBC nie powinien być używany z serwerem Zabbix ani proxy Zabbix skompilowanymi z biblioteką łącznika MariaDB i odwrotnie; jeśli to możliwe, lepiej również unikać używania tego samego łącznika co sterownika ze względu na błąd po stronie projektu upstream. Zalecana konfiguracja:

Łącznik PostgreSQL, SQLite lub Oracle → sterownik MariaDB lub MySQL unixODBC Łącznik MariaDB → sterownik MariaDB unixODBC Łącznik MySQL → sterownik MySQL unixODBC

Więcej informacji oraz dostępne obejścia można znaleźć w ZBX-7665.

- Dane XML pobierane z Microsoft SQL Server mogą być obcinane na różne sposoby w systemach Linux i UNIX.
- Zaobserwowano, że używanie kontroli ODBC do monitorowania baz danych Oracle przy użyciu różnych wersji Oracle Instant Client dla systemu Linux powoduje awarie serwera Zabbix. Zobacz także: ZBX-18402, ZBX-20803.
- W przypadku używania sterownika FreeTDS UnixODBC należy dodać na początku zapytania SQL instrukcję 'SET NOCOUNT ON' (na przykład `SET NOCOUNT ON DECLARE @strsql NVARCHAR(max) SET @strsql = ....`). W przeciwnym razie pozycja monitorowania bazy danych w Zabbix nie będzie mogła pobrać informacji i zwróci błąd "Zapytanie SQL zwróciło pusty wynik".
  Więcej informacji można znaleźć w ZBX-19917.

Nieprawidłowy parametr metody żądania w pozycjach

Parametr metody żądania, używany wyłącznie w kontrolach HTTP, może być nieprawidłowo ustawiony na „1", czyli wartość inną niż domyślna dla wszystkich pozycji, w wyniku aktualizacji z wersji Zabbix starszej niż 4.0. Szczegółowe informacje o tym, jak naprawić tę sytuację, można znaleźć w ZBX-19308.

Monitorowanie WWW i agent HTTP

Serwer Zabbix powoduje wyciek pamięci w niektórych dystrybucjach Linuksa z powodu błędu upstream, gdy opcja „SSL verify peer" jest włączona w scenariuszach WWW lub w agencie HTTP. Więcej informacji oraz dostępne obejścia problemu można znaleźć w ZBX-10486.

Proste testy

W wersjach **fping** wcześniejszych niż v3.10 występuje błąd powodujący nieprawidłową obsługę zduplikowanych pakietów odpowiedzi echo. Może to powodować nieoczekiwane wyniki dla pozycji `icmpping`, `icmppingloss`, `icmppingsec`. Zaleca się używanie najnowszej wersji **fping**. Więcej szczegółów można znaleźć w ZBX-11726.

Błędy wykonywania fping w kontenerach rootless

Gdy kontenery działają w trybie rootless lub w środowisku z określonymi ograniczeniami, podczas wykonywania kontroli ICMP mogą wystąpić błędy związane z uruchamianiem fping, takie jak `fping: Operation not permitted` lub utrata wszystkich pakietów do wszystkich zasobów.

Aby rozwiązać ten problem, dodaj `--cap-add=net_raw` do poleceń "docker run" lub "podman run".

Dodatkowo uruchamianie fping w środowiskach bez uprawnień roota może wymagać modyfikacji sysctl, tj.:

```
sudo sysctl -w "net.ipv4.ping_group_range=0 1995"
```

gdzie "1995" to GID użytkownika zabbix. Więcej informacji można znaleźć w ZBX-22833.

Kontrole SNMP

Jeśli używany jest system operacyjny OpenBSD, błąd use-after-free w bibliotece Net-SNMP do wersji 5.7.3 może spowodować awarię serwera Zabbix, jeśli parametr SourceIP jest ustawiony w pliku konfiguracyjnym serwera Zabbix. Jako obejście problemu nie należy ustawiać parametru SourceIP. Ten sam problem dotyczy również systemu Linux, ale nie powoduje zatrzymania pracy serwera Zabbix. Lokalna poprawka dla pakietu net-snmp w OpenBSD została zastosowana i zostanie wydana wraz z OpenBSD 6.3.

Skoki danych SNMP

Zaobserwowano skoki danych SNMP, które mogą być związane z pewnymi czynnikami fizycznymi, takimi jak skoki napięcia w sieci elektrycznej. Więcej szczegółów znajduje się w ZBX-14318.

Pułapki SNMP

Pakiet "net-snmp-perl", wymagany do obsługi pułapek SNMP, został usunięty w RHEL 8.0-8.2; ponownie dodany w RHEL 8.3.

Jeśli więc używasz RHEL 8.0-8.2, najlepszym rozwiązaniem jest aktualizacja do RHEL 8.3.

Aby uzyskać więcej informacji, zobacz także ZBX-17192.

Awaria procesu alerter w RHEL 7

W RHEL 7 odnotowano przypadki awarii procesu alerter serwera Zabbix. Szczegółowe informacje znajdują się w ZBX-10461.

Aktualizacja Zabbix agent 2 (6.0.5 lub starszy)

Podczas aktualizacji Zabbix agent 2 (wersja 6.0.5 lub starsza) z pakietów może wystąpić błąd konfliktu plików związany z wtyczkami. Aby naprawić ten błąd, wykonaj kopię zapasową konfiguracji agent 2 (jeśli to konieczne), odinstaluj agent 2 i zainstaluj go ponownie.

W systemach opartych na RHEL uruchom:

```
dnf remove zabbix-agent2
dnf install zabbix-agent2
```

W systemach opartych na Debian uruchom:

```
apt remove zabbix-agent2
apt install zabbix-agent2
```

Aby uzyskać więcej informacji, zobacz ZBX-23250.

Przełączanie ustawień regionalnych frontend

Zaobserwowano, że ustawienia regionalne frontend mogą zmieniać się bez wyraźnej logiki, tzn. niektóre strony (lub części stron) są wyświetlane w jednym języku, podczas gdy inne strony (lub części stron) w innym języku. Zwykle problem może wystąpić, gdy jest kilku użytkowników, z których część używa jednych ustawień regionalnych, a pozostali innych.

Znanym obejściem tego problemu jest wyłączenie wielowątkowości w PHP i Apache.

Problem jest związany ze sposobem działania ustawiania locale w PHP: informacje o locale są utrzymywane na poziomie procesu, a nie wątku. Dlatego w środowisku wielowątkowym, gdy kilka projektów jest uruchamianych przez ten sam proces Apache, możliwe jest, że locale zostanie zmienione w innym wątku, co wpływa na sposób przetwarzania danych w wątku Zabbix.

Więcej informacji można znaleźć w powiązanych zgłoszeniach problemów:

- ZBX-10911 (Problem z przełączaniem ustawień regionalnych frontend)
- ZBX-16297 (Problem z przetwarzaniem liczb na wykresach przy użyciu funkcji `bcdiv` z zestawu funkcji BC Math)

Wykresy

Problemy z wykresami (klasycznymi)

Jeśli napotkasz problemy z klasycznymi wykresami, zaleca się aktualizację biblioteki GD (libgd) do wersji 2.3.3-13 lub nowszej oraz PHP do wersji 8.0.19, 8.1.33, 8.2.29, 8.3.25, 8.4.12 lub nowszej.

Czas letni

Zmiany związane z czasem letnim (DST) powodują nieprawidłowości podczas wyświetlania etykiet osi X (duplikacja dat, brak dat itp.).

Agregacja sumy

W przypadku użycia agregacji sumy na wykresie dla okresu krótszego niż jedna godzina, wykresy wyświetlają nieprawidłowe (pomnożone) wartości, gdy dane pochodzą z trendów.

Nakładanie się tekstu

W przypadku niektórych języków frontendu (np. japońskiego) lokalne czcionki mogą powodować nakładanie się tekstu w legendzie wykresu. Aby tego uniknąć, użyj PHP GD extension w wersji 2.3.0 (lub nowszej).

Monitorowanie plików dziennika

Pozycje `log[]` i `logrt[]` wielokrotnie odczytują ponownie plik dziennika od początku, jeśli system plików jest zapełniony w 100% i do pliku dziennika są dopisywane nowe dane (więcej informacji można znaleźć w ZBX-10884).

Wolne zapytania MySQL

Serwer Zabbix generuje wolne zapytania `SELECT` w przypadku nieistniejących wartości dla pozycji. Ten problem występuje w wersjach MySQL 5.6/5.7 (szersze omówienie znajduje się w ZBX-10652) i w określonych przypadkach może również występować w nowszych wersjach MySQL. Obejściem tego problemu jest wyłączenie optymalizatora `index_condition_pushdown` lub `prefer_ordering_index` w MySQL. Należy jednak pamiętać, że to obejście może nie rozwiązać wszystkich problemów związanych z wolnymi zapytaniami.

Trwałe ustawienia filtra z linków

Po otwarciu linku do strony Zabbix frontend, który zawiera ustawienia filtra, w tym selektor czasu, filtr jest automatycznie zapisywany w bazie danych dla użytkownika, zastępując wcześniej zapisany filtr i/lub ustawienia selektora czasu dla tej strony. Ustawienia te pozostają aktywne, dopóki użytkownik nie zaktualizuje ich ręcznie lub nie zresetuje.

Problem z adresem IPv6 w pułapkach SNMPv3

Z powodu błędu net-snmp adres IPv6 może nie być poprawnie wyświetlany podczas używania SNMPv3 w pułapkach SNMP. Więcej szczegółów oraz możliwe obejście problemu można znaleźć w ZBX-14541.

Przycięty długi adres IPv6 w informacji o nieudanym logowaniu

Komunikat o nieudanej próbie logowania wyświetli tylko pierwsze 39 znaków zapisanego adresu IP, ponieważ jest to limit znaków w polu bazy danych. Oznacza to, że adresy IPv6 dłuższe niż 39 znaków będą wyświetlane niekompletnie.

Kontrole Zabbix agent w systemie Windows

Nieistniejące wpisy DNS w parametrze `Server` pliku konfiguracyjnego Zabbix agent (zabbix_agentd.conf) mogą wydłużyć czas odpowiedzi Zabbix agent w systemie Windows. Dzieje się tak, ponieważ demon buforowania DNS systemu Windows nie buforuje odpowiedzi negatywnych dla adresów IPv4. Jednak w przypadku adresów IPv6 odpowiedzi negatywne są buforowane, więc możliwym obejściem tego problemu jest wyłączenie IPv4 na hoście.

Eksport/import YAML

Istnieją pewne znane problemy z eksportem/importem:

- Komunikaty o błędach nie podlegają tłumaczeniu;
- Prawidłowy JSON z rozszerzeniem pliku .yaml czasami nie może zostać zaimportowany;
- Daty czytelne dla człowieka bez cudzysłowów są automatycznie konwertowane na znaczniki czasu Unix.

Kreator konfiguracji na SUSE z NGINX i php-fpm

Kreator konfiguracji frontendu nie może zapisać pliku konfiguracyjnego na SUSE z NGINX + php-fpm. Jest to spowodowane ustawieniem w jednostce /usr/lib/systemd/system/php-fpm.service, które uniemożliwia Zabbixowi zapis do /etc. (wprowadzone w PHP 7.4).

Dostępne są dwie opcje obejścia problemu:

- Ustaw opcję ProtectSystem na 'true' zamiast 'full' w jednostce systemd php-fpm.
- Zapisz ręcznie plik /etc/zabbix/web/zabbix.conf.php.

Przekazywanie nagłówka Authorization

W niektórych przypadkach Apache lub NGINX mogą uniemożliwiać dotarcie nagłówka Authorization w żądaniach API do Zabbix. Może to powodować problemy z uwierzytelnianiem podczas korzystania z Zabbix API lub usług jednokrotnego logowania (SSO), takich jak SAML z Okta.

Aby rozwiązać ten problem, zaktualizuj konfigurację swojego serwera WWW.

W przypadku **Apache**, jeśli używasz go jako reverse proxy (konfiguracja bez CGI), dodaj następującą dyrektywę do `/etc/httpd/conf/httpd` (w systemach opartych na RHEL) lub `/etc/apache2/apache2.conf` (w Debian/Ubuntu):

```
SetEnvIfNoCase ^Authorization$ "(.+)" HTTP_AUTHORIZATION=$1
```

Jeśli Apache bezpośrednio wykonuje skrypty obsługujące żądania (np. przy użyciu mod_cgi), zamiast tego dodaj następującą dyrektywę:

```
CGIPassAuth On
```

Natomiast **NGINX** obsługuje nagłówek Authorization automatycznie. Jeśli jednak NGINX działa jako reverse proxy, możesz jawnie przekazywać nagłówek Authorization, dodając następujące dyrektywy do `/etc/nginx/nginx.conf` (dla lokalizacji twojego frontend Zabbix):

```
...
location / {
...
    proxy_set_header Authorization $http_authorization;
    proxy_pass http://backend_server;
...
}
```

Po zaktualizowaniu konfiguracji uruchom ponownie swój serwer WWW.

Więcej informacji znajdziesz tutaj:

- ZBX-22952
- Apache 2.4 + PHP-FPM and Authorization headers
- Dyrektywy SetEnvIfNoCase i CGIPassAuth
- NGINX Reverse Proxy

Chromium dla usługi web Zabbix w Ubuntu 20

Chociaż w większości przypadków usługa web Zabbix może działać z Chromium, w Ubuntu 20.04 użycie Chromium powoduje następujący błąd:

```
Cannot fetch data: chrome failed to start:cmd_run.go:994:
WARNING: cannot create user data directory: cannot create
"/var/lib/zabbix/snap/chromium/1564": mkdir /var/lib/zabbix: permission denied
Sorry, home directories outside of /home are not currently supported. See https://forum.snapcraft.io/t/112
```

Ten błąd występuje, ponieważ `/var/lib/zabbix` jest używany jako katalog domowy użytkownika „zabbix”.

Niestandardowe kody błędów MySQL

Gdy Zabbix wykryje, że baza danych backend jest niedostępna, wysyła powiadomienie i nadal próbuje się połączyć. Dla niektórych silników baz danych rozpoznawane są określone kody błędów. W MySQL do rozpoznawanych kodów błędów należą:

- CR_CONN_HOST_ERROR
- CR_SERVER_GONE_ERROR
- CR_CONNECTION_ERROR
- CR_SERVER_LOST
- CR_UNKNOWN_HOST
- ER_SERVER_SHUTDOWN
- ER_ACCESS_DENIED_ERROR
- ER_ILLEGAL_GRANT_FOR_TABLE
- ER_TABLEACCESS_DENIED_ERROR
- ER_UNKNOWN_ERROR

Dodatkowo podczas używania Zabbix z instalacją MySQL na platformie Azure w logach Zabbix może pojawić się ogólny komunikat o błędzie *[9002] Some errors occurred*. Ten komunikat jest wysyłany przez bazę danych do serwera lub proxy Zabbix. Aby ustalić przyczynę błędu, sprawdź logi Azure.

Nieprawidłowe wyrażenia regularne po przełączeniu na PCRE2

W Zabbix 6.0 dodano obsługę PCRE2. Mimo że PCRE jest nadal obsługiwane, pakiety instalacyjne Zabbix dla RHEL 7 i nowszych, SLES (wszystkie wersje), Debian 9 i nowszych, Ubuntu 16.04 i nowszych zostały zaktualizowane tak, aby używać PCRE2. Chociaż zmiana na PCRE2 przynosi wiele korzyści, może spowodować, że niektóre istniejące wzorce regexp PCRE staną się nieprawidłowe lub będą działać inaczej. W szczególności dotyczy to wzorca *^[\w-\.]*. Aby ponownie uczynić to wyrażenie regularne prawidłowym bez wpływu na jego semantykę, zmień wyrażenie na *^[-\w\.]* . Dzieje się tak dlatego, że PCRE2 traktuje znak myślnika jako separator, tworząc zakres wewnątrz klasy znaków.

Błąd widżetu Geomap

Mapy w widżecie Geomap mogą nie ładować się poprawnie, jeśli przeprowadzono aktualizację ze starszej wersji Zabbix z NGINX i podczas aktualizacji nie przełączono się na nowy plik konfiguracyjny NGINX.

Aby rozwiązać ten problem, można odrzucić stary plik konfiguracyjny, użyć pliku konfiguracyjnego z pakietu bieżącej wersji i ponownie go skonfigurować zgodnie z opisem w instrukcjach pobierania w sekcji *e. Configure PHP for Zabbix frontend*.

Alternatywnie można ręcznie edytować istniejący plik konfiguracyjny NGINX (zwykle */etc/zabbix/nginx.conf*). Aby to zrobić, otwórz plik i znajdź następujący blok:

```
location ~ /(api\/|conf[^\.]|include|locale|vendor) {
        deny            all;
        return          404;
}
```

Następnie zastąp ten blok następującym:

```
location ~ /(api\/|conf[^\.]|include|locale) {
        deny            all;
        return          404;
}

location /vendor {
        deny            all;
        return          404;
}
```

Wstępne przetwarzanie — zmienne globalne są niebezpieczne

JavaScript we wstępnym przetwarzaniu jest uruchamiany dla każdego żądania, ale przypisania do niezadeklarowanych identyfikatorów (na przykład `secret = value`) tworzą niejawne zmienne globalne, które mogą utrzymywać się poza bieżącym wykonaniem. Przechowywanie danych wrażliwych (tokenów, haseł itp.) w niejawnych zmiennych globalnych zwiększa ryzyko przypadkowego

ujawnienia lub ponownego użycia przez kolejne uruchomienia wstępnego przetwarzania albo inne integracje wykonywane w tym samym środowisku.

Nie polegaj na niejawnych zmiennych globalnych. Zawsze deklaruj zmienne za pomocą `var` lub `const` i unikaj dołączania sekretów do obiektów globalnych (na przykład `globalThis` lub `window`). Nie ma obsługiwanego sposobu zastępowania wbudowanych obiektów globalnych z poziomu wstępnego przetwarzania.

Bezpieczny przykład:

```
var apiToken = payload.token;
var count = 1;
return JSON.stringify({ token: apiToken, calls: count });
```

Grupy procesorów w systemie Windows

Dokumentacja firmy Microsoft stwierdza, że systemy z mniej niż 64 procesorami logicznymi zawsze mają jedną grupę procesorów, Grupę 0. Jednak użytkownicy Zabbix zgłosili rzadki błąd ZBX-20260, gdy w systemach z 64 lub mniejszą liczbą procesorów logicznych występowały dwie grupy procesorów. Skutkowało to dostępnością liczników wydajności "\Processor(n)" tylko dla jednej z dwóch grup procesorów. Rzeczywista przyczyna źródłowa tego błędu nie jest znana. Jednak podobny przypadek opisano na stackoverflow.com, a jego przyczyną była współpraca między BIOS-em a systemem Windows.

Ograniczenia filtrowania przy użyciu porównań utf8mb4

Filtry (np. w *Data collection* > *Maintenance*) mogą nie działać poprawnie, gdy są stosowane do encji zawierających określone znaki Unicode (np. 𝓒, 𝔈). Problem ten wynika ze sposobu, w jaki domyślne porównanie utf8mb4_bin w bazach danych MySQL lub MariaDB obsługuje sortowanie i porównywanie znaków Unicode.

Aby obejść to ograniczenie, użytkownicy mogą zmienić porównanie kolumn bazy danych na alternatywne, takie jak utf8mb4_0900_bin, utf8mb4_0900_ai_ci lub utf8mb4_unicode_520_ci. Należy jednak pamiętać, że zmiana porównania może powodować nieoczekiwane zachowanie przy obsłudze pustych znaków, a także podczas sortowania i filtrowania innych znaków.

Więcej informacji o zmianie porównań można znaleźć w dokumentacji MySQL lub dokumentacji MariaDB. Szczegółowe informacje o różnicach między porównaniami znajdują się w sekcji Unicode Character Sets w dokumentacji MySQL.

Dostęp do elementów interfejsu użytkownika przy użyciu MariaDB 10.5.1–10.5.9

Uzyskiwanie dostępu do frontend Zabbix z rolą inną niż Super Admin może skutkować wyświetleniem komunikatu: „Wystąpił błąd systemowy. Skontaktuj się z administratorem Zabbix.". Ten problem dotyczy instalacji korzystających z wersji MariaDB od 10.5.1 do 10.5.9.

Aby uniknąć tego problemu, zaktualizuj MariaDB do wersji nowszej niż 10.5.9. Więcej informacji znajduje się w ZBX-25746.

Profilowanie nadmiernego użycia pamięci za pomocą tcmalloc

Jeśli podejrzewasz, że Twoja instalacja Zabbix używa zbyt dużo pamięci, możesz skorzystać z funkcji profilowania pamięci tcmalloc, aby zbadać zużycie pamięci przez serwer/proxy Zabbix.

1. Podczas instalacji Zabbix ze źródeł skonfiguruj dodatkowe flagi:

```
export CFLAGS="-std=gnu99 -g -O0"
```

Flaga `-std=gnu99` jest wymagana do budowania serwera Zabbix, proxy Zabbix lub agenta Zabbix. Flaga `-g` dodaje dodatkowe informacje debugowania, natomiast `-O0` wyłącza optymalizacje, które mogą zakłócać profilowanie przez tcmalloc.

2. Ustaw następujące zmienne środowiskowe przed uruchomieniem serwera Zabbix. Zmienne te informują tcmalloc, jak śledzić i raportować użycie pamięci:

```
LD_PRELOAD="/usr/lib/aarch64-linux-gnu/libtcmalloc.so" \
HEAPPROFILE=./heap_profile \
HEAP_PROFILE_ALLOCATION_INTERVAL=0 \
HEAP_PROFILE_INUSE_INTERVAL=4294967296 \
HEAPPROFILESIGNAL=5 \
MALLOCSTATS=1 \
./sbin/zabbix_server -f -c /etc/zabbix/zabbix_server.conf
```

3. Wyzwól zrzut profilu, wysyłając sygnał 5 do procesu docelowego. Zastąp 1234 rzeczywistym identyfikatorem procesu (PID):

```
kill -5 1234
```

4. Wyświetl wygenerowany profil:

```
pprof-symbolize -text ./sbin/zabbix_server ./heap_profile.0001.heap

Using local file ./sbin/zabbix_server.
```

```
Using local file ./heap_profile.0001.heap.
Total: 1078.1 MB
  1076.8  99.9%  99.9%   1076.8  99.9% zbx_malloc2
     1.0   0.1% 100.0%      1.0   0.1% __GI___strdup
     0.2   0.0% 100.0%      0.2   0.0% CRYPTO_zalloc@@OPENSSL_3.0.0
     0.1   0.0% 100.0%      0.1   0.0% OPENSSL_LH_insert@@OPENSSL_3.0.0
     0.0   0.0% 100.0%      0.0   0.0% zbx_realloc2
     0.0   0.0% 100.0%      0.1   0.0% PKCS7_decrypt@@OPENSSL_3.0.0
     0.0   0.0% 100.0%      0.0   0.0% find_best_tree_node
     0.0   0.0% 100.0%      0.0   0.0% CRYPTO_strndup@@OPENSSL_3.0.0
     ...
     0.0   0.0% 100.0%      0.0   0.0% preprocessing_flush_value
     0.0   0.0% 100.0%   1074.0  99.6% preprocessor_add_request
```

W tym przykładzie zbx_malloc2 odpowiada za prawie wszystkie alokacje pamięci.

Zobacz także:

- ZBX-25050 i ZBX-25584 — powiązane zgłoszenia problemów.
- GCC Option Summary — informacje o opcjach kompilacji (`-std=gnu99`, `-g`, `-O0` itd.).
- Dokumentacja Gperftools Heap Profiler dotycząca zmiennych środowiskowych używanych do profilowania tcmalloc.

Replikacja grupowa MySQL 8.0 w trybie multi-primary

Podczas korzystania z replikacji grupowej MySQL 8.0 w trybie multi-primary możesz napotkać błąd podczas zatwierdzania transakcji podobny do następującego:

```
1531697:20250128:064734.697 query [txnlev:1] [update alerts set status=1,retries=0,error='' where alertid=
1531697:20250128:064734.713 query [txnlev:1] [commit;]
1531697:20250128:064734.753 [Z3005] query failed: [3101] Plugin instructed the server to rollback the curr
```

Wygląda na to, że ten błąd jest wywoływany przez problemy z operacjami wycofywania transakcji obejmującymi ograniczenia kluczy obcych.

Zobacz także:

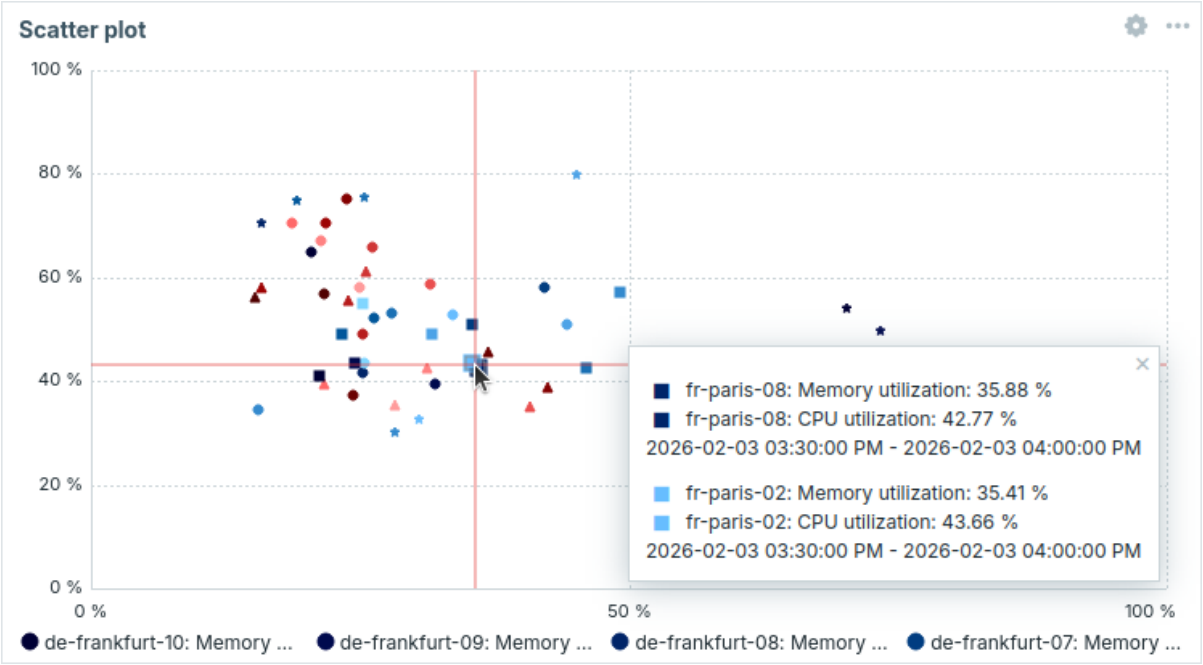
- ZBX-26060 — powiązane zgłoszenie problemu.
- MySQL Bug #96758 "Rollbacks with Foreign Keys on single node" — nadrzędny problem.

2 Co nowego w Zabbix 8.0

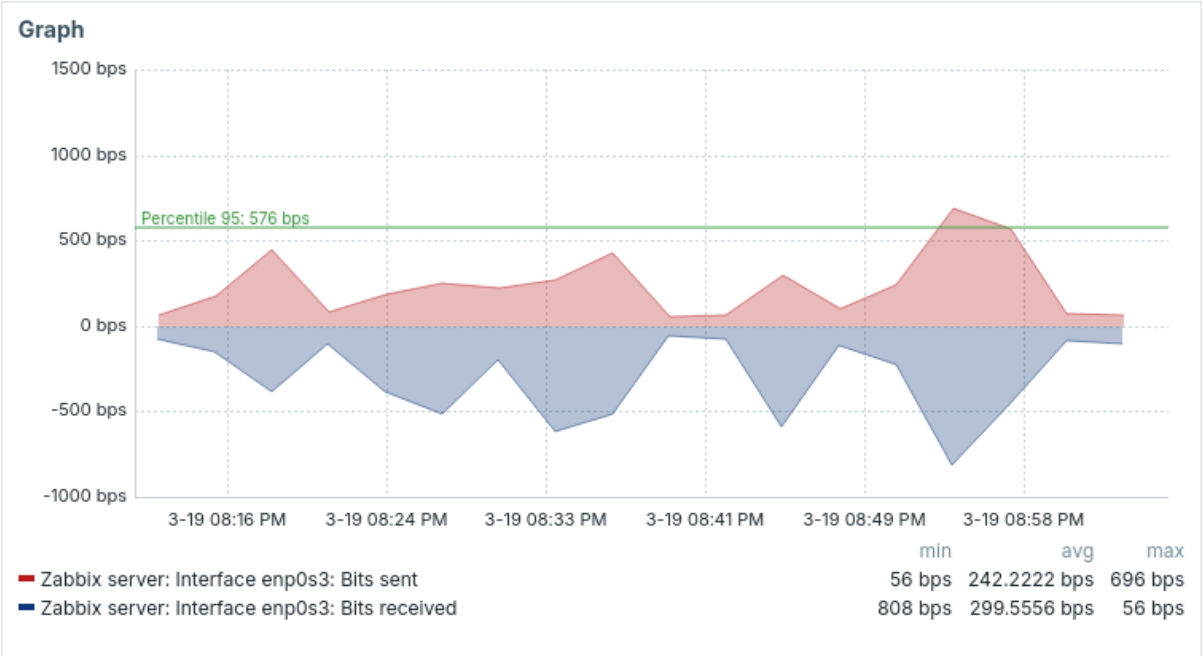
Zabbix 8.0.0 jest kontynuacją Zabbix 7.4.0, dodając nowe funkcje i ulepszenia.

Zobacz niekompatybilne zmiany dla tej wersji.

Widżet wykresu rozrzutu Widżet Scatter plot został dodany do widżetów pulpitu. Wyświetla zależność między dwiema metrykami poprzez nanoszenie pojedynczych punktów danych wzdłuż osi X i Y. Pomaga to ujawnić wzorce, skupiska, korelacje i wartości odstające w zbiorze danych.



Odwrócenie osi Y dla widżetu Graph Wykresy w widżecie Graph mogą być teraz wyświetlane z odwróconymi wartościami osi Y. Nowe ustawienie *Odwróć wartości* umożliwia pomnożenie wartości osi Y przez −1 bez zmiany oryginalnych danych.



Zobacz także: Ulepszenia widżetu Graph.

Szablony

Nowe szablony

- Aruba CX 8300s by SNMP, szablon zapewniający monitorowanie oparte na SNMP dla serii przełączników Aruba CX 8300.
- Zestaw szablonów AWS by HTTP został uzupełniony o szablon *AWS Backup Vault by HTTP*.
- Zestaw szablonów Azure by HTTP został uzupełniony o szablon *Azure Sentinel by HTTP*.
- Ciena 3906 by SNMP, szablon do monitorowania urządzeń Ciena 3906.
- Cisco Secure Firewall Threat Defense by HTTP, szablon zapewniający możliwości monitorowania urządzeń Cisco Secure Firewall Threat Defense przy użyciu REST API.
- Cradlepoint NCM v2 by HTTP, zestaw szablonów do monitorowania Cradlepoint NCM v2 i jego urządzeń przez HTTP.
- Domain RDAP by HTTP, szablon do monitorowania danych rejestracji domen za pomocą protokołu RDAP.
- IBM Maximo Service Request, szablon oparty na webhook, który umożliwia połączenie Zabbix z IBM Maximo.
- MariaDB by ODBC, szablon do monitorowania baz danych MariaDB przez ODBC.
- Microsoft Hyper-V Failover Cluster by SSH oraz Microsoft Hyper-V Standalone by SSH, szablony do monitorowania klastrów Microsoft Hyper-V i samodzielnych hostów przez SSH.

- OpenAI Platform by HTTP, szablon do monitorowania platformy deweloperskiej OpenAI.
- Percona by ODBC, szablon do monitorowania baz danych Percona przez ODBC.
- Ribbon SBC Edge by HTTP, szablon do monitorowania urządzeń Ribbon SBC Edge (dawniej SWe Lite) przez HTTP.
- Ribbon SBC SWe Core by HTTP, szablon do monitorowania urządzeń SBC SWe Core przez HTTP, oraz Ribbon SBC SWe CE by HTTP, szablon do monitorowania instancji Ribbon SBC SWe Call Engine (CE) przez HTTP.
- Stormshield SNS by SNMP, szablon do monitorowania urządzeń Stormshield Network Security (SNS) przez SNMP.
- VeloCloud SD-WAN Edge by HTTP, szablon do monitorowania urządzeń VeloCloud SD-WAN Edge przez HTTP.
- Vyatta Virtual Router by SNMP, szablon do monitorowania routera wirtualnego Vyatta 1908e.

Zaktualizowane szablony

- Ciena 3906 by SNMP został zaktualizowany o pozycje monitorujące system plików i obciążenie CPU.
- Zestaw szablonów GCP by HTTP został uzupełniony o szablon *GCP Cloud Run Service by HTTP*.
- GitHub organization by HTTP został zaktualizowany o pozycje do monitorowania Microsoft Copilot.
- Microsoft 365 reports by HTTP został zaktualizowany o pozycje do monitorowania Microsoft Copilot.
- MySQL by Zabbix agent, MySQL by Zabbix agent 2, MySQL by Zabbix agent active, MySQL by Zabbix agent 2 active oraz MySQL by ODBC zostały zaktualizowane, aby obsługiwać zarówno `SHOW SLAVE STATUS` (stara składnia), jak i `SHOW REPLICA STATUS` (nowa składnia).
- MySQL by ODBC został również zaktualizowany o nowe metryki, reguły wykrywania dla tabel i replik oraz ulepszony dashboard.
- PostgreSQL by ODBC został zaktualizowany o nowe metryki, reguły wykrywania i dashboardy, a także ogólne usprawnienia wydajności i obserwowalności.
- Proxmox VE by HTTP został zaktualizowany o funkcjonalność zagnieżdżonego LLD. Ponadto format jednostek dla pozycji wyświetlających wartości procentowe został dostosowany dla większej przejrzystości.
- VeloCloud SD-WAN by HTTP, wcześniej *VMWare SD-WAN VeloCloud by HTTP*, został przemianowany i zaktualizowany tak, aby był zgodny z najnowszą platformą VeloCloud SD-WAN.
- Vyatta Virtual Router by SNMP został zaktualizowany o nowe pozycje OID i ulepszenia dashboardu.

Pozycje

Typ danych JSON Zabbix obsługuje teraz JSON jako typ danych dla wartości pozycji.

Wcześniej wartości JSON były zbierane przez pozycje tekstowe i przechowywane jako ciągi znaków z limitem 64 KB. Teraz Zabbix może przechowywać wartości JSON natywnie z limitem 128 MiB, a także odrzucać nieprawidłowe wartości JSON (np. zawierające klucze bez cudzysłowów, końcowe przecinki, niedopasowane nawiasy).

Typ danych JSON jest obsługiwany przez wszystkie typy pozycji i prototypy pozycji (z wyjątkiem *Calculated*) oraz jest dostępny w eksporcie danych w czasie rzeczywistym i konektorach. Wartości JSON mogą być przechowywane we wszystkich obsługiwanych bazach danych oraz w Elasticsearch. Jeśli używasz TimescaleDB, zobacz uwagi dotyczące aktualizacji.

Należy pamiętać, że pozycje JSON nie mogą być używane w wyzwalaczach; można jednak wyodrębniać pola JSON za pomocą pozycji zależnych, które mają typ danych inny niż JSON, i używać ich w wyzwalaczach.

Pozycje zwracające ciąg JSON (`net.if.discovery`, `vfs.file.get` itd.) nadal są pozycjami tekstowymi; w razie potrzeby można jednak zmienić je na JSON.

Więcej szczegółów oraz limity danych JSON można znaleźć w konfiguracji pozycji.

Parametr type dla wykrywania dysków S.M.A.R.T. Pozycja smart.disk.discovery (wtyczka S.M.A.R.T. dla Zabbix agent 2) akceptuje teraz opcjonalny parametr **type**, aby określić wartość używaną do skanowania dysków.

Wtyczki

Wtyczka Ceph Ta wtyczka działa teraz w dwóch trybach:

- **native** - Ten tryb używa biblioteki go-ceph do bezpośredniej komunikacji z klastrem Ceph przy użyciu natywnego API Ceph (protokół msgr2). Jest to zalecany tryb dla nowoczesnych instalacji Ceph, ale jest obsługiwany **tylko w systemie Linux** i począwszy od Ceph 16.
- **restful** (przestarzały) - Ten tryb używa Ceph RESTful API do komunikacji. Jest to tryb domyślny ze względu na zachowanie wstecznej kompatybilności, ale nie będzie działać z Ceph w wersji 20 (Tentacle) lub nowszej z powodu usunięcia modułu mgr/restful.

O tym, którego trybu użyć, decyduje wartość parametru mode (native/restful):

- `Plugins.Ceph.Default.Mode=native` - ustaw natywny tryb dla wtyczki
- `Plugins.Ceph.Sessions.<SessionName>.Mode=native` - ustaw natywny tryb dla nazwanej sesji

Należy pamiętać, że zestaw poświadczeń użytkownika różni się dla każdego trybu i nie są one ze sobą kompatybilne. Parametr `Plugins.Ceph.InsecureSkipVerify` jest ignorowany w trybie native, ponieważ bezpieczeństwo połączenia jest definiowane po stronie klastra Ceph przez protokół msgr2 (domyślnie bezpieczny).

Należy pamiętać, że wtyczka Ceph dla Zabbix agent 2 jest teraz wtyczką ładowalną i wymaga dodatkowych kroków instalacyjnych. Wynika to z wymogu pakietu librados (dla trybu native). Szczegóły znajdują się w pliku readme wtyczki Ceph.

Wtyczka MongoDB Zabbix agent 2 wtyczka MongoDB oferuje wiele usprawnień: - Pełne wsparcie dla standardowego parsowania URI MongoDB, z obsługą schematów `mongodb://` i `mongodb+srv://`. - Automatyczne wykrywanie węzłów zestawu replik MongoDB, co zwiększa możliwości monitorowania klastrów MongoDB. - Obsługa uwierzytelniania x509, umożliwiająca bezpieczne połączenia z MongoDB przy użyciu certyfikatów klienta.

Wtyczka Oracle Oracle plugin w Zabbix agent 2 obsługuje teraz szyfrowane połączenia z bazami danych Oracle przy użyciu protokołu TCPS (TLS). Dodaje to możliwość monitorowania instancji Oracle przez gniazda zabezpieczone TLS, zwiększając bezpieczeństwo zdalnego monitorowania.

Wtyczka Redis — obsługa TLS i walidacja podczas uruchamiania Do wtyczki Redis dla Zabbix agent 2 dodano obsługę TLS.

Zaimplementowano walidację konfiguracji TLS wtyczki podczas uruchamiania oraz ulepszono komunikaty walidacyjne/błędów. Nieprawidłowa logika konfiguracji (na przykład użycie typu połączenia `verify_full` bez określenia `TLSCAFile`) może uniemożliwić uruchomienie Zabbix agent 2.

Tryb wykonywania testowego dla ładowalnych pluginów Ładowalne pluginy można teraz uruchamiać w trybie testowym przy użyciu flagi `-t` (`--test`), przekazując jako argument klucz pozycji. W tym trybie plugin działa do celów debugowania i programowania, a pliki konfiguracyjne pluginu są ignorowane.

Wykrywanie niskiego poziomu

Pole wyboru Convert to JSON w formularzach wykrywania Nowe pole wyboru *Convert to JSON* zostało dodane do formularza reguły wykrywania oraz formularza prototypu wykrywania, które jest wyświetlane po wybraniu opcji "HTTP agent" z listy rozwijanej *Type*. Ta opcja pozwala oznaczyć pobrane dane do automatycznej konwersji do formatu JSON przed dalszym przetwarzaniem.

Obsługa makr w zagnieżdżonym wykrywaniu niskiego poziomu Makra wykrywania niskiego poziomu są teraz obsługiwane w zagnieżdżonych regułach wykrywania niskiego poziomu w:

- parametrach wstępnego przetwarzania JSONPath parameters
- polu JSONPath dla niestandardowych makr LLD

Edytowalne tagi dla wyzwalaczy utworzonych przez wykrywanie niskiego poziomu Wyzwalacze utworzone z prototypów wyzwalaczy mogą teraz mieć tagi dodawane ręcznie. Tagi dziedziczone z prototypów wyzwalaczy są nadal stosowane automatycznie. Tagi dodane ręcznie mogą być modyfikowane w odkrytych wyzwalaczach i będą uwzględniane w tablicach tagów zdarzeń oraz dostępne dla funkcji obsługujących tagi, takich jak filtry, widżety pulpitu i makra powiadomień.

Procesy

Buforowanie i ponowne użycie EngineID SNMPv3 Zabbix buforuje teraz mapowania EngineID SNMPv3 → IP i będzie próbował ponownie używać zbuforowanych EngineID przy kolejnych kontrolach SNMPv3, ograniczając ruch sondujący i poprawiając wydajność pollera. Jeśli ponownie użyty EngineID nie odpowiada, poller wraca do sondowania EngineID i może usuwać nieaktualne wpisy po zmianach interfejsu lub w przypadku utrzymujących się błędów.

Udoskonalone ograniczanie proxy podczas odzyskiwania pamięci podręcznej historii Logika ograniczania proxy została udoskonalona, aby poprawić stabilność serwera podczas odzyskiwania pamięci podręcznej historii. Gdy wykorzystanie pamięci podręcznej historii osiągnie próg ograniczania, serwer nadal przestaje przyjmować dane z proxy, tak jak wcześniej. Gdy wykorzystanie pamięci podręcznej spadnie do 60%, serwer zaczyna przetwarzać listę ograniczania, ale nadal może odrzucać przesyłanie danych z proxy zawierające bardzo duże partie danych (w przybliżeniu ponad 10 tys. rekordów), dopóki obciążenie pamięci podręcznej nie zmniejszy się bardziej. Ta zmiana zmniejsza ryzyko powtarzających się przeciążeń pamięci podręcznej podczas odzyskiwania przez serwer.

Zwiększono maksymalny limit czasu dla zabbix_get i zabbix_js Maksymalna wartość parametru `timeout` dla narzędzi wiersza poleceń zabbix_get i zabbix_js została zwiększona do 600 sekund.

Zoptymalizowane housekeeping Housekeeping został zoptymalizowany poprzez przeniesienie tworzenia zadań housekeepera do wyzwalaczy bazy danych. Gdy pozycje (w tym reguły wykrywania niskiego poziomu), wyzwalacze, usługi lub reguły wykrywania sieci są usuwane, wyzwalacze bazy danych (zamiast jawnych wywołań na poziomie aplikacji) wypełniają teraz tabelę `housekeeper` zadaniami czyszczenia. Szczegóły znajdują się w opisie procedury housekeeping.

Housekeeper usuwa teraz również zdarzenia wykrywania sieci wygenerowane na podstawie wykrytych hostów lub usług, które zostały następnie usunięte, a także wszystkie zdarzenia powiązane z problemami wyzwalaczy, które również zostały usunięte (wcześniej usuwane były tylko same problemy; powiązane zdarzenia były usuwane dopiero po upływie okresu *Trigger data storage period* housekeepera).

Ręczne zamknięcie — tagi wyzwalacza dziedziczone przez zdarzenia odtworzenia Zdarzenia odtworzenia utworzone po ręcznym zamknięciu dziedziczą tagi wyzwalacza oprócz tagów pozycji i hosta. Tagi te są obecne w tablicy tagów zdarzenia i są dostępne dla makr powiadomień, takich jak `{EVENT.RECOVERY.TAGS}` oraz `{EVENT.RECOVERY.TAGSJSON}`.

Buforowanie zapytań DNS dla demonów Zabbix Zabbix serwer, Zabbix proxy i Zabbix agent otrzymały obsługę używania resolvera c-ares dla wszystkich żądań DNS, zapewniając buforowanie zapytań DNS oraz ulepszone przełączanie awaryjne resolvera, gdy Zabbix jest zbudowany z `--with-ares`. Buforowanie zapytań DNS wymaga c-ares 1.26.0 lub nowszego.

Obsługa kompilacji c-ares w systemie Windows Zabbix agent można teraz skompilować z resolverem c-ares w systemie Microsoft Windows. c-ares można zainstalować za pomocą vcpkg, a kompilacja agenta obsługuje zarówno `ARES=<vcpkg prefix>`, jak i oddzielne ścieżki `ARESINCDIR`/`ARESLIBDIR` dla katalogów plików nagłówkowych i bibliotek.

Uwierzytelnianie

Importowalne certyfikaty SAML do logowania jednokrotnego Użytkownicy typu Super admin mogą teraz importować certyfikaty i klucze prywatne bezpośrednio we frontendzie na potrzeby konfiguracji SAML. Do *Administration* > *Authentication* > *SAML* dodano trzy nowe pola:

- *Certyfikat IdP* — certyfikat X.509 przedstawiany przez dostawcę tożsamości
- *Certyfikat SP* — certyfikat dostawcy usług używany do wymiany danych SAML
- *Klucz prywatny SP* — klucz prywatny odpowiadający certyfikatowi SP

Te elementy sterujące umożliwiają dodawanie nowych wartości lub modyfikowanie istniejących z poziomu karty ustawień SAML. Certyfikaty i klucze prywatne są sprawdzane przed zapisaniem w wybranym backendzie pamięci masowej; nieprawidłowe lub uszkodzone wartości są odrzucane wraz z objaśniającym błędem.

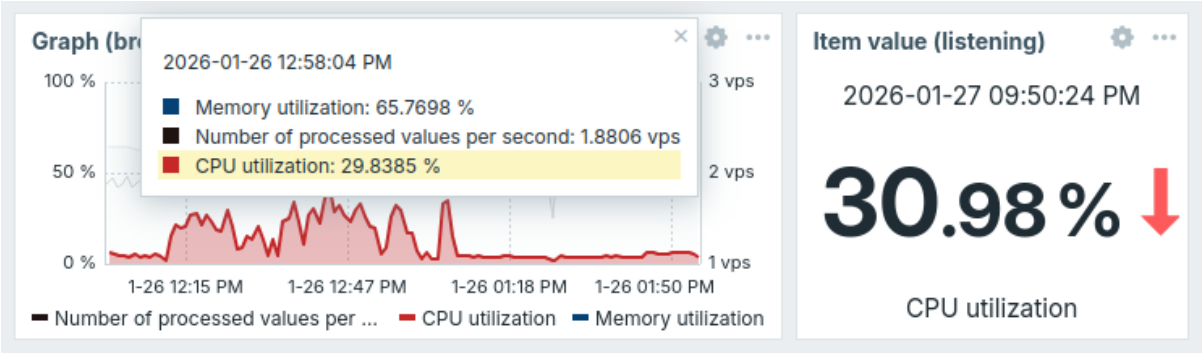
Widżety

Grupowanie markerów hostów na mapie geomap Widget Geomap obsługuje teraz parametr *Clustering*, który pozwala kontrolować, w jaki sposób pobliskie markery hostów są łączone w jeden marker z licznikiem. Ustawiając poziom powiększenia mapy dla grupowania, można zachować czytelność dużych map i utrzymać precyzyjną widoczność po przybliżeniu.

Kolumny agregowane w Top items Widget Top items może teraz grupować wzorce pozycji w pojedynczą agregowaną kolumnę lub wiersz, co ułatwia prezentowanie połączonych metryk (na przykład: całkowity ruch przychodzący na wszystkich interfejsach sieciowych hosta). Podczas konfigurowania kolumn pozycji dodano trzy nowe opcje: *Agreguj kolumny*, *Funkcja agregacji kolumn* oraz *Nazwa kolumny łączonej*.

Ulepszenia widgetu Graph Widget Graph oferuje wiele usprawnień zwiększających użyteczność:

- Pozycje w podpowiedzi danych wykresu, która pojawia się po najechaniu kursorem na wykres, są sortowane według wartości w kolejności malejącej.
- Najechanie kursorem na pozycję w podpowiedzi powoduje wyróżnienie jej wykresu przy jednoczesnym przyciemnieniu pozostałych.
- Wybranie pozycji w podpowiedzi rozgłasza jej dane do innych widgetów, które obsługują ich nasłuchiwanie.
- Usunięto limit liczby pozycji wyświetlanych w podpowiedzi.
- Nowe ustawienie *Host names in labels* pozwala wybrać, czy nazwy hostów mają być wyświetlane w podpowiedzi i legendzie wykresu.



- Nowe ustawienie *Invert values* umożliwia odwrócenie wykresu.

Frontend

Nowe i osadzone czcionki Zabbix zawiera teraz nowe i osadzone czcionki, które poprawiają czytelność, ładują się szybciej i wyświetlają dodatkowe języki frontend z minimalnym wpływem na układ. Dzięki osadzeniu czcionki te zapewniają również spójny wygląd w różnych systemach.

Nowe czcionki:

Linux by Zabbix agent: Available memory in %: Memory utilization	Triggers 1	vm.memory.utilization
Linux by Zabbix agent: Total memory	Triggers 1	vm.memory.size[total]
Linux by Zabbix agent: Total swap space	Triggers 1	system.swap.size[,total]

Starsze czcionki:

Linux by Zabbix agent: Available memory in %: Memory utilization	Triggers 1	vm.memory.utilization
Linux by Zabbix agent: Total memory	Triggers 1	vm.memory.size[total]
Linux by Zabbix agent: Total swap space	Triggers 1	system.swap.size[,total]

Nowe czcionki są używane w niemal wszystkich motywach. W razie potrzeby nowo dodane motywy *Blue (classic)* i *Dark (classic)* są dostępne ze starszymi czcionkami.

Rodzina czcionek dla treści o stałej szerokości i wykresów pozostaje bez zmian.

Walidacja wbudowana Następujące formularze we frontendzie zostały dodane do zestawu formularzy obsługujących walidację wbudowaną:

- Token API
- Uwierzytelnianie
- Autorejestracja
- Konektor
- Mapy geograficzne
- Grupa hostów
- Prototypy hostów
- Mapowanie ikon
- Obrazy
- Okres konserwacji
- Typ nośnika
- Powiadomienia
- Profil
- Proxy
- Wyrażenia regularne
- Usługa
- SLA
- Grupa szablonów
- Aktualizacja problemu

- Globalne makra użytkownika
- Role użytkowników
- Użytkownicy

Błędy danych wejściowych są wyświetlane natychmiast po wypełnieniu pól, co poprawia użyteczność i ogranicza liczbę błędów konfiguracyjnych.

Formularze modalne W konfiguracji wykrywania niskiego poziomu formularz konfiguracji prototypu hosta jest teraz otwierany w modalnym oknie (wyskakującym oknie).

Dziedziczone tagi widoczne w hostach, szablonach, pozycjach i wyzwalaczach Dziedziczone tagi są teraz wyświetlane i zwracane w spójny sposób w szablonach, hostach, pozycjach, scenariuszach WWW i wyzwalaczach. Tagi dziedziczone z łańcuchów szablonów/hostów są widoczne w *Monitoring > Latest data*. Filtrowanie według dziedziczonych tagów jest dostępne wszędzie tam, gdzie obsługiwane jest filtrowanie po tagach — w tym w sekcjach *Monitoring > Latest data* i *Data collection*, a także we wszystkich widżetach pulpitu, które umożliwiają filtrowanie według tagów hosta, pozycji, wyzwalacza lub scenariusza WWW — dzięki czemu wybór i podfiltrowywanie oparte na tagach działają tak samo niezależnie od tego, gdzie tag został zdefiniowany.

Karta *Tags* w formularzach konfiguracji szablonu, hosta i prototypu hosta udostępnia teraz element opcji pozwalający wybrać sposób prezentacji tagów: szablony pokazują *Template tags* / *Inherited and template tags*, a hosty i prototypy hostów pokazują *Host tags* / *Inherited and host tags*. Dziedziczone tagi są wizualnie wyróżnione nową ikoną obramowanego dokumentu obok etykiety tagu.

Widżety Graph i Pie chart zawierają nowe ustawienie *Item tags*.

Pozycjonowanie podpowiedzi Podpowiedzi można teraz przestawiać, przeciągając je w nowe miejsce. Dotyczy to na przykład podpowiedzi Graph, a także podpowiedzi z opisami w sekcjach Latest Data lub Problems.

Dokumentacja

Skonsolidowane strony dokumentacji dla wydań pobocznych Dokumentacja wydań dla wersji pobocznych głównego wydania Zabbix będzie teraz gromadzona odpowiednio na pojedynczych stronach dokumentacji dotyczących nowych funkcji i uwag dotyczących aktualizacji.

Co nowego w Zabbix 8.0.x

Ta strona zawiera zbiorcze informacje o nowych funkcjach uwzględnionych w wydaniach pobocznych głównej wersji Zabbix.

Zobacz także Co nowego dla głównej wersji.

Informacje o zmianach w istniejących szablonach oraz o nowych szablonach obejmujących różne urządzenia, usługi i rozwiązania partnerów można znaleźć w sekcji Zmiany w szablonach.

Co nowego w Zabbix 8.0.1 Ta wersja nie została jeszcze wydana.

3 Urządzenie Zabbix

Przegląd Zabbix appliance umożliwia natychmiastowe wdrożenie serwera Zabbix i frontend, zamiast konfigurowania ich ręcznie lub ponownego wykorzystywania istniejącego serwera dla Zabbix.

Appliance bazuje na AlmaLinux 8 (x86_64) i zawiera wstępnie skonfigurowany serwer Zabbix działający na MySQL oraz frontend działający na serwerze WWW Nginx.

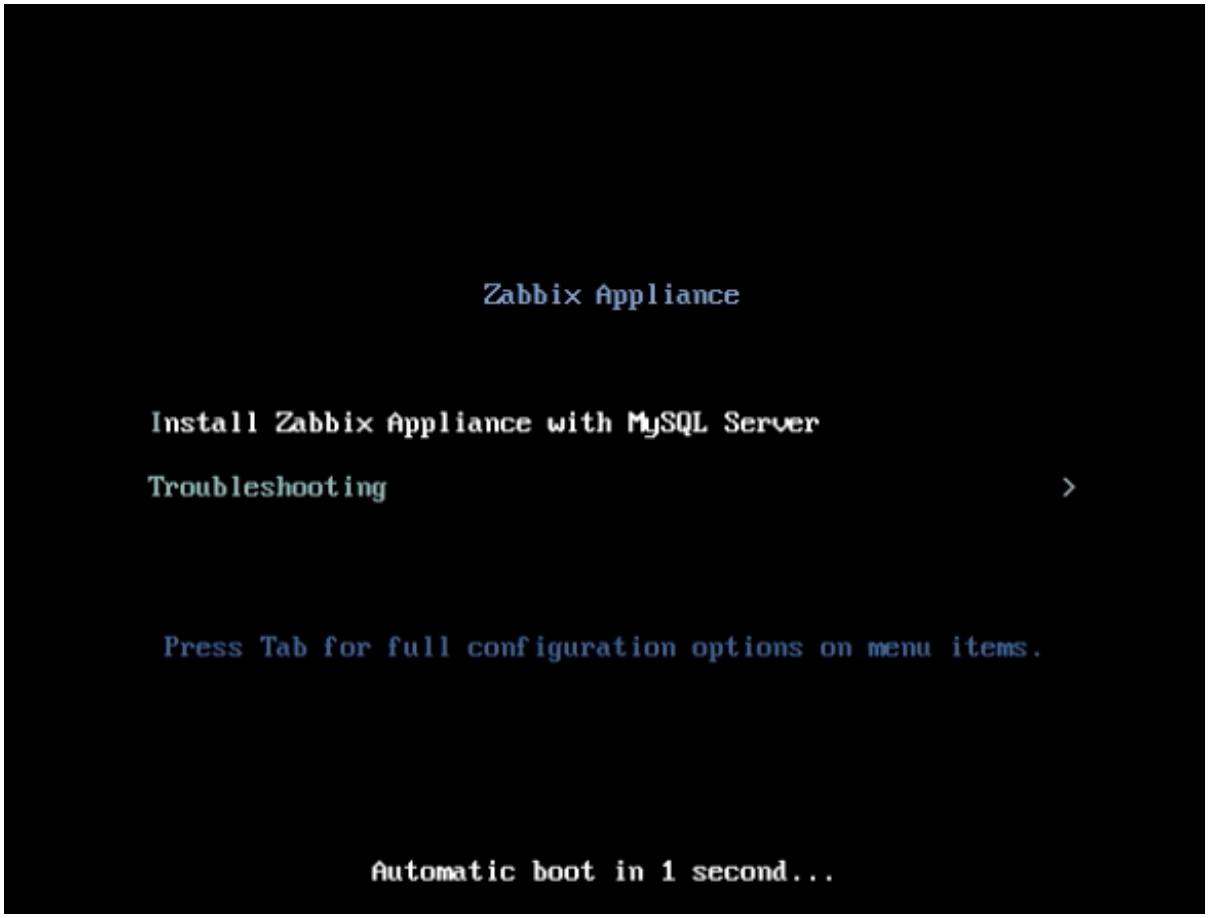
> **Attention:**
> To appliance jest przeznaczone do oceny Zabbix. Nie zaleca się używania go w poważnych środowiskach produkcyjnych.

Obrazy appliance są dostępne do pobrania w następujących formatach:

- Instalacyjny CD/DVD (.iso)
- VMware (.vmx) - zobacz uwagi
- Open virtualization format (.ovf)
- Microsoft Hyper-V (.vhd/.vhdx) - zobacz uwagi
- KVM, Parallels, QEMU, pamięć USB, VirtualBox, Xen (.raw) - zobacz uwagi

- KVM, QEMU (.qcow2)

Menu rozruchowe instalacyjnego CD/DVD Zabbix:



Szybki start Wymagania wstępne

1. Upewnij się, że maszyna hosta ma wystarczające zasoby, aby spełnić wymagania systemowe maszyny wirtualnej:

- *RAM*: 4 GB
- *Miejsce na dysku*: dla maszyny wirtualnej należy przydzielić co najmniej 8 GB
- *CPU*: minimum 2 rdzenie

2. Jeśli oprogramowanie do wirtualizacji służące do uruchamiania obrazu appliance nie jest jeszcze zainstalowane, zainstaluj je (na przykład VirtualBox).
3. Pobierz appliance w formacie obsługiwanym przez używane oprogramowanie do wirtualizacji.
4. Sprawdź ustawienia sieciowe, aby upewnić się, że DHCP jest włączone na maszynie hosta.

Instalacja

1. Uruchom appliance jako maszynę wirtualną z pobranego obrazu.
2. Skonfiguruj ustawienia sieciowe maszyny wirtualnej tak, aby umożliwić dostęp z przeglądarki na maszynie hosta. Można to osiągnąć, włączając *tryb mostkowany*.
3. Zaloguj się do maszyny wirtualnej przy użyciu domyślnych danych uwierzytelniających.
4. Aby uzyskać adres IP, uruchom na maszynie wirtualnej następujące polecenie:

```
ip addr show
```

5. Otwórz przeglądarkę na maszynie hosta i przejdź do adresu IP, który appliance otrzymał przez DHCP.
6. Zaloguj się do Zabbix przy użyciu domyślnych danych uwierzytelniających i rozpocznij monitorowanie.

Konfiguracja Ta sekcja opisuje często wymagane domyślne ustawienia konfiguracji wraz z dostępnymi opcjami dostosowania.

Dane uwierzytelniające

System

- Nazwa użytkownika: root
- Hasło: zabbix

Frontend Zabbix

- Nazwa użytkownika: Admin
- Hasło: zabbix

Po zalogowaniu możesz zmienić domyślne hasło w ustawieniach profilu użytkownika lub utworzyć nowych użytkowników i usunąć domyślnego użytkownika.

Baza danych

Hasła dla wszystkich użytkowników bazy danych są generowane losowo podczas procesu instalacji. Dla bazy danych zdefiniowano następujących użytkowników:

Root:

- Nazwa użytkownika: root
- Hasło: hasło jest przechowywane w pliku `/root/.my.cnf`. Nie jest wymagane podawanie hasła na koncie root.

Serwer Zabbix:

- Nazwa użytkownika: zabbix_srv
- Hasło: hasło jest przechowywane w pliku `/etc/zabbix/zabbix\_server.conf`

Frontend Zabbix:

- Nazwa użytkownika: zabbix_web
- Hasło: hasło jest przechowywane w pliku `/etc/zabbix/web/zabbix.conf.php`

Aby zmienić hasło użytkownika bazy danych, zmodyfikuj je w MySQL oraz w odpowiednim pliku konfiguracyjnym.

Dostęp do frontend

Do frontend Zabbix można uzyskać dostęp pod adresem *http://<IP maszyny wirtualnej>*.

Domyślnie dostęp jest dozwolony z dowolnego miejsca. Aby ograniczyć dostęp, zmodyfikuj plik `/etc/nginx/conf.d/zabbix.conf`. Po zapisaniu zmodyfikowanego pliku uruchom ponownie Nginx, logując się przez SSH jako użytkownik root i wykonując:

```
systemctl restart nginx
```

Statyczny adres IP

Domyślnie appliance używa DHCP do uzyskania adresu IP. Aby ustawić statyczny adres IP:

- Zaloguj się jako użytkownik root.
- Uruchom następujące polecenia, zastępując wartości własnymi adresami IP:

```
nmcli connection modify eth0 ipv4.addresses 192.168.1.10/24    # Adres IP appliance/prefiks CIDR
nmcli connection modify eth0 ipv4.gateway 192.168.1.1     # Adres IP bramy
nmcli connection modify eth0 ipv4.dns 8.8.8.8    # Adres IP serwera DNS
nmcli connection modify eth0 ipv4.method manual
systemctl restart network
```

Alternatywnie możesz otworzyć plik `/etc/NetworkManager/system-connections/eth0.nmconnection` i dodać następujące linie:

```
[ipv4]
address1=192.168.1.10/24,192.168.1.1
dns=8.8.8.8
method=manual
```

Po zapisaniu zmodyfikowanego pliku uruchom polecenie `systemctl restart network`.

Konfiguracja zapory sieciowej

Do zarządzania ustawieniami zapory urządzenie appliance używa iptables ze wstępnie zdefiniowanymi regułami:

- Otwarty port SSH (22 TCP)
- Otwarte porty Zabbix agent (10050 TCP) i Zabbix trapper (10051 TCP)
- Otwarte porty HTTP (80 TCP) i HTTPS (443 TCP)
- Otwarty port pułapek SNMP (162 UDP)
- Otwarte połączenia wychodzące do portu NTP (123 UDP)
- Ograniczenie pakietów ICMP do 5 pakietów na sekundę
- Odrzucanie wszystkich pozostałych połączeń przychodzących

Aby otworzyć dodatkowe porty, zmodyfikuj plik `/etc/sysconfig/iptables` i przeładuj reguły zapory:

```
systemctl reload iptables
```

Repozytoria

Urządzenie Zabbix appliance używa pakietu *zabbix-release* z repozytorium Zabbix. Repozytoria są skonfigurowane w katalogu `/etc/yum.repos.d/*`.

Strefa czasowa

Domyślnie appliance używa UTC dla zegara systemowego. Aby zmienić strefę czasową, skopiuj odpowiedni plik z `/usr/share/zoneinfo` do `/etc/localtime`, na przykład:

```
cp /usr/share/zoneinfo/Europe/Riga /etc/localtime
```

> **Note:**
> Strefa czasowa frontendu Zabbix jest ustawiana oddzielnie i może zostać zmieniona w ustawieniach frontendu. Domyślna strefa czasowa dla frontendu Zabbix to Europe/Riga.

Lokalizacje plików

- Pliki konfiguracyjne znajdują się w `/etc/zabbix`
- Pliki dziennika serwera Zabbix, proxy i agenta znajdują się w `/var/log/zabbix`
- Zabbix frontend znajduje się w `/usr/share/zabbix`
- Katalog domowy użytkownika *zabbix* to `/var/lib/zabbix`

Usługi systemowe

Usługi systemd są dostępne. Aby wyświetlić listę usług Zabbix, uruchom następujące polecenie na maszynie wirtualnej:

```
systemctl list-units zabbix*
```

Uwagi dotyczące formatu obrazu VMware

Obrazy w formacie *vmdk* mogą być używane bezpośrednio w produktach VMware Player, Server i Workstation. Aby używać ich w ESX, ESXi i vSphere, należy je przekonwertować za pomocą VMware vCenter Converter (do pobrania wymagane jest uwierzytelnienie). Jeśli używasz VMware vCenter Converter, możesz napotkać problemy z hybrydowym adapterem sieciowym. W takim przypadku możesz spróbować wskazać adapter E1000 podczas procesu konwersji. Alternatywnie, po zakończeniu konwersji możesz usunąć istniejący adapter i dodać adapter E1000.

Obraz HDD/flash (raw)

Aby uruchomić obraz, wykonaj:

```
dd if=./zabbix_appliance_8.0.0.raw of=/dev/sdc bs=4k conv=fdatasync
```

Zastąp `/dev/sdc` ścieżką do urządzenia dysku Flash/HDD.

Hyper-V

Jeśli appliance nie uruchamia się w Hyper-V, spróbuj nacisnąć **Ctrl+Alt+F2**, aby przełączyć sesję TTY.

Rozwiązywanie problemów Jeśli podczas próby zalogowania się do frontend pojawi się komunikat o błędzie *Access denied for user 'replace_user'@'localhost' (using password: YES)*, może to oznaczać, że instalacja jest nadal w toku.



Jeśli błąd nadal występuje po odczekaniu kilku minut lub jeśli zaobserwujesz jakiekolwiek inne nieoczekiwane zachowanie, prawdopodobnie oznacza to, że proces instalacji nie zakończył się pomyślnie. W takim przypadku zalecamy usunięcie bieżącego appliance i ponowne wdrożenie go zgodnie z tą samą instrukcją instalacji. Ten krok zazwyczaj rozwiązuje problem.

Należy pamiętać, że podejmowanie prób ręcznego naprawienia uszkodzonej instalacji nie jest zalecane, ponieważ może prowadzić do dalszych komplikacji.

4 Procesy Zabbix

Użyj paska bocznego, aby uzyskać dostęp do treści w sekcji procesów Zabbix.

1 Server

Przegląd

Serwer Zabbix jest centralnym procesem oprogramowania Zabbix.

Serwer wykonuje odpytywanie i przechwytywanie danych, oblicza wyzwalacze oraz wysyła powiadomienia do użytkowników. Jest to centralny komponent, do którego agenty i proxy Zabbix raportują dane o dostępności i integralności systemów. Serwer może również samodzielnie zdalnie sprawdzać usługi sieciowe (takie jak serwery WWW i serwery pocztowe) przy użyciu prostych testów usług.

Serwer jest centralnym repozytorium, w którym przechowywane są wszystkie dane konfiguracyjne, statystyczne i operacyjne, oraz elementem Zabbix, który aktywnie alarmuje administratorów, gdy w którymkolwiek z monitorowanych systemów pojawią się problemy.

Działanie podstawowego serwera Zabbix jest podzielone na trzy odrębne komponenty; są to: serwer Zabbix, frontend WWW i baza danych.

Wszystkie informacje konfiguracyjne Zabbix są przechowywane w bazie danych, z którą współpracują zarówno serwer, jak i frontend WWW. Na przykład, gdy tworzysz nową pozycję przy użyciu frontend WWW (lub API), jest ona dodawana do tabeli items w bazie danych. Następnie, mniej więcej raz na minutę, serwer Zabbix odpytuje tabelę items o listę aktywnych pozycji, która jest następnie przechowywana w pamięci podręcznej serwera Zabbix. Dlatego wprowadzenie zmian w frontend Zabbix może spowodować, że ich pojawienie się w sekcji najnowszych danych zajmie do dwóch minut.

Uruchamianie serwera

Jeśli zainstalowano z pakietu

Serwer Zabbix działa jako proces demona. Serwer można uruchomić, wykonując:

```
systemctl start zabbix-server
```

To zadziała w większości systemów GNU/Linux. W innych systemach może być konieczne uruchomienie:

```
/etc/init.d/zabbix-server start
```

Podobnie, aby zatrzymać/uruchomić ponownie/sprawdzić stan, użyj następujących poleceń:

```
systemctl stop zabbix-server
systemctl restart zabbix-server
systemctl status zabbix-server
```

Uruchamianie ręczne

Jeśli powyższe nie działa, musisz uruchomić go ręcznie. Znajdź ścieżkę do pliku binarnego zabbix_server i wykonaj:

```
zabbix_server
```

Możesz użyć następujących parametrów wiersza poleceń z serwerem Zabbix:

```
-c --config <file>              ścieżka do pliku konfiguracyjnego (domyślnie /usr/local/etc/zabbix_server.
-f --foreground                 uruchom serwer Zabbix na pierwszym planie
-R --runtime-control <option>   wykonaj funkcje administracyjne
-T --test-config                sprawdź poprawność pliku konfiguracyjnego i zakończ
-h --help                       wyświetl tę pomoc
-V --version                    wyświetl numer wersji
```

Przykłady uruchamiania serwera Zabbix z parametrami wiersza poleceń:

```
zabbix_server -c /usr/local/etc/zabbix_server.conf
zabbix_server --help
zabbix_server -V
```

Kontrola w czasie działania

Opcje kontroli w czasie działania:

Option	Description	Target
config_cache_reload	Przeładuj pamięć podręczną konfiguracji. Ignorowane, jeśli pamięć podręczna jest obecnie ładowana.	
history_cache_clear=<target>	Wyczyść pamięć podręczną historii dla pozycji określonej przez jej ID. Wpływa na wszystkie wartości pozycji, z wyjątkiem pierwszej i ostatniej wartości.	**target** - ID pozycji
diaginfo[=<**section**>]	Zbierz informacje diagnostyczne w pliku logu serwera.	**historycache** - statystyki pamięci podręcznej historii **valuecache** - statystyki pamięci podręcznej wartości **preprocessing** - statystyki menedżera przetwarzania wstępnego **alerting** - statystyki menedżera alertów **lld** - statystyki menedżera LLD **locks** - lista mutexów (pusta w systemach *BSD*) **connector** - statystyki dla konektorów z największą kolejką
ha_status	Zapisz stan klastra wysokiej dostępności (HA) w logu.	
ha_remove_node=target	Usuń węzeł wysokiej dostępności (HA) określony przez jego nazwę lub ID. Należy pamiętać, że aktywne/rezerwowe węzły nie mogą zostać usunięte.	**target** - nazwa lub ID węzła (można uzyskać, uruchamiając ha_status)
ha_set_failover_delay=delay	Ustaw opóźnienie przełączenia awaryjnego wysokiej dostępności (HA). Obsługiwane są sufiksy czasu, np. 10s, 1m.	
proxy_config_cache_reload[=<**target**>]	Przeładuj pamięć podręczną konfiguracji proxy.	**target** - lista nazw proxy rozdzielona przecinkami Jeśli target nie zostanie określony, konfiguracja zostanie przeładowana dla wszystkich proxy
secrets_reload	Przeładuj sekrety z Vault.	
service_cache_reload	Przeładuj pamięć podręczną menedżera usług.	
snmp_cache_reload	Przeładuj pamięć podręczną SNMP — wyczyść właściwości silnika SNMP (czas silnika, liczba uruchomień silnika, ID silnika, poświadczenia) dla wszystkich hostów. Użyj, aby wymusić globalne wyczyszczenie pamięci podręcznej podczas rozwiązywania problemów z SNMP.	
housekeeper_execute	Uruchom procedurę housekeeping. Ignorowane, jeśli procedura housekeeping jest obecnie w toku.	
trigger_housekeeper_execute	Uruchom procedurę housekeeping dla wyzwalaczy procedurę housekeeping. Ignorowane, jeśli procedura housekeeping wyzwalaczy jest obecnie w toku.	
log_level_increase[=<**target**>]	Zwiększ poziom logowania; jeśli target nie zostanie określony, dotyczy to wszystkich procesów. Nieobsługiwane w systemach *BSD*.	**process type** - Wszystkie procesy określonego typu (np. poller) Zobacz wszystkie typy procesów serwera. **process type,N** - Typ procesu i numer (np. poller,3) **pid** - Identyfikator procesu (od 1 do 65535). Dla większych wartości określ target jako 'process type,N'.
log_level_decrease[=<**target**>]	Zmniejsz poziom logowania; jeśli target nie zostanie określony, dotyczy to wszystkich procesów. Nieobsługiwane w systemach *BSD*.	

Option	Description	Target
prof_enable[=<**target**>]	Włącz profilowanie. Jeśli target nie zostanie określony, dotyczy to wszystkich procesów. Włączone profilowanie dostarcza szczegóły wszystkich rwlocków/mutexów według nazwy funkcji.	**process type** - Wszystkie procesy określonego typu (np. history syncer) Obsługiwane typy procesów jako cele profilowania: alerter, alert manager, availability manager, configuration syncer, discovery manager, escalator, history poller, history syncer, housekeeper, http poller, icmp pinger, ipmi manager, ipmi poller, java poller, lld manager, lld worker, odbc poller, poller, preprocessing manager, preprocessing worker, proxy poller, self-monitoring, service manager, snmp trapper, task manager, timer, trapper, unreachable poller, vmware collector **process type,N** - Typ procesu i numer (np. history syncer,1) **pid** - Identyfikator procesu (od 1 do 65535). Dla większych wartości określ target jako 'process type,N'. **scope** - `rwlock`, `mutex`, `processing` mogą być używane z typem procesu i numerem (np. history syncer,1,processing) lub wszystkimi procesami danego typu (np. history syncer,rwlock)
prof_disable[=<**target**>]	Wyłącz profilowanie. Jeśli target nie zostanie określony, dotyczy to wszystkich procesów.	**process type** - Wszystkie procesy określonego typu (np. history syncer) Obsługiwane typy procesów jako cele profilowania: zobacz `prof_enable` **process type,N** - Typ procesu i numer (np. history syncer,1) **pid** - Identyfikator procesu (od 1 do 65535). Dla większych wartości określ target jako 'process type,N'.

Przykład użycia kontroli w czasie działania do przeładowania pamięci podręcznej konfiguracji serwera:

```
zabbix_server -c /usr/local/etc/zabbix_server.conf -R config_cache_reload
```

Przykłady użycia kontroli w czasie działania do przeładowania konfiguracji proxy:

```
### Przeładuj konfigurację wszystkich proxy:
zabbix_server -R proxy_config_cache_reload

### Przeładuj konfigurację Proxy1 i Proxy2:
zabbix_server -R proxy_config_cache_reload=Proxy1,Proxy2
```

Przykład użycia kontroli w czasie działania do wyczyszczenia pamięci podręcznej historii dla pozycji:

```
zabbix_server -c /usr/local/etc/zabbix_server.conf -R history_cache_clear=42243
```

Przykłady użycia kontroli w czasie działania do zebrania informacji diagnostycznych:

```
### Zbierz wszystkie dostępne informacje diagnostyczne w pliku dziennika serwera:
zabbix_server -R diaginfo

### Zbierz statystyki pamięci podręcznej historii w pliku dziennika serwera:
zabbix_server -R diaginfo=historycache
```

Przykład użycia kontroli w czasie działania do przeładowania pamięci podręcznej SNMP:

```
zabbix_server -R snmp_cache_reload
```

Attention:
Gdy interfejs SNMPv3 jest aktualizowany za pomocą interfejsu użytkownika Zabbix, Zabbix w większości przypadków automatycznie przeładuje nowe poświadczenia SNMPv3 dla tego interfejsu; używaj `-R snmp_cache_reload` tylko wtedy, gdy odpytywanie nadal kończy się niepowodzeniem po zmianie poświadczeń (na przykład z powodu niespójności engineBoots/engineID lub urządzeń niezgodnych z RFC), albo gdy trzeba wymusić globalne wyczyszczenie pamięci podręcznej SNMP na potrzeby rozwiązywania problemów.

Przykład użycia kontroli w czasie działania do wyzwolenia wykonania housekeepera:

```
zabbix_server -c /usr/local/etc/zabbix_server.conf -R housekeeper_execute
```

Przykłady użycia kontroli w czasie działania do zmiany poziomu logowania:

```
### Zwiększ poziom logowania wszystkich procesów:
zabbix_server -c /usr/local/etc/zabbix_server.conf -R log_level_increase

### Zwiększ poziom logowania drugiego procesu pollera:
zabbix_server -c /usr/local/etc/zabbix_server.conf -R log_level_increase=poller,2

### Zwiększ poziom logowania procesu o PID 1234:
zabbix_server -c /usr/local/etc/zabbix_server.conf -R log_level_increase=1234

### Zmniejsz poziom logowania wszystkich procesów http poller:
zabbix_server -c /usr/local/etc/zabbix_server.conf -R log_level_decrease="http poller"
```

Przykład ustawienia opóźnienia przełączenia awaryjnego HA na minimalne 10 sekund:

```
zabbix_server -R ha_set_failover_delay=10s
```

Użytkownik procesu

Serwer Zabbix został zaprojektowany do działania jako użytkownik niebędący rootem. Będzie działał jako dowolny użytkownik niebędący rootem, pod którym został uruchomiony. Dlatego możesz uruchomić serwer jako dowolnego użytkownika niebędącego rootem bez żadnych problemów.

Jeśli spróbujesz uruchomić go jako 'root', przełączy się na zakodowanego na stałe użytkownika 'zabbix', który musi być obecny w systemie. Możesz uruchomić serwer jako 'root' tylko wtedy, gdy odpowiednio zmodyfikujesz parametr 'AllowRoot' w pliku konfiguracyjnym serwera.

Jeśli serwer Zabbix i agent są uruchomione na tej samej maszynie, zaleca się użycie innego użytkownika do uruchamiania serwera niż do uruchamiania agenta. W przeciwnym razie, jeśli oba procesy są uruchomione jako ten sam użytkownik, agent może uzyskać dostęp do pliku konfiguracyjnego serwera, a każdy użytkownik z poziomem Admin w Zabbix może stosunkowo łatwo odczytać na przykład hasło do bazy danych.

Plik konfiguracyjny

Szczegółowe informacje na temat konfiguracji zabbix_server można znaleźć w opcjach pliku konfiguracyjnego.

Skrypty startowe

Skrypty są używane do automatycznego uruchamiania/zatrzymywania procesów Zabbix podczas uruchamiania/zamykania systemu. Skrypty znajdują się w katalogu misc/init.d.

Typy procesów serwera i wątki

- `agent poller` - asynchroniczny proces odpytywania dla pasywnych kontroli z wątkiem roboczym
- `alert manager` - menedżer kolejki alertów
- `alert syncer` - proces zapisujący alerty do bazy danych
- `alerter` - proces wysyłania powiadomień
- `availability manager` - proces aktualizacji dostępności hostów
- `browser poller` - proces odpytywania dla kontroli pozycji przeglądarki
- `configuration syncer` - proces zarządzania pamięcią podręczną danych konfiguracyjnych w pamięci
- `configuration syncer worker` - proces rozwiązywania i synchronizacji wartości makr użytkownika w nazwach pozycji
- `connector manager` - proces menedżera konektorów
- `connector worker` - proces obsługi żądań od menedżera konektorów
- `discovery manager` - proces menedżera wykrywania urządzeń
- `discovery worker` - proces obsługi zadań wykrywania od menedżera wykrywania

- escalator - proces eskalacji działań
- ha manager - proces zarządzania wysoką dostępnością
- history poller - proces obsługi kontroli obliczanych wymagających połączenia z bazą danych
- history syncer - proces zapisujący historię do bazy danych
- housekeeper - proces usuwania nieaktualnych danych (historii i trendów pozycji, sesji użytkowników, zdarzeń itp.), a także danych pozostawionych przez usunięte obiekty
- http agent poller - asynchroniczny proces odpytywania dla kontroli HTTP z wątkiem roboczym
- http poller - proces odpytywania monitorowania WWW
- icmp pinger - proces odpytywania dla kontroli icmpping
- internal poller - proces odpytywania dla kontroli wewnętrznych
- ipmi manager - menedżer procesów odpytywania IPMI
- ipmi poller - proces odpytywania dla kontroli IPMI
- java poller - proces odpytywania dla kontroli Java
- lld manager - proces menedżera zadań wykrywania niskiego poziomu
- lld worker - proces roboczy zadań wykrywania niskiego poziomu
- odbc poller - proces odpytywania dla kontroli ODBC
- poller - zwykły proces odpytywania dla pasywnych kontroli
- preprocessing manager - menedżer zadań przetwarzania wstępnego z wątkami roboczymi przetwarzania wstępnego
- preprocessing worker - wątek przetwarzania wstępnego danych
- proxy poller - proces odpytywania dla pasywnych proxy
- proxy group manager - menedżer równoważenia obciążenia proxy i wysokiej dostępności
- report manager- menedżer zadań generowania raportów cyklicznych
- report writer - proces generowania raportów cyklicznych
- self-monitoring - proces zbierania wewnętrznych statystyk serwera
- service manager - proces zarządzania usługami poprzez odbieranie informacji o problemach, tagach problemów i odtworzeniu problemów z history syncer, task manager i alert manager
- snmp poller - asynchroniczny proces odpytywania dla kontroli SNMP z wątkiem roboczym (tylko pozycje walk[OID] i get[OID])
- snmp trapper - trapper dla pułapek SNMP
- task manager - proces zdalnego wykonywania zadań żądanych przez inne komponenty (np. zamknięcie problemu, potwierdzenie problemu, sprawdzenie wartości pozycji teraz, funkcjonalność zdalnych poleceń)
- timer - timer do przetwarzania okresów utrzymania
- trapper - trapper dla aktywnych kontroli, trapów, komunikacji proxy
- trigger housekeeper - proces usuwania problemów i zdarzeń wygenerowanych przez wyzwalacze, które zostały od tego czasu usunięte
- unreachable poller - proces odpytywania dla nieosiągalnych urządzeń
- vmware collector - kolektor danych VMware odpowiedzialny za zbieranie danych z usług VMware

Plik dziennika serwera może być używany do obserwowania tych typów procesów.

Plik dziennika serwera jest tworzony z uprawnieniami odczytu i zapisu tylko dla właściciela pliku. Dodatkowo plik jest dostępny do odczytu dla grupy właściciela. Wszystkie pozostałe uprawnienia są zabronione.

Różne typy procesów serwera Zabbix mogą być monitorowane przy użyciu wewnętrznej **pozycji** zabbix\[process,<type>,<mode>,<stat
item.

Statystyki transakcji synchronizatora historii

Tytuł procesu synchronizatora historii wyświetla szczegółowe statystyki dotyczące transakcji synchronizatora historii:

```
205182 ?        S      0:00  zabbix_server: history syncer #2 [processed 0 values, 0+0 triggers in 0.00002
205183 ?        S      0:00  zabbix_server: history syncer #3 [processed 18 values, 7+0 triggers in 0.0026
205184 ?        S      0:00  zabbix_server: history syncer #4 [processed 0 values, 0+0 triggers in 0.00002
```

W „A+B triggers”:

- A - wyzwalacze przetworzone z powodu wartości historii;
- B - wyzwalacze przetworzone z powodu timerów.

Czasy w „processed...in N (<timings>) sec” oznaczają:

- Czas poświęcony na zapisywanie wartości pozycji do bazy danych;
- Czas poświęcony na aktualizację danych pozycji (stan, błędy, inwentarz hosta itp.);
- Czas poświęcony na opróżnianie trendów do bazy danych;
- Czas poświęcony na obliczanie wyzwalaczy;
- Czas poświęcony na przetwarzanie zdarzeń i akcji.

Procedura housekeeping

Proces housekeeper okresowo usuwa nieaktualne dane (historię i trendy pozycja, sesje użytkowników, zdarzenia itp.), a także dane pozostawione po usuniętych obiektach. Działa cyklicznie, a częstotliwość i limit usuwania na cykl są określane przez HousekeepingFrequency oraz MaxHousekeeperDelete. Wszelkie dane nieusunięte w jednym cyklu są przenoszone do następnego. Automatyczny housekeeping można włączyć i skonfigurować w *Administracja* > *Housekeeping*.

W celu usuwania danych pozostawionych po usuniętych obiektach proces housekeeper opiera się na zadaniach z tabeli housekeeper, która jest wypełniana przy każdym usunięciu obiektu. Na przykład po usunięciu hosta Zabbix usuwa również jego pozycje, ale nie ich historii, trendów ani problemów. Zamiast tego wyzwalacze bazy danych wypełniają tabelę housekeeper zadaniami składającymi się z następujących pól:

- housekeeperid - ID zadania
- object - typ obiektu (0 - pozycja; 1 - wyzwalacz; 2 - usługa; 3 - wykryty host; 4 - wykryta usługa)
- objectid - ID obiektu (pomaga procesowi housekeeper znaleźć dane powiązane z obiektem)

Na przykład usunięcie hosta z dwiema pozycjami i jednym wyzwalaczem wypełnia tabelę housekeeper w następujący sposób:

```
+---------------+--------+----------+
| housekeeperid | object | objectid |
+---------------+--------+----------+
|             1 |      1 |    28724 |
|             2 |      0 |    59396 |
|             3 |      0 |    59397 |
+---------------+--------+----------+
```

Wyzwalacze bazy danych wypełniają tabelę housekeeper bez sprawdzania danych powiązanych z obiektem; sprawdzenie to wykonuje proces housekeeper.

Każde zadanie skutkuje jedną lub większą liczbą operacji housekeeper, które zależą od typu obiektu:

- Dla pozycji (w tym reguł LLD) - usuwa dane ze wszystkich tabel historii i trendów (history, history_str, history_log, history_uint, history_text, history_bin, history_json, trends, trends_uint), które zawierają wartości dla tych pozycji. Dodatkowo sprawdza tabelę problems i usuwa nieaktualne zdarzenia wewnętrzne powiązane z tymi pozycjami.
- Dla wyzwalaczy - sprawdza tabele powiązane ze zdarzeniami (problem, event_symptom, event_recovery, events) i usuwa nieaktualne zdarzenia powiązane z tymi wyzwalaczami, a także powiadamia proces service manager o usuniętych zdarzeniach.

Note:
Oddzielny proces trigger housekeeper realizuje węższe zadanie — usuwa problemy i zdarzenia, które nie mają znanego źródłowego wyzwalacza. Częstotliwość jego uruchamiania jest kontrolowana przez ProblemHousekeepingFrequency.

 Do czasu uruchomienia procedury housekeeping wyzwalaczy problemy spowodowane przez wyzwalacze, które zostały już usunięte, mogą nadal generować problemy usług i przypisywać je do usług. Jeśli Twoja konfiguracja obejmuje wiele reguł obliczania statusu usług opartych na często wykrywanych/zanikających wyzwalaczach, rozważ zwiększenie częstotliwości procedury housekeeping przez dostosowanie parametru konfiguracyjnego serwer ProblemHousekeepingFrequency.

- Dla usług - sprawdza tabelę problems i usuwa nieaktualne zdarzenia usług, a także nieaktualne problemy usług, rozwiązując je tym samym w momencie działania housekeeping.
- Dla wykrywania sieci - usuwa nieaktualne zdarzenia wykrywania z tabeli problems.

Proces housekeeper usuwa tylko te zdarzenia, które nie są powiązane z problemami. Na przykład nieaktualne zdarzenie problemu/odzyskania nie zostanie usunięte, jeśli jest powiązane z otwartym problemem. Gdy proces housekeeper usuwa nieaktualne encje, najpierw usuwa problemy, a następnie zdarzenia.

Note:
Tabele używające trybu partition (tabele partycjonowane TimescaleDB) są pomijane; przetwarzane są tylko tabele używające trybu regular.

Obsługiwane platformy

Ze względu na wymagania bezpieczeństwa oraz krytyczny charakter działania serwera, UNIX jest jedynym systemem operacyjnym, który może konsekwentnie zapewniać wymaganą wydajność, odporność na awarie i niezawodność. Zabbix działa na wiodących na rynku wersjach systemu.

Serwer Zabbix jest testowany na następujących platformach:

- Linux
- Solaris

- AIX
- HP-UX
- Mac OS X
- FreeBSD
- OpenBSD
- NetBSD
- SCO Open Server

Note:
Zabbix może działać również na innych systemach operacyjnych typu Unix.

Ustawienia regionalne

Należy pamiętać, że serwer wymaga ustawień regionalnych UTF-8, aby niektóre tekstowe pozycje mogły być poprawnie interpretowane. Większość nowoczesnych systemów typu Unix ma domyślnie ustawienia regionalne UTF-8, jednak istnieją systemy, w których może być konieczne ich jawne skonfigurowanie.

1 Wysoka dostępność

Przegląd

Wysoka dostępność (HA) jest zwykle wymagana w infrastrukturach krytycznych, które mogą sobie pozwolić praktycznie na zerowy czas przestoju. Dlatego dla każdej usługi, która może ulec awarii, musi istnieć opcja przełączenia awaryjnego, aby przejąć jej działanie w przypadku awarii aktualnie działającej usługi.

Zabbix oferuje **natywne** rozwiązanie wysokiej dostępności, które jest łatwe w konfiguracji i nie wymaga wcześniejszej wiedzy specjalistycznej z zakresu HA. Natywne HA w Zabbix może być przydatne jako dodatkowa warstwa ochrony przed awariami oprogramowania/sprzętu serwer Zabbix lub w celu ograniczenia przestojów związanych z konserwacją.

W trybie wysokiej dostępności Zabbix wiele serwerów Zabbix działa jako węzły w klastrze. Gdy jeden serwer Zabbix w klastrze jest aktywny, pozostałe pozostają w trybie gotowości, gotowe do przejęcia jego roli w razie potrzeby.



Przejście na HA w Zabbix nie jest zobowiązujące. W dowolnym momencie można powrócić do pracy w trybie samodzielnym.

Zobacz także: Szczegóły implementacji

Włączanie wysokiej dostępności

Uruchamianie serwera Zabbix jako węzła klastra

Do uruchomienia serwera Zabbix jako węzła klastra wymagane są dwa parametry w konfiguracji serwera:

- Parametr **HANodeName** musi być określony dla każdego serwera Zabbix, który będzie węzłem klastra HA.

Jest to unikalny identyfikator węzła (np. `zabbix-node-01`), do którego serwer będzie się odwoływał w konfiguracjach agent i proxy. Jeśli nie określisz HANodeName, serwer zostanie uruchomiony w trybie samodzielnym.

- Parametr **NodeAddress** musi być określony dla każdego węzła.

Parametr NodeAddress (adres:port) będzie używany przez frontend Zabbix do łączenia się z aktywnym węzłem serwera. NodeAddress musi odpowiadać adresowi IP lub nazwie FQDN odpowiedniego serwera Zabbix.

Po wprowadzeniu zmian w plikach konfiguracyjnych uruchom ponownie wszystkie serwery Zabbix. Zostaną one teraz uruchomione jako węzły klastra. Nowy stan serwerów można zobaczyć w sekcji *Raporty* → *Informacje o systemie*, a także po uruchomieniu:

```
zabbix_server -R ha_status
```

To polecenie runtime zapisze bieżący stan klastra HA w logu serwera Zabbix (oraz na stdout):

```
Failover delay: 60 seconds
Cluster status:
   #  ID                        Name                Address                Status      Last Access
   1. ckzxxqg7u0001lsropenyzh3m zabbix-node-01      64.227.66.193:10051    standby     0s
   2. ckzxyqo1k00013frpq539e1jp zabbix-node-02      64.227.74.25:10051     active      3s
```

Przygotowanie frontend

Upewnij się, że adres:port serwera Zabbix **nie jest zdefiniowany** w konfiguracji frontendu (znajdującej się w `conf/zabbix.conf.php` w katalogu plików frontendu).

```
// Uncomment and set to desired values to override Zabbix hostname/IP and port.
// $ZBX_SERVER                  = '';
// $ZBX_SERVER_PORT             = '';
```

Frontend Zabbix automatycznie wykryje aktywny węzeł, odczytując ustawienia z tabeli nodes w bazie danych Zabbix. Adres węzła aktywnego zostanie użyty jako adres serwera Zabbix.

Konfiguracja proxy

Węzły klastra HA (serwery) muszą być wymienione w konfiguracji pasywnego lub aktywnego proxy Zabbix.

W przypadku pasywnego proxy nazwy węzłów muszą być podane w parametrze Server parameter proxy, oddzielone **przecinkiem**.

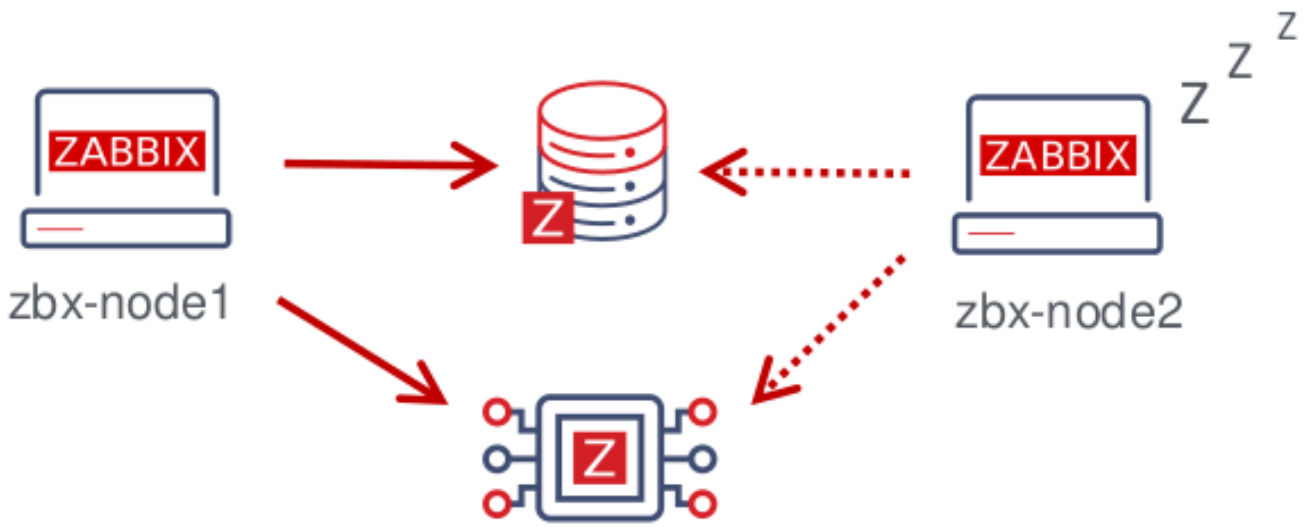
```
Server=zabbix-node-01,zabbix-node-02
```

W przypadku aktywnego proxy nazwy węzłów muszą być podane w parametrze Server parameter proxy, oddzielone **średnikiem**.

```
Server=zabbix-node-01;zabbix-node-02
```

Konfiguracja agenta

Węzły klastra HA (serwery) muszą być wymienione w konfiguracji Zabbix agent lub Zabbix agent 2.



Aby włączyć sprawdzenia pasywne, nazwy węzłów muszą być wymienione w parametrze Server parameter, oddzielone **przecinkiem**.

```
Server=zabbix-node-01,zabbix-node-02
```

Aby włączyć sprawdzenia aktywne, nazwy węzłów muszą być wymienione w parametrze ServerActive parameter. Należy pamiętać, że w przypadku sprawdzeń aktywnych węzły muszą być oddzielone przecinkiem od wszelkich innych serwerów, natomiast same węzły muszą być oddzielone **średnikiem**, np.:

```
ServerActive=zabbix-node-01;zabbix-node-02
```

Przełączenie awaryjne na węzeł zapasowy

Zabbix automatycznie przełączy się awaryjnie na inny węzeł, jeśli aktywny węzeł przestanie działać. Aby przełączenie awaryjne mogło nastąpić, co najmniej jeden węzeł musi mieć status standby.

Jak szybko nastąpi przełączenie awaryjne? Wszystkie węzły aktualizują czas ostatniego dostępu (oraz status, jeśli uległ zmianie) co 5 sekund. Zatem:

- Jeśli aktywny węzeł zostanie wyłączony i zdoła zgłosić swój status jako "stopped", inny węzeł przejmie jego rolę w ciągu **5 sekund**.
- Jeśli aktywny węzeł zostanie wyłączony lub stanie się niedostępny bez możliwości zaktualizowania swojego statusu, węzły standby będą czekać **opóźnienie przełączenia awaryjnego** + 5 sekund, zanim przejmą jego rolę

Opóźnienie przełączenia awaryjnego jest konfigurowalne, a obsługiwany zakres wynosi od 10 sekund do 15 minut (domyślnie jedna minuta). Aby zmienić opóźnienie przełączenia awaryjnego, można uruchomić:

```
zabbix_server -R ha_set_failover_delay=5m
```

Zarządzanie klastrem HA

Bieżący stan klastra HA można zarządzać za pomocą dedykowanych opcji kontroli w czasie działania:

- `ha_status` — zapisuje stan klastra HA w logu serwera Zabbix (oraz na stdout)
- `ha_remove_node=target` — usuwa węzeł HA zidentyfikowany przez <target> — nazwę lub ID węzła (nazwę/ID można uzyskać z danych wyjściowych polecenia ha_status), np.:

```
zabbix_server -R ha_remove_node=zabbix-node-02
```

Należy pamiętać, że aktywne/zapasowe węzły nie mogą zostać usunięte.

- `ha_set_failover_delay=delay` — ustawia opóźnienie przełączenia awaryjnego HA (od 10 sekund do 15 minut; obsługiwane są sufiksy czasu, np. 10s, 1m)

Stan węzłów można monitorować:

- w *Raporty* → *Informacje o systemie*
- w widżecie pulpitu *Informacje o systemie*
- za pomocą opcji kontroli w czasie działania `ha_status` serwera (zobacz powyżej).

Wewnętrzna pozycja `zabbix[cluster,discovery,nodes]` może być używana do wykrywania węzłów, ponieważ zwraca JSON z informacjami o węzłach wysokiej dostępności.

Wyłączanie klastra HA

Aby wyłączyć klaster wysokiej dostępności:

- wykonaj kopie zapasowe plików konfiguracyjnych
- zatrzymaj węzły zapasowe
- usuń parametr HANodeName z aktywnego głównego serwera
- uruchom ponownie główny serwer (zostanie uruchomiony w trybie samodzielnym)

Aktualizacja klastra HA

Aby przeprowadzić aktualizację głównej wersji dla węzłów HA:

- zatrzymaj wszystkie węzły;
- utwórz pełną kopię zapasową bazy danych;
- jeśli baza danych używa replikacji, upewnij się, że wszystkie węzły są zsynchronizowane i nie występują żadne problemy. Nie przeprowadzaj aktualizacji, jeśli replikacja jest uszkodzona.
- wybierz jeden węzeł, który przeprowadzi aktualizację bazy danych, zmień jego konfigurację na tryb standalone, komentując parametr HANodeName, i zaktualizuj go;
- upewnij się, że aktualizacja bazy danych została w pełni zakończona (*Informacje o systemie* powinny wskazywać, że serwer Zabbix jest uruchomiony);
- uruchom ponownie węzeł w trybie HA;
- zaktualizuj i uruchom pozostałe węzły (nie ma potrzeby przełączania ich do trybu standalone, ponieważ na tym etapie baza danych jest już zaktualizowana).

W przypadku aktualizacji wersji pobocznej wystarczy zaktualizować pierwszy węzeł, upewnić się, że został zaktualizowany i działa, a następnie rozpocząć aktualizację kolejnego węzła.

Szczegóły implementacji

Klaster wysokiej dostępności (HA) jest rozwiązaniem opcjonalnym i jest obsługiwany dla serwera Zabbix. Natywne rozwiązanie HA zostało zaprojektowane tak, aby było proste w użyciu, działało między lokalizacjami i nie miało szczególnych wymagań wobec baz

danych obsługiwanych przez Zabbix. Użytkownicy mogą korzystać z natywnego rozwiązania Zabbix HA lub z rozwiązania HA innej firmy, w zależności od tego, co najlepiej odpowiada wymaganiom wysokiej dostępności w ich środowisku.

Rozwiązanie składa się z wielu instancji zabbix_server lub węzłów. Każdy węzeł:

- jest konfigurowany oddzielnie
- używa tej samej bazy danych
- może działać w kilku trybach: active, standby, unavailable, stopped

W danym momencie aktywny (działający) może być tylko jeden węzeł. Węzeł standby uruchamia tylko jeden proces — menedżera HA. Węzeł standby nie zbiera danych, nie przetwarza ich ani nie wykonuje innych regularnych działań serwera; nie nasłuchuje na portach; ma minimalną liczbę połączeń z bazą danych.

Zarówno węzły active, jak i standby aktualizują czas ostatniego dostępu co 5 sekund. Każdy węzeł standby monitoruje czas ostatniego dostępu aktywnego węzła. Jeśli czas ostatniego dostępu aktywnego węzła przekroczy wartość 'failover delay' sekund, węzeł standby przełącza się na aktywny i przypisuje status 'unavailable' wcześniej aktywnemu węzłowi.

Aktywny węzeł monitoruje własną łączność z bazą danych — jeśli zostanie ona utracona na dłużej niż `failover delay`−5 sekund, musi zatrzymać całe przetwarzanie i przełączyć się w tryb standby. Aktywny węzeł monitoruje również status węzłów standby — jeśli czas ostatniego dostępu węzła standby przekroczy wartość 'failover delay' sekund, temu węzłowi standby zostaje przypisany status 'unavailable'.

Węzły zostały zaprojektowane tak, aby były kompatybilne między pomniejszymi wersjami Zabbix.

2 Agent

Przegląd

Agent Zabbix jest wdrażany na monitorowanym celu, aby aktywnie monitorować lokalne zasoby i aplikacje (dyski twarde, pamięć, statystyki procesora itp.).

Agent lokalnie zbiera informacje operacyjne i przekazuje dane do serwer Zabbix w celu dalszego przetwarzania. W przypadku awarii (takich jak zapełnienie dysku twardego lub awaria procesu usługi) serwer Zabbix może aktywnie powiadamiać administratorów konkretnej maszyny, która zgłosiła awarię.

Agenty Zabbix są bardzo wydajne dzięki wykorzystaniu natywnych wywołań systemowych do zbierania informacji statystycznych.

Kontrole pasywne i aktywne

Agenty Zabbix mogą wykonywać kontrole pasywne i aktywne:

- Kontrole pasywne — agent Zabbix odpowiada na żądanie z serwera Zabbix (lub proxy). Na przykład serwer żąda danych (np. obciążenia CPU), a agent zwraca wynik.
- Kontrole aktywne — agent Zabbix zbiera i wysyła dane bez oczekiwania na żądanie z serwera Zabbix (lub proxy). Najpierw pobiera z serwera listę monitorowanych pozycji (obciążenie CPU, dostępna pamięć itp.), a następnie zbiera wymagane dane i okresowo odsyła do niego nowe wartości.

Typ kontroli agenta konfiguruje się przez wybranie odpowiedniego monitorowanego typu pozycji. Agent Zabbix przetwarza pozycje typu „Agent Zabbix" lub „Agent Zabbix (aktywny)".

Obsługiwane platformy

Informacje o obsługiwanych platformach można znaleźć na stronie Wymagania.

Agent w systemach typu UNIX

Agent Zabbix w systemach typu UNIX jest uruchamiany na monitorowanym hoście.

Instalacja

Zabbix agent można zainstalować w systemach opartych na Linuksie, korzystając z jednej z następujących metod:

- Pakiety Zabbix — wybierz komponent Agent (po wybraniu wersji Zabbix, dystrybucji systemu operacyjnego i wersji systemu operacyjnego) i postępuj zgodnie z podanymi instrukcjami.
- Źródła Zabbix — pobierz pliki źródłowe i skompiluj Zabbix agent, konfigurując źródła z opcją `--enable-agent`.

Attention:
Ogólnie rzecz biorąc, 32-bitowe agenty Zabbix będą działać w systemach 64-bitowych, ale w niektórych przypadkach mogą zawieść.

Note:
Wstępnie skompilowane pliki binarne Zabbix agent są dostępne do pobrania dla systemów macOS, IBM AIX, FreeBSD, OpenBSD i Solaris. Starsze pliki binarne, zgodne z obecną wersją serwera/proxy Zabbix, są dostępne dla systemów NetBSD i HP-UX.

Jeśli zainstalowano jako pakiet

Agent Zabbix działa jako proces demona. Agent można uruchomić, wykonując:

```
systemctl start zabbix-agent
```

To zadziała w większości systemów GNU/Linux. W innych systemach może być konieczne uruchomienie:

```
/etc/init.d/zabbix-agent start
```

Aby zatrzymać, uruchomić ponownie lub sprawdzić status agenta Zabbix, użyj następujących poleceń:

```
systemctl stop zabbix-agent
systemctl restart zabbix-agent
systemctl status zabbix-agent
```

Uruchamianie ręczne

Możesz uruchomić agent Zabbix, lokalizując plik binarny `zabbix_agentd` i uruchamiając go bezpośrednio; na przykład:

```
zabbix_agentd
```

Agent w systemach Windows

Agent Zabbix w systemach Windows działa jako usługa systemu Windows.

Instalacja

Agent Zabbix można zainstalować w systemie Windows, korzystając z jednej z następujących metod:

- Wstępnie skompilowane pliki binarne agenta Zabbix — pobierz pakiet instalatora MSI agenta Zabbix i postępuj zgodnie z instrukcjami na stronie Instalacja agenta Windows z pakietu MSI.
- Źródła Zabbix — pobierz pliki źródłowe i postępuj zgodnie z instrukcjami na stronie Budowanie agenta Zabbix w systemie Windows.

Dodatkowe informacje na temat instalacji agenta Zabbix (z archiwum ZIP) jako usługi systemu Windows można znaleźć na stronie Agent Zabbix w systemie Microsoft Windows.

Opcje

Możliwe jest uruchomienie wielu instancji agent na hoście. Pojedyncza instancja może używać domyślnego pliku konfiguracyjnego lub pliku konfiguracyjnego określonego w wierszu poleceń. W przypadku wielu instancji każda instancja agent musi mieć własny plik konfiguracyjny (jedna z instancji może używać domyślnego pliku konfiguracyjnego).

Następujące parametry wiersza poleceń mogą być używane z Zabbix agent:

Parameter	Description
UNIX and Windows agent	
-c --config <config-file>	Ścieżka do pliku konfiguracyjnego. Możesz użyć tej opcji, aby wskazać plik konfiguracyjny inny niż domyślny. W systemach UNIX domyślną wartością jest /usr/local/etc/zabbix_agentd.conf lub wartość ustawiona przez zmienne compile-time *--sysconfdir* lub *--prefix* W systemie Windows domyślną wartością jest C:\Program Files\Zabbix Agent\zabbix_agentd.conf
-f --foreground	Uruchom Zabbix agent na pierwszym planie (domyślnie: true).
-p --print	Wyświetl znane pozycje i zakończ działanie. *Uwaga*: Aby zwracać również wyniki user parameter, musisz podać plik konfiguracyjny (jeśli nie znajduje się w domyślnej lokalizacji).
-t --test <item key>	Przetestuj określoną pozycję i zakończ działanie. *Uwaga*: Aby zwracać również wyniki user parameter, musisz podać plik konfiguracyjny (jeśli nie znajduje się w domyślnej lokalizacji).
-T --test-config	Sprawdź poprawność pliku konfiguracyjnego i zakończ działanie.
-h --help	Wyświetl informacje pomocy.
-V --version	Wyświetl numer wersji.
UNIX agent only	

Parameter	Description
-R --runtime-control <option>	Wykonaj funkcje administracyjne. Zobacz runtime control.
Windows agent only	
-m --multiple-agents	Użyj wielu instancji agent (z opcjami -i, -d, -s, -x). Aby rozróżnić nazwy usług instancji, każda nazwa usługi będzie zawierać wartość Hostname z określonego pliku konfiguracyjnego.
-S --startup-type <value>	Ustaw typ uruchamiania usługi Zabbix Windows agent. Dozwolone wartości: `automatic` - *(domyślnie)* uruchom usługę automatycznie podczas startu systemu Windows; `delayed` - opóźnij uruchomienie usługi do momentu zakończenia uruchamiania usług startowanych automatycznie (dostępne w Windows Server 2008/Vista i nowszych wersjach); `manual` - uruchom usługę ręcznie (przez użytkownika lub aplikację); `disabled` - wyłącz usługę, aby nie mogła zostać uruchomiona przez użytkownika lub aplikację. Możesz użyć tej opcji razem z opcją -i lub osobno, aby zmodyfikować typ uruchamiania już zainstalowanej usługi.
-i --install	Zainstaluj Zabbix Windows agent jako usługę.
-d --uninstall	Odinstaluj usługę Zabbix Windows agent.
-s --start	Uruchom usługę Zabbix Windows agent.
-x --stop	Zatrzymaj usługę Zabbix Windows agent.

Szczegółowe **przykłady** użycia parametrów wiersza poleceń:

- wyświetlenie wszystkich wbudowanych pozycji agent wraz z wartościami
- testowanie parametru użytkownika z kluczem ”mysql.ping” zdefiniowanym w określonym pliku konfiguracyjnym
- instalacja usługi ”Zabbix Agent” dla systemu Windows z użyciem domyślnej ścieżki do pliku konfiguracyjnego C:\Program Files\Zabbix Agent\zabbix_agentd.conf
- instalacja usługi ”Zabbix Agent [Hostname]” dla systemu Windows z użyciem pliku konfiguracyjnego zabbix_agentd.conf znajdującego się w tym samym folderze co plik wykonywalny agent oraz nadanie unikalnej nazwy usługi przez rozszerzenie jej o wartość Hostname z pliku konfiguracyjnego
- modyfikacja typu uruchamiania zainstalowanej usługi ”Zabbix Agent” dla systemu Windows z użyciem pliku konfiguracyjnego zabbix_agentd.conf znajdującego się w tym samym folderze co plik wykonywalny agent

```
zabbix_agentd --print
zabbix_agentd -t "mysql.ping" -c /etc/zabbix/zabbix_agentd.conf
zabbix_agentd.exe -i
zabbix_agentd.exe -i -m -c zabbix_agentd.conf
zabbix_agentd.exe -c zabbix_agentd.conf -S delayed
```

Sterowanie w czasie działania

Za pomocą opcji sterowania w czasie działania można zmienić poziom logowania procesów agent.

Opcja	Opis	Cel
log_level_increase[=<target>]	Zwiększa poziom logowania. Jeśli cel nie zostanie określony, zmiana dotyczy wszystkich procesów.	Cel można określić jako: **typ procesu** - wszystkie procesy określonego typu (np. listener) Zobacz wszystkie typy procesów agent. **typ procesu,N** - typ procesu i numer (np. listener,3) **pid** - identyfikator procesu (od 1 do 65535). Dla większych wartości określ cel jako „typ-procesu,N”.
log_level_decrease[=<target>]	Zmniejsza poziom logowania. Jeśli cel nie zostanie określony, zmiana dotyczy wszystkich procesów.	
userparameter_reload	Przeładowuje wartości opcji *UserParameter* i *Include* z bieżącego pliku konfiguracyjnego.	

Przykłady:

- zwiększenie poziomu logowania wszystkich procesów
- zwiększenie poziomu logowania trzeciego procesu listener
- zwiększenie poziomu logowania procesu o PID 1234

- zmniejszenie poziomu logowania wszystkich procesów aktywnych kontroli

```
zabbix_agentd -R log_level_increase
zabbix_agentd -R log_level_increase=listener,3
zabbix_agentd -R log_level_increase=1234
zabbix_agentd -R log_level_decrease="active checks"
```

Note:
Sterowanie w czasie działania nie jest obsługiwane w systemach OpenBSD, NetBSD i Windows.

Typy procesów agenta

- `active checks` — proces wykonujący aktywne sprawdzenia
- `collector` — proces do zbierania danych
- `listener` — proces nasłuchujący sprawdzeń pasywnych

Plik dziennika agenta może być używany do obserwowania tych typów procesów.

Plik dziennika agenta jest tworzony z uprawnieniami odczytu i zapisu tylko dla właściciela pliku. Dodatkowo plik jest dostępny do odczytu dla grupy właściciela. Wszystkie pozostałe uprawnienia są zabronione.

Użytkownik procesu

Agent Zabbix w systemach UNIX został zaprojektowany do działania jako użytkownik nieuprzywilejowany. Będzie działać jako dowolny użytkownik nieuprzywilejowany, z uprawnieniami którego został uruchomiony. Dlatego możesz uruchomić agent jako dowolnego użytkownika nieuprzywilejowanego bez żadnych problemów.

Jeśli spróbujesz uruchomić go jako „root", przełączy się na wpisanego na stałe użytkownika „zabbix", który musi istnieć w systemie. Możesz uruchomić agent jako „root" tylko wtedy, gdy odpowiednio zmodyfikujesz parametr „AllowRoot" w pliku konfiguracyjnym agenta.

Plik konfiguracyjny

Szczegółowe informacje na temat konfiguracji Zabbix agent można znaleźć w opcjach pliku konfiguracyjnego dla zabbix_agentd lub agenta Windows.

Ustawienia regionalne

Należy pamiętać, że agent wymaga ustawień regionalnych UTF-8, aby niektóre tekstowe pozycje agenta mogły zwracać oczekiwaną zawartość. Większość nowoczesnych systemów typu Unix domyślnie używa ustawień regionalnych UTF-8, jednak istnieją systemy, w których może być konieczne ich jawne skonfigurowanie.

Kod zakończenia

Zabbix agent zwraca 0 w przypadku pomyślnego zakończenia i 1 w przypadku niepowodzenia.

3 Agent 2

Przegląd

Zabbix agent 2 to nowa generacja Zabbix agent, napisana w Go (z wykorzystaniem części kodu C ponownie użytego z Zabbix agent). Został zaprojektowany, aby:

- Zmniejszyć liczbę połączeń TCP.
- Zapewnić lepszą współbieżność kontroli.
- Umożliwić łatwe rozszerzanie za pomocą wtyczek, które zapewniają proste kontrole przy minimalnej ilości kodu oraz obsługują złożone kontrole składające się z długotrwale działających skryptów i niezależnego zbierania danych z okresowym raportowaniem.
- Działać jako zamiennik Zabbix agent, obsługując wszystkie wcześniejsze funkcje.

Kontrole pasywne i aktywne

Zabbix agent 2 obsługuje kontrole pasywne i aktywne, podobnie jak Zabbix agent. Dodatkowo, kontrole aktywne Zabbix agent 2 obsługują elastyczne interwały/harmonogramy oraz współbieżność kontroli w ramach jednego aktywnego serwera.

Note:
Domyślnie po restarcie Zabbix agent 2 zaplanuje pierwsze pobranie danych dla kontroli aktywnych na warunkowo losowy moment w ramach interwału aktualizacji pozycji, aby zapobiec skokom wykorzystania zasobów. Aby wykonywać kontrole aktywne, które nie mają interwału aktualizacji *Scheduling* update interval bezpośrednio po restarcie agenta, ustaw parametr `ForceActiveChecksOnStart` (na poziomie globalnym) lub `Plugins.<Plugin name>.System.ForceActiveChecksOnStart` (wpływa tylko na kontrole określonej wtyczki) w pliku konfiguracyjnym. Parametr na poziomie wtyczki, jeśli jest ustawiony, zastąpi parametr globalny.

Współbieżność sprawdzeń

Sprawdzenia z różnych wtyczek mogą być wykonywane współbieżnie. Liczba współbieżnych sprawdzeń w ramach jednej wtyczki jest ograniczona przez ustawienie pojemności wtyczki. Każda wtyczka może mieć zakodowane na stałe ustawienie pojemności (domyślnie 1000), które można obniżyć za pomocą ustawienia `Plugins.<PluginName>.System.Capacity=N` w konfiguracyjnym parametrze *Plugins*.

Obsługiwane platformy

Informacje o obsługiwanych platformach można znaleźć na stronie Wymagania.

Agent 2 w systemach uniksopodobnych

Zabbix agent 2 w systemach uniksopodobnych jest uruchamiany na monitorowanym hoście.

Instalacja

Zabbix agent 2 można zainstalować w systemach opartych na Linuksie, korzystając z jednej z następujących metod:

- Pakiety Zabbix — wybierz komponent Agent 2 (po wybraniu wersji Zabbix, dystrybucji systemu operacyjnego i wersji systemu operacyjnego) i postępuj zgodnie z instrukcjami.
- Źródła Zabbix — pobierz pliki źródłowe i skompiluj agent, konfigurując go z opcją `--enable-agent2`.

Note:
Możliwości monitorowania Zabbix agent 2 można rozszerzyć za pomocą ładowalnych wtyczek, które są dostępne oddzielnie. Szczegółowe informacje można znaleźć w sekcji Ładowalne wtyczki.

Jeśli zainstalowano jako pakiet

Zabbix agent 2 działa jako proces pierwszoplanowy i polega na zewnętrznym menedżerze usług (np. systemd) w zakresie uruchamiania w tle; Zabbix agent 2 nie ma wbudowanej obsługi demonizacji w systemie Linux.

Agent można uruchomić, wykonując:

```
systemctl start zabbix-agent2
```

Aby zatrzymać, uruchomić ponownie lub sprawdzić stan Zabbix agent 2, użyj następujących poleceń:

```
systemctl stop zabbix-agent2
systemctl restart zabbix-agent2
systemctl status zabbix-agent2
```

Uruchamianie ręczne

Możesz uruchomić agent Zabbix, lokalizując plik binarny zabbix_agent2 i uruchamiając go bezpośrednio; na przykład:

```
zabbix_agent2
```

Agent 2 w systemach Windows

Zabbix agent 2 działa jako samodzielny proces; może jednak również działać jako usługa systemu Windows.

Instalacja

Zabbix agent 2 można zainstalować w systemie Windows, korzystając z jednej z następujących metod:

- Wstępnie skompilowane pliki binarne Zabbix agent - pobierz pakiet instalatora MSI agenta i postępuj zgodnie z instrukcjami na stronie Instalacja agenta Windows z pakietu MSI.
- Źródła Zabbix - pobierz pliki źródłowe i postępuj zgodnie z instrukcjami na stronie Kompilowanie Zabbix agent 2 w systemie Windows.

Note:
Możliwości monitorowania Zabbix agent 2 można rozszerzyć za pomocą ładowalnych wtyczek, które są dostępne oddzielnie. Szczegółowe informacje można znaleźć w sekcji Ładowalne wtyczki.

Dodatkowe informacje na temat instalacji Zabbix agent 2 (z archiwum ZIP) jako usługi systemu Windows można znaleźć na stronie Zabbix agent w systemie Microsoft Windows.

Opcje

Następujące parametry wiersza poleceń mogą być używane z Zabbix agent 2:

Parameter	Description
UNIX and Windows agent	
-c --config <config-file>	Ścieżka do pliku konfiguracyjnego. Możesz użyć tej opcji, aby wskazać plik konfiguracyjny inny niż domyślny. W systemach UNIX domyślną wartością jest /usr/local/etc/zabbix_agent2.conf lub wartość ustawiona przez zmienne compile-time *--sysconfdir* lub *--prefix* W systemie Windows domyślną wartością jest C:\Program Files\Zabbix Agent 2\zabbix_agent2.conf
-f --foreground	Uruchom Zabbix agent na pierwszym planie (domyślnie: true).
-p --print	Wyświetl znane pozycje i zakończ. *Uwaga*: Aby zwracać również wyniki parametrów użytkownika, musisz określić plik konfiguracyjny (jeśli nie znajduje się w domyślnej lokalizacji).
-t --test <item key>	Przetestuj określoną pozycję i zakończ. *Uwaga*: Aby zwracać również wyniki parametrów użytkownika, musisz określić plik konfiguracyjny (jeśli nie znajduje się w domyślnej lokalizacji).
-T --test-config	Zweryfikuj plik konfiguracyjny i zakończ.
-h --help	Wyświetl informacje pomocy i zakończ.
-v --verbose	Wyświetl informacje debugowania. Używaj tej opcji z opcjami -p i -t.
-V --version	Wyświetl wersję agent oraz informacje o licencji.
-R --runtime-control <option>	Wykonaj funkcje administracyjne. Zobacz runtime control.
Windows agent only	
-m --multiple-agents	Używaj wielu instancji agent (z opcjami -i, -d, -s, -x). Aby rozróżnić nazwy usług instancji, każda nazwa usługi będzie zawierać wartość Hostname z określonego pliku konfiguracyjnego.
-S --startup-type <value>	Ustaw typ uruchamiania usługi Zabbix Windows agent. Dozwolone wartości: `automatic` - *(domyślnie)* uruchom usługę automatycznie podczas startu systemu Windows; `delayed` - opóźnij uruchomienie usługi do momentu zakończenia uruchamiania usług startowanych automatycznie; `manual` - uruchom usługę ręcznie (przez użytkownika lub aplikację); `disabled` - wyłącz usługę, aby nie mogła zostać uruchomiona przez użytkownika lub aplikację. Możesz użyć tej opcji razem z opcją -i lub osobno, aby zmodyfikować typ uruchamiania już zainstalowanej usługi.
-i --install	Zainstaluj Zabbix Windows agent jako usługę.
-d --uninstall	Odinstaluj usługę Zabbix Windows agent.
-s --start	Uruchom usługę Zabbix Windows agent.
-x --stop	Zatrzymaj usługę Zabbix Windows agent.

Konkretne **przykłady** użycia parametrów wiersza poleceń:

- wyświetlenie wszystkich wbudowanych pozycji agent wraz z wartościami
- przetestowanie parametru użytkownika z kluczem ”mysql.ping” zdefiniowanym w określonym pliku konfiguracyjnym
- instalacja usługi ”Zabbix Agent” dla systemu Windows przy użyciu domyślnej ścieżki do pliku konfiguracyjnego C:\Program Files\Zabbix Agent 2\zabbix_agent2.conf
- modyfikacja typu uruchamiania zainstalowanej usługi ”Zabbix Agent” dla systemu Windows przy użyciu pliku konfiguracyjnego zabbix_agent2.conf znajdującego się w tym samym folderze co plik wykonywalny agent

```
zabbix_agent2 --print
zabbix_agent2 -t "mysql.ping" -c /etc/zabbix/zabbix_agentd.conf
zabbix_agent2.exe -i
zabbix_agent2.exe -c zabbix_agent2.conf -S delayed
```

Kontrola w czasie działania

Kontrola w czasie działania udostępnia kilka opcji zdalnego sterowania.

Opcja	Opis
log_level_increase	Zwiększ poziom logowania.
log_level_decrease	Zmniejsz poziom logowania.
metrics	Wyświetl listę dostępnych metryk.
version	Wyświetl wersję agenta.
userparameter_reload	Przeładuj wartości opcji *UserParameter* i *Include* z bieżącego pliku konfiguracyjnego.
help	Wyświetl informacje pomocy dotyczące kontroli w czasie działania.

Przykłady:

- zwiększenie poziomu logowania dla agenta 2
- wyświetlenie opcji kontroli w czasie działania

```
zabbix_agent2 -R log_level_increase
zabbix_agent2 -R help
```

Plik konfiguracyjny

Parametry konfiguracyjne agent 2 są w większości zgodne z Zabbix agent, z kilkoma wyjątkami.

Nowe parametry	Opis
ControlSocket	Ścieżka do gniazda sterowania w czasie działania. Agent 2 używa gniazda sterowania do poleceń wykonywanych w czasie działania.
EnablePersistentBuffer, *PersistentBufferFile*, *PersistentBufferPeriod*	Te parametry są używane do konfiguracji trwałej pamięci na agent 2 dla aktywnych pozycji.
ForceActiveChecksOnStart	Określa, czy agent powinien wykonywać aktywne testy natychmiast po restarcie, czy rozłożyć je równomiernie w czasie.
Plugins	Wtyczki mogą mieć własne parametry w formacie `Plugins.<Plugin name>.<Parameter>=<value>`. Wspólnym parametrem wtyczek jest *System.Capacity*, ustawiający limit testów, które mogą być wykonywane jednocześnie.
StatusPort	Port, na którym agent 2 będzie nasłuchiwał żądań statusu HTTP oraz wyświetlał listę skonfigurowanych wtyczek i niektóre parametry wewnętrzne
Usunięte parametry	**Opis**
AllowRoot, *User*	Nieobsługiwane, ponieważ daemonizacja nie jest obsługiwana.
LoadModule, *LoadModulePath*	Ładowalne moduły nie są obsługiwane.
StartAgents	Ten parametr był używany w Zabbix agent do zwiększenia współbieżności testów pasywnych lub ich wyłączenia. W Agent 2 współbieżność jest konfigurowana na poziomie wtyczki i może być ograniczona ustawieniem pojemności.

Aby uzyskać więcej informacji, zobacz opcje pliku konfiguracyjnego dla zabbix_agent2.

Kody wyjścia

Zabbix agent 2 może być również skompilowany ze starszymi wersjami OpenSSL (1.0.1, 1.0.2).

W takim przypadku Zabbix udostępnia muteksy do blokowania w OpenSSL. Jeśli zablokowanie lub odblokowanie muteksu zakończy się niepowodzeniem, w standardowym strumieniu błędów (STDERR) zostanie wyświetlony komunikat o błędzie, a Agent 2 zakończy działanie z kodem wyjścia odpowiednio 2 lub 3.

Agent vs agent 2 comparison

This section describes the differences between the Zabbix agent and the Zabbix agent 2.

Parameter	Zabbix agent	Zabbix agent 2
Programming language	C	Go with some parts in C
Daemonization	yes	by systemd only (yes on Windows)
Supported extensions	Custom loadable modules in C.	Custom plugins in Go.
Requirements		

Parameter	Zabbix agent	Zabbix agent 2
Supported platforms	Linux, IBM AIX, FreeBSD, NetBSD, OpenBSD, HP-UX, Mac OS X, Solaris: 9, 10, 11, Windows: all desktop and server versions since XP	Linux, Windows: all desktop and server versions, on which a supported Go version can be installed.
Supported crypto libraries	GnuTLS 3.1.18 and newer OpenSSL 1.0.1, 1.0.2, 1.1.0, 1.1.1, 3.0.x LibreSSL - tested with versions 2.7.4, 2.8.2 (certain limitations apply, see the Encryption page for details).	Linux: OpenSSL 1.0.1 and later. MS Windows: OpenSSL 1.1.1 or later. The OpenSSL library must have PSK support enabled. LibreSSL is not supported.
Monitoring processes		
Processes	A separate active check process for each server/proxy record.	Single process with automatically created threads. The maximum number of threads is determined by the GOMAXPROCS environment variable.
Metrics	**UNIX**: see a list of supported items. **Windows**: see a list of additional Windows-specific items.	**UNIX**: All metrics supported by Zabbix agent. Additionally, the agent 2 provides Zabbix-native monitoring solution for: Docker, Memcached, MySQL, PostgreSQL, Redis, systemd, and other monitoring targets - see a full list of agent 2 specific items. **Windows**: All metrics supported by Zabbix agent, and also net.tcp.service* checks of HTTPS, LDAP. Additionally, the agent 2 provides Zabbix-native monitoring solution for: PostgreSQL, Redis.
Concurrency	Active checks for single server are executed sequentially.	Checks from different plugins or multiple checks within one plugin can be executed concurrently.
Third-party traps	no	yes
Additional features		
Persistent storage	no	yes
Persistent files for log*[] metrics	yes (only on Unix)	no
Log data upload	Can be performed during log gathering to free the buffer.	Log gathering is stopped when the buffer is full, therefore the BufferSize parameter must be at least MaxLinesPerSecond x 2.
Changes user at runtime	yes (Unix-like systems only)	no (controlled by systemd)
User-configurable ciphersuites	yes	no

See also:

- *Zabbix processes description*: Zabbix agent, Zabbix agent 2
- *Configuration parameters*: Zabbix agent UNIX / Windows, Zabbix agent 2 UNIX / Windows

Built-in plugins

These plugins are built into Zabbix agent 2 and are available out-of-the-box. Click on the plugin name to go to the plugin repository with additional information.

Plugin name	Description	Supported item keys	Comments
Agent	Metrics of the Zabbix agent being used.	agent.hostname, agent.ping, agent.version	Supported keys have the same parameters as Zabbix agent keys.

Plugin name	Description	Supported item keys	Comments
CPU	System CPU monitoring (number of CPUs/CPU cores, discovered CPUs, utilization percentage).	system.cpu.discovery, system.cpu.num, system.cpu.util	Supported keys have the same parameters as Zabbix agent keys.
Docker	Monitoring of Docker containers.	docker.container_info, docker.container_stats, docker.containers, docker.containers.discovery, docker.data_usage, docker.images, docker.images.discovery, docker.info, docker.ping	See also: Configuration parameters
File	File metrics collection.	vfs.file.cksum, vfs.file.contents, vfs.file.exists, vfs.file.md5sum, vfs.file.regexp, vfs.file.regmatch, vfs.file.size, vfs.file.time	Supported keys have the same parameters as Zabbix agent keys.
Kernel	Kernel monitoring.	kernel.maxfiles, kernel.maxproc	Supported keys have the same parameters as Zabbix agent keys.
Log	Log file monitoring.	log, log.count, logrt, logrt.count	Supported keys have the same parameters as Zabbix agent keys. See also: Plugin configuration parameters (Unix/Windows)
Memcached	Memcached server monitoring.	memcached.ping, memcached.stats	
Modbus	Reads Modbus data.	modbus.get	Supported keys have the same parameters as Zabbix agent keys.
MQTT	Receives published values of MQTT topics.	mqtt.get	To configure an encrypted connection to the MQTT broker, specify TLS parameters in the agent configuration file as a named session or default parameters. Currently TLS parameters cannot be passed as item key parameters.
MySQL	Monitoring of MySQL and its forks.	mysql.custom.query, mysql.db.discovery, mysql.db.size, mysql.get_status_variables, mysql.ping, mysql.replication.discovery, mysql.replication.get_slave_status, mysql.version	To configure an encrypted connection to the database, specify TLS parameters in the agent configuration file as a named session or default parameters. Currently TLS parameters cannot be passed as item key parameters.
NetIf	Monitoring of network interfaces.	net.if.collisions, net.if.discovery, net.if.in, net.if.out, net.if.total	Supported keys have the same parameters as Zabbix agent keys.

Plugin name	Description	Supported item keys	Comments
Oracle	Oracle Database monitoring.	oracle.diskgroups.stats, oracle.diskgroups.discovery, oracle.archive.info, oracle.archive.discovery, oracle.cdb.info, oracle.custom.query, oracle.datafiles.stats, oracle.db.discovery, oracle.fra.stats, oracle.instance.info, oracle.pdb.info, oracle.pdb.discovery, oracle.pga.stats, oracle.ping, oracle.proc.stats, oracle.redolog.info, oracle.sga.stats, oracle.sessions.stats, oracle.sys.metrics, oracle.sys.params, oracle.ts.stats, oracle.ts.discovery, oracle.user.info, oracle.version	Install the Oracle Instant Client before using the plugin.
Proc	Process CPU utilization percentage.	proc.cpu.util	Supported key has the same parameters as Zabbix agent key.
Redis	Redis server monitoring.	redis.config, redis.info, redis.ping, redis.slowlog.count	To configure an encrypted connection to Redis, specify TLS parameters in the agent configuration file as a named session or default parameters. TLS parameters cannot be passed as item key parameters. Note that an incorrect or otherwise invalid TLS configuration can prevent Zabbix agent 2 from starting, so verify certificate files, permissions and paths before enabling TLS.

Smart	S.M.A.R.T. monitoring.	smart.attribute.discovery, smart.disk.discovery, smart.disk.get	The minimum required smartctl version is 7.1.
			Sudo/root access rights to smartctl are required for the user executing Zabbix agent 2. The plugin uses only the following commands:
			`/usr/sbin/smartctl -a *`
			`/usr/sbin/smartctl --scan *`
			`/usr/sbin/smartctl -j -V`
			
			Supported keys can be used with Zabbix agent 2 only on Linux/Windows, both as a passive and active check.
			See also:
			Configuration parameters

SW	Listing of installed packages.	system.sw.packages, system.sw.packages.get	The supported keys have the same parameters as Zabbix agent key.
Swap	Swap space size in bytes/percentage.	system.swap.size	Supported key has the same parameters as Zabbix agent key.
SystemRun	Runs specified command.	system.run	Supported key has the same parameters as Zabbix agent key. See also: Plugin configuration parameters (Unix/Windows)

Plugin name	Description	Supported item keys	Comments
Systemd	Monitoring of systemd services.	systemd.unit.discovery, systemd.unit.get, systemd.unit.info	
TCP	TCP connection availability check.	net.tcp.port	Supported key has the same parameters as Zabbix agent key.
UDP	Monitoring of the UDP services availability and performance.	net.udp.service, net.udp.service.perf	Supported keys have the same parameters as Zabbix agent keys.
Uname	Retrieval of information about the system.	system.hostname, system.sw.arch, system.uname	Supported keys have the same parameters as Zabbix agent keys.
Uptime	System uptime metrics collection.	system.uptime	Supported key has the same parameters as Zabbix agent key.
VFSDev	VFS metrics collection.	vfs.dev.discovery, vfs.dev.read, vfs.dev.write	Supported keys have the same parameters as Zabbix agent keys.
WebCertificate	Monitoring of TLS/SSL website certificates.	web.certificate.get	
WebPage	Web page monitoring.	web.page.get, web.page.perf, web.page.regexp	Supported keys have the same parameters as Zabbix agent keys.
ZabbixAsync	Asynchronous metrics collection.	net.tcp.listen, net.udp.listen, sensor, system.boottime, system.cpu.intr, system.cpu.load, system.cpu.switches, system.hw.cpu, system.hw.macaddr, system.localtime, system.sw.os, system.swap.in, system.swap.out, vfs.fs.discovery	Supported keys have the same parameters as Zabbix agent keys.
ZabbixStats	Zabbix server/proxy internal metrics or number of delayed items in a queue.	zabbix.stats	Supported keys have the same parameters as Zabbix agent keys.
ZabbixSync	Synchronous metrics collection.	net.dns, net.dns.record, net.tcp.service, net.tcp.service.perf, proc.mem, proc.num, system.hw.chassis, system.hw.devices, system.sw.packages, system.users.num, vfs.dir.count, vfs.dir.size, vfs.fs.get, vfs.fs.inode, vfs.fs.size, vm.memory.size.	Supported keys have the same parameters as Zabbix agent keys.

Loadable plugins

Loadable plugins are not available out-of-the-box for Zabbix agent 2 and need to be installed separately:

- On Linux, you can use packages (e.g., install Ember+ on Ubuntu with `apt install zabbix-agent2-plugin-ember-plus`) or build plugins
- On Windows, you can install from MSI or build plugins

Attention:
Before installing a plugin, please check its README file. It may contain specific requirements and installation instructions.

Click on the plugin name to go to the plugin repository, which contains the plugin README file with additional information.

Plugin name	Description	Supported item keys	Comments
Ceph	Ceph monitoring.	ceph.df.details, ceph.osd.stats, ceph.osd.discovery, ceph.osd.dump, ceph.ping, ceph.pool.discovery, ceph.status	See also Ceph plugin configuration parameters.
Ember+	Monitoring of Ember+.	ember.get	See also Ember+ plugin configuration parameters.
MongoDB	Monitoring of MongoDB servers and clusters (document-based, distributed database).	mongodb.cfg.discovery, mongodb.collection.stats, mongodb.collections.discovery, mongodb.collections.usage, mongodb.connpool.stats, mongodb.db.stats, mongodb.db.discovery, mongodb.jumbo_chunks.count, mongodb.oplog.stats, mongodb.ping, mongodb.rs.config, mongodb.rs.status, mongodb.server.status, mongodb.sh.discovery, mongodb.version	To configure encrypted connections to the database, specify TLS parameters in the agent configuration file as a named session parameters. Currently TLS parameters cannot be passed as item key parameters. See also MongoDB plugin configuration parameters.
MSSQL	Monitoring of MSSQL database.	mssql.availability.group.get, mssql.custom.query, mssql.db.get, mssql.job.status.get, mssql.last.backup.get, mssql.local.db.get, mssql.mirroring.get, mssql.nonlocal.db.get, mssql.perfcounter.get, mssql.ping, mssql.quorum.get, mssql.quorum.member.get, mssql.replica.get, mssql.version	To configure an encrypted connection to the database, specify TLS parameters in the agent configuration file as a named session or default parameters. Currently TLS parameters cannot be passed as item key parameters. See also MSSQL plugin configuration parameters.

Plugin name	Description	Supported item keys	Comments
NVIDIA GPU	Monitoring of NVIDIA GPU.	nvml.device.count, nvml.device.decoder.utilization, nvml.device.ecc.mode, nvml.device.encoder.stats.get, nvml.device.encoder.utilization, nvml.device.energy.consumption, nvml.device.errors.memory, nvml.device.errors.register, nvml.device.fan.speed.avg, nvml.device.get, nvml.device.graphics.frequency, nvml.device.memory.bar1.get, nvml.device.memory.fb.get, nvml.device.memory.frequency, nvml.device.pci.utilization, nvml.device.performance.state, nvml.device.power.limit, nvml.device.power.usage, nvml.device.serial, nvml.device.sm.frequency, nvml.device.temperature, nvml.device.utilization, nvml.device.video.frequency, nvml.system.driver.version, nvml.version	See also NVIDIA GPU plugin configuration parameters.
PostgreSQL	Monitoring of PostgreSQL and its forks.	pgsql.autovacuum.count, pgsql.archive, pgsql.bgwriter, pgsql.cache.hit, pgsql.connections, pgsql.custom.query, pgsql.dbstat, pgsql.dbstat.sum, pgsql.db.age, pgsql.db.bloating_tables, pgsql.db.discovery, pgsql.db.size, pgsql.locks, pgsql.oldest.xid, pgsql.ping, pgsql.queries, pgsql.replication.count, pgsql.replication.process, pgsql.replication.process.discovery, pgsql.replication.recovery_role, pgsql.replication.status, pgsql.replication_lag.b, pgsql.replication_lag.sec, pgsql.uptime, pgsql.version, pgsql.wal.stat	To configure encrypted connections to the database, specify TLS parameters in the agent configuration file as a named session or default parameters. Currently TLS parameters cannot be passed as item key parameters. See also PostgreSQL plugin configuration parameters.

Note:
Loadable plugins, when launched with:
 - `-V --version` - print plugin version and license information;
 - `-h --help` - print help information.
 - `-t, --test <item key>` — launch plugin for testing (plugin config ignored).

4 Proxy

Przegląd

Zabbix proxy to proces, który może zbierać dane monitoringu z jednego lub większej liczby monitorowanych urządzeń i wysyłać te informacje do serwera Zabbix, działając zasadniczo w imieniu serwera. Wszystkie zebrane dane są buforowane lokalnie, a następnie przesyłane do serwera Zabbix, do którego należy dany proxy.

Wdrożenie proxy jest opcjonalne, ale może być bardzo korzystne dla rozłożenia obciążenia pojedynczego serwera Zabbix. Jeśli dane zbierają wyłącznie proxy, przetwarzanie na serwerze wymaga mniej zasobów CPU i operacji wejścia/wyjścia dysku.

Zabbix proxy jest idealnym rozwiązaniem do scentralizowanego monitorowania zdalnych lokalizacji, oddziałów i sieci bez lokalnych administratorów.

Zabbix proxy wymaga oddzielnej bazy danych.

Attention:
Należy pamiętać, że bazami danych obsługiwanymi przez Zabbix proxy są SQLite, MySQL i PostgreSQL.

Zobacz także: Używanie proxy w środowisku rozproszonym

Uruchamianie proxy

Jeśli zainstalowano jako pakiet

Zabbix proxy działa jako proces demona. Proxy można uruchomić, wykonując:

```
systemctl start zabbix-proxy
```

To zadziała w większości systemów GNU/Linux. W innych systemach może być konieczne uruchomienie:

```
/etc/init.d/zabbix-proxy start
```

Podobnie, aby zatrzymać/uruchomić ponownie/wyświetlić status Zabbix proxy, użyj następujących poleceń:

```
systemctl stop zabbix-proxy
systemctl restart zabbix-proxy
systemctl status zabbix-proxy
```

Uruchom ręcznie

Jeśli powyższe nie działa, musisz uruchomić go ręcznie. Znajdź ścieżkę do pliku binarnego zabbix_proxy i wykonaj:

```
zabbix_proxy
```

Możesz użyć następujących parametrów wiersza poleceń z Zabbix proxy:

```
-c --config <file>              ścieżka do pliku konfiguracyjnego
-f --foreground                 uruchom Zabbix proxy na pierwszym planie
-R --runtime-control <option>   wykonaj funkcje administracyjne
-T --test-config                sprawdź poprawność pliku konfiguracyjnego i zakończ
-h --help                       wyświetl tę pomoc
-V --version                    wyświetl numer wersji
```

Przykłady uruchamiania Zabbix proxy z parametrami wiersza poleceń:

```
zabbix_proxy -c /usr/local/etc/zabbix_proxy.conf
zabbix_proxy --help
zabbix_proxy -V
```

Sterowanie w czasie działania

Opcje sterowania w czasie działania:

Option	Description	Target
config_cache_reload	Przeładuj pamięć podręczną konfiguracji. Ignorowane, jeśli pamięć podręczna jest obecnie ładowana. Aktywny Zabbix proxy połączy się z Zabbix server i zażąda danych konfiguracyjnych. Pasywny Zabbix proxy zażąda danych konfiguracyjnych z Zabbix server przy następnym połączeniu serwera z proxy.	

Option	Description	Target
history_cache_clear=<**target**>	Wyczyść pamięć podręczną historii dla pozycji określonej przez jej ID. Wpływa na wszystkie wartości pozycji, z wyjątkiem pierwszej i ostatniej wartości.	**target** - ID pozycji
diaginfo[=<**section**>]	Zbierz informacje diagnostyczne w pliku logu proxy.	**historycache** - statystyki pamięci podręcznej historii **preprocessing** - statystyki menedżera przetwarzania wstępnego **locks** - lista muteksów (jest pusta w systemach *BSD*)
snmp_cache_reload	Przeładuj pamięć podręczną SNMP — wyczyść właściwości silnika SNMP (czas silnika, uruchomienia silnika, ID silnika, poświadczenia) dla wszystkich hostów. Użyj tej opcji, aby wymusić globalne wyczyszczenie pamięci podręcznej podczas rozwiązywania problemów z SNMP.	
housekeeper_execute	Uruchom procedurę housekeeping. Ignorowane, jeśli procedura housekeeping jest obecnie w toku.	
log_level_increase[=<**target**>]	Zwiększ poziom logowania; wpływa na wszystkie procesy, jeśli target nie został określony. Nieobsługiwane w systemach *BSD*.	**process type** - Wszystkie procesy określonego typu (np. poller) Zobacz wszystkie typy procesów proxy. **process type,N** - Typ procesu i numer (np. poller,3) **pid** - Identyfikator procesu (od 1 do 65535). Dla większych wartości określ target jako 'process type,N'.
log_level_decrease[=<**target**>]	Zmniejsz poziom logowania; wpływa na wszystkie procesy, jeśli target nie został określony. Nieobsługiwane w systemach *BSD*.	
prof_enable[=<**target**>]	Włącz profilowanie. Wpływa na wszystkie procesy, jeśli target nie został określony. Włączone profilowanie dostarcza szczegóły wszystkich rwlocków/muteksów według nazwy funkcji.	**process type** - Wszystkie procesy określonego typu (np. history syncer) Zobacz wszystkie typy procesów proxy. **process type,N** - Typ procesu i numer (np. history syncer,1) **pid** - Identyfikator procesu (od 1 do 65535). Dla większych wartości określ target jako 'process type,N'. **scope** - `rwlock`, `mutex`, `processing` mogą być używane z typem procesu i numerem (np. history syncer,1,processing) lub dla wszystkich procesów danego typu (np. history syncer,rwlock)
prof_disable[=<**target**>]	Wyłącz profilowanie. Wpływa na wszystkie procesy, jeśli target nie został określony.	**process type** - Wszystkie procesy określonego typu (np. history syncer) Zobacz wszystkie typy procesów proxy. **process type,N** - Typ procesu i numer (np. history syncer,1) **pid** - Identyfikator procesu (od 1 do 65535). Dla większych wartości określ target jako 'process type,N'.

Przykład użycia sterowania w czasie działania do przeładowania pamięci podręcznej konfiguracji proxy:

```
zabbix_proxy -c /usr/local/etc/zabbix_proxy.conf -R config_cache_reload
```

Przykład użycia sterowania w czasie działania do wyczyszczenia pamięci podręcznej historii dla pozycji:

```
zabbix_proxy -c /usr/local/etc/zabbix_proxy.conf -R history_cache_clear=42243
```

Przykłady użycia sterowania w czasie działania do zbierania informacji diagnostycznych:

```
### Zbierz wszystkie dostępne informacje diagnostyczne w pliku logu proxy:
zabbix_proxy -R diaginfo
```

```
### Zbierz statystyki pamięci podręcznej historii w pliku logu proxy:
zabbix_proxy -R diaginfo=historycache
```

Przykład użycia sterowania w czasie działania do przeładowania pamięci podręcznej SNMP:

```
zabbix_proxy -R snmp_cache_reload
```

Attention:
Gdy interfejs SNMPv3 zostanie zaktualizowany za pomocą interfejsu Zabbix, Zabbix w większości przypadków automatycznie przeładuje nowe poświadczenia SNMPv3 dla tego interfejsu; używaj `-R snmp_cache_reload` tylko wtedy, gdy odpytywanie nadal kończy się niepowodzeniem po zmianie poświadczeń (na przykład z powodu niespójności engineBoots/engineID lub urządzeń niezgodnych z RFC), albo gdy trzeba wymusić globalne wyczyszczenie pamięci podręcznej SNMP na potrzeby rozwiązywania problemów.

Przykład użycia sterowania w czasie działania do wyzwolenia wykonania housekeepera:

```
zabbix_proxy -c /usr/local/etc/zabbix_proxy.conf -R housekeeper_execute
```

Przykłady użycia sterowania w czasie działania do zmiany poziomu logowania:

```
### Zwiększ poziom logowania wszystkich procesów:
zabbix_proxy -c /usr/local/etc/zabbix_proxy.conf -R log_level_increase

### Zwiększ poziom logowania drugiego procesu poller:
zabbix_proxy -c /usr/local/etc/zabbix_proxy.conf -R log_level_increase=poller,2

### Zwiększ poziom logowania procesu o PID 1234:
zabbix_proxy -c /usr/local/etc/zabbix_proxy.conf -R log_level_increase=1234

### Zmniejsz poziom logowania wszystkich procesów http poller:
zabbix_proxy -c /usr/local/etc/zabbix_proxy.conf -R log_level_decrease="http poller"
```

Użytkownik procesu

Zabbix proxy został zaprojektowany do działania jako użytkownik niebędący rootem. Będzie działać jako dowolny użytkownik niebędący rootem, jako który został uruchomiony. Dlatego możesz uruchamiać proxy jako dowolny użytkownik niebędący rootem bez żadnych problemów.

Jeśli spróbujesz uruchomić go jako 'root', przełączy się na zakodowanego na stałe użytkownika 'zabbix', który musi być obecny w twoim systemie. Możesz uruchamiać proxy jako 'root' tylko wtedy, gdy odpowiednio zmodyfikujesz parametr 'AllowRoot' w pliku konfiguracyjnym proxy.

Plik konfiguracyjny

Szczegółowe informacje na temat konfiguracji zabbix_proxy można znaleźć w opcjach pliku konfiguracyjnego.

Typy procesów i wątków proxy

- `agent poller` - asynchroniczny proces odpytywania dla pasywnych kontroli z wątkiem roboczym
- `availability manager` - proces aktualizacji dostępności hostów
- `browser poller` - proces odpytywania dla kontroli pozycji przeglądarkowych
- `configuration syncer` - proces zarządzania pamięcią podręczną danych konfiguracyjnych w pamięci
- `data sender` - nadawca danych proxy
- `discovery manager` - proces menedżera wykrywania urządzeń
- `discovery worker` - proces obsługi zadań wykrywania od menedżera wykrywania
- `history syncer` - zapisujący historię do bazy danych
- `housekeeper` - proces usuwania nieaktualnej historii pozycji
- `http agent poller` - asynchroniczny proces odpytywania dla kontroli HTTP z wątkiem roboczym
- `http poller` - proces odpytywania monitoringu WWW
- `icmp pinger` - proces odpytywania dla kontroli icmpping
- `internal poller` - proces odpytywania dla kontroli wewnętrznych
- `ipmi manager` - menedżer procesów odpytywania IPMI
- `ipmi poller` - proces odpytywania dla kontroli IPMI
- `java poller` - proces odpytywania dla kontroli Java
- `odbc poller` - proces odpytywania dla kontroli ODBC
- `poller` - zwykły proces odpytywania dla pasywnych kontroli
- `preprocessing manager` - menedżer zadań przetwarzania wstępnego z wątkami roboczymi przetwarzania wstępnego

- `preprocessing worker` - wątek przetwarzania wstępnego danych
- `self-monitoring` - proces zbierania wewnętrznych statystyk serwera
- `snmp poller` - asynchroniczny proces odpytywania dla kontroli SNMP z wątkiem roboczym (tylko pozycje `walk[OID]` i `get[OID]`)
- `snmp trapper` - trapper dla pułapek SNMP
- `task manager` - proces zdalnego wykonywania zadań żądanych przez inne komponenty (np. zamknięcie problemu, potwierdzenie problemu, sprawdzenie teraz wartości pozycji, funkcja zdalnych poleceń)
- `trapper` - trapper dla aktywnych kontroli, pułapek, komunikacji proxy
- `unreachable poller` - proces odpytywania dla nieosiągalnych urządzeń
- `vmware collector` - kolektor danych VMware odpowiedzialny za zbieranie danych z usług VMware

Plik dziennika proxy może być używany do obserwowania tych typów procesów.

Plik dziennika proxy jest tworzony z uprawnieniami odczytu i zapisu tylko dla właściciela pliku. Dodatkowo plik jest dostępny do odczytu dla grupy właściciela. Wszystkie pozostałe uprawnienia są zabronione.

Różne typy procesów Zabbix proxy mogą być monitorowane przy użyciu wewnętrznej **pozycji zabbix[process,<type>,<mode>,<state>]** item.

Statystyki transakcji synchronizatora historii

Tytuł procesu synchronizatora historii wyświetla szczegółowe statystyki dotyczące transakcji synchronizatora historii.

```
205276 ?        S      0:00  zabbix_proxy: history syncer #1 [processed 1 values in 0.001179 (0.001167,0.0
205277 ?        S      0:00  zabbix_proxy: history syncer #2 [processed 0 values in 0.000022 (0.000000,0.0
```

Czasy w wyrażeniu „processed...in N (<timings>) sec" oznaczają:

- Czas poświęcony na zapisywanie wartości pozycji do bazy danych;
- Czas poświęcony na aktualizację danych pozycji (stan, błędy).

Procedura housekeeping

Proxy Zabbix ma proces `housekeeper`, który usuwa nieaktualną historię i trendy pozycji. Działa on cyklicznie, z częstotliwością określoną przez `HousekeepingFrequency`, a limit usuwania na cykl jest określany przez `ProxyLocalBuffer` i `ProxyOfflineBuffer`. W przeciwieństwie do procedury housekeeping w serwerze Zabbix, proces `housekeeper` proxy nie używa tabeli `housekeeper` — usuwa wszystkie nieaktualne dane raz na każdy cykl housekeeping.

Obsługiwane platformy

Zabbix proxy działa na tej samej liście obsługiwanych platform co serwer Zabbix.

Bufor pamięci

Bufor pamięci umożliwia przechowywanie nowych danych (wartości pozycji, wykrywanie sieci, autorejestracja hostów) w buforze i przesyłanie ich do serwera Zabbix bez dostępu do bazy danych. Bufor pamięci został wprowadzony dla proxy od wersji Zabbix 7.0.

W instalacjach sprzed Zabbix 7.0 zebrane dane były przechowywane w bazie danych przed przesłaniem do serwera Zabbix. Dla tych instalacji po aktualizacji do Zabbix 7.0 pozostaje to domyślnym zachowaniem.

W celu uzyskania zoptymalizowanej wydajności zaleca się skonfigurowanie użycia bufora pamięci na proxy. Jest to możliwe przez zmianę wartości ProxyBufferMode z "disk" (domyślna wartość zakodowana na stałe dla istniejących instalacji) na "hybrid" (zalecane) lub "memory". Wymagane jest również ustawienie rozmiaru bufora pamięci (parametr ProxyMemoryBufferSize).

W trybie hybrydowym bufor jest chroniony przed utratą danych przez zapisywanie niewysłanych danych do bazy danych, jeśli proxy zostanie zatrzymany, bufor się zapełni lub dane będą zbyt stare. Po zapisaniu wszystkich wartości do bazy danych proxy wraca do używania bufora pamięci.

W trybie pamięci bufor pamięci będzie używany, jednak nie ma ochrony przed utratą danych. Jeśli proxy zostanie zatrzymany lub pamięć zostanie przepełniona, niewysłane dane zostaną odrzucone.

Tryb hybrydowy (ProxyBufferMode=hybrid) jest stosowany we wszystkich nowych instalacjach od wersji Zabbix 7.0.

Dodatkowe parametry, takie jak ProxyMemoryBufferSize oraz ProxyMemoryBufferAge, definiują odpowiednio rozmiar bufora pamięci i maksymalny wiek danych w buforze.

Uwaga: w przypadku sprzecznej konfiguracji proxy wypisze błąd i nie uruchomi się, na przykład jeśli:

- ProxyBufferMode jest ustawiony na "hybrid" lub "memory", a ProxyMemoryBufferSize ma wartość "0";
- ProxyBufferMode jest ustawiony na "hybrid" lub "memory", a ProxyLocalBuffer nie ma wartości "0".

Ustawienia regionalne

Zwróć uwagę, że proxy wymaga ustawień regionalnych UTF-8, aby niektóre tekstowe pozycje mogły być poprawnie interpretowane. Większość nowoczesnych systemów typu Unix ma domyślnie ustawienia regionalne UTF-8, jednak istnieją systemy, w których trzeba je skonfigurować ręcznie.

Obliczanie kolejek podczas konserwacji

Attention:
Proxy Zabbix nie jest świadomy okresów konserwacji; szczegóły znajdują się w sekcji Obliczanie kolejek podczas konserwacji.

5 Java gateway

Przegląd

Zabbix Java gateway można zainstalować z kodu źródłowego lub z pakietów.

Natywna obsługa monitorowania aplikacji JMX jest dostępna w postaci demona Zabbix o nazwie „Zabbix Java gateway". Zabbix Java gateway jest demonem napisanym w języku Java. Aby ustalić wartość określonego licznika JMX na hoście, serwer Zabbix odpytuje Zabbix Java gateway, który używa API zarządzania JMX do zdalnego odpytywania interesującej aplikacji. Aplikacja nie wymaga instalacji żadnego dodatkowego oprogramowania, musi jedynie zostać uruchomiona z opcją `-Dcom.sun.management.jmxremote` w wierszu poleceń.

Java gateway akceptuje połączenia przychodzące z serwera Zabbix lub proxy i może być używany wyłącznie jako „pasywny proxy". W przeciwieństwie do Zabbix proxy, może być również używany przez Zabbix proxy (proxy Zabbix nie mogą być łączone kaskadowo). Dostęp do każdego Java gateway jest konfigurowany bezpośrednio w pliku konfiguracji serwera Zabbix lub proxy, dlatego dla jednego serwera Zabbix lub jednego proxy Zabbix można skonfigurować tylko jeden Java gateway. Jeśli host będzie miał pozycje typu **JMX agent** oraz pozycje innego typu, tylko pozycje typu **JMX agent** będą przekazywane do Java gateway w celu pobrania danych.

Gdy pozycja musi zostać zaktualizowana przez Java gateway, serwer Zabbix lub proxy połączy się z Java gateway i zażąda wartości, którą Java gateway z kolei pobierze i przekaże z powrotem do serwera lub proxy. W związku z tym Java gateway nie buforuje żadnych wartości.

Serwer Zabbix lub proxy ma określony typ procesów, które łączą się z Java gateway, kontrolowany przez opcję **StartJavaPollers**. Wewnętrznie Java gateway uruchamia wiele wątków, kontrolowanych przez opcję **START_POLLERS**. Po stronie serwera, jeśli połączenie trwa dłużej niż **Timeout** sekund, zostanie zakończone, ale Java gateway może nadal być zajęty pobieraniem wartości z licznika JMX. Aby rozwiązać ten problem, w Java gateway dostępna jest opcja **TIMEOUT**, która pozwala ustawić limit czasu dla operacji sieciowych JMX.

Serwer Zabbix lub proxy będzie próbował w jak największym stopniu grupować żądania do jednego celu JMX razem (z uwzględnieniem interwałów pozycji) i wysyłać je do Java gateway w ramach jednego połączenia w celu uzyskania lepszej wydajności.

Zaleca się, aby **StartJavaPollers** było mniejsze lub równe **START_POLLERS**, w przeciwnym razie mogą wystąpić sytuacje, w których w Java gateway nie będzie dostępnych wątków do obsługi przychodzących żądań; w takim przypadku Java gateway używa ThreadPoolExecutor.CallerRunsPolicy, co oznacza, że główny wątek będzie obsługiwał przychodzące żądanie i tymczasowo nie będzie przyjmował żadnych nowych żądań.

Jeśli próbujesz monitorować aplikacje Java oparte na Wildfly za pomocą Zabbix Java gateway, zainstaluj najnowszy plik jboss-client.jar dostępny na stronie pobierania Wildfly.

2 Konfiguracja z pakietów RHEL

Przegląd

Jeśli zainstalowano z pakietów, poniższe informacje pomogą w konfiguracji Zabbix Java gateway.

Konfigurowanie i uruchamianie Java gateway

Parametry konfiguracyjne Zabbix Java gateway można dostosować w pliku:

```
/etc/zabbix/zabbix_java_gateway.conf
```

Aby uzyskać więcej informacji, zobacz parametry konfiguracji Zabbix Java gateway parameters.

Aby uruchomić Zabbix Java gateway:

```
systemctl restart zabbix-java-gateway
```

Aby automatycznie uruchamiać Zabbix Java gateway podczas startu systemu:

RHEL 7 i nowsze:

```
systemctl enable zabbix-java-gateway
```

RHEL wcześniejsze niż 7:

```
chkconfig --level 12345 zabbix-java-gateway on
```

Konfigurowanie serwera do użycia z Java gateway

Gdy Java gateway jest uruchomiony i działa, musisz wskazać serwerowi Zabbix, gdzie znajduje się Zabbix Java gateway. Robi się to przez określenie parametrów JavaGateway i JavaGatewayPort w pliku konfiguracyjnym serwera. Jeśli host, na którym działa aplikacja JMX, jest monitorowany przez proxy Zabbix, wtedy parametry połączenia należy określić zamiast tego w pliku konfiguracyjnym proxy.

```
JavaGateway=192.168.3.14
JavaGatewayPort=10052
```

Domyślnie serwer nie uruchamia żadnych procesów związanych z monitorowaniem JMX. Jeśli jednak chcesz z niego korzystać, musisz określić liczbę wstępnie uruchamianych instancji odpytywaczy Java. Robi się to w taki sam sposób, jak w przypadku zwykłych odpytywaczy i trapperów.

```
StartJavaPollers=5
```

Nie zapomnij zrestartować serwera lub proxy po zakończeniu ich konfiguracji.

Debugowanie Java gateway

Plik dziennika Zabbix Java gateway to:

```
/var/log/zabbix/zabbix_java_gateway.log
```

Jeśli chcesz zwiększyć poziom logowania, edytuj plik:

```
/etc/zabbix/zabbix_java_gateway_logback.xml
```

i zmień `level="info"` na ”debug” lub nawet ”trace” (w celu dogłębnego rozwiązywania problemów):

```
<configuration scan="true" scanPeriod="15 seconds">
[...]
      <root level="info">
              <appender-ref ref="FILE" />
      </root>

</configuration>
```

Monitorowanie JMX

Więcej szczegółów znajduje się na stronie Monitorowanie JMX.

3 Konfiguracja z pakietów Debian/Ubuntu

Przegląd

Jeśli zainstalowano z pakietów, poniższe informacje pomogą w konfiguracji Zabbix Java gateway.

Konfigurowanie i uruchamianie Java gateway

Konfigurację Java gateway można dostosować w pliku:

```
/etc/zabbix/zabbix_java_gateway.conf
```

Aby uzyskać więcej informacji, zobacz parametry konfiguracji Zabbix Java gateway.

Aby uruchomić Zabbix Java gateway:

```
systemctl restart zabbix-java-gateway
```

Aby automatycznie uruchamiać Zabbix Java gateway podczas startu systemu:

```
systemctl enable zabbix-java-gateway
```

Konfigurowanie serwera do użycia z Java gateway

Gdy Java gateway jest uruchomiony i działa, musisz wskazać serwerowi Zabbix, gdzie znajduje się Zabbix Java gateway. Robi się to przez określenie parametrów JavaGateway i JavaGatewayPort w pliku konfiguracji serwera. Jeśli host, na którym działa aplikacja JMX, jest monitorowany przez Zabbix proxy, wtedy parametry połączenia należy określić zamiast tego w pliku konfiguracji proxy.

```
JavaGateway=192.168.3.14
JavaGatewayPort=10052
```

Domyślnie serwer nie uruchamia żadnych procesów związanych z monitorowaniem JMX. Jeśli jednak chcesz z niego korzystać, musisz określić liczbę wstępnie uruchamianych instancji Java pollerów. Robi się to w taki sam sposób, jak w przypadku zwykłych pollerów i trapperów.

```
StartJavaPollers=5
```

Nie zapomnij zrestartować serwera lub proxy po zakończeniu ich konfiguracji.

Debugowanie Java gateway

Plik dziennika Zabbix Java gateway to:

```
/var/log/zabbix/zabbix_java_gateway.log
```

Jeśli chcesz zwiększyć poziom logowania, edytuj plik:

```
/etc/zabbix/zabbix_java_gateway_logback.xml
```

i zmień `level="info"` na ”debug” lub nawet ”trace” (w celu dogłębnego rozwiązywania problemów):

```
<configuration scan="true" scanPeriod="15 seconds">
[...]
      <root level="info">
              <appender-ref ref="FILE" />
      </root>

</configuration>
```

Monitorowanie JMX

Więcej szczegółów znajduje się na stronie Monitorowanie JMX.

Konfiguracja ze źródeł

Przegląd

Jeśli zainstalowano ze źródeł, poniższe informacje pomogą w konfiguracji Zabbix Java gateway.

Przegląd plików

Jeśli uzyskano Java gateway ze źródeł, powinien powstać zestaw skryptów powłoki, plików JAR i plików konfiguracyjnych w katalogu $PREFIX/sbin/zabbix_java. Rola tych plików została podsumowana poniżej.

```
bin/zabbix-java-gateway-$VERSION.jar
```

Sam plik JAR Java gateway.

```
lib/logback-core-1.5.16.jar
lib/logback-classic-1.5.16.jar
lib/slf4j-api-2.0.16.jar
lib/android-json-4.3_r3.1.jar
```

Zależności Java gateway: Logback, SLF4J oraz biblioteka Android JSON.

```
lib/logback.xml
lib/logback-console.xml
```

Pliki konfiguracyjne dla Logback.

```
shutdown.sh
startup.sh
```

Pomocnicze skrypty do uruchamiania i zatrzymywania Java gateway.

```
settings.sh
```

Plik konfiguracyjny wczytywany przez powyższe skrypty startup i shutdown.

Konfigurowanie i uruchamianie Java gateway

Domyślnie Java gateway nasłuchuje na porcie 10052. Jeśli planujesz uruchomić Java gateway na innym porcie, możesz określić to w skrypcie settings.sh. Zobacz opis pliku konfiguracyjnego Java gateway, aby dowiedzieć się, jak określić tę i inne opcje.

Warning:
Port 10052 nie jest zarejestrowany przez IANA registered.

Gdy ustawienia będą już odpowiednie, możesz uruchomić Java gateway, wykonując skrypt startowy:

```
./startup.sh
```

Podobnie, gdy Java gateway nie będzie już potrzebny, uruchom skrypt zatrzymania, aby go wyłączyć:

```
./shutdown.sh
```

Zwróć uwagę, że w przeciwieństwie do serwer lub proxy, Java gateway jest lekki i nie wymaga bazy danych.

Konfigurowanie serwera do użycia z Java gateway

Gdy Java gateway jest uruchomiony i działa, należy poinformować serwer Zabbix, gdzie znajduje się Zabbix Java gateway. Odbywa się to przez określenie parametrów JavaGateway oraz JavaGatewayPort w pliku konfiguracyjnym serwera. Jeśli host, na którym działa aplikacja JMX, jest monitorowany przez Zabbix proxy, należy zamiast tego określić parametry połączenia w pliku konfiguracyjnym proxy.

```
JavaGateway=192.168.3.14
JavaGatewayPort=10052
```

Domyślnie serwer nie uruchamia żadnych procesów związanych z monitorowaniem JMX. Jeśli jednak chcesz z niego korzystać, musisz określić liczbę wstępnie utworzonych instancji procesów Java poller. Robi się to w taki sam sposób, jak w przypadku zwykłych pollerów i trapperów.

```
StartJavaPollers=5
```

Nie zapomnij zrestartować serwera lub proxy po zakończeniu ich konfiguracji.

Debugowanie Java gateway

W przypadku jakichkolwiek problemów z Java gateway lub gdy komunikat o błędzie, który widzisz dla pozycji we frontend, nie jest wystarczająco opisowy, warto zajrzeć do pliku dziennika Java gateway.

Domyślnie Java gateway zapisuje swoją aktywność do pliku /tmp/zabbix_java.log z poziomem logowania „info". Czasami te informacje nie są wystarczające i potrzebne są informacje z poziomu logowania „debug". Aby zwiększyć poziom logowania, zmodyfikuj plik lib/logback.xml i zmień atrybut level znacznika <root> na „debug":

```
<root level="debug">
  <appender-ref ref="FILE" />
</root>
```

Zwróć uwagę, że w przeciwieństwie do Zabbix server lub Zabbix proxy, nie ma potrzeby ponownego uruchamiania Zabbix Java gateway po zmianie pliku logback.xml — zmiany w logback.xml zostaną wykryte automatycznie. Po zakończeniu debugowania możesz przywrócić poziom logowania do „info".

Jeśli chcesz zapisywać logi do innego pliku lub do całkowicie innego medium, takiego jak baza danych, dostosuj plik logback.xml do swoich potrzeb. Więcej szczegółów znajdziesz w podręczniku Logback.

Czasami na potrzeby debugowania przydatne jest uruchomienie Java gateway jako aplikacji konsolowej zamiast jako demona. Aby to zrobić, zakomentuj zmienną PID_FILE w settings.sh. Jeśli PID_FILE zostanie pominięte, skrypt startup.sh uruchomi Java gateway jako aplikację konsolową i sprawi, że Logback będzie używać pliku lib/logback-console.xml, który nie tylko zapisuje logi do konsoli, ale ma również włączony poziom logowania „debug".

Na koniec zwróć uwagę, że ponieważ Java gateway używa SLF4J do logowania, możesz zastąpić Logback frameworkiem według własnego wyboru, umieszczając odpowiedni plik JAR w katalogu lib. Więcej szczegółów znajdziesz w podręczniku SLF4J.

Monitorowanie JMX

Więcej szczegółów znajduje się na stronie Monitorowanie JMX.

6 Sender

Przegląd

Zabbix sender to narzędzie wiersza poleceń, które może być używane do wysyłania danych wydajnościowych do serwera Zabbix w celu ich przetwarzania.

Narzędzie to jest zwykle używane w długotrwale działających skryptach użytkownika do okresowego wysyłania danych o dostępności i wydajności.

Aby wysyłać wyniki bezpośrednio do serwera Zabbix lub proxy, musi być skonfigurowana pozycja typu trapper item.

Zobacz także bibliotekę Python dla Zabbix, która ma wbudowaną funkcjonalność działania jak Zabbix sender.

Uruchamianie Zabbix sender

Przykład uruchomienia Zabbix sender w systemie UNIX:

```
cd bin
./zabbix_sender -z zabbix -s "Linux DB3" -k db.connections -o 43
```

gdzie:

- z - host serwera Zabbix (można również użyć adresu IP)
- s - nazwa techniczna monitorowanego hosta (zgodnie z rejestracją w frontendzie Zabbix)
- k - klucz pozycji
- o - wartość do wysłania

Attention:
Opcje zawierające białe znaki muszą być ujęte w podwójne cudzysłowy.

Zabbix sender może być używany do wysyłania wielu wartości z pliku wejściowego. Więcej informacji można znaleźć na stronie podręcznika man Zabbix sender.

Jeśli określono plik konfiguracyjny, Zabbix sender używa wszystkich adresów zdefiniowanych w parametrze konfiguracyjnym ServerActive agenta do wysyłania danych. Jeśli wysyłanie na jeden adres się nie powiedzie, sender próbuje wysłać dane na pozostałe adresy. Jeśli wysyłanie partii danych do jednego adresu zakończy się niepowodzeniem, kolejne partie nie są już wysyłane na ten adres.

Zabbix sender akceptuje ciągi znaków w kodowaniu UTF-8 (zarówno w systemach typu UNIX, jak i Windows), bez znacznika kolejności bajtów (BOM) na początku pliku.

Zabbix sender w systemie Windows można uruchomić w podobny sposób:

```
zabbix_sender.exe [options]
```

Scenariusze wysyłania w czasie rzeczywistym zabbix_sender zbierają wiele wartości przekazanych do niego w krótkich odstępach czasu i wysyłają je do serwera w ramach jednego połączenia. Wartość, która nie jest oddalona od poprzedniej o więcej niż 0,2 sekundy, może zostać umieszczona w tym samym stosie, ale maksymalny czas odpytywania nadal wynosi 1 sekundę.

Note:
Zabbix sender zakończy działanie, jeśli w określonym pliku konfiguracyjnym znajduje się nieprawidłowy wpis parametru (niezgodny z notacją *parameter=value*).

Uruchamianie Zabbix sender z wykrywaniem niskiego poziomu

Przykład uruchomienia Zabbix sender w celu wysłania wartości w formacie JSON dla wykrywania niskiego poziomu:

```
./zabbix_sender -z 192.168.1.113 -s "Zabbix server" -k trapper.discovery.item -o '[{"{#FSNAME}":"/","{#FST
```

Aby to działało, reguła wykrywania niskiego poziomu musi mieć typ pozycji Zabbix trapper (w tym przykładzie z kluczem `trapper.discovery.item`).

7 Get

Przegląd

Zabbix get to narzędzie wiersza poleceń, które może być używane do komunikacji z agent i pobierania wymaganych informacji z agent.

Narzędzie to jest zwykle używane do rozwiązywania problemów z agentami Zabbix.

Zobacz także bibliotekę Python dla Zabbix, która ma wbudowaną funkcjonalność działania jak Zabbix get.

Uruchamianie Zabbix get

Przykład uruchomienia Zabbix get w systemie UNIX w celu pobrania wartości obciążenia procesora z agent:

```
cd bin
./zabbix_get -s 127.0.0.1 -p 10050 -k system.cpu.load[all,avg1]
```

Inny przykład uruchomienia Zabbix get do przechwycenia ciągu znaków ze strony internetowej:

```
cd bin
./zabbix_get -s 192.168.1.1 -p 10050 -k "web.page.regexp[www.example.com,,,\"USA: ([a-zA-Z0-9.-]+)\",,\1]"
```

Zwróć uwagę, że klucz pozycji zawiera tutaj spację, dlatego do oznaczenia klucza pozycji dla powłoki użyto cudzysłowów. Cudzysłowy nie są częścią klucza pozycji; zostaną usunięte przez powłokę i nie zostaną przekazane do Zabbix agent.

Jeśli klucz pozycji nie jest obsługiwany, Zabbix get zwróci kod wyjścia 1.

Zabbix get akceptuje następujące parametry wiersza poleceń:

```
-s --host <host name or IP>             Określ nazwę hosta lub adres IP hosta
-p --port <port number>                 Określ numer portu agent uruchomionego na hoście (domyślnie: 10050
-I --source-address <IP address>        Określ źródłowy adres IP
-t --timeout <seconds>                  Określ limit czasu. Prawidłowy zakres: 1-600 sekund (domyślnie: 30
-k --key <item key>                     Określ klucz pozycji, dla której ma zostać pobrana wartość
-P --protocol <value>                   Protokół używany do komunikacji z agent. Wartości:
                                            auto - połącz przy użyciu protokołu JSON, w razie niepowodzeni
                                            json - połącz przy użyciu protokołu JSON
                                            plaintext - połącz przy użyciu protokołu tekstowego, w którym
-h --help                               Wyświetl ten komunikat pomocy
-V --version                            Wyświetl numer wersji

--tls-connect <value>                   Sposób połączenia z agent. Wartości:
                                            unencrypted - połącz bez szyfrowania (domyślnie)
                                            psk - połącz przy użyciu TLS i klucza współdzielonego
                                            cert - połącz przy użyciu TLS i certyfikatu
--tls-ca-file <CA file>                 Pełna ścieżka do pliku zawierającego certyfikaty głównych urzędów
--tls-crl-file <CRL file>               Pełna ścieżka do pliku zawierającego unieważnione certyfikaty
--tls-agent-cert-issuer <cert issuer>   Dozwolony wystawca certyfikatu agent
--tls-agent-cert-subject <cert subject> Dozwolony temat certyfikatu agent
--tls-cert-file <cert file>             Pełna ścieżka do pliku zawierającego certyfikat lub łańcuch certyf
--tls-key-file <key file>               Pełna ścieżka do pliku zawierającego klucz prywatny
--tls-psk-identity <PSK-identity>       Unikalny ciąg znaków rozróżniający wielkość liter, używany do iden
--tls-psk-file <PSK-file>               Pełna ścieżka do pliku zawierającego klucz współdzielony
--tls-cipher13 <cipher-string>          Ciąg szyfrów dla OpenSSL 1.1.1 lub nowszego dla TLS 1.3. Zastępuje
--tls-cipher <cipher-string>            Ciąg priorytetów GnuTLS (dla TLS 1.2 i nowszych) lub ciąg szyfrów
```

Zobacz także stronę podręcznika Zabbix get, aby uzyskać więcej informacji.

Zabbix get w systemie Windows można uruchomić podobnie:

```
zabbix_get.exe [options]
```

8 JS

Przegląd

zabbix_js to narzędzie wiersza poleceń, które może być używane do testowania osadzonych skryptów.

To narzędzie wykona skrypt użytkownika z parametrem typu string i wyświetli wynik. Skrypty są wykonywane przy użyciu osadzonego silnika skryptowego Zabbix.

W przypadku błędów kompilacji lub wykonania zabbix_js wypisze błąd do stderr i zakończy działanie z kodem 1.

Użycie

```
zabbix_js -s script-file -p input-param [-l log-level] [-t timeout]
zabbix_js -s script-file -i input-file [-l log-level] [-t timeout]
zabbix_js -h
zabbix_js -V
```

zabbix_js akceptuje następujące parametry wiersza poleceń:

```
-s, --script script-file          Określa nazwę pliku skryptu do wykonania. Jeśli jako nazwa pliku zostani
-i, --input input-file            Określa nazwę pliku z danymi wejściowymi. Jego zawartość zostanie przeka
-p, --param input-param           Określa parametr wejściowy: zmienną, która zostanie przekazana do skrypt
-l, --loglevel log-level          Określa poziom logowania. Zakres: 0-5.
-t, --timeout timeout             Określa limit czasu w sekundach. Prawidłowy zakres: 1-600 sekund (domyśl
-h, --help                        Wyświetla informacje pomocy.
-V, --version                     Wyświetla numer wersji.
-w <webdriver url>                Włącza monitorowanie przeglądarki.
```

Przykłady:

Przykład 1: Wykonanie skryptu ze zmienną zawierającą wartość

Skrypt (`script-file.js`):

```
return value;
```

Użycie:

```
zabbix_js -s script-file.js -p example_value
```

Dane wyjściowe: `example_value`

Przykład 2: Wykonanie skryptu z plikiem zawierającym dane wejściowe

Plik ze skryptem (`script-file.js`):

```
return value;
```

Plik z danymi wejściowymi (`example.txt`):

```
Example of input information from the file
```

Użycie:

```
zabbix_js -s script-file.js -i example.txt
```

Dane wyjściowe: `Example of input information from the file`

Przykład 3: Wykonanie skryptu z danymi wejściowymi odczytanymi ze stdin

Plik ze skryptem (`script-file.js`):

```
return value;
```

Użycie:

```
zabbix_js -s script-file.js -i -
```

Dane wejściowe (stdin):

```
Example of input from stdin
```

Dane wyjściowe: `Example of input from stdin`

9 Usługa sieciowa

Przegląd

Usługa internetowa Zabbix to proces używany do komunikacji z zewnętrznymi usługami internetowymi. Obecnie usługa internetowa Zabbix jest używana do generowania i wysyłania zaplanowanych raportów, a w przyszłości planowane jest dodanie kolejnych funkcji.

Serwer Zabbix łączy się z usługą internetową przez HTTP(S). Usługa internetowa Zabbix wymaga, aby Google Chrome był zainstalowany na tym samym hoście; w niektórych dystrybucjach usługa może również działać z Chromium (zobacz znane problemy).

Instalacja

Oficjalny pakiet zabbix-web-service jest dostępny w repozytorium Zabbix.

Aby skompilować usługę internetową Zabbix ze źródeł, należy podać opcję konfiguracji `--enable-webservice`.

Aby skonfigurować usługę internetową Zabbix, zaktualizuj parametry pliku konfiguracyjnego `zabbix_web_service.conf`.

Attention:
Zdecydowanie zaleca się skonfigurowanie szyfrowania między serwerem Zabbix a usługą internetową Zabbix przy użyciu certyfikatów. Domyślnie dane przesyłane między serwerem Zabbix a usługą internetową Zabbix nie są szyfrowane, co może prowadzić do nieautoryzowanego dostępu.

5 Konfiguracja

Aby uzyskać dostęp do treści w sekcji Konfiguracja, skorzystaj z paska bocznego.

1 Konfigurowanie szablonu

Przegląd

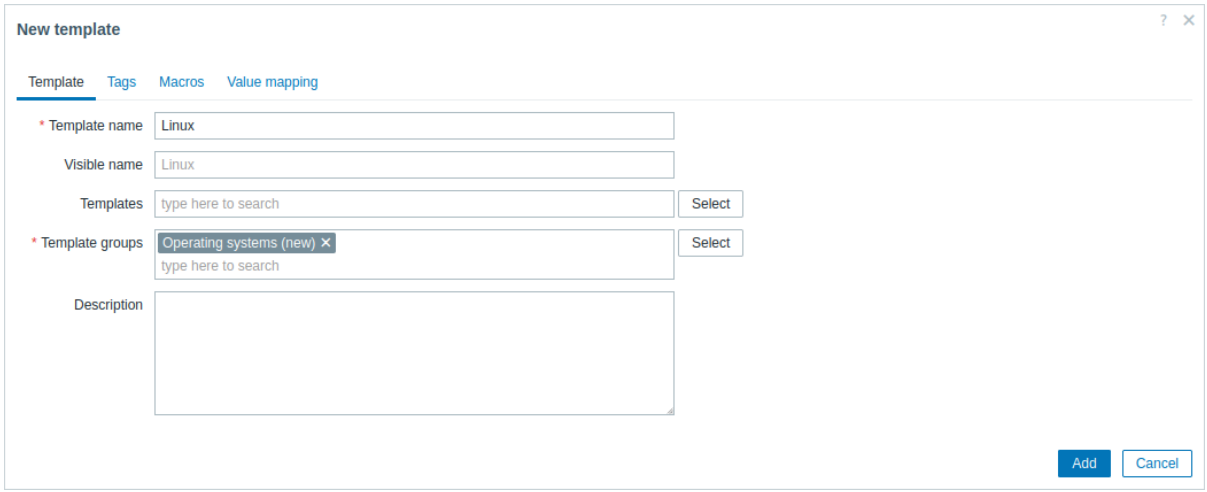
Konfiguracja szablonu wymaga najpierw utworzenia szablonu poprzez zdefiniowanie jego ogólnych parametrów, a następnie dodania do niego encji (pozycji, wyzwalaczy, wykresów itp.).

Tworzenie szablonu

Aby utworzyć szablon, wykonaj następujące czynności:

1. Przejdź do *Data collection* > *Templates*.
2. Kliknij *Create template*.
3. Edytuj atrybuty szablonu.

Zakładka **Template** zawiera ogólne atrybuty szablonu.



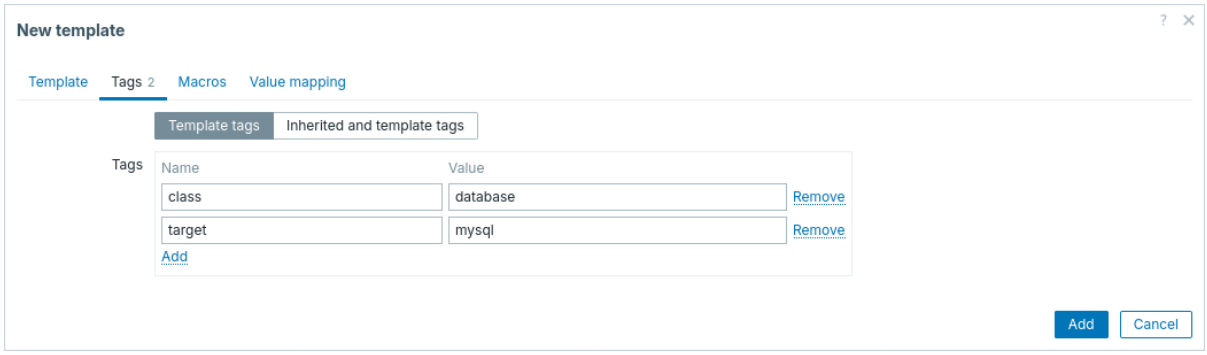
Wszystkie wymagane pola wejściowe są oznaczone czerwoną gwiazdką.

Atrybuty szablonu:

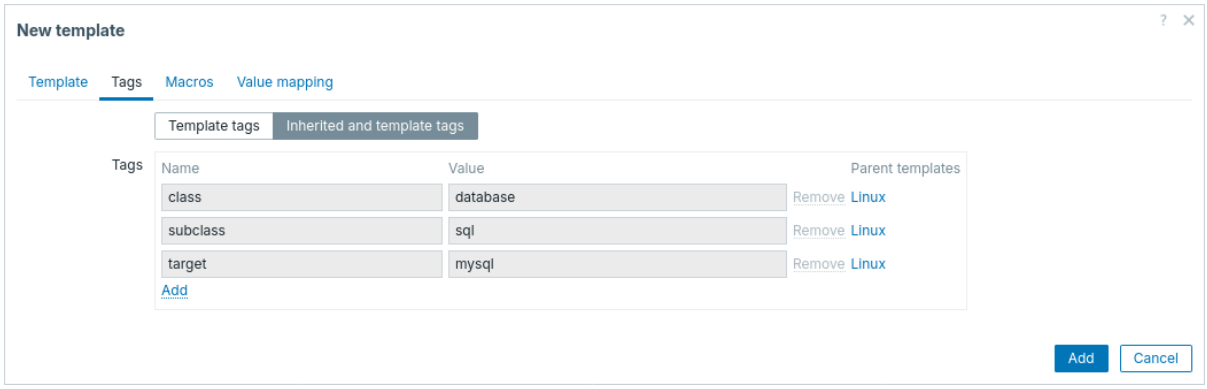
Parameter	Description
Template name	Unikalna nazwa szablonu. Dozwolone są znaki alfanumeryczne, spacje, kropki, myślniki i podkreślenia. Niedozwolone są spacje na początku i na końcu.
Visible name	Jeśli ustawisz tę nazwę, będzie ona widoczna na listach, mapach itp.

Parameter	Description
Templates	Połącz z tym szablonem jeden lub więcej szablonów. Wszystkie encje (pozycje, wyzwalacze itp.) będą dziedziczone z połączonych szablonów. Aby połączyć nowy szablon, wpisz jego nazwę w polu *Templates* — spowoduje to wyświetlenie rozwijanej listy pasujących szablonów. Alternatywnie kliknij *Select*, aby otworzyć wyskakujące okno *Templates*, które początkowo nie pokazuje żadnych szablonów. Aby wypełnić listę, wpisz nazwę grupy szablonów w polu *Template group* (i wybierz jedną z sugerowanej listy) albo naciśnij przycisk *Select* obok pola *Template group*, aby otworzyć wyskakujące okno *Template groups*. Po wybraniu grupy szablonów wyskakujące okno *Templates* zostanie zaktualizowane i pokaże szablony należące do tej grupy. Wybrane szablony zostaną połączone po zapisaniu lub zaktualizowaniu konfiguracji. Aby odłączyć szablon, użyj jednej z dwóch opcji w bloku *Templates*: *Unlink* - odłącz szablon, ale zachowaj jego encje (pozycje, wyzwalacze itp.); *Unlink and clear* - odłącz szablon i usuń wszystkie jego encje (pozycje, wyzwalacze itp.).
Template groups	Grupy szablonów, do których należy szablon.
Description	Opis szablonu.
Vendor and version	Dostawca i wersja szablonu; wyświetlane tylko podczas aktualizacji istniejących szablonów (gotowych szablonów dostarczanych przez Zabbix, importowanych szablonów lub szablonów zmodyfikowanych za pomocą Template API), jeśli konfiguracja szablonu zawiera takie informacje. Nie można ich modyfikować w frontend Zabbix. Dla gotowych szablonów wersja jest wyświetlana w następujący sposób: główna wersja Zabbix, separator (”-”), numer rewizji (zwiększany z każdą nową wersją szablonu i resetowany przy każdej głównej wersji Zabbix). Na przykład 7.0-0, 7.0-5, 8.0-0, 8.0-3.

Zakładka **Tags** umożliwia definiowanie tagów na poziomie szablonu. Wszystkie problemy hostów połączonych z tym szablonem będą oznaczane tagami z wartościami wprowadzonymi tutaj.



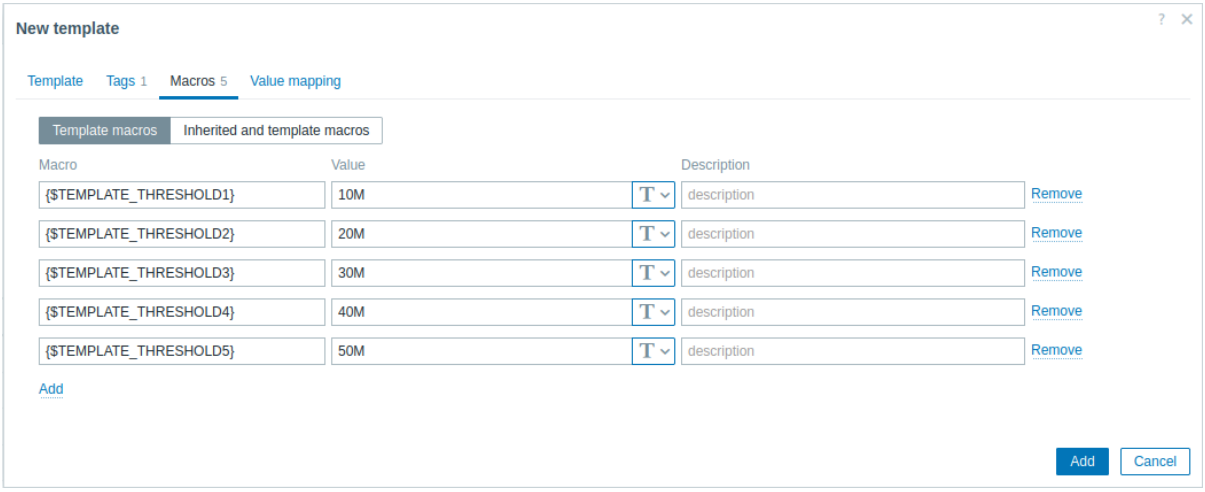
Jeśli wybierzesz opcję *Inherited and template tags*, możesz również wyświetlić tagi z połączonych szablonów, które szablon odziedziczy.



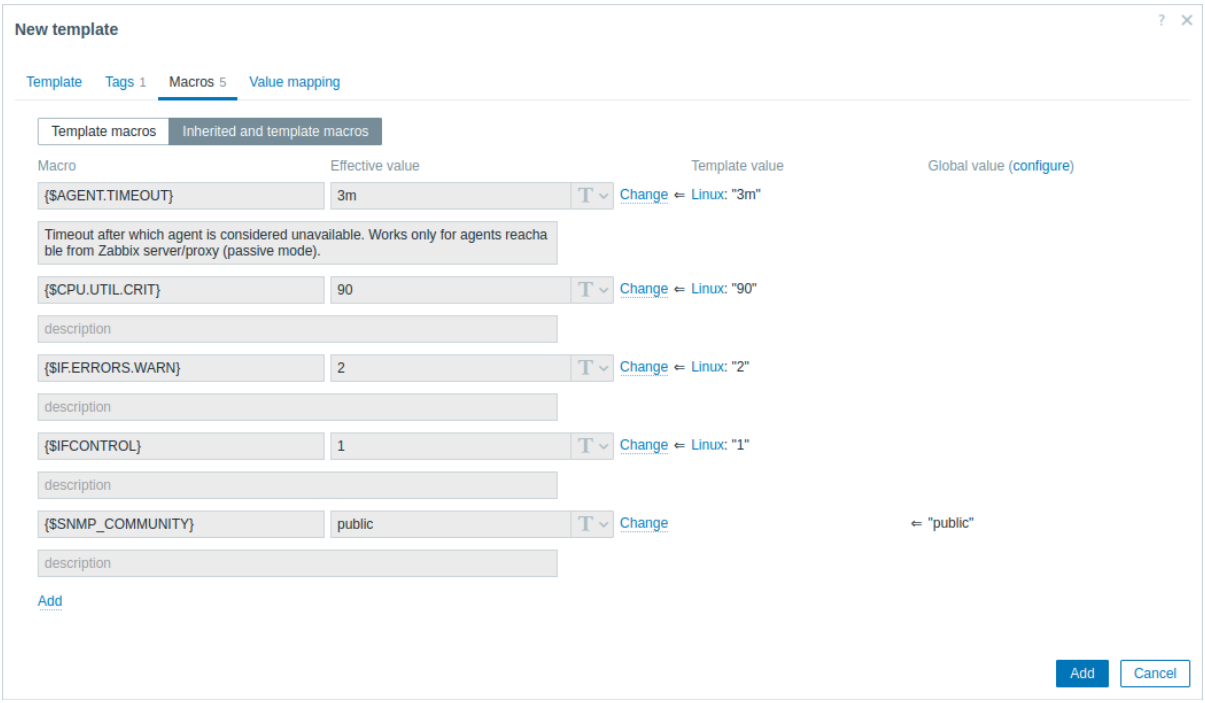
Dla wygody udostępniono odnośniki do odpowiednich szablonów.

W tagach obsługiwane są makra użytkownika, makra {INVENTORY.*}, {HOST.HOST}, {HOST.NAME}, {HOST.CONN}, {HOST.DNS}, {HOST.IP}, {HOST.PORT} oraz {HOST.ID}.

Zakładka **Macros** umożliwia definiowanie makr użytkownika na poziomie szablonu jako par nazwa-wartość. Zwróć uwagę, że wartości makr mogą być przechowywane jako zwykły tekst, tajny tekst lub sekret Vault. Obsługiwane jest również dodawanie opisu.



Jeśli wybierzesz opcję *Inherited and template macros*, możesz również wyświetlić makra z połączonych szablonów i makra globalne, które szablon odziedziczy, a także wartości, do których makra zostaną rozwinięte.



Dla wygody udostępniono odnośniki do odpowiednich szablonów, a także odnośnik do konfiguracji makr globalnych. Można również edytować makro połączonego szablonu lub makro globalne na poziomie szablonu, co w praktyce tworzy kopię makra w szablonie.

Zakładka **Value mapping** umożliwia skonfigurowanie przyjaznej dla użytkownika reprezentacji danych pozycji w mapowaniach wartości.

Przyciski:

Add	Dodaj szablon. Dodany szablon powinien pojawić się na liście.
Update	Zaktualizuj właściwości istniejącego szablonu.
Clone	Utwórz kolejny szablon na podstawie właściwości bieżącego szablonu. To **obejmuje** encje (pozycje, wyzwalacze itp.) zarówno dziedziczone z połączonych szablonów, jak i bezpośrednio przypisane do bieżącego szablonu, ale **nie obejmuje** dostawcy i wersji bieżącego szablonu, aby sklonowany szablon można było odróżnić od oryginału.
Delete	Usuń szablon; encje szablonu (pozycje, wyzwalacze itp.) pozostaną przy połączonych hostach.
Delete and clear	Usuń szablon i wszystkie jego encje z połączonych hostów.

Cancel	Anuluj edycję właściwości szablonu.

Dodawanie pozycji, wyzwalaczy, wykresów

Attention:
Pozycje należy najpierw dodać do szablonu. Wyzwalaczy i wykresów nie można dodać bez odpowiadającej im pozycji.

Istnieją dwa sposoby dodawania pozycji do szablonu:

1. Aby utworzyć nowe pozycje, postępuj zgodnie ze wskazówkami w sekcji Tworzenie pozycji.

2. Aby dodać istniejące pozycje do szablonu:

- Przejdź do *Data collection* > *Hosts* (lub *Templates*).
- Kliknij *Items* w wierszu wymaganego hosta/szablonu.
- Zaznacz pola wyboru pozycji, które chcesz dodać do szablonu.
- Kliknij *Copy* pod listą pozycji.
- Wybierz szablon (lub grupę szablonów), do którego mają zostać skopiowane pozycje, i kliknij *Copy*.
  Wszystkie wybrane pozycje powinny zostać skopiowane do szablonu.

Dodawanie wyzwalaczy i wykresów odbywa się w podobny sposób (odpowiednio z listy wyzwalaczy i wykresów), ponownie pamiętając, że można je dodać tylko wtedy, gdy wymagane pozycje zostały wcześniej dodane.

Dodawanie pulpitów

Aby dodać pulpity do szablonu w *Zbieranie danych* > *Szablony*, wykonaj następujące czynności:

1. Kliknij *Pulpity* w wierszu szablonu.
2. Skonfiguruj pulpit zgodnie ze wskazówkami w sekcji konfigurowania pulpitów.

Attention:
Podczas konfigurowania widżetów na pulpicie szablonu (zamiast na pulpicie globalnym) parametry związane z hostem nie są dostępne, a niektóre parametry mają inną etykietę. Wynika to z tego, że pulpity szablonów wyświetlają dane tylko z hosta, do którego szablon jest podłączony. Na przykład parametry *Grupy hostów*, *Wyklucz grupy hostów* i *Hosty* w widżecie *Problemy* nie są dostępne, parametr *Grupy hostów* w widżecie *Dostępność hosta* nie jest dostępny, a parametr *Pokaż hosty w utrzymaniu* został przemianowany na *Pokaż dane w utrzymaniu* itd. Więcej informacji o dostępności parametrów w widżetach pulpitu szablonu można znaleźć w opisie parametrów poszczególnych widżetów pulpitu.

Note:
Szczegółowe informacje o dostępie do pulpitów hosta utworzonych na podstawie pulpitów szablonu można znaleźć w sekcji pulpitów hosta.

Konfigurowanie reguł wykrywania niskiego poziomu

Zobacz sekcję wykrywanie niskiego poziomu w podręczniku.

Dodawanie scenariuszy WWW

Aby dodać scenariusze WWW do szablonu w *Zbieranie danych* > *Szablony*, wykonaj następujące czynności:

1. Kliknij *WWW* w wierszu szablonu.
2. Skonfiguruj scenariusz WWW zgodnie ze standardową metodą opisaną w konfigurowaniu scenariuszy WWW.

2 Konfigurowanie grupy szablonów

Overview

Template groups are used for the logical grouping of templates and assigning user permissions to them.

Each template must have at least one template group assigned. A template may belong to multiple template groups, and each template group may contain multiple templates.

Note that in Zabbix, all permissions are based on groups: user groups, host groups, and template groups. So, even if a single user needs access to a single template, it is granted by adding the user to a user group that has permission to access the template group containing that template.

Konfiguracja

> **Attention:**
> Tylko użytkownicy typu Super admin mogą tworzyć grupy szablonów.

Istnieją dwie opcje tworzenia grupy szablonów w frontend Zabbix.

Opcja pierwsza:

- Przejdź do: *Data collection* → *Template groups*
- Kliknij *Create template group* w prawym górnym rogu ekranu
- Wprowadź nazwę grupy w formularzu



Opcja druga: podczas konfigurowania szablonu wprowadź nieistniejącą nazwę grupy w polu wejściowym *Template groups*.

Po utworzeniu grupy szablonów możesz kliknąć nazwę szablonu na liście w sekcji *Data collection* → *Template groups*, aby edytować nazwę grupy, sklonować grupę lub usunąć grupę.

Usunięcie grupy szablonów powoduje usunięcie tylko grupy logicznej, a nie szablonów w tej grupie. Nie można usunąć grupy szablonów, która jest jedyną grupą dla jakiegokolwiek istniejącego szablonu.

Tworzenie podgrup szablonów

Podgrupa szablonu (lub zagnieżdżona grupa szablonów) jest elementem podrzędnym nadrzędnej grupy szablonów, która ją zawiera.

Podgrupę tworzy się przy użyciu ukośnika '/' w polu wprowadzania nazwy grupy, aby określić jej relację do grupy nadrzędnej lub grup nadrzędnych. Na przykład:

- wpisanie `Linux servers/Databases` tworzy podgrupę `Linux servers/Databases` w nadrzędnej grupie `Linux servers`.
- wpisanie `Linux servers/Databases/MySQL/Tokyo` tworzy odpowiednią podgrupę w zagnieżdżonych grupach nadrzędnych `Linux servers`, `Linux servers/Databases`, `Linux servers/Databases/MySQL`.

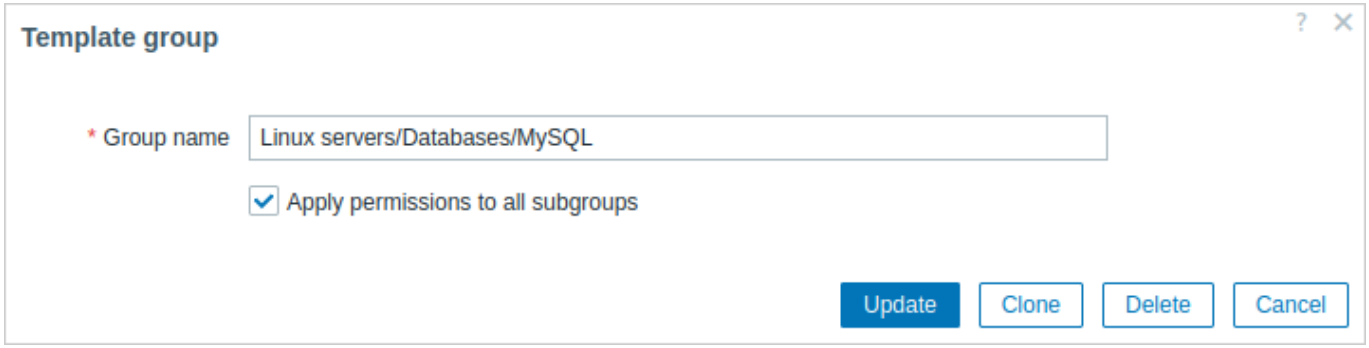
Podczas tworzenia podgrupy nie można używać ukośników na początku ani na końcu nazwy ani kilku ukośników z rzędu. Znak '/' nie obsługuje sekwencji ucieczki.

Nie jest wymagane tworzenie żadnych nadrzędnych grup szablonów przed utworzeniem podgrupy. Możesz zdecydować, czy zacząć od utworzenia podgrupy (na przykład `Linux servers/Databases`), czy dowolnej nadrzędnej grupy szablonów (w naszym przykładzie `Linux servers`). Jeśli zaczniesz od utworzenia podgrupy, nadrzędne grupy szablonów **nie** zostaną utworzone automatycznie.

Uprawnienia do grup szablonów

- Podczas tworzenia podgrupy w istniejącej nadrzędnej grupie szablonów (na przykład tworzenia `Linux servers/Databases`, gdy `Linux servers` już istnieje), uprawnienia grupy użytkowników do podgrupy są dziedziczone z grupy nadrzędnej.
- Podczas tworzenia nadrzędnej grupy szablonów dla istniejącej podgrupy (na przykład tworzenia `Linux servers`, gdy `Linux servers/Databases` już istnieje), dla grupy nadrzędnej nie są ustawiane żadne uprawnienia.

Podczas edycji dowolnej grupy szablonów można również ustawić dodatkową opcję: *Zastosuj uprawnienia do wszystkich podgrup*.



Zaznaczenie tego pola wyboru i kliknięcie *Aktualizuj* spowoduje zastosowanie tego samego poziomu uprawnień do wszystkich bieżących i przyszłych podgrup edytowanej grupy szablonów.

Jeśli więc jakimkolwiek grupom użytkowników nadano różne uprawnienia do podgrup edytowanej grupy szablonów, zaznaczenie tego pola wyboru nada wszystkim bieżącym i przyszłym podgrupom takie same uprawnienia użytkowników jak edytowanej grupie.

Należy pamiętać, że ta opcja nie jest zapisywana w bazie danych i zastąpi istniejące uprawnienia. Wszelkie zmiany wprowadzone za pomocą tej opcji można cofnąć wyłącznie ręcznie.

3 Podłączanie/odłączanie

Przegląd

Podłączanie to proces, w którym szablony są stosowane do hostów, natomiast odłączanie usuwa powiązanie z szablonem z hosta.

Podłączanie szablonu

Aby podłączyć szablon do hosta, wykonaj następujące czynności:

1. Przejdź do *Data collection* → *Hosts*.
2. Kliknij wymagany host.
3. Zacznij wpisywać nazwę szablonu w polu *Templates*. Pojawi się lista pasujących szablonów; przewiń w dół, aby wybrać odpowiedni. Alternatywnie możesz kliknąć *Select* obok pola i wybrać jeden lub kilka szablonów z listy w wyskakującym oknie.
4. Kliknij *Add/Update* w formularzu atrybutów hosta.

Host będzie teraz miał wszystkie encje szablonu. Obejmuje to pozycje, wyzwalacze, wykresy, reguły wykrywania niskiego poziomu, scenariusze WWW, a także pulpity.

Attention:
Podłączenie wielu szablonów do tego samego hosta zakończy się niepowodzeniem, jeśli szablony te zawierają pozycje z takim samym kluczem pozycji. Ponadto, ponieważ wyzwalacze i wykresy używają pozycji, również one nie mogą zostać podłączone do jednego hosta z wielu szablonów, jeśli używane są identyczne klucze pozycji.

Gdy encje (pozycje, wyzwalacze itp.) są dodawane z szablonu:

- wcześniej istniejące identyczne encje na hoście są aktualizowane jako encje szablonu, a **wszelkie istniejące dostosowania encji na poziomie hosta zostają utracone**;
- encje z szablonu są dodawane;
- wszelkie bezpośrednio podłączone encje, które przed podłączeniem szablonu istniały tylko na hoście, pozostają bez zmian.

Na listach wszystkie encje pochodzące z szablonu są teraz poprzedzone nazwą szablonu, co wskazuje, że należą do danego szablonu. Sama nazwa szablonu (szarym tekstem) jest linkiem umożliwiającym dostęp do listy tych encji na poziomie szablonu.

Note:
Dla niektórych pozycji, takich jak external checks, HTTP agent checks, simple checks, SSH checks oraz Telnet checks, interfejs hosta jest opcjonalny. Jeśli w momencie podłączania szablonu host nie ma zdefiniowanego interfejsu, te pozycje zostaną dodane bez interfejsu. Jeśli później dodasz interfejs hosta, nie zostanie on automatycznie przypisany do już istniejących pozycji. Aby przypisać nowo dodany interfejs hosta do wszystkich pozycji szablonu jednocześnie, odłącz szablon od hosta, a następnie podłącz go ponownie. Aby zachować historię pozycji, użyj opcji *Unlink*, nie używaj *Unlink and clear*.

Jeśli jakaś encja nie jest poprzedzona nazwą szablonu, oznacza to, że istniała na hoście wcześniej i nie została dodana przez szablon.

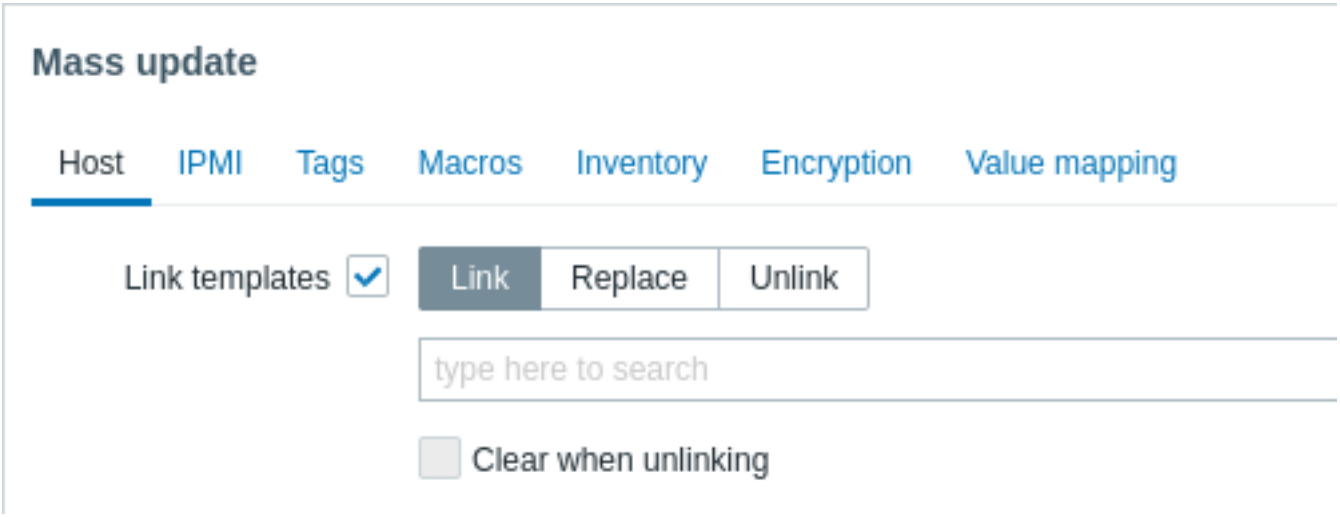
Kryteria unikalności encji

Podczas dodawania encji (pozycji, wyzwalaczy itp.) z szablonu ważne jest, aby wiedzieć, które z tych encji już istnieją na hoście i wymagają aktualizacji, a które encje się różnią. Kryteria unikalności służące do określenia, czy encje są takie same, czy różne, są następujące:

- dla pozycji - klucz pozycji;
- dla wyzwalaczy - nazwa wyzwalacza i wyrażenie;
- dla niestandardowych wykresów - nazwa wykresu i jego pozycje.

Podłączanie szablonów do wielu hostów

Aby zaktualizować powiązania szablonów dla wielu hostów, w *Data collection* → *Hosts* zaznacz wybrane hosty, zaznaczając ich pola wyboru, a następnie kliknij **Mass update** pod listą i wybierz *Link templates*:



Aby podłączyć dodatkowe szablony, zacznij wpisywać nazwę szablonu w polu autouzupełniania, aż pojawi się rozwijana lista z pasującymi szablonami. Następnie przewiń listę i wybierz szablon do podłączenia.

Opcja *Replace* umożliwia podłączenie nowego szablonu przy jednoczesnym odłączeniu wszystkich szablonów, które były wcześniej podłączone do hostów. Opcja *Unlink* umożliwia określenie, które szablony mają zostać odłączone. Opcja *Clear when unlinking* pozwala nie tylko odłączyć wcześniej podłączone szablony, ale także usunąć wszystkie encje odziedziczone z tych szablonów (pozycje, wyzwalacze itd.).

Note:
Zabbix oferuje obszerny zestaw predefiniowanych szablonów. Możesz używać ich jako punktu odniesienia, ale zachowaj ostrożność przy stosowaniu ich bez zmian w środowisku produkcyjnym, ponieważ mogą zawierać zbyt wiele pozycji i zbyt często odpytywać o dane. Jeśli chcesz ich używać, dostosuj je do swoich rzeczywistych potrzeb.

Edycja podlinkowanych encji

Jeśli spróbujesz edytować pozycja lub wyzwalacz, które zostały podlinkowane z szablon, możesz zauważyć, że wiele kluczowych opcji edycji jest wyłączonych. Ma to sens, ponieważ idea szablonów polega na tym, że elementy są edytowane centralnie na poziomie szablonu. Nadal jednak możesz na przykład włączać/wyłączać pozycja na poszczególnych hostach oraz ustawiać interwał aktualizacji, długość historii i niektóre inne parametry.

Jeśli chcesz w pełni edytować encję, musisz zrobić to na poziomie szablonu (skrót do poziomu szablonu jest wyświetlany w nazwie formularza), pamiętając, że te zmiany wpłyną na wszystkie hosty, które mają podlinkowany ten szablon.

Attention:
Wszelkie dostosowania encji wprowadzone na poziomie szablonu zastąpią wcześniejsze dostosowania encji na poziomie hosta.

Odłączanie szablonu

Aby odłączyć szablon od hosta, wykonaj następujące czynności:

1. Przejdź do *Data collection* → *Hosts*.
2. Kliknij wymagany host i znajdź pole *Templates*.
3. Kliknij *Unlink* lub *Unlink and clear* obok szablonu, aby odłączyć szablon.
4. Kliknij *Update* w formularzu atrybutów hosta.

Wybranie opcji *Unlink* spowoduje jedynie usunięcie powiązania z szablonem, przy jednoczesnym pozostawieniu wszystkich jego encji przy hoście. Obejmuje to pozycje, wyzwalacze, wykresy, reguły wykrywania niskiego poziomu i scenariusze WWW, ale nie obejmuje pulpitów. Należy pamiętać, że mapy wartości i tagi odziedziczone z podłączonych szablonów również zostaną usunięte.

Wybranie opcji *Unlink and clear* spowoduje usunięcie zarówno powiązania z szablonem, jak i wszystkich jego encji (pozycji, wyzwalaczy itd.).

4 Zagnieżdżanie

Przegląd

Zagnieżdżanie to sposób, w jaki jeden szablon obejmuje jeden lub więcej innych szablonów.

Ponieważ sensowne jest rozdzielenie encji na osobne szablony dla różnych usług, aplikacji itp., możesz ostatecznie mieć całkiem sporo szablonów, z których wszystkie mogą wymagać podłączenia do wielu hostów. Aby uprościć ten obraz, możliwe jest połączenie kilku szablonów razem w jednym szablonie.

Korzyść z zagnieżdżania polega na tym, że do hosta trzeba podłączyć tylko jeden szablon, a host automatycznie odziedziczy wszystkie encje z szablonów, które są podłączone do tego jednego szablonu. Na przykład, jeśli podłączymy *T1* i *T2* do *T3*, uzupełnimy *T3* o wszystkie encje z *T1* i *T2*, ale nie odwrotnie. Jeśli podłączymy *T1* do *T2* i *T3*, uzupełnimy *T2* i *T3* o encje z *T1*.

Konfigurowanie zagnieżdżonych szablonów

Aby połączyć szablony, należy wybrać istniejący szablon (lub utworzyć nowy), a następnie:

1. Otworzyć formularz konfiguracji szablonu.
2. Odszukać pole *Templates*.
3. Kliknąć *Select*, aby otworzyć wyskakujące okno *Templates*.
4. W wyskakującym oknie wybrać wymagane szablony, a następnie kliknąć *Select*, aby dodać szablony do listy.
5. Kliknąć *Add* lub *Update* w formularzu konfiguracji szablonu.

W rezultacie wszystkie encje skonfigurowanego szablonu, a także wszystkie encje połączonych szablonów będą teraz widoczne w konfiguracji szablonu. Obejmuje to pozycje, wyzwalacze, wykresy, reguły wykrywania niskiego poziomu oraz scenariusze WWW, ale nie obejmuje pulpitów. Jednak pulpity połączonych szablonów będą mimo to dziedziczone przez hosty.

Aby odłączyć dowolny z połączonych szablonów, kliknij *Unlink* lub *Unlink and clear* w formularzu konfiguracji szablonu, a następnie kliknij *Update*.

Opcja *Unlink* po prostu usunie powiązanie z połączonym szablonem, nie usuwając żadnych jego encji (pozycji, wyzwalaczy itd.).

Opcja *Unlink and clear* usunie zarówno powiązanie z połączonym szablonem, jak i wszystkie jego encje (pozycje, wyzwalacze itd.).

5 Masowa aktualizacja

Przegląd

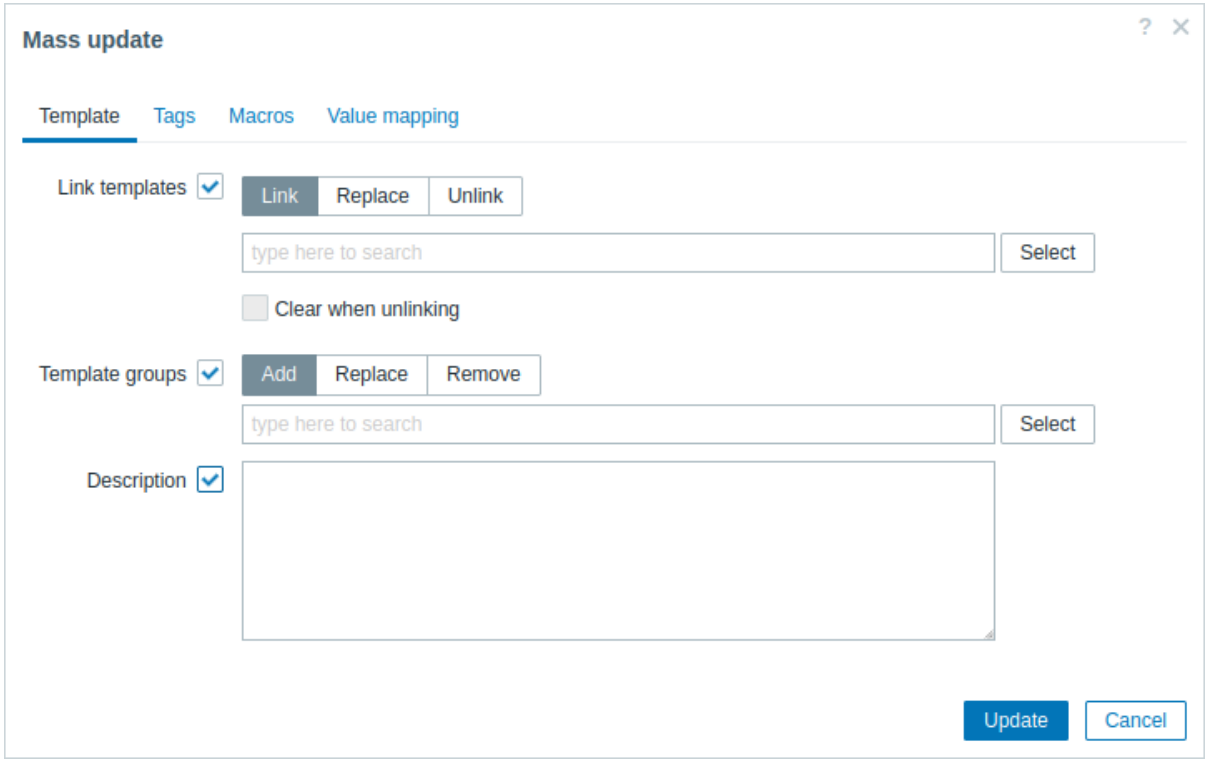
Czasami możesz chcieć zmienić jakiś atrybut dla wielu szablonów jednocześnie. Zamiast otwierać każdy pojedynczy szablon do edycji, możesz w tym celu użyć funkcji masowej aktualizacji.

Używanie masowej aktualizacji

Aby masowo zaktualizować niektóre szablony, wykonaj następujące czynności:

1. Zaznacz pola wyboru przy szablonach, które chcesz zaktualizować, na liście szablonów.
2. Kliknij *Mass update* poniżej listy.
3. Przejdź do zakładki z wymaganymi atrybutami (*Template*, *Tags*, *Macros* lub *Value mapping*).
4. Zaznacz pola wyboru przy atrybutach, które chcesz zaktualizować, i wprowadź dla nich nową wartość.

Karta **Szablon** zawiera ogólne opcje masowej aktualizacji szablonów.



Po wybraniu odpowiedniego przycisku dla aktualizacji *Podłącz szablony* dostępne są następujące opcje:

- *Podłącz* — określa, które dodatkowe szablony należy podłączyć;
- *Zastąp* — określa, które szablony należy podłączyć, jednocześnie odłączając wszystkie wcześniej podłączone szablony;
- *Odłącz* — określa, które szablony należy odłączyć.

Aby określić szablony do podłączenia/odłączenia, zacznij wpisywać nazwę szablonu w polu autouzupełniania, aż pojawi się lista rozwijana z pasującymi szablonami. Wystarczy przewinąć w dół, aby wybrać wymagane szablony.

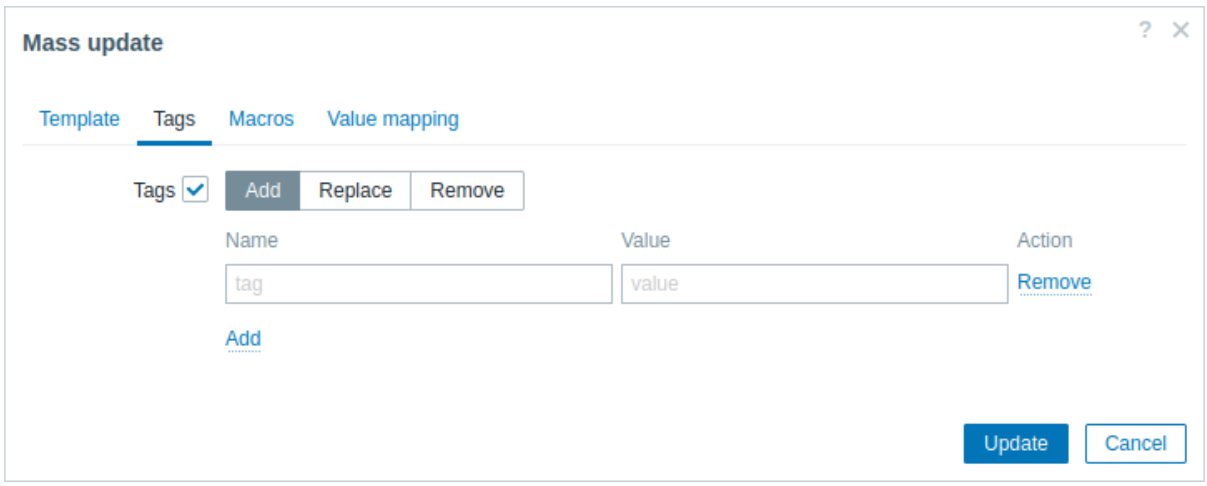
Opcja *Wyczyść przy odłączaniu* umożliwia odłączenie wszystkich wcześniej podłączonych szablonów, a także usunięcie wszystkich elementów odziedziczonych z tych szablonów (pozycji, wyzwalaczy, wykresów itp.).

Po wybraniu odpowiedniego przycisku dla aktualizacji *Grupy szablonów* dostępne są następujące opcje:

- *Dodaj* — umożliwia określenie dodatkowych grup szablonów spośród istniejących lub wprowadzenie całkowicie nowych grup szablonów dla szablonów;
- *Zastąp* — usunie szablon z wszystkich istniejących grup szablonów i zastąpi je grupą/grupami określoną/określonymi w tym polu (istniejącymi lub nowymi grupami szablonów);
- *Usuń* — usunie określone grupy szablonów z szablonów.

Pola te obsługują autouzupełnianie — rozpoczęcie wpisywania powoduje wyświetlenie listy rozwijanej z pasującymi grupami szablonów. Jeśli grupa szablonów jest nowa, również pojawi się na liście rozwijanej i będzie oznaczona dopiskiem *(new)* po nazwie. Wystarczy przewinąć w dół, aby ją wybrać.

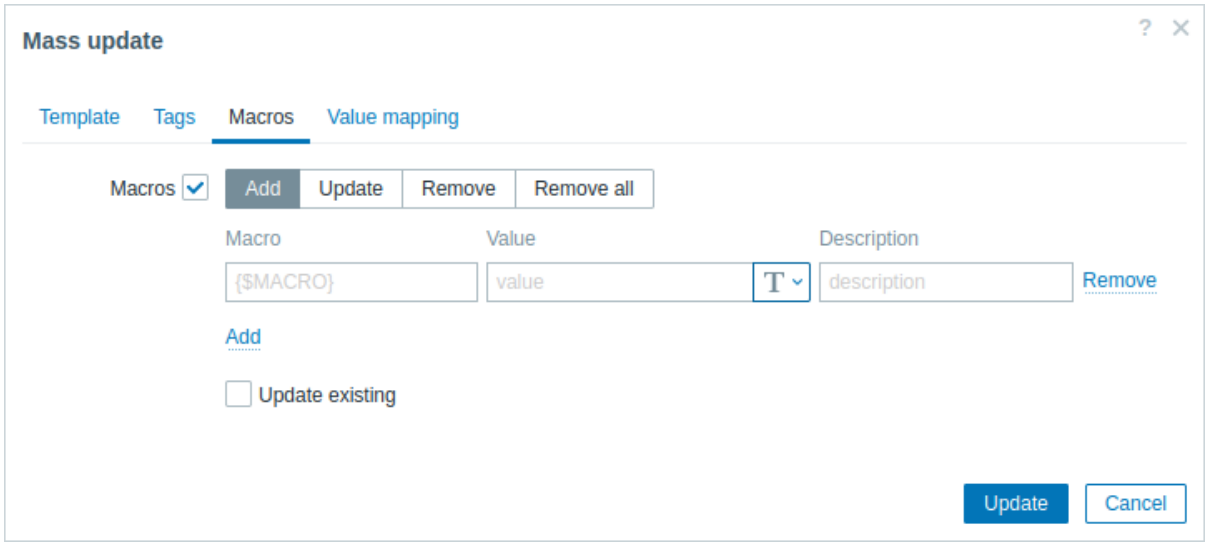
Zakładka **Tagi** umożliwia masową aktualizację tagów na poziomie szablonu.



Makra użytkownika, makra {INVENTORY.*}, {HOST.HOST}, {HOST.NAME}, {HOST.CONN}, {HOST.DNS}, {HOST.IP}, {HOST.PORT}

oraz {HOST.ID} są obsługiwane w tagach. Należy pamiętać, że tagi o tej samej nazwie, ale o różnych wartościach, nie są uznawane za „duplikaty” i mogą zostać dodane do tego samego szablonu.

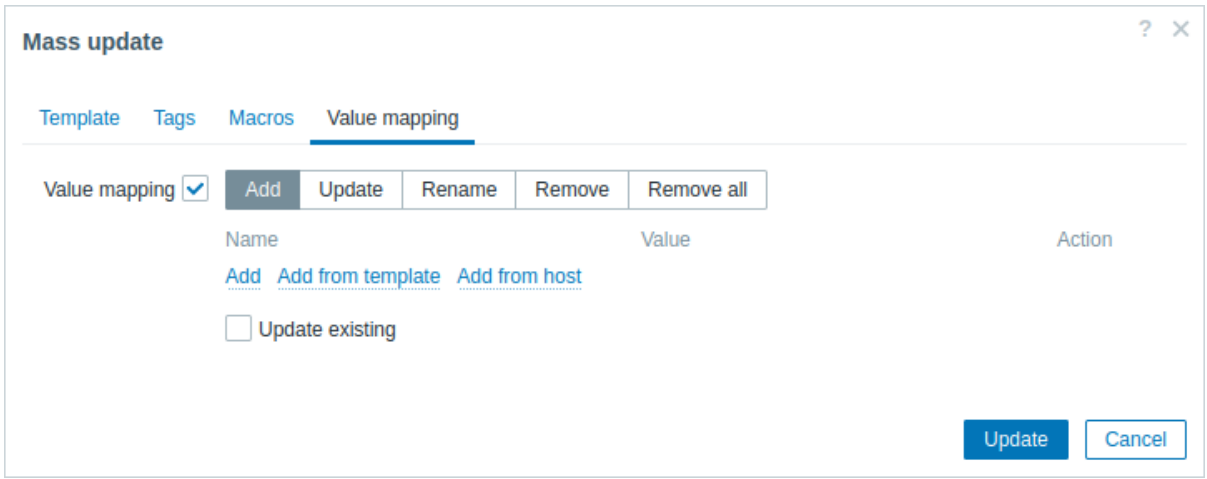
Karta **Makra** umożliwia masową aktualizację makr na poziomie szablonu.



Dostępne są następujące opcje po wybraniu odpowiedniego przycisku aktualizacji makr:

- *Dodaj* — umożliwia określenie dodatkowych makr użytkownika dla szablonów. Jeśli pole wyboru *Aktualizuj istniejące* jest zaznaczone, wartość, typ i opis dla podanej nazwy makra zostaną zaktualizowane. Jeśli nie jest zaznaczone i makro o tej nazwie już istnieje w szablonie(ach), nie zostanie zaktualizowane.
- *Aktualizuj* — zastąpi wartości, typy i opisy makr określonych na tej liście. Jeśli pole wyboru *Dodaj brakujące* jest zaznaczone, makro, które wcześniej nie istniało w szablonie, zostanie dodane jako nowe makro. Jeśli nie jest zaznaczone, zaktualizowane zostaną tylko makra, które już istnieją w szablonie.
- *Usuń* — usunie określone makra z szablonów. Jeśli pole *Z wyjątkiem wybranych* jest zaznaczone, wszystkie makra z wyjątkiem tych określonych na liście zostaną usunięte. Jeśli nie jest zaznaczone, usunięte zostaną tylko makra określone na liście.
- *Usuń wszystko* — usunie wszystkie makra użytkownika z szablonów. Jeśli pole *Potwierdzam usunięcie wszystkich makr* nie jest zaznaczone, otworzy się nowe wyskakujące okno z prośbą o potwierdzenie usunięcia wszystkich makr.

Zakładka **Mapowanie wartości** umożliwia masową aktualizację mapowań wartości.



Dostępne są przyciski z następującymi opcjami aktualizacji mapowań wartości:

- *Dodaj* — dodaje mapowania wartości do szablonów. Jeśli zaznaczysz opcję *Aktualizuj istniejące*, wszystkie właściwości mapowania wartości o tej nazwie zostaną zaktualizowane. W przeciwnym razie, jeśli mapowanie wartości o tej nazwie już istnieje, nie zostanie zaktualizowane.
- *Aktualizuj* — aktualizuje istniejące mapowania wartości. Jeśli zaznaczysz opcję *Dodaj brakujące*, mapowanie wartości, które wcześniej nie istniało w szablonie, zostanie dodane jako nowe mapowanie wartości. W przeciwnym razie zaktualizowane zostaną tylko te mapowania wartości, które już istnieją w szablonie.
- *Zmień nazwę* — nadaje nową nazwę istniejącemu mapowaniu wartości.
- *Usuń* — usuwa określone mapowania wartości z szablonów. Jeśli zaznaczysz opcję *Z wyjątkiem wybranych*, wszystkie mapowania wartości zostaną usunięte **z wyjątkiem** tych, które zostały wskazane.
- *Usuń wszystkie* — usuwa wszystkie mapowania wartości z szablonów. Jeśli pole wyboru *Potwierdzam usunięcie wszystkich mapowań wartości* nie jest zaznaczone, otworzy się nowe wyskakujące okno z prośbą o potwierdzenie usunięcia.

Opcje *Dodaj z szablonu* i *Dodaj z hosta* są dostępne dla operacji dodawania/aktualizacji mapowań wartości. Umożliwiają one wybór mapowań wartości odpowiednio z szablonu lub hosta.

Po wprowadzeniu wszystkich wymaganych zmian kliknij *Aktualizuj*. Atrybuty zostaną odpowiednio zaktualizowane dla wszystkich wybranych szablonów.

1 Hosty i grupy hostów

Czym jest „host”?

W Zabbix „host” oznacza dowolne urządzenie fizyczne lub wirtualne, aplikację, usługę albo dowolny inny logicznie powiązany zbiór monitorowanych parametrów.

Tworzenie hostów jest jednym z pierwszych zadań związanych z monitorowaniem w Zabbix. Na przykład, jeśli chcesz monitorować niektóre parametry na serwerze „x”, musisz najpierw utworzyć host o nazwie, na przykład, „Serwer X”, a następnie możesz dodać do niego pozycje monitorowania.

Hosty są organizowane w grupy hostów.

Przejdź do:

- Kreator hosta — aby skorzystać z prowadzonego krok po kroku interfejsu do tworzenia i konfigurowania nowego lub istniejącego hosta.
- Konfigurowanie hosta — aby skorzystać z klasycznego podejścia do tworzenia i konfigurowania hosta.

1 Kreator hosta

Przegląd

Kreator hosta to interfejs prowadzony krok po kroku, służący do konfigurowania monitorowanego obiektu (urządzenia, aplikacji, usługi itp.) w Zabbix. Prowadzi on przez następujące kroki:

- Wybór szablonu
- Utworzenie lub wybranie hosta
- Instalacja Zabbix agent lub agent 2
- Dodanie interfejsu hosta
- Zastosowanie dodatkowej konfiguracji do monitorowanego obiektu lub hosta Zabbix (jeśli jest wymagana przez szablon)

Aby uzyskać dostęp do Kreatora hosta w frontendzie Zabbix, wykonaj następujące czynności:

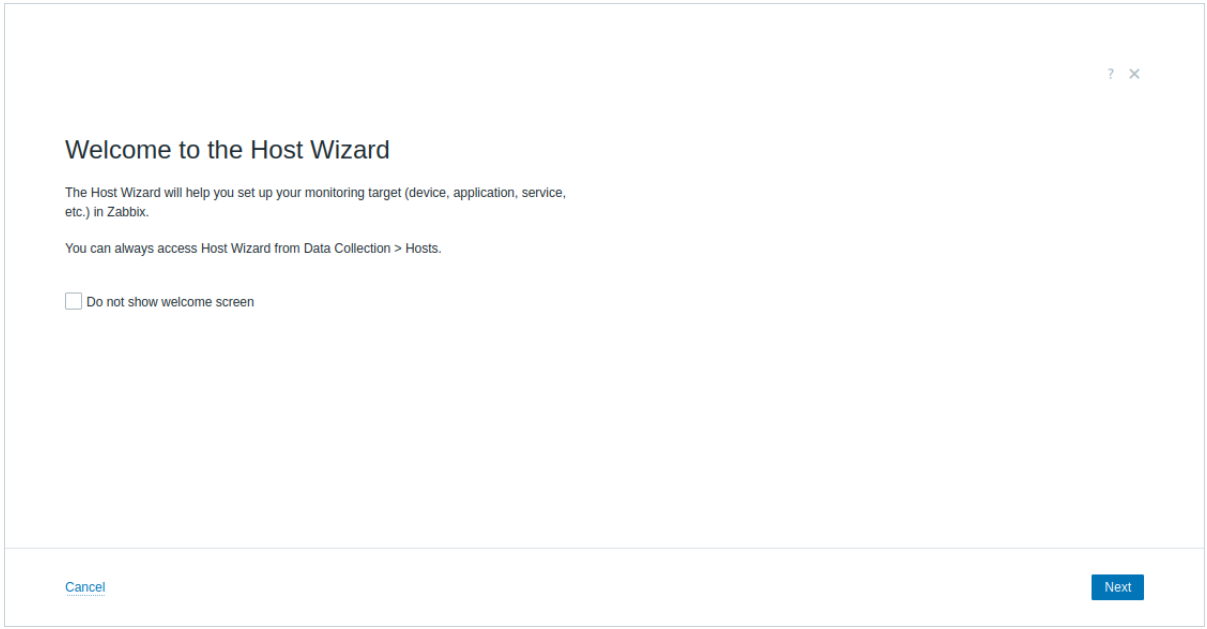
- Przejdź do: *Data collection* > *Hosts*
- Kliknij *Host Wizard* w prawym górnym rogu ekranu
- Postępuj zgodnie z instrukcjami w kreatorze

Możesz także edytować istniejącego hosta, klikając jego nazwę (lub ikonę trzech kropek obok niej) w różnych sekcjach frontendu, aby uzyskać dostęp do Kreatora hosta z poziomu menu hosta. Pamiętaj, że podczas edycji istniejącego hosta niektóre kroki są pomijane, jeśli zawiera on już konfigurację wymaganą przez wybrany szablon.

Alternatywnie możesz skorzystać z klasycznego podejścia do tworzenia i konfigurowania hosta.

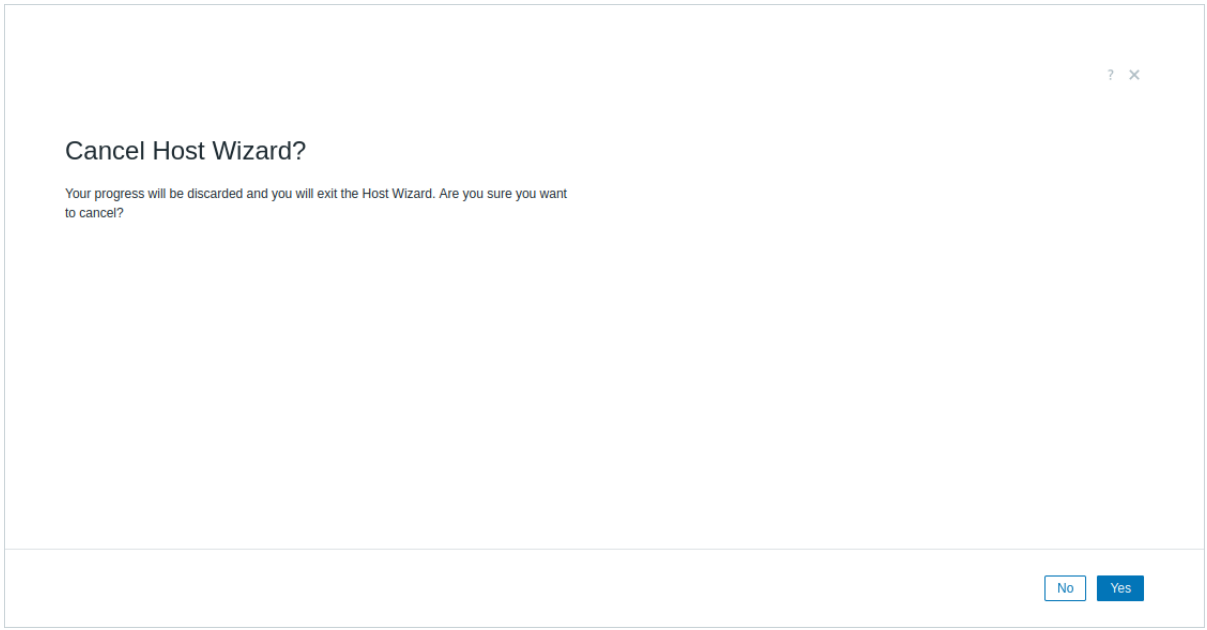
Witamy w kreatorze hosta

Po uruchomieniu kreatora hosta wyświetlany jest ekran powitalny:



Aby pominąć ten ekran w przyszłych sesjach, możesz zaznaczyć pole wyboru *Nie pokazuj ekranu powitalnego* i kliknąć *Dalej*.

Jeśli rozpoczniesz konfigurowanie ustawień w kolejnych krokach kreatora hosta i spróbujesz zamknąć kreator, klikając ikonę zamknięcia lub naciskając ESC, pojawi się ekran potwierdzenia:



Kliknięcie *Tak* spowoduje zamknięcie kreatora hosta bez zapisania postępu. Kliknięcie *Nie*, naciśnięcie ESC lub kliknięcie ikony zamknięcia spowoduje powrót do ostatniego kroku.

Wybierz szablon

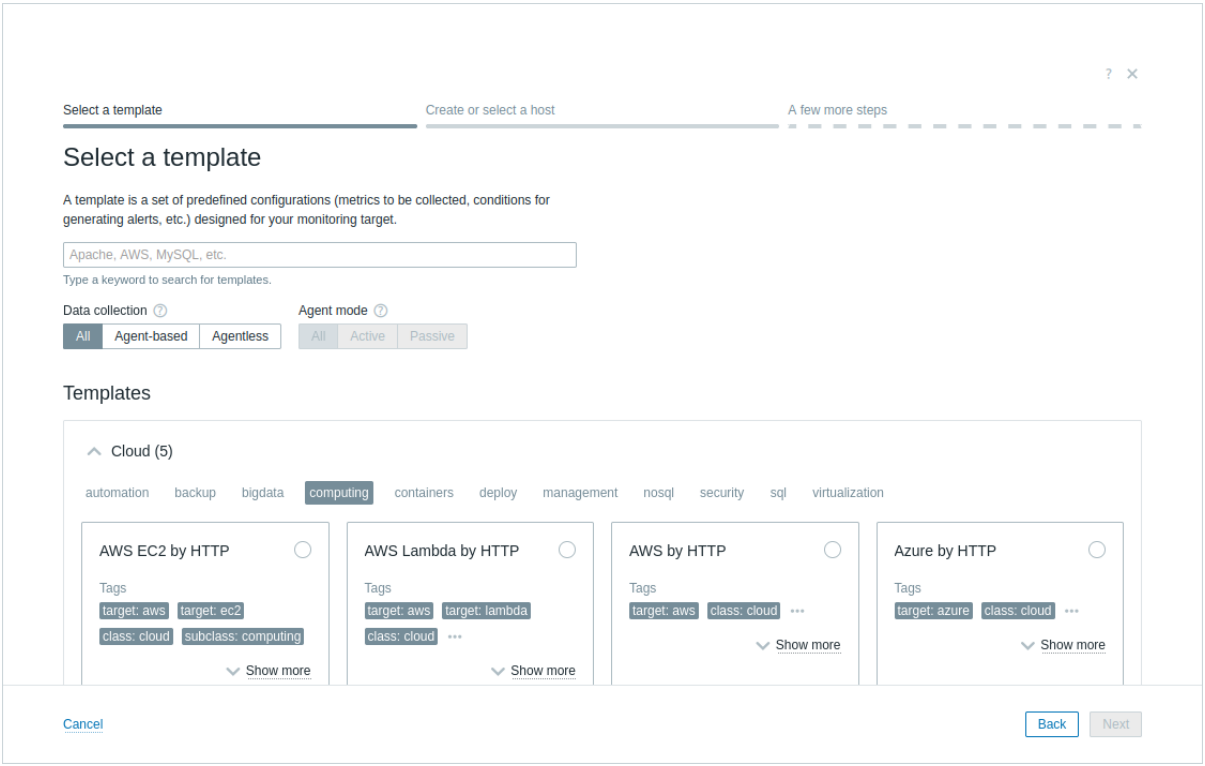
Pierwszym krokiem konfiguracji monitorowanego celu jest wybranie szablonu — zestawu predefiniowanych konfiguracji (metryk do zbierania, warunków generowania alertów itp.) przeznaczonych dla monitorowanego celu.

Gotowe szablony Zabbix oferują różnorodne predefiniowane konfiguracje monitorowania dla systemów operacyjnych, aplikacji, baz danych, urządzeń sieciowych, usług i nie tylko.

W tym kroku możesz:

- Przeglądać szablony według klasy (Cloud, Database, Network itp.) i podklasy (np. automation, backup), opartych na tagach szablonu.
- Wyszukiwać szablony według słów kluczowych w nazwie szablonu lub nazwach i wartościach tagów szablonu.
- Filtrować szablony według metody zbierania danych (z użyciem agenta lub bez agenta; szablony oparte na agencie zawierają co najmniej jedną pozycję Zabbix agent).
- Filtrować szablony według trybu agenta (aktywny lub pasywny; aktywne szablony zawierają co najmniej jedną pozycję Zabbix agent (active), natomiast pasywne szablony zawierają co najmniej jedną pozycję pasywną; szczegóły znajdują się w sekcji Passive and active agent checks).

- Podczas używania Kreatora hosta do konfiguracji istniejącego hosta możesz także filtrować szablony już podłączone do hosta.



Attention:
Podczas wybierania szablonu możesz zobaczyć następujący komunikat: *Niektóre szablony (n) są niezgodne z Kreatorem hosta. Zobacz, jak je zaktualizować. Szablony niestandardowe nie są obsługiwane.* Oznacza to, że niektóre gotowe szablony nie są jeszcze zgodne z Kreatorem hosta i wymagają aktualizacji; zobacz instrukcje aktualizacji szablonów.

Wybrany szablon określi kolejne kroki w Kreatorze hosta. Na przykład, jeśli wybierzesz szablon *MySQL by Zabbix agent*, który używa Zabbix agent do zbierania danych, kreator przeprowadzi Cię przez proces instalacji agenta.

Utwórz lub wybierz host

Szablon musi być podłączony do hosta — encji w Zabbix, która reprezentuje monitorowany obiekt. Po podłączeniu host otrzymuje wszystkie encje szablonu, takie jak pozycje (metryki do zbierania) i wyzwalacze (warunki generowania alertów), które są wymagane do monitorowania.

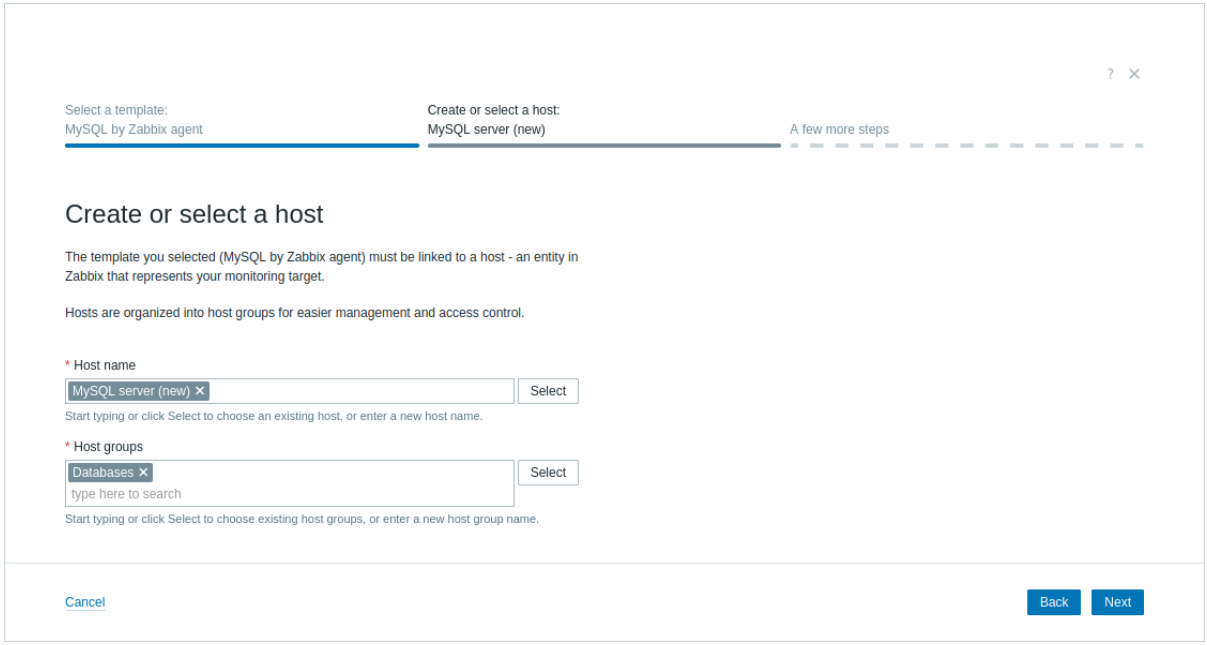
Każdy host musi również należeć do co najmniej jednej grupy hostów, która służy do organizowania hostów i przypisywania do nich uprawnień użytkowników.

W tym kroku możesz:

- Utworzyć nowy host i grupę hostów, wprowadzając nazwy dla obu.
- Utworzyć nowy host, wprowadzając jego nazwę, oraz wybrać istniejącą grupę hostów, do której nowy host zostanie przypisany.
- Wybrać istniejący host; możesz również przypisać tego hosta do dodatkowych grup hostów bez usuwania go z żadnych obecnych grup.

Note:
Wybranie istniejącego hosta nie usuwa ani nie nadpisuje jego bieżącej konfiguracji, chyba że zostanie to wyraźnie wskazane w kolejnych krokach. Wykryte hosty nie mogą zostać wybrane.

Na przykład możesz utworzyć nowy host o nazwie *MySQL server*, aby reprezentował lokalnie zainstalowany serwer MySQL, który chcesz monitorować. Wcześniej wybrany szablon *MySQL by Zabbix agent* zostanie podłączony do tego hosta. Dodatkowo możesz wybrać istniejącą grupę hostów *Databases* (lub utworzyć nową, np. *MySQL servers*), aby uporządkować hosta razem z innymi hostami związanymi z bazami danych i później uprościć zarządzanie uprawnieniami.



Instalacja Zabbix agent

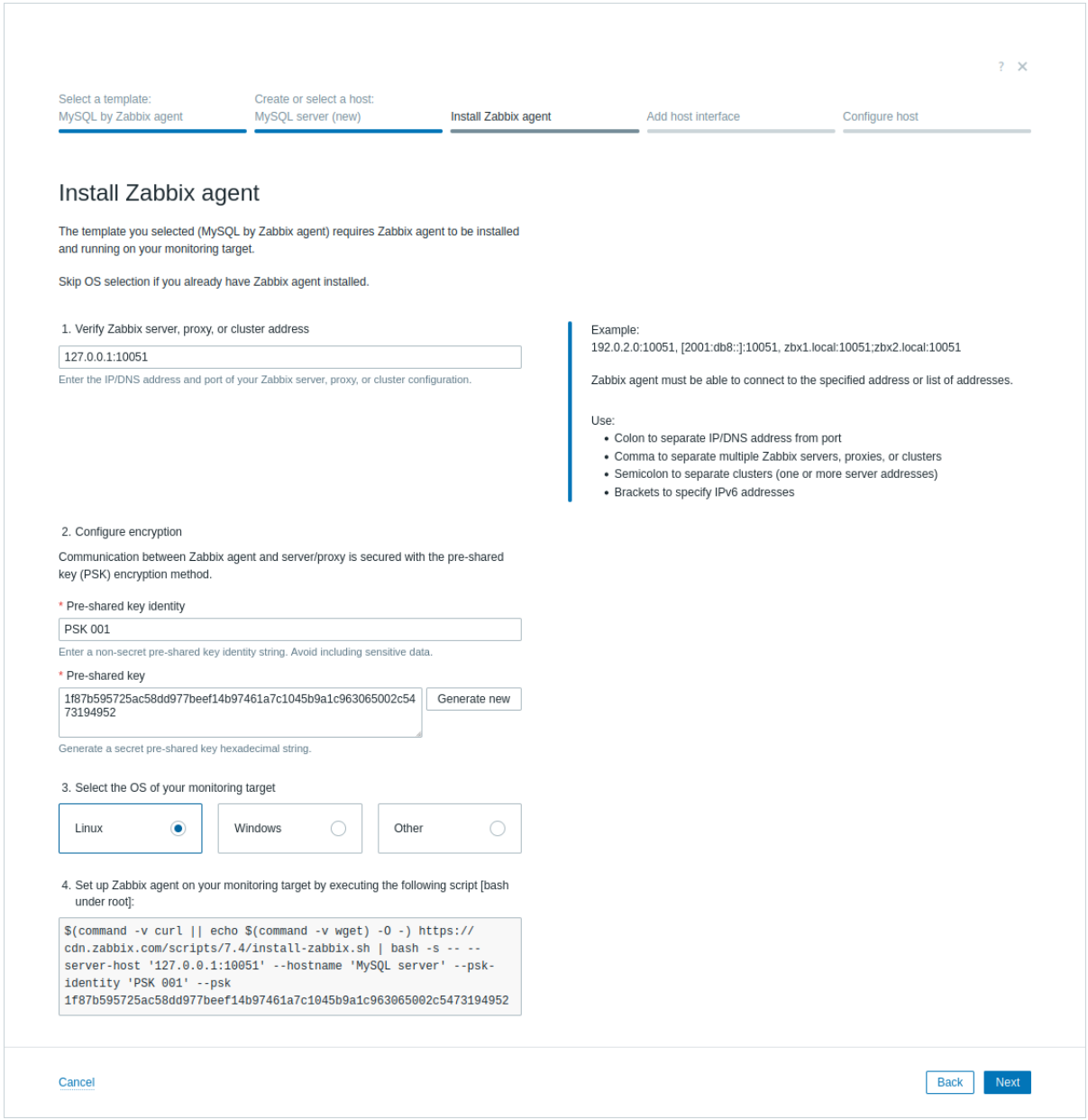
Szablony oparte na agencie (takie jak *MySQL by Zabbix agent*) wymagają zainstalowania Zabbix agent lub agent 2 — procesu wdrażanego na monitorowanym celu w celu aktywnego monitorowania lokalnych zasobów i aplikacji (jeśli wymaga tego szablon).

W tym kroku:

- Zweryfikuj adres serwera, proxy lub klastra Zabbix (np. 192.0.2.0:10051). Ta wartość zostanie użyta do skonfigurowania parametrów Server i ServerActive dla Zabbix agent.
- Wprowadź nową, unikalną i niejawną tożsamość klucza współdzielonego (np. *PSK 001* lub *mysql-agent-psk1*) i wygeneruj klucz współdzielony. Te wartości zostaną użyte do skonfigurowania szyfrowania pre-shared key (PSK) dla hosta Zabbix (np. *serwer MySQL*) i Zabbix agent.
- Wybierz system operacyjny maszyny, na której znajduje się monitorowany cel.
- Zainstaluj Zabbix agent w tym systemie, uruchamiając na nim dostarczony skrypt lub postępując zgodnie z instrukcjami instalacji.

Attention:
Podczas edycji istniejącego hosta konfiguracja PSK nadpisze wszystkie istniejące ustawienia szyfrowania na hoście.

Na przykład możesz ustawić *Pre-shared key identity* na *PSK 001* i wygenerować nowy *Pre-shared key*. Następnie możesz wybrać *Linux* jako system operacyjny i uruchomić dostarczony skrypt w tym systemie. Po zainstalowaniu Zabbix agent wróć do Kreatora hosta.

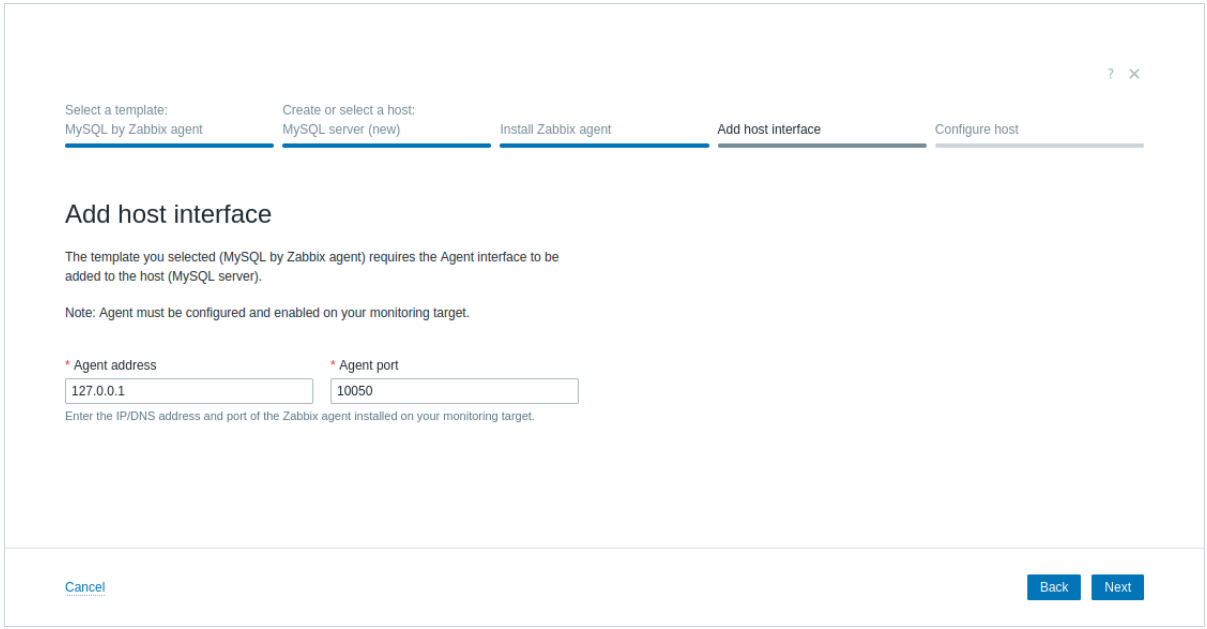


Dodaj interfejs hosta

Interfejs hosta określa, w jaki sposób serwer Zabbix łączy się przez sieć z monitorowanym celem. Definiuje parametry połączenia, takie jak adres IP, nazwa DNS, port oraz typ interfejsu (agent, SNMP, JMX lub IPMI), w zależności od metody zbierania danych wymaganej przez wybrany szablon.

W tym kroku wprowadź szczegóły interfejsu hosta wymagane przez wybrany szablon.

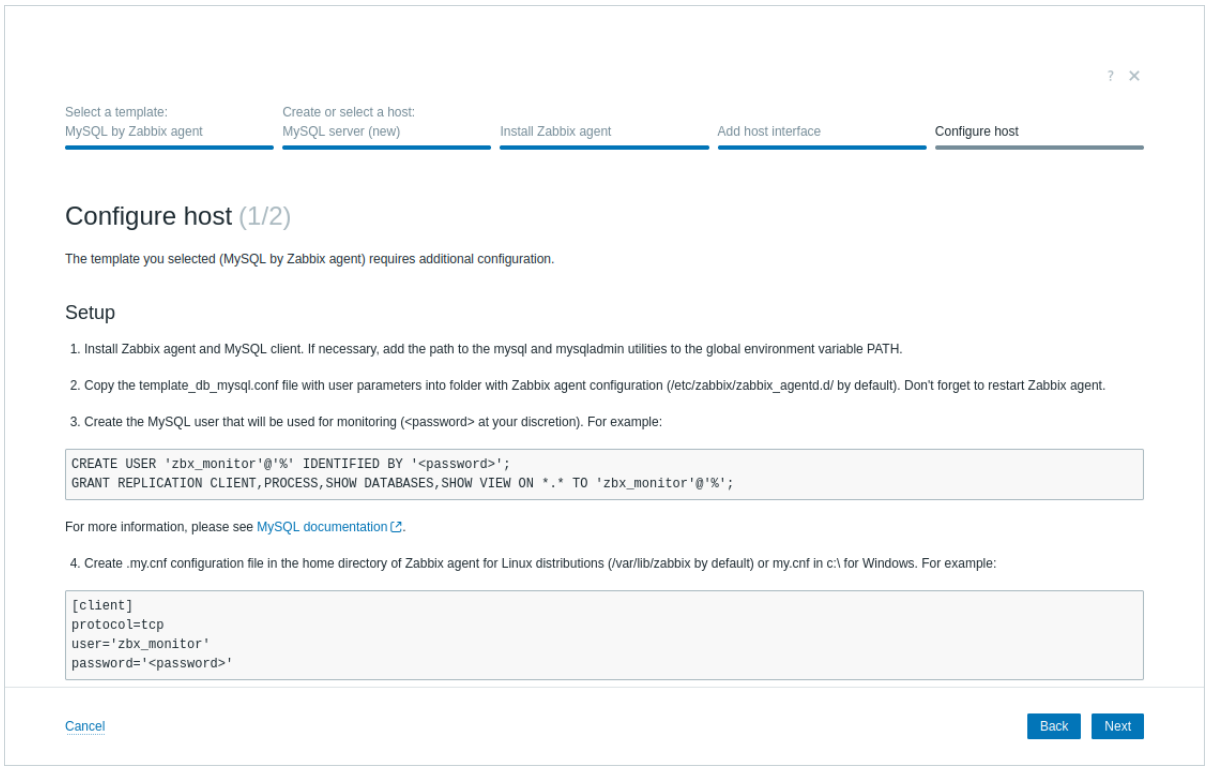
Na przykład możesz użyć domyślnego adresu agenta (127.0.0.1) i portu (10050), jeśli serwer Zabbix, agent Zabbix i serwer MySQL działają lokalnie na tej samej maszynie.



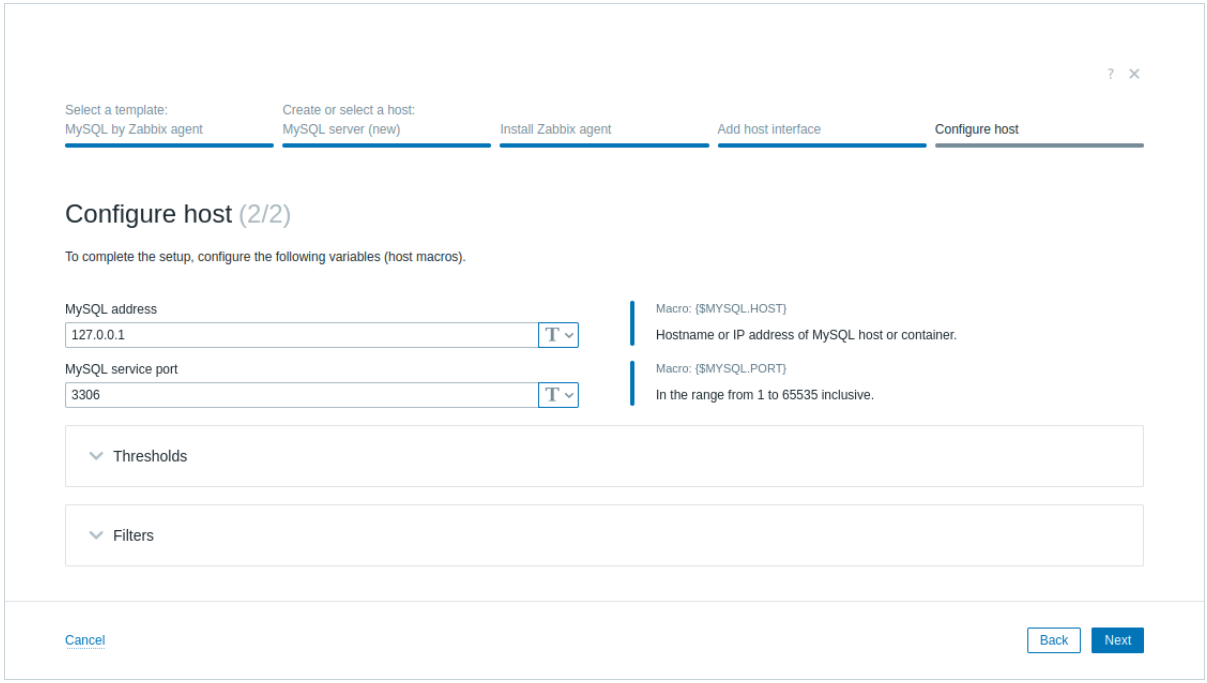
Konfiguracja hosta

Niektóre szablony wymagają dodatkowej konfiguracji, zanim host będzie mógł zostać utworzony. Może to obejmować:

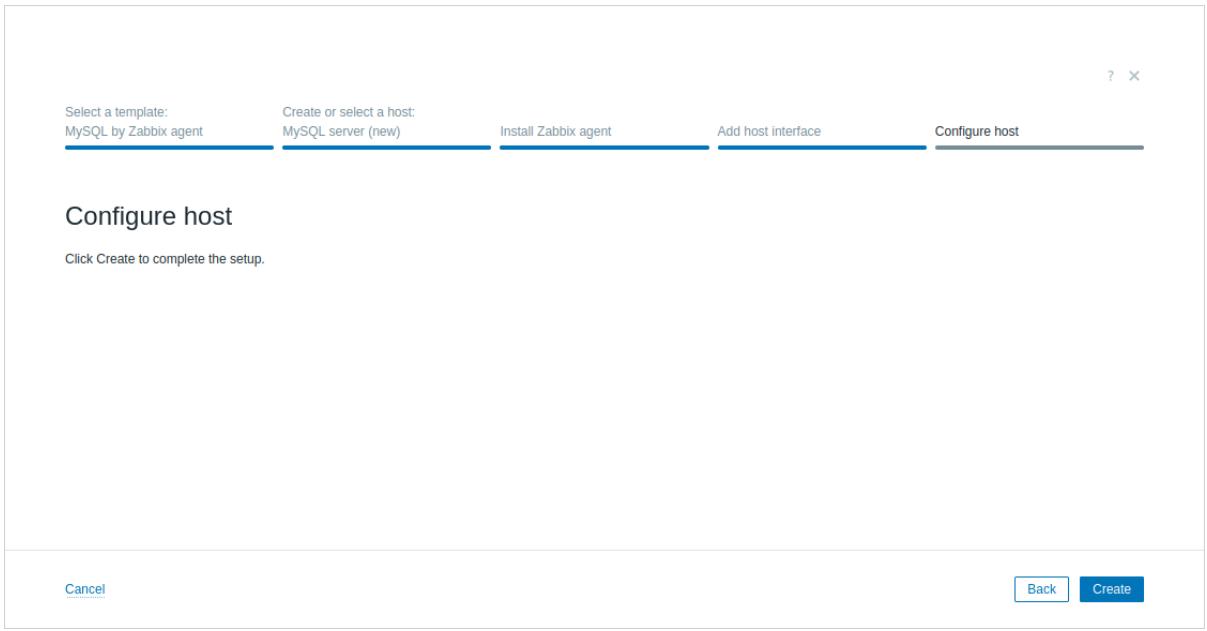
- Ręczną konfigurację monitorowanego celu (np. włączenie określonych usług, utworzenie użytkowników usług lub nadanie uprawnień):



- Definiowanie makr hosta — zmiennych kontrolujących działanie pozycji, ustawienia połączenia, dane uwierzytelniające i inne parametry:



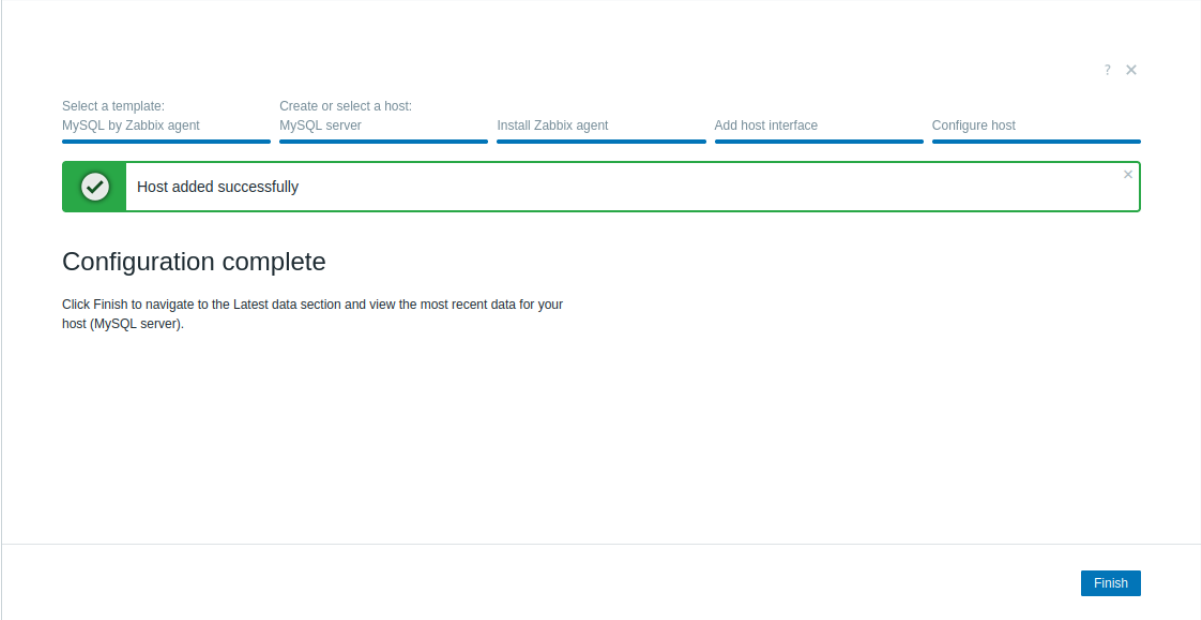
Po wykonaniu wszystkich wymaganych kroków konfiguracji kliknij *Create*, aby dodać host do Zabbix (lub *Update*, aby zaktualizować konfigurację istniejącego hosta):



Konfiguracja zakończona

W tym momencie Zabbix monitoruje już wskazany cel.

W przypadku nowych hostów kliknij *Zakończ*, aby przejść do sekcji Najnowsze dane i wyświetlić najnowsze dane dla swojego hosta. W przypadku istniejących hostów kliknij *Zakończ*, aby zamknąć Kreator hosta i wrócić do ekranu, z którego został otwarty.



2 Konfigurowanie hosta

Przegląd

Aby skonfigurować host w frontend Zabbix, wykonaj następujące kroki:

- Przejdź do: *Data collection* > *Hosts* lub *Monitoring* > *Hosts*
- Kliknij *Create host* w prawym górnym rogu ekranu (lub nazwę hosta, aby edytować istniejący host)
- Wprowadź parametry hosta w formularzu

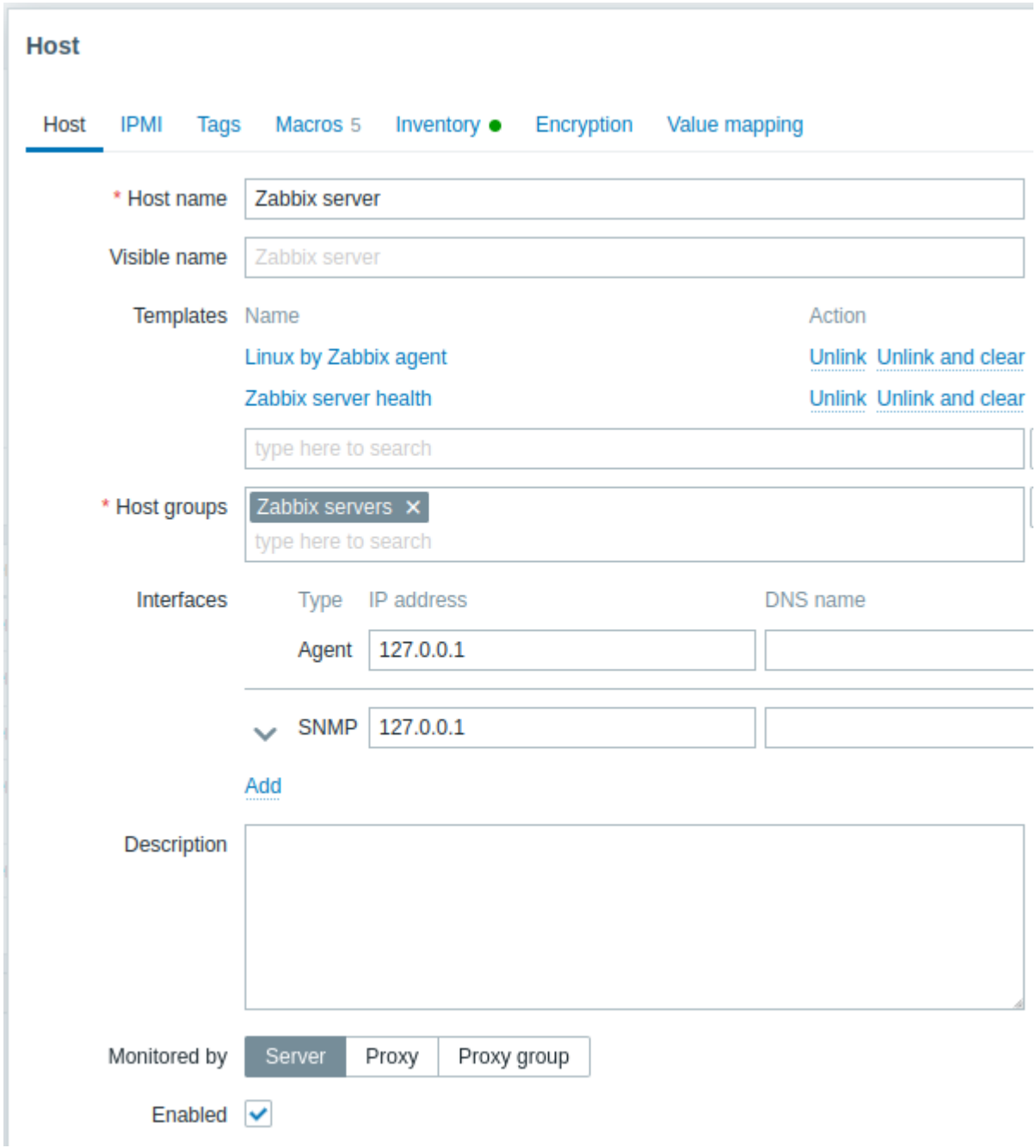
Możesz także użyć przycisku *Clone* w formularzu konfiguracji istniejącego hosta, aby utworzyć nowy host. Ten host będzie miał wszystkie właściwości istniejącego hosta, w tym podłączone szablony, encje (pozycje, wyzwalacze itp.) z tych szablonów, a także encje bezpośrednio przypisane do istniejącego hosta.

Pamiętaj, że po sklonowaniu host zachowa wszystkie encje szablonu w ich oryginalnej postaci z szablonu. Wszelkie zmiany wprowadzone w tych encjach na poziomie istniejącego hosta (takie jak zmieniony interwał pozycji, zmodyfikowane wyrażenie regularne lub dodane prototypy do reguły wykrywania niskopoziomowego) nie zostaną sklonowane do nowego hosta; zamiast tego będą one takie jak w szablonie.

Alternatywnie możesz użyć Kreatora hosta, aby skonfigurować host za pomocą prowadzonego, krok po kroku interfejsu.

Konfiguracja

Karta **Host** zawiera ogólne atrybuty hosta:



Wszystkie wymagane pola wejściowe są oznaczone czerwoną gwiazdką.

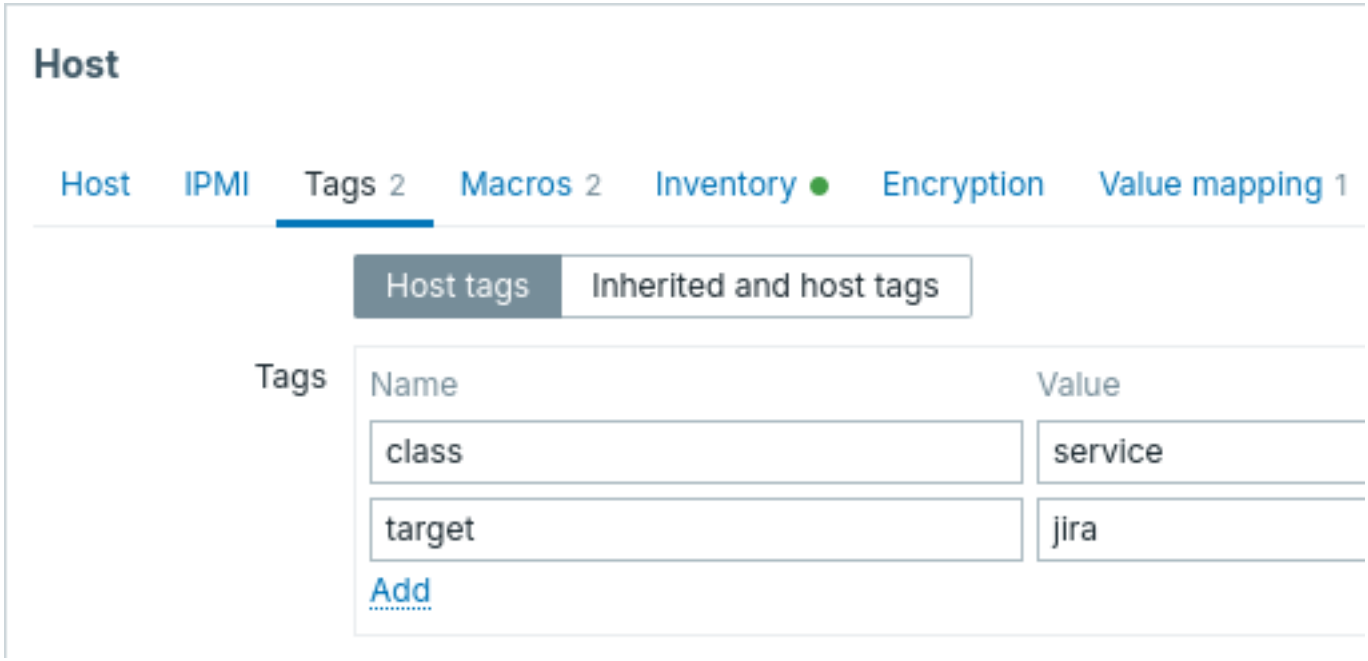
Parametr	Opis
Host name	Wprowadź unikalną nazwę hosta. Dozwolone są znaki alfanumeryczne, spacje, kropki, myślniki i podkreślenia. Jednak spacje na początku i na końcu są niedozwolone. *Uwaga:* Jeśli na konfigurowanym hoście działa Zabbix agent, parametr *Hostname* w pliku konfiguracyjnym agenta musi mieć taką samą wartość jak nazwa hosta wprowadzona tutaj. Nazwa w parametrze jest potrzebna do przetwarzania active checks.
Visible name	Wprowadź unikalną widoczną nazwę hosta. Jeśli ustawisz tę nazwę, będzie ona widoczna na listach, mapach itp. zamiast technicznej nazwy hosta. Ten atrybut obsługuje UTF-8.

Parametr	Opis
Templates	Powiąż szablony z hostem. Wszystkie encje (pozycje, wyzwalacze, itd.) zostaną odziedziczone z szablonu. Aby powiązać nowy szablon, zacznij wpisywać nazwę szablonu w tekstowym polu wejściowym. Pojawi się lista pasujących szablonów; przewiń ją, aby wybrać odpowiedni. Alternatywnie możesz kliknąć *Select* obok pola i wybrać szablony z listy w wyskakującym oknie. Wszystkie wybrane szablony zostaną powiązane z hostem po zapisaniu lub zaktualizowaniu formularza konfiguracji hosta. Aby odłączyć szablon, użyj jednej z dwóch opcji w bloku *Linked templates*: *Unlink* - odłącza szablon, ale zachowuje jego encje (pozycje, wyzwalacze, itd.); *Unlink and clear* - odłącza szablon i usuwa wszystkie jego encje (pozycje, wyzwalacze, itd.). Wyświetlane nazwy szablonów są klikalnymi odnośnikami prowadzącymi do formularza konfiguracji szablonu.
Host groups	Wybierz grupy hostów, do których należy host. Host musi należeć przynajmniej do jednej grupy hostów. Nową grupę można utworzyć i powiązać z hostem, dodając nazwę nieistniejącej grupy.
Interfaces	Dla hosta obsługiwanych jest kilka typów interfejsów: *Agent*, *SNMP*, *JMX* i *IPMI*. Domyślnie nie są zdefiniowane żadne interfejsy. Aby dodać nowy interfejs, kliknij *Add* w bloku *Interfaces*, wybierz typ interfejsu i wprowadź informacje *IP/DNS*, *Connect to* oraz *Port*. *Uwaga:* Interfejsy używane w dowolnych pozycjach nie mogą zostać usunięte, a odnośnik *Remove* jest dla nich wyszarzony. „IP" lub „DNS" z interfejsu SNMP jest również używane dla SNMP traps. Podczas dopasowywania używane jest tylko wybrane „IP" lub „DNS" w interfejsie hosta. Zobacz Configuring SNMP monitoring, aby uzyskać dodatkowe informacje o konfiguracji interfejsu SNMP (v1, v2 i v3).
IP address	Adres IP hosta (opcjonalnie).
DNS name	Nazwa DNS hosta (opcjonalnie).
Connect to	Kliknięcie odpowiedniego przycisku określa, czego Zabbix server ma używać do pobierania danych z agentów: **IP** - połącz z adresem IP hosta (zalecane) **DNS** - połącz z nazwą DNS hosta
Port	Numer portu TCP/UDP. Wartości domyślne to: 10050 dla Zabbix agent, 161 dla agenta SNMP, 12345 dla JMX i 623 dla IPMI.
Default	Zaznacz przycisk opcji, aby ustawić interfejs domyślny.
Description	Wprowadź opis hosta.
Monitored by	Wybierz, czy host jest monitorowany przez: **Server** - host jest monitorowany przez Zabbix server; **Proxy** - host jest monitorowany przez samodzielny proxy; **Proxy group** - host jest monitorowany przez grupę proxy.
Proxy	Wyświetlana jest nazwa przypisanego proxy (tylko jeśli Zabbix server przypisał go z wybranej grupy proxy). To pole jest wyświetlane tylko wtedy, gdy host jest monitorowany przez grupę proxy.
Enabled	Gdy pole wyboru jest zaznaczone, host jest włączony — gotowy do monitorowania. Gdy pole wyboru jest odznaczone, host jest wyłączony — nie jest monitorowany: W przypadku pasywnych żądań danych inicjowanych przez Zabbix server/proxy (na przykład Zabbix agent, SNMP agent, simple checks), monitorowanie zostaje wyłączone po synchronizacji konfiguracji. Wyzwalacze i akcje powiązane z hostem również są wyłączane dopiero po ponownym wczytaniu konfiguracji. W przypadku active checks Zabbix agent monitorowanie zatrzymuje się w czasie (około 5 sekund), w którym Zabbix agent otrzymuje informację o wyłączeniu hosta. W tym krótkim przedziale host nadal będzie lokalnie zbierał dane dla active checks i próbował wysyłać je do serwera/proxy; jednak ponieważ host jest oznaczony jako *Disabled*, serwer/proxy odrzuci te dane. Po wyłączeniu hosta jego pozycje są natychmiast usuwane z pamięci podręcznej historii (z wyjątkiem ich ostatnich wartości, które są zachowywane dla logów).

Karta **IPMI** zawiera atrybuty zarządzania IPMI.

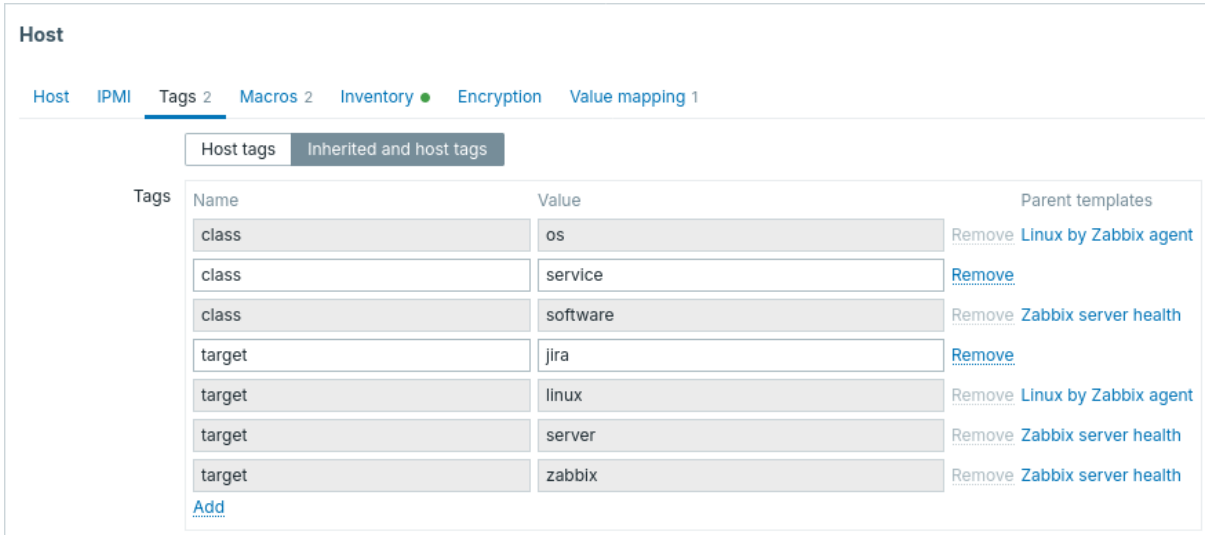
Parametr	Opis
Authentication algorithm	Wybierz algorytm uwierzytelniania.
Privilege level	Wybierz poziom uprawnień.
Username	Nazwa użytkownika do uwierzytelniania. Można używać makr użytkownika.
Password	Hasło do uwierzytelniania. Można używać makr użytkownika.

Karta **Tags** umożliwia definiowanie tagów na poziomie hosta. Wszystkie problemy tego hosta będą oznaczone tagami z wartościami wprowadzonymi tutaj.



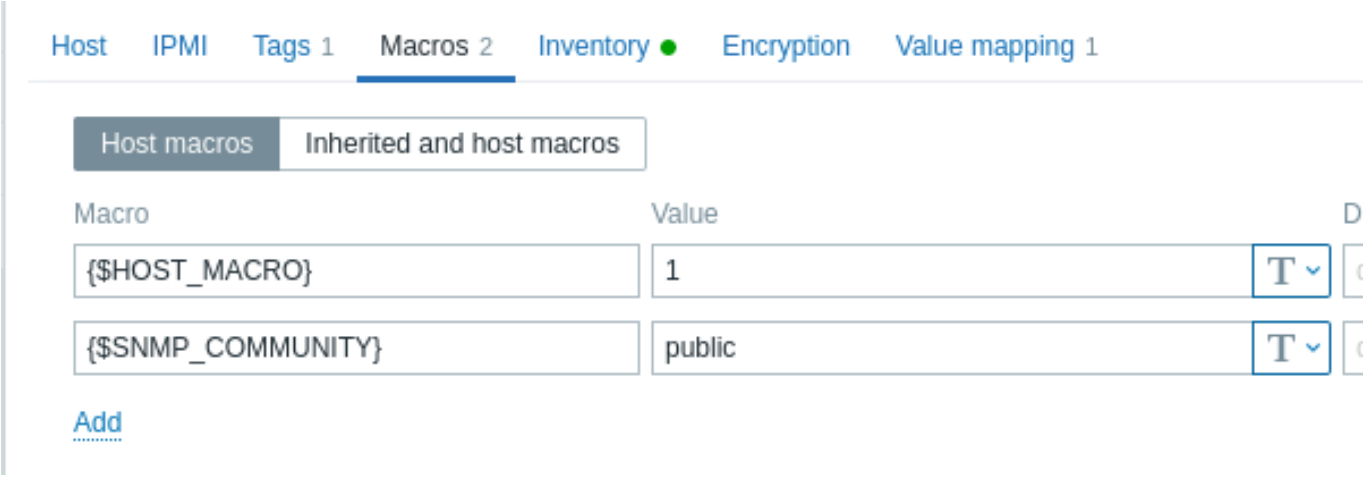
W tagach obsługiwane są makra użytkownika, makra {INVENTORY.*}, {HOST.HOST}, {HOST.NAME}, {HOST.CONN}, {HOST.DNS}, {HOST.IP}, {HOST.PORT} oraz {HOST.ID}.

Możesz również wyświetlić tutaj tagi na poziomie szablonu, jeśli wybierzesz opcję *Inherited and host tags*. W tym miejscu wyświetlane są wszystkie zdefiniowane tagi użytkownika dla hosta wraz z ich pochodzeniem.

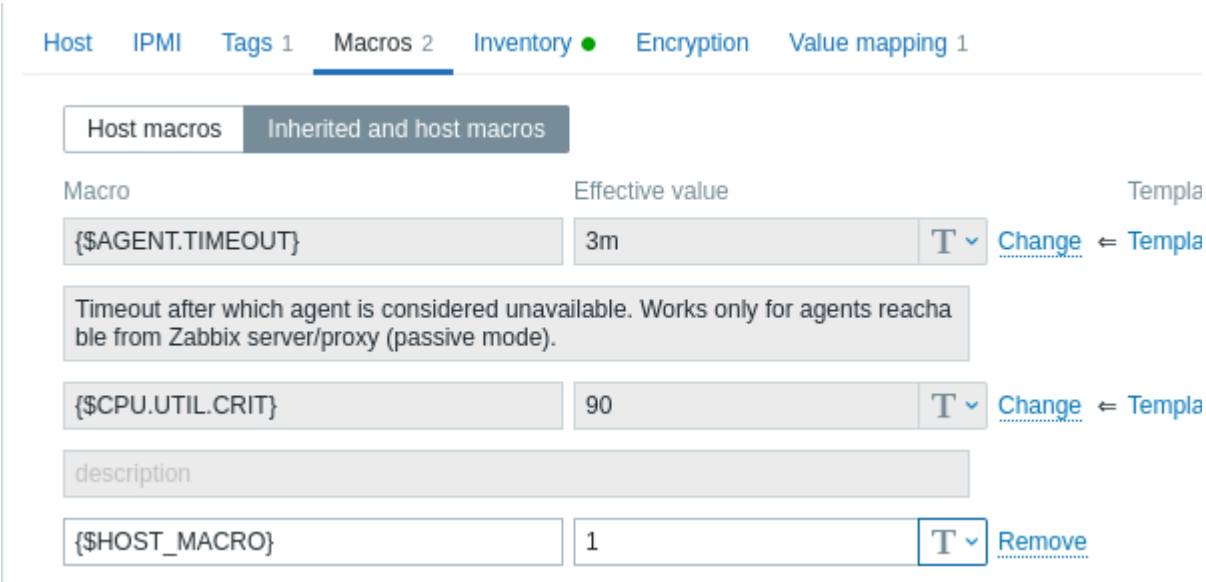


Dla wygody udostępniono odnośniki do odpowiednich szablonów.

Karta **Macros** umożliwia definiowanie makr użytkownika na poziomie hosta jako par nazwa-wartość. Pamiętaj, że wartości makr mogą być przechowywane jako zwykły tekst, tajny tekst lub sekret Vault. Obsługiwane jest również dodawanie opisu.

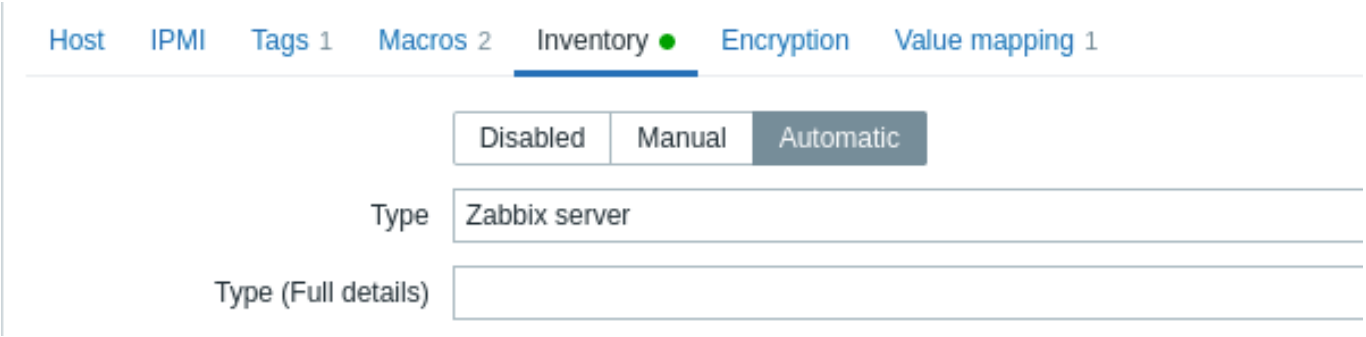


Możesz również wyświetlić tutaj makra użytkownika na poziomie szablonu i globalnym, jeśli wybierzesz opcję *Inherited and host macros*. W tym miejscu wyświetlane są wszystkie zdefiniowane makra użytkownika dla hosta wraz z wartością, do której są rozwijane, oraz ich pochodzeniem.



Dla wygody udostępniono odnośniki do odpowiednich szablonów oraz konfiguracji makr globalnych. Można również edytować makro szablonu/globalne na poziomie hosta, co w praktyce tworzy kopię makra na hoście.

Karta **Inventory** umożliwia ręczne wprowadzanie informacji inventory dla hosta. Możesz także wybrać włączenie *Automatic* uzupełniania inventory lub wyłączyć uzupełnianie inventory dla tego hosta.



Jeśli inventory jest włączone (ręcznie lub automatycznie), przy nazwie karty wyświetlana jest zielona kropka.

Szyfrowanie

Zakładka **Szyfrowanie** umożliwia wymaganie szyfrowanych połączeń z hostem.

Parametr	Opis
Połączenia do hosta	Określa, w jaki sposób serwer lub proxy Zabbix łączy się z agent Zabbix na hoście: bez szyfrowania (domyślnie), przy użyciu PSK (klucza współdzielonego) lub certyfikatu.

Parametr	Opis
Połączenia z hosta	Wybierz, jakie typy połączeń są dozwolone z hosta (tj. z agent Zabbix i Zabbix sender). Jednocześnie można wybrać kilka typów połączeń (co jest przydatne podczas testowania i przełączania na inny typ połączenia). Wartością domyślną jest „Bez szyfrowania”.
Issuer	Dozwolony wystawca certyfikatu. Certyfikat jest najpierw weryfikowany przez CA (urząd certyfikacji). Jeśli jest prawidłowy i podpisany przez CA, pole *Issuer* może zostać użyte do dalszego ograniczenia dozwolonych CA. To pole jest przeznaczone do użycia, jeśli instalacja Zabbix korzysta z certyfikatów od wielu CA. Jeśli to pole jest puste, akceptowany jest dowolny CA.
Subject	Dozwolony podmiot certyfikatu. Certyfikat jest najpierw weryfikowany przez CA. Jeśli jest prawidłowy i podpisany przez CA, pole *Subject* może zostać użyte do dopuszczenia tylko jednej wartości ciągu *Subject*. Jeśli to pole jest puste, akceptowany jest dowolny prawidłowy certyfikat podpisany przez skonfigurowany CA.
PSK identity	Ciąg identyfikacyjny klucza współdzielonego. Nie umieszczaj poufnych informacji w identyfikatorze PSK, ponieważ jest on przesyłany przez sieć bez szyfrowania, aby poinformować odbiorcę, którego PSK należy użyć.
PSK	Klucz współdzielony (ciąg szesnastkowy). Maksymalna długość: 512 cyfr szesnastkowych (256-bajtowy PSK), jeśli Zabbix używa biblioteki GnuTLS lub OpenSSL, 64 cyfry szesnastkowe (32-bajtowy PSK), jeśli Zabbix używa biblioteki mbed TLS (PolarSSL). Przykład: 1f87b595725ac58dd977beef14b97461a7c1045b9a1c963065002c5473194952

Mapowanie wartości

Zakładka **Mapowanie wartości** umożliwia skonfigurowanie przyjaznej dla użytkownika reprezentacji danych pozycji w mapowaniach wartości.

3 Konfigurowanie grupy hostów

Przegląd

Grupy hostów służą do logicznego grupowania hostów oraz przypisywania do nich uprawnień użytkowników.

Każdy host musi mieć przypisaną co najmniej jedną grupę hostów. Host może należeć do wielu grup hostów, a każda grupa hostów może zawierać wiele hostów.

Należy pamiętać, że w Zabbix wszystkie uprawnienia są oparte na grupach: grupach użytkowników, grupach hostów oraz grupach szablonów. Dlatego nawet jeśli pojedynczy użytkownik potrzebuje dostępu do pojedynczego hosta, jest on przyznawany przez dodanie użytkownika do grupy użytkowników, która ma uprawnienia dostępu do grupy hostów zawierającej tego hosta.

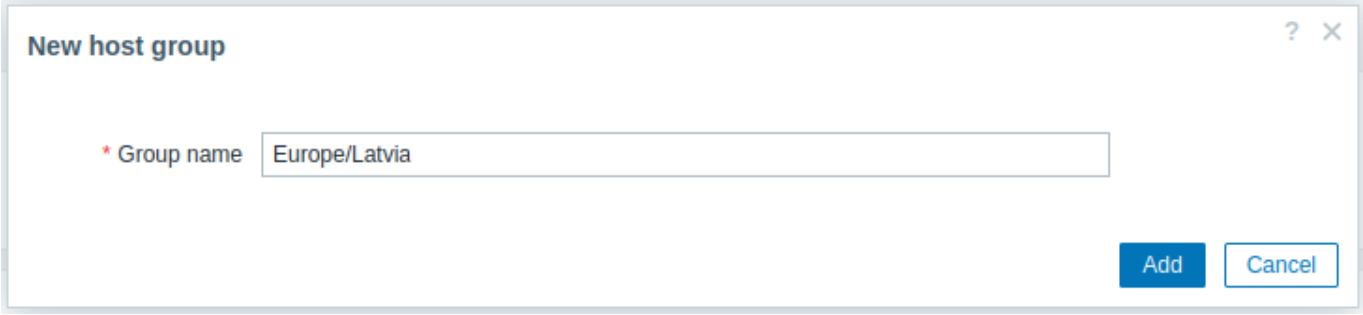
Konfiguracja

> **Attention:**
> Tylko użytkownicy typu Super admin mogą tworzyć grupy hostów.

Istnieją dwie opcje tworzenia grupy hostów w frontend Zabbix.

Opcja pierwsza:

- Przejdź do: *Data collection* → *Host groups*
- Kliknij *Create host group* w prawym górnym rogu ekranu
- Wprowadź nazwę grupy w formularzu



Opcja druga: podczas konfigurowania hosta wprowadź nieistniejącą nazwę grupy w polu *Host groups*.

Po utworzeniu grupy hostów możesz kliknąć nazwę grupy na liście w sekcji *Data collection* → *Host groups*, aby edytować nazwę grupy, sklonować grupę lub ją usunąć.

Usunięcie grupy hostów powoduje usunięcie tylko grupy logicznej, a nie hostów w tej grupie. Nie można usunąć grupy hostów, która jest jedyną grupą dla jakiegokolwiek istniejącego hosta.

Tworzenie podgrup hostów

Podgrupa hostów (lub zagnieżdżona grupa hostów) jest elementem podrzędnym nadrzędnej grupy hostów, która ją zawiera.

Podgrupę tworzy się przy użyciu ukośnika '/' w polu wprowadzania nazwy grupy, aby określić jej relację do grupy nadrzędnej lub grup nadrzędnych. Na przykład:

- wpisanie `Europe/Latvia` tworzy podgrupę `Europe/Latvia` w nadrzędnej grupie `Europe`.
- wpisanie `Europe/Latvia/Riga/Zabbix servers` tworzy odpowiednią podgrupę w zagnieżdżonych grupach nadrzędnych `Europe`, `Europe/Latvia`, `Europe/Latvia/Riga`.

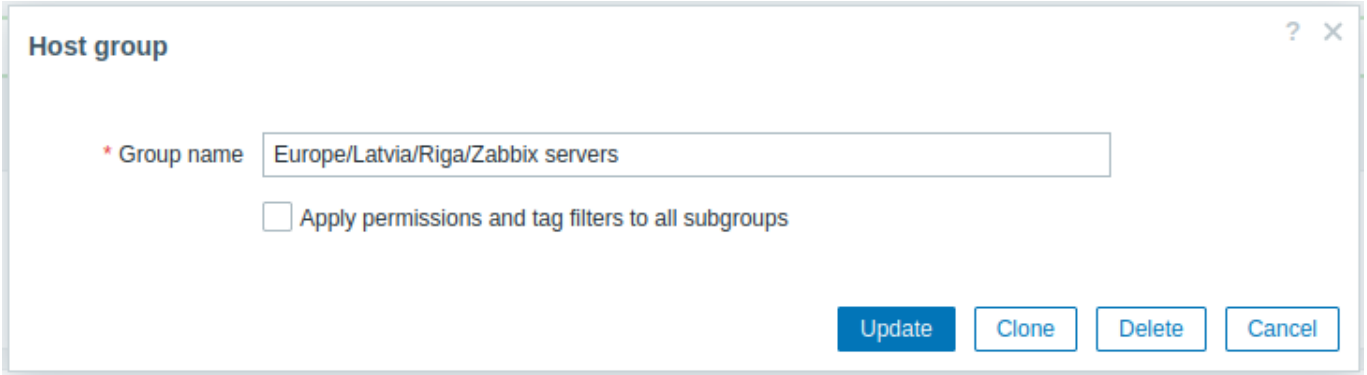
Podczas tworzenia podgrupy nie można używać ukośników na początku ani na końcu nazwy, ani kilku ukośników z rzędu. Escapowanie znaku '/' nie jest obsługiwane.

Nie jest wymagane tworzenie żadnych nadrzędnych grup hostów przed utworzeniem podgrupy. Możesz zdecydować, czy zacząć od utworzenia podgrupy (na przykład `Europe/Latvia`), czy dowolnej nadrzędnej grupy hostów (w naszym przykładzie `Europe`). Jeśli zaczniesz od utworzenia podgrupy, nadrzędne grupy hostów **nie** zostaną utworzone automatycznie.

Uprawnienia do grup hostów

- Podczas tworzenia podgrupy w istniejącej nadrzędnej grupie hostów (na przykład tworzenia `Europe/Latvia`, gdy `Europe` już istnieje), uprawnienia grupy użytkowników do podgrupy są dziedziczone z grupy nadrzędnej.
- Podczas tworzenia nadrzędnej grupy hostów dla istniejącej podgrupy (na przykład tworzenia `Europe`, gdy `Europe/Latvia` już istnieje), żadne uprawnienia do grupy nadrzędnej nie są ustawiane.

Podczas edycji dowolnej grupy hostów można również ustawić dodatkową opcję: *Zastosuj uprawnienia i filtry tagów do wszystkich podgrup*.



Zaznaczenie tego pola wyboru i kliknięcie *Aktualizuj* spowoduje zastosowanie tego samego poziomu uprawnień i filtrów tagów do wszystkich obecnych i przyszłych podgrup edytowanej grupy hostów.

Jeśli więc jakimkolwiek grupom użytkowników przyznano różne uprawnienia do podgrup edytowanej grupy hostów, zaznaczenie tego pola wyboru nada wszystkim obecnym i przyszłym podgrupom takie same uprawnienia użytkowników i uprawnienia oparte na tagach jak w edytowanej grupie.

Należy pamiętać, że ta opcja nie jest zapisywana w bazie danych i zastąpi istniejące uprawnienia. Wszelkie zmiany wprowadzone za pomocą tej opcji można cofnąć wyłącznie ręcznie.

4 Inwentaryzacja

Przegląd

Możesz przechowywać inwentarz urządzeń sieciowych w Zabbix.

W Zabbix frontend dostępne jest specjalne menu *Inwentarz*. Jednak początkowo nie zobaczysz tam żadnych danych i nie jest to miejsce do ich wprowadzania. Tworzenie danych inwentarza odbywa się ręcznie podczas konfigurowania hosta lub automatycznie przy użyciu niektórych opcji automatycznego uzupełniania.

Tworzenie inwentarza

Tryb ręczny

Podczas konfigurowania hosta, na karcie *Inventory* można wprowadzić takie szczegóły, jak typ urządzenia, numer seryjny, lokalizacja, osoba odpowiedzialna, adresy URL itp. — dane, które wypełnią informacje inwentaryzacyjne.

Jeśli adres URL jest zawarty w informacjach inwentaryzacyjnych hosta i zaczyna się od „http” lub „https”, w sekcji *Inventory* będzie wyświetlany jako klikalny link.

Tryb automatyczny

Inwentarz hosta może być również uzupełniany automatycznie. Aby to działało, podczas konfigurowania hosta tryb inwentarza na karcie *Inventory* musi być ustawiony na *Automatic*.

Następnie można skonfigurować pozycje hosta, aby uzupełniały dowolne pole inwentarza hosta swoją wartością, wskazując pole docelowe za pomocą odpowiedniego atrybutu (o nazwie *Item will populate host inventory field*) w konfiguracji pozycji.

Pozycje szczególnie przydatne do automatycznego zbierania danych inwentarzowych:

- system.hw.chassis[full|type|vendor|model|serial] — domyślnie [full], wymagane uprawnienia root
- system.hw.cpu[all|cpunum,full|maxfreq|vendor|model|curfreq] — domyślnie [all,full]
- system.hw.devices[pci|usb] — domyślnie [pci]
- system.hw.macaddr[interface,short|full] — domyślnie [all,full], interface jest wyrażeniem regularnym
- system.sw.arch
- system.sw.os[name|short|full] — domyślnie [name]
- system.sw.packages[regexp,manager,short|full] — domyślnie [all,all,full]

Wybór trybu inwentaryzacji

Tryb inwentaryzacji można wybrać w formularzu konfiguracji hosta.

Domyślny tryb inwentaryzacji dla nowych hostów jest wybierany na podstawie ustawienia *Default host inventory mode* w *Administration → General → Other*.

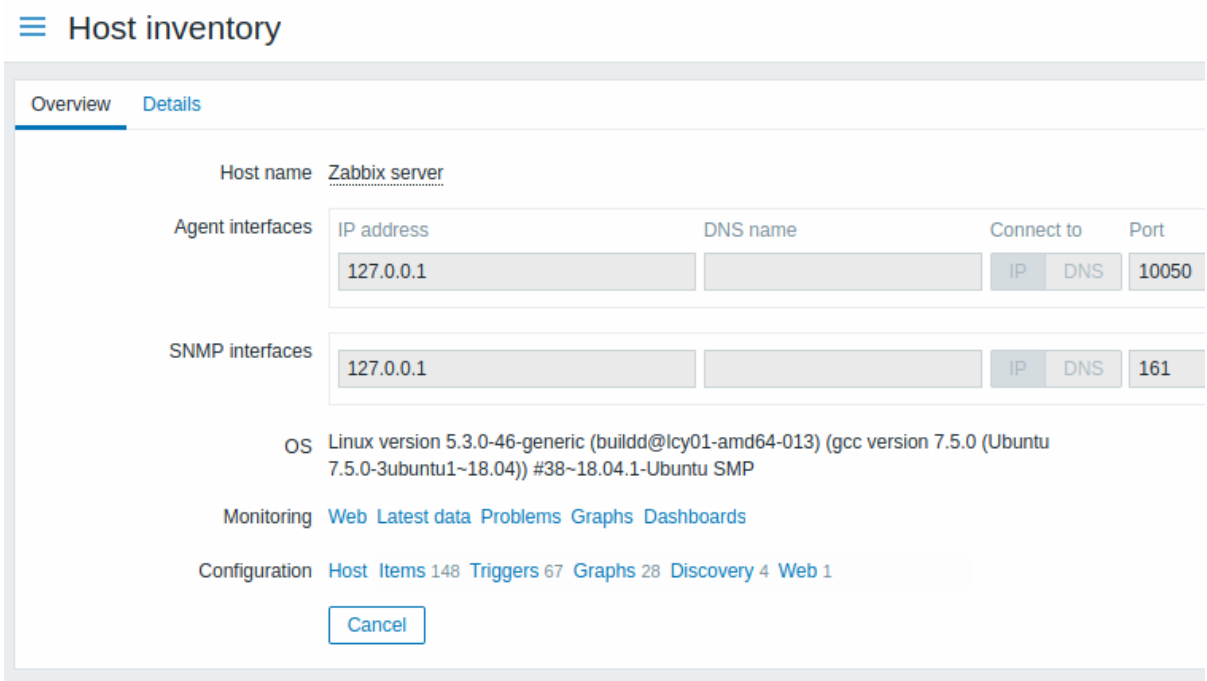
Dla hostów dodanych przez wykrywanie sieci lub akcje autorejestracji można zdefiniować operację *Set host inventory mode*, wybierając tryb ręczny lub automatyczny. Ta operacja zastępuje ustawienie *Default host inventory mode*.

Przegląd inwentaryzacji

Szczegóły wszystkich istniejących danych inwentaryzacyjnych są dostępne w menu *Inventory*.

W *Inventory → Overview* można uzyskać liczbę hostów według różnych pól inwentaryzacji.

W *Inventory → Hosts* można zobaczyć wszystkie hosty, które mają informacje inwentaryzacyjne. Kliknięcie nazwy hosta spowoduje wyświetlenie szczegółów inwentaryzacji w formularzu.



Karta **Overview** pokazuje:

Parameter	Description
Host name	Nazwa hosta. Kliknięcie nazwy otwiera menu ze skryptami zdefiniowanymi dla hosta. Nazwa hosta jest wyświetlana z pomarańczową ikoną, jeśli host jest w trybie konserwacji.
Visible name	Widoczna nazwa hosta (jeśli została zdefiniowana).

Parameter	Description
Host (Agent, SNMP, JMX, IPMI) interfaces	Ten blok zawiera szczegóły interfejsów skonfigurowanych dla hosta.
OS	Pole inwentaryzacji systemu operacyjnego hosta (jeśli zostało zdefiniowane).
Hardware	Pole inwentaryzacji sprzętu hosta (jeśli zostało zdefiniowane).
Software	Pole inwentaryzacji oprogramowania hosta (jeśli zostało zdefiniowane).
Description	Opis hosta.
Monitoring	Łącza do sekcji monitorowania z danymi dla tego hosta: *Web*, *Latest data*, *Problems*, *Graphs*, *Dashboards*.
Configuration	Łącza do sekcji konfiguracji dla tego hosta: *Host*, *Items*, *Triggers*, *Graphs*, *Discovery*, *Web*. Liczba skonfigurowanych encji jest podana po każdym łączu.

Karta **Details** pokazuje wszystkie wypełnione pola inwentaryzacji (nie są puste).

Makra inwentarza

Dostępne są makra inwentarza hosta {INVENTORY.*}, których można używać w powiadomieniach, na przykład:

„Serwer w {INVENTORY.LOCATION1} ma problem, osobą odpowiedzialną jest {INVENTORY.CONTACT1}, numer telefonu {INVENTORY.POC.PRIMARY.PHONE.A1}.”

Aby uzyskać więcej szczegółów, zobacz stronę Obsługiwane makra.

5 Aktualizacja masowa

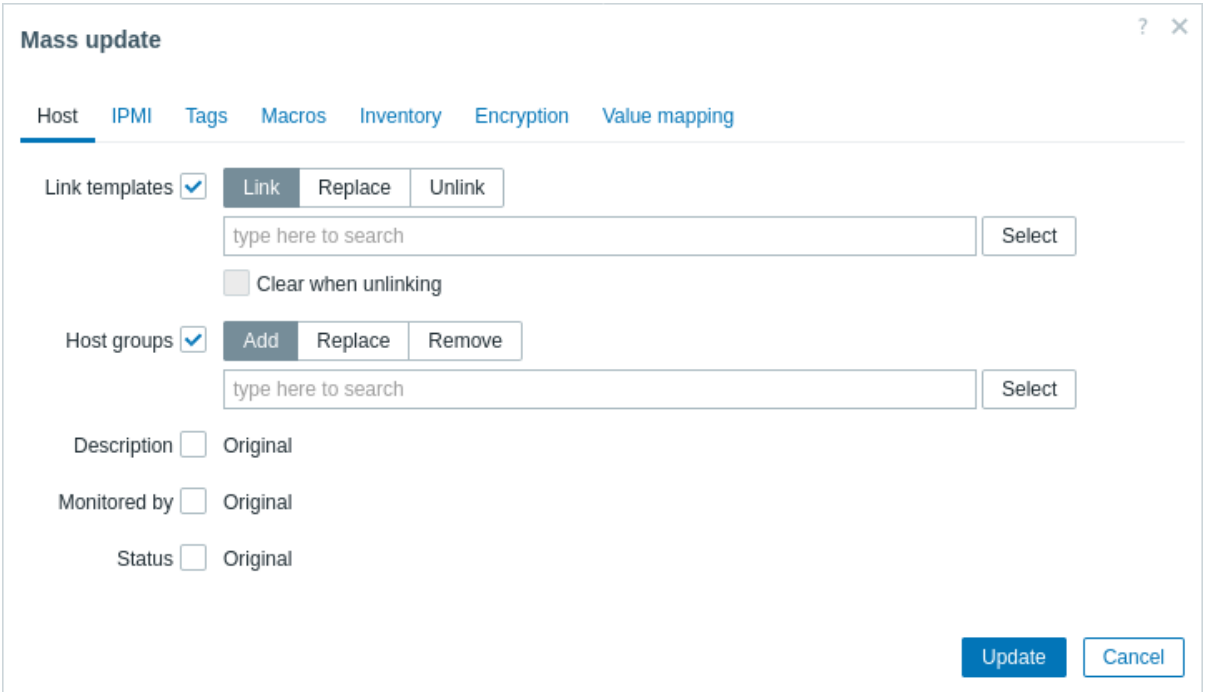
Przegląd

Czasami możesz chcieć naraz zmienić pewien atrybut dla wielu hostów. Zamiast otwierać każdy host do edycji z osobna, możesz skorzystać z funkcji aktualizacji masowej.

Korzystanie z masowej aktualizacji

Aby masowo zaktualizować wybrane hosty, wykonaj następujące czynności:

- Zaznacz pola wyboru przy hostach, które chcesz zaktualizować, na liście hostów
- Kliknij *Mass update* pod listą
- Przejdź do karty z wymaganymi atrybutami (*Host*, *IPMI*, *Tags*, *Macros*, *Inventory*, *Encryption* lub *Value mapping*)
- Zaznacz pola wyboru przy atrybutach, które chcesz zaktualizować, i wprowadź dla nich nowe wartości



Po wybraniu odpowiedniego przycisku aktualizacji powiązań **szablonów** dostępne są następujące opcje:

- *Link* - określa, które dodatkowe szablony mają zostać podłączone
- *Replace* - określa, które szablony mają zostać podłączone, jednocześnie odłączając wszystkie szablony, które były wcześniej podłączone do hostów

- *Unlink* - określa, które szablony mają zostać odłączone

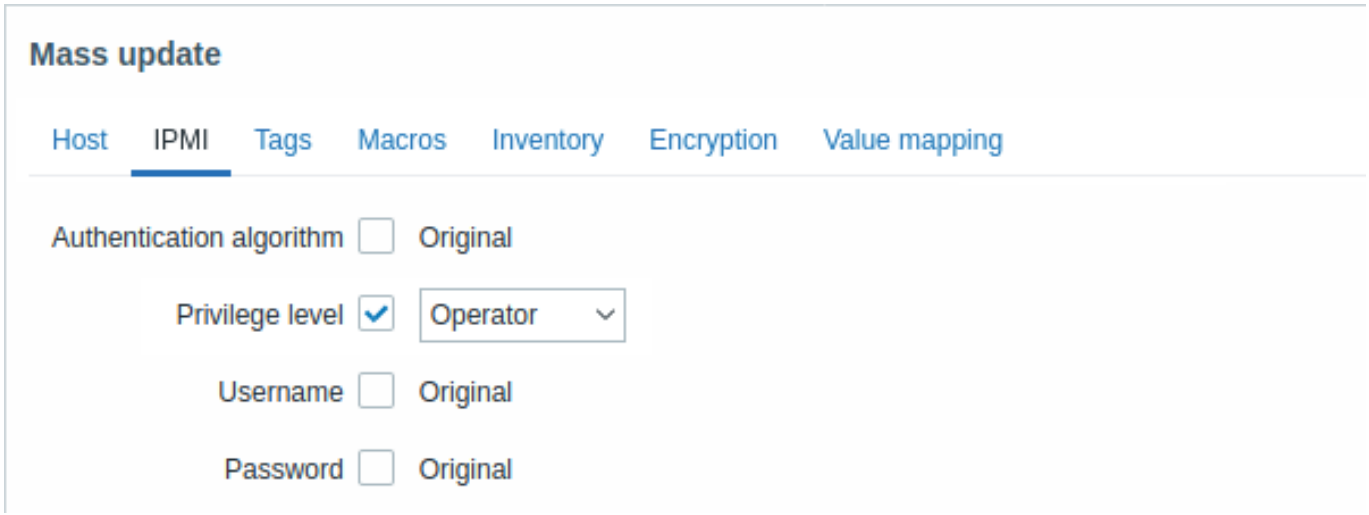
Aby określić szablony do podłączenia/odłączenia, zacznij wpisywać nazwę szablonu w polu autouzupełniania, aż pojawi się rozwijana lista z pasującymi szablonami. Następnie przewiń listę i wybierz wymagany szablon.

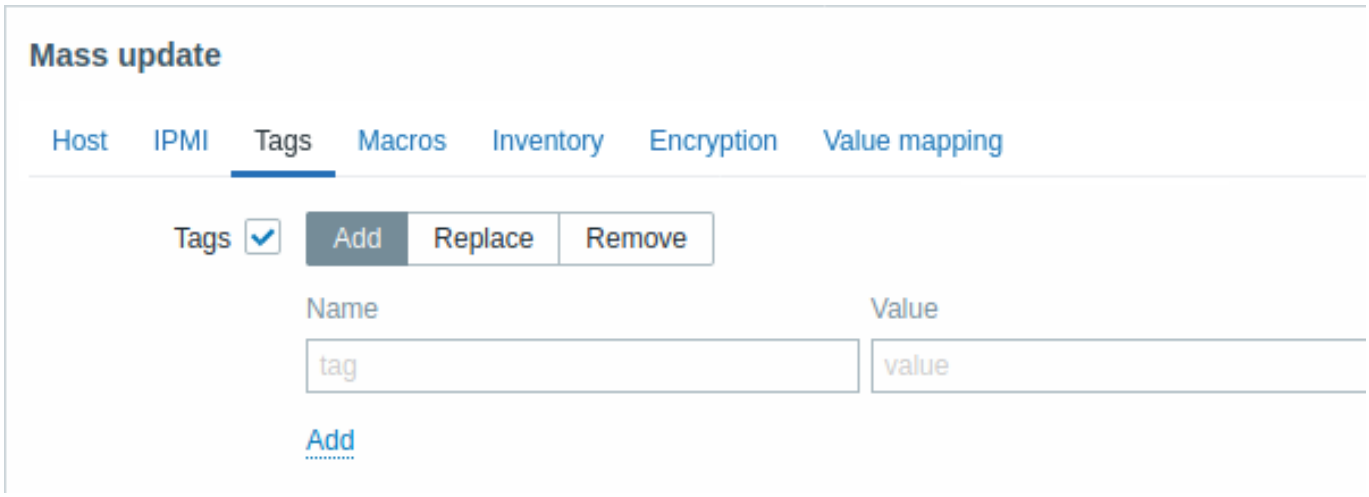
Opcja *Clear when unlinking* pozwala nie tylko odłączyć wcześniej podłączone szablony, ale także usunąć wszystkie elementy odziedziczone po nich (pozycje, wyzwalacze itd.).

Po wybraniu odpowiedniego przycisku aktualizacji **grup hostów** dostępne są następujące opcje:

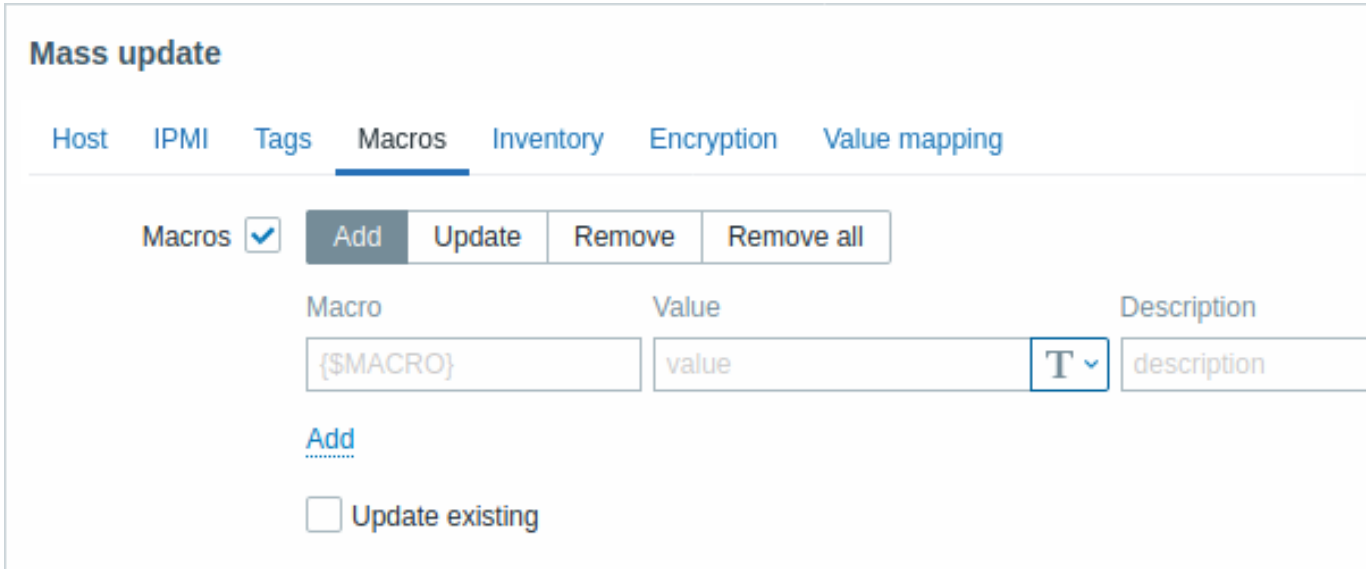
- *Add* - umożliwia określenie dodatkowych grup hostów spośród już istniejących lub wprowadzenie całkowicie nowych grup hostów dla hostów
- *Replace* - usunie host z wszystkich istniejących grup hostów i zastąpi je grupą/grupami określonymi w tym polu (istniejącymi lub nowymi grupami hostów)
- *Remove* - usunie określone grupy hostów z hostów

Pola te obsługują autouzupełnianie — rozpoczęcie wpisywania powoduje wyświetlenie rozwijanej listy pasujących grup hostów. Jeśli grupa hostów jest nowa, również pojawi się na liście i będzie oznaczona dopiskiem *(new)* po ciągu znaków. Wystarczy przewinąć listę i ją wybrać.



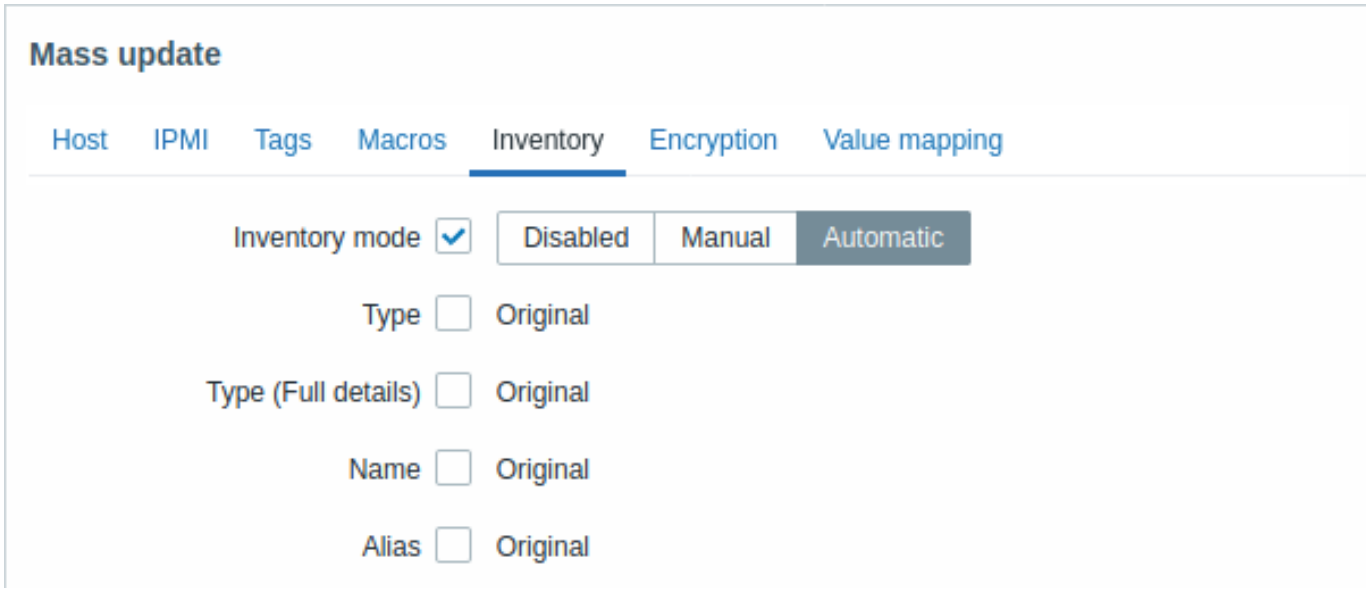


Makra użytkownika, makra {INVENTORY.*}, {HOST.HOST}, {HOST.NAME}, {HOST.CONN}, {HOST.DNS}, {HOST.IP}, {HOST.PORT} oraz {HOST.ID} są obsługiwane w tagach. Zwróć uwagę, że tagi o tej samej nazwie, ale różnych wartościach, nie są uznawane za „duplikaty” i mogą zostać dodane do tego samego hosta.

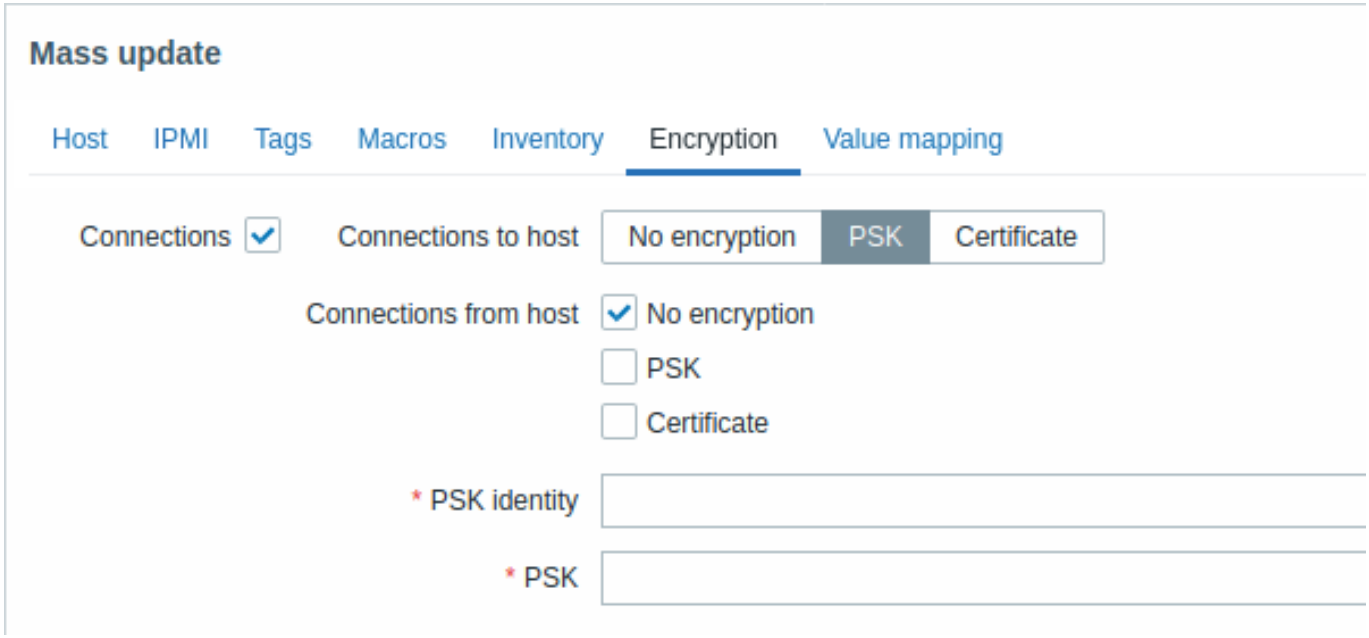


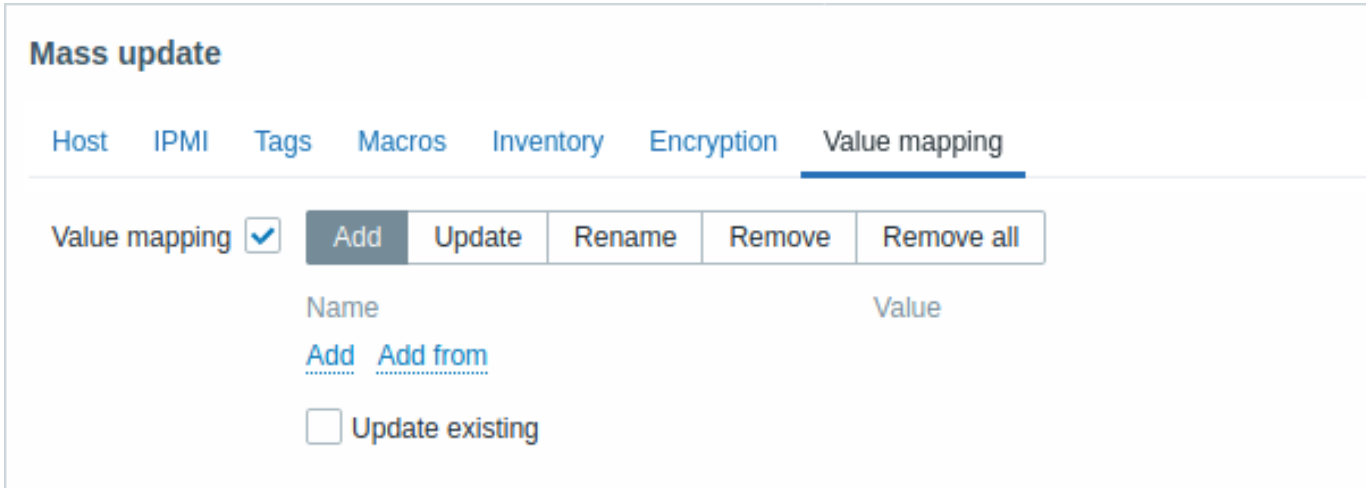
Po wybraniu odpowiedniego przycisku aktualizacji makr dostępne są następujące opcje:

- *Add* - umożliwia określenie dodatkowych makr użytkownika dla hostów. Jeśli zaznaczone jest pole wyboru *Update existing*, wartość, typ i opis dla wskazanej nazwy makra zostaną zaktualizowane. Jeśli pole nie jest zaznaczone i makro o tej nazwie już istnieje na hoście/hostach, nie zostanie zaktualizowane.
- *Update* - zastąpi wartości, typy i opisy makr określonych na tej liście. Jeśli zaznaczone jest pole wyboru *Add missing*, makro, które wcześniej nie istniało na hoście, zostanie dodane jako nowe. Jeśli pole nie jest zaznaczone, zaktualizowane zostaną tylko makra, które już istnieją na hoście.
- *Remove* - usunie określone makra z hostów. Jeśli zaznaczone jest pole *Except selected*, wszystkie makra poza wskazanymi na liście zostaną usunięte. Jeśli pole nie jest zaznaczone, usunięte zostaną tylko makra wskazane na liście.
- *Remove all* - usunie wszystkie makra użytkownika z hostów. Jeśli pole wyboru *I confirm to remove all macros* nie jest zaznaczone, otworzy się nowe wyskakujące okno z prośbą o potwierdzenie usunięcia wszystkich makr.



Aby możliwa była masowa aktualizacja pól inwentarza, *Inventory mode* powinien być ustawiony na „Manual” lub „Automatic”.





W przypadku aktualizacji map wartości dostępne są przyciski z następującymi opcjami:

- *Add* - dodaje mapy wartości do hostów. Jeśli zaznaczysz *Update existing*, wszystkie właściwości mapy wartości o tej nazwie zostaną zaktualizowane. W przeciwnym razie, jeśli mapa wartości o tej nazwie już istnieje, nie zostanie zaktualizowana.
- *Update* - aktualizuje istniejące mapy wartości. Jeśli zaznaczysz *Add missing*, mapa wartości, która wcześniej nie istniała na hoście, zostanie dodana jako nowa mapa wartości. W przeciwnym razie zaktualizowane zostaną tylko mapy wartości, które już istnieją na hoście.
- *Rename* - nadaje nową nazwę istniejącej mapie wartości
- *Remove* - usuwa określone mapy wartości z hostów. Jeśli zaznaczysz *Except selected*, wszystkie mapy wartości zostaną usunięte **z wyjątkiem** tych, które zostały wskazane.
- *Remove all* - usuwa wszystkie mapy wartości z hostów. Jeśli pole wyboru *I confirm to remove all value maps* nie jest zaznaczone, otworzy się nowe wyskakujące okno z prośbą o potwierdzenie usunięcia.

Po wprowadzeniu wszystkich wymaganych zmian kliknij *Update*. Atrybuty zostaną odpowiednio zaktualizowane dla wszystkich wybranych hostów.

2 Pozycje

#####Przegląd

Pozycja to indywidualna metryka.

Pozycje są używane do zbierania danych. Po skonfigurowaniu hosta, musisz dodać pozycje, aby uzyskać rzeczywiste dane. Jednym ze sposobów szybkiego dodawania wielu pozycji jest dołączenie jednego z predefiniowanych szablonów do hosta. Jednakże w celu zoptymalizowania wydajności systemu może zaistnieć potrzeba dostosowania szablonów tak, aby zawierały liczbę pozycji i częstotliwość monitorowania, o ile to konieczne.

Aby określić, jakie dane zbierać z hosta, użyj klucza pozycji. Na przykład, pozycja o kluczu **system.cpu.load** zbierze dane o obciążeniu procesora, podczas gdy pozycja o kluczu **net.if.in** zbierze informacje o przychodzącym ruchu sieciowym.

Dodatkowe parametry można określić w nawiasach kwadratowych po nazwie klucza. Na przykład, system.cpu.load**[avg5]** zwróci średnie obciążenie procesora (load) z ostatnich 5 minut, podczas gdy net.if.in**[eth0]** pokaże ilość przychodzącego ruchu na interfejsie ”eth0”.

Note:
Zobacz poszczególne sekcje typów pozycji dla wszystkich obsługiwanych typów pozycji i kluczy pozycji.

Przejdź do tworzenia i konfigurowania pozycji.

1 Tworzenie pozycji

Przegląd

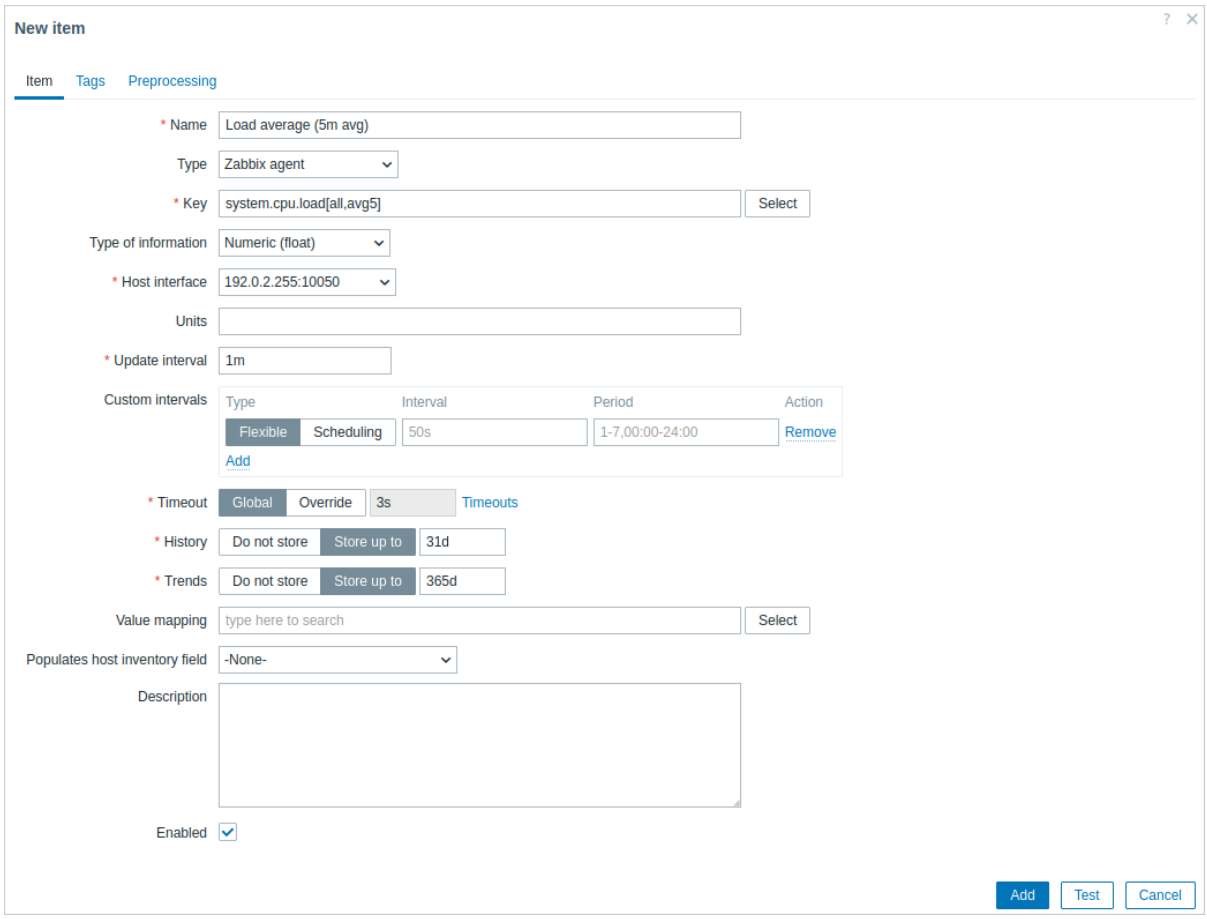
Aby utworzyć pozycję w frontendzie Zabbix, wykonaj następujące czynności:

- Przejdź do: *Data collection* > *Hosts*
- Kliknij *Items* w wierszu hosta
- Kliknij *Create item* w prawym górnym rogu ekranu
- Wprowadź parametry pozycji w formularzu

Możesz również utworzyć pozycję, otwierając istniejącą, naciskając przycisk *Clone*, a następnie zapisując ją pod inną nazwą.

Konfiguracja

Zakładka **Pozycja** zawiera ogólne atrybuty pozycji.



Wszystkie wymagane pola wejściowe są oznaczone czerwoną gwiazdką.

Parametr	Opis
Name	Nazwa pozycji. Obsługiwane są makra użytkownika.
Type	Typ pozycji. Zobacz poszczególne sekcje typów pozycji.

Parametr	Opis
Key	Klucz pozycji (do 2048 znaków). Obsługiwane klucze pozycji można znaleźć w sekcjach poszczególnych typów pozycji. Klucz musi być unikalny w obrębie pojedynczego hosta. Jeśli typ klucza to „Zabbix agent”, „Zabbix agent (active)” lub „Simple check”, wartość klucza musi być obsługiwana przez Zabbix agent lub Zabbix serwer. Zobacz także: poprawny format klucza.
Type of information	Typ danych używany do walidacji wartości pozycji i przechowywania jej w bazie danych, również po wszelkich konwersjach: **Numeric (unsigned)** - 64-bitowa liczba całkowita bez znaku; **Numeric (float)** - 64-bitowa liczba zmiennoprzecinkowa; **Character** - krótki tekst; **Log** - długi tekst z właściwościami logu lub bez nich (znacznik czasu, źródło, ważność, ID zdarzenia logu); **Text** - długi tekst; **Binary** - liczba binarna (obsługiwana tylko dla pozycji zależnych); **JSON** - strukturalne dane JSON, przechowywane natywnie w bazie danych (nieobsługiwane dla pozycji obliczanych). Pozycje zwracające wartości typu danych binary lub JSON nie są obsługiwane w formułach pozycji obliczanych ani w wyrażeniach wyzwalaczy. Informacje o limitach przechowywania dla każdego typu danych i silnika bazy danych znajdują się w sekcji limity danych pozycji. Dla pozycji, które zwracają dane w jednym określonym formacie, odpowiedni typ danych jest wybierany automatycznie — na przykład `system.cpu.load` i `system.cpu.util` zwracają 64-bitową liczbę zmiennoprzecinkową, więc *Numeric (float)* jest wybierane automatycznie.
Host interface	Wybierz interfejs hosta. To pole jest dostępne podczas edycji pozycji na poziomie hosta.
Units	Jeśli ustawiono symbol jednostki, Zabbix stosuje przetwarzanie końcowe do odebranej wartości pozycji i wyświetla ją z określonym przyrostkiem jednostki. Obsługiwane symbole jednostek ze specjalnym formatowaniem (oraz przykłady odebranej wartości pozycji → wyświetlanej wartości): **B** - bajty (1024 → 1 KB) **Bps** - bajty na sekundę (1024 → 1 KBps) **s** - sekundy, wyświetlane z użyciem maksymalnie trzech największych niezerowych jednostek czasu (881764 → 10d 4h 56m) **uptime** - czas działania w formacie hh:mm:ss lub N dni, hh:mm:ss (881764 → 10 dni, 04:56:04) **unixtime** - znacznik czasu Unix, formatowany jako yyyy.mm.dd hh:mm:ss (881764 → 1970-01-11 04:56:04 AM); dla poprawnego formatowania odebrana wartość pozycji musi mieć typ *Numeric (unsigned)*. Dla innych jednostek (takich jak Hz, W itp.), jeśli odebrana wartość przekracza 1000, jest dzielona przez 1000 i wyświetlana z odpowiednim prefiksem (5000 → 5 KHz, 881764 → 881.76 KW). Jeśli symbol jednostki jest poprzedzony prefiksem `!`, konwersja jednostki i dodawanie prefiksu są wyłączone (1024 !B → 1024 B, 61 !s → 61 s). Więcej przykładów i szczegółów dotyczących symboli jednostek oraz konwersji jednostek znajduje się w sekcji Sufiksy wartości pozycji.
Update interval	Pobieraj nową wartość dla tej pozycji co N sekund. Maksymalny dozwolony interwał aktualizacji to 86400 sekund (1 dzień). Obsługiwane są sufiksy czasu, np. 30s, 1m, 2h, 1d. Obsługiwane są makra użytkownika. Pojedyncze makro musi wypełniać całe pole. Wiele makr w jednym polu lub makra zmieszane z tekstem nie są obsługiwane. *Uwaga*: interwał aktualizacji można ustawić na „0” tylko wtedy, gdy istnieją niestandardowe interwały z wartością różną od zera. Jeśli ustawiono „0”, a istnieje niestandardowy interwał (elastyczny lub harmonogram) z wartością różną od zera, pozycja będzie odpytywana w czasie trwania niestandardowego interwału. *Uwaga*, że pierwsze odpytanie pozycji po jej aktywacji lub po zmianie interwału aktualizacji może nastąpić wcześniej niż skonfigurowana wartość. Nowe pozycje będą sprawdzane w ciągu 60 sekund od ich utworzenia, chyba że mają harmonogram lub elastyczny interwał aktualizacji, a *Update interval* ustawiono na 0. Istniejącą pasywną pozycję można odpytać natychmiast, naciskając przycisk *Execute now* button.

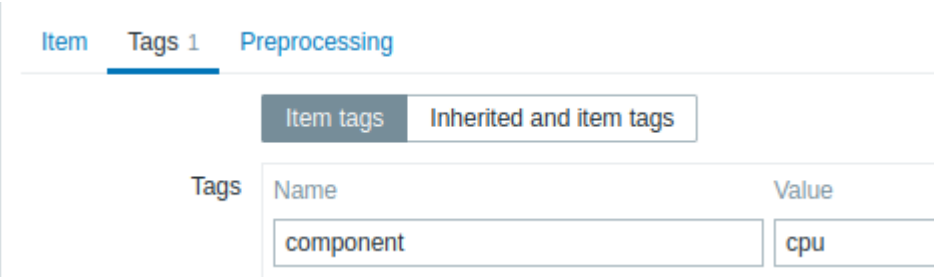
Parametr	Opis
Custom intervals	Możesz utworzyć niestandardowe reguły sprawdzania pozycji: **Flexible** - utwórz wyjątek od *Update interval* (interwał z inną częstotliwością). **Scheduling** - utwórz niestandardowy harmonogram odpytywania. Szczegółowe informacje znajdują się w sekcji Niestandardowe interwały. W polu *Interval* obsługiwane są sufiksy czasu, np. 30s, 1m, 2h, 1d. Obsługiwane są makra użytkownika. Pojedyncze makro musi wypełniać całe pole. Wiele makr w jednym polu lub makra zmieszane z tekstem nie są obsługiwane.
Timeout	Ustaw limit czasu sprawdzania pozycji (dostępne dla obsługiwanych typów pozycji). Wybierz opcję limitu czasu: **Global** - używany jest globalny limit czasu/proxy (wyświetlany w wyszarzonym polu *Timeout*). **Override** - używany jest niestandardowy limit czasu (ustawiany w polu *Timeout*; dozwolony zakres: 1 - 600s). Obsługiwane są sufiksy czasu, np. 30s, 1m, oraz makra użytkownika. Kliknięcie łącza *Timeouts* umożliwia skonfigurowanie limitów czasu proxy lub limitów globalnych (jeśli proxy nie jest używany). Należy pamiętać, że łącze *Timeouts* jest widoczne tylko dla użytkowników typu *Super admin* z uprawnieniami do sekcji frontend *Administration* > *General* lub *Administration* > *Proxies*.
History	Wybierz jedną z opcji: **Do not store** - historia pozycji nie jest przechowywana. Przydatne dla pozycji nadrzędnych, jeśli tylko pozycje zależne mają zachowywać historię. Tego ustawienia nie można nadpisać globalnymi ustawieniami housekeepera. **Store up to** - określ czas przechowywania szczegółowej historii w bazie danych (od 1 godziny do 25 lat). Starsze dane zostaną usunięte przez housekeeper. Wartość jest przechowywana w sekundach. Obsługiwane są sufiksy czasu, np. 2h, 1d. Obsługiwane są makra użytkownika. Wartość *Store up to* może zostać nadpisana globalnie w *Administration* > *Housekeeping*. Jeśli istnieje globalne ustawienie nadpisujące, wyświetlana jest pomarańczowa ikona informacji  . Po najechaniu na nią kursorem wyświetlany jest komunikat ostrzegawczy, np. *Overridden by global housekeeper settings (1d)*. Zaleca się przechowywanie zarejestrowanych wartości przez możliwie najkrótszy czas, aby zmniejszyć rozmiar historii wartości w bazie danych. Zamiast przechowywać długą historię wartości, można dłużej przechowywać dane trendów. Zobacz także Historia i trendy.
Trends	Wybierz jedną z opcji: **Do not store** - trendy nie są przechowywane. Tego ustawienia nie można nadpisać globalnymi ustawieniami housekeepera. **Store up to** - określ czas przechowywania zagregowanej historii (godzinowe min, max, avg, count) w bazie danych (od 1 dnia do 25 lat). Starsze dane zostaną usunięte przez housekeeper. Wartość jest przechowywana w sekundach. Obsługiwane są sufiksy czasu, np. 24h, 1d. Obsługiwane są makra użytkownika. Wartość *Store up to* może zostać nadpisana globalnie w *Administration* > *Housekeeping*. Jeśli istnieje globalne ustawienie nadpisujące, wyświetlana jest pomarańczowa ikona informacji  . Po najechaniu na nią kursorem wyświetlany jest komunikat ostrzegawczy, np. *Overridden by global housekeeper settings (7d)*. *Uwaga:* przechowywanie trendów nie jest dostępne dla danych nienumerycznych — character, log i text. Zobacz także Historia i trendy.
Value mapping	Zastosuj mapowanie wartości do tej pozycji. Mapowanie wartości nie zmienia odebranych wartości, służy wyłącznie do wyświetlania danych. Działa z pozycjami *Numeric(unsigned)*, *Numeric(float)* i *Character*. Na przykład „Windows service states”.

Parametr	Opis
Log time format	Dostępne tylko dla pozycji typu **Log**. Obsługiwane symbole zastępcze: **y**: *Rok (1970-2038)*. **M**: *Miesiąc (01-12)*. **d**: *Dzień (01-31)*. **h**: *Godzina (00-23)*. **m**: *Minuta (00-59)*. **s**: *Sekunda (00-59)*. Jeśli pole pozostanie puste, znacznik czasu zostanie ustawiony na 0 w czasie Unix, co odpowiada 1 stycznia 1970 roku. Na przykład rozważmy następujący wiersz z pliku logu Zabbix agent: " 23480:20100328:154718.045 Zabbix agent started. Zabbix 1.8.2 (revision 11211)." Zaczyna się on od sześciu pozycji znakowych dla PID, po których następują data, czas i reszta komunikatu. Format czasu logu dla tego wiersza to „pppppp:yyyyMMdd:hhmmss". Zwróć uwagę, że znaki „p" i „:" są symbolami zastępczymi i mogą być dowolnymi znakami z wyjątkiem „yMdhms".
Populates host inventory field	Możesz wybrać pole inwentarza hosta, które zostanie wypełnione wartością pozycji. Będzie to działać, jeśli dla hosta włączone jest automatyczne wypełnianie inwentarza oraz dla pozycji *Numeric(unsigned)*, *Numeric(float)*, *Character* i *Text*.
Description	Wprowadź opis pozycji. Obsługiwane są makra użytkownika.
Enabled	Zaznacz pole wyboru, aby włączyć pozycję, dzięki czemu będzie przetwarzana. Po wyłączeniu pozycji jest ona natychmiast usuwana z pamięci podręcznej historii (z wyjątkiem jej ostatniej wartości, która jest zachowywana dla logów).
Latest data	Kliknij łącze, aby wyświetlić najnowsze dane dla pozycji. To łącze jest dostępne tylko podczas edycji już istniejącej pozycji.

Note:
Pola specyficzne dla typu pozycji są opisane na odpowiednich stronach.

Note:
Podczas edycji istniejącej pozycji na poziomie szablonu z poziomu hosta część pól jest tylko do odczytu. Możesz użyć łącza w nagłówku formularza, przejść do poziomu szablonu i edytować je tam, pamiętając, że zmiany na poziomie szablonu zmienią pozycję dla wszystkich hostów, do których ten szablon jest podłączony.

Zakładka **Tags** umożliwia definiowanie tagów na poziomie pozycji.



Wstępne przetwarzanie wartości pozycji

Zakładka **Preprocessing** umożliwia zdefiniowanie reguł transformacji dla otrzymanych wartości.

Testowanie pozycji

Attention:
Aby przeprowadzić testowanie pozycji, upewnij się, że czas systemowy na serwerze i proxy jest zsynchronizowany. Jeśli czas na serwerze jest opóźniony, testowanie pozycji może zwrócić komunikat o błędzie „The task has been expired." Ustawienie różnych stref czasowych na serwerze i proxy nie wpłynie jednak na wynik testu.

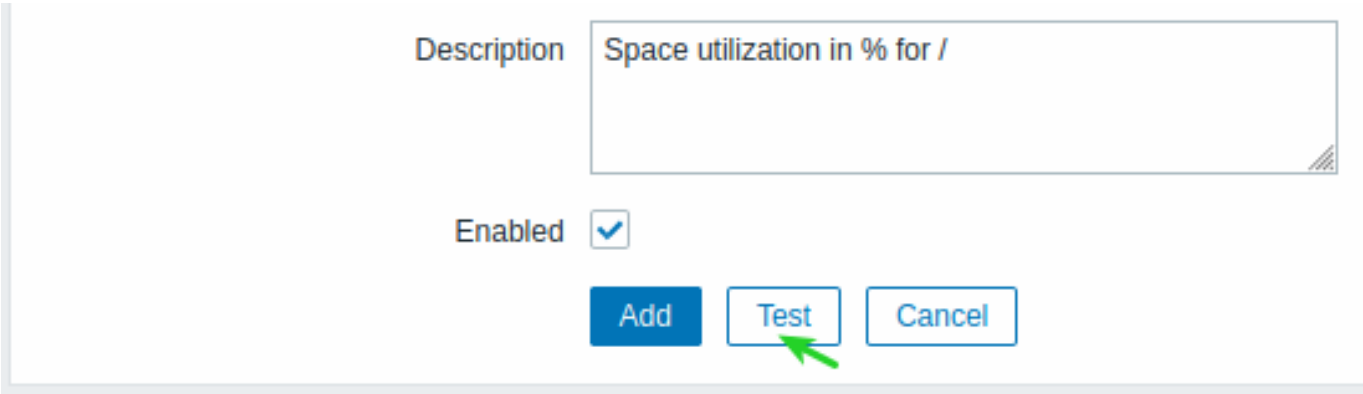
Możliwe jest przetestowanie pozycji i, jeśli jest ona poprawnie skonfigurowana, uzyskanie w odpowiedzi rzeczywistej wartości. Testowanie może odbywać się jeszcze przed zapisaniem pozycji.

Testowanie jest dostępne dla pozycji hosta i szablonu, prototypów pozycji oraz reguł wykrywania niskiego poziomu. Testowanie nie jest dostępne dla pozycji aktywnych.

Testowanie pozycji jest dostępne dla następujących typów pozycji pasywnych:

- agent Zabbix
- agent SNMP (v1, v2, v3)
- agent IPMI
- kontrole SSH
- kontrole Telnet
- agent JMX
- proste kontrole (z wyjątkiem pozycji `icmpping*`, `vmware.*`)
- wewnętrzne Zabbix
- pozycje kalkulowane
- kontrole zewnętrzne
- monitor bazy danych
- agent HTTP
- skrypt
- przeglądarka

Aby przetestować pozycję, kliknij przycisk *Test* na dole formularza konfiguracji pozycji. Pamiętaj, że przycisk *Test* będzie wyłączony dla pozycji, których nie można testować (takich jak kontrole aktywne, wykluczone proste kontrole).

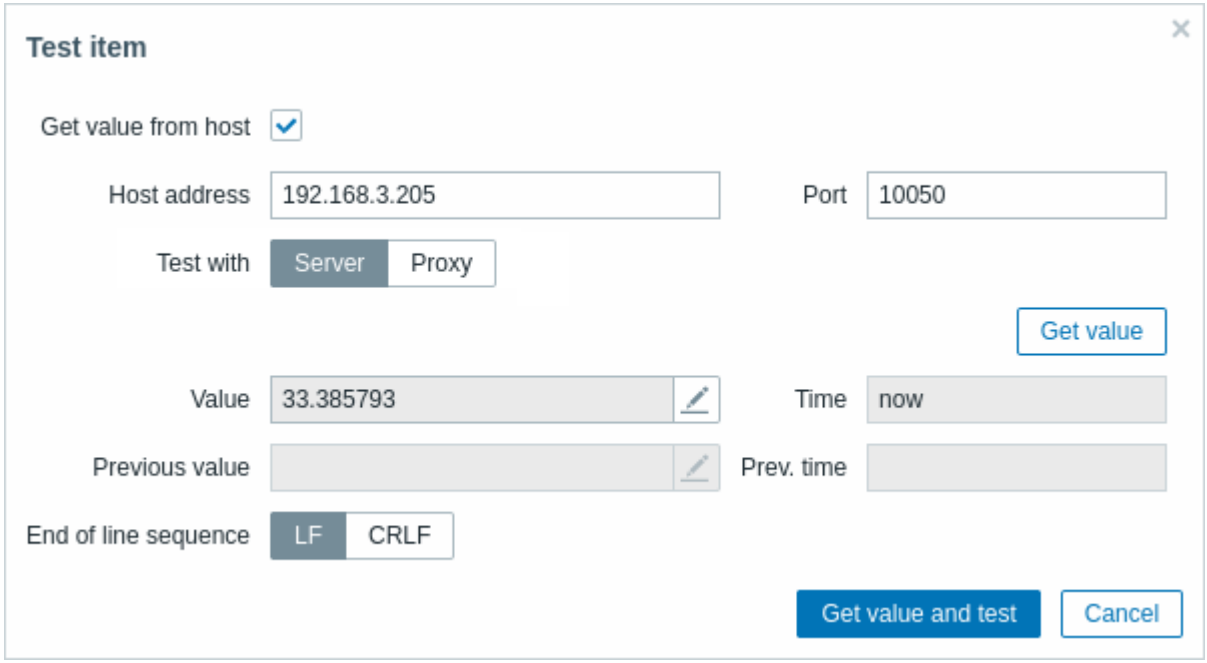


Formularz testowania pozycji zawiera pola dla wymaganych parametrów hosta (adres hosta, port, test z serwerem/proxy (nazwa proxy)) oraz szczegóły specyficzne dla pozycji (takie jak community SNMPv2 lub poświadczenia bezpieczeństwa SNMPv3). Pola te są zależne od kontekstu:

- Wartości są wstępnie uzupełniane, gdy jest to możliwe, tj. dla pozycji wymagających agent, poprzez pobranie informacji z wybranego interfejsu agent hosta.
- Wartości muszą być wprowadzane ręcznie dla pozycji szablonu.
- Wartości makr w postaci zwykłego tekstu są rozwijane.
- Pola, w których wartość (lub część wartości) jest tajnym makrem lub makrem Vault, są puste i muszą zostać uzupełnione ręcznie. Jeśli dowolny parametr pozycji zawiera wartość tajnego makra, wyświetlany jest następujący komunikat ostrzegawczy: „Pozycja zawiera makra użytkownika z tajnymi wartościami. Wartości tych makr należy wprowadzić ręcznie.”
- Pola są wyłączone, gdy nie są potrzebne w kontekście typu pozycji (np. pole adresu hosta i pole proxy są wyłączone dla pozycji kalkulowanych)

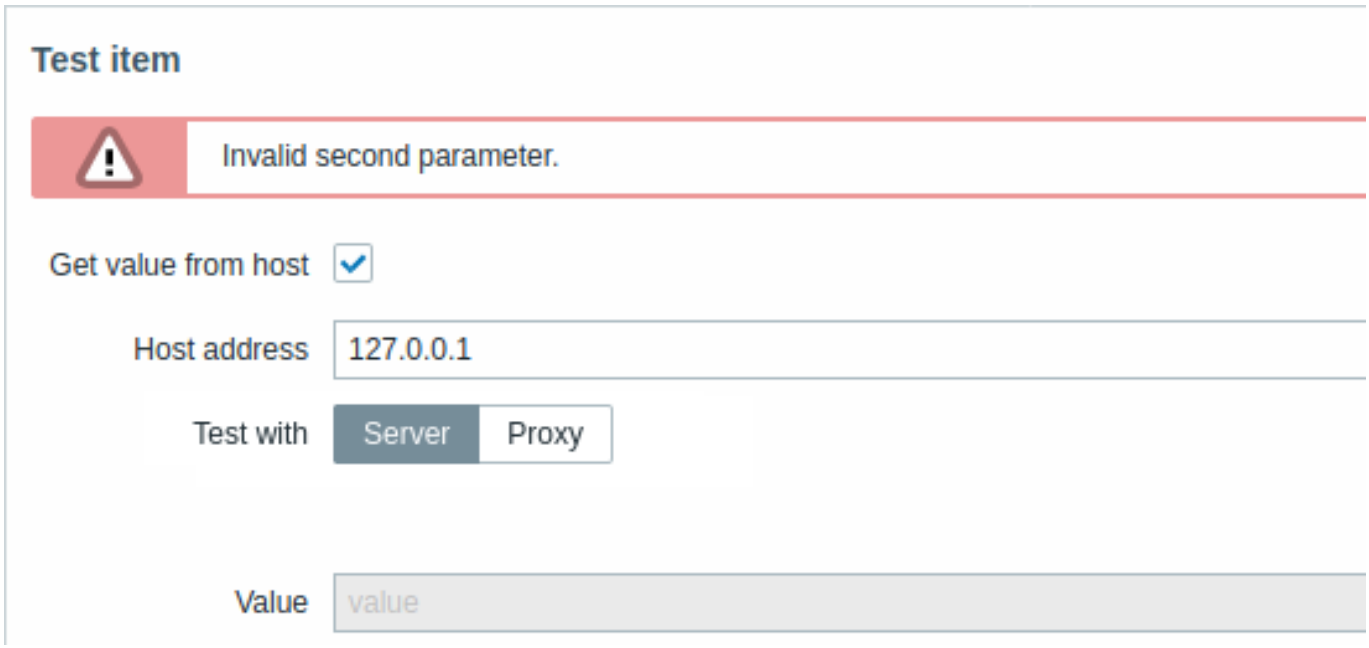
Aby przetestować pozycję, kliknij *Get value*. Jeśli wartość zostanie pomyślnie pobrana, wypełni pole *Value*, przenosząc bieżącą wartość (jeśli istnieje) do pola *Previous value*, jednocześnie obliczając pole *Prev. time*, tj. różnicę czasu między dwiema wartościami (kliknięciami), oraz próbując wykryć sekwencję EOL i przełączyć na CRLF po wykryciu ”\n\r” w pobranej wartości.

Kliknij *Get value and test*, aby przetestować preprocessing.



Wartości pobrane z hosta i wyniki testów są obcinane do maksymalnego rozmiaru 512KB podczas wysyłania do frontend. Jeśli wynik testu zostanie obcięty, wyświetlana jest ikona ostrzeżenia; najedź na nią kursorem, aby zobaczyć szczegóły. Jeśli wartość zostanie obcięta, może nie przejść walidacji typu danych w kolejnych testach porównujących duże wartości (np. JSON); w takich przypadkach wyświetlany jest komunikat o błędzie. Pamiętaj, że dane większe niż 512KB są nadal w pełni przetwarzane przez serwer Zabbix.

Jeśli konfiguracja jest nieprawidłowa, wyświetlany jest komunikat o błędzie opisujący możliwą przyczynę.



Pomyślnie pobrana wartość z hosta może być również użyta do testowania kroków preprocessing.

Przyciski formularza

Przyciski na dole formularza umożliwiają wykonanie kilku operacji.

Add	Dodaj pozycję. Ten przycisk jest dostępny tylko dla nowych pozycji.
Update	Zaktualizuj właściwości pozycji.
Clone	Utwórz kolejną pozycję na podstawie właściwości bieżącej pozycji.

Execute now	Natychmiast wykonaj sprawdzenie nowej wartości pozycji. Obsługiwane tylko dla sprawdzeń **pasywnych** (zobacz więcej szczegółów). *Uwaga:* podczas natychmiastowego sprawdzania wartości pamięć podręczna konfiguracji nie jest aktualizowana, dlatego wartość nie będzie odzwierciedlać bardzo niedawnych zmian w konfiguracji pozycji.
Test	Przetestuj, czy konfiguracja pozycji jest poprawna, pobierając wartość.
Clear history and trends	Usuń historię i trendy pozycji.
Delete	Usuń pozycję.
Cancel	Anuluj edycję właściwości pozycji.

Limity danych pozycji

Limity danych pozycji zależą od typu danych pozycji oraz silnika bazy danych.

Wartości numeryczne (unsigned) są przechowywane bez zmian. Jeśli zostanie odebrana wartość zmiennoprzecinkowa, zapisywana jest tylko część całkowita (np. 1.23 → 1).

Wartości numeryczne (float) są przechowywane bez zmian i obsługują około 15 do 17 cyfr precyzji, w zakresie od około -1.79E+308 do 1.79E+308. Obsługiwane są również wartości w notacji naukowej (np. 1.23E+7, 1e308, 1.1E-4).

Wartości tekstowe są obcinane przed zapisaniem, aby odpowiadały limitowi typu wartości w bazie danych:

Baza danych	Typ informacji		
	Znakowy	**Log**	**Tekst**
MySQL	255 znaków	65536 bajtów	65536 bajtów
PostgreSQL	255 znaków	65536 znaków	65536 znaków
SQLite (tylko Zabbix proxy)	255 znaków	65536 znaków	65536 znaków

Wartości binarne są ograniczone do 16MiB (16777216 bajtów). Wartości przekraczające ten limit są odrzucane, a odpowiedni błąd jest wyświetlany we frontend.

Wartości z typem danych JSON są ograniczone do 128MiB (134217728 bajtów). Wartości przekraczające ten limit są odrzucane, a odpowiedni błąd jest wyświetlany we frontend. W przypadku MySQL/MariaDB należy rozważyć skonfigurowanie dziennych partycji dla tabeli `history_json` (używanej do przechowywania wartości JSON), ponieważ może ona szybko rosnąć i blokować housekeeper przez dłuższy czas. Jeśli Twój przypadek użycia obejmuje duże wartości JSON (1MiB lub więcej), zobacz, jak skonfigurować system pod kątem obsługi dużych wartości JSON.

Gdy Zabbix zapisuje jakiekolwiek dane pozycji do bazy danych, używa zapytań INSERT i rejestruje je w logach (jeśli `DebugLevel` jest ustawiony na 4 lub 5). Duże wpisy logów są obcinane do 64KB.

Limit skryptu niestandardowego

Dostępna długość skryptu niestandardowego zależy od używanej bazy danych:

Baza danych	Limit znaków	Limit bajtów
MySQL	65535	65535
PostgreSQL	65535	bez ograniczeń
SQLite (tylko Zabbix proxy)	65535	bez ograniczeń

Limit czasu pozycji

Limit czasu pozycji określa, jak długo Zabbix powinien czekać przed przerwaniem sprawdzania i oznaczeniem go jako nieudanego.

Po osiągnięciu limitu czasu sprawdzanie jest przerywane, nawet jeśli pobieranie danych nie zostało zakończone. Jeśli dane zostaną odebrane częściowo, pozycja stanie się nieobsługiwana, a komunikat o błędzie zostanie zapisany w logu (na przykład, jeśli podczas sprawdzania SNMP dane zostaną pomyślnie zebrane tylko dla jednego z wielu OID).

Dla wielu typów pozycji można ustawić **elastyczne** limity czasu pozycji:

- dla pojedynczej pozycji
- dla typu pozycji (na poziomie proxy)
- dla typu pozycji (na poziomie globalnym)

Niestandardowy limit czasu *dla pojedynczej pozycji* jest przydatny, jeśli chcesz określić dłuższy limit czasu dla konkretnej pozycji, zachowując jednocześnie niskie limity czasu dla innych pozycji.

Priorytet limitów czasu

1. Limit czasu pojedynczej pozycji ma pierwszeństwo przed wszystkimi innymi limitami czasu.
2. Limity czasu na poziomie proxy mają pierwszeństwo przed globalnymi limitami czasu.

Limit czasu z konfiguracji Zabbix serwer lub proxy **nie** odgrywa żadnej roli w sprawdzaniach, dla których ustawiono elastyczne limity czasu.

Obsługa elastycznych limitów czasu

Elastyczne limity czasu pozycji są obsługiwane dla następujących typów pozycji:

- agent Zabbix (zarówno dla sprawdzeń pasywnych, jak i aktywnych)
- agent SNMP (z wyjątkiem starszych sprawdzeń SNMP[1])
- Proste sprawdzenie (z wyjątkiem `icmpping*` i pozycji VMware[2])
- agent SSH
- agent Telnet
- Sprawdzenie zewnętrzne
- Monitor bazy danych
- Skrypt
- agent HTTP
- Przeglądarka

[1] W przypadku starszych sprawdzeń SNMP (odpytanie pojedynczego OID) stosowane są ustawienia limitu czasu z konfiguracji serwer lub proxy.
 [2] W przypadku pozycji `icmpping*` wartość limitu czasu jest określana bezpośrednio w kluczu pozycji; obowiązuje również zakodowany na stałe maksymalny limit czasu wynoszący 600 sekund. Pozycje monitorowania VMware używają własnego parametru VMwareTimeout z konfiguracji serwer lub proxy.

Nieobsługiwane pozycje

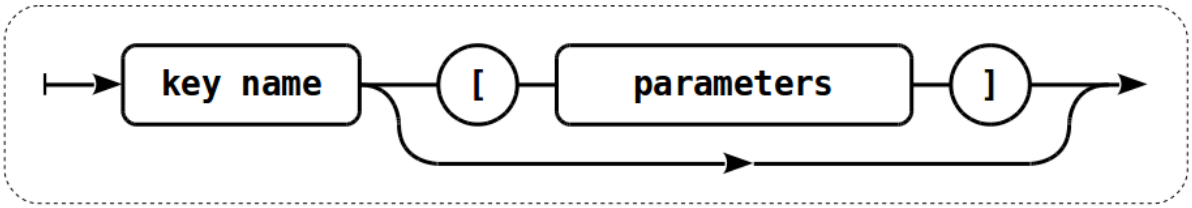
Nieobsługiwane pozycje są zgłaszane ze statusem *Nieobsługiwane* i nadal są ponownie sprawdzane zgodnie z ich standardowym *Interwałem aktualizacji*.

Pozycja staje się nieobsługiwana, jeśli z jakiegoś powodu nie można pobrać jej wartości (np. błąd połączenia, brak skonfigurowanych pollerów do przetwarzania pozycji). Dodatkowo pozycje, które nie otrzymują danych historycznych, pozostają w statusie *Nieobsługiwane*. Jest to oczekiwane zachowanie — pozycja przechodzi do statusu *Normalny* dopiero wtedy, gdy otrzyma nowe, prawidłowe dane historyczne.

Podobnie jak problemy, nieobsługiwane pozycje są ponownie oceniane tylko wtedy, gdy nadejdą nowe dane — nawet jeśli dla danej pozycji nie są już dostępne żadne dane historyczne. Innymi słowy, pozycje i wyzwalacze zmieniają swój stan wyłącznie po otrzymaniu nowych danych. Jednak jeśli wyrażenie wyzwalacza zawiera funkcję date and time i/lub nodata(), wyzwalacz będzie przeliczany co 30 sekund (szczegóły znajdują się w czasie obliczania wyzwalaczy).

1 Format klucza pozycji

Format klucza pozycji, w tym parametry klucza, musi być zgodny z regułami składni. Poniższe ilustracje przedstawiają obsługiwaną składnię. Dozwolone elementy i znaki w każdym miejscu można określić, podążając za strzałkami — jeśli do jakiegoś bloku można dotrzeć po linii, jest on dozwolony, jeśli nie — nie jest dozwolony.



Aby utworzyć prawidłowy klucz pozycji, należy zacząć od określenia nazwy klucza, następnie można wybrać, czy mają występować parametry, czy nie — jak pokazano przez dwie linie, którymi można podążać.

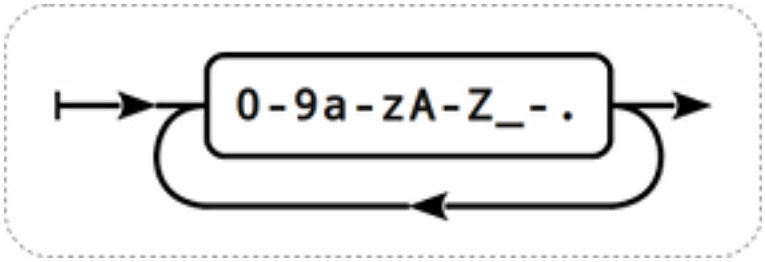
Nazwa klucza

Sama nazwa klucza ma ograniczony zakres dozwolonych znaków, które mogą występować jeden po drugim. Dozwolone znaki to:

0-9a-zA-Z_-.

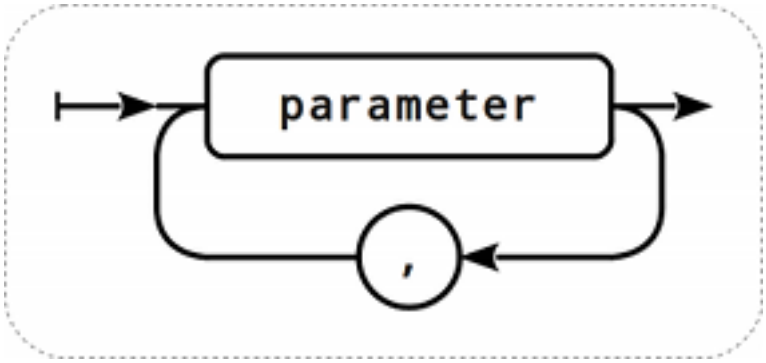
Co oznacza:

- wszystkie cyfry;
- wszystkie małe litery;
- wszystkie wielkie litery;
- podkreślenie;
- myślnik;
- kropka.

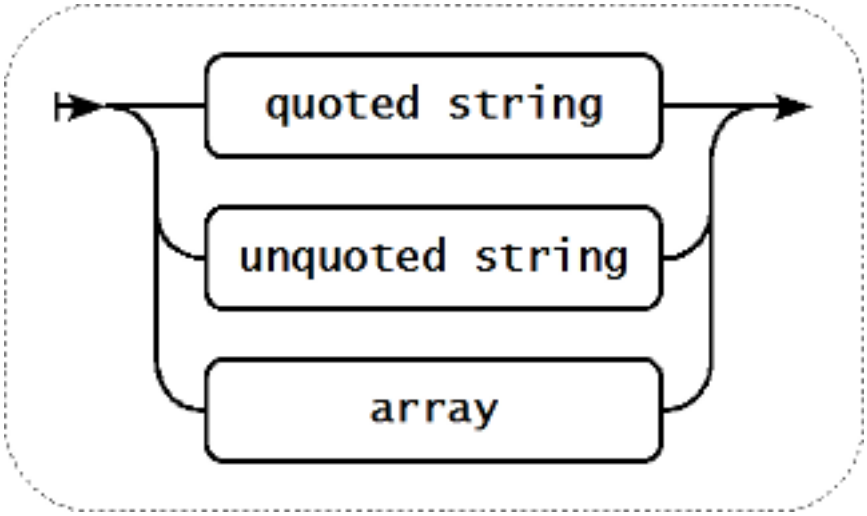


Kluczowe parametry

Klucz pozycji może mieć wiele parametrów oddzielonych przecinkami.



Każdy parametr klucza może być ujętym w cudzysłów ciągiem znaków, ciągiem znaków bez cudzysłowów albo tablicą.



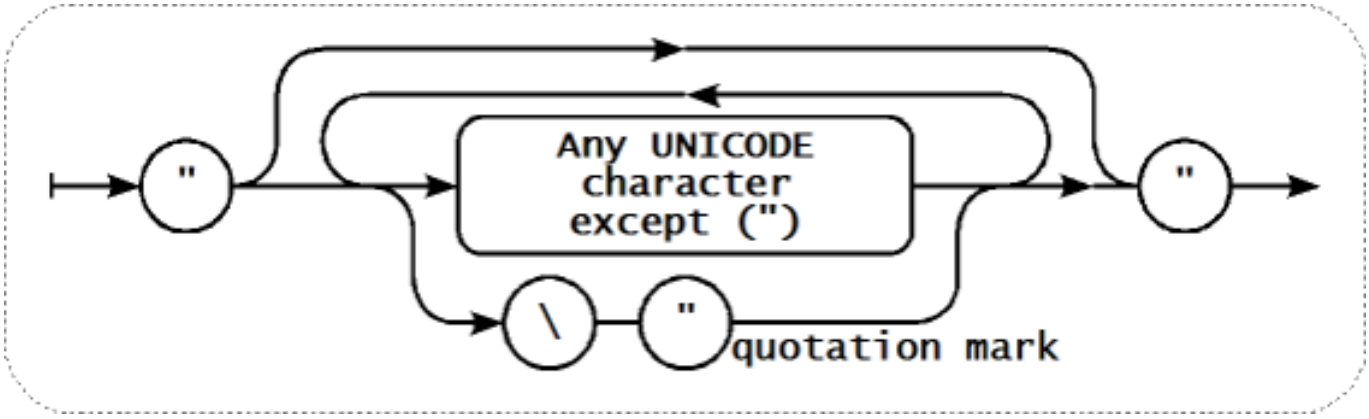
Parametr można również pozostawić pusty, używając w ten sposób wartości domyślnej. W takim przypadku należy dodać odpowiednią liczbę przecinków, jeśli określono jakiekolwiek dalsze parametry. Na przykład klucz pozycji **icmpping[„200„500]** oznacza, że interwał między poszczególnymi pingami wynosi 200 milisekund, limit czasu - 500 milisekund, a wszystkie pozostałe parametry pozostają ustawione na wartości domyślne.

Możliwe jest użycie makr w parametrach. Mogą to być makra użytkownika lub niektóre z wbudowanych makr. Aby sprawdzić, które konkretne wbudowane makra są obsługiwane w parametrach klucza pozycji, wyszukaj na stronie Obsługiwane makra frazę „item key parameters”.

Parametr - ciąg znaków w cudzysłowie

Jeśli parametr klucza jest ciągiem znaków ujętym w cudzysłów, dozwolony jest dowolny znak Unicode. Jeśli ciąg parametru klucza zawiera znak cudzysłowu, parametr ten musi być ujęty w cudzysłów, a każdy cudzysłów będący częścią ciągu parametru musi

zostać poprzedzony znakiem ukośnika odwrotnego (\). Jeśli ciąg parametru klucza zawiera przecinek, parametr ten musi być ujęty w cudzysłów.

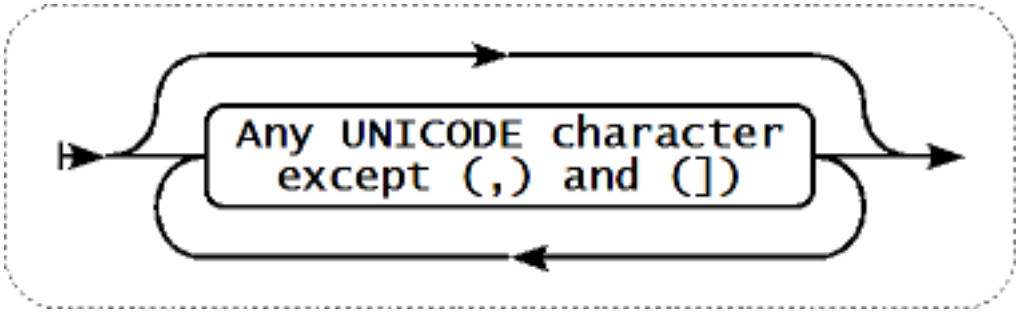


Warning:
Do ujmowania parametrów klucza pozycja w cudzysłów używaj wyłącznie podwójnych cudzysłowów. Pojedyncze cudzysłowy nie są obsługiwane.

Attention:
Wielopoziomowe tablice parametrów, np. `[a,[b,[c,d]],e]`, nie są dozwolone.

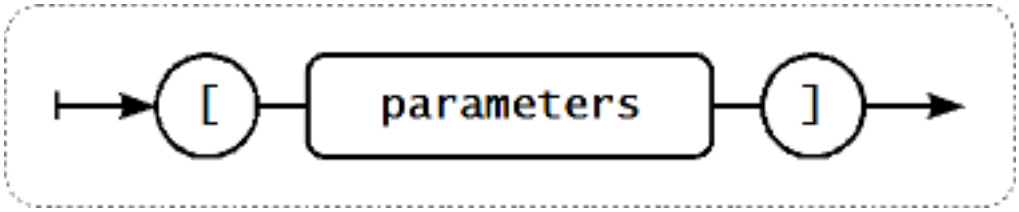
Parametr - ciąg znaków bez cudzysłowu

Jeśli parametr klucza jest ciągiem znaków bez cudzysłowu, dozwolony jest dowolny znak Unicode z wyjątkiem przecinka i prawego nawiasu kwadratowego (]). Parametr bez cudzysłowu nie może zaczynać się od lewego nawiasu kwadratowego ([).



Parametr - array

Jeśli parametr klucza jest tablicą, jest on ponownie ujmowany w nawiasy kwadratowe, gdzie poszczególne parametry są zgodne z zasadami i składnią określania wielu parametrów.



2 Interwały niestandardowe

Przegląd

Możliwe jest tworzenie własnych reguł dotyczących czasu, w którym pozycja jest sprawdzana. Służą do tego dwie metody: *Elastyczne interwały*, które pozwalają na ponowne zdefiniowanie domyślnego interwału aktualizacji, oraz *Harmonogramowanie*, dzięki któremu sprawdzenie pozycji może zostać wykonane o określonej godzinie lub w określonej sekwencji czasów.

Elastyczne interwały

Elastyczne interwały pozwalają na ponowne zdefiniowanie domyślnego interwału aktualizacji dla określonych okresów czasu. Elastyczny interwał jest definiowany za pomocą *Interwału* i *Okresu*, gdzie:

- *Interwał* – interwał aktualizacji dla określonego okresu czasu. Obsługiwane są sufiksy czasu, np. 30s, 1m, 2h, 1d.

- *Okres* – okres czasu, w którym elastyczny interwał jest aktywny (szczegółowy opis formatu *Okresu* znajduje się w sekcji okresy czasu)

Jeśli wiele elastycznych interwałów nakłada się na siebie, dla nakładającego się okresu używana jest najmniejsza wartość *Interwału*. Należy pamiętać, że jeśli najmniejsza wartość nakładających się elastycznych interwałów wynosi „0”, odpytywanie nie będzie wykonywane. Poza elastycznymi interwałami używany jest domyślny interwał aktualizacji.

Należy pamiętać, że jeśli elastyczny interwał jest równy długości okresu, pozycja zostanie sprawdzona dokładnie raz. Jeśli elastyczny interwał jest większy niż okres, pozycja może zostać sprawdzona raz albo może nie zostać sprawdzona wcale (dlatego taka konfiguracja nie jest zalecana). Jeśli elastyczny interwał jest mniejszy niż okres, pozycja zostanie sprawdzona co najmniej raz.

Jeśli elastyczny interwał jest ustawiony na „0”, pozycja nie jest odpytywana w czasie trwania okresu elastycznego interwału i wznawia odpytywanie zgodnie z domyślnym *Interwałem aktualizacji* po zakończeniu tego okresu. Przykłady:

Interval	Period	Opis
10	1-5,09:00-18:00	Pozycja będzie sprawdzana co 10 sekund w godzinach pracy.
0	1-7,00:00-7:00	Pozycja nie będzie sprawdzana w nocy.
0	7-7,00:00-24:00	Pozycja nie będzie sprawdzana w niedziele.
60	1-7,12:00-12:01	Pozycja będzie sprawdzana codziennie o 12:00. Należy pamiętać, że było to używane jako obejście dla zaplanowanych kontroli i zaleca się używanie interwałów harmonogramu dla takich kontroli.

Interwały harmonogramu

Interwały harmonogramu są używane do sprawdzania pozycji o określonych porach. Podczas gdy elastyczne interwały służą do redefiniowania domyślnego interwału aktualizacji pozycji, interwały harmonogramu są używane do określenia niezależnego harmonogramu sprawdzania, który jest wykonywany równolegle.

Interwał harmonogramu jest definiowany jako: `md<filter>wd<filter>h<filter>m<filter>s<filter>`, gdzie:

- **md** - dni miesiąca
- **wd** - dni tygodnia
- **h** - godziny
- **m** - minuty
- **s** – sekundy

`<filter>` służy do określania wartości dla swojego prefiksu (dni, godziny, minuty, sekundy) i jest definiowany jako: `[<from>[-<to>]][/<step>][,<filter>]`, gdzie:

- `<from>` i `<to>` definiują zakres pasujących wartości (włącznie). Jeśli `<to>` zostanie pominięte, filtr dopasowuje zakres `<from> - <from>`. Jeśli `<from>` również zostanie pominięte, filtr dopasowuje wszystkie możliwe wartości.
- `<step>` definiuje krok przeskakiwania wartości liczbowych w obrębie zakresu. Domyślnie `<step>` ma wartość 1, co oznacza, że dopasowywane są wszystkie wartości zdefiniowanego zakresu.

Chociaż definicje filtrów są opcjonalne, musi zostać użyty co najmniej jeden filtr. Filtr musi mieć zdefiniowany albo zakres, albo wartość *<step>*.

Pusty filtr dopasowuje albo „0”, jeśli nie zdefiniowano filtra niższego poziomu, albo wszystkie możliwe wartości w przeciwnym razie. Na przykład, jeśli filtr godzin zostanie pominięty, dopasowana zostanie tylko godzina „0”, pod warunkiem że filtry minut i sekund również są pominięte; w przeciwnym razie pusty filtr godzin dopasuje wszystkie wartości godzin.

Prawidłowe wartości `<from>` i `<to>` dla odpowiednich prefiksów filtrów to:

Prefix	Opis	*<from>*	*<to>*
md	Dni miesiąca	1-31	1-31
wd	Dni tygodnia	1-7	1-7
h	Godziny	0-23	0-23
m	Minuty	0-59	0-59
s	Sekundy	0-59	0-59

Wartość `<from>` musi być mniejsza lub równa wartości `<to>`. Wartość `<step>` musi być większa lub równa 1 oraz mniejsza lub równa `<to> - <from>`.

Jednocyfrowe wartości dni miesiąca, godzin, minut i sekund mogą być poprzedzone zerem. Na przykład `md01-31` i `h/02` są prawidłowymi interwałami, ale `md01-031` i `wd01-07` już nie.

W Zabbix frontend wiele interwałów harmonogramu wprowadza się w osobnych wierszach. W Zabbix API są one łączone w jeden ciąg znaków z separatorem w postaci średnika `;`.

Jeśli dany czas pasuje do kilku interwałów, zostanie wykonany tylko raz. Na przykład `wd1h9;h9` zostanie wykonane tylko raz w poniedziałek o 9:00.

Przykłady:

Interwał	Zostanie wykonany
m0-59	co minutę
h9-17/2	co 2 godziny, zaczynając od 9:00 (9:00, 11:00 ...)
m0,30 or m/30	co godzinę o hh:00 i hh:30
m0,5,10,15,20,25,30,35,40,45,50,55 or m/5	co pięć minut
wd1-5h9	od poniedziałku do piątku o 9:00
wd1-5h9-18	od poniedziałku do piątku o 9:00,10:00,...,18:00
h9,10,11 or h9-11	codziennie o 9:00, 10:00 i 11:00
md1h9m30	każdego 1. dnia miesiąca o 9:30
md1wd1h9m30	każdego 1. dnia miesiąca o 9:30, jeśli jest to poniedziałek
h9m/30	codziennie o 9:00, 9:30
h9m0-59/30	codziennie o 9:00, 9:30
h9,10m/30	codziennie o 9:00, 9:30, 10:00, 10:30
h9-10m30	codziennie o 9:30, 10:30
h9m10-40/30	codziennie o 9:10, 9:40
h9,10m10-40/30	codziennie o 9:10, 9:40, 10:10, 10:40
h9-10m10-40/30	codziennie o 9:10, 9:40, 10:10, 10:40
h9m10-40	codziennie o 9:10, 9:11, 9:12, ... 9:40
h9m10-40/1	codziennie o 9:10, 9:11, 9:12, ... 9:40
h9-12,15	codziennie o 9:00, 10:00, 11:00, 12:00, 15:00
h9-12,15m0	codziennie o 9:00, 10:00, 11:00, 12:00, 15:00
h9-12,15m0s30	codziennie o 9:00:30, 10:00:30, 11:00:30, 12:00:30, 15:00:30
h9-12s30	codziennie o 9:00:30, 9:01:30, 9:02:30 ... 12:58:30, 12:59:30
h9m/30;h10 (*składnia specyficzna dla API*)	codziennie o 9:00, 9:30, 10:00
h9m/30 h10 (*dodaj to jako kolejny wiersz w frontend*)	codziennie o 9:00, 9:30, 10:00

Wyrównanie stref czasowych dla proxy i agent

Należy pamiętać, że proxy i agent Zabbix używają swoich lokalnych stref czasowych podczas przetwarzania interwałów harmonogramu.

Z tego powodu, gdy interwały harmonogramu są stosowane do pozycji monitorowanych przez proxy Zabbix lub aktywnych pozycji agent, zaleca się ustawienie strefy czasowej odpowiednich proxy lub agent na taką samą jak na serwerze Zabbix, w przeciwnym razie kolejka może nieprawidłowo zgłaszać opóźnienia pozycji.

Strefę czasową dla proxy Zabbix lub agent można ustawić za pomocą zmiennej środowiskowej `TZ` w pliku jednostki `systemd`:

```
[Service]
...
Environment="TZ=Europe/Amsterdam"
```

2 Wstępne przetwarzanie wartości pozycji

Przegląd

Wstępne przetwarzanie umożliwia stosowanie przekształceń do odebranych wartości pozycji przed zapisaniem ich do bazy danych. Te przekształcenia/kroki wstępnego przetwarzania są wykonywane przez serwer Zabbix lub proxy (jeśli pozycje są monitorowane przez proxy).

Ta funkcja obsługuje różne przypadki użycia, takie jak:

- konwersja bajtów na bity (np. mnożenie wartości ruchu sieciowego przez „8”);
- obliczanie statystyk na sekundę dla wartości rosnących przyrostowo;

- stosowanie wyrażeń regularnych do wyodrębniania lub modyfikowania wartości;
- wykonywanie niestandardowych skryptów na wartościach;
- odrzucanie niezmienionych wartości w celu optymalizacji przechowywania danych w bazie.

Dla pozycji można skonfigurować jeden lub więcej kroków wstępnego przetwarzania. Kroki te są wykonywane w kolejności, w jakiej zostały skonfigurowane.

Attention:
Jeśli krok wstępnego przetwarzania zakończy się niepowodzeniem, pozycja stanie się nieobsługiwana. Można tego uniknąć dzięki obsłudze błędów *Custom on fail* (dostępnej dla większości przekształceń), która pozwala odrzucać wartości lub ustawiać wartości niestandardowe.

 W przypadku pozycji logów metadane logu (bez wartości) zawsze zresetują stan nieobsługiwanej pozycji, przywracając jej stan obsługiwany. Dzieje się tak nawet wtedy, gdy początkowy błąd wystąpił po odebraniu wartości logu od agent.

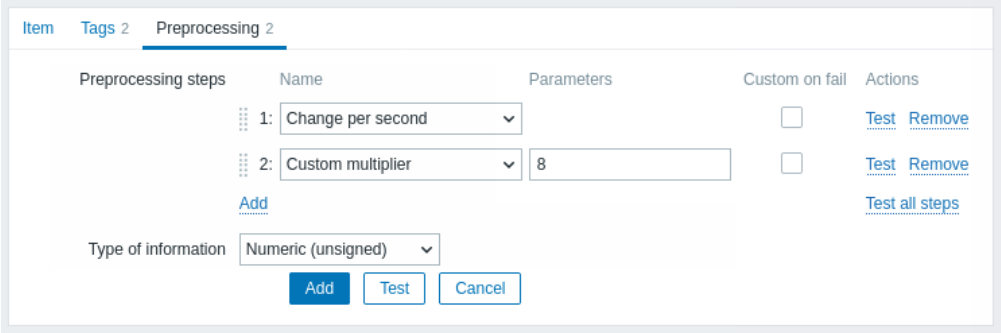
Wszystkie wartości przekazywane do wstępnego przetwarzania są początkowo traktowane jako ciągi znaków. Konwersja do żądanego typu wartości (zgodnie z definicją w konfiguracji pozycji) jest wykonywana na końcu potoku wstępnego przetwarzania. Jednak określone kroki wstępnego przetwarzania mogą wymuszać wcześniejsze konwersje, jeśli jest to wymagane. Szczegółowe informacje techniczne można znaleźć w sekcji Szczegóły wstępnego przetwarzania.

Aby upewnić się, że konfiguracja wstępnego przetwarzania działa zgodnie z oczekiwaniami, możesz ją przetestować.

Zobacz także: Przykłady wstępnego przetwarzania

Konfiguracja

Kroki przetwarzania wstępnego są definiowane na karcie **Preprocessing** formularza konfiguracji pozycji.



Kliknij *Add*, aby wybrać obsługiwaną transformację.

Pole *Type of information* jest wyświetlane na dole karty, gdy zdefiniowano co najmniej jeden krok przetwarzania wstępnego. W razie potrzeby można zmienić typ informacji bez opuszczania karty *Preprocessing*. Szczegółowy opis parametrów znajduje się w sekcji Tworzenie pozycji.

Obsługiwane transformacje

Wszystkie obsługiwane transformacje są wymienione poniżej. Kliknij nazwę transformacji, aby zobaczyć jej pełny opis.

Nazwa	Opis	Typ
Wyrażenie regularne	Dopasuj wartość do wyrażenia regularnego i zastąp ją wymaganym wynikiem.	Tekst
Zamień	Znajdź wyszukiwany ciąg i zastąp go innym (lub niczym).	
Przytnij	Usuń określone znaki z początku i końca wartości.	
Przytnij z prawej	Usuń określone znaki z końca wartości.	
Przytnij z lewej	Usuń określone znaki z początku wartości.	
XML XPath	Wyodrębnij wartość lub fragment z danych XML przy użyciu funkcji XPath.	Dane strukturalne
JSON Path	Wyodrębnij wartość lub fragment z danych JSON przy użyciu funkcji JSONPath.	
CSV do JSON	Konwertuj dane pliku CSV do formatu JSON.	
XML do JSON	Konwertuj dane w formacie XML do JSON.	
Wartość SNMP walk	Wyodrębnij wartość według określonej nazwy OID/MIB i zastosuj opcje formatowania.	SNMP
SNMP walk do JSON	Konwertuj wartości SNMP do JSON.	
Wartość SNMP get	Zastosuj opcje formatowania do wartości SNMP get.	
Mnożnik niestandardowy	Pomnóż wartość przez określoną liczbę całkowitą lub zmiennoprzecinkową.	Arytmetyka
Prosta zmiana	Oblicz różnicę między bieżącą a poprzednią wartością.	Zmiana

Nazwa	Opis	Typ
Zmiana na sekundę	Oblicz szybkość zmiany wartości na sekundę (różnicę między bieżącą a poprzednią wartością).	
Wartość logiczna na dziesiętną	Konwertuj wartość z formatu logicznego na dziesiętny.	Systemy liczbowe
Ósemkowy na dziesiętny	Konwertuj wartość z formatu ósemkowego na dziesiętny.	
Szesnastkowy na dziesiętny	Konwertuj wartość z formatu szesnastkowego na dziesiętny.	
JavaScript	Wprowadź kod JavaScript.	Skrypty niestandardowe
W zakresie	Zdefiniuj zakres, w którym powinna znajdować się wartość.	Walidacja
Pasuje do wyrażenia regularnego	Określ wyrażenie regularne, do którego wartość musi pasować.	
Nie pasuje do wyrażenia regularnego	Określ wyrażenie regularne, do którego wartość nie może pasować.	
Sprawdź błąd w JSON	Sprawdź komunikat błędu na poziomie aplikacji znajdujący się pod JSONPath.	
Sprawdź błąd w XML	Sprawdź komunikat błędu na poziomie aplikacji znajdujący się pod XPath.	
Sprawdź błąd przy użyciu wyrażenia regularnego	Sprawdź komunikat błędu na poziomie aplikacji przy użyciu wyrażenia regularnego.	
Sprawdź nieobsługiwaną wartość	Sprawdź, czy nie udało się pobrać żadnej wartości pozycji.	
Odrzuć niezmienione	Odrzuć wartość, jeśli nie uległa zmianie.	Ograniczanie częstotliwości
Odrzuć niezmienione z heartbeat	Odrzuć wartość, jeśli nie uległa zmianie w zdefiniowanym okresie czasu.	
Wzorzec Prometheus	Użyj poniższego zapytania, aby wyodrębnić wymagane dane z metryk Prometheus.	Prometheus
Prometheus do JSON	Konwertuj wymagane metryki Prometheus do JSON.	

Należy pamiętać, że dla kroków preprocessing typu *Zmiana* i *Ograniczanie częstotliwości* Zabbix musi zapamiętać ostatnią wartość, aby obliczyć/porównać nową wartość zgodnie z wymaganiami. Te poprzednie wartości są obsługiwane przez menedżera preprocessing. Jeśli serwer Zabbix lub proxy zostanie zrestartowany albo zostaną wprowadzone jakiekolwiek zmiany w krokach preprocessing, ostatnia wartość odpowiedniej pozycji zostanie zresetowana, co skutkuje:

- dla kroków *Prosta zmiana*, *Zmiana na sekundę* — następna wartość zostanie zignorowana, ponieważ nie ma poprzedniej wartości, na podstawie której można obliczyć zmianę;
- dla kroków *Odrzuć niezmienione*, *Odrzuć niezmienione z heartbeat* — następna wartość nigdy nie zostanie odrzucona, nawet jeśli powinna zostać odrzucona zgodnie z regułami odrzucania.

Wyrażenie regularne

Dopasuj wartość do wyrażenia regularnego i zastąp ją wymaganym wynikiem.

Parametry:

- **pattern** - wyrażenie regularne;
- **output** - szablon formatowania danych wyjściowych. Sekwencja ucieczki \N (gdzie N=1…9) jest zastępowana N-tą dopasowaną grupą. Sekwencja ucieczki \0 jest zastępowana dopasowanym tekstem.

Uwagi:

- Brak dopasowania wartości wejściowej spowoduje, że pozycja stanie się nieobsługiwana;
- Wyrażenie regularne obsługuje wyodrębnienie maksymalnie 10 przechwyconych grup za pomocą sekwencji \N;
- Jeśli zaznaczysz pole wyboru *Custom on fail*, możliwe jest określenie niestandardowych opcji obsługi błędów: odrzucenie wartości, ustawienie określonej wartości lub ustawienie określonego komunikatu błędu. W przypadku niepowodzenia kroku przetwarzania wstępnego pozycja nie stanie się nieobsługiwana, jeśli wybrano opcję odrzucenia wartości lub ustawienia określonej wartości.
- Przykłady można znaleźć w sekcji regular expressions.

Zamień

Znajdź wyszukiwany ciąg i zastąp go innym ciągiem (lub niczym).

Parametry:

- **wyszukiwany ciąg** - ciąg do znalezienia i zastąpienia, z rozróżnianiem wielkości liter (wymagane);
- **zamiennik** - ciąg, którym zostanie zastąpiony wyszukiwany ciąg. Ciąg zamiennika może być również pusty, co w praktyce pozwala usunąć wyszukiwany ciąg po jego znalezieniu.

Uwagi:

- Wszystkie wystąpienia wyszukiwanego ciągu zostaną zastąpione;
- Możliwe jest użycie sekwencji ucieczki do wyszukiwania lub zastępowania znaków nowej linii, powrotu karetki, tabulatorów i spacji ”\n \r \t \s”; ukośnik odwrotny można zapisać jako ”\\”, a sekwencje ucieczki można zapisać jako ”\\n”;
- Escapowanie znaków nowej linii, powrotu karetki i tabulatorów jest wykonywane automatycznie podczas wykrywania niskiego poziomu.

Przytnij

Usuń określone znaki z początku i końca wartości.

Przycinanie z prawej strony

Usuń określone znaki z końca wartości.

Przycinanie z lewej

Usuń określone znaki z początku wartości.

XML XPath

Wyodrębnij wartość lub fragment z danych XML przy użyciu funkcji XPath.

Uwagi:

- Aby ta opcja działała, serwer Zabbix (lub Zabbix proxy) musi być skompilowany z obsługą libxml;
- Przestrzenie nazw nie są obsługiwane;
- Jeśli zaznaczysz pole wyboru *Custom on fail*, można określić niestandardowe opcje obsługi błędów: odrzucenie wartości, ustawienie określonej wartości lub ustawienie określonego komunikatu o błędzie. W przypadku niepowodzenia kroku preprocessing pozycja nie stanie się nieobsługiwana, jeśli wybrano opcję odrzucenia wartości lub ustawienia określonej wartości.

Przykłady:

```
number(/document/item/value) #wyodrębni '10' z <document><item><value>10</value></item></document>
number(/document/item/@attribute) #wyodrębni '10' z <document><item attribute="10"></item></document>
/document/item #wyodrębni '<item><value>10</value></item>' z <document><item><value>10</value></item></doc
```

Ścieżka JSON

Wyodrębnij wartość lub fragment z danych JSON przy użyciu funkcjonalności JSONPath.

Jeśli zaznaczysz pole wyboru *Custom on fail*, możliwe jest określenie niestandardowych opcji obsługi błędów: odrzucenie wartości, ustawienie określonej wartości lub ustawienie określonego komunikatu błędu. W przypadku niepowodzenia kroku przetwarzania wstępnego pozycja nie stanie się nieobsługiwana, jeśli wybrano opcję odrzucenia wartości lub ustawienia określonej wartości.

CSV do JSON

Konwertuj dane pliku CSV do formatu JSON.

Aby uzyskać więcej informacji, zobacz: Wstępne przetwarzanie CSV do JSON.

XML do JSON

Konwertuj dane w formacie XML do JSON.

Więcej informacji znajduje się tutaj: Zasady serializacji.

Jeśli zaznaczysz pole wyboru *Custom on fail*, można określić niestandardowe opcje obsługi błędów: odrzucenie wartości, ustawienie określonej wartości lub ustawienie określonego komunikatu o błędzie. W przypadku nieudanego kroku przetwarzania wstępnego pozycja nie stanie się nieobsługiwana, jeśli wybrano opcję odrzucenia wartości lub ustawienia określonej wartości.

Wartość SNMP walk

Wyodrębnij wartość według określonej nazwy OID/MIB i zastosuj opcje formatowania:

- **Bez zmian** — zwróć ciąg szesnastkowy jako nieescapowany ciąg szesnastkowy (*uwaga*: wskazówki wyświetlania są nadal stosowane);
- **UTF-8 z hex-STRING** — przekonwertuj ciąg szesnastkowy na ciąg UTF-8;
- **MAC z hex-STRING** — zweryfikuj ciąg szesnastkowy jako adres MAC i zwróć poprawny ciąg adresu MAC (gdzie `' '` są zastępowane przez `':'`);

- **Liczba całkowita z BITS** — przekonwertuj pierwsze 8 bajtów ciągu bitowego wyrażonego jako sekwencja znaków szesnastkowych (np. „1A 2B 3C 4D”) na 64-bitową liczbę całkowitą bez znaku. W ciągach bitowych dłuższych niż 8 bajtów kolejne bajty zostaną zignorowane.

Jeśli zaznaczysz pole wyboru *Custom on fail*, można określić niestandardowe opcje obsługi błędów: odrzucenie wartości, ustawienie określonej wartości lub ustawienie określonego komunikatu błędu. W przypadku nieudanego kroku preprocessing pozycja nie stanie się nieobsługiwana, jeśli wybrano opcję odrzucenia wartości lub ustawienia określonej wartości.

SNMP walk do JSON

Konwertuj wartości SNMP do formatu JSON.

Określ nazwę pola w JSON oraz odpowiadającą jej ścieżkę SNMP OID. Wartości pól zostaną wypełnione wartościami z określonej ścieżki SNMP OID.

Uwagi:

- Dostępne są opcje formatowania wartości podobne do tych w kroku *Wartość SNMP walk*;
- Możesz użyć tego kroku przetwarzania wstępnego do wykrywania SNMP OID;
- Jeśli zaznaczysz pole wyboru *Custom on fail*, możliwe będzie określenie niestandardowych opcji obsługi błędów: odrzucenie wartości, ustawienie określonej wartości lub ustawienie określonego komunikatu o błędzie. W przypadku niepowodzenia kroku przetwarzania wstępnego pozycja nie stanie się nieobsługiwana, jeśli wybrano opcję odrzucenia wartości lub ustawienia określonej wartości.

Wartość SNMP get

Zastosuj opcje formatowania do wartości SNMP get:

- **UTF-8 from Hex-STRING** — konwertuje ciąg szesnastkowy na ciąg UTF-8;
- **MAC from Hex-STRING** — sprawdza poprawność ciągu szesnastkowego jako adresu MAC i zwraca prawidłowy ciąg adresu MAC (gdzie `' '` są zastępowane przez `':'`);
- **Integer from BITS** — konwertuje pierwsze 8 bajtów ciągu bitowego wyrażonego jako sekwencja znaków szesnastkowych (np. „1A 2B 3C 4D”) na 64-bitową liczbę całkowitą bez znaku. W ciągach bitowych dłuższych niż 8 bajtów kolejne bajty zostaną zignorowane.

Jeśli zaznaczysz pole wyboru *Custom on fail*, możliwe jest określenie niestandardowych opcji obsługi błędów: odrzucenie wartości, ustawienie określonej wartości lub ustawienie określonego komunikatu o błędzie. W przypadku niepowodzenia kroku preprocessing pozycja nie stanie się nieobsługiwana, jeśli wybrano opcję odrzucenia wartości lub ustawienia określonej wartości.

Mnożnik niestandardowy

Pomnóż wartość przez określoną liczbę całkowitą lub zmiennoprzecinkową.

Uwagi:

- Użyj tej opcji, aby konwertować wartości otrzymywane w KB, MBps itp. na B, Bps. W przeciwnym razie Zabbix nie będzie mógł poprawnie ustawić prefiksów (K, M, G itd.).
- Należy pamiętać, że jeśli typ informacji pozycji to *Numeric (unsigned)*, przychodzące wartości z częścią ułamkową zostaną obcięte (tj. „0.9” stanie się „0”) przed zastosowaniem mnożnika niestandardowego;
- Jeśli używasz mnożnika niestandardowego lub przechowujesz wartość jako *Change per second* dla pozycji z typem informacji ustawionym na *Numeric (unsigned)*, a wynikowa obliczona wartość jest w rzeczywistości liczbą zmiennoprzecinkową, obliczona wartość nadal jest akceptowana jako poprawna po obcięciu części dziesiętnej i zapisaniu wartości jako liczby całkowitej;
- Obsługiwane: notacja naukowa, na przykład 1e+70; makra użytkownika i makra LLD; ciągi znaków zawierające makra, na przykład `{#MACRO}e+10`, `{$MACRO1}e+{$MACRO2}`. Makra muszą zostać rozwinięte do liczby całkowitej lub zmiennoprzecinkowej.
- Jeśli zaznaczysz pole wyboru *Custom on fail*, możliwe jest określenie niestandardowych opcji obsługi błędów: odrzucenie wartości, ustawienie określonej wartości lub ustawienie określonego komunikatu o błędzie. W przypadku niepowodzenia kroku preprocessing pozycja nie stanie się nieobsługiwana, jeśli wybrano opcję odrzucenia wartości lub ustawienia określonej wartości.

Zmiana prosta

Oblicza różnicę między bieżącą a poprzednią wartością.

Uwagi:

- Ten krok może być przydatny do pomiaru stale rosnącej wartości;
- Obliczane jako **value**-**prev_value**, gdzie *value* — wartość bieżąca; *prev_value* — poprzednio odebrana wartość;
- Dozwolona jest tylko jedna operacja zmiany na pozycja („Zmiana prosta” lub „Zmiana na sekundę”);
- Jeśli bieżąca wartość jest mniejsza od poprzedniej, Zabbix odrzuca tę różnicę (nic nie zapisuje) i czeka na kolejną wartość;

- Jeśli zaznaczysz pole wyboru *Custom on fail*, można określić niestandardowe opcje obsługi błędów: odrzucenie wartości, ustawienie określonej wartości lub ustawienie określonego komunikatu błędu. W przypadku nieudanego kroku przetwarzania wstępnego pozycja nie stanie się nieobsługiwana, jeśli wybrano opcję odrzucenia wartości lub ustawienia określonej wartości.

Zmiana na sekundę

Oblicza szybkość zmiany wartości (różnicę między bieżącą a poprzednią wartością) na sekundę.

Uwagi:

- Ten krok jest przydatny do obliczania szybkości na sekundę dla stale rosnącej wartości;
- Ponieważ to obliczenie może dawać liczby zmiennoprzecinkowe, zaleca się ustawienie pola „Type of information" na *Numeric (float)*, nawet jeśli przychodzące surowe wartości są liczbami całkowitymi. Jest to szczególnie istotne w przypadku małych liczb, gdzie część dziesiętna ma znaczenie. Jeśli wartości zmiennoprzecinkowe są duże i mogą przekroczyć długość pola „float", co może spowodować utratę całej wartości, zaleca się użycie *Numeric (unsigned)*, a tym samym obcięcie jedynie części dziesiętnej.
- Obliczane jako (**value**-**prev_value**)/(**time**-**prev_time**), gdzie *value* — bieżąca wartość; *prev_value* — poprzednio odebrana wartość; *time* — bieżący znacznik czasu; *prev_time* — znacznik czasu poprzedniej wartości;
- Dozwolona jest tylko jedna operacja zmiany na pozycja („Simple change" lub „Change per second");
- Jeśli bieżąca wartość jest mniejsza od poprzedniej, Zabbix odrzuca tę różnicę (nic nie zapisuje) i oczekuje na kolejną wartość. Pomaga to poprawnie działać na przykład w przypadku zawijania (przepełnienia) 32-bitowych liczników SNMP.
- Jeśli zaznaczysz pole wyboru *Custom on fail*, można określić niestandardowe opcje obsługi błędów: odrzucenie wartości, ustawienie określonej wartości lub ustawienie określonego komunikatu o błędzie. W przypadku niepowodzenia kroku preprocessing pozycja nie stanie się nieobsługiwana, jeśli wybrano opcję odrzucenia wartości lub ustawienia określonej wartości.

Wartość logiczna na dziesiętną

Konwertuje wartość z formatu logicznego na dziesiętny.

Uwagi:

- Reprezentacja tekstowa jest tłumaczona odpowiednio na 0 lub 1. W związku z tym „TRUE" jest zapisywane jako 1, a „FALSE" jako 0. Wszystkie wartości są dopasowywane bez rozróżniania wielkości liter. Obecnie rozpoznawane wartości to, dla *TRUE* — true, t, yes, y, on, up, running, enabled, available, ok, master; dla *FALSE* — false, f, no, n, off, down, unused, disabled, unavailable, err, slave. Dodatkowo każda niezerowa wartość liczbowa jest uznawana za TRUE, a zero jest uznawane za FALSE.
- Jeśli zaznaczysz pole wyboru *Custom on fail*, można określić niestandardowe opcje obsługi błędów: odrzucenie wartości, ustawienie określonej wartości lub ustawienie określonego komunikatu o błędzie. W przypadku nieudanego kroku preprocessing pozycja nie stanie się nieobsługiwana, jeśli wybrano opcję odrzucenia wartości lub ustawienia określonej wartości.

Ósemkowy na dziesiętny

Konwertuje wartość z formatu ósemkowego na dziesiętny.

Jeśli zaznaczysz pole wyboru *Niestandardowo w przypadku błędu*, można określić niestandardowe opcje obsługi błędów: odrzucenie wartości, ustawienie określonej wartości lub ustawienie określonego komunikatu o błędzie. W przypadku niepowodzenia kroku przetwarzania wstępnego pozycja nie stanie się nieobsługiwana, jeśli wybrano opcję odrzucenia wartości lub ustawienia określonej wartości.

Szesnastkowy na dziesiętny

Konwertuje wartość z formatu szesnastkowego na dziesiętny.

Jeśli zaznaczysz pole wyboru *Custom on fail*, można określić niestandardowe opcje obsługi błędów: odrzucenie wartości, ustawienie określonej wartości lub ustawienie określonego komunikatu o błędzie. W przypadku niepowodzenia kroku preprocessing pozycja nie stanie się nieobsługiwana, jeśli wybrano opcję odrzucenia wartości lub ustawienia określonej wartości.

JavaScript

Wprowadź kod JavaScript w modalnym edytorze, który otwiera się po kliknięciu w polu parametru lub ikonie ołówka obok niego.

> **Attention:**
> Nie używaj niezadeklarowanych przypisań w kodzie JavaScript przetwarzania wstępnego. Użyj `var`, aby zadeklarować zmienne lokalne.

Uwagi:

- Dostępna długość kodu JavaScript zależy od używanej bazy danych;
- Więcej informacji można znaleźć tutaj: Przetwarzanie wstępne JavaScript.

W zakresie

Zdefiniuj zakres, w którym powinna znajdować się wartość, określając wartości minimalne/maksymalne (włącznie).

Uwagi:

- Akceptowane są wartości liczbowe (w tym dowolna liczba cyfr, opcjonalna część dziesiętna i opcjonalna część wykładnicza, wartości ujemne);
- Wartość minimalna powinna być mniejsza od wartości maksymalnej;
- Musi istnieć co najmniej jedna wartość;
- Można używać makr użytkownika i makr wykrywania niskiego poziomu;
- Jeśli zaznaczysz pole wyboru *Niestandardowo w przypadku błędu*, można określić niestandardowe opcje obsługi błędów: odrzucenie wartości, ustawienie określonej wartości lub ustawienie określonego komunikatu o błędzie. W przypadku nieudanego kroku przetwarzania wstępnego pozycja nie stanie się nieobsługiwana, jeśli wybrano opcję odrzucenia wartości lub ustawienia określonej wartości.

Pasuje do wyrażenia regularnego

Określ wyrażenie regularne, do którego wartość musi pasować.

Jeśli zaznaczysz pole wyboru *Niestandardowe przy błędzie*, możliwe jest określenie niestandardowych opcji obsługi błędów: odrzucenie wartości, ustawienie określonej wartości lub ustawienie określonego komunikatu o błędzie. W przypadku niepowodzenia kroku preprocessing pozycja nie stanie się nieobsługiwana, jeśli wybrano opcję odrzucenia wartości lub ustawienia określonej wartości.

Nie pasuje do wyrażenia regularnego

Określ wyrażenie regularne, do którego wartość nie może pasować.

Jeśli zaznaczysz pole wyboru *Niestandardowo w przypadku błędu*, możliwe jest określenie niestandardowych opcji obsługi błędów: odrzucenie wartości, ustawienie określonej wartości lub ustawienie określonego komunikatu o błędzie. W przypadku niepowodzenia kroku przetwarzania wstępnego pozycja nie stanie się nieobsługiwana, jeśli wybrano opcję odrzucenia wartości lub ustawienia określonej wartości.

Sprawdzenie błędu w JSON

Sprawdza komunikat błędu na poziomie aplikacji znajdujący się pod JSONPath. Przetwarzanie zostanie zatrzymane, jeśli operacja się powiedzie, a komunikat nie będzie pusty; w przeciwnym razie przetwarzanie będzie kontynuowane z wartością sprzed tego kroku przetwarzania wstępnego.

Uwagi:

- Te błędy usług zewnętrznych są zgłaszane użytkownikowi w niezmienionej postaci, bez dodawania informacji o kroku przetwarzania wstępnego;
- W przypadku niepowodzenia parsowania nieprawidłowego JSON nie zostanie zgłoszony żaden błąd;
- Jeśli zaznaczysz pole wyboru *Custom on fail*, możliwe jest określenie własnych opcji obsługi błędów: odrzucenie wartości, ustawienie określonej wartości lub ustawienie określonego komunikatu błędu. W przypadku nieudanego kroku przetwarzania wstępnego pozycja nie stanie się nieobsługiwana, jeśli wybrano opcję odrzucenia wartości lub ustawienia określonej wartości.

Sprawdzenie błędu w XML

Sprawdza komunikat błędu na poziomie aplikacji znajdujący się pod XPath. Przetwarzanie zostanie zatrzymane, jeśli zakończy się powodzeniem i komunikat nie jest pusty; w przeciwnym razie przetwarzanie będzie kontynuowane z wartością sprzed tego kroku wstępnego przetwarzania.

Uwagi:

- Błędy tych usług zewnętrznych są zgłaszane użytkownikowi w niezmienionej postaci, bez dodawania informacji o kroku wstępnego przetwarzania;
- W przypadku niepowodzenia parsowania nieprawidłowego XML nie zostanie zgłoszony żaden błąd;
- Jeśli zaznaczysz pole wyboru *Custom on fail*, możliwe jest określenie niestandardowych opcji obsługi błędów: odrzucenie wartości, ustawienie określonej wartości lub ustawienie określonego komunikatu błędu. W przypadku nieudanego kroku wstępnego przetwarzania pozycja nie stanie się nieobsługiwana, jeśli wybrano opcję odrzucenia wartości lub ustawienia określonej wartości.

Sprawdzenie błędu za pomocą wyrażenia regularnego

Sprawdź komunikat błędu na poziomie aplikacji za pomocą wyrażenia regularnego. Zatrzymaj przetwarzanie, jeśli zakończy się powodzeniem i komunikat nie jest pusty; w przeciwnym razie kontynuuj przetwarzanie z wartością, która była przed tym krokiem przetwarzania wstępnego.

Parametry:

- **pattern** - wyrażenie regularne;

- **output** - szablon formatowania danych wyjściowych. Sekwencja ucieczki \N (gdzie N=1…9) jest zastępowana N-tą dopasowaną grupą. Sekwencja ucieczki \0 jest zastępowana dopasowanym tekstem.

Uwagi:

- Te błędy usług zewnętrznych są zgłaszane użytkownikowi w niezmienionej postaci, bez dodawania informacji o kroku przetwarzania wstępnego;
- Jeśli zaznaczysz pole wyboru *Custom on fail*, możliwe jest określenie niestandardowych opcji obsługi błędów: odrzucenie wartości, ustawienie określonej wartości lub ustawienie określonego komunikatu błędu. W przypadku niepowodzenia kroku przetwarzania wstępnego pozycja nie stanie się nieobsługiwana, jeśli wybrano opcję odrzucenia wartości lub ustawienia określonej wartości.

Sprawdzenie nieobsługiwanej wartości

Sprawdź, czy nie udało się pobrać żadnej wartości pozycji. Określ, jak przetworzyć błąd, na podstawie analizy zwróconego komunikatu o błędzie.

Parametry:

- **scope** — wybierz zakres przetwarzania błędu:
dowolny błąd — dowolny błąd;
błąd pasuje — tylko błąd pasujący do wyrażenia regularnego określonego w *pattern*;
błąd nie pasuje — tylko błąd, który nie pasuje do wyrażenia regularnego określonego w *pattern*
- **pattern** — wyrażenie regularne, do którego ma pasować błąd. Jeśli w parametrze scope wybrano *dowolny błąd*, to pole to nie jest wyświetlane. Jeśli jest wyświetlane, to pole jest wymagane.

Uwagi:

- Zwykle brak wartości lub niepowodzenie pobrania wartości powoduje, że pozycja staje się nieobsługiwana. Ten krok preprocessing umożliwia zmianę tego zachowania. Jeśli zaznaczysz pole wyboru *Custom on fail* (dla tego kroku preprocessing zawsze zaznaczone i wyszarzone), można określić niestandardowe opcje obsługi błędów: odrzucenie wartości, ustawienie określonej wartości lub ustawienie określonego komunikatu o błędzie. W przypadku niepowodzenia kroku preprocessing pozycja nie stanie się nieobsługiwana, jeśli wybrano opcję odrzucenia wartości lub ustawienia określonej wartości.
- Ten krok preprocessing sprawdza tylko, czy nie udało się pobrać wartości pozycji. Nie sprawdza na przykład, czy typ pobranej wartości (np. string) odpowiada typowi informacji pozycji (np. numeric); szczegóły znajdują się w Przykładach preprocessing. Jeśli występuje niezgodność typów, pozycja może nadal stać się nieobsługiwana po wykonaniu wszystkich kroków preprocessing. Aby sprawdzić niezgodność typów, można użyć na przykład kroku preprocessing *Custom multiplier*; zobacz Przykłady preprocessing.
- Przechwytywanie grup wyrażeń regularnych jest obsługiwane w polach *Set value to* lub *Set error to*. Użyj \N (gdzie N=1…9), aby pobrać N-tą dopasowaną grupę; użyj \0, aby pobrać dopasowany tekst;
- Te kroki są zawsze wykonywane jako pierwsze kroki preprocessing i po zapisaniu zmian w pozycji są umieszczane nad wszystkimi pozostałymi;
- Obsługiwanych jest wiele kroków *Check for not supported value*, w określonej kolejności. Krok dla *dowolny błąd* zostanie automatycznie umieszczony jako ostatni krok w tej grupie.

Odrzuć niezmienione

Odrzuć wartość, jeśli nie uległa zmianie.

Uwagi:

- Jeśli wartość zostanie odrzucona, nie jest zapisywana w bazie danych, a serwer Zabbix nie ma wiedzy o tym, że ta wartość została odebrana. Wyrażenia wyzwalaczy nie będą oceniane, w rezultacie nie zostaną utworzone/rozwiązane żadne problemy dla powiązanych wyzwalaczy. Funkcje będą działać wyłącznie na podstawie danych, które są faktycznie zapisane w bazie danych. Ponieważ trendy są tworzone na podstawie danych w bazie danych, jeśli przez godzinę nie zostanie zapisana żadna wartość, to dla tej godziny również nie będzie danych trendów.
- Dla jednej pozycji można określić tylko jedną opcję ograniczania.

Odrzuć niezmienione z heartbeat

Odrzuć wartość, jeśli nie zmieniła się w zdefiniowanym okresie czasu (w sekundach).

Uwagi:

- Obsługiwane są dodatnie wartości całkowite do określenia liczby sekund (minimum — 1 sekunda);
- Można używać sufiksów czasu (np. 30s, 1m, 2h, 1d);
- Można używać makr użytkownika i makr wykrywania niskiego poziomu;
- Jeśli wartość zostanie odrzucona, nie jest zapisywana w bazie danych, a serwer Zabbix nie ma informacji, że ta wartość została odebrana. Żadne wyrażenia wyzwalaczy nie będą obliczane, w rezultacie nie zostaną utworzone/rozwiązane żadne problemy dla powiązanych wyzwalaczy. Funkcje będą działać wyłącznie na podstawie danych, które są faktycznie zapisane w bazie danych. Ponieważ trendy są tworzone na podstawie danych w bazie danych, jeśli przez godzinę nie zostanie zapisana żadna wartość, to również nie będzie danych trendów dla tej godziny.

- Dla jednej pozycji można określić tylko jedną opcję ograniczania.

Wzorzec Prometheus

Użyj następującego zapytania, aby wyodrębnić wymagane dane z metryk Prometheus.

Więcej szczegółów znajduje się w sekcji sprawdzanie Prometheus.

Prometheus do JSON

Konwertuj wymagane metryki Prometheus do formatu JSON.

Więcej informacji znajduje się w sekcji Prometheus checks.

Obsługa makr

Makra użytkownika oraz makra użytkownika z kontekstem są obsługiwane w:

- parametrach kroku przetwarzania wstępnego, w tym w kodzie JavaScript;
- parametrach niestandardowej obsługi błędów (pola *Ustaw wartość na* i *Ustaw błąd na*).

Note:
Kontekst makra jest ignorowany, gdy makro jest zastępowane swoją wartością. Wartość makra jest wstawiana do kodu w postaci niezmienionej; nie ma możliwości dodania dodatkowego escapingu przed umieszczeniem wartości w kodzie JavaScript. Należy pamiętać, że w niektórych przypadkach może to powodować błędy JavaScript.

Testowanie

Zobacz testowanie preprocessing.

1 Testowanie przetwarzania wstępnego

Testowanie

Testowanie kroków przetwarzania wstępnego jest przydatne, aby upewnić się, że złożone potoki przetwarzania wstępnego dają oczekiwane wyniki, bez konieczności czekania na odebranie i wstępne przetworzenie wartości pozycji.

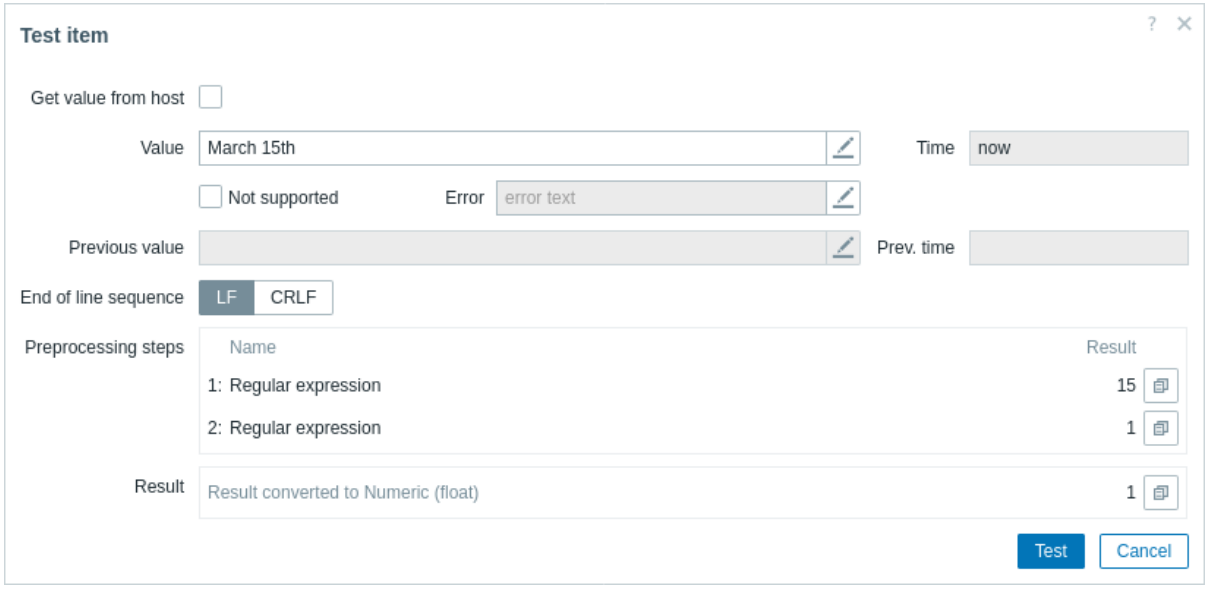


Możliwe jest testowanie:

- względem hipotetycznej wartości
- względem rzeczywistej wartości z hosta

Każdy krok przetwarzania wstępnego można testować indywidualnie, a także można testować wszystkie kroki razem. Po kliknięciu odpowiednio przycisku *Test* lub *Test all steps* w bloku Actions otwierane jest okno testowania.

Testowanie wartości hipotetycznej



Parametr	Opis
Pobierz wartość z hosta	Jeśli chcesz przetestować wartość hipotetyczną, pozostaw to pole wyboru niezaznaczone. Zobacz także: Testowanie wartości rzeczywistej.
Wartość	Wprowadź wartość wejściową do przetestowania. Kliknięcie w polu parametru lub przycisku podglądu/edycji otworzy okno obszaru tekstowego do wprowadzenia wartości lub bloku kodu.
Nieobsługiwane	Zaznacz to pole wyboru, aby przetestować nieobsługiwaną wartość. Ta opcja jest przydatna do testowania kroku przetwarzania wstępnego *Sprawdź pod kątem nieobsługiwanej wartości*.
Błąd	Wprowadź tekst błędu. To pole jest włączone, gdy *Pobierz wartość z hosta* jest odznaczone, a *Nieobsługiwane* jest zaznaczone. Jeśli *Pobierz wartość z hosta* jest zaznaczone, to pole zostanie wypełnione rzeczywistym komunikatem błędu (tylko do odczytu) z hosta.
Czas	Wyświetlany jest czas wartości wejściowej: `now` (tylko do odczytu).
Poprzednia wartość	Wprowadź poprzednią wartość wejściową do porównania. Tylko dla kroków przetwarzania wstępnego *Zmiana* i *Ograniczanie*.
Poprzedni czas	Wprowadź czas poprzedniej wartości wejściowej do porównania. Tylko dla kroków przetwarzania wstępnego *Zmiana* i *Ograniczanie*. Wartość domyślna jest oparta na wartości pola „Interwał aktualizacji” pozycji (jeśli „1m”, to to pole zostanie wypełnione wartością `now-1m`). Jeśli nic nie określono lub użytkownik nie ma dostępu do hosta, wartością domyślną jest `now-30s`.
Makra	Jeśli używane są jakiekolwiek makra, są one wyświetlane wraz ze swoimi wartościami. Wartości można edytować na potrzeby testowania, ale zmiany zostaną zapisane tylko w kontekście testowania.
Sekwencja końca linii	Wybierz sekwencję końca linii dla wielowierszowych wartości wejściowych: **LF** - sekwencja LF (line feed) **CRLF** - sekwencja CRLF (carriage-return line-feed).
Kroki przetwarzania wstępnego	Wyświetlane są kroki przetwarzania wstępnego; wynik testu dla każdego kroku jest pokazywany po kliknięciu przycisku *Test*. Wyniki testu są obcinane do maksymalnego rozmiaru 512KB podczas wysyłania do frontend. Wyniki testu można kopiować (nie więcej niż obcięte 512KB). Jeśli wynik zostanie obcięty, wyświetlana jest ikona ostrzeżenia. Opis ostrzeżenia jest wyświetlany po najechaniu kursorem. Należy pamiętać, że dane większe niż 512KB są nadal w pełni przetwarzane przez serwer Zabbix. Jeśli krok zakończył się niepowodzeniem podczas testowania, wyświetlana jest ikona błędu. Opis błędu jest wyświetlany po najechaniu kursorem. Jeśli dla kroku określono „Custom on fail” i to działanie zostało wykonane, bezpośrednio po wierszu kroku testu przetwarzania wstępnego pojawia się nowy wiersz pokazujący, jakie działanie zostało wykonane i jaki rezultat przyniosło (błąd lub wartość).

Parametr	Opis
Wynik	Końcowy wynik testowania kroków przetwarzania wstępnego jest wyświetlany we wszystkich przypadkach, gdy wszystkie kroki są testowane razem (po kliknięciu przycisku *Test all steps*). Wyświetlany jest również typ konwersji do typu wartości pozycji, na przykład `Result converted to Numeric (unsigned)`. Wyniki testu są obcinane do maksymalnego rozmiaru 512KB podczas wysyłania do frontend. Końcowy wynik można kopiować (nie więcej niż obcięte 512KB). Jeśli wynik zostanie obcięty, wyświetlana jest ikona ostrzeżenia. Opis ostrzeżenia jest wyświetlany po najechaniu kursorem. Należy pamiętać, że dane większe niż 512KB są nadal w pełni przetwarzane przez serwer Zabbix.

Kliknij *Test*, aby zobaczyć wynik po każdym kroku przetwarzania wstępnego.

Wartości testowe są przechowywane między sesjami testowymi zarówno dla poszczególnych kroków, jak i dla wszystkich kroków, co pozwala użytkownikowi zmieniać kroki przetwarzania wstępnego lub konfigurację pozycji, a następnie wrócić do okna testowania bez konieczności ponownego wprowadzania informacji. Wartości są jednak tracone po odświeżeniu strony.

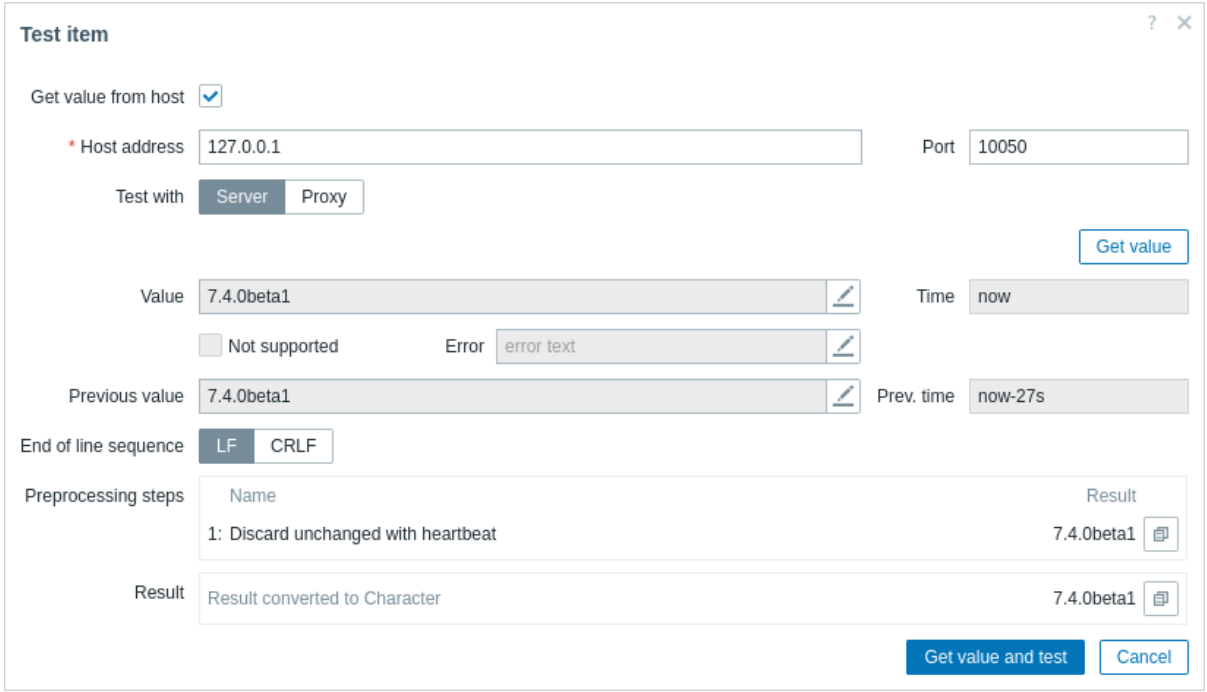
Testowanie jest wykonywane przez serwer Zabbix. frontend wysyła odpowiednie żądanie do serwer i oczekuje na wynik. Żądanie zawiera wartość wejściową oraz kroki przetwarzania wstępnego (z rozwiniętymi makrami użytkownika). Dla kroków *Zmiana* i *Ograniczanie* można określić opcjonalną poprzednią wartość i czas. serwer odpowiada wynikami dla każdego kroku przetwarzania wstępnego.

Wszystkie błędy techniczne lub błędy walidacji danych wejściowych są wyświetlane w polu błędu u góry okna testowania.

Testowanie rzeczywistej wartości

Aby przetestować preprocessing na podstawie rzeczywistej wartości:

- Zaznacz pole wyboru *Get value from host*
- Wprowadź lub zweryfikuj parametry hosta (adres hosta, port, nazwa proxy/brak proxy) oraz szczegóły specyficzne dla pozycji (takie jak community SNMPv2 lub poświadczenia bezpieczeństwa SNMPv3). Te pola są zależne od kontekstu:
  - Wartości są wstępnie uzupełniane, gdy to możliwe, tj. dla pozycji wymagających agent, poprzez pobranie informacji z wybranego interfejsu agent hosta
  - Wartości muszą zostać wprowadzone ręcznie dla pozycji szablonu
  - Wartości makr w postaci zwykłego tekstu są rozwijane
  - Jeśli wartość pola (lub część wartości) jest tajnym makrem albo makrem Vault, pole będzie puste i trzeba je uzupełnić ręcznie. Jeśli dowolny parametr pozycji zawiera wartość tajnego makra, wyświetlany jest następujący komunikat ostrzegawczy: "Pozycja zawiera makra zdefiniowane przez użytkownika z tajnymi wartościami. Wartości tych makr należy wprowadzić ręcznie."
  - Pola są wyłączone, gdy nie są potrzebne w kontekście typu pozycji (np. pola adresu hosta i proxy są wyłączone dla pozycji obliczanych)
- Kliknij *Get value and test*, aby przetestować preprocessing



Jeśli w formularzu konfiguracji pozycji określono mapowanie wartości (pole „Show value”), okno dialogowe testu pozycji pokaże dodatkowy wiersz po wyniku końcowym, o nazwie „Result with value map applied”.

Parametry specyficzne dla pobierania rzeczywistej wartości z hosta:

Parameter	Description
Get value from host	Zaznacz to pole wyboru, aby pobrać rzeczywistą wartość z hosta.
Host address	Wprowadź adres hosta. To pole jest automatycznie wypełniane adresem interfejsu hosta pozycji.
Port	Wprowadź port hosta. To pole jest automatycznie wypełniane portem interfejsu hosta pozycji.
Additional fields for SNMP interfaces (SNMP version, SNMP community, Context name, etc.)	Zobacz Configuring SNMP monitoring, aby uzyskać dodatkowe informacje o konfiguracji interfejsu SNMP (v1, v2 i v3). Pola te są automatycznie wypełniane na podstawie interfejsu hosta pozycji.
Proxy	Określ proxy, jeśli host jest monitorowany przez proxy. To pole jest automatycznie wypełniane proxy hosta (jeśli istnieje).
Value	Wartość pobrana z hosta. Kliknięcie w polu parametru lub przycisku podglądu/edycji otworzy okno obszaru tekstowego z wartością lub blokiem kodu. Wartości są obcinane do maksymalnego rozmiaru 512 KB i tylko we frontend. Jeśli wynik zostanie obcięty, wyświetlana jest ikona ostrzeżenia. Opis ostrzeżenia jest wyświetlany po najechaniu kursorem. Należy pamiętać, że dane większe niż 512 KB są nadal w pełni przetwarzane przez serwer Zabbix.

Dla pozostałych parametrów zobacz Testing hypothetical value powyżej.

2 Szczegóły przetwarzania wstępnego

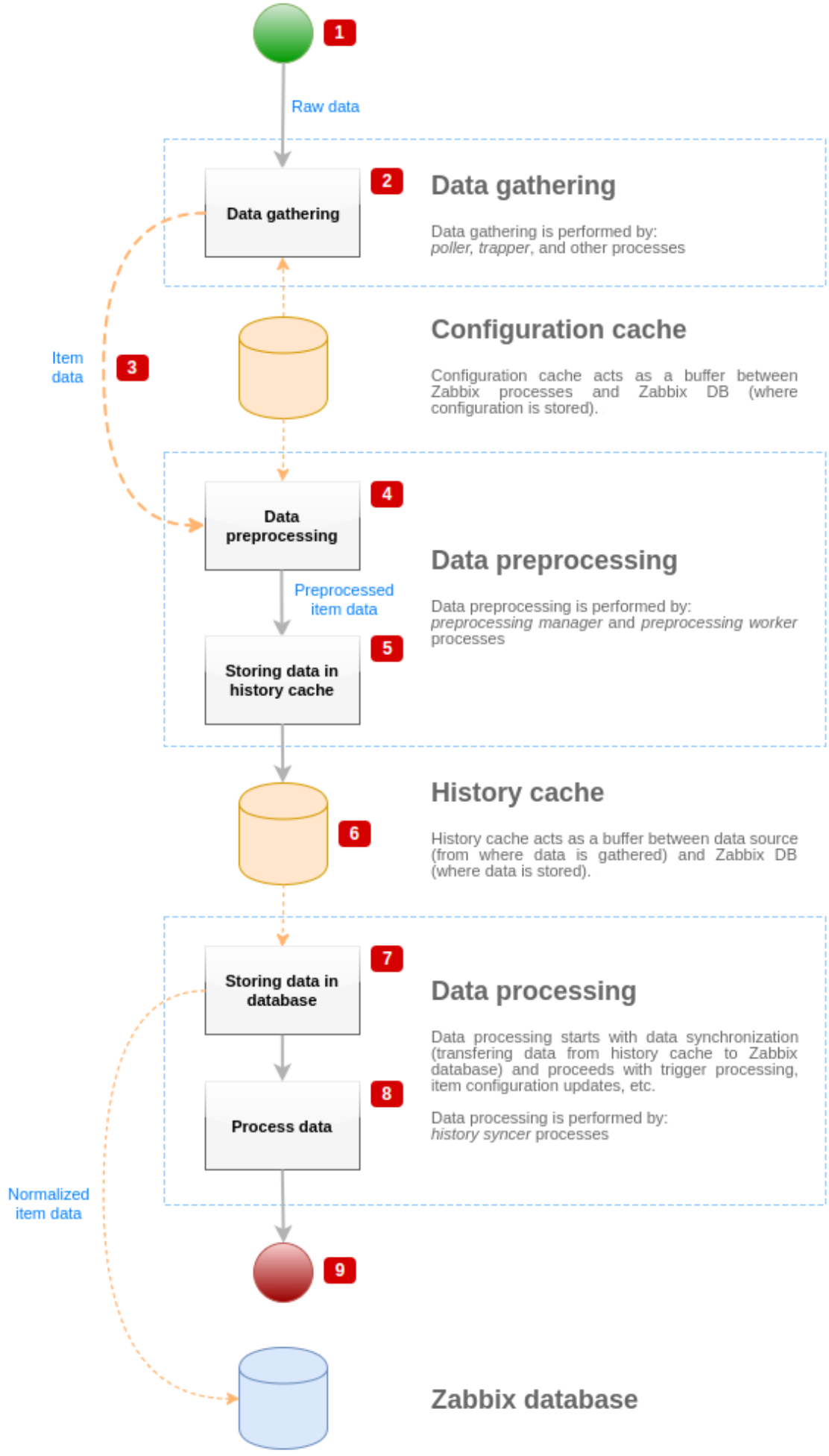
Przegląd

Ta sekcja zawiera szczegółowe informacje o wstępnym przetwarzaniu wartości pozycji. Wstępne przetwarzanie wartości pozycji pozwala definiować i wykonywać reguły transformacji dla otrzymanych wartości pozycji.

Wstępne przetwarzanie jest zarządzane przez proces menedżera wstępnego przetwarzania wraz z workerami wstępnego przetwarzania, które wykonują kroki wstępnego przetwarzania. Wszystkie wartości ze wstępnym przetwarzaniem, otrzymane od różnych modułów zbierania danych, przechodzą przez menedżera wstępnego przetwarzania, zanim zostaną dodane do pamięci podręcznej historii. Używana jest komunikacja IPC oparta na gniazdach między modułami zbierania danych (pollerami, trapperami itp.) a procesem wstępnego przetwarzania. Kroki wstępnego przetwarzania wykonuje serwer Zabbix lub proxy Zabbix (dla pozycji monitorowanych przez proxy).

Przetwarzanie wartości pozycji

Aby zwizualizować przepływ danych od źródła danych do bazy danych Zabbix, możemy użyć następującego uproszczonego diagramu:


1
Raw data
Data gathering
2
Data gathering
Data gathering is performed by:
poller, trapper, and other processes
Item data
3
Configuration cache
Configuration cache acts as a buffer between Zabbix processes and Zabbix DB (where configuration is stored).
Data preprocessing
4
Data preprocessing
Data preprocessing is performed by:
preprocessing manager and preprocessing worker processes
Preprocessed item data
Storing data in history cache
5
History cache
6
History cache acts as a buffer between data source (from where data is gathered) and Zabbix DB (where data is stored).
Storing data in database
7
Data processing
Data processing starts with data synchronization (transfering data from history cache to Zabbix database) and proceeds with trigger processing, item configuration updates, etc.
Process data
8
Data processing is performed by:
history syncer processes
Normalized item data
9
Zabbix database

Powyższy diagram pokazuje tylko procesy, obiekty i działania związane z przetwarzaniem wartości pozycji w **uproszczonej** formie. Diagram nie pokazuje warunkowych zmian kierunku, obsługi błędów ani pętli. Nie pokazano również lokalnej pamięci podręcznej danych menedżera preprocessing, ponieważ nie wpływa ona bezpośrednio na przepływ danych. Celem tego diagramu jest pokazanie procesów biorących udział w przetwarzaniu wartości pozycji oraz sposobu ich współdziałania.

- Zbieranie danych rozpoczyna się od surowych danych ze źródła danych. Na tym etapie dane zawierają tylko identyfikator, znacznik czasu i wartość (może to być również wiele wartości).
- Niezależnie od tego, jaki typ mechanizmu zbierania danych jest używany, idea jest taka sama dla sprawdzeń aktywnych i pasywnych, dla pozycji trapper itd., ponieważ zmienia się tylko format danych i inicjator komunikacji (albo mechanizm zbierania danych oczekuje na połączenie i dane, albo inicjuje komunikację i żąda danych). Surowe dane są walidowane, konfiguracja pozycji jest pobierana z pamięci podręcznej konfiguracji (dane są wzbogacane o dane konfiguracyjne).
- Mechanizm IPC oparty na gniazdach jest używany do przekazywania danych z mechanizmów zbierania danych do menedżera preprocessing. W tym momencie mechanizm zbierania danych kontynuuje zbieranie danych bez oczekiwania na odpowiedź od menedżera preprocessing.
- Wykonywane jest preprocessing danych. Obejmuje to wykonanie kroków preprocessing oraz przetwarzanie pozycji zależnych.

Note:
Pozycja może zmienić swój stan na NOT SUPPORTED podczas wykonywania preprocessing, jeśli którykolwiek z kroków preprocessing zakończy się niepowodzeniem.

- Dane historyczne z lokalnej pamięci podręcznej danych menedżera preprocessing są opróżniane do pamięci podręcznej historii.
- W tym momencie przepływ danych zatrzymuje się do czasu następnej synchronizacji pamięci podręcznej historii (gdy proces synchronizacji historii wykonuje synchronizację danych).
- Proces synchronizacji rozpoczyna się od normalizacji danych przed zapisaniem ich w bazie danych Zabbix. Normalizacja danych wykonuje konwersje do żądanego typu pozycji (typu zdefiniowanego w konfiguracji pozycji), w tym obcinanie danych tekstowych na podstawie predefiniowanych rozmiarów dozwolonych dla tych typów (HISTORY_STR_VALUE_LEN dla string, HISTORY_TEXT_VALUE_LEN dla text oraz HISTORY_LOG_VALUE_LEN dla wartości log). Po zakończeniu normalizacji dane są wysyłane do bazy danych Zabbix.

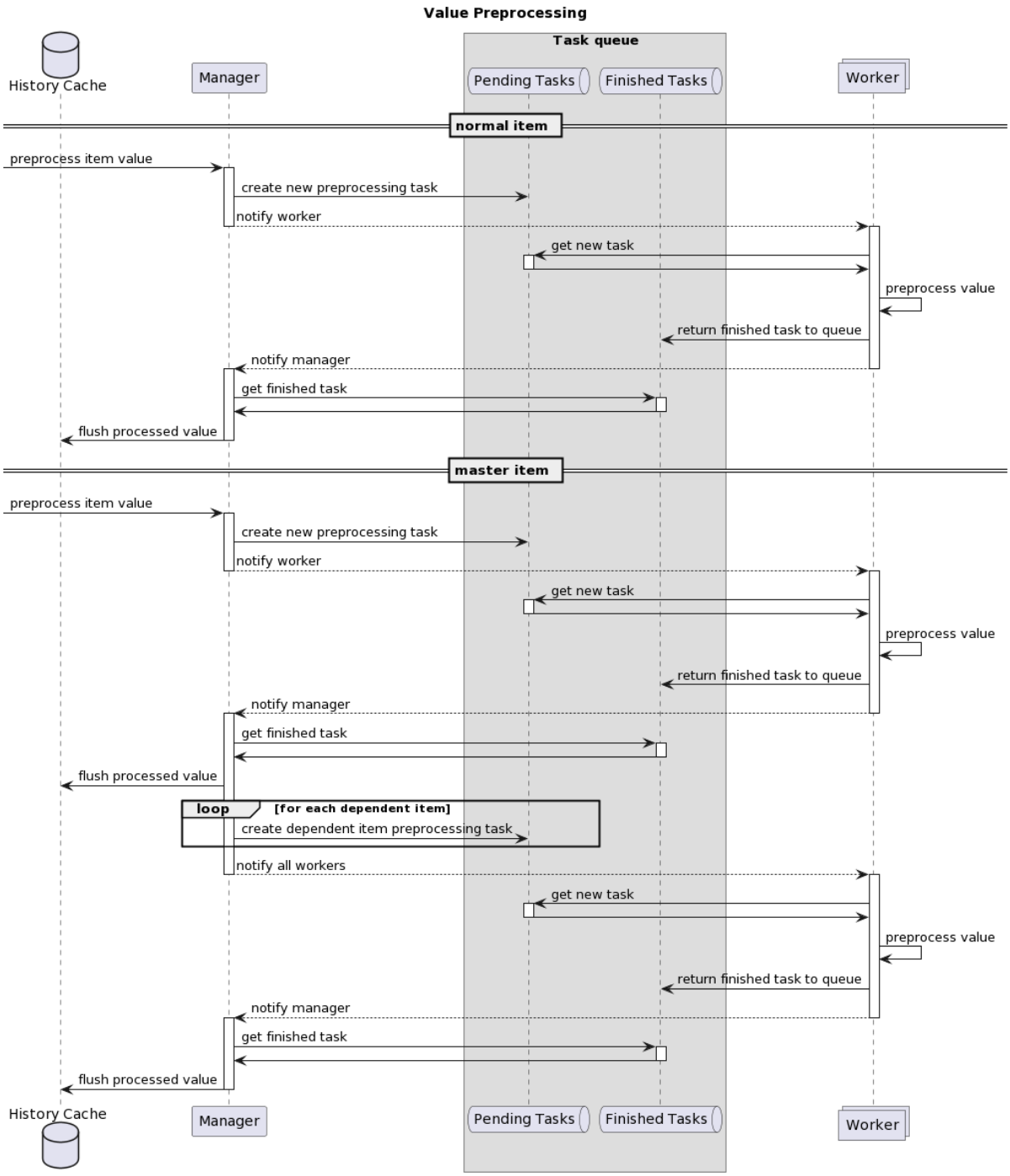
Note:
Pozycja może zmienić swój stan na NOT SUPPORTED, jeśli normalizacja danych zakończy się niepowodzeniem (na przykład gdy wartości tekstowej nie można przekonwertować na liczbę).

- Zebrane dane są przetwarzane — sprawdzane są wyzwalacze, konfiguracja pozycji jest aktualizowana, jeśli pozycja staje się NOT SUPPORTED itd.
- Jest to uznawane za koniec przepływu danych z punktu widzenia przetwarzania wartości pozycji.

Wstępne przetwarzanie wartości pozycji

Wstępne przetwarzanie danych odbywa się w następujących krokach:

- Jeśli pozycja nie ma ani wstępnego przetwarzania, ani pozycji zależnych, jej wartość jest albo dodawana do pamięci podręcznej historii, albo wysyłana do menedżera LLD. W przeciwnym razie wartość pozycji jest przekazywana do menedżera wstępnego przetwarzania za pomocą mechanizmu IPC opartego na gniazdach UNIX.
- Tworzone jest zadanie wstępnego przetwarzania, dodawane do kolejki, a workery wstępnego przetwarzania są powiadamiane o nowym zadaniu.
- W tym momencie przepływ danych zatrzymuje się, dopóki nie będzie dostępny co najmniej jeden nieużywany (tj. niewykonujący żadnych zadań) worker wstępnego przetwarzania.
- Gdy worker wstępnego przetwarzania jest dostępny, pobiera następne zadanie z kolejki.
- Po zakończeniu wstępnego przetwarzania (zarówno w przypadku nieudanego, jak i udanego wykonania kroków wstępnego przetwarzania) wstępnie przetworzona wartość jest dodawana do kolejki zakończonych zadań, a menedżer jest powiadamiany o nowym zakończonym zadaniu.
- Menedżer wstępnego przetwarzania konwertuje wynik do żądanego formatu (zdefiniowanego przez typ wartości pozycji) i albo dodaje go do pamięci podręcznej historii, albo wysyła do menedżera LLD.
- Jeśli dla przetwarzanej pozycji istnieją pozycje zależne, są one dodawane do kolejki wstępnego przetwarzania z użyciem wstępnie przetworzonej wartości nadrzędnej pozycji. Pozycje zależne są umieszczane w kolejce z pominięciem zwykłych żądań wstępnego przetwarzania wartości, ale tylko dla pozycji nadrzędnych z ustawioną wartością i niebędących w stanie NOT SUPPORTED.



Należy pamiętać, że na diagramie wstępne przetwarzanie pozycji nadrzędnej jest nieco uproszczone przez pominięcie buforowania wstępnego przetwarzania.

Kolejka przetwarzania wstępnego

Kolejka przetwarzania wstępnego jest zorganizowana następująco:

- lista oczekujących zadań:
  - zadania utworzone bezpośrednio na podstawie żądań przetwarzania wstępnego wartości, w kolejności ich otrzymania
- lista zadań natychmiastowych (przetwarzanych przed zadaniami oczekującymi):
  - zadania testowe (tworzone w odpowiedzi na żądania testowania pozycja/przetwarzania wstępnego przez frontend)
  - zadania zależnych pozycji
  - zadania sekwencyjne (zadania, które muszą być wykonywane w ścisłej kolejności):
    * posiadające kroki przetwarzania wstępnego wykorzystujące ostatnią wartość:
      · zmiana
      · ograniczanie
      · JavaScript (buforowanie kodu bajtowego)
    * buforowanie przetwarzania wstępnego zależnych pozycji
- lista zakończonych zadań

Buforowanie przetwarzania wstępnego

Buforowanie przetwarzania wstępnego zostało wprowadzone w celu poprawy wydajności przetwarzania wstępnego dla wielu zależnych pozycji mających podobne kroki przetwarzania wstępnego (co jest częstym rezultatem LLD).

Buforowanie polega na przetworzeniu wstępnym jednej zależnej pozycji i ponownym wykorzystaniu części wewnętrznych danych przetwarzania wstępnego dla pozostałych zależnych pozycji. Pamięć podręczna przetwarzania wstępnego jest obsługiwana tylko dla pierwszego kroku przetwarzania wstępnego następujących typów:

- Wzorzec Prometheus (indeksuje dane wejściowe według metryk)
- JSONPath (parsuje dane do drzewa obiektów i indeksuje pierwsze wyrażenie `[?(@.path == "value")]`)

Workery przetwarzania wstępnego

Plik konfiguracyjny serwera Zabbix pozwala użytkownikom ustawić liczbę wątków workerów przetwarzania wstępnego. Parametr konfiguracyjny StartPreprocessors powinien zostać użyty do ustawienia liczby wstępnie uruchamianych instancji workerów przetwarzania wstępnego, która powinna co najmniej odpowiadać liczbie dostępnych rdzeni CPU.

Jeśli zadania przetwarzania wstępnego nie są ograniczone wydajnością CPU i obejmują częste żądania sieciowe, zaleca się skonfigurowanie dodatkowych workerów. Optymalna liczba workerów przetwarzania wstępnego może zależeć od wielu czynników, w tym liczby „przetwarzalnych" pozycji (pozycji, które wymagają wykonania jakichkolwiek kroków przetwarzania wstępnego), liczby procesów zbierania danych, średniej liczby kroków przetwarzania wstępnego dla pozycji itd. Niewystarczająca liczba workerów może prowadzić do wysokiego zużycia pamięci. Informacje o rozwiązywaniu problemów z nadmiernym zużyciem pamięci w instalacji Zabbix można znaleźć w sekcji Profiling excessive memory usage with tcmalloc.

Zakładając jednak, że nie występują ciężkie operacje przetwarzania wstępnego, takie jak analizowanie dużych fragmentów XML/JSON, liczba workerów przetwarzania wstępnego może odpowiadać łącznej liczbie procesów zbierających dane. W ten sposób w większości przypadków (z wyjątkiem sytuacji, gdy dane od procesu zbierającego napływają zbiorczo) będzie dostępny co najmniej jeden nieużywany worker przetwarzania wstępnego dla zebranych danych.

Warning:
Zbyt duża liczba procesów zbierania danych (pollers, unreachable pollers, ODBC pollers, HTTP pollers, Java pollers, pingers, trappers, proxypollers) wraz z IPMI manager, SNMP trapper i workerami przetwarzania wstępnego może wyczerpać limit deskryptorów plików na proces dla menedżera przetwarzania wstępnego.

 Wyczerpanie limitu deskryptorów plików na proces spowoduje zatrzymanie serwera Zabbix, zwykle krótko po uruchomieniu, choć czasami może to nastąpić później. Aby uniknąć takich problemów, przejrzyj plik konfiguracyjny serwera Zabbix, aby zoptymalizować liczbę równoczesnych kontroli i procesów. Dodatkowo, w razie potrzeby upewnij się, że limit deskryptorów plików jest ustawiony wystarczająco wysoko, sprawdzając i dostosowując limity systemowe.

Potok przetwarzania wartości

Przetwarzanie wartości pozycji jest wykonywane w wielu krokach (lub fazach) przez wiele procesów. Może to powodować:

- Zależna pozycja może otrzymywać wartości, podczas gdy wartość główna NIE może. Można to osiągnąć przy użyciu następującego przypadku użycia:
  - Główna pozycja ma typ wartości `UINT` (można użyć trapper item), zależna pozycja ma typ wartości `TEXT`.
  - Dla głównej i zależnej pozycji nie są wymagane żadne kroki preprocessing.
  - Wartość tekstowa (na przykład „abc") powinna zostać przekazana do głównej pozycji.
  - Ponieważ nie ma kroków preprocessing do wykonania, menedżer preprocessing sprawdza, czy główna pozycja nie jest w stanie NOT SUPPORTED oraz czy wartość jest ustawiona (oba warunki są spełnione), a następnie umieszcza zależną pozycję w kolejce z tą samą wartością co główna pozycja (ponieważ nie ma kroków preprocessing).
  - Gdy zarówno główna, jak i zależna pozycja osiągną fazę synchronizacji historii, główna pozycja przechodzi w stan NOT SUPPORTED z powodu błędu konwersji wartości (dane tekstowe nie mogą zostać przekonwertowane na liczbę całkowitą bez znaku).

W rezultacie zależna pozycja otrzymuje wartość, podczas gdy główna pozycja zmienia swój stan na NOT SUPPORTED.

- Zależna pozycja otrzymuje wartość, która nie jest obecna w historii głównej pozycji. Ten przypadek użycia jest bardzo podobny do poprzedniego, z wyjątkiem typu głównej pozycji. Na przykład, jeśli dla głównej pozycji używany jest typ `CHAR`, to wartość głównej pozycji zostanie obcięta w fazie synchronizacji historii, podczas gdy zależne pozycje otrzymają swoje wartości z początkowej (nieobciętej) wartości głównej pozycji.

3 Przykłady przetwarzania wstępnego

Przegląd

W tej sekcji przedstawiono przykłady użycia kroków przetwarzania wstępnego do realizacji niektórych praktycznych zadań.

Filtrowanie rekordów dziennika zdarzeń VMware

Ten przykład wykorzystuje krok przetwarzania wstępnego Matches regular expression do odfiltrowania niepotrzebnych zdarzeń z dziennika zdarzeń VMware.

1. Na działającym hoście VMware Hypervisor sprawdź, czy pozycja vmware.eventlog jest obecna i działa prawidłowo. Zwróć uwagę, że pozycja dziennika zdarzeń może już być obecna na hypervisorze, jeśli podczas tworzenia hosta został podłączony szablon VMware.

2. Na hoście VMware Hypervisor utwórz pozycję zależną typu *Log* i ustaw pozycję dziennika zdarzeń jako jej pozycję nadrzędną.

3. Na karcie *Preprocessing* pozycji zależnej kliknij *Add*, aby utworzyć krok przetwarzania wstępnego, i wybierz *Matches regular expression* z listy rozwijanej. Następnie określ jeden z następujących wzorców:

- Aby filtrować wszystkie zdarzenia dziennika:

```
.* logged in .*
```

- Aby filtrować wiersze zawierające nazwy użytkowników po "User":

```
\bUser\s+\K\S+
```

Attention:
Jeśli wyrażenie regularne nie zostanie dopasowane, pozycja zależna stanie się nieobsługiwana i zostanie wyświetlony odpowiedni komunikat o błędzie. Aby tego uniknąć, zaznacz pole wyboru *Custom on fail* i wybierz opcję, taką jak odrzucenie wartości lub ustawienie wartości niestandardowej. Pamiętaj, że wartości discarded nie są przechowywane w bazie danych; w rezultacie wyzwalacze nie są oceniane, a dane trendu nie są generowane.

Alternatywnie możesz użyć kroku przetwarzania wstępnego Regular expression, aby wyodrębnić pasujące grupy i kontrolować dane wyjściowe:

- Aby wyodrębnić i zwrócić całe zdarzenie dziennika zawierające "logged in", podaj następujące parametry:

```
Pattern: .*logged in.*
Output: \0
```

- Aby wyodrębnić i zwrócić nazwy użytkowników występujące po "User":

```
Pattern: User (.*?)(?=\ )
Output: \1
```

Sprawdzanie typu pobranej wartości

W tym przykładzie użyto kroku przetwarzania wstępnego Custom multiplier, aby sprawdzić, czy typ pobranej wartości pozycji jest numeryczny.

Na karcie *Preprocessing* pozycji wybierz krok przetwarzania wstępnego *Custom multiplier* i określ następujący parametr (mnoży pobraną wartość przez 1):

```
1
```

Attention:
Jeśli przetwarzanie wstępne zakończy się niepowodzeniem (np. dane wejściowe nie są numeryczne), pozycja stanie się nieobsługiwana i zostanie wyświetlony odpowiedni komunikat o błędzie. Aby tego uniknąć, zaznacz pole wyboru *Custom on fail* i wybierz opcję, taką jak odrzucenie wartości lub ustawienie wartości niestandardowej. Należy pamiętać, że wartości discarded nie są przechowywane w bazie danych; w rezultacie wyzwalacze nie są oceniane, a dane trendu nie są generowane.

Sprawdzanie nieobsługiwanej wartości

Ten przykład wykorzystuje krok preprocessing Check for not supported value do sprawdzenia, czy nie udało się pobrać wartości pozycji.

Gdy proces pollera serwera/proxy Zabbix próbuje pobrać wartość pozycji, może:

- Zwrócić prawidłowy wynik.
- Zwrócić wynik, który początkowo wydaje się prawidłowy, ale później może stać się nieobsługiwany (np. z powodu niezgodności typu wartości po preprocessing).
- Zwrócić błąd podczas pobierania wartości, powodując, że pozycja stanie się nieobsługiwana. Typowe przyczyny obejmują:
  - Nieznany klucz pozycji (dla pozycji Zabbix agent, Simple check lub Zabbix internal)
  - Nieznany OID (SNMP agent), nieznany sensor (IPMI agent) lub brak metryki JMX (JMX agent)
  - Nie można odczytać pliku trap (SNMP trap)
  - Nie znaleziono skryptu (External check)

- Taki URL nie istnieje (HTTP agent, Browser)
- Logowanie nie powiodło się (SSH agent, TELNET agent)
- Nieprawidłowa składnia formuły (Calculated), błąd składni JavaScript (Script) lub nieprawidłowe SQL (Database monitor)

Aby wykrywać i obsługiwać błędy pobierania wartości pozycji, można użyć kroku preprocessing *Check for not supported value*. Należy pamiętać, że ten krok jest zawsze wykonywany jako pierwszy i wykrywa tylko błędy, które występują przed rozpoczęciem preprocessing.

Na karcie *Preprocessing* pozycji wybierz krok preprocessing *Check for not supported value* i określ jeden z następujących parametrów:

- Dla dowolnych błędów:

```
Parameter: any error
```

- Dla błędów zawierających ”cannot connect”:

```
Parameter: error matches
Pattern: (?i)cannot connect
```

Następnie użyj opcji *Custom on fail*, aby odrzucić wartość (w tym przypadku błąd), ustawić wartość niestandardową lub zwrócić niestandardowy komunikat o błędzie. Pamiętaj, że wartości discarded nie są przechowywane w bazie danych; w rezultacie wyzwalacze nie są obliczane, a dane trendu nie są generowane.

4 Funkcjonalność JSONPath

Przegląd

Ta sekcja przedstawia obsługiwaną funkcjonalność JSONPath w krokach wstępnego przetwarzania wartości pozycji.

JSONPath składa się z segmentów oddzielonych kropkami. Segment może mieć postać prostego słowa, reprezentującego nazwę wartości JSON, znaku wieloznacznego (`*`) lub bardziej złożonej konstrukcji ujętej w nawiasy kwadratowe. Kropka przed segmentem ujętym w nawiasy jest opcjonalna i może zostać pominięta.

Przykład JSONPath	Opis
`$.object.name`	Zwraca zawartość `object.name`.
`$.object['name']`	Zwraca zawartość `object.name`.
`$.object.['name']`	Zwraca zawartość `object.name`.
`$["object"]['name']`	Zwraca zawartość `object.name`.
`$.['object'].["name"]`	Zwraca zawartość `object.name`.
`$.object.history.length()`	Zwraca liczbę elementów tablicy `object.history`.
`$[?(@.name == 'Object')].price.first()`	Zwraca wartość właściwości `price` z pierwszego obiektu o nazwie „Object”.
`$[?(@.name == 'Object')].history.first().length()`	Zwraca liczbę elementów tablicy historii z pierwszego obiektu o nazwie „Object”.
`$[?(@.price > 10)].length()`	Zwraca liczbę obiektów z ceną większą niż 10.

Zobacz także: Escaping special characters from LLD macro values in JSONPath.

Obsługiwane segmenty

Segment	Opis
`<name>`	Dopasowuje właściwość obiektu według nazwy.
`*`	Dopasowuje wszystkie właściwości obiektu.
`['<name>']`	Dopasowuje właściwość obiektu według nazwy.
`['<name>', '<name>', ...]`	Dopasowuje właściwość obiektu według dowolnej z podanych nazw.
`[<index>]`	Dopasowuje element tablicy według indeksu.
`[<number>, <number>, ...]`	Dopasowuje element tablicy według dowolnego z podanych indeksów.
`[*]`	Dopasowuje wszystkie właściwości obiektu lub elementy tablicy.

Segment	Opis
`[<start>:<end>]`	Dopasowuje elementy tablicy według zdefiniowanego zakresu: **<start>** - pierwszy dopasowywany indeks (włącznie); jeśli nie został określony, dopasowywane są wszystkie elementy tablicy od początku; jeśli jest ujemny, określa przesunięcie początkowe liczone od końca tablicy; **<end>** - ostatni dopasowywany indeks (z wyłączeniem); jeśli nie został określony, dopasowywane są wszystkie elementy tablicy do końca; jeśli jest ujemny, określa przesunięcie początkowe liczone od końca tablicy.
`[?(<expression>)]`	Dopasowuje obiekty/elementy tablicy przez zastosowanie wyrażenia filtra.

Aby znaleźć pasujący segment z pominięciem jego pochodzenia (segment odłączony), należy poprzedzić go dwiema kropkami (`..`). Na przykład `$..name` lub `$..['name']` zwracają wartości wszystkich właściwości `name`.

Nazwy dopasowanych elementów można wyodrębnić, dodając do JSONPath sufiks tyldy (`~`). Zwraca on nazwę dopasowanego obiektu lub indeks dopasowanego elementu tablicy w formacie ciągu znaków. Format wyjściowy jest zgodny z tymi samymi zasadami co w przypadku innych zapytań JSONPath — wyniki ścieżki określonej są zwracane „tak jak są", a wyniki ścieżki nieokreślonej są zwracane w tablicy. Jednak wyodrębnianie nazwy elementu dopasowanego przez ścieżkę określoną ma niewielką wartość, ponieważ jest ona już znana.

Wyrażenie filtra

Wyrażenie filtra jest wyrażeniem arytmetycznym w notacji infiksowej.

Obsługiwane operandy:

Operand	Opis

`"<text>"`
`'<text>'`
	Stała tekstowa.
	
	Przykład:
	`'value: \\'1\\''`
	`"value: '1'"`

`<number>`	Stała liczbowa obsługująca notację naukową. Przykład: 123
`<jsonpath starting with $>`	Wartość wskazywana przez JSONPath od węzła głównego dokumentu wejściowego; obsługiwane są tylko ścieżki jednoznaczne. Przykład: `$.object.name`
`<jsonpath starting with @>`	Wartość wskazywana przez JSONPath od bieżącego obiektu/elementu; obsługiwane są tylko ścieżki jednoznaczne. Przykład: `@.name`

Obsługiwane operatory:

Operator	Typ	Opis	Wynik
-	Binarny	Odejmowanie	Liczba
+	Binarny	Dodawanie	Liczba
/	Binarny	Dzielenie	Liczba
*	Binarny	Mnożenie	Liczba
==	Binarny	Równość	Wartość logiczna (1/0)
!=	Binarny	Nierówność	Wartość logiczna (1/0)
	Binarny	Mniejsze niż	Wartość logiczna (1/0)
<=	Binarny	Mniejsze niż lub równe	Wartość logiczna (1/0)
>	Binarny	Większe niż	Wartość logiczna (1/0)
>=	Binarny	Większe niż lub równe	Wartość logiczna (1/0)
=~	Binarny	Pasuje do wyrażenia regularnego	Wartość logiczna (1/0)
!	Unarny	Logiczne NOT	Wartość logiczna (1/0)
||	Binarny	Logiczne OR	Wartość logiczna (1/0)
&&	Binarny	Logiczne AND	Wartość logiczna (1/0)

Funkcje

Funkcje mogą być używane na końcu JSONPath. Można łączyć wiele funkcji w łańcuch, jeśli poprzedzająca funkcja zwraca wartość akceptowaną przez następną funkcję.

Obsługiwane funkcje:

Funkcja	Opis	Wejście	Wyjście
`avg`	Średnia wartość liczb w tablicy wejściowej	Tablica liczb	Liczba
`min`	Minimalna wartość liczb w tablicy wejściowej	Tablica liczb	Liczba
`max`	Maksymalna wartość liczb w tablicy wejściowej	Tablica liczb	Liczba
`sum`	Suma liczb w tablicy wejściowej	Tablica liczb	Liczba
`length`	Liczba elementów w tablicy wejściowej	Tablica	Liczba
`first`	Pierwszy element tablicy	Tablica	Konstrukcja JSON (obiekt, tablica, wartość) zależnie od zawartości tablicy wejściowej

Funkcje agregujące JSONPath akceptują ujęte w cudzysłów wartości liczbowe. Wartości te są automatycznie konwertowane z ciągów znaków na typy liczbowe, gdy wymagana jest agregacja. Niezgodne dane wejściowe spowodują wygenerowanie błędu przez funkcję.

Wartość wyjściowa

Ścieżki JSONPath można podzielić na ścieżki określone i nieokreślone. Ścieżka określona może zwrócić tylko null lub jedno dopasowanie. Ścieżka nieokreślona może zwrócić wiele dopasowań: JSONPath z odłączonymi segmentami, wieloma listami nazw/indeksów, wycinkami tablic lub segmentami wyrażeń. Jednak gdy używana jest funkcja, JSONPath staje się ścieżką określoną, ponieważ funkcje zawsze zwracają pojedynczą wartość.

Ścieżka określona zwraca obiekt/tablicę/wartość, do których się odwołuje. Natomiast ścieżka nieokreślona zwraca tablicę dopasowanych obiektów/tablic/wartości.

> **Attention:**
> Kolejność właściwości w wynikach zapytania JSONPath może nie odpowiadać oryginalnej kolejności właściwości w JSON ze względu na wewnętrzne metody optymalizacji. Na przykład JSONPath `$.books[1]["author", "title"]` może zwrócić `["title", "author"]`. Jeśli zachowanie oryginalnej kolejności właściwości jest istotne, należy rozważyć alternatywne metody przetwarzania po wykonaniu zapytania.

Zasady formatowania ścieżki

Białe znaki (spacja, znak tabulacji) mogą być używane w segmentach notacji nawiasowej i wyrażeniach, na przykład: `$[ 'a' ][ 0 ][ ?( $.b == 'c' ) ][ : -1 ].first( )`.

Ciągi znaków powinny być ujmowane w pojedyncze (') lub podwójne (") cudzysłowy. Wewnątrz ciągów znaków pojedyncze lub podwójne cudzysłowy (w zależności od tego, które są używane do ich ujmowania) oraz ukośniki odwrotne (\) są poprzedzane znakiem ukośnika odwrotnego (\).

Przykład

```
{
  "books": [
    {
      "category": "reference",
      "author": "Nigel Rees",
      "title": "Powiedzenia stulecia",
      "price": 8.95,
      "id": 1
    },
    {
      "category": "fiction",
      "author": "Evelyn Waugh",
      "title": "Miecz honoru",
      "price": 12.99,
      "id": 2
    },
    {
```

```
    "category": "fiction",
    "author": "Herman Melville",
    "title": "Moby Dick",
    "isbn": "0-553-21311-3",
    "price": 8.99,
    "id": 3
  },
  {
    "category": "fiction",
    "author": "J. R. R. Tolkien",
    "title": "Władca Pierścieni",
    "isbn": "0-395-19395-8",
    "price": 22.99,
    "id": 4
  }
],
"services": {
  "delivery": {
    "servicegroup": 1000,
    "description": "Dostawa następnego dnia na terenie lokalnego miasta",
    "active": true,
    "price": 5
  },
  "bookbinding": {
    "servicegroup": 1001,
    "description": "Druk i składanie książki w formacie A5",
    "active": true,
    "price": 154.99
  },
  "restoration": {
    "servicegroup": 1002,
    "description": "Różne metody renowacji",
    "active": false,
    "methods": [
      {
        "description": "Czyszczenie chemiczne",
        "price": 46
      },
      {
        "description": "Prasowanie stron uszkodzonych przez wilgoć",
        "price": 24.5
      },
      {
        "description": "Ponowne oprawienie rozdartej książki",
        "price": 99.49
      }
    ]
  }
},
"filters": {
  "price": 10,
  "category": "fiction",
  "no filters": "brak \"filtrów\""
},
"closed message": "Sklep jest zamknięty",
"tags": [
  "a",
  "b",
  "c",
  "d",
  "e"
]
```

```
}
```

JSONPath	Type	Wynik
`$.filters.price`	definite	10
`$.filters.category`	definite	fiction
`$.filters['no filters']`	definite	brak ”filtrów”
`$.filters`	definite	{ ”price”: 10, ”category”: ”fiction”, ”no filters”: ”brak \”filtrów\”” }
`$.books[1].title`	definite	Miecz honoru
`$.books[-1].author`	definite	J. R. R. Tolkien
`$.books.length()`	definite	4
`$.tags[:]`	indefinite	[”a”, ”b”, ”c”, ”d”, ”e”]
`$.tags[2:]`	indefinite	[”c”, ”d”, ”e”]
`$.tags[:3]`	indefinite	[”a”, ”b”, ”c”]
`$.tags[1:4]`	indefinite	[”b”, ”c”, ”d”]
`$.tags[-2:]`	indefinite	[”d”, ”e”]
`$.tags[:-3]`	indefinite	[”a”, ”b”]
`$.tags[:-3].length()`	definite	2
`$.books[0, 2].title`	indefinite	[”Moby Dick”, ”Powiedzenia stulecia”]
`$.books[1]['author', "title"]`	indefinite	[”Miecz honoru”, ”Evelyn Waugh”]
`$..id`	indefinite	[1, 2, 3, 4]
`$.services..price`	indefinite	[154.99, 5, 46, 24.5, 99.49]
`$.books[?(@.id == 4 - 0.4 * 5)].title`	indefinite	[”Miecz honoru”] Uwaga: To zapytanie pokazuje, że w zapytaniach można używać operacji arytmetycznych; można je uprościć do `$.books[?(@.id == 2)].title`
`$.books[?(@.id == 2 || @.id == 4)].title`	indefinite	[”Miecz honoru”, ”Władca Pierścieni”]
`$.books[?(!(@.id == 2))].title`	indefinite	[”Powiedzenia stulecia”, ”Moby Dick”, ”Władca Pierścieni”]
`$.books[?(@.id != 2)].title`	indefinite	[”Powiedzenia stulecia”, ”Moby Dick”, ”Władca Pierścieni”]
`$.books[?(@.title =~ " of ")].title`	indefinite	[”Powiedzenia stulecia”, ”Miecz honoru”, ”Władca Pierścieni”]
`$.books[?(@.price > 12.99)].title`	indefinite	[”Władca Pierścieni”]
`$.books[?(@.author > "Herman Melville")].title`	indefinite	[”Powiedzenia stulecia”, ”Władca Pierścieni”]
`$.books[?(@.price > $.filters.price)].title`	indefinite	[”Miecz honoru”, ”Władca Pierścieni”]
`$.books[?(@.category == $.filters.category)].title`	indefinite	[”Miecz honoru”,”Moby Dick”,”Władca Pierścieni”]
`$.books[?(@.category == "fiction" && @.price < 10)].title`	indefinite	[”Moby Dick”]

JSONPath	Type	Wynik

`$..[?(@.id)]`	indefinite	[
		{
		”price”: 8.95,
		”id”: 1,
		”category”: ”reference”,
		”author”: ”Nigel Rees”,
		”title”: ”Powiedzenia stulecia”
		},
		{
		”price”: 12.99,
		”id”: 2,
		”category”: ”fiction”,
		”author”: ”Evelyn Waugh”,
		”title”: ”Miecz honoru”
		},
		{
		”price”: 8.99,
		”id”: 3,
		”category”: ”fiction”,
		”author”: ”Herman Melville”,
		”title”: ”Moby Dick”,
		”isbn”: ”0-553-21311-3”
		},
		{
		”price”: 22.99,
		”id”: 4,
		”category”: ”fiction”,
		”author”: ”J. R. R. Tolkien”,
		”title”: ”Władca Pierścieni”,
		”isbn”: ”0-395-19395-8”
		}
		]

`$.services..[?(@.price > 50)].description`	indefinite	[”Druk i składanie książki w formacie A5”, ”Ponowne oprawienie rozdartej książki”]
`$..id.length()`	definite	4
`$.books[?(@.id == 2)].title.first()`	definite	Miecz honoru
`$..tags.first().length()`	definite	5 Uwaga: `$..tags` jest ścieżką indefinite, więc zwraca tablicę dopasowanych elementów, tj. `[["a", "b", "c", "d", "e" ]]`; `first()` zwraca pierwszy element, tj. `["a", "b", "c", "d", "e"]`; `length()` oblicza długość elementu, tj. 5.
`$.books[*].price.min()`	definite	8.95
`$..price.max()`	definite	154.99
`$.books[?(@.category == "fiction")].price.avg()`	definite	14.99
`$.books[?(@.category == $.filters.xyz)].title`	indefinite	Uwaga: Zapytanie bez dopasowania zwraca NULL dla ścieżek definite i indefinite.
`$.services[?(@.active=="true")].servicegroup`	indefinite	[1001,1000] Uwaga: W porównaniach wartości logicznych należy używać stałych tekstowych.
`$.services[?(@.active=="false")].servicegroup`	indefinite	[1002] Uwaga: W porównaniach wartości logicznych należy używać stałych tekstowych.
`$.services[?(@.servicegroup=="1002")].description`	definite	test

1 Escapowanie znaków specjalnych z wartości makr LLD w JSONPath

Gdy makra wykrywania niskiego poziomu są używane we wstępnym przetwarzaniu JSONPath i ich wartości są rozwijane, stosowane są następujące reguły escapowania znaków specjalnych:

- tylko znaki backslash (\) i cudzysłów (") są brane pod uwagę przy escapowaniu;
- jeśli rozwinięta wartość makra zawiera te znaki, każdy z nich jest poprzedzany znakiem backslash;
- jeśli są już poprzedzone znakiem backslash, nie jest to traktowane jako escapowanie i zarówno backslash, jak i następujące po nim znaki specjalne są escapowane ponownie.

Na przykład:

JSONPath	Wartość makra LLD	Po podstawieniu
$.[?(@.value == "{#MACRO}")]	special "value"	$.[?(@.value == "special \"value\"")]
	c:\temp	$.[?(@.value == "c:\\temp")]
	a\\b	$.[?(@.value == "a\\\\b")]

W przypadku użycia w wyrażeniu makro, które może zawierać znaki specjalne, powinno być ujęte w cudzysłowy:

JSONPath	Wartość makra LLD	Po podstawieniu	Wynik
$.[?(@.value == "{#MACRO}")]	special "value"	$.[?(@.value == "special \"value\"")]	OK
$.[?(@.value == {#MACRO})]		$.[?(@.value == special \"value\")]	**Nieprawidłowe wyrażenie JSONPath**

W przypadku użycia w ścieżce makro, które może zawierać znaki specjalne, powinno być ujęte w nawiasy kwadratowe **oraz** cudzysłowy:

JSONPath	Wartość makra LLD	Po podstawieniu	Wynik
$.["{#MACRO}"].value	c:\temp	$.["c:\\temp"].value	OK
$.{#MACRO}.value		$.c:\\temp.value	**Nieprawidłowe wyrażenie JSONPath**

5 Wstępne przetwarzanie JavaScript

Przegląd

Ta sekcja zawiera szczegółowe informacje dotyczące preprocessingu za pomocą JavaScript.

> **Attention:**
> Nie używaj niezadeklarowanych przypisań w JavaScript używanym do preprocessingu. Użyj `var`, aby deklarować zmienne lokalne.

Wstępne przetwarzanie JavaScript

Wstępne przetwarzanie JavaScript jest wykonywane przez wywołanie funkcji JavaScript z pojedynczym parametrem „value" oraz treścią funkcji dostarczoną przez użytkownika. Wynikiem kroku wstępnego przetwarzania jest wartość zwrócona przez tę funkcję; na przykład, aby wykonać konwersję ze stopni Fahrenheita na stopnie Celsjusza, wprowadź:

```
return (value - 32)  * 5 / 9
```

w parametrach wstępnego przetwarzania JavaScript; zostanie to opakowane przez serwer w funkcję JavaScript:

```
function (value)
{
   return (value - 32) * 5 / 9
}
```

Parametr wejściowy „value" jest zawsze przekazywany jako ciąg znaków. Wartość zwracana jest automatycznie konwertowana do ciągu znaków za pomocą metody toString() (jeśli to się nie powiedzie, błąd zostanie zwrócony jako wartość tekstowa), z kilkoma wyjątkami:

- zwrócenie wartości undefined spowoduje błąd;
- zwrócenie wartości null spowoduje odrzucenie wartości wejściowej, podobnie jak wstępne przetwarzanie „Discard value” przy akcji „Custom on fail”.

Błędy mogą być zwracane przez zgłaszanie wartości/obiektów (zwykle są to ciągi znaków albo obiekty Error).

Na przykład:

```
if (value == 0)
    throw "Zero input value"
return 1/value
```

Każdy skrypt ma limit czasu wykonania wynoszący 10 sekund (w zależności od skryptu zadziałanie limitu czasu może potrwać dłużej); jego przekroczenie spowoduje zwrócenie błędu. Obowiązuje limit sterty wynoszący 512 megabajtów.

Kod bajtowy kroku wstępnego przetwarzania JavaScript jest buforowany i używany ponownie przy następnym zastosowaniu tego kroku. Wszelkie zmiany w krokach wstępnego przetwarzania pozycji spowodują zresetowanie skryptu w pamięci podręcznej i jego późniejszą ponowną kompilację.

Kolejne błędy wykonania w czasie działania (3 z rzędu) spowodują ponowną inicjalizację silnika, aby ograniczyć możliwość, że jeden skrypt uszkodzi środowisko wykonywania kolejnych skryptów (to działanie jest rejestrowane przy DebugLevel 4 i wyższym).

Wstępne przetwarzanie JavaScript jest zaimplementowane przy użyciu silnika JavaScript Duktape.

Zobacz także: Dodatkowe obiekty JavaScript i globalne funkcje

Używanie makr w skryptach

Możliwe jest używanie makr użytkownika (a także makr LLD w kontekście wykrywania niskiego poziomu) w kodzie JavaScript. Jeśli skrypt zawiera makra użytkownika, makra te są rozwiązywane przez serwer/proxy przed wykonaniem określonych kroków preprocessing. Należy pamiętać, że podczas testowania kroków preprocessing w frontend wartości makr nie będą pobierane i trzeba je wprowadzić ręcznie.

> **Note:**
> Kontekst jest ignorowany, gdy makro jest zastępowane swoją wartością. Wartość makra jest wstawiana do kodu w niezmienionej postaci; nie ma możliwości dodania dodatkowego escaping przed umieszczeniem wartości w kodzie JavaScript. Należy pamiętać, że w niektórych przypadkach może to powodować błędy JavaScript.

W poniższym przykładzie, jeśli odebrana wartość przekracza wartość makra {$THRESHOLD}, zamiast niej zostanie zwrócona wartość progu (jeśli jest obecna):

```
var threshold = '{$THRESHOLD}';
return (!isNaN(threshold) && value > threshold) ? threshold : value;
```

Przykłady

Poniższe przykłady ilustrują, jak można używać preprocessingu JavaScript.

Każdy przykład zawiera krótki opis, treść funkcji dla parametrów preprocessingu JavaScript oraz wynik kroku preprocessingu — wartość zwracaną przez funkcję.

Przykład 1: Konwersja liczby (notacja naukowa na liczbę całkowitą)

Przekonwertuj liczbę „2.62128e+07” z notacji naukowej na liczbę całkowitą.

```
return (Number(value))
```

Wartość zwrócona przez funkcję: 26212800.

Przykład 2: Konwersja liczby (z systemu binarnego na dziesiętny)

Przekonwertuj liczbę binarną „11010010” na liczbę dziesiętną.

```
return(parseInt(value,2))
```

Wartość zwrócona przez funkcję: 210.

Przykład 3: Zaokrąglanie liczby

Zaokrąglij liczbę „18.2345” do 2 cyfr.

```
return(Math.round(value* 100) / 100)
```

Wartość zwrócona przez funkcję: 18.23.

Przykład 4: Zliczanie liter w ciągu znaków

Policz liczbę liter w ciągu znaków „Zabbix”.

```
return (value.length)
```

Wartość zwrócona przez funkcję: 6.

Przykład 5: Pobierz pozostały czas

Pobierz pozostały czas (w sekundach) do daty wygaśnięcia certyfikatu (Feb 12 12:33:56 2022 GMT).

```
var split = value.split(' '),
    MONTHS_LIST = ['Jan', 'Feb', 'Mar', 'Apr', 'May', 'Jun', 'Jul', 'Aug', 'Sep', 'Oct', 'Nov', 'Dec'],
    month_index = ('0' + (MONTHS_LIST.indexOf(split[0]) + 1)).slice(-2),
    ISOdate = split[3] + '-' + month_index + '-' + split[1] + 'T' + split[2],
    now = Date.now();

return parseInt((Date.parse(ISOdate) - now) / 1000);
```

Wartość zwracana przez funkcję: 44380233.

Przykład 6: Usuń właściwości JSON

Zmodyfikuj strukturę danych JSON, usuwając wszystkie właściwości z kluczem "data_size" lub "index_size".

```
var obj=JSON.parse(value);

for (i = 0; i < Object.keys(obj).length; i++) {
    delete obj[i]["data_size"];
    delete obj[i]["index_size"];
}

return JSON.stringify(obj)
```

Wartość przyjmowana przez funkcję:

```
[
    {
        "table_name":"history",
        "data_size":"326.05",
        "index_size":"174.34"
    },
    {
        "table_name":"history_log",
        "data_size":"6.02",
        "index_size":"3.45"
    }
]
```

Wartość zwracana przez funkcję:

```
[
    {
        "table_name":"history"
    },
    {
        "table_name":"history_log"
    }
]
```

Przykład 7: Konwersja statusu Apache do formatu JSON

Przekształć wartość otrzymaną z pozycji Zabbix agent web.page.get (np. web.page.get[http://127.0.0.1:80/server-status?auto]) na obiekt JSON.

```
// Konwersja statusu Apache do formatu JSON

// Podziel wartość na podciągi i umieść te podciągi w tablicy
var lines = value.split('\n');
```

```
// Utwórz pusty obiekt "output"
var output = {};

// Utwórz obiekt "workers" ze wstępnie zdefiniowanymi właściwościami
var workers = {
    '_': 0, 'S': 0, 'R': 0, 'W': 0,
    'K': 0, 'D': 0, 'C': 0, 'L': 0,
    'G': 0, 'I': 0, '.': 0
};

// Dodaj podciągi z tablicy "lines" do obiektu "output" jako właściwości (pary klucz-wartość)
for (var i = 0; i < lines.length; i++) {
    var line = lines[i].match(/([A-z0-9 ]+): (.*)/);

    if (line !== null) {
        output[line[1]] = isNaN(line[2]) ? line[2] : Number(line[2]);
    }
}

// Metryki wielowersyjne
output.ServerUptimeSeconds = output.ServerUptimeSeconds || output.Uptime;
output.ServerVersion = output.ServerVersion || output.Server;

// Przeanalizuj właściwość "Scoreboard", aby uzyskać liczbę workerów
if (typeof output.Scoreboard === 'string') {
    for (var i = 0; i < output.Scoreboard.length; i++) {
        var char = output.Scoreboard[i];

        workers[char]++;
    }
}

// Dodaj dane workerów do obiektu "output"
output.Workers = {
    waiting: workers['_'], starting: workers['S'], reading: workers['R'],
    sending: workers['W'], keepalive: workers['K'], dnslookup: workers['D'],
    closing: workers['C'], logging: workers['L'], finishing: workers['G'],
    cleanup: workers['I'], slot: workers['.']
};

// Zwróć ciąg JSON
return JSON.stringify(output);
```

Wartość akceptowana przez funkcję:

```
HTTP/1.1 200 OK
Date: Mon, 27 Mar 2023 11:08:39 GMT
Server: Apache/2.4.52 (Ubuntu)
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 405
Content-Type: text/plain; charset=ISO-8859-1

127.0.0.1
ServerVersion: Apache/2.4.52 (Ubuntu)
ServerMPM: prefork
Server Built: 2023-03-08T17:32:01
CurrentTime: Monday, 27-Mar-2023 14:08:39 EEST
RestartTime: Monday, 27-Mar-2023 12:19:59 EEST
ParentServerConfigGeneration: 1
ParentServerMPMGeneration: 0
ServerUptimeSeconds: 6520
ServerUptime: 1 hour 48 minutes 40 seconds
```

```
Load1: 0.56
Load5: 0.33
Load15: 0.28
Total Accesses: 2476
Total kBytes: 8370
Total Duration: 52718
CPUUser: 8.16
CPUSystem: 3.44
CPUChildrenUser: 0
CPUChildrenSystem: 0
CPULoad: .177914
Uptime: 6520
ReqPerSec: .379755
BytesPerSec: 3461.58
BytesPerReq: 3461.58
DurationPerReq: 21.2916
BusyWorkers: 2
IdleWorkers: 6
Scoreboard: ____KW__.....................................................................................
```

Wartość zwracana przez funkcję:


```
{
    "Date": "Mon, 27 Mar 2023 11:08:39 GMT",
    "Server": "Apache/2.4.52 (Ubuntu)",
    "Vary": "Accept-Encoding",
    "Encoding": "gzip",
    "Length": 405,
    "Type": "text/plain; charset=ISO-8859-1",
    "ServerVersion": "Apache/2.4.52 (Ubuntu)",
    "ServerMPM": "prefork",
    "Server Built": "2023-03-08T17:32:01",
    "CurrentTime": "Monday, 27-Mar-2023 14:08:39 EEST",
    "RestartTime": "Monday, 27-Mar-2023 12:19:59 EEST",
    "ParentServerConfigGeneration": 1,
    "ParentServerMPMGeneration": 0,
    "ServerUptimeSeconds": 6520,
    "ServerUptime": "1 hour 48 minutes 40 seconds",
    "Load1": 0.56,
    "Load5": 0.33,
    "Load15": 0.28,
    "Total Accesses": 2476,
    "Total kBytes": 8370,
    "Total Duration": 52718,
    "CPUUser": 8.16,
    "CPUSystem": 3.44,
    "CPUChildrenUser": 0,
    "CPUChildrenSystem": 0,
    "CPULoad": 0.177914,
    "Uptime": 6520,
    "ReqPerSec": 0.379755,
    "BytesPerSec": 1314.55,
    "BytesPerReq": 3461.58,
    "DurationPerReq": 21.2916,
    "BusyWorkers": 2,
    "IdleWorkers": 6,
    "Scoreboard": "____KW__.....................................................................................
    "Workers": {
        "waiting": 6,
        "starting": 0,
        "reading": 0,
        "sending": 1,
        "keepalive": 1,
```

```
        "dnslookup": 0,
        "closing": 0,
        "logging": 0,
        "finishing": 0,
        "cleanup": 0,
        "slot": 142
    }
}
```

1 Dodatkowe obiekty JavaScript

Przegląd

Ta sekcja opisuje dodatki Zabbix do języka JavaScript zaimplementowanego przy użyciu Duktape oraz obsługiwane globalne funkcje JavaScript.

Attention:
Nie używaj niezadeklarowanych przypisań w skryptach JavaScript przetwarzania wstępnego. Używaj `var` do deklarowania zmiennych lokalnych.

Wbudowane obiekty

Zabbix

Obiekt Zabbix umożliwia interakcję z wewnętrzną funkcjonalnością Zabbix.

Method	Description
`log(loglevel, message)`	Zapisuje <message> do logu Zabbix z użyciem poziomu logowania <loglevel> (zobacz parametr DebugLevel w pliku konfiguracyjnym).

Przykład:

```
Zabbix.log(3, "this is a log entry written with 'Warning' log level")
```

Możesz używać następujących aliasów:

Alias	Alias to
console.log(object)	Zabbix.log(4, JSON.stringify(object))
console.warn(object)	Zabbix.log(3, JSON.stringify(object))
console.error(object)	Zabbix.log(2, JSON.stringify(object))

Attention:
Łączny rozmiar wszystkich rejestrowanych komunikatów jest ograniczony do 8 MB na jedno wykonanie skryptu.

Method	Description
`sleep(delay)`	Opóźnia wykonanie JavaScript o `delay` milisekund.

Przykład (opóźnienie wykonania o 15 sekund):

```
Zabbix.sleep(15000)
```

HttpRequest

Ten obiekt hermetyzuje uchwyt cURL, umożliwiając wykonywanie prostych żądań HTTP. Błędy są zgłaszane jako wyjątki.

Attention:
Inicjalizacja wielu obiektów `HttpRequest` jest ograniczona do 10 na jedno wykonanie skryptu.

Method	Description
`addHeader(value)`	Dodaje pole nagłówka HTTP. To pole jest używane dla wszystkich kolejnych żądań, dopóki nie zostanie wyczyszczone metodą `clearHeader()`. Łączna długość pól nagłówka, które można dodać do pojedynczego obiektu `HttpRequest`, jest ograniczona do 128 KB (łącznie ze znakami specjalnymi i nazwami nagłówków).
`clearHeader()`	Czyści nagłówek HTTP. Jeśli nie ustawiono żadnych pól nagłówka, `HttpRequest` ustawi Content-Type na application/json, jeśli wysyłane dane są w formacie JSON; w przeciwnym razie text/plain.
`connect(url)`	Wysyła żądanie HTTP CONNECT do URL i zwraca odpowiedź.
`customRequest(method, url, data)`	Umożliwia określenie dowolnej metody HTTP w pierwszym parametrze. Wysyła żądanie wskazaną metodą do URL z opcjonalnym ładunkiem *data* i zwraca odpowiedź.
`delete(url, data)`	Wysyła żądanie HTTP DELETE do URL z opcjonalnym ładunkiem *data* i zwraca odpowiedź.
`getHeaders(<asArray>)`	Zwraca obiekt odebranych pól nagłówka HTTP. Parametr `asArray` może być ustawiony na "true" (np. `getHeaders(true)`), "false" lub może być niezdefiniowany. Jeśli jest ustawiony na "true", wartości odebranych pól nagłówka HTTP zostaną zwrócone jako tablice; należy tego używać do pobierania wartości pól wielu nagłówków o tej samej nazwie. Jeśli parametr nie jest ustawiony lub jest ustawiony na "false", wartości odebranych pól nagłówka HTTP zostaną zwrócone jako ciągi znaków.
`get(url, data)`	Wysyła żądanie HTTP GET do URL z opcjonalnym ładunkiem *data* i zwraca odpowiedź.
`head(url)`	Wysyła żądanie HTTP HEAD do URL i zwraca odpowiedź.
`options(url)`	Wysyła żądanie HTTP OPTIONS do URL i zwraca odpowiedź.
`patch(url, data)`	Wysyła żądanie HTTP PATCH do URL z opcjonalnym ładunkiem *data* i zwraca odpowiedź.
`put(url, data)`	Wysyła żądanie HTTP PUT do URL z opcjonalnym ładunkiem *data* i zwraca odpowiedź.
`post(url, data)`	Wysyła żądanie HTTP POST do URL z opcjonalnym ładunkiem *data* i zwraca odpowiedź.
`getStatus()`	Zwraca kod statusu ostatniego żądania HTTP.
`setProxy(proxy)`	Ustawia HTTP proxy na wartość "proxy". Jeśli ten parametr jest pusty, proxy nie jest używany.

`setHttpAuth(bitmask, username, password)`	Ustawia włączone metody uwierzytelniania HTTP (HTTPAUTH_BASIC, HTTPAUTH_DIGEST, HTTPAUTH_NEGOTIATE, HTTPAUTH_NTLM, HTTPAUTH_NONE) w parametrze 'bitmask'.
	Flaga HTTPAUTH_NONE umożliwia wyłączenie uwierzytelniania HTTP.
	Przykłady:
	`request.setHttpAuth(HTTPAUTH_NTLM | HTTPAUTH_BASIC, username, password)`
	`request.setHttpAuth(HTTPAUTH_NONE)`

`trace(url, data)`	Wysyła żądanie HTTP TRACE do URL z opcjonalnym ładunkiem *data* i zwraca odpowiedź.

Przykład:

```
try {
    Zabbix.log(4, 'jira webhook script value='+value);

    var result = {
        'tags': {
            'endpoint': 'jira'
        }
    },
    params = JSON.parse(value),
    req = new HttpRequest(),
    fields = {},
    resp;

    req.addHeader('Content-Type: application/json');
    req.addHeader('Authorization: Basic '+params.authentication);

    fields.summary = params.summary;
    fields.description = params.description;
    fields.project = {"key": params.project_key};
    fields.issuetype = {"id": params.issue_id};
    resp = req.post('https://jira.example.com/rest/api/2/issue/',
        JSON.stringify({"fields": fields})
    );

    if (req.getStatus() != 201) {
```

```
        throw 'Response code: '+req.getStatus();
    }

    resp = JSON.parse(resp);
    result.tags.issue_id = resp.id;
    result.tags.issue_key = resp.key;
} catch (error) {
    Zabbix.log(4, 'jira issue creation failed json : '+JSON.stringify({"fields": fields}));
    Zabbix.log(4, 'jira issue creation failed : '+error);

    result = {};
}

return JSON.stringify(result);
```

XML

Obiekt XML umożliwia przetwarzanie danych XML we wstępnym przetwarzaniu pozycji i wykrywaniu niskopoziomowym oraz w webhookach.

> **Attention:**
> Aby używać obiektu XML, serwer/proxy musi być skompilowany z obsługą libxml2.

Method	Description
`XML.query(data, expression)`	Pobiera zawartość węzła przy użyciu XPath. Zwraca null, jeśli węzeł nie zostanie znaleziony. **expression** - wyrażenie XPath; **data** - dane XML jako ciąg znaków.
`XML.toJson(data)`	Konwertuje dane w formacie XML do JSON.
`XML.fromJson(object)`	Konwertuje dane w formacie JSON do XML.

Przykład:

Wejście:

```
<menu>
    <food type = "breakfast">
        <name>Chocolate</name>
        <price>$5.95</price>
        <description></description>
        <calories>650</calories>
    </food>
</menu>
```

Wyjście:

```
{
    "menu": {
        "food": {
            "@type": "breakfast",
            "name": "Chocolate",
            "price": "$5.95",
            "description": null,
            "calories": "650"
        }
    }
}
```

Zasady serializacji

Konwersja XML do JSON będzie przetwarzana zgodnie z następującymi zasadami (w przypadku konwersji JSON do XML stosowane są zasady odwrotne):

1. Atrybuty XML zostaną przekonwertowane na klucze, których nazwy są poprzedzone znakiem '@'.

Przykład:

Wejście:

```
<xml foo="FOO">
  <bar>
    <baz>BAZ</baz>
  </bar>
</xml>
```

Wyjście:

```
{
  "xml": {
    "@foo": "FOO",
    "bar": {
      "baz": "BAZ"
    }
  }
}
```

2. Elementy samozamykające się (<foo/>) zostaną przekonwertowane tak, jakby miały wartość 'null'.

Przykład:

Wejście:

```
<xml>
  <foo/>
</xml>
```

Wyjście:

```
{
  "xml": {
    "foo": null
  }
}
```

3. Puste atrybuty (o wartości "") zostaną przekonwertowane tak, jakby miały wartość pustego ciągu znaków (").

Przykład:

Wejście:

```
<xml>
  <foo bar="" />
</xml>
```

Wyjście:

```
{
  "xml": {
    "foo": {
      "@bar": ""
    }
  }
}
```

4. Wiele węzłów podrzędnych o tej samej nazwie elementu zostanie przekonwertowanych na pojedynczy klucz, którego wartością będzie tablica wartości.

Przykład:

Wejście:

```
<xml>
  <foo>BAR</foo>
  <foo>BAZ</foo>
  <foo>QUX</foo>
</xml>
```

Wyjście:

```
{
  "xml": {
    "foo": ["BAR", "BAZ", "QUX"]
  }
}
```

5. Jeśli element tekstowy nie ma atrybutów ani elementów podrzędnych, zostanie przekonwertowany jako ciąg znaków.

Przykład:

Wejście:

```
<xml>
    <foo>BAZ</foo>
</xml>
```

Wyjście:

```
{
  "xml": {
    "foo": "BAZ"
   }
}
```

6. Jeśli element tekstowy nie ma elementów podrzędnych, ale ma atrybuty, zawartość tekstowa zostanie przekonwertowana na element z kluczem '#text', a zawartość będzie jego wartością; atrybuty zostaną przekonwertowane zgodnie z zasadą serializacji 1.

Przykład:

Wejście:

```
<xml>
  <foo bar="BAR">
    BAZ
  </foo>
</xml>
```

Wyjście:

```
{
  "xml": {
    "foo": {
      "@bar": "BAR",
      "#text": "BAZ"
    }
  }
}
```

Globalne funkcje JavaScript

Dodatkowe globalne funkcje JavaScript zostały zaimplementowane przy użyciu Duktape:

- `btoa(data)` - koduje dane do ciągu base64.
- `atob(base64_string)` - dekoduje ciąg base64 jako bufor Uint8Array.

```
try {
    b64 = btoa("test string");
    buffer = atob(b64);

    // Należy pamiętać, że logika dekodowania zależy od formatu danych w buforze.
    decoded = String.fromCharCode.apply(this, [].slice.call(buffer));
}
catch (error) {
    return {'error.name' : error.name, 'error.message' : error.message};
}
```

- `md5(data)` - oblicza skrót MD5 danych.
- `sha256(data)` - oblicza skrót SHA256 danych.

- `hmac('<hash type>',key,data)` - zwraca skrót HMAC jako ciąg w formacie szesnastkowym; jako `hash type` obsługiwane są `md5` i `sha256`; parametry `key` i `data` obsługują dane binarne.

  Przykłady:

  - `hmac('md5',key,data)`
  - `hmac('sha256',key,data)`

- `sign(hash,key,data)` - zwraca obliczony podpis (podpis RSA z SHA-256) jako ciąg, gdzie:
 hash - dozwolone jest tylko `sha256`, w przeciwnym razie zostanie zgłoszony błąd.
 key - klucz prywatny. Powinien być zgodny ze standardem PKCS#1 lub PKCS#8. Klucz może być podany w różnych formach:

  - ze spacjami zamiast znaków nowej linii
  - z poprzedzonymi znakiem ucieczki lub niepoprzedzonymi znakiem ucieczki `\n` zamiast znaków nowej linii
  - bez żadnych znaków nowej linii, jako ciąg jednoliniowy
  - jako ciąg w formacie JSON

  Klucz może być również wczytany z makra użytkownika/tajnego makra/sejfu.

  data - dane, które zostaną podpisane. Mogą to być ciąg znaków (obsługiwane są również dane binarne) lub bufor (Uint8Array/ArrayBuffer).

  Przykład:

  - `sign('sha256',key,data)`

  Do obliczania podpisów używany jest OpenSSL lub GnuTLS. Jeśli Zabbix został zbudowany bez którejkolwiek z tych bibliotek szyfrowania, zostanie zgłoszony błąd ('missing OpenSSL or GnuTLS library').

2 Obiekty JavaScript pozycji przeglądarki

Przegląd

Ta sekcja opisuje rozszerzenia języka JavaScript w Zabbix zaimplementowane przy użyciu Duktape do użycia w skrypcie pozycji Browser. Rozszerzenia te uzupełniają obiekty JavaScript opisane na stronie Dodatkowe obiekty JavaScript.

Browser

Obiekt `Browser` zarządza sesjami WebDriver, inicjalizując sesję podczas tworzenia i kończąc ją podczas niszczenia obiektu. Pojedynczy skrypt może obsługiwać maksymalnie cztery obiekty `Browser`.

Aby utworzyć obiekt `Browser`, użyj składni `new Browser(options)`. Parametr `options` (*obiekt JSON*) określa opcje przeglądarki, zwykle wynik metody opcji WebDriver (na przykład `Browser.chromeOptions()`).

Obiekt `Browser` obsługuje następujące metody.

Method	Description
`navigate(url)`	Przejdź do określonego adresu URL. Parametry: `url` - (string) Adres URL, do którego należy przejść.
`getUrl()`	Zwraca ciąg znaków z adresem URL otwartej strony.
`getPageSource()`	Zwraca ciąg znaków z kodem źródłowym otwartej strony.
`findElement(strategy, selector)`	Zwraca obiekt `Element` z jednym elementem na otwartej stronie (lub zwraca `null`, jeśli żadne elementy nie pasują do `strategy` i `selector`). Parametry: `strategy` - (string, css selector/link text/partial link text/tag name/xpath) Strategia lokalizacji; `selector` - (string) Selektor elementu używający określonej strategii lokalizacji.
`findElements(strategy, target)`	Zwraca tablicę obiektów `Element` z wieloma elementami na otwartej stronie (lub zwraca pustą tablicę, jeśli żadne elementy nie pasują do strategii lokalizacji i celu). Parametry: `strategy` - (string, css selector/link text/partial link text/tag name/xpath) Strategia lokalizacji; `target` - (string) Selektor elementu używający określonej strategii lokalizacji.
`getCookies()`	Zwraca tablicę obiektów `Cookie`.

Method	Description
`addCookie(cookie)`	Ustawia pliki cookie. Parametry: `cookie` - (`Cookie` object) Plik cookie do ustawienia.
`getScreenshot()`	Zwraca ciąg znaków zakodowany w base64, reprezentujący obraz obszaru widoku przeglądarki.
`setScreenSize(x,y)`	Ustawia rozmiar obszaru widoku przeglądarki. Parametry: `x` - (string) Szerokość w pikselach; `y` - (string) Wysokość w pikselach.
`setScriptTimeout(timeout)`	Ustawia limit czasu ładowania skryptu. Parametry: `timeout` - (integer) Wartość limitu czasu w milisekundach.
`setSessionTimeout(timeout)`	Ustawia limit czasu sesji (ładowania strony). Parametry: `timeout` - (integer) Wartość limitu czasu w milisekundach.
`setElementWaitTimeout(timeout)`	Ustawia limit czasu strategii lokalizacji elementu (implicit). Parametry: `timeout` - (integer) Wartość limitu czasu w milisekundach.
`collectPerfEntries(mark)`	Zbiera wpisy wydajności do pobrania metodą `getResult()`. Parametry: `mark` - (string, optional) Znacznik migawki wydajności.
`getRawPerfEntries()`	Zwraca tablicę obiektów wpisów wydajności.
`getResult()`	Zwraca obiekt `Result` ze statystykami sesji przeglądarki (informacje o błędach, migawki wydajności itp.).
`getError()`	Zwraca obiekt `BrowserError` z błędami przeglądarki (lub zwraca `null`, jeśli nie ma błędów przeglądarki).
`setError(message)`	Ustawia niestandardowy komunikat błędu, który ma zostać uwzględniony w obiekcie `Result`. Parametry: `message` - (string) Komunikat błędu.
`discardError()`	Odrzuca błąd, który ma zostać zwrócony w obiekcie `Result`.
`getAlert()`	Zwraca obiekt `Alert` z alertami przeglądarki (lub zwraca `null`, jeśli nie ma alertów przeglądarki).
`chromeOptions()`	Zwraca obiekt `chromeOptions` ze wstępnie zdefiniowanymi opcjami przeglądarki Chrome.
`firefoxOptions()`	Zwraca obiekt `firefoxOptions` ze wstępnie zdefiniowanymi opcjami przeglądarki Firefox.
`safariOptions()`	Zwraca obiekt `safariOptions` ze wstępnie zdefiniowanymi opcjami przeglądarki Safari.
`edgeOptions()`	Zwraca obiekt `edgeOptions` ze wstępnie zdefiniowanymi opcjami przeglądarki Edge.
`switchFrame(target)`	Przełącza do określonej ramki. Parametry: `target` - (browser element or integer, optional) Ramka docelowa. Aby wybrać ramkę według elementu, przekaż element. Aby wybrać ramkę według indeksu, przekaż liczbę. Jeśli pozostawiono puste, nastąpi przełączenie do kontekstu przeglądania najwyższego poziomu.

Wszystkie metody Browser mogą zgłaszać następujące błędy:

- `BrowserError` - dziedziczony z obiektu `Error`, zgłaszany, jeśli konstruktor `Browser` zakończy się niepowodzeniem; zawiera dodatkową właściwość `browser` z obiektem `Browser`, który zgłosił ten `BrowserError`.
- `WebdriverError` - dziedziczony z `BrowserError`; zawiera te same właściwości co obiekt `BrowserError`, które wskazują, czy błąd został wygenerowany w odpowiedzi na błąd w odpowiedzi WebDriver.

Element

Obiekt `Element` jest zwracany przez metody `findElement()`/`findElements()` obiektu `Browser` i nie może być tworzony bezpośrednio.

Obiekt `Element` reprezentuje element na stronie internetowej i udostępnia metody do interakcji z nim.

Poniższe metody są obsługiwane przez obiekt `Element`.

Method	Description
`getAttribute(name)`	Zwraca ciąg wartości atrybutu elementu (lub zwraca `null`, jeśli określony atrybut nie został znaleziony). Parametry: `name` - (string) Nazwa atrybutu.
`getProperty(name)`	Zwraca ciąg wartości właściwości elementu (lub zwraca `null`, jeśli określona właściwość nie została znaleziona). Parametry: `name` - (string) Nazwa właściwości.
`getText()`	Zwraca ciąg wartości tekstowej tekstu elementu.
`click()`	Kliknij element.
`clear()`	Wyczyść zawartość edytowalnego elementu.
`sendKeys(keys)`	Wysyła klawisze. Parametry: `keys` - (string) Klawisze do wysłania.

Cookie

Obiekt `Cookie` jest zwracany przez metodę `getCookies()` obiektu `Browser` i przekazywany do metody `addCookie()`.

Chociaż obiekt `Cookie` nie ma żadnych metod, może zawierać następujące właściwości:

Właściwość	Typ	Opis
name	string	Nazwa pliku cookie.
value	string	Wartość pliku cookie.
path	string	Ścieżka, dla której plik cookie jest prawidłowy. Domyślnie `"/"`, jeśli zostanie pominięta podczas dodawania pliku cookie.
domain	string	Domena, dla której plik cookie jest widoczny. Domyślnie domena URL aktywnego dokumentu bieżącego kontekstu przeglądania sesji, jeśli zostanie pominięta podczas dodawania pliku cookie.
secure	boolean	Wskazuje, czy plik cookie jest bezpieczny. Domyślnie `false`, jeśli zostanie pominięte podczas dodawania pliku cookie.
httpOnly	boolean	Wskazuje, czy plik cookie jest dostępny tylko przez HTTP. Domyślnie `false`, jeśli zostanie pominięte podczas dodawania pliku cookie.
expiry	integer	Czas wygaśnięcia pliku cookie (w sekundach od epoki Unix). Nie może być ustawiony, jeśli zostanie pominięty podczas dodawania pliku cookie.
sameSite	string	Atrybut `sameSite` pliku cookie, który określa, czy plik cookie powinien być ograniczony do kontekstu first-party lub same-site. Może być ustawiony na `"Lax"` lub `"Strict"`. Domyślnie `"None"`, jeśli zostanie pominięty podczas dodawania pliku cookie.

Alert

Obiekt `Alert` reprezentuje alert strony internetowej, jest zwracany przez metodę `getAlert()` obiektu `Browser` i nie może być tworzony bezpośrednio.

Obiekt `Alert` zawiera właściwość `text` z tekstem alertu (lub `null`, jeśli nie ma alertów).

Następujące metody są obsługiwane przez obiekt `Alert`.

Method	Description
`accept()`	Akceptuje alert.
`dismiss()`	Odrzuca alert.

Wynik

Obiekt `Result` zawiera statystyki sesji i jest zwracany przez metodę `getResult()` obiektu `Browser`.

Zazwyczaj obiekt `Result` jest konwertowany do postaci ciągu znaków i zwracany ze skryptu, a następnie przetwarzany na wartości zależnych pozycji za pomocą preprocessing.

Chociaż obiekt `Result` nie ma żadnych metod, może zawierać następujące właściwości.

Właściwość	Typ	Opis
duration	string	Czas trwania sesji od utworzenia sesji do pobrania wyniku.
error	object	Informacje o błędzie.
http_status	integer	Status HTTP zwrócony przez WebDriver (lub 0, jeśli nie ma błędów WebDriver).
error_code	string	Błąd zwrócony przez WebDriver (lub pusty ciąg znaków, jeśli nie ma błędów WebDriver).
message	string	Komunikat błędu WebDriver (lub pusty ciąg znaków, jeśli nie ma błędów WebDriver).
performance_data	object	Statystyki wydajności.
summary	object	Podsumowanie wydajności.
navigation	object	Podsumowanie nawigacji.
resource	object	Podsumowanie zasobów.
details	array of objects	Statystyki wydajności po każdej operacji, która mogła skutkować nawigacją.
mark	string	*(opcjonalnie)* Oznaczenie migawki wydajności określone za pomocą metody `collectPerfEntries()`.
navigation	object	Statystyki nawigacji.
resource	object	Podsumowanie zasobów dla tego kroku.
user	array of objects	Tablica statystyk typu mark/measure.
marks	array of objects	Indeksy oznaczonych migawek wydajności.
name	string	Nazwa oznaczenia migawki wydajności.
index	integer	Indeks migawki wydajności w tablicy details.

6 Przetwarzanie wstępne CSV do JSON

Przegląd

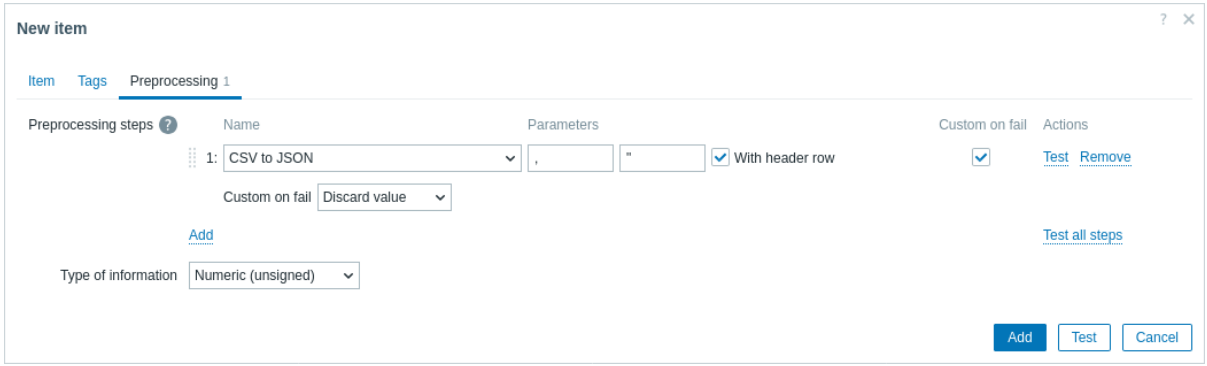
W tym kroku przetwarzania wstępnego można przekonwertować dane pliku CSV do formatu JSON. Jest to obsługiwane w:

- pozycjach (prototypach pozycji)
- regułach wykrywania niskiego poziomu

Configuration

To configure a CSV to JSON preprocessing step:

- Go to the Preprocessing tab in item/discovery rule configuration
- Click on *Add*
- Select the *CSV to JSON* option



The first parameter allows to set a custom delimiter. Note that if the first line of CSV input starts with "Sep=" and is followed by a single UTF-8 character then that character will be used as the delimiter in case the first parameter is not set. If the first parameter is not set and a delimiter is not retrieved from the "Sep=" line, then a comma is used as a separator.

The second optional parameter allows to set a quotation symbol.

If the *With header row* checkbox is marked, the header line values will be interpreted as column names (see Header processing for more information).

If the *Custom on fail* checkbox is marked, the item will not become unsupported in case of a failed preprocessing step. Additionally custom error handling options may be set: discard the value, set a specified value or set a specified error message.

Header processing

The CSV file header line can be processed in two different ways:

- If the *With header row* checkbox is marked - header line values are interpreted as column names. In this case the column names must be unique and the data row should not contain more columns than the header row;
- If the *With header row* checkbox is not marked - the header line is interpreted as data. Column names are generated automatically (1,2,3,4...)

CSV file example:

```
Nr,Item name,Key,Qty
1,active agent item,agent.hostname,33
"2","passive agent item","agent.version","44"
3,"active,passive agent items",agent.ping,55
```

Note:
A quotation character within a quoted field in the input must be escaped by preceding it with another quotation character.

Processing header line

JSON output when a header line is expected:

```
[
   {
      "Nr":"1",
      "Item name":"active agent item",
      "Key":"agent.hostname",
      "Qty":"33"
   },
   {
      "Nr":"2",
      "Item name":"passive agent item",
      "Key":"agent.version",
      "Qty":"44"
   },
   {
      "Nr":"3",
      "Item name":"active,passive agent items",
      "Key":"agent.ping",
      "Qty":"55"
   }
]
```

No header line processing

JSON output when a header line is not expected:

```
[
   {
      "1":"Nr",
      "2":"Item name",
      "3":"Key"
      "4":"Qty"
   },
   {
      "1":"1",
      "2":"active agent item",
      "3":"agent.hostname"
      "4":"33"
   },
   {
      "1":"2",
      "2":"passive agent item",
      "3":"agent.version"
      "4":"44"
   },
   {
      "1":"3",
      "2":"active,passive agent items",
      "3":"agent.ping"
      "4":"55"
   }
]
```

3 Typy pozycji

Przegląd

Typy pozycji obejmują różne metody pozyskiwania danych z systemu. Każdy typ pozycji ma własny zestaw obsługiwanych kluczy pozycji oraz wymaganych parametrów.

Zabbix oferuje obecnie następujące typy pozycji:

- Kontrole agenta Zabbix
- Kontrole agenta SNMP
- Pułapki SNMP
- Kontrole IPMI
- Kontrole proste
  - Monitorowanie VMware
- Monitorowanie plików dziennika
- Pozycje obliczane
  - Obliczenia agregujące
- Wewnętrzne kontrole Zabbix
- Kontrole SSH
- Kontrole Telnet
- Kontrole zewnętrzne
- Pozycje trappera
- Monitorowanie JMX
- Kontrole ODBC
- Pozycje zależne
- Kontrole HTTP
- Kontrole Prometheus
- Pozycje skryptowe
- Pozycje przeglądarkowe

Szczegóły dotyczące wszystkich typów pozycji znajdują się na podstronach tej sekcji. Mimo że typy pozycji oferują wiele możliwości zbierania danych, dostępne są także dodatkowe opcje poprzez parametry użytkownika lub moduły ładowalne.

Niektóre kontrole są wykonywane wyłącznie przez serwer Zabbix (jako monitorowanie bez agenta), podczas gdy inne wymagają agenta Zabbix lub nawet Zabbix Java gateway (w przypadku monitorowania JMX).

Attention:
Jeśli określony typ pozycji wymaga określonego interfejsu (na przykład kontrola IPMI wymaga interfejsu IPMI na hoście), ten interfejs musi istnieć w definicji hosta.

W definicji hosta można ustawić wiele interfejsów: agent Zabbix, agent SNMP, JMX i IPMI. Jeśli pozycja może używać więcej niż jednego interfejsu, wyszuka ona dostępne interfejsy hosta (w kolejności: Agent→SNMP→JMX→IPMI), aby powiązać się z pierwszym odpowiednim.

Wszystkie pozycje, które zwracają tekst (typy informacji: znakowy, log, tekst), mogą również zwracać wyłącznie białe znaki (tam, gdzie ma to zastosowanie), ustawiając wartość zwracaną na pusty ciąg znaków (obsługiwane od wersji 2.0).

1 Agent Zabbix

Przegląd

Ta sekcja zawiera szczegółowe informacje o kluczach pozycji, które wykorzystują komunikację z agent do zbierania danych.

Istnieją pasywne i aktywne kontrole agent. Podczas konfigurowania pozycji można wybrać wymagany typ:

- *Zabbix agent* — dla kontroli pasywnych
- *Zabbix agent (active)* — dla kontroli aktywnych

Należy pamiętać, że wszystkie klucze pozycji obsługiwane przez Zabbix agent są również obsługiwane przez nowej generacji Zabbix agent 2. Zobacz dodatkowe klucze pozycji, których można używać wyłącznie z agent 2.

Obsługiwane klucze pozycji

Klucze pozycji, których można używać z Zabbix agent, są wymienione poniżej.

Klucze pozycji są podane bez parametrów i dodatkowych informacji. Kliknij klucz pozycji, aby zobaczyć pełne szczegóły.

Klucz pozycji	Opis	Grupa pozycji
kernel.maxfiles	Maksymalna liczba otwartych plików obsługiwana przez system operacyjny.	Jądro
kernel.maxproc	Maksymalna liczba procesów obsługiwana przez system operacyjny.	
kernel.openfiles	Liczba aktualnie otwartych deskryptorów plików.	
log	Monitorowanie pliku dziennika.	Monitorowanie logów
log.count	Liczba dopasowanych wierszy w monitorowanym pliku dziennika.	
logrt	Monitorowanie rotowanego pliku dziennika.	
logrt.count	Liczba dopasowanych wierszy w monitorowanym, rotowanym pliku dziennika.	
modbus.get	Odczytuje dane Modbus.	Modbus
net.dns	Sprawdza stan usługi DNS.	Sieć
net.dns.perf	Sprawdza wydajność usługi DNS.	
net.dns.record	Wykonuje zapytanie DNS.	
net.if.collisions	Liczba kolizji out-of-window.	
net.if.discovery	Lista interfejsów sieciowych.	
net.if.in	Statystyki ruchu przychodzącego na interfejsie sieciowym.	
net.if.out	Statystyki ruchu wychodzącego na interfejsie sieciowym.	
net.if.total	Suma statystyk ruchu przychodzącego i wychodzącego na interfejsie sieciowym.	
net.tcp.listen	Sprawdza, czy ten port TCP jest w stanie LISTEN.	
net.tcp.port	Sprawdza, czy możliwe jest nawiązanie połączenia TCP z określonym portem.	
net.tcp.service	Sprawdza, czy usługa działa i akceptuje połączenia TCP.	
net.tcp.service.perf	Sprawdza wydajność usługi TCP.	
net.tcp.socket.count	Zwraca liczbę gniazd TCP pasujących do parametrów.	
net.udp.listen	Sprawdza, czy ten port UDP jest w stanie LISTEN.	
net.udp.service	Sprawdza, czy usługa działa i odpowiada na żądania UDP.	
net.udp.service.perf	Sprawdza wydajność usługi UDP.	
net.udp.socket.count	Zwraca liczbę gniazd UDP pasujących do parametrów.	
proc.cpu.util	Procent wykorzystania CPU przez proces.	Procesy
proc.get	Lista procesów systemu operacyjnego i ich parametrów.	
proc.mem	Pamięć używana przez proces w bajtach.	
proc.num	Liczba procesów.	

Klucz pozycji	Opis	Grupa pozycji
sensor	Odczyt czujnika sprzętowego.	Czujniki
system.boottime	Czas uruchomienia systemu.	System
system.cpu.discovery	Lista wykrytych CPU/rdzeni CPU.	
system.cpu.intr	Przerwania urządzeń.	
system.cpu.load	Obciążenie CPU.	
system.cpu.num	Liczba CPU.	
system.cpu.switches	Liczba przełączeń kontekstu.	
system.cpu.util	Procent wykorzystania CPU.	
system.hostname	Nazwa hosta systemu.	
system.hw.chassis	Informacje o obudowie.	
system.hw.cpu	Informacje o CPU.	
system.hw.devices	Lista urządzeń PCI lub USB.	
system.hw.macaddr	Lista adresów MAC.	
system.localtime	Czas systemowy.	
system.run	Uruchamia określone polecenie na hoście.	
system.stat	Statystyki systemowe.	
system.sw.arch	Informacje o architekturze oprogramowania.	
system.sw.os	Informacje o systemie operacyjnym.	
system.sw.os.get	Szczegółowe informacje o systemie operacyjnym (wersja, typ, nazwa dystrybucji, wersja główna i pomocnicza itd.).	
system.sw.packages	Lista zainstalowanych pakietów.	
system.sw.packages.get	Szczegółowa lista zainstalowanych pakietów.	
system.swap.in	Statystyki swap-in (z urządzenia do pamięci).	
system.swap.out	Statystyki swap-out (z pamięci na urządzenie).	
system.swap.size	Rozmiar przestrzeni wymiany w bajtach lub jako procent całości.	
system.uname	Identyfikacja systemu.	
system.uptime	Czas działania systemu w sekundach.	
system.users.num	Liczba zalogowanych użytkowników.	
vfs.dev.discovery	Lista urządzeń blokowych i ich typów.	Systemy plików wirtualnych
vfs.dev.read	Statystyki odczytu dysku.	
vfs.dev.write	Statystyki zapisu dysku.	
vfs.dir.count	Liczba wpisów w katalogu.	
vfs.dir.get	Lista wpisów w katalogu.	
vfs.dir.size	Rozmiar katalogu.	
vfs.file.cksum	Suma kontrolna pliku obliczona algorytmem UNIX cksum.	
vfs.file.contents	Pobieranie zawartości pliku.	
vfs.file.exists	Sprawdza, czy plik istnieje.	
vfs.file.get	Zwraca informacje o pliku.	
vfs.file.md5sum	Suma kontrolna MD5 pliku.	
vfs.file.owner	Pobiera właściciela pliku.	
vfs.file.permissions	Zwraca 4-cyfrowy ciąg zawierający liczbę ósemkową z uprawnieniami UNIX.	
vfs.file.regexp	Pobiera ciąg znaków z pliku.	
vfs.file.regmatch	Znajduje ciąg znaków w pliku.	
vfs.file.size	Rozmiar pliku.	
vfs.file.time	Informacje o czasie pliku.	
vfs.fs.discovery	Lista zamontowanych systemów plików wraz z ich typem i opcjami montowania.	
vfs.fs.get	Lista zamontowanych systemów plików wraz z ich typem, dostępną przestrzenią dyskową, statystykami inode i opcjami montowania.	
vfs.fs.inode	Liczba lub procent inode.	
vfs.fs.size	Przestrzeń dyskowa w bajtach lub jako procent całości.	
vm.memory.size	Rozmiar pamięci w bajtach lub jako procent całości.	Pamięć wirtualna
web.page.get	Pobiera zawartość strony internetowej.	Monitorowanie WWW
web.page.perf	Czas ładowania pełnej strony internetowej.	
web.page.regexp	Znajduje ciąg znaków na stronie internetowej.	
agent.hostmetadata	Metadane hosta agenta.	Zabbix
agent.hostname	Nazwa hosta agenta.	
agent.ping	Sprawdzenie dostępności agenta.	

Klucz pozycji	Opis	Grupa pozycji
agent.variant	Wariant Zabbix agent (Zabbix agent lub Zabbix agent 2).	
agent.version	Wersja Zabbix agent.	
zabbix.stats	Zwraca zestaw wewnętrznych metryk Zabbix serwer lub proxy. Jeśli określono `ip` i `port`, metryki są pobierane ze zdalnej instancji; w przeciwnym razie z instancji lokalnej.	
zabbix.stats	Zwraca liczbę monitorowanych pozycji w kolejce, które są opóźnione na Zabbix serwer lub proxy. Jeśli określono `ip` i `port`, metryki są pobierane ze zdalnej instancji; w przeciwnym razie z instancji lokalnej.	

Obsługiwane platformy

O ile w szczegółach pozycji nie określono inaczej, pozycje agenta (oraz wszystkie parametry) są obsługiwane na:

- **Linux**
- **FreeBSD**
- **Solaris**
- **HP-UX**
- **AIX**
- **MacOS X**
- **OpenBSD**
- **NetBSD**

Wiele pozycji agenta jest również obsługiwanych w systemie **Windows**. Szczegóły można znaleźć na stronie Windows agent item.

Szczegóły klucza pozycji

Parametry bez nawiasów ostrych są obowiązkowe. Parametry oznaczone nawiasami ostrymi **< >** są opcjonalne.

kernel.maxfiles

 Maksymalna liczba otwartych plików obsługiwana przez system operacyjny.
 Zwracana wartość: *Liczba całkowita*.
 Obsługiwane platformy: Linux, FreeBSD, MacOS X, OpenBSD, NetBSD.

kernel.maxproc

 Maksymalna liczba procesów obsługiwana przez system operacyjny.
 Zwracana wartość: *Integer*.
 Obsługiwane platformy: Linux 2.6 i nowsze, FreeBSD, Solaris, MacOS X, OpenBSD, NetBSD.

kernel.openfiles

 Liczba aktualnie otwartych deskryptorów plików.
 Zwracana wartość: *Integer*.
 Obsługiwane platformy: Linux (pozycja może działać na innych platformach typu UNIX).

log[file,<regexp>,<encoding>,<maxlines>,<mode>,<output>,<maxdelay>,<options>,<persistent dir>]

 Monitorowanie pliku dziennika.
 Zwracana wartość: *Log*.
 Zobacz obsługiwane platformy.

Parametry:

- **file** - pełna ścieżka i nazwa pliku dziennika;
- **regexp** - regularne wyrażenie opisujące wymagany wzorzec;
- **encoding** - identyfikator strony kodowej;
- **maxlines** - maksymalna liczba nowych linii na sekundę, które agent wyśle do serwer Zabbix lub proxy. Ten parametr nadpisuje wartość 'MaxLinesPerSecond' w zabbix_agentd.conf;
- **mode** - możliwe wartości: *all* (domyślnie) lub *skip* - pomiń przetwarzanie starszych danych (dotyczy tylko nowo utworzonych pozycji);
- **output** - opcjonalny szablon formatowania danych wyjściowych. Sekwencja ucieczki **\0** jest zastępowana dopasowaną częścią tekstu (od pierwszego znaku, od którego zaczyna się dopasowanie, do znaku, na którym dopasowanie się kończy), natomiast sekwencja ucieczki **\N** (gdzie N=1...9) jest zastępowana N-tą dopasowaną grupą (lub pustym ciągiem, jeśli N przekracza liczbę przechwyconych grup);
- **maxdelay** - maksymalne opóźnienie w sekundach. Typ: float. Wartości: 0 - (domyślnie) nigdy nie ignoruj linii pliku dziennika; > 0.0 - ignoruj starsze linie, aby analizować najnowsze linie w czasie "maxdelay" sekund. Przed użyciem przeczytaj uwagi dotyczące maxdelay!
- **options** - dodatkowe opcje:
mtime-noreread - nieunikalne rekordy, odczytuj ponownie tylko wtedy, gdy zmienia się rozmiar pliku (ignoruj zmianę czasu modyfikacji). (Ten parametr jest przestarzały od wersji 5.0.2, ponieważ obecnie mtime jest ignorowany.)

- **persistent dir** (tylko w zabbix_agentd w systemach Unix; nieobsługiwane w Zabbix agent 2) - bezwzględna ścieżka katalogu, w którym mają być przechowywane pliki trwałe. Zobacz także dodatkowe uwagi dotyczące plików trwałych.

Komentarze:

- Pozycja musi być skonfigurowana jako active check.
- Jeśli plik nie istnieje lub uprawnienia nie pozwalają na dostęp, pozycja staje się nieobsługiwana.
- Jeśli `output` pozostanie puste - zwracana jest cała linia zawierająca dopasowany tekst. Zwróć uwagę, że wszystkie typy globalnych wyrażeń regularnych z wyjątkiem 'Result is TRUE' zawsze zwracają całą dopasowaną linię, a parametr `output` jest ignorowany.
- Wyodrębnianie zawartości przy użyciu parametru `output` odbywa się po stronie agenta.

Przykłady:

```
log[/var/log/syslog]
log[/var/log/syslog,error]
log[/home/zabbix/logs/logfile,,,100]
```

Przykład użycia parametru `output` do wyodrębnienia liczby z rekordu dziennika:

```
log[/app1/app.log,"task run [0-9.]+ sec, processed ([0-9]+) records, [0-9]+ errors",,,,\1] #ta pozycja dop
```

Przykład użycia parametru `output` do przepisania rekordu dziennika przed wysłaniem do serwer:

```
log[/app1/app.log,"([0-9 :-]+) task run ([0-9.]+) sec, processed ([0-9]+) records, ([0-9]+) errors",,,,"\1
```

log.count[file,<regexp>,<encoding>,<maxproclines>,<mode>,<maxdelay>,<options>,<persistent dir>]

 Liczba dopasowanych wierszy w monitorowanym pliku dziennika.
 Zwracana wartość: *Integer*.
 Zobacz obsługiwane platformy.

Parametry:

- **file** - pełna ścieżka i nazwa pliku dziennika;
- **regexp** - wyrażenie regularne opisujące wymagany wzorzec;
- **encoding** - identyfikator strony kodowej;
- **maxproclines** - maksymalna liczba nowych wierszy na sekundę, które agent przeanalizuje (nie może przekraczać 10000). Wartość domyślna to 10*'MaxLinesPerSecond' w zabbix_agentd.conf.
- **mode** - możliwe wartości: *all* (domyślnie) lub *skip* - pomiń przetwarzanie starszych danych (dotyczy tylko nowo utworzonych pozycji).
- **maxdelay** - maksymalne opóźnienie w sekundach. Typ: float. Wartości: 0 - (domyślnie) nigdy nie ignoruj wierszy pliku dziennika; > 0.0 - ignoruj starsze wiersze, aby analizować najnowsze wiersze w ciągu "maxdelay" sekund. Przed użyciem przeczytaj uwagi dotyczące maxdelay!
- **options** - dodatkowe opcje:
mtime-noreread - nieunikalne rekordy, odczytuj ponownie tylko wtedy, gdy zmieni się rozmiar pliku (ignoruj zmianę czasu modyfikacji). (Ten parametr jest przestarzały od wersji 5.0.2, ponieważ obecnie mtime jest ignorowany.)
- **persistent dir** (tylko w zabbix_agentd w systemach Unix; nieobsługiwane w Zabbix agent 2) - bezwzględna ścieżka katalogu, w którym mają być przechowywane pliki trwałe. Zobacz także dodatkowe uwagi dotyczące plików trwałych.

Komentarze:

- Pozycja musi być skonfigurowana jako sprawdzanie aktywne.
- Dopasowane wiersze są zliczane wśród nowych wierszy od ostatniego sprawdzenia dziennika przez agent, a zatem zależą od interwału aktualizacji pozycji.
- Jeśli plik nie istnieje lub uprawnienia nie pozwalają na dostęp, pozycja staje się nieobsługiwana.

logrt[file regexp,<regexp>,<encoding>,<maxlines>,<mode>,<output>,<maxdelay>,<options>,<persistent dir>]

 Monitorowanie rotowanego pliku dziennika.
 Zwracana wartość: *Log*.
 Zobacz obsługiwane platformy.

Parametry:

- **file regexp** - bezwzględna ścieżka do pliku, z nazwą pliku określoną za pomocą regularnego wyrażenia. Pamiętaj, że wyrażenie regularne ma zastosowanie tylko do nazwy pliku i nie musi pasować do całej nazwy (np. /path/to/agent będzie pasować do zabbix_agentd.log).
- **regexp** - regularne wyrażenie opisujące wymagany wzorzec zawartości.
- **encoding** - identyfikator strony kodowej.
- **maxlines** - maksymalna liczba nowych linii na sekundę, które agent wyśle do serwer lub proxy. Ten parametr nadpisuje wartość 'MaxLinesPerSecond' w zabbix_agentd.conf.
- **mode** - możliwe wartości: *all* (domyślnie) lub *skip* - pomiń przetwarzanie starszych danych (dotyczy tylko nowo utworzonych pozycji).

- **output** - opcjonalny szablon formatowania wyjścia. Sekwencja ucieczki **\0** jest zastępowana dopasowaną częścią tekstu (od pierwszego znaku, od którego zaczyna się dopasowanie, do znaku, na którym dopasowanie się kończy), natomiast sekwencja ucieczki **\N** (gdzie N=1...9) jest zastępowana N-tą dopasowaną grupą (lub pustym ciągiem, jeśli N przekracza liczbę przechwyconych grup).
- **maxdelay** - maksymalne opóźnienie w sekundach. Typ: float. Wartości: 0 - (domyślnie) nigdy nie ignoruj linii pliku dziennika; > 0.0 - ignoruj starsze linie, aby analizować najnowsze linie w czasie "maxdelay" sekund. Przed użyciem przeczytaj uwagi dotyczące maxdelay!
- **options** - typ rotacji pliku dziennika i inne opcje. Możliwe wartości:
rotate (domyślnie),
copytruncate - pamiętaj, że *copytruncate* nie może być używane razem z *maxdelay*. W takim przypadku *maxdelay* musi mieć wartość 0 lub nie może być podane; zobacz uwagi dotyczące copytruncate,
mtime-reread - nieunikalne rekordy, odczytuj ponownie, jeśli zmieni się czas modyfikacji lub rozmiar (używane domyślnie, jeśli żadna opcja `mtime-*` nie została jawnie ustawiona),
mtime-noreread - nieunikalne rekordy, odczytuj ponownie tylko wtedy, gdy zmieni się rozmiar (ignoruj zmianę czasu modyfikacji).
- **persistent dir** (tylko w zabbix_agentd w systemach Unix; nieobsługiwane w Zabbix agent 2) - bezwzględna ścieżka katalogu, w którym mają być przechowywane pliki trwałe. Zobacz także dodatkowe uwagi dotyczące plików trwałych.

Komentarze:

- Pozycja musi być skonfigurowana jako active check.
- Rotacja dziennika opiera się na czasie ostatniej modyfikacji plików.
- Pamiętaj, że logrt jest zaprojektowane do pracy z jednym aktualnie aktywnym plikiem dziennika oraz kilkoma innymi pasującymi nieaktywnymi plikami po rotacji. Jeśli na przykład katalog zawiera wiele aktywnych plików dziennika, dla każdego z nich należy utworzyć osobną pozycję logrt. W przeciwnym razie, jeśli jedna pozycja logrt obejmie zbyt wiele plików, może to doprowadzić do wyczerpania pamięci i awarii monitorowania.
- Jeśli `output` pozostanie puste - zwracana jest cała linia zawierająca dopasowany tekst. Pamiętaj, że wszystkie globalne typy wyrażeń regularnych z wyjątkiem 'Result is TRUE' zawsze zwracają całą dopasowaną linię, a parametr `output` jest ignorowany.
- Wyodrębnianie zawartości przy użyciu parametru `output` odbywa się po stronie agenta.
- W parametrze `file regexp` ścieżka katalogu dziennika i wyrażenie regularne nazwy pliku dziennika muszą być rozdzielone poprawnym separatorem katalogów:
  - W systemie Windows separatorem musi być ukośnik wsteczny (\); ukośniki zwykłe mogą być tolerowane w innych pozycjach, z wyjątkiem tego, który rozdziela ścieżkę katalogu dziennika i wyrażenie regularne nazwy pliku dziennika (zobacz przykłady poniżej).
  - W innych systemach musi to być ukośnik zwykły (/).

Przykłady dla Windows:

```
logrt["c:/dir1/dir2/dir3\filename.*\.log","pattern_to_match"] #ta pozycja będzie zbierać dane z plików dzi
logrt["//example.com/share/dir1/dir2/dir3\filename.*\.log","pattern_to_match"] #ta pozycja będzie zbierać
```

Przykłady dla innych systemów:

```
logrt["/home/zabbix/logs/^logfile[0-9]{1,3}$",,,100] #ta pozycja dopasuje plik taki jak "logfile1" (nie do
logrt["/home/user/^logfile_.*_[0-9]{1,3}$","pattern_to_match","UTF-8",100] #ta pozycja będzie zbierać dane
```

Przykład użycia parametru `output` do wyodrębnienia liczby z rekordu dziennika:

```
logrt[/app1/^test.*log$,"task run [0-9.]+ sec, processed ([0-9]+) records, [0-9]+ errors",,,,\1] #ta pozyc
```

Przykład użycia parametru `output` do przepisania rekordu dziennika przed wysłaniem do serwer:

```
logrt[/app1/^test.*log$,"([0-9 :-]+) task run ([0-9.]+) sec, processed ([0-9]+) records, ([0-9]+) errors",
```

logrt.count[file regexp,<regexp>,<encoding>,<maxproclines>,<mode>,<maxdelay>,<options>,<persistent dir>]

 Liczba dopasowanych linii w monitorowanym pliku logu podlegającym rotacji.
 Zwracana wartość: *Integer*.
 Zobacz obsługiwane platformy.

Parametry:

- **file regexp** - bezwzględna ścieżka do pliku, z nazwą pliku określoną za pomocą regularnego wyrażenia. Pamiętaj, że wyrażenie regularne ma zastosowanie tylko do nazwy pliku i nie musi pasować do całej nazwy (np. /path/to/agent będzie pasować do zabbix_agentd.log).
- **regexp** - regularne wyrażenie opisujące wymagany wzorzec.
- **encoding** - identyfikator strony kodowej.
- **maxproclines** - maksymalna liczba nowych linii na sekundę, które agent przeanalizuje (nie może przekraczać 10000). Wartość domyślna to 10*'MaxLinesPerSecond' w zabbix_agentd.conf.
- **mode** - możliwe wartości: *all* (domyślnie) lub *skip* - pomiń przetwarzanie starszych danych (dotyczy tylko nowo utworzonych pozycji).

- **maxdelay** - maksymalne opóźnienie w sekundach. Typ: float. Wartości: 0 - (domyślnie) nigdy nie ignoruj linii pliku logu; > 0.0 - ignoruj starsze linie, aby przeanalizować najnowsze linie w ciągu „maxdelay" sekund. Przed użyciem przeczytaj uwagi dotyczące maxdelay!
- **options** - typ rotacji pliku logu i inne opcje. Możliwe wartości:
rotate (domyślnie),
copytruncate - pamiętaj, że *copytruncate* nie może być używane razem z *maxdelay*. W takim przypadku *maxdelay* musi mieć wartość 0 lub nie może być określone; zobacz uwagi dotyczące copytruncate,
mtime-reread - nieunikalne rekordy, odczytuj ponownie, jeśli zmieni się czas modyfikacji lub rozmiar (domyślnie),
mtime-noreread - nieunikalne rekordy, odczytuj ponownie tylko wtedy, gdy zmieni się rozmiar (ignoruj zmianę czasu modyfikacji).
- **persistent dir** (tylko w zabbix_agentd w systemach Unix; nieobsługiwane w Zabbix agent 2) - bezwzględna ścieżka katalogu, w którym mają być przechowywane pliki trwałe. Zobacz także dodatkowe uwagi dotyczące plików trwałych.

Uwagi:

- Pozycja musi być skonfigurowana jako active check.
- Dopasowane linie są zliczane wśród nowych linii od ostatniego sprawdzenia logu przez agent, a więc zależą od interwału aktualizacji pozycji.
- Rotacja logu opiera się na czasie ostatniej modyfikacji plików.
- W parametrze `file regexp` ścieżka katalogu logu i wyrażenie regularne pliku logu muszą być rozdzielone poprawnym separatorem katalogów:
  - W systemie Windows separatorem musi być ukośnik odwrotny (\); ukośniki zwykłe mogą być tolerowane w innych miejscach, z wyjątkiem tego, które rozdziela ścieżkę katalogu logu i wyrażenie regularne pliku logu (zobacz przykłady poniżej).
  - W innych systemach musi to być ukośnik zwykły (/).

Przykłady dla systemu Windows:

```
logrt.count["c:/dir1/dir2/dir3\filename.*\.log","pattern_to_match"] #this item will count the number of ma
logrt.count["//example.com/share/dir1/dir2/dir3\filename.*\.log","pattern_to_match"] #this item will count
```

Przykłady dla innych systemów:

```
logrt.count["/home/zabbix/logs/.*","^logfile[0-9]{1,3}$",,100] #this item will count the number of matches
logrt.count["/home/user/^logfile_.*_[0-9]{1,3}$","pattern_to_match","UTF-8",100] #this item will count the
```

modbus.get[endpoint,<slave id>,<function>,<address>,<count>,<type>,<endianness>,<offset>]

 Odczytuje dane Modbus.
 Wartość zwracana: *ciąg JSON*.
 Obsługiwane platformy: Linux, Windows.

Parametry:

- **endpoint** - punkt końcowy zdefiniowany jako `protocol://connection_string`;
- **slave id** - identyfikator slave;
- **function** - funkcja Modbus;
- **address** - adres pierwszego rejestru, cewki lub wejścia;
- **count** - liczba rekordów do odczytu;
- **type** - typ danych;
- **endianness** - konfiguracja kolejności bajtów;
- **offset** - liczba rejestrów, począwszy od `address`, których wyniki zostaną odrzucone.

W systemie Windows ta pozycja podąża za ścieżkami UNC w parametrze **endpoint**, co może stanowić zagrożenie bezpieczeństwa.

Zobacz szczegółowy opis parametrów.

net.dns[<ip>,name,<type>,<timeout>,<count>,<protocol>]

 Sprawdza stan usługi DNS.
 Zwracane wartości: 0 - rozwiązywanie DNS nie powiodło się (serwer DNS nie odpowiedział lub zwrócił błąd); 1 - rozwiązywanie DNS zakończyło się powodzeniem.
 Zobacz obsługiwane platformy.

Parametry:

- **ip** (ignorowane w systemie Windows, chyba że używany jest Zabbix agent 2) - adres IP serwera DNS (pozostaw puste dla domyślnego serwera DNS);
- **name** - nazwa DNS do odpytania;
- **type** - typ rekordu, o który zostanie wykonane zapytanie (domyślnie *SOA*);
- **timeout** (ignorowane w systemie Windows, chyba że używany jest Zabbix agent 2) - limit czasu żądania w sekundach (domyślnie 1 sekunda);
- **count** (ignorowane w systemie Windows, chyba że używany jest Zabbix agent 2) - liczba prób dla żądania (domyślnie 2);
- **protocol** - protokół używany do wykonywania zapytań DNS: *udp* (domyślnie) lub *tcp*.

Uwagi:

- Możliwe wartości parametru `type` to: *ANY*, *A*, *NS*, *CNAME*, *MB*, *MG*, *MR*, *PTR*, *MD*, *MF*, *MX*, *SOA*, *NULL*, *WKS* (nieobsługiwane przez Zabbix agent w systemie Windows, Zabbix agent 2 we wszystkich systemach operacyjnych), *HINFO*, *MINFO*, *TXT*, *SRV*.
- W przypadku odwrotnych wyszukiwań DNS (gdy `type` jest ustawione na *PTR*) można podać nazwę DNS zarówno w formacie odwróconym, jak i nieodwróconym (zobacz przykłady poniżej). Pamiętaj, że gdy żądany jest rekord PTR, nazwa DNS jest w rzeczywistości adresem IP.
- Międzynarodowe nazwy domen nie są obsługiwane; zamiast tego użyj nazw zakodowanych w IDNA.

Przykłady:

```
net.dns[198.51.100.1,example.com,MX,2,1]

net.dns[,198.51.100.1,PTR]
net.dns[,1.100.51.198.in-addr.arpa,PTR]

net.dns[,2a00:1450:400f:800::200e,PTR]
net.dns[,e.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.0.f.0.0.4.0.5.4.1.0.0.a.2.ip6.arpa,PTR]
```

net.dns.perf[<ip>,name,<type>,<timeout>,<count>,<protocol>]

 Sprawdza wydajność usługi DNS.
 Zwracana wartość: *Float* (0 - usługa jest niedostępna; sekundy - liczba sekund spędzonych na oczekiwaniu na odpowiedź z usługi).
 Zobacz obsługiwane platformy.

Parametry:

- **ip** (ignorowane w systemie Windows, chyba że używany jest Zabbix agent 2) - adres IP serwera DNS (pozostaw puste dla domyślnego serwera DNS);
- **name** - nazwa DNS do odpytania;
- **type** - typ rekordu, o który zostanie wykonane zapytanie (domyślnie *SOA*);
- **timeout** (ignorowane w systemie Windows, chyba że używany jest Zabbix agent 2) - limit czasu żądania w sekundach (domyślnie 1 sekunda);
- **count** (ignorowane w systemie Windows, chyba że używany jest Zabbix agent 2) - liczba prób wykonania żądania (domyślnie 2);
- **protocol** - protokół używany do wykonywania zapytań DNS: *udp* (domyślnie) lub *tcp*.

Uwagi:

- Możliwe wartości parametru `type` to:
ANY, *A*, *NS*, *CNAME*, *MB*, *MG*, *MR*, *PTR*, *MD*, *MF*, *MX*, *SOA*, *NULL*, *WKS* (nieobsługiwane przez Zabbix agent w systemie Windows, Zabbix agent 2 we wszystkich systemach operacyjnych), *HINFO*, *MINFO*, *TXT*, *SRV*.
- W przypadku odwrotnych wyszukiwań DNS (gdy `type` jest ustawione na *PTR*) można podać nazwę DNS zarówno w formacie odwróconym, jak i nieodwróconym (zobacz przykłady poniżej). Należy pamiętać, że gdy żądany jest rekord PTR, nazwa DNS jest w rzeczywistości adresem IP.
- Międzynarodowe nazwy domen nie są obsługiwane; zamiast tego należy używać nazw zakodowanych w IDNA.
- pozycja zwraca czas odpowiedzi zamiast 0, gdy serwer DNS odpowiada kodem błędu (na przykład `NXDOMAIN` lub `SERVFAIL`).

Przykłady:

```
net.dns.perf[198.51.100.1,example.com,MX,2,1]

net.dns.perf[,198.51.100.1,PTR]
net.dns.perf[,1.100.51.198.in-addr.arpa,PTR]

net.dns.perf[,2a00:1450:400f:800::200e,PTR]
net.dns.perf[,e.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.0.f.0.0.4.0.5.4.1.0.0.a.2.ip6.arpa,PTR]
```

net.dns.record[<ip>,name,<type>,<timeout>,<count>,<protocol>]

 Wykonuje zapytanie DNS.

Zabbix agent 2 udostępnia również net.dns.get, które oferuje dodatkowe funkcje, takie jak większa liczba typów rekordów oraz większa kontrola nad monitorowaniem DNS. Wartość zwracana: ciąg znaków zawierający wymagany typ informacji.
 Zobacz obsługiwane platformy.

Parametry:

- **ip** (ignorowane w systemie Windows, chyba że używany jest Zabbix agent 2) - adres IP serwera DNS (pozostaw puste, aby użyć domyślnego serwera DNS);
- **name** - nazwa DNS, o którą ma zostać wykonane zapytanie;
- **type** - typ rekordu, o który ma zostać wykonane zapytanie (domyślnie *SOA*);

- **timeout** (ignorowane w systemie Windows, chyba że używany jest Zabbix agent 2) - limit czasu żądania w sekundach (domyślnie 1 sekunda);
- **count** (ignorowane w systemie Windows, chyba że używany jest Zabbix agent 2) - liczba prób wykonania żądania (domyślnie 2);
- **protocol** - protokół używany do wykonywania zapytań DNS: *udp* (domyślnie) lub *tcp*.

Uwagi:

- Możliwe wartości parametru `type` to:
ANY, *A*, *NS*, *CNAME*, *MB*, *MG*, *MR*, *PTR*, *MD*, *MF*, *MX*, *SOA*, *NULL*, *WKS* (nieobsługiwane przez Zabbix agent w systemie Windows oraz przez Zabbix agent 2 we wszystkich systemach operacyjnych), *HINFO*, *MINFO*, *TXT*, *SRV*.
- W przypadku odwrotnych wyszukiwań DNS (gdy `type` jest ustawione na *PTR*) można podać nazwę DNS w formacie odwróconym lub nieodwróconym (zobacz przykłady poniżej). Należy pamiętać, że gdy żądany jest rekord PTR, nazwa DNS jest w rzeczywistości adresem IP.
- Międzynarodowe nazwy domen nie są obsługiwane; zamiast tego należy używać nazw zakodowanych w IDNA.

Przykłady:

```
net.dns.record[198.51.100.1,example.com,MX,2,1]

net.dns.record[,198.51.100.1,PTR]
net.dns.record[,1.100.51.198.in-addr.arpa,PTR]

net.dns.record[,2a00:1450:400f:800::200e,PTR]
net.dns.record[,e.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.0.f.0.0.4.0.5.4.1.0.0.a.2.ip6.arpa,PTR]
```

net.if.collisions[if]

 Liczba kolizji poza oknem czasowym.
 Wartość zwracana: *Integer*.
 Obsługiwane platformy: Linux, FreeBSD, Solaris, AIX, MacOS X, OpenBSD, NetBSD. Uprawnienia root są wymagane w NetBSD.

Parametr:

- **if** - nazwa interfejsu sieciowego

net.if.discovery

 Lista interfejsów sieciowych. Używana do wykrywania niskiego poziomu.
 Wartość zwracana: *ciąg JSON*.
 Obsługiwane platformy: Linux, FreeBSD, Solaris, HP-UX, AIX, OpenBSD, NetBSD, Windows.

net.if.in[if,<mode>]

 Statystyki ruchu przychodzącego na interfejsie sieciowym.
 Zwracana wartość: *Integer*.
 Obsługiwane platformy: Linux, FreeBSD, Solaris[5], HP-UX, AIX, MacOS X, OpenBSD, NetBSD, Windows. Uprawnienia root są wymagane w systemie NetBSD.

Parametry:

- **if** - nazwa interfejsu sieciowego (Unix); pełny opis interfejsu sieciowego lub adres IPv4; albo, jeśli ujęty w nawiasy klamrowe, GUID interfejsu sieciowego (Windows);
- **mode** - możliwe wartości:
bytes - liczba bajtów (domyślnie)
packets - liczba pakietów
errors - liczba błędów
dropped - liczba odrzuconych pakietów
overruns (fifo) - liczba błędów bufora FIFO
frame - liczba błędów ramkowania pakietów
compressed - liczba skompresowanych pakietów odebranych przez sterownik urządzenia
multicast - liczba ramek multicast odebranych przez sterownik urządzenia

Uwagi:

- Możesz użyć tego klucza razem z krokiem przetwarzania wstępnego *Change per second*, aby uzyskać statystyki liczby bajtów na sekundę.
- Tryb *dropped* jest obsługiwany tylko w systemach Linux, FreeBSD, HP-UX, MacOS X, OpenBSD, NetBSD.
- Tryby *overruns*, *frame*, *compressed*, *multicast* są obsługiwane tylko w systemie Linux.
- W systemie HP-UX ta pozycja nie dostarcza szczegółów dotyczących interfejsów loopback (np. lo0).

Przykłady:

```
net.if.in[eth0]
net.if.in[eth0,errors]
```

net.if.out[if,<mode>]

 Statystyki ruchu wychodzącego na interfejsie sieciowym.
 Zwracana wartość: *Integer*.
 Obsługiwane platformy: Linux, FreeBSD, Solaris[5], HP-UX, AIX, MacOS X, OpenBSD, NetBSD, Windows. Uprawnienia root są wymagane w systemie NetBSD.

Parametry:

- **if** - nazwa interfejsu sieciowego (Unix); pełny opis interfejsu sieciowego lub adres IPv4; albo, jeśli ujęty w nawiasy klamrowe, GUID interfejsu sieciowego (Windows);
- **mode** - możliwe wartości:
bytes - liczba bajtów (domyślnie)
packets - liczba pakietów
errors - liczba błędów
dropped - liczba odrzuconych pakietów
overruns (fifo) - liczba błędów bufora FIFO
collisions (colls) - liczba kolizji wykrytych na interfejsie
carrier - liczba utrat nośnej wykrytych przez sterownik urządzenia
compressed - liczba skompresowanych pakietów przesłanych przez sterownik urządzenia

Uwagi:

- Możesz użyć tego klucza z krokiem przetwarzania wstępnego *Zmiana na sekundę*, aby uzyskać statystyki bajtów na sekundę.
- Tryb *dropped* jest obsługiwany tylko w systemach Linux, HP-UX.
- Tryby *overruns*, *collision*, *carrier*, *compressed* są obsługiwane tylko w systemie Linux.
- W systemie HP-UX ta pozycja nie dostarcza szczegółów dotyczących interfejsów loopback (np. lo0).

Przykłady:

```
net.if.out[eth0]
net.if.out[eth0,errors]
```

net.if.total[if,<mode>]

 Suma statystyk ruchu przychodzącego i wychodzącego na interfejsie sieciowym.
 Zwracana wartość: *Integer*.
 Obsługiwane platformy: Linux, FreeBSD, Solaris[5], HP-UX, AIX, MacOS X, OpenBSD, NetBSD, Windows. Uprawnienia root są wymagane w systemie NetBSD.

Parametry:

- **if** - nazwa interfejsu sieciowego (Unix); pełny opis interfejsu sieciowego lub adres IPv4; albo, jeśli ujęty w nawiasy klamrowe, GUID interfejsu sieciowego (Windows);
- **mode** - możliwe wartości:
bytes - liczba bajtów (domyślnie)
packets - liczba pakietów
errors - liczba błędów
dropped - liczba odrzuconych pakietów
overruns (fifo) - liczba błędów bufora FIFO
collisions (colls) - liczba kolizji wykrytych na interfejsie
compressed - liczba skompresowanych pakietów wysłanych lub odebranych przez sterownik urządzenia

Uwagi:

- Możesz użyć tego klucza z krokiem preprocessing *Change per second*, aby uzyskać statystyki bajtów na sekundę.
- Tryb *dropped* jest obsługiwany tylko w systemach Linux i HP-UX. Odrzucone pakiety są obsługiwane tylko wtedy, gdy zarówno `net.if.in`, jak i `net.if.out` działają dla odrzuconych pakietów na Twojej platformie.
- Tryby *overruns*, *collision*, *compressed* są obsługiwane tylko w systemie Linux.
- W systemie HP-UX ta pozycja nie dostarcza szczegółów dotyczących interfejsów loopback (np. lo0).

Przykłady:

```
net.if.total[eth0]
net.if.total[eth0,errors]
```

net.tcp.listen[port]

 Sprawdza, czy ten port TCP jest w stanie LISTEN.
 Zwracane wartości: 0 - nie jest w stanie LISTEN; 1 - jest w stanie LISTEN.
 Obsługiwane platformy: Linux, FreeBSD, Solaris, MacOS X, Windows.

Parametr:

- **port** - numer portu TCP

W jądrach Linux 2.6.14 i nowszych informacje o nasłuchujących gniazdach TCP są pobierane, jeśli to możliwe, z interfejsu NETLINK jądra. W przeciwnym razie informacje są pobierane z plików /proc/net/tcp i /roc/net/tcp6.

Przykład:

```
net.tcp.listen[80]
```

net.tcp.port[<ip>,port]

 Sprawdza, czy możliwe jest nawiązanie połączenia TCP z określonym portem.
 Zwracane wartości: 0 - nie można się połączyć; 1 - można się połączyć.
 Zobacz obsługiwane platformy.

Parametry:

- **ip** - adres IP lub nazwa DNS (domyślnie 127.0.0.1);
- **port** - numer portu.

Uwagi:

- Do prostego testowania wydajności TCP użyj `net.tcp.service.perf[tcp,<ip>,<port>]`.
- Te testy mogą powodować pojawianie się dodatkowych komunikatów w plikach dziennika demona systemowego (zwykle rejestrowane są sesje SMTP i SSH).

Przykład:

```
net.tcp.port[,80] #tej pozycji można użyć do testowania dostępności serwera WWW działającego na porcie 80
```

net.tcp.service[service,<ip>,<port>]

 Sprawdza, czy usługa działa i akceptuje połączenia TCP.
 Zwracane wartości: 0 - usługa jest niedostępna; 1 - usługa działa.
 Zobacz obsługiwane platformy.

Parametry:

- **service** - *ssh*, *ldap*, *smtp*, *ftp*, *http*, *pop*, *nntp*, *imap*, *tcp*, *https* lub *telnet* (zobacz szczegóły);
- **ip** - adres IP lub nazwa DNS (domyślnie 127.0.0.1);
- **port** - numer portu (domyślnie używany jest standardowy numer portu usługi).

Uwagi:

- Te testy mogą powodować pojawianie się dodatkowych komunikatów w plikach dziennika demonów systemowych (zwykle rejestrowane są sesje SMTP i SSH).
- Sprawdzanie szyfrowanych protokołów (takich jak IMAP na porcie 993 lub POP na porcie 995) nie jest obecnie obsługiwane. Jako obejście należy użyć `net.tcp.port[]` do takich testów.
- Sprawdzanie LDAP i HTTPS w systemie Windows jest obsługiwane tylko przez Zabbix agent 2.
- Test telnet szuka monitu logowania (':' na końcu).

Przykład:

```
net.tcp.service[ftp,,45] #tej pozycji można użyć do testowania dostępności serwera FTP na porcie TCP 45
```

net.tcp.service.perf[service,<ip>,<port>]

 Sprawdza wydajność usługi TCP.
 Zwracane wartości: *Float* (0 - usługa jest niedostępna; sekundy - liczba sekund oczekiwania na odpowiedź od usługi).
 Zobacz obsługiwane platformy.

Parametry:

- **service** - *ssh*, *ldap*, *smtp*, *ftp*, *http*, *pop*, *nntp*, *imap*, *tcp*, *https* lub *telnet* (zobacz szczegóły);
- **ip** - adres IP lub nazwa DNS (domyślnie 127.0.0.1);
- **port** - numer portu (domyślnie używany jest standardowy numer portu usługi).

Uwagi:

- Sprawdzanie szyfrowanych protokołów (takich jak IMAP na porcie 993 lub POP na porcie 995) nie jest obecnie obsługiwane. Jako obejście, do takich kontroli użyj `net.tcp.service.perf[tcp,<ip>,<port>]`.
- Kontrola telnet szuka monitu logowania (':' na końcu).

Przykład:

```
net.tcp.service.perf[ssh] #ta pozycja może być użyta do testowania szybkości początkowej odpowiedzi z serw
```

net.tcp.socket.count[<laddr>,<lport>,<raddr>,<rport>,<state>]

 Zwraca liczbę gniazd TCP pasujących do parametrów.
 Zwracana wartość: *Integer*.
 Obsługiwane platformy: Linux, Windows.

Parametry:

- **laddr** - lokalny adres IPv4/6 lub podsieć CIDR;
- **lport** - numer portu lokalnego lub nazwa usługi;
- **raddr** - zdalny adres IPv4/6 lub podsieć CIDR;
- **rport** - numer portu zdalnego lub nazwa usługi;
- **state** - stan połączenia (*established*, *syn_sent*, *syn_recv*, *fin_wait1*, *fin_wait2*, *time_wait*, *close*, *close_wait*, *last_ack*, *listen*, *closing*).

Przykład:

```
net.tcp.socket.count[,80,,,established] #liczba połączeń z lokalnym portem TCP 80 w stanie established
```

net.udp.listen[port]

 Sprawdza, czy ten port UDP jest w stanie LISTEN.
 Zwracane wartości: 0 - nie jest w stanie LISTEN; 1 - jest w stanie LISTEN.
 Obsługiwane platformy: Linux, FreeBSD, Solaris, MacOS X.

Parametr:

- **port** - numer portu UDP

Przykład:

```
net.udp.listen[68]
```

net.udp.service[service,<ip>,<port>]

 Sprawdza, czy usługa działa i odpowiada na żądania UDP.
 Zwracane wartości: 0 - usługa jest niedostępna; 1 - usługa działa.
 Zobacz obsługiwane platformy.

Parametry:

- **service** - *ntp* (zobacz szczegóły);
- **ip** - adres IP lub nazwa DNS (domyślnie 127.0.0.1);
- **port** - numer portu (domyślnie używany jest standardowy numer portu usługi).

Przykład:

```
net.udp.service[ntp,,45] #this item can be used to test the availability of NTP service on UDP port 45
```

net.udp.service.perf[service,<ip>,<port>]

 Sprawdza wydajność usługi UDP.
 Zwracane wartości: *Float* (0 - usługa jest niedostępna; sekundy - liczba sekund oczekiwania na odpowiedź z usługi).
 Zobacz obsługiwane platformy.

Parametry:

- **service** - *ntp* (zobacz szczegóły);
- **ip** - adres IP lub nazwa DNS (domyślnie 127.0.0.1);
- **port** - numer portu (domyślnie używany jest standardowy numer portu usługi).

Przykład:

```
net.udp.service.perf[ntp] #tej pozycji można użyć do testowania czasu odpowiedzi usługi NTP
```

net.udp.socket.count[<laddr>,<lport>,<raddr>,<rport>,<state>]

 Zwraca liczbę gniazd UDP pasujących do parametrów.
 Wartość zwracana: *Integer*.
 Obsługiwane platformy: Linux, Windows.

Parametry:

- **laddr** - lokalny adres IPv4/6 lub podsieć CIDR;
- **lport** - numer portu lokalnego lub nazwa usługi;
- **raddr** - zdalny adres IPv4/6 lub podsieć CIDR;
- **rport** - numer portu zdalnego lub nazwa usługi;
- **state** - stan połączenia (*established*, *unconn*).

Przykład:

```
net.udp.socket.count[,,,,established] #zwraca liczbę gniazd UDP w stanie połączenia
```

proc.cpu.util[<name>,<user>,<type>,<cmdline>,<mode>,<zone>]

 Procent wykorzystania CPU procesu.
 Zwracana wartość: *Float*.
 Obsługiwane platformy: Linux, Solaris[6].

Parametry:

- **name** - nazwa procesu (domyślnie *wszystkie procesy*);
- **user** - nazwa użytkownika (domyślnie *wszyscy użytkownicy*);
- **type** - typ wykorzystania CPU: *total* (domyślnie), *user* lub *system*;
- **cmdline** - filtrowanie według wiersza poleceń (jest to wyrażenie regularne);
- **mode** - tryb zbierania danych: *avg1* (domyślnie), *avg5* lub *avg15*;
- **zone** - docelowa strefa: *current* (domyślnie) lub *all*. Ten parametr jest obsługiwany tylko w systemie Solaris.

Komentarze:

- Zwracana wartość jest oparta na procencie wykorzystania pojedynczego rdzenia CPU. Na przykład wykorzystanie CPU przez proces w pełni używający dwóch rdzeni wynosi 200%.
- Dane o wykorzystaniu CPU procesu są zbierane przez kolektor, który obsługuje maksymalnie 1024 unikalne zapytania (według nazwy, użytkownika i wiersza poleceń). Zapytania, do których nie odwoływano się w ciągu ostatnich 24 godzin, są usuwane z kolektora.

- Jeśli parametr zone jest ustawiony na *current* (lub domyślnie), a agent został skompilowany w systemie Solaris bez obsługi stref, ale działa na nowszym systemie Solaris, w którym strefy są obsługiwane, agent zwróci NOTSUPPORTED (agent nie może ograniczyć wyników tylko do bieżącej strefy). Jednak w takim przypadku *all* jest obsługiwane.

Przykłady:

```
proc.cpu.util[,root] #wykorzystanie CPU wszystkich procesów uruchomionych przez użytkownika "root"
proc.cpu.util[zabbix_server,zabbix] #wykorzystanie CPU wszystkich procesów zabbix_server uruchomionych prz
```

proc.get[<name>,<user>,<cmdline>,<mode>]

 Lista procesów systemu operacyjnego i ich parametrów. Może być używana do wykrywania niskiego poziomu.
 Zwracana wartość: *ciąg JSON*.
 Obsługiwane platformy: Linux, FreeBSD, Windows, OpenBSD, NetBSD.

Parametry:

- **name** - nazwa procesu (domyślnie *wszystkie procesy*);
- **user** - nazwa użytkownika (domyślnie *wszyscy użytkownicy*);
- **cmdline** - filtrowanie według wiersza poleceń (jest to regularne wyrażenie). Ten parametr nie jest obsługiwany w systemie Windows; na innych platformach nie jest obsługiwany, jeśli mode jest ustawiony na 'summary'.
- **mode** - możliwe wartości:
process (domyślnie), *thread* (nieobsługiwane w NetBSD), *summary*. Zobacz listę parametrów procesu zwracanych dla każdego trybu i systemu operacyjnego.

Uwagi:

- Jeśli nie można pobrać wartości, na przykład z powodu błędu (proces już zakończył działanie, brak uprawnień, błąd wywołania systemowego), zostanie zwrócone −1.
- Zobacz uwagi dotyczące wybierania procesów za pomocą parametrów `name` i `cmdline` (dotyczy tylko systemu Linux).

Przykłady:

```
proc.get[zabbix_server,zabbix,,process] #lista wszystkich procesów zabbix_server uruchomionych przez użytk
proc.get[java,,,thread] #lista wszystkich procesów Java, zwraca jeden wpis na wątek
proc.get[,zabbix,,summary] #połączone dane dla procesów każdego typu uruchomionych przez użytkownika zabbi
```

proc.mem[<name>,<user>,<mode>,<cmdline>,<memtype>]

 Pamięć używana przez proces w bajtach.
 Wartość zwracana: *Integer* - gdy `mode` ma wartość *max*, *min*, *sum*; *Float* - gdy `mode` ma wartość *avg*
 Obsługiwane platformy: Linux, FreeBSD, Solaris, AIX, OpenBSD, NetBSD.

Parametry:

- **name** - nazwa procesu (domyślnie *wszystkie procesy*);
- **user** - nazwa użytkownika (domyślnie *wszyscy użytkownicy*);
- **mode** - możliwe wartości: *avg*, *max*, *min* lub *sum* (domyślnie);
- **cmdline** - filtrowanie według linii poleceń (jest to regularne wyrażenie);
- **memtype** - typ pamięci używanej przez proces

Uwagi:

- Parametr `memtype` jest obsługiwany tylko w systemach Linux, FreeBSD, Solaris[6], AIX.
- Gdy kilka procesów używa pamięci współdzielonej, suma pamięci używanej przez procesy może dawać duże, nierealistyczne wartości.

Zobacz uwagi dotyczące wybierania procesów za pomocą parametrów `name` i `cmdline` (dotyczy tylko Linuxa).

Gdy ta pozycja jest wywoływana z wiersza poleceń i zawiera parametr linii poleceń (np. przy użyciu trybu testowego agent: `zabbix_agentd -t proc.mem[,,,apache2]`), zostanie zliczony jeden dodatkowy proces, ponieważ agent policzy również samego siebie.

Przykłady:

```
proc.mem[,root] #pamięć używana przez wszystkie procesy uruchomione przez użytkownika "root"
proc.mem[zabbix_server,zabbix] #pamięć używana przez wszystkie procesy zabbix_server uruchomione przez uży
proc.mem[,oracle,max,oracleZABBIX] #pamięć używana przez proces zużywający najwięcej pamięci, uruchomiony
```

proc.num[<name>,<user>,<state>,<cmdline>,<zone>]

 Liczba procesów.
 Zwracana wartość: *Integer*.
 Obsługiwane platformy: Linux, FreeBSD, Solaris[6], HP-UX, AIX, OpenBSD, NetBSD, Windows.

Parametry:

- **name** - nazwa procesu (domyślnie *wszystkie procesy*);
- **user** - nazwa użytkownika (domyślnie *wszyscy użytkownicy*);

- **state** - możliwe wartości:
all (domyślnie),
disk - nieprzerywalny sen,
run - uruchomiony,
sleep - przerywalny sen,
trace - zatrzymany,
zomb - zombie;
- **cmdline** - filtrowanie według wiersza poleceń (jest to wyrażenie regularne);
- **zone** - docelowa strefa: *current* (domyślnie) lub *all*. Ten parametr jest obsługiwany tylko w systemie Solaris.

Uwagi:

- Parametry stanu *disk* i *trace* są obsługiwane tylko w systemach Linux, FreeBSD, OpenBSD, NetBSD.
- W systemie Windows obsługiwane są tylko parametry `name` i `user`.
- Gdy ta pozycja jest wywoływana z wiersza poleceń i zawiera parametr wiersza poleceń (na przykład przy użyciu trybu testowego agenta: `zabbix_agentd -t proc.num[,,,apache2]`), zostanie zliczony jeden dodatkowy proces, ponieważ agent policzy samego siebie.
- Jeśli parametr `zone` zostanie ustawiony na `current` (lub domyślny), a agent został skompilowany w systemie Solaris bez obsługi stref, ale działa na nowszym systemie Solaris, w którym strefy są obsługiwane, agent zwróci NOTSUPPORTED (agent nie może ograniczyć wyników tylko do bieżącej strefy). Jednak w takim przypadku *all* jest obsługiwane.
- Zobacz uwagi dotyczące wybierania procesów za pomocą parametrów `name` i `cmdline` (dotyczy tylko systemu Linux).

Przykłady:

```
proc.num[,mysql] #liczba procesów uruchomionych przez użytkownika mysql
proc.num[apache2,www-data] #liczba procesów apache2 uruchomionych przez użytkownika www-data
proc.num[,oracle,sleep,oracleZABBIX] #liczba procesów w stanie sleep uruchomionych przez użytkownika Oracl
```

sensor[device,sensor,<mode>]

 Odczyt czujnika sprzętowego.
 Zwracana wartość: *Float*.
 Obsługiwane platformy: Linux, OpenBSD.

Parametry:

- **device** - nazwa urządzenia;
- **sensor** - nazwa czujnika;
- **mode** - możliwe wartości: *avg*, *max* lub *min*.

Uwagi:

- Odczytuje /proc/sys/dev/sensors w systemie Linux 2.4.
- Odczytuje /sys/class/hwmon w systemie Linux 2.6+. Zobacz bardziej szczegółowy opis pozycji sensor w systemie Linux.
- Odczytuje MIB *hw.sensors* w systemie OpenBSD.
- W systemie Linux 2.4, jeśli określisz mode, wtedy device i sensor są traktowane jako wyrażenia regularne.
- W systemie Linux 2.6+ i OpenBSD lub jeśli mode zostanie pominięty, device i sensor są traktowane dosłownie.

Przykłady:

```
sensor[w83781d-i2c-0-2d,temp1]
sensor[cpu0,temp0] #the temperature of one CPU
sensor["cpu[0-2]$",temp,avg] #the average temperature of the first three CPUs
```

system.boottime

 Czas uruchomienia systemu.
 Zwracana wartość: *Liczba całkowita (znacznik czasu Unix)*.
 Obsługiwane platformy: Linux, FreeBSD, Solaris, MacOS X, OpenBSD, NetBSD.

system.cpu.discovery

 Lista wykrytych procesorów CPU/rdzeni CPU. Używana do wykrywania niskiego poziomu.
 Zwracana wartość: *ciąg JSON*.
 Zobacz obsługiwane platformy.

system.cpu.intr

 Przerwania urządzenia.
 Zwracana wartość: *Liczba całkowita*.
 Obsługiwane platformy: Linux, FreeBSD, Solaris, AIX, OpenBSD, NetBSD.

system.cpu.load[<cpu>,<mode>]

 Obciążenie CPU.
 Zwracana wartość: *Float*.
 Zobacz obsługiwane platformy.

Parametry:

- **cpu** — możliwe wartości: *all* (domyślnie) lub *percpu* (całkowite obciążenie podzielone przez liczbę aktywnych CPU);
- **mode** — możliwe wartości: *avg1* (średnia z jednej minuty, domyślnie), *avg5* lub *avg15*.

Przykład:

```
system.cpu.load[,avg5]
```

system.cpu.num[<type>]

 Liczba procesorów.
 Zwracana wartość: *Integer*.
 Obsługiwane platformy: Linux, FreeBSD, Solaris, HP-UX, AIX, MacOS X, OpenBSD, NetBSD, Windows.

Parametr:

- **type** — możliwe wartości: *online* (domyślnie) lub *max*

Parametr typu *max* jest obsługiwany tylko w systemach Linux, FreeBSD, Solaris, MacOS X.

Przykład:

```
system.cpu.num
```

system.cpu.switches

 Liczba przełączeń kontekstu.
 Zwracana wartość: *Integer*.
 Obsługiwane platformy: Linux, FreeBSD, Solaris, AIX, OpenBSD, NetBSD.

system.cpu.util[<cpu>,<type>,<mode>,<logical or physical>]

 Procent wykorzystania CPU.
 Zwracana wartość: *Float*.
 Obsługiwane platformy: Linux, FreeBSD, Solaris, HP-UX, AIX, OpenBSD, NetBSD, Windows.

Parametry:

- **cpu** - <*numer CPU*> lub *all* (domyślnie);
- **type** - możliwe wartości: *user* (domyślnie), *idle*, *nice*, *system*, *iowait*, *interrupt*, *softirq*, *steal*, *spin* (w OpenBSD), *guest* (w jądrach Linux 2.6.24 i nowszych) lub *guest_nice* (w jądrach Linux 2.6.33 i nowszych);
- **mode** - możliwe wartości: *avg1* (średnia jednominutowa, domyślnie), *avg5* lub *avg15*;
- **logical or physical** - możliwe wartości: *logical* (domyślnie) lub *physical*. Ten parametr jest obsługiwany tylko w AIX.

Uwagi:

- Parametr typu *nice* jest obsługiwany tylko w systemach Linux, FreeBSD, HP-UX, OpenBSD, NetBSD.
- Parametr typu *iowait* jest obsługiwany tylko w systemach Linux 2.6 i nowszych, Solaris, AIX.
- Parametr typu *interrupt* jest obsługiwany tylko w systemach Linux 2.6 i nowszych, FreeBSD, OpenBSD.
- Parametry typu *softirq*, *steal*, *guest*, *guest_nice* są obsługiwane tylko w systemach Linux 2.6 i nowszych.
- Parametry trybu *avg5* i *avg15* są obsługiwane w systemach Linux, FreeBSD, Solaris, HP-UX, AIX, OpenBSD, NetBSD.

Przykład:

```
system.cpu.util[0,user,avg5]
```

system.hostname[<type>,<transform>]

 Nazwa hosta systemu.
 Zwracana wartość: *String*.
 Zobacz obsługiwane platformy.

Parametry:

- **type** - możliwe wartości: *netbios* (domyślnie w systemie Windows), *host* (domyślnie w systemie Linux), *shorthost* (zwraca część nazwy hosta przed pierwszą kropką, pełny ciąg dla nazw bez kropek), *fqdn* (zwraca w pełni kwalifikowaną nazwę domenową, Fully Qualified Domain Name);
- **transform** - możliwe wartości: *none* (domyślnie) lub *lower* (konwertuje na małe litery).

Wartość jest pobierana z `nodename` w danych wyjściowych systemowego API uname().

Przykłady zwracanych wartości:

```
system.hostname → linux-w7x1
system.hostname → example.com
system.hostname[shorthost] → example
system.hostname → WIN-SERV2008-I6
system.hostname[host] → Win-Serv2008-I6LonG
system.hostname[host,lower] → win-serv2008-i6long
system.hostname[fqdn,lower] → blog.zabbix.com
```

system.hw.chassis[<info>]

 Informacje o obudowie.
 Zwracana wartość: *String*.
 Obsługiwane platformy: Linux.

Parametr:

- **info** - możliwe wartości: *full* (domyślnie), *model*, *serial*, *type* lub *vendor*

Uwagi:

- Ten klucz pozycji zależy od dostępności tabeli SMBIOS.
- Nastąpi próba odczytu tabeli DMI z sysfs; jeśli dostęp do sysfs się nie powiedzie, zostanie podjęta próba bezpośredniego odczytu z pamięci.
- Wymagane są **uprawnienia root**, ponieważ wartość jest uzyskiwana przez odczyt z sysfs lub pamięci.

Przykład:

```
system.hw.chassis[full] → Hewlett-Packard HP Pro 3010 Small Form Factor PC CZXXXXXXXX Desktop
```

system.hw.cpu[<cpu>,<info>]

 Informacje o CPU.
 Zwracana wartość: *String* lub *Integer*.
 Obsługiwane platformy: Linux.

Parametry:

- **cpu** — <*numer CPU*> lub *all* (domyślnie);
- **info** — możliwe wartości: *full* (domyślnie), *curfreq*, *maxfreq*, *model* lub *vendor*.

Uwagi:

- Zbiera informacje z `/proc/cpuinfo` oraz `/sys/devices/system/cpu/[cpunum]/cpufreq/cpuinfo_max_freq`.
- Jeśli podano numer CPU oraz *curfreq* lub *maxfreq*, zwracana jest wartość liczbowa (Hz).

Przykład:

```
system.hw.cpu[0,vendor] → AuthenticAMD
```

system.hw.devices[<type>]

 Lista urządzeń PCI lub USB.
 Zwracana wartość: *Tekst*.
 Obsługiwane platformy: Linux.

Parametr:

- **type** - *pci* (domyślnie) lub *usb*

Zwraca dane wyjściowe narzędzia lspci lub lsusb (uruchamianego bez żadnych parametrów).

Przykład:

```
system.hw.devices → 00:00.0 Host bridge: Advanced Micro Devices [AMD] RS780 Host Bridge
```

system.hw.macaddr[<interface>,<format>]

 Lista adresów MAC.
 Zwracana wartość: *String*.
 Obsługiwane platformy: Linux.

Parametry:

- **interface** - *all* (domyślnie) lub regularne wyrażenie;
- **format** - *full* (domyślnie) lub *short*

Uwagi:

- Wyświetla adresy MAC interfejsów, których nazwa pasuje do podanego regularnego wyrażenia `interface` (*all* wyświetla dla wszystkich interfejsów).
- Jeśli `format` jest określony jako *short*, nazwy interfejsów i identyczne adresy MAC nie są wyświetlane.

Przykład:

```
system.hw.macaddr["eth0$",full] → [eth0] 00:11:22:33:44:55
```

system.localtime[<type>]

 Czas systemowy.
 Zwracana wartość: *Integer* — gdy `type` ma wartość *utc*; *String* — gdy `type` ma wartość *local*.
 Zobacz obsługiwane platformy.

Parametry:

- **type** — możliwe wartości: *utc* — (domyślnie) czas od Epoki (00:00:00 UTC, 1 stycznia 1970), mierzony w sekundach, lub *local* — czas w formacie 'yyyy-mm-dd,hh:mm:ss.nnn,+hh:mm'

Musi być używane jako sprawdzenie pasywne dla Zabbix agent; w Zabbix agent 2 może być skonfigurowane jako sprawdzenie aktywne.

Przykład:

```
system.localtime[local] #utwórz pozycję przy użyciu tego klucza, a następnie użyj jej do wyświetlenia czas
```

system.run[command,<mode>]

 Uruchom określone polecenie na hoście.
 Wartość zwracana: wynik polecenia w postaci *tekstu* lub 1 - gdy mode ma wartość *nowait* (niezależnie od wyniku polecenia).
 Zobacz obsługiwane platformy.

Parametry:

- **command** - polecenie do wykonania;
- **mode** - możliwe wartości: *wait* - czekaj na zakończenie wykonania (domyślnie) lub *nowait* - nie czekaj.

Uwagi:

- Ta pozycja jest domyślnie wyłączona. Dowiedz się, jak je włączyć.
- Wartością zwracaną przez pozycję jest standardowe wyjście wraz ze standardowym wyjściem błędów generowanym przez polecenie. Sprawdzanie kodu zakończenia nie jest wykonywane.
- Aby wartość zwracana była poprawnie przetwarzana, musi mieć typ danych `text`. Dozwolony jest również pusty wynik.
- Wartość zwracana jest ograniczona do 16 MB (włącznie z końcowymi białymi znakami, które są obcinane); obowiązują również ograniczenia bazy danych.
- Zobacz także: Wykonywanie poleceń.

Przykład:

```
system.run[ls -l /] #zwraca szczegółową listę plików w katalogu głównym
```

system.stat[resource,<type>]

 Statystyki systemu.
 Zwracana wartość: *Integer* lub *float*.
 Obsługiwane platformy: AIX.

Parametry:

- **ent** - liczba jednostek procesora, do których ta partycja jest uprawniona (float);
- **kthr,<type>** - informacje o stanach wątków jądra:
r - średnia liczba wątków jądra gotowych do uruchomienia (float)
b - średnia liczba wątków jądra umieszczonych w kolejce oczekiwania Menedżera Pamięci Wirtualnej (float)
- **memory,<type>** - informacje o użyciu pamięci wirtualnej i rzeczywistej:
avm - aktywne strony wirtualne (integer)
fre - rozmiar listy wolnych stron (integer)
- **page,<type>** - informacje o błędach stron i aktywności stronicowania:
fi - liczba stron plików wczytanych na sekundę (float)
fo - liczba stron plików zapisanych na sekundę (float)
pi - strony wczytane z przestrzeni stronicowania (float)
po - strony zapisane do przestrzeni stronicowania (float)
fr - zwolnione strony (zastępowanie stron) (float)
sr - strony przeskanowane przez algorytm zastępowania stron (float)
- **faults,<type>** - częstotliwość pułapek i przerwań:
in - przerwania urządzeń (float)
sy - wywołania systemowe (float)
cs - przełączenia kontekstu wątków jądra (float)
- **cpu,<type>** - podział procentowego wykorzystania czasu procesora:
us - czas użytkownika (float)
sy - czas systemowy (float)
id - czas bezczynności (float)
wa - czas bezczynności, podczas którego system miał oczekujące żądania wejścia/wyjścia dysku/NFS (float)
pc - liczba wykorzystanych fizycznych procesorów (float)
ec - procent wykorzystanej przydzielonej mocy obliczeniowej (float)
lbusy - wskazuje procent wykorzystania procesorów logicznych, który wystąpił podczas wykonywania na poziomie użytkownika i systemu (float)
app - wskazuje dostępne procesory fizyczne we wspólnej puli (float)
- **disk,<type>** - statystyki dysku:
bps - wskazuje ilość danych przesłanych (odczytanych lub zapisanych) na dysk w bajtach na sekundę (integer)
tps - wskazuje liczbę transferów na sekundę skierowanych do fizycznego dysku/taśmy (float)

Uwagi:

- Zwróć uwagę na następujące ograniczenia tych pozycji:
 `system.stat[cpu,app]` - obsługiwane tylko w AIX LPAR typu "Shared";
 `system.stat[cpu,ec]` - obsługiwane w AIX LPAR typu "Shared" i "Dedicated" ("Dedicated" zawsze zwraca 100 (procent));
 `system.stat[cpu,lbusy]` - obsługiwane tylko w AIX LPAR typu "Shared";
 `system.stat[cpu,pc]` - obsługiwane w AIX LPAR typu "Shared" i "Dedicated";
 `system.stat[ent]` - obsługiwane w AIX LPAR typu "Shared" i "Dedicated".

system.sw.arch

 Informacja o architekturze oprogramowania.
 Zwracana wartość: *String*.
 Zobacz obsługiwane platformy.

Informacja jest pobierana za pomocą funkcji `uname()`.

Przykład:

```
system.sw.arch → i686
```

system.sw.os[<info>]

 Informacje o systemie operacyjnym.
 Zwracana wartość: *String*.
 Obsługiwane platformy: Linux, Windows.

Parametr:

- **info** - możliwe wartości: *full* (domyślnie), *short* lub *name*

Informacje są pobierane z (należy pamiętać, że nie wszystkie pliki i opcje są obecne we wszystkich dystrybucjach):

- `/proc/version` (*full*) w systemie Linux;
- `/proc/version_signature` (*short*) w systemie Linux;
- parametr PRETTY_NAME z `/etc/os-release` w systemach Linux, które go obsługują, lub `/etc/issue.net` (*name*);
- klucz rejestru `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion` w systemie Windows.

Przykłady:

```
system.sw.os[short] → Ubuntu 2.6.35-28.50-generic 2.6.35.11
system.sw.os[full] → [s|Windows 10 Enterprise 22621.1.asd64fre.ni_release.220506-1250 Build 22621.963]
```

system.sw.os.get

 Szczegółowe informacje o systemie operacyjnym (wersja, typ, nazwa dystrybucji, wersja główna i pomocnicza itp.).
 Zwracana wartość: *ciąg JSON*.
 Obsługiwane platformy: Linux, Windows.

system.sw.packages[<regexp>,<manager>,<format>]

 Lista zainstalowanych pakietów.
 Zwracana wartość: *Tekst*.
 Obsługiwane platformy: Linux.

Parametry:

- **regexp** - *all* (domyślnie) lub regularne wyrażenie;
- **manager** - *all* (domyślnie) lub menedżer pakietów;
- **format** - *full* (domyślnie) lub *short*.

Uwagi:

- Wyświetla (alfabetycznie) zainstalowane pakiety, których nazwa pasuje do podanego regularnego wyrażenia (*all* wyświetla wszystkie).
- Obsługiwane menedżery pakietów (wykonywane polecenie):
  - dpkg (dpkg --get-selections)
  - pkgtool (ls /var/log/packages)
  - rpm (rpm -qa)
  - pacman (pacman -Q)
portage
- Jeśli parametr `format` ma wartość *full*, pakiety są grupowane według menedżerów pakietów (każdy menedżer w osobnym wierszu rozpoczynającym się od jego nazwy w nawiasach kwadratowych).
- Jeśli parametr `format` ma wartość *short*, pakiety nie są grupowane i są wyświetlane w jednym wierszu.

Przykład:

```
system.sw.packages[mini,dpkg,short] → python-minimal, python2.6-minimal, ubuntu-minimal
```

system.sw.packages.get[<regexp>,<manager>]

 Szczegółowa lista zainstalowanych pakietów.
 Wartość zwracana: *ciąg JSON*.
 Obsługiwane platformy: Linux.

Parametry:

- **regexp** — *all* (domyślnie) lub regularne wyrażenie;
- **manager** — *all* (domyślnie) lub menedżer pakietów (możliwe wartości: *rpm*, *dpkg*, *pkgtool*, *pacman* lub *portage*).

Uwagi:

- Zwraca niesformatowany JSON z zainstalowanymi pakietami, których nazwa pasuje do podanego wyrażenia regularnego.
- Dane wyjściowe są tablicą obiektów, z których każdy zawiera następujące klucze: name, manager, version, size, architecture, buildtime oraz installtime (zobacz więcej szczegółów).

system.swap.in[<device>,<type>]

 Statystyki swap-in (z urządzenia do pamięci).
 Zwracana wartość: *Integer*.
 Obsługiwane platformy: Linux, FreeBSD, OpenBSD.

Parametry:

- **device** - określa urządzenie używane do swapowania (tylko Linux) lub *all* (domyślnie);

- **type** - możliwe wartości: *count* (liczba operacji swap-in, domyślnie na platformach innych niż Linux), *sectors* (sektory przeniesione do pamięci), lub *pages* (strony przeniesione do pamięci, domyślnie w systemie Linux).

Uwagi:

- Źródłem tych informacji są:
  - `/proc/swaps`, `/proc/partitions`, `/proc/stat` (Linux 2.4)
  - `/proc/swaps`, `/proc/diskstats`, `/proc/vmstat` (Linux 2.6)
- Należy pamiętać, że parametr *pages* będzie działał tylko wtedy, gdy urządzenie nie zostało określone.
- Parametr typu *sectors* jest obsługiwany tylko w systemie Linux.

Przykład:

```
system.swap.in[,pages]
```

system.swap.out[<device>,<type>]

 Statystyki swap-out (z pamięci na urządzenie).
 Zwracana wartość: *Integer*.
 Obsługiwane platformy: Linux, FreeBSD, OpenBSD.

Parametry:

- **device** - określa urządzenie używane do swapowania (tylko Linux) lub *all* (domyślnie);
- **type** - możliwe wartości: *count* (liczba operacji swap-out, domyślnie na platformach innych niż Linux), *sectors* (sektory przeniesione do obszaru wymiany) lub *pages* (strony przeniesione do obszaru wymiany, domyślnie w systemie Linux).

Uwagi:

- Źródłem tych informacji są:
`/proc/swaps`, `/proc/partitions`, `/proc/stat` (Linux 2.4)
`/proc/swaps`, `/proc/diskstats`, `/proc/vmstat` (Linux 2.6)
- Należy pamiętać, że *pages* będzie działać tylko wtedy, gdy nie określono urządzenia.
- Parametr typu *sectors* jest obsługiwany tylko w systemie Linux.

Przykład:

```
system.swap.out[,pages]
```

system.swap.size[<device>,<type>]

 Rozmiar przestrzeni wymiany w bajtach lub jako procent całości.
 Zwracana wartość: *Integer* - dla bajtów; *Float* - dla wartości procentowej.
 Obsługiwane platformy: Linux, FreeBSD, Solaris, AIX, OpenBSD, Windows.

Parametry:

- **device** - określa urządzenie używane do swapu (tylko FreeBSD) lub *all* (domyślnie);
- **type** - możliwe wartości: *free* (wolna przestrzeń wymiany, domyślnie), *pfree* (wolna przestrzeń wymiany, w procentach), *pused* (używana przestrzeń wymiany, w procentach), *total* (całkowita przestrzeń wymiany) lub *used* (używana przestrzeń wymiany).

Uwagi:

- Należy pamiętać, że *pfree*, *pused* nie są obsługiwane w systemie Windows, jeśli rozmiar swapu wynosi 0.
- Jeśli urządzenie nie zostanie określone, agent Zabbix uwzględni tylko urządzenia (pliki) swapu, a pamięć fizyczna zostanie pominięta. Na przykład w systemach Solaris polecenie `swap -s` uwzględnia część pamięci fizycznej oraz urządzenia swapu (w przeciwieństwie do `swap -l`).

Przykład:

```
system.swap.size[,pfree] → procent wolnej przestrzeni wymiany
```

system.uname

 Identyfikacja systemu.
 Zwracana wartość: *String*.
 Zobacz obsługiwane platformy.

Uwagi:

- W systemach UNIX wartość tej pozycji jest uzyskiwana za pomocą wywołania systemowego uname().
- W systemie Windows pozycja zwraca architekturę systemu operacyjnego, natomiast w systemach UNIX zwraca architekturę CPU.

Przykłady:

```
system.uname → FreeBSD localhost 4.2-RELEASE FreeBSD 4.2-RELEASE #0: Mon Nov i386
system.uname → Windows ZABBIX-WIN 6.0.6001 Microsoft® Windows Server® 2008 Standard Service Pack 1 x86
```

system.uptime

 Czas działania systemu w sekundach.
 Zwracana wartość: *Integer*.
 Obsługiwane platformy: Linux, FreeBSD, Solaris, AIX, MacOS X, OpenBSD, NetBSD, Windows.

W konfiguracji pozycji użyj jednostek **s** lub **uptime**, aby uzyskać czytelne wartości.

system.users.num

 Liczba zalogowanych użytkowników.
 Wartość zwracana: *Integer*.
 Zobacz obsługiwane platformy.

Do uzyskania tej wartości po stronie agent używane jest polecenie **who**.

vfs.dev.discovery

 Lista urządzeń blokowych i ich typów. Używane do wykrywania niskiego poziomu.
 Wartość zwracana: *ciąg JSON*.
 Obsługiwane platformy: Linux.

vfs.dev.read[<device>,<type>,<mode>]

 Statystyki odczytu dysku.
 Zwracana wartość: *Integer* - gdy `type` ma wartość *sectors*, *operations*, *bytes*; *Float* - gdy `type` ma wartość *sps*, *ops*, *bps*.
 Obsługiwane platformy: Linux, FreeBSD, Solaris, AIX, OpenBSD.

Parametry:

- **device** - urządzenie dyskowe (domyślnie *all* [3]);
- **type** - możliwe wartości: *sectors*, *operations*, *bytes*, *sps*, *ops* lub *bps* (*sps*, *ops*, *bps* oznaczają odpowiednio: sektory, operacje, bajty na sekundę);
- **mode** - możliwe wartości: *avg1* (średnia jednominutowa, domyślnie), *avg5* lub *avg15*. Ten parametr jest obsługiwany tylko wtedy, gdy `type` ma jedną z wartości: sps, ops, bps.

Uwagi:

- W przypadku użycia interwału aktualizacji wynoszącego trzy godziny lub więcej[2], ta pozycja będzie zawsze zwracać '0'.
- Parametry typu *sectors* i *sps* są obsługiwane tylko w systemie Linux.
- Parametr typu *ops* jest obsługiwany tylko w systemach Linux i FreeBSD.
- Parametr typu *bps* jest obsługiwany tylko w systemie FreeBSD.
- Parametr typu *bytes* jest obsługiwany tylko w systemach FreeBSD, Solaris, AIX, OpenBSD.
- Parametr `mode` jest obsługiwany tylko w systemach Linux i FreeBSD.
- Można używać względnych nazw urządzeń (na przykład `sda`), jak również opcjonalnego prefiksu `/dev/` (na przykład `/dev/sda`).
- Obsługiwane są woluminy logiczne LVM.
- Domyślne wartości parametru 'type' dla różnych systemów operacyjnych:
  - *AIX* - operations
  - *FreeBSD* - bps
  - *Linux* - sps
  - *OpenBSD* - operations
  - *Solaris* - bytes
- *sps*, *ops* i *bps* na obsługiwanych platformach są ograniczone do 1024 urządzeń (1023 indywidualnych i jedno dla *all*).

Przykład:

```
vfs.dev.read[,operations]
```

vfs.dev.write[<device>,<type>,<mode>]

 Statystyki zapisu na dysku.
 Zwracana wartość: *Integer* - gdy `type` ma wartość *sectors*, *operations*, *bytes*; *Float* - gdy `type` ma wartość *sps*, *ops*, *bps*.
 Obsługiwane platformy: Linux, FreeBSD, Solaris, AIX, OpenBSD.

Parametry:

- **device** - urządzenie dyskowe (domyślnie *all* [3]);
- **type** - możliwe wartości: *sectors*, *operations*, *bytes*, *sps*, *ops* lub *bps* (*sps*, *ops*, *bps* oznaczają odpowiednio: sektory, operacje, bajty na sekundę);
- **mode** - możliwe wartości: *avg1* (średnia jednominutowa, domyślnie), *avg5* lub *avg15*. Ten parametr jest obsługiwany tylko wtedy, gdy `type` ma jedną z wartości: sps, ops, bps.

Uwagi:

- W przypadku użycia interwału aktualizacji wynoszącego trzy godziny lub więcej[2], ta pozycja zawsze będzie zwracać '0'.
- Parametry typu *sectors* i *sps* są obsługiwane tylko w systemie Linux.
- Parametr typu *ops* jest obsługiwany tylko w systemach Linux i FreeBSD.
- Parametr typu *bps* jest obsługiwany tylko w systemie FreeBSD.

- Parametr typu *bytes* jest obsługiwany tylko w systemach FreeBSD, Solaris, AIX, OpenBSD.
- Parametr `mode` jest obsługiwany tylko w systemach Linux i FreeBSD.
- Można używać względnych nazw urządzeń (na przykład `sda`), a także opcjonalnego prefiksu `/dev/` (na przykład `/dev/sda`).
- Woluminy logiczne LVM są obsługiwane.
- Domyślne wartości parametru 'type' dla różnych systemów operacyjnych:
  - *AIX* - operations
  - *FreeBSD* - bps
  - *Linux* - sps
  - *OpenBSD* - operations
  - *Solaris* - bytes
- *sps*, *ops* i *bps* na obsługiwanych platformach są ograniczone do 1024 urządzeń (1023 indywidualnych i jedno dla *all*).

Przykład:

```
vfs.dev.write[,operations]
```

vfs.dir.count[dir,<regex incl>,<regex excl>,<types incl>,<types excl>,<max depth>,<min size>,<max size>,<min age>,<max age>,<regex excl dir>]

 Liczba wpisów katalogu.
 Zwracana wartość: *Integer*.
 Zobacz obsługiwane platformy.

Parametry:

- **dir** - ścieżka bezwzględna do katalogu;
- **regex incl** - wyrażenie regularne opisujące wzorzec nazwy encji (pliku, katalogu, dowiązania symbolicznego), które mają zostać uwzględnione; jeśli puste, uwzględniane są wszystkie (wartość domyślna);
- **regex excl** - wyrażenie regularne opisujące wzorzec nazwy encji (pliku, katalogu, dowiązania symbolicznego), które mają zostać wykluczone; jeśli puste, nic nie jest wykluczane (wartość domyślna);
- **types incl** - typy wpisów katalogu do zliczania, możliwe wartości: *file* - zwykły plik, *dir* - podkatalog, *sym* - dowiązanie symboliczne, *sock* - gniazdo, *bdev* - urządzenie blokowe, *cdev* - urządzenie znakowe, *fifo* - FIFO, *dev* - synonim "bdev,cdev", *all* - wszystkie typy (domyślnie), tj. "file,dir,sym,sock,bdev,cdev,fifo". Wiele typów musi być oddzielonych przecinkiem i ujętych w cudzysłów.
- **types excl** - typy wpisów katalogu (zobacz `types incl`), które NIE mają być zliczane. Jeśli jakiś typ wpisu występuje zarówno w `types incl`, jak i `types excl`, wpisy katalogu tego typu NIE są zliczane.
- **max depth** - maksymalna głębokość przeszukiwania podkatalogów:
-1 (domyślnie) - bez ograniczeń,
0 - bez schodzenia do podkatalogów.
- **min size** - minimalny rozmiar (w bajtach) pliku, aby został zliczony. Mniejsze pliki nie będą zliczane. Można używać sufiksów pamięci.
- **max size** - maksymalny rozmiar (w bajtach) pliku, aby został zliczony. Większe pliki nie będą zliczane. Można używać sufiksów pamięci.
- **min age** - minimalny wiek (w sekundach) wpisu katalogu, aby został zliczony. Nowsze wpisy nie będą zliczane. Można używać sufiksów czasu.
- **max age** - maksymalny wiek (w sekundach) wpisu katalogu, aby został zliczony. Wpisy starsze oraz o dokładnie takim wieku nie będą zliczane (czas modyfikacji). Można używać sufiksów czasu.
- **regex excl dir** - wyrażenie regularne opisujące wzorzec nazwy katalogu, który ma zostać wykluczony. Cała zawartość katalogu zostanie wykluczona (w przeciwieństwie do regex_excl)

Uwagi:

- W systemie Windows ta pozycja podąża za ścieżkami UNC, co może stanowić zagrożenie bezpieczeństwa.
- Zmienne środowiskowe, np. %APP_HOME%, $HOME i %TEMP%, nie są obsługiwane.
- Pseudokatalogi "." i ".." nigdy nie są zliczane.
- Dowiązania symboliczne nigdy nie są śledzone podczas przechodzenia po katalogach.
- Zarówno `regex incl`, jak i `regex excl` są stosowane do plików i katalogów podczas obliczania liczby wpisów, ale są ignorowane przy wybieraniu podkatalogów do przeszukiwania (jeśli `regex incl` ma wartość "(?i)^.+\.zip$" i `max depth` nie jest ustawione, wtedy wszystkie podkatalogi zostaną przeszukane, ale zliczone zostaną tylko pliki typu zip).
- Czas wykonania jest ograniczony przez wartość timeout w konfiguracji agent (3 sek.). Ponieważ przeszukiwanie dużych katalogów może trwać dłużej, żadne dane nie zostaną zwrócone, a pozycja stanie się nieobsługiwana. Częściowy wynik zliczania nie zostanie zwrócony.
- Przy filtrowaniu według rozmiaru tylko zwykłe pliki mają znaczące rozmiary. W systemach Linux i BSD katalogi również mają rozmiary różne od zera (zwykle kilka KB). Urządzenia mają rozmiar zero, np. rozmiar **/dev/sda1** nie odzwierciedla rozmiaru odpowiedniej partycji. Dlatego przy używaniu <min_size> i <max_size> zaleca się określenie <types_incl> jako "*file*", aby uniknąć niespodzianek.

Przykłady:

```
vfs.dir.count[/dev] #monitoruje liczbę urządzeń w /dev (Linux)
vfs.dir.count["C:\Users\ADMINI~1\AppData\Local\Temp"] #monitoruje liczbę plików w katalogu tymczasowym
```

vfs.dir.get[dir,<regex incl>,<regex excl>,<types incl>,<types excl>,<max depth>,<min size>,<max size>,<min age>,<max age>,<regex excl dir>]

 Lista wpisów katalogu.
 Zwracana wartość: *ciąg JSON*.
 Zobacz obsługiwane platformy.

Parametry:

- **dir** - ścieżka bezwzględna do katalogu;
- **regex incl** - regularne wyrażenie opisujące wzorzec nazwy encji (pliku, katalogu, dowiązania symbolicznego), która ma zostać uwzględniona; jeśli puste, uwzględniane są wszystkie (wartość domyślna);
- **regex excl** - regularne wyrażenie opisujące wzorzec nazwy encji (pliku, katalogu, dowiązania symbolicznego), która ma zostać wykluczona; jeśli puste, nic nie jest wykluczane (wartość domyślna);
- **types incl** - typy wpisów katalogu do wyświetlenia, możliwe wartości: *file* - zwykły plik, *dir* - podkatalog, *sym* - dowiązanie symboliczne, *sock* - gniazdo, *bdev* - urządzenie blokowe, *cdev* - urządzenie znakowe, *fifo* - FIFO, *dev* - synonim „bdev,cdev", *all* - wszystkie typy (domyślnie), tj. „file,dir,sym,sock,bdev,cdev,fifo". Wiele typów musi być oddzielonych przecinkiem i ujętych w cudzysłów.
- **types excl** - typy wpisów katalogu (zobacz `types incl`), które NIE mają być wyświetlane. Jeśli jakiś typ wpisu występuje zarówno w `types incl`, jak i `types excl`, wpisy katalogu tego typu NIE będą wyświetlane.
- **max depth** - maksymalna głębokość przeszukiwania podkatalogów:
-1 (domyślnie) - bez ograniczeń,
0 - bez schodzenia do podkatalogów.
- **min size** - minimalny rozmiar (w bajtach) pliku, który ma zostać wyświetlony. Mniejsze pliki nie będą wyświetlane. Można używać sufiksów pamięci.
- **max size** - maksymalny rozmiar (w bajtach) pliku, który ma zostać wyświetlony. Większe pliki nie będą wyświetlane. Można używać sufiksów pamięci.
- **min age** - minimalny wiek (w sekundach) wpisu katalogu, który ma zostać wyświetlony. Nowsze wpisy nie będą wyświetlane. Można używać sufiksów czasu.
- **max age** - maksymalny wiek (w sekundach) wpisu katalogu, który ma zostać wyświetlony. Wpisy tak stare i starsze nie będą wyświetlane (czas modyfikacji). Można używać sufiksów czasu.
- **regex excl dir** - regularne wyrażenie opisujące wzorzec nazwy katalogu, który ma zostać wykluczony. Cała zawartość katalogu zostanie wykluczona (w przeciwieństwie do `regex excl`)

Uwagi:

- W systemie Windows ta pozycja podąża za ścieżkami UNC, co może stanowić zagrożenie bezpieczeństwa.
- Zmienne środowiskowe, np. %APP_HOME%, $HOME i %TEMP%, nie są obsługiwane.
- Pseudokatalogi "." i ".." nigdy nie są wyświetlane.
- Dowiązania symboliczne nigdy nie są śledzone podczas przeszukiwania katalogów.
- Zarówno `regex incl`, jak i `regex excl` są stosowane do plików i katalogów podczas generowania listy wpisów, ale są ignorowane przy wybieraniu podkatalogów do przeszukania (jeśli `regex incl` ma wartość "(?i)^.+\.zip$" i `max depth` nie jest ustawione, wtedy wszystkie podkatalogi zostaną przeszukane, ale zliczane będą tylko pliki typu zip).
- Czas wykonania jest ograniczony przez wartość timeout w konfiguracji agent. Ponieważ przeszukiwanie dużych katalogów może trwać dłużej, żadne dane nie zostaną zwrócone, a pozycja stanie się nieobsługiwana. Częściowa lista nie zostanie zwrócona.
- Podczas filtrowania według rozmiaru tylko zwykłe pliki mają sensowne rozmiary. W systemach Linux i BSD katalogi również mają rozmiary różne od zera (zwykle kilka KB). Urządzenia mają rozmiar zero, np. rozmiar **/dev/sda1** nie odzwierciedla rozmiaru odpowiedniej partycji. Dlatego przy używaniu `min size` i `max size` zaleca się ustawienie `types incl` na "*file*", aby uniknąć niespodzianek.

Przykłady:

```
vfs.dir.get[/dev] #pobiera listę urządzeń w /dev (Linux)
vfs.dir.get["C:\Users\ADMINI~1\AppData\Local\Temp"] #pobiera listę plików w katalogu tymczasowym
```

vfs.dir.size[dir,<regex incl>,<regex excl>,<mode>,<max depth>,<regex excl dir>]

 Rozmiar katalogu (w bajtach).
 Zwracana wartość: *Integer*.
 Obsługiwane platformy: Linux, Windows. Ta pozycja może działać także na innych platformach typu UNIX.

Parametry:

- **dir** - ścieżka bezwzględna do katalogu;
- **regex incl** - wyrażenie regularne opisujące wzorzec nazwy encji (pliku, katalogu, dowiązania symbolicznego), która ma zostać uwzględniona; jeśli puste, uwzględniane są wszystkie (wartość domyślna);
- **regex excl** - wyrażenie regularne opisujące wzorzec nazwy encji (pliku, katalogu, dowiązania symbolicznego), która ma zostać wykluczona; jeśli puste, nic nie jest wykluczane (wartość domyślna);

- **mode** - możliwe wartości: *apparent* (domyślnie) - pobiera pozorne rozmiary plików zamiast użycia dysku (działa jak `du -sb dir`), *disk* - pobiera użycie dysku (działa jak `du -s -B1 dir`). W przeciwieństwie do polecenia du, pozycja vfs.dir.size uwzględnia ukryte pliki przy obliczaniu rozmiaru katalogu (działa jak `du -sb .[^.]* *` w obrębie dir).
- **max depth** - maksymalna głębokość przeszukiwanych podkatalogów: **-1** (domyślnie) - bez ograniczeń, **0** - bez schodzenia do podkatalogów.
- **regex excl dir** - wyrażenie regularne opisujące wzorzec nazwy katalogu, który ma zostać wykluczony. Cała zawartość katalogu zostanie wykluczona (w przeciwieństwie do `regex excl`)

Uwagi:

- W systemie Windows ta pozycja obsługuje ścieżki UNC, co może stanowić zagrożenie bezpieczeństwa.
- Obliczane są tylko katalogi, do których użytkownik *zabbix* ma co najmniej uprawnienie odczytu. Dla katalogów mających tylko uprawnienie odczytu obliczany jest rozmiar samego katalogu. Dla katalogów mających uprawnienia odczytu i wykonania obliczany jest rozmiar wraz z zawartością.
- W przypadku dużych katalogów lub wolnych dysków dla tej pozycji może wystąpić przekroczenie czasu z powodu ustawienia Timeout w plikach konfiguracyjnych agent oraz serwer/proxy. W razie potrzeby zwiększ wartości timeout.
- Limit rozmiaru pliku zależy od obsługi dużych plików.

Przykłady:

```
vfs.dir.size[/tmp,log] #oblicza rozmiar wszystkich plików w /tmp zawierających 'log' w nazwie
vfs.dir.size[/tmp,log,^.+\.old$] #oblicza rozmiar wszystkich plików w /tmp zawierających 'log' w nazwie, z
```

vfs.file.cksum[file,<mode>]

 Suma kontrolna pliku, obliczana za pomocą algorytmu UNIX cksum.
 Zwracana wartość: *Integer* - gdy `mode` to *crc32*, *String* - gdy `mode` to *md5*, *sha256*.
 Zobacz obsługiwane platformy.

Parametry:

- **file** - pełna ścieżka do pliku;
- **mode** - *crc32* (domyślnie), *md5* lub *sha256*.

Uwagi:

- W systemie Windows ta pozycja podąża za ścieżkami UNC, co może stanowić zagrożenie bezpieczeństwa.
- Limit rozmiaru pliku zależy od obsługi dużych plików.

Przykład:

```
vfs.file.cksum[/etc/passwd]
```

Przykłady zwracanych wartości (odpowiednio crc32/md5/sha256):

```
675436101
9845acf68b73991eb7fd7ee0ded23c44
ae67546e4aac995e5c921042d0cf0f1f7147703aa42bfbfb65404b30f238f2dc
```

vfs.file.contents[file,<encoding>]

 Pobieranie zawartości pliku[7].
 Zwracana wartość: *Tekst*.
 Zobacz obsługiwane platformy.

Parametry:

- **file** - pełna ścieżka do pliku;
- **encoding** - identyfikator strony kodowej identifier.

Uwagi:

- W systemie Windows ta pozycja podąża za ścieżkami UNC, co może stanowić zagrożenie bezpieczeństwa.
- Zwracana wartość jest ograniczona do 16 MB (wliczając końcowe białe znaki, które są obcinane); obowiązują również ograniczenia bazy danych.
- Pusty ciąg jest zwracany, jeśli plik jest pusty lub zawiera wyłącznie znaki LF/CR.
- Znacznik kolejności bajtów (BOM) jest wykluczany z danych wyjściowych.

Przykład:

```
vfs.file.contents[/etc/passwd]
```

vfs.file.exists[file,<types incl>,<types excl>]

 Sprawdza, czy plik istnieje.
 Zwracana wartość: 0 - nie znaleziono; 1 - istnieje plik określonego typu.
 Zobacz obsługiwane platformy.

Parametry:

- **file** - pełna ścieżka do pliku;
- **types incl** - lista typów plików do uwzględnienia, możliwe wartości: *file* (zwykły plik, domyślnie, jeśli types_excl nie jest ustawiony), *dir* (katalog), *sym* (dowiązanie symboliczne), *sock* (gniazdo), *bdev* (urządzenie blokowe), *cdev* (urządzenie znakowe), *fifo* (FIFO), *dev* (synonim „bdev,cdev"), *all* (wszystkie wymienione typy, domyślnie, jeśli types_excl jest ustawiony).
- **types excl** - lista typów plików do wykluczenia, możliwe wartości jak dla types_incl (domyślnie żadne typy nie są wykluczane)

Uwagi:

- W systemie Windows ta pozycja podąża za ścieżkami UNC, co może stanowić zagrożenie bezpieczeństwa.
- Wiele typów musi być oddzielonych przecinkiem, a cały zestaw musi być ujęty w cudzysłowy "".
- Jeśli ten sam typ występuje zarówno w <types_incl>, jak i <types_excl>, pliki tego typu są wykluczane.
- Limit rozmiaru pliku zależy od obsługi dużych plików.

Przykłady:

```
vfs.file.exists[/tmp/application.pid]
vfs.file.exists[/tmp/application.pid,"file,dir,sym"]
vfs.file.exists[/tmp/application_dir,dir]
```

vfs.file.get[file]

 Zwraca informacje o pliku.
 Wartość zwracana: *ciąg JSON*.
 Zobacz obsługiwane platformy.

Parametr:

- **file** — pełna ścieżka do pliku

Uwagi:

- W systemie Windows ta pozycja obsługuje ścieżki UNC, co może stanowić zagrożenie bezpieczeństwa.
- Obsługiwane typy plików w systemach typu UNIX: plik zwykły, katalog, dowiązanie symboliczne, gniazdo, urządzenie blokowe, urządzenie znakowe, FIFO.
- Limit rozmiaru pliku zależy od obsługi dużych plików.

Przykład:

```
vfs.file.get[/etc/passwd] #zwraca JSON z informacjami o pliku /etc/passwd (typ, użytkownik, uprawnienia, S
```

vfs.file.md5sum[file]

 Suma kontrolna MD5 pliku.
 Zwracana wartość: Ciąg znaków (skrót MD5 pliku).
 Zobacz obsługiwane platformy.

Parametr:

- **file** - pełna ścieżka do pliku

Komentarze:

- W systemie Windows ta pozycja obsługuje ścieżki UNC, co może stanowić zagrożenie bezpieczeństwa.
- Limit rozmiaru pliku zależy od obsługi dużych plików.

Przykład:

```
vfs.file.md5sum[/usr/local/etc/zabbix_agentd.conf]
```

Przykład zwracanej wartości:

```
b5052decb577e0fffd622d6ddc017e82
```

vfs.file.owner[file,<ownertype>,<resulttype>]

 Pobiera właściciela pliku.
 Zwracana wartość: *String*.
 Zobacz obsługiwane platformy.

Parametry:

- **file** - pełna ścieżka do pliku;
- **ownertype** - *user* (domyślnie) lub *group* (tylko Unix);
- **resulttype** - *name* (domyślnie) lub *id*; dla id - zwraca uid/gid w systemie Unix, SID w systemie Windows.

Uwagi:

- W systemie Windows ta pozycja podąża za ścieżkami UNC, co może stanowić zagrożenie bezpieczeństwa.
- Limit rozmiaru pliku zależy od obsługi dużych plików.

Przykłady:

```
vfs.file.owner[/tmp/zabbix_server.log] #zwraca właściciela pliku /tmp/zabbix_server.log
vfs.file.owner[/tmp/zabbix_server.log,,id] #zwraca identyfikator właściciela pliku /tmp/zabbix_server.log
```

vfs.file.permissions[file]

 Zwraca 4-cyfrowy ciąg zawierający liczbę ósemkową z uprawnieniami UNIX.
 Zwracana wartość: *String*.
 Obsługiwane platformy: Linux. Pozycja może działać na innych platformach typu UNIX.

Parametry:

- **file** — pełna ścieżka do pliku

Limit rozmiaru pliku zależy od obsługi dużych plików.

Przykład:

```
vfs.file.permissions[/etc/passwd] #zwraca uprawnienia dla /etc/passwd, na przykład '0644'
```

vfs.file.regexp[file,regexp,<encoding>,<start line>,<end line>,<output>]

 Pobiera ciąg znaków z pliku[7].
 Wartość zwracana: Wiersz zawierający dopasowany ciąg znaków lub wartość określona przez opcjonalny parametr `output`.
 Zobacz obsługiwane platformy.

Parametry:

- **file** - pełna ścieżka do pliku;
- **regexp** - wyrażenie regularne opisujące wymagany wzorzec;
- **encoding** - identyfikator strony kodowej;
- **start line** - numer pierwszego wiersza do przeszukania (domyślnie pierwszy wiersz pliku);
- **end line** - numer ostatniego wiersza do przeszukania (domyślnie ostatni wiersz pliku);
- **output** - opcjonalny szablon formatowania danych wyjściowych. Sekwencja ucieczki **\0** jest zastępowana dopasowaną częścią tekstu (od pierwszego znaku, od którego zaczyna się dopasowanie, do znaku, na którym dopasowanie się kończy), natomiast sekwencja ucieczki **\N** (gdzie N=1...9) jest zastępowana N-tą dopasowaną grupą (lub pustym ciągiem, jeśli N przekracza liczbę przechwyconych grup).

Uwagi:

- W systemie Windows ta pozycja obsługuje ścieżki UNC, co może stanowić zagrożenie bezpieczeństwa.
- Limit rozmiaru pliku zależy od obsługi dużych plików.
- Zwracany jest tylko pierwszy pasujący wiersz.
- Jeśli żaden wiersz nie pasuje do wyrażenia, zwracany jest pusty ciąg.
- Znacznik kolejności bajtów (BOM) jest wykluczany z danych wyjściowych.
- Wyodrębnianie zawartości przy użyciu parametru `output` odbywa się po stronie agent.

Przykłady:

```
vfs.file.regexp[/etc/passwd,zabbix]
vfs.file.regexp[/path/to/some/file,"([0-9]+)$",,3,5,\1]
vfs.file.regexp[/etc/passwd,"^zabbix:.:([0-9]+)",,,,\1] → pobranie identyfikatora użytkownika *zabbix*
```

vfs.file.regmatch[file,regexp,<encoding>,<start line>,<end line>]

 Znajduje ciąg znaków w pliku[7].
 Zwracane wartości: 0 - nie znaleziono dopasowania; 1 - znaleziono.
 Zobacz obsługiwane platformy.

Parametry:

- **file** - pełna ścieżka do pliku;
- **regexp** - regularne wyrażenie opisujące wymagany wzorzec;
- **encoding** - identyfikator strony kodowej;
- **start line** - numer pierwszego wiersza do przeszukania (domyślnie pierwszy wiersz pliku);
- **end line** - numer ostatniego wiersza do przeszukania (domyślnie ostatni wiersz pliku).

Uwagi:

- W systemie Windows ta pozycja obsługuje ścieżki UNC, co może stanowić zagrożenie bezpieczeństwa.
- Limit rozmiaru pliku zależy od obsługi dużych plików.
- Znacznik kolejności bajtów (BOM) jest ignorowany.

Przykład:

```
vfs.file.regmatch[/var/log/app.log,error]
```

vfs.file.size[file,<mode>]

 Rozmiar pliku (w bajtach).
 Zwracana wartość: *Integer*.
 Zobacz obsługiwane platformy.

Parametry:

- **file** - pełna ścieżka do pliku;
- **mode** - możliwe wartości: *bytes* (domyślnie) lub *lines* (liczone są również puste wiersze).

Uwagi:

- W systemie Windows ta pozycja podąża za ścieżkami UNC, co może stanowić zagrożenie bezpieczeństwa.
- Plik musi mieć uprawnienia do odczytu dla użytkownika *zabbix*.
- Limit rozmiaru pliku zależy od obsługi dużych plików.

Przykład:

```
vfs.file.size[/var/log/syslog]
```

vfs.file.time[file,<mode>]

 Informacje o czasie pliku.
 Zwracana wartość: *Integer* (znacznik czasu Unix).
 Zobacz obsługiwane platformy.

Parametry:

- **file** - pełna ścieżka do pliku;
- **mode** - możliwe wartości:
modify (domyślnie) - czas ostatniej modyfikacji zawartości pliku,
access - czas ostatniego odczytu pliku,
change - czas ostatniej zmiany właściwości pliku

Uwagi:

- W systemie Windows ta pozycja obsługuje ścieżki UNC, co może stanowić zagrożenie bezpieczeństwa.
- Limit rozmiaru pliku zależy od obsługi dużych plików.

Przykład:

```
vfs.file.time[/etc/passwd,modify]
```

vfs.fs.discovery

 Lista zamontowanych systemów plików wraz z ich typem i opcjami montowania. Używana do wykrywania niskiego poziomu.
 Zwracana wartość: *ciąg JSON*.
 Obsługiwane platformy: Linux, FreeBSD, Solaris, HP-UX, AIX, MacOS X, OpenBSD, NetBSD, Windows.

vfs.fs.get

 Lista zamontowanych systemów plików wraz z ich typem, dostępnym miejscem na dysku, statystykami inode oraz opcjami montowania. Może być używana do wykrywania niskiego poziomu.
 Zwracana wartość: *ciąg JSON*.
 Obsługiwane platformy: Linux, FreeBSD, Solaris, HP-UX, AIX, MacOS X, OpenBSD, NetBSD, Windows.

Uwagi:

- Systemy plików z liczbą inode równą zero, co może mieć miejsce w przypadku systemów plików z dynamicznymi inode (np. btrfs), są również raportowane.
- Zobacz także: Wykrywanie zamontowanych systemów plików.

vfs.fs.inode[fs,<mode>]

 Liczba lub wartość procentowa inode'ów.
 Zwracana wartość: *Integer* - dla liczby; *Float* - dla wartości procentowej.
 Zobacz obsługiwane platformy.

Parametry:

- **fs** - system plików;
- **mode** - możliwe wartości: *total* (domyślnie), *free*, *used*, *pfree* (wolne, procentowo) lub *pused* (użyte, procentowo).

Jeśli liczba inode'ów jest równa zero, co może mieć miejsce w przypadku systemów plików z dynamicznymi inode'ami (np. btrfs), wartości pfree/pused będą raportowane odpowiednio jako „100" i „0".

Przykład:

```
vfs.fs.inode[/,pfree]
```

vfs.fs.size[fs,<mode>]

 Miejsce na dysku w bajtach lub jako wartość procentowa całkowitej pojemności.
 Zwracana wartość: *Integer* - dla bajtów; *Float* - dla wartości procentowej.
 Zobacz obsługiwane platformy.

Parametry:

- **fs** - system plików;
- **mode** - możliwe wartości: *total* (domyślnie), *free*, *used*, *pfree* (wolne, procentowo) lub *pused* (użyte, procentowo).

Uwagi:

- Jeśli system plików nie jest zamontowany, zwracany jest rozmiar lokalnego systemu plików, w którym znajduje się punkt montowania.
- Uwzględniana jest zarezerwowana przestrzeń systemu plików i nie jest ona wliczana przy użyciu trybu *free*.

Przykład:

```
vfs.fs.size[/tmp,free]
```

vm.memory.size[<mode>]

 Rozmiar pamięci w bajtach lub jako wartość procentowa całkowitej pamięci.
 Zwracana wartość: *Integer* - dla bajtów; *Float* - dla wartości procentowej.
 Zobacz obsługiwane platformy.

Parametr:

- **mode** - możliwe wartości: *total* (domyślnie), *active*, *anon*, *buffers*, *cached*, *exec*, *file*, *free*, *inactive*, *pinned*, *shared*, *slab*, *wired*, *used*, *pused* (używana, wartość procentowa), *available* lub *pavailable* (dostępna, wartość procentowa).

Komentarze:

- Ta pozycja akceptuje trzy kategorie parametrów:
  - *total* - całkowita ilość pamięci;
  - specyficzne dla platformy typy pamięci: *active*, *anon*, *buffers*, *cached*, *exec*, *file*, *free*, *inactive*, *pinned*, *shared*, *slab*, *wired*;
  - oszacowania na poziomie użytkownika dotyczące ilości używanej i dostępnej pamięci: *used*, *pused*, *available*, *pavailable*.
- Parametr trybu *active* jest obsługiwany tylko w systemach FreeBSD, HP-UX, MacOS X, OpenBSD, NetBSD.
- Parametry trybu *anon*, *exec*, *file* są obsługiwane tylko w systemie NetBSD.
- Parametr trybu *buffers* jest obsługiwany tylko w systemach Linux, FreeBSD, OpenBSD, NetBSD.
- Parametr trybu *cached* jest obsługiwany tylko w systemach Linux, FreeBSD, AIX, OpenBSD, NetBSD.
- Parametry trybu *inactive*, *wired* są obsługiwane tylko w systemach FreeBSD, MacOS X, OpenBSD, NetBSD.
- Parametr trybu *pinned* jest obsługiwany tylko w systemie AIX.
- Parametr trybu *shared* jest obsługiwany tylko w systemach Linux 2.4, FreeBSD, OpenBSD, NetBSD.
- Zobacz także dodatkowe szczegóły dotyczące tej pozycji.

Przykład:

```
vm.memory.size[pavailable]
```

web.page.get[host,<path>,<port>]

 Pobiera zawartość strony internetowej.
 Wartość zwracana: kod źródłowy strony internetowej jako tekst (łącznie z nagłówkami).
 Zobacz obsługiwane platformy.

Parametry:

- **host** — nazwa hosta lub URL (w postaci `scheme://host:port/path`, gdzie wymagany jest tylko *host*). Dozwolone schematy URL: *http*, *https*[4]. Brakujący schemat będzie traktowany jako *http*. Jeśli podano URL, parametry `path` i `port` muszą być puste. Podanie nazwy użytkownika/hasła podczas łączenia z serwerami wymagającymi uwierzytelniania, na przykład: `http://user:password@www.example.com`, jest możliwe tylko przy obsłudze cURL [4]. Punycode jest obsługiwany w nazwach hostów.
- **path** — ścieżka do dokumentu HTML (domyślnie /);
- **port** — numer portu (domyślnie 80 dla HTTP)

Uwagi:

- Ta pozycja staje się nieobsługiwana, jeśli zasób określony w `host` nie istnieje lub jest niedostępny.
- `host` może być nazwą hosta, nazwą domenową, adresem IPv4 lub IPv6. Jednak w przypadku adresu IPv6 agent Zabbix musi być skompilowany z włączoną obsługą IPv6.

Przykłady:

```
web.page.get[www.example.com,index.php,80]
web.page.get[https://www.example.com]
web.page.get[https://blog.example.com/?s=zabbix]
```

```
web.page.get[localhost:80]
web.page.get["[::1]/server-status"]
```

web.page.perf[host,<path>,<port>]

 Czas ładowania pełnej strony WWW (w sekundach).
 Zwracana wartość: *Float*.
 Zobacz obsługiwane platformy.

Parametry:

- **host** — nazwa hosta lub URL (w postaci `scheme://host:port/path`, gdzie tylko *host* jest obowiązkowy). Dozwolone schematy URL: *http*, *https*[4]. Brakujący schemat będzie traktowany jako *http*. Jeśli podano URL, `path` i `port` muszą być puste. Podanie nazwy użytkownika/hasła podczas łączenia z serwerami wymagającymi uwierzytelnienia, na przykład: `http://user:password@www.example.com`, jest możliwe tylko przy obsłudze cURL [4]. Punycode jest obsługiwany w nazwach hostów.
- **path** — ścieżka do dokumentu HTML (domyślnie /);
- **port** — numer portu (domyślnie 80 dla HTTP)

Uwagi:

- Ta pozycja staje się nieobsługiwana, jeśli zasób określony w `host` nie istnieje lub jest niedostępny.
- `host` może być nazwą hosta, nazwą domenową, adresem IPv4 lub IPv6. Jednak w przypadku adresu IPv6 agent Zabbix musi być skompilowany z włączoną obsługą IPv6.

Przykłady:

```
web.page.perf[www.example.com,index.php,80]
web.page.perf[https://www.example.com]
```

web.page.regexp[host,<path>,<port>,regexp,<length>,<output>]

 Znajdź ciąg znaków na stronie internetowej.
 Zwracana wartość: Dopasowany ciąg znaków lub wartość określona przez opcjonalny parametr `output`.
 Zobacz obsługiwane platformy.

Parametry:

- **host** — nazwa hosta lub URL (w postaci `scheme://host:port/path`, gdzie tylko *host* jest obowiązkowy). Dozwolone schematy URL: *http*, *https*[4]. Brakujący schemat będzie traktowany jako *http*. Jeśli podano URL, parametry `path` i `port` muszą być puste. Podanie nazwy użytkownika/hasła podczas łączenia z serwerami wymagającymi uwierzytelniania, na przykład: `http://user:password@www.example.com`, jest możliwe tylko przy obsłudze cURL [4]. Punycode jest obsługiwany w nazwach hostów.
- **path** — ścieżka do dokumentu HTML (domyślnie /);
- **port** — numer portu (domyślnie 80 dla HTTP)
- **regexp** — regularne wyrażenie opisujące wymagany wzorzec;
- **length** — maksymalna liczba znaków do zwrócenia;
- **output** — opcjonalny szablon formatowania danych wyjściowych. Sekwencja ucieczki **\0** jest zastępowana dopasowaną częścią tekstu (od pierwszego znaku, od którego zaczyna się dopasowanie, do znaku, na którym dopasowanie się kończy), natomiast sekwencja ucieczki **\N** (gdzie N=1...9) jest zastępowana N-tą dopasowaną grupą (lub pustym ciągiem, jeśli N przekracza liczbę przechwyconych grup).

Uwagi:

- Ta pozycja staje się nieobsługiwana, jeśli zasób określony w `host` nie istnieje lub jest niedostępny.
- `host` może być nazwą hosta, nazwą domenową, adresem IPv4 lub IPv6. Jednak w przypadku adresu IPv6 agent Zabbix musi być skompilowany z włączoną obsługą IPv6.
- Ekstrakcja zawartości przy użyciu parametru `output` odbywa się po stronie agenta.

Przykłady:

```
web.page.regexp[www.example.com,index.php,80,OK,2]
web.page.regexp[https://www.example.com,,,OK,2]
```

agent.hostmetadata

 Metadane hosta agenta.
 Zwracana wartość: *String*.
 Zobacz obsługiwane platformy.

Zwraca wartość parametrów HostMetadata lub HostMetadataItem, albo pusty ciąg znaków, jeśli żaden z nich nie jest zdefiniowany.

agent.hostname

 Nazwa hosta agenta.
 Zwracana wartość: *String*.
 Zobacz obsługiwane platformy.

Zwraca:

- Jako sprawdzenie pasywne — nazwę pierwszego hosta wymienionego w parametrze Hostname pliku konfiguracyjnego agenta;
- Jako sprawdzenie aktywne — nazwę bieżącego hosta.

agent.ping

 Sprawdzenie dostępności agenta.
 Zwracana wartość: Nic — niedostępny; 1 — dostępny.
 Zobacz obsługiwane platformy.

Użyj funkcji wyzwalacza **nodata()**, aby sprawdzić niedostępność hosta.

agent.variant

 Wariant agenta Zabbix (Zabbix agent lub Zabbix agent 2).
 Zwracana wartość: 1 - Zabbix agent; 2 - Zabbix agent 2.
 Zobacz obsługiwane platformy.

agent.version

 Wersja agenta Zabbix.
 Zwracana wartość: *String*.
 Zobacz obsługiwane platformy.

Przykład zwracanej wartości:

```
6.0.3
```

zabbix.stats[<ip>,<port>]

 Zwraca zestaw wewnętrznych metryk serwera lub proxy Zabbix. Jeśli określono `ip` i `port`, metryki są pobierane ze zdalnej instancji; w przeciwnym razie z instancji lokalnej.
 Wartość zwracana: *ciąg JSON*.
 Zobacz obsługiwane platformy.

Parametry:

- **ip** — lista IP/DNS/masek sieciowych serwerów/proxy, które mają być odpytywane zdalnie (domyślnie 127.0.0.1);
- **port** — port serwera/proxy, który ma być odpytywany zdalnie (domyślnie 10051)

Uwagi:

- Ta pozycja zwraca wybrany zestaw wewnętrznych metryk. Szczegóły znajdują się w sekcji Zdalne monitorowanie statystyk Zabbix.
- Należy pamiętać, że żądanie statystyk zostanie zaakceptowane tylko z adresów wymienionych w parametrze 'StatsAllowedIP' serwer/proxy w instancji docelowej.

zabbix.stats[<ip>,<port>,queue,<from>,<to>]

 Zwraca liczbę monitorowanych pozycji w kolejce, które są opóźnione na serwerze Zabbix lub proxy. Jeśli określono `ip` i `port`, metryki są pobierane ze zdalnej instancji; w przeciwnym razie z instancji lokalnej.
 Wartość zwracana: *ciąg JSON*.
 Zobacz obsługiwane platformy.

Parametry:

- **ip** — lista IP/DNS/masek sieciowych serwerów/proxy, które mają być odpytywane zdalnie (domyślnie 127.0.0.1);
- **port** — port serwera/proxy, który ma być odpytywany zdalnie (domyślnie 10051)
- **queue** — stała (należy użyć bez zmian)
- **from** — opóźnienie co najmniej o (domyślnie 6 sekund)
- **to** — opóźnienie co najwyżej o (domyślnie nieskończoność)

Należy pamiętać, że żądanie statystyk zostanie zaakceptowane tylko z adresów wymienionych w parametrze 'StatsAllowedIP' instancji docelowej serwera/proxy.

Przypisy

[1] Uwaga specyficzna dla systemu Linux. Zabbix agent musi mieć dostęp tylko do odczytu do systemu plików */proc*. Łaty jądra z www.grsecurity.org ograniczają prawa dostępu użytkowników nieuprzywilejowanych.

[2] `vfs.dev.read[]`, `vfs.dev.write[]`: Zabbix agent zakończy „nieaktywne" połączenia urządzeń, jeśli wartości pozycji nie będą odczytywane przez ponad 3 godziny. Może się tak zdarzyć, jeśli system ma urządzenia z dynamicznie zmieniającymi się ścieżkami lub jeśli urządzenie zostanie ręcznie usunięte. Należy również pamiętać, że te pozycje, jeśli używają interwału aktualizacji wynoszącego 3 godziny lub więcej, zawsze zwrócą „0".

[3] `vfs.dev.read[]`, `vfs.dev.write[]`: Jeśli dla pierwszego parametru użyta jest domyślna wartość *all*, klucz zwróci statystyki zbiorcze obejmujące wszystkie urządzenia blokowe, takie jak sda, sdb i ich partycje (sda1, sda2, sdb3...), a także urządzenia wielodyskowe (MD raid) oparte na tych urządzeniach blokowych/partycjach oraz woluminy logiczne (LVM) oparte na tych urządzeniach blokowych/partycjach. W takich przypadkach zwracane wartości należy traktować wyłącznie jako wartości względne (zmienne w czasie), a nie jako wartości bezwzględne.

[4] SSL (HTTPS) jest obsługiwane tylko wtedy, gdy agent został skompilowany z obsługą cURL. W przeciwnym razie pozycja stanie się nieobsługiwana.

[5] Wartości `bytes` i `errors` nie są obsługiwane dla interfejsów loopback w systemach Solaris do wersji Solaris 10 6/06 włącznie, ponieważ statystyki bajtów, błędów i wykorzystania nie są przechowywane i/lub raportowane przez jądro. Jeśli jednak monitorujesz system Solaris przez net-snmp, wartości mogą być zwracane, ponieważ net-snmp zawiera starszy kod z cmu-snmp, datowany nawet na 1997 rok, który w przypadku niepowodzenia odczytu wartości bajtów ze statystyk interfejsu zwraca licznik pakietów (który istnieje na interfejsach loopback) pomnożony przez arbitralną wartość 308. Zakłada to, że średnia długość pakietu wynosi 308 oktetów, co jest bardzo przybliżonym oszacowaniem, ponieważ limit MTU dla interfejsów loopback w systemach Solaris wynosi 8892 bajty. Nie należy zakładać, że te wartości są poprawne ani nawet w przybliżeniu dokładne. Są to jedynie szacunki. Zabbix agent nie stosuje żadnych przybliżeń, ale net-snmp zwróci wartość dla tych pól.

[6] Wiersz poleceń w systemie Solaris, pobierany z /proc/pid/psinfo, jest ograniczony do 80 bajtów i zawiera wiersz poleceń w postaci z momentu uruchomienia procesu.

[7] Pozycje `vfs.file.contents[]`, `vfs.file.regexp[]`, `vfs.file.regmatch[]` mogą być używane do pobierania zawartości plików. Jeśli chcesz ograniczyć dostęp do określonych plików zawierających informacje wrażliwe, uruchom Zabbix agent jako użytkownika, który nie ma uprawnień dostępu do przeglądania tych plików.

Użycie z narzędziami wiersza poleceń

Należy pamiętać, że podczas testowania lub używania kluczy pozycji za pomocą `zabbix_agentd` lub `zabbix_get` z wiersza poleceń należy również uwzględnić składnię powłoki.

Na przykład, jeśli określony parametr klucza musi być ujęty w podwójne cudzysłowy, należy jawnie poprzedzić podwójne cudzysłowy znakiem ucieczki, w przeciwnym razie zostaną one usunięte przez powłokę jako znaki specjalne i nie zostaną przekazane do narzędzia Zabbix.

Przykłady:

```
zabbix_agentd -t 'vfs.dir.count[/var/log,,,"file,dir",,0]'

zabbix_agentd -t vfs.dir.count[/var/log,,,\"file,dir\",,0]
```

Ustawienia kodowania

Aby upewnić się, że pozyskane dane nie są uszkodzone, można określić prawidłowe kodowanie do przetwarzania sprawdzenia (np. `vfs.file.contents`) w parametrze `encoding`. Listę obsługiwanych kodowań (identyfikatorów stron kodowych) można znaleźć w dokumentacji libiconv (projekt GNU) lub w dokumentacji Microsoft Windows SDK dla "Code Page Identifiers". Należy pamiętać, że Microsoft czasami oznacza niektóre strony kodowe jako „dostępne tylko dla aplikacji zarządzanych" — tj. udostępniane wyłącznie przez środowisko uruchomieniowe .NET i niedostępne przez natywne interfejsy API Win32. Zabbix agent implementuje własną logikę konwersji kodowania, dlatego te strony kodowe są obsługiwane przez Zabbix agent nawet wtedy, gdy natywne funkcje systemu Windows ich nie udostępniają.

Jeśli w parametrze `encoding` nie określono kodowania, stosowane są następujące strategie rozpoznawania:

- Jeśli kodowanie nie jest określone (lub jest pustym ciągiem), przyjmuje się UTF-8, a dane są przetwarzane „tak jak są";
- Analiza BOM — dotyczy pozycji `vfs.file.contents`, `vfs.file.regexp`, `vfs.file.regmatch`. Podejmowana jest próba określenia prawidłowego kodowania przy użyciu znacznika kolejności bajtów (BOM) na początku pliku. Jeśli BOM nie występuje, zamiast tego stosowane jest standardowe rozpoznawanie (zob. wyżej).

Rozwiązywanie problemów z pozycjami agenta

W przypadku sprawdzeń pasywnych, aby zapobiec sytuacji, w której pozycja nie otrzyma żadnej wartości, ponieważ żądanie serwera do agenta najpierw przekroczy limit czasu, należy zwrócić uwagę na następujące kwestie:

- Jeśli wersja agenta jest starsza niż wersja serwera, wartość *Timeout* w konfiguracji pozycji (lub globalny limit czasu) może wymagać ustawienia na wyższą niż wartość `Timeout` w pliku konfiguracyjnym agenta.
- Jeśli wersja agenta jest nowsza niż wersja serwera, wartość `Timeout` w pliku konfiguracyjnym serwera może wymagać ustawienia na wyższą niż wartość `Timeout` w pliku konfiguracyjnym agenta.

1 Zabbix agent 2

Zabbix agent 2 obsługuje wszystkie klucze pozycji obsługiwane przez Zabbix agent w systemach Unix i Windows. Ta strona zawiera szczegółowe informacje o dodatkowych kluczach pozycji, których można używać wyłącznie z Zabbix agent 2, pogrupowanych według pluginu, do którego należą.

Klucze pozycji są wymienione bez parametrów i dodatkowych informacji. Kliknij klucz pozycji, aby zobaczyć pełne szczegóły.

Klucz pozycji	Opis	Plugin
ceph.df.details	Wykorzystanie danych klastra i ich dystrybucja między pulami.	Ceph
ceph.osd.stats	Zagregowane statystyki i statystyki dla poszczególnych OSD.	
ceph.osd.discovery	Lista wykrytych OSD.	
ceph.osd.dump	Progi wykorzystania i statusy OSD.	
ceph.ping	Sprawdza, czy można nawiązać połączenie z Ceph.	
ceph.pool.discovery	Lista wykrytych pul.	
ceph.status	Ogólny status klastra.	
docker.container_info	Informacje niskiego poziomu o kontenerze.	Docker
docker.container_stats	Statystyki wykorzystania zasobów kontenera.	
docker.containers	Zwraca listę kontenerów.	
docker.containers.discovery	Zwraca listę kontenerów. Używane do wykrywania niskiego poziomu.	
docker.data.usage	Informacje o bieżącym wykorzystaniu danych.	
docker.images	Zwraca listę obrazów.	
docker.images.discovery	Zwraca listę obrazów. Używane do wykrywania niskiego poziomu.	
docker.info	Informacje o systemie.	
docker.ping	Sprawdza, czy demon Docker działa.	
ember.get	Zwraca wynik dla wymaganego urządzenia.	Ember+
memcached.ping	Sprawdza, czy połączenie jest aktywne.	Memcached
memcached.stats	Pobiera dane wyjściowe polecenia STATS.	
mongodb.collection.stats	Zwraca różne statystyki pamięci masowej dla danej kolekcji.	MongoDB
mongodb.cfg.discovery	Zwraca listę wykrytych serwerów konfiguracyjnych.	MongoDB
mongodb.collections.discovery	Zwraca listę wykrytych kolekcji.	
mongodb.collections.usage	Zwraca statystyki wykorzystania dla kolekcji.	
mongodb.connpool.stats	Zwraca informacje o otwartych połączeniach wychodzących z bieżącej instancji bazy danych do innych członków klastra shardowanego lub zestawu replik.	
mongodb.db.stats	Zwraca statystyki odzwierciedlające stan danego systemu bazy danych.	
mongodb.db.discovery	Zwraca listę wykrytych baz danych.	
mongodb.jumbo_chunks.count	Zwraca liczbę dużych chunków.	
mongodb.oplog.stats	Zwraca status zestawu replik na podstawie danych pobranych z oplogu.	
mongodb.ping	Sprawdza, czy połączenie jest aktywne.	
mongodb.rs.config	Zwraca bieżącą konfigurację zestawu replik.	
mongodb.rs.status	Zwraca status zestawu replik z punktu widzenia członka, na którym uruchomiono metodę.	
mongodb.server.status	Zwraca stan bazy danych.	
mongodb.sh.discovery	Zwraca listę wykrytych shardów obecnych w klastrze.	
mongodb.version	Zwraca wersję serwera bazy danych.	
mqtt.get	Subskrybuje określony temat lub tematy (z symbolami wieloznacznymi) podanego brokera i oczekuje na publikacje.	MQTT
mssql.availability.group.get	Zwraca grupy dostępności.	MSSQL
mssql.custom.query	Zwraca wynik niestandardowego zapytania.	
mssql.db.get	Zwraca wszystkie dostępne bazy danych MSSQL.	
mssql.job.status.get	Zwraca status zadań.	
mssql.last.backup.get	Zwraca czas ostatniej kopii zapasowej dla wszystkich baz danych.	
mssql.local.db.get	Zwraca bazy danych uczestniczące w grupie dostępności Always On i replice (podstawowej lub pomocniczej), które znajdują się na serwerze, z którym nawiązano połączenie.	
mssql.mirroring.get	Zwraca informacje o mirroringu.	
mssql.nonlocal.db.get	Zwraca bazy danych uczestniczące w grupie dostępności Always On i replice (podstawowej lub pomocniczej), znajdujące się na innych serwerach (baza danych nie jest lokalna dla instancji SQL Server, z którą nawiązano połączenie).	
mssql.perfcounter.get	Zwraca liczniki wydajności.	
mssql.ping	Sprawdza, czy połączenie jest aktywne.	
mssql.quorum.get	Zwraca informacje o kworum.	
mssql.quorum.member.get	Zwraca członków kworum.	
mssql.replica.get	Zwraca repliki.	
mssql.version	Zwraca wersję MSSQL.	
mysql.custom.query	Zwraca wynik niestandardowego zapytania.	MySQL
mysql.db.discovery	Zwraca listę baz danych MySQL.	
mysql.db.size	Rozmiar bazy danych w bajtach.	
mysql.get_status_variables	Wartości globalnych zmiennych statusu.	
mysql.ping	Sprawdza, czy połączenie jest aktywne.	

Klucz pozycji	Opis	Plugin
mysql.replication.discovery	Zwraca listę replikacji MySQL.	
mysql.replication.get_slave_status	Status replikacji.	
mysql.version	Wersja MySQL.	
net.dns.get	Wykonuje zapytanie DNS i zwraca szczegółowe informacje o rekordzie DNS.	Network
nvml.device.count	Liczba urządzeń GPU.	NVIDIA GPU
nvml.device.decoder.utilization	Wykorzystanie dekodera urządzenia GPU.	
nvml.device.ecc.mode	Tryb ECC urządzenia GPU.	
nvml.device.encoder.stats.get	Statystyki enkodera urządzenia GPU.	
nvml.device.encoder.utilization	Wykorzystanie enkodera urządzenia GPU.	
nvml.device.energy.consumption	Zużycie energii przez urządzenie GPU.	
nvml.device.errors.memory	Informacje o błędach pamięci ECC urządzenia GPU.	
nvml.device.errors.register	Informacje o błędach rejestru ECC urządzenia GPU.	
nvml.device.fan.speed.avg	Średnia prędkość wentylatora urządzenia GPU.	
nvml.device.get	Wykryte GPU z UUID i nazwą.	
nvml.device.graphics.frequency	Częstotliwość zegara grafiki urządzenia GPU.	
nvml.device.memory.bar1.get	Informacje o pamięci BAR1 urządzenia GPU.	
nvml.device.memory.fb.get	Informacje o pamięci framebuffer urządzenia GPU.	
nvml.device.memory.frequency	Częstotliwość zegara pamięci urządzenia GPU.	
nvml.device.pci.utilization	Wykorzystanie PCI urządzenia GPU.	
nvml.device.performance.state	Stan wydajności urządzenia GPU.	
nvml.device.power.limit	Limit mocy urządzenia GPU.	
nvml.device.power.usage	Pobór mocy urządzenia GPU.	
nvml.device.serial	Numer seryjny urządzenia GPU.	
nvml.device.sm.frequency	Częstotliwość zegara multiprocesora strumieniowego urządzenia GPU.	
nvml.device.temperature	Temperatura urządzenia GPU.	
nvml.device.utilization	Statystyki wykorzystania urządzenia GPU.	
nvml.device.video.frequency	Częstotliwość zegara wideo urządzenia GPU.	
nvml.system.driver.version	Wersja sterownika NVIDIA.	
nvml.version	Wersja biblioteki NVML.	
oracle.diskgroups.stats	Zwraca statystyki grup dysków Automatic Storage Management (ASM).	Oracle
oracle.diskgroups.discovery	Zwraca listę grup dysków ASM.	
oracle.archive.info	Statystyki logów archiwalnych.	
oracle.cdb.info	Informacje o bazach danych kontenerowych (CDB).	
oracle.custom.query	Wynik niestandardowego zapytania.	
oracle.datafiles.stats	Zwraca statystyki plików danych.	
oracle.db.discovery	Zwraca listę baz danych.	
oracle.fra.stats	Zwraca statystyki Fast Recovery Area (FRA).	
oracle.instance.info	Statystyki instancji.	
oracle.pdb.info	Informacje o bazach danych typu Pluggable Database (PDB).	
oracle.pdb.discovery	Zwraca listę PDB.	
oracle.pga.stats	Zwraca statystyki Program Global Area (PGA).	
oracle.ping	Sprawdza, czy można nawiązać połączenie z Oracle.	
oracle.proc.stats	Zwraca statystyki procesów.	
oracle.redolog.info	Informacje o pliku logu z pliku kontrolnego.	
oracle.sga.stats	Zwraca statystyki System Global Area (SGA).	
oracle.sessions.stats	Zwraca statystyki sesji.	
oracle.sys.metrics	Zwraca zestaw wartości metryk systemowych.	
oracle.sys.params	Zwraca zestaw wartości parametrów systemowych.	
oracle.ts.stats	Zwraca statystyki tablespace’ów.	
oracle.ts.discovery	Zwraca listę tablespace’ów.	
oracle.user.info	Zwraca informacje o użytkownikach Oracle.	
oracle.version	Zwraca wersję serwera bazy danych.	
pgsql.autovacuum.count	Liczba workerów autovacuum.	PostgreSQL
pgsql.archive	Informacje o zarchiwizowanych plikach.	
pgsql.bgwriter	Łączna liczba checkpointów dla klastra bazy danych z podziałem według typu checkpointu.	
pgsql.cache.hit	Współczynnik trafień pamięci podręcznej buforów PostgreSQL.	
pgsql.connections	Zwraca połączenia według typu.	
pgsql.custom.query	Zwraca wynik niestandardowego zapytania.	
pgsql.db.age	Wiek najstarszego FrozenXID bazy danych.	

Klucz pozycji	Opis	Plugin
pgsql.db.bloating_tables	Liczba rozdętych tabel na bazę danych.	
pgsql.db.discovery	Lista baz danych PostgreSQL.	
pgsql.db.size	Rozmiar bazy danych w bajtach.	
pgsql.dbstat	Zbiera statystyki dla każdej bazy danych.	
pgsql.dbstat.sum	Dane zbiorcze dla wszystkich baz danych w klastrze.	
pgsql.locks	Informacje o przyznanych blokadach dla każdej bazy danych.	
pgsql.oldest.xid	Wiek najstarszego XID.	
pgsql.ping	Sprawdza, czy połączenie jest aktywne.	
pgsql.queries	Metryki zapytań według czasu wykonania.	
pgsql.replication.count	Liczba serwerów standby.	
pgsql.replication.process	Opóźnienie flush, write i replay dla każdego procesu nadawcy.	
pgsql.replication.process.discovery	Wykrywanie nazw procesów replikacji.	
pgsql.replication.recovery_role	Status odzyskiwania.	
pgsql.replication.status	Status replikacji.	
pgsql.replication_lag.b	Opóźnienie replikacji w bajtach.	
pgsql.replication_lag.sec	Opóźnienie replikacji w sekundach.	
pgsql.uptime	Czas działania PostgreSQL w milisekundach.	
pgsql.version	Zwraca wersję PostgreSQL.	
pgsql.wal.stat	Statystyki WAL.	
redis.config	Pobiera parametry konfiguracyjne instancji Redis pasujące do wzorca.	Redis
redis.info	Pobiera dane wyjściowe polecenia INFO.	
redis.ping	Sprawdza, czy połączenie jest aktywne.	
redis.slowlog.count	Liczba wpisów slow log od uruchomienia Redis.	
smart.attribute.discovery	Zwraca listę atrybutów urządzeń S.M.A.R.T.	S.M.A.R.T.
smart.disk.discovery	Zwraca listę urządzeń S.M.A.R.T.	
smart.disk.get	Zwraca wszystkie dostępne właściwości urządzeń S.M.A.R.T.	
systemd.unit.get	Zwraca wszystkie właściwości jednostki systemd.	Systemd
systemd.unit.info	Informacje o jednostce systemd.	
systemd.unit.discovery	Lista jednostek systemd i ich szczegóły.	
web.certificate.get	Weryfikuje certyfikaty i zwraca szczegóły certyfikatu.	Web certificates

Zobacz także:

- Wbudowane pluginy
- Ładowalne pluginy

Szczegóły klucza pozycji

Parametry bez nawiasów ostrych są obowiązkowe. Parametry oznaczone nawiasami ostrymi **< >** są opcjonalne.

ceph.df.details[connString,<user>,<apikey>]

 Wykorzystanie danych klastra i ich dystrybucja pomiędzy pulami.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **connString** — URI lub nazwa sesji;
- **user, apikey** — nazwa użytkownika i klucz API do połączenia z Ceph.

ceph.osd.stats[connString,<user>,<apikey>]

 Statystyki zagregowane i dla poszczególnych OSD.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **connString** - URI lub nazwa sesji;
- **user, apikey** - nazwa użytkownika i klucz API do połączenia z Ceph.

ceph.osd.discovery[connString,<user>,<apikey>]

 Lista wykrytych OSD. Używane do odkrywania niskiego poziomu.
 Wartość zwracana: *obiekt JSON*.

Parametry:

- **connString** — URI lub nazwa sesji;
- **user, apikey** — nazwa użytkownika i klucz API do połączenia z Ceph.

ceph.osd.dump[connString,<user>,<apikey>]

 Progi wykorzystania i statusy OSD.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **connString** - URI lub nazwa sesji;
- **user, apikey** - nazwa użytkownika i klucz API do połączenia z Ceph.

ceph.ping[connString,<user>,<apikey>]

 Sprawdza, czy można nawiązać połączenie z Ceph.
 Wartość zwracana: *0* - połączenie jest przerwane (jeśli występuje jakikolwiek błąd, w tym problemy z AUTH i konfiguracją); *1* - połączenie zostało nawiązane pomyślnie.

Parametry:

- **connString** - URI lub nazwa sesji;
- **user, apikey** - nazwa użytkownika i klucz API do łączenia z Ceph.

ceph.pool.discovery[connString,<user>,<apikey>]

 Lista wykrytych puli. Używane do odkrywania niskiego poziomu.
 Wartość zwracana: *obiekt JSON*.

Parametry:

- **connString** — URI lub nazwa sesji;
- **user, apikey** — nazwa użytkownika i klucz API do połączenia z Ceph.

ceph.status[connString,<user>,<apikey>]

 Ogólny status klastra.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **connString** — URI lub nazwa sesji;
- **user, apikey** — nazwa użytkownika i klucz API do połączenia z Ceph.

docker.container_info[<ID>,<info>]

 Informacje niskiego poziomu o kontenerze.
 Zwracana wartość: Dane wyjściowe wywołania API ContainerInspect zserializowane jako JSON.

Parametry:

- **ID** - identyfikator lub nazwa kontenera;
- **info** - ilość zwracanych informacji. Obsługiwane wartości: *short* (domyślnie) lub *full*.

Użytkownik Agent 2 (’zabbix’) musi zostać dodany do grupy ’docker’, aby miał wystarczające uprawnienia. W przeciwnym razie sprawdzenie zakończy się niepowodzeniem.

docker.container_stats[<ID>]

 Statystyki użycia zasobów kontenera.
 Wartość zwracana: dane wyjściowe wywołania API ContainerStats oraz procent użycia CPU zserializowane jako JSON.

Parametr:

- **ID** — identyfikator lub nazwa kontenera.

Użytkownik Agent 2 („zabbix”) musi zostać dodany do grupy „docker”, aby mieć wystarczające uprawnienia. W przeciwnym razie sprawdzenie zakończy się niepowodzeniem.

docker.containers

 Lista kontenerów.
 Zwracana wartość: Dane wyjściowe wywołania API ContainerList zserializowane jako JSON.

Użytkownik Agent 2 („zabbix”) musi zostać dodany do group „docker”, aby miał wystarczające uprawnienia. W przeciwnym razie sprawdzenie zakończy się niepowodzeniem.

docker.containers.discovery[<options>]

 Zwraca listę kontenerów. Używane do odkrywania niskiego poziomu.
 Zwracana wartość: *obiekt JSON*.

Parametr:

- **options** — określa, czy mają zostać wykryte wszystkie kontenery, czy tylko uruchomione. Obsługiwane wartości: *true* — zwraca wszystkie kontenery; *false* — zwraca tylko uruchomione kontenery (domyślnie).

Użytkownik Agent 2 („zabbix”) musi zostać dodany do grupy „docker”, aby miał wystarczające uprawnienia. W przeciwnym razie sprawdzenie zakończy się niepowodzeniem.

docker.data.usage

 Informacje o bieżącym użyciu danych.
 Zwracana wartość: Dane wyjściowe wywołania API SystemDataUsage zserializowane jako JSON.

Użytkownik Agent 2 („zabbix”) musi zostać dodany do group „docker”, aby miał wystarczające uprawnienia. W przeciwnym razie sprawdzenie zakończy się niepowodzeniem.

docker.images

 Zwraca listę obrazów.
 Wartość zwracana: dane wyjściowe wywołania API ImageList zserializowane do formatu JSON.

Użytkownik Agent 2 („zabbix”) musi zostać dodany do grupy „docker”, aby miał wystarczające uprawnienia. W przeciwnym razie sprawdzenie zakończy się niepowodzeniem.

docker.images.discovery

 Zwraca listę obrazów. Używane do odkrywania niskiego poziomu.
 Zwracana wartość: *obiekt JSON*.

Użytkownik Agent 2 („zabbix”) musi zostać dodany do grupy „docker”, aby miał wystarczające uprawnienia. W przeciwnym razie sprawdzenie zakończy się niepowodzeniem.

docker.info

 Informacje o systemie.
 Wartość zwracana: Dane wyjściowe wywołania API SystemInfo zserializowane jako JSON.

Użytkownik Agent 2 („zabbix”) musi zostać dodany do grupy „docker”, aby miał wystarczające uprawnienia. W przeciwnym razie sprawdzenie zakończy się niepowodzeniem.

docker.ping

 Sprawdza, czy demon Docker działa, czy nie.
 Zwracana wartość: *1* - połączenie działa; *0* - połączenie jest zerwane.

Użytkownik Agent 2 („zabbix”) musi zostać dodany do grupy „docker”, aby mieć wystarczające uprawnienia. W przeciwnym razie sprawdzenie zakończy się niepowodzeniem.

ember.get[<uri>,<path>]

 Zwraca wynik wymaganego urządzenia.
 Wartość zwracana: *obiekt JSON*.

Parametry:

- **uri** - URI urządzenia Ember+. Domyślnie: 127.0.0.1:9998;
- **path** - ścieżka OID do urządzenia. Domyślnie pusta, zwraca dane kolekcji głównej.

memcached.ping[connString,<user>,<password>]

 Sprawdza, czy połączenie jest aktywne.
 Zwracana wartość: *1* — połączenie jest aktywne; *0* — połączenie jest zerwane (jeśli wystąpi dowolny błąd, w tym problemy z AUTH i konfiguracją).

Parametry:

- **connString** — URI lub nazwa sesji;
- **user, password** — dane logowania do Memcached.

memcached.stats[connString,<user>,<password>,<type>]

 Pobiera dane wyjściowe polecenia STATS.
 Wartość zwracana: *JSON* - dane wyjściowe są serializowane do formatu JSON.

Parametry:

- **connString** - URI lub nazwa sesji;
- **user, password** - dane logowania do Memcached;
- **type** - typ statystyk do zwrócenia: *items*, *sizes*, *slabs* lub *settings* (domyślnie pusty, zwraca statystyki ogólne).

mongodb.collection.stats[connString,<user>,<password>,<database>,collection]

 Zwraca różne statystyki pamięci masowej dla danej kolekcji.
 Wartość zwracana: *obiekt JSON*.

Parametry:

- **connString** - URI lub nazwa sesji;
- **user, password** - dane logowania do MongoDB;
- **database** - nazwa bazy danych (domyślnie: admin);
- **collection** - nazwa kolekcji.

mongodb.cfg.discovery[connString,<user>,<password>]

 Zwraca listę wykrytych serwerów konfiguracji.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **connString** — URI lub nazwa sesji;
- **user, password** — dane logowania do MongoDB.

mongodb.collections.discovery[connString,<user>,<password>]

 Zwraca listę wykrytych kolekcji. Używane do odkrywania niskiego poziomu.
 Wartość zwracana: *obiekt JSON*.

Parametry:

- **connString** — URI lub nazwa sesji;
- **user, password** — dane logowania do MongoDB.

mongodb.collections.usage[connString,<user>,<password>]

 Zwraca statystyki użycia dla kolekcji.
 Wartość zwracana: *obiekt JSON*.

Parametry:

- **connString** - URI lub nazwa sesji;
- **user, password** - dane logowania do MongoDB.

mongodb.connpool.stats[connString,<user>,<password>]

 Zwraca informacje dotyczące otwartych połączeń wychodzących z bieżącej instancji bazy danych do innych członków klastra shardingu lub zestawu replik.
 Wartość zwracana: *obiekt JSON*.

Parametry:

- **connString** - URI lub nazwa sesji;
- **user, password** - dane logowania do MongoDB.

mongodb.db.stats[connString,<user>,<password>,<database>]

 Zwraca statystyki odzwierciedlające stan danego systemu bazy danych.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **connString** - URI lub nazwa sesji;
- **user, password** - dane logowania do MongoDB;
- **database** - nazwa bazy danych (domyślnie: admin).

mongodb.db.discovery[connString,<user>,<password>]

 Zwraca listę wykrytych baz danych. Używane do odkrywania niskiego poziomu.
 Wartość zwracana: *obiekt JSON*.

Parametry:

- **connString** — URI lub nazwa sesji;
- **user, password** — dane logowania do MongoDB.

mongodb.jumbo_chunks.count[connString,<user>,<password>]

 Zwraca liczbę jumbo chunks.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **connString** - URI lub nazwa sesji;
- **user, password** - dane logowania do MongoDB.

mongodb.oplog.stats[connString,<user>,<password>]

 Zwraca stan zestawu replik, używając danych pobranych z oplog.
 Wartość zwracana: *obiekt JSON*.

Parametry:

- **connString** - URI lub nazwa sesji;
- **user, password** - dane logowania do MongoDB.

mongodb.ping[connString,<user>,<password>]

 Sprawdza, czy połączenie jest aktywne, czy nie.
 Zwracana wartość: *1* - połączenie jest aktywne; *0* - połączenie jest zerwane (jeśli wystąpi jakikolwiek błąd, w tym problemy z AUTH i konfiguracją).

Parametry:

- **connString** - URI lub nazwa sesji;
- **user, password** - dane logowania do MongoDB.

mongodb.rs.config[connString,<user>,<password>]

 Zwraca bieżącą konfigurację zestawu replik.
 Wartość zwracana: *obiekt JSON*.

Parametry:

- **connString** — URI lub nazwa sesji;
- **user, password** — dane logowania do MongoDB.

mongodb.rs.status[connString,<user>,<password>]

 Zwraca status zestawu replik z punktu widzenia członka, na którym uruchomiono tę metodę.
 Wartość zwracana: *obiekt JSON*.

Parametry:

- **connString** - URI lub nazwa sesji;
- **user, password** - dane logowania do MongoDB.

mongodb.server.status[connString,<user>,<password>]

 Zwraca stan bazy danych.
 Wartość zwracana: *obiekt JSON*.

Parametry:

- **connString** - URI lub nazwa sesji;
- **user, password** - dane logowania do MongoDB.

mongodb.sh.discovery[connString,<user>,<password>]

 Zwraca listę wykrytych shardów obecnych w klastrze.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **connString** - URI lub nazwa sesji;
- **user, password** - dane logowania do MongoDB.

mongodb.version[connString,<user>,<password>]

 Zwraca wersję serwera bazy danych.
 Wartość zwracana: *String*.

Parametry:

- **connString** — URI lub nazwa sesji;
- **user, password** — dane logowania do MongoDB.

mqtt.get[<broker url>,topic,<user>,<password>]

 Subskrybuje określony temat lub tematy (z symbolami wieloznacznymi) podanego brokera i oczekuje na publikacje.
 Wartość zwracana: Zależy od zawartości tematu. Jeśli używane są symbole wieloznaczne, zwracana jest zawartość tematu w formacie JSON.

Parametry:

- **broker url** — URL brokera MQTT w formacie `protocol://host:port` bez parametrów zapytania (obsługiwane protokoły: `tcp`, `ssl`, `ws`). Jeśli nie podano wartości, agent użyje `tcp://localhost:1883`. Jeśli pominięto protokół lub port, zostanie użyty domyślny protokół (`tcp`) lub port (1883);
- **topic** — temat MQTT (wymagany). Obsługiwane są symbole wieloznaczne (+,#);
- **user, password** — dane uwierzytelniające (jeśli są wymagane).

Uwagi:

- pozycja musi być skonfigurowana jako sprawdzenie aktywne (typ pozycji „Zabbix agent (active)”);
- Certyfikaty szyfrowania TLS mogą być używane po zapisaniu ich w domyślnej lokalizacji (np. katalog `/etc/ssl/certs/` w Ubuntu). Dla TLS użyj schematu `tls://`.

mssql.availability.group.get[URI,<user>,<password>]

 Zwraca grupy dostępności.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **URI** — URI serwera MSSQL (jedynym obsługiwanym schematem jest `sqlserver://`). Osadzone dane uwierzytelniające zostaną zignorowane. Można określić nazwę instancji jako część URI, np.: `sqlserver://localhost/InstanceName` (bez portu). Jeśli określono port, nazwa instancji jest ignorowana;

- **user, password** — nazwa użytkownika, hasło wysyłane do chronionego serwera MSSQL.

Więcej informacji można znaleźć w pliku readme wtyczki MSSQL.

mssql.custom.query[URI,<user>,<password>,queryName,<args...>]

 Zwraca wynik niestandardowego zapytania.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **URI** - URI serwera MSSQL (jedynym obsługiwanym schematem jest `sqlserver://`). Osadzone dane uwierzytelniające zostaną zignorowane. Można określić nazwę instancji jako część URI, np.: `sqlserver://localhost/InstanceName` (bez portu). Jeśli określono port, nazwa instancji jest ignorowana;
- **user, password** - nazwa użytkownika, hasło wysyłane do chronionego serwera MSSQL;
- **queryName** - nazwa niestandardowego zapytania skonfigurowanego w `Plugins.MSSQL.CustomQueriesDir` bez rozszerzenia .sql;
- **args** - jeden lub kilka argumentów oddzielonych przecinkami, przekazywanych do zapytania.

Więcej informacji można znaleźć w pliku readme wtyczki MSSQL.

mssql.db.get

 Zwraca wszystkie dostępne bazy danych MSSQL.
 Wartość zwracana: *obiekt JSON*.

Więcej informacji można znaleźć w pliku readme wtyczki MSSQL.

mssql.job.status.get

 Zwraca status zadań.
 Wartość zwracana: *obiekt JSON*.

Więcej informacji można znaleźć w pliku readme wtyczki MSSQL.

mssql.last.backup.get

 Zwraca czas ostatniej kopii zapasowej dla wszystkich baz danych.
 Zwracana wartość: *obiekt JSON*.

Więcej informacji można znaleźć w pliku readme wtyczki MSSQL.

mssql.local.db.get

 Zwraca bazy danych, które uczestniczą w grupie dostępności Always On i replice (podstawowej lub pomocniczej) oraz znajdują się na serwerze, z którym ustanowiono połączenie.
 Zwracana wartość: *obiekt JSON*.

Więcej informacji można znaleźć w pliku readme wtyczki MSSQL.

mssql.mirroring.get

 Zwraca informacje o mirroringu.
 Zwracana wartość: *obiekt JSON*.

Więcej informacji można znaleźć w pliku readme wtyczki MSSQL.

mssql.nonlocal.db.get

 Zwraca bazy danych uczestniczące w grupie dostępności Always On oraz replice (podstawowej lub pomocniczej) znajdującej się na innych serwerach (baza danych nie jest lokalna dla instancji SQL Server, z którą nawiązano połączenie).
 Zwracana wartość: *obiekt JSON*.

Więcej informacji można znaleźć w pliku readme wtyczki MSSQL.

mssql.perfcounter.get

 Zwraca liczniki wydajności.
 Zwracana wartość: *obiekt JSON*.

Więcej informacji można znaleźć w pliku readme wtyczki MSSQL.

mssql.ping

 Sprawdza dostępność bazy danych. Testuje, czy połączenie jest poprawnie skonfigurowane.
 Zwracana wartość: *1* - działa, *0* - nie działa.

Więcej informacji można znaleźć w pliku readme wtyczki MSSQL.

mssql.quorum.get

 Zwraca informacje o kworum.
 Zwracana wartość: *obiekt JSON*.

Więcej informacji można znaleźć w pliku readme wtyczki MSSQL.

mssql.quorum.member.get

 Zwraca członków kworum.
 Wartość zwracana: *obiekt JSON*.

Więcej informacji można znaleźć w pliku readme wtyczki MSSQL.

mssql.replica.get

 Zwraca repliki.
 Wartość zwracana: *obiekt JSON*.

Więcej informacji można znaleźć w pliku readme wtyczki MSSQL.

mssql.version

 Zwraca wersję MSSQL.
 Zwracana wartość: *String*.

Więcej informacji można znaleźć w pliku readme wtyczki MSSQL.

mysql.custom.query[connString,<user>,<password>,queryName,<args...>]

 Zwraca wynik niestandardowego zapytania.
 Wartość zwracana: *obiekt JSON*.

Parametry:

- **connString** - URI lub nazwa sesji;
- **user, password** - dane logowania MySQL;
- **queryName** - nazwa niestandardowego zapytania; musi odpowiadać nazwie pliku SQL bez rozszerzenia;
- **args** - jeden lub kilka argumentów rozdzielonych przecinkami, przekazywanych do zapytania.

Aby uzyskać więcej informacji, zobacz plik readme wtyczki MySQL, sekcję *Niestandardowe zapytania*.

mysql.db.discovery[connString,<user>,<password>]

 Zwraca listę baz danych MySQL. Używane w odkrywaniu niskiego poziomu.
 Wartość zwracana: wynik zapytania SQL „show databases” w formacie JSON LLD.

Parametry:

- **connString** — URI lub nazwa sesji;
- **user, password** — dane logowania do MySQL.

mysql.db.size[connString,<user>,<password>,<database name>]

 Rozmiar bazy danych w bajtach.
 Zwracana wartość: wynik zapytania SQL „select coalesce(sum(data_length + index_length),0) as size from information_schema.tables where table_schema=?” dla określonej bazy danych, w bajtach.

Parametry:

- **connString** — URI lub nazwa sesji;
- **user, password** — dane logowania MySQL;
- **database name** — nazwa bazy danych.

mysql.get_status_variables[connString,<user>,<password>]

 Wartości globalnych zmiennych statusu.
 Wartość zwracana: Wynik zapytania SQL „show global status” w formacie JSON.

Parametry:

- **connString** — URI lub nazwa sesji;
- **user, password** — dane logowania MySQL.

mysql.ping[connString,<user>,<password>]

 Sprawdza, czy połączenie jest aktywne.
 Zwracana wartość: *1* - połączenie jest aktywne; *0* - połączenie jest zerwane (jeśli wystąpi jakikolwiek błąd, w tym problemy z AUTH i konfiguracją).

Parametry:

- **connString** - URI lub nazwa sesji;
- **user, password** - dane logowania do MySQL.

mysql.replication.discovery[connString,<user>,<password>]

 Zwraca listę replikacji MySQL. Używane do odkrywania niskiego poziomu.
 Wartość zwracana: wynik zapytania SQL `SHOW SLAVE STATUS` lub `SHOW REPLICA STATUS` w formacie LLD JSON.

Parametry:

- **connString** - URI lub nazwa sesji;
- **user, password** - dane logowania MySQL.

mysql.replication.get_slave_status[connString,<user>,<password>,<master host>]

 Status replikacji.
 Zwracana wartość: wynik zapytania SQL `SHOW SLAVE STATUS` lub `SHOW REPLICA STATUS` w formacie JSON.

Parametry:

- **connString** — URI lub nazwa sesji;
- **user, password** — dane logowania do MySQL;
- **master host** — nazwa hosta głównego replikacji. Jeśli nie znaleziono żadnego, zwracany jest błąd. Jeśli ten parametr nie jest określony, zwracane są wszystkie hosty.

mysql.version[connString,<user>,<password>]

 Wersja MySQL.
 Zwracana wartość: *String* (z wersją instancji MySQL).

Parametry:

- **connString** - URI lub nazwa sesji;
- **user, password** - dane logowania do MySQL.

net.dns.get[<ip>,name,<type>,<timeout>,<count>,<protocol>,"<flags>"]

Wykonuje zapytanie DNS i zwraca szczegółowe informacje o rekordzie DNS.
 Ta pozycja jest rozszerzoną wersją pozycji agenta Zabbix `net.dns.record`, obsługującą większą liczbę typów rekordów i konfigurowalne flagi.
 Zwracane wartości: *obiekt JSON*

Parametry:

- **ip** - adres IP serwera DNS (pozostaw puste, aby użyć domyślnego serwera DNS);
- **name** - nazwa DNS, o którą ma zostać wykonane zapytanie;
- **type** - typ rekordu, o który ma zostać wykonane zapytanie (domyślnie *SOA*);
- **timeout** - limit czasu żądania w sekundach (domyślnie 1 sekunda);
- **count** - liczba prób wykonania żądania (domyślnie 2);
- **protocol** - protokół używany do wykonywania zapytań DNS: *udp* (domyślnie) lub *tcp*;
- **flags** - jeden lub więcej argumentów rozdzielonych przecinkami, przekazywanych do zapytania.

Uwagi:

- Możliwe wartości parametru `type` to: *A*, *NS*, *MD*, *MF*, *CNAME*, *SOA*, *MB*, *MG*, *MR*, *NULL*, *PTR*, *HINFO*, *MINFO*, *MX*, *TXT*, *RP*, *AFSDB*, *X25*, *ISDN*, *RT*, *NSAPPTR*, *SIG*, *KEY*, *PX*, *GPOS*, *AAAA*, *LOC*, *NXT*, *EID*, *NIMLOC*, *SRV*, *ATMA*, *NAPTR*, *KX*, *CERT*, *DNAME*, *OPT*, *APL*, *DS*, *SSHFP*, *IPSECKEY*, *RRSIG*, *NSEC*, *DNSKEY*, *DHCID*, *NSEC3*, *NSEC3PARAM*, *TLSA*, *SMIMEA*, *HIP*, *NINFO*, *RKEY*, *TALINK*, *CDS*, *CDNSKEY*, *OPENPGPKEY*, *CSYNC*, *ZONEMD*, *SVCB*, *HTTPS*, *SPF*, *UINFO*, *UID*, *GID*, *UNSPEC*, *NID*, *L32*, *L64*, *LP*, *EUI48*, *EUI64*, *URI*, *CAA*, *AVC*, *AMTRELAY*. Pamiętaj, że wartości muszą być podawane wyłącznie wielkimi literami; wartości zapisane małymi literami lub w formacie mieszanym nie są obsługiwane.
- W przypadku odwrotnych wyszukiwań DNS (gdy `type` jest ustawiony na *PTR*) można podać nazwę DNS zarówno w formacie odwróconym, jak i nieodwróconym (zobacz przykłady poniżej). Pamiętaj, że gdy żądany jest rekord PTR, nazwa DNS jest w rzeczywistości adresem IP.
- Możliwe wartości parametru `flags` to: *cdflag* lub *nocdflag* (domyślnie), *rdflag* (domyślnie) lub *nordflag*, *dnssec* lub *nodnssec* (domyślnie), *nsid* lub *nonsid* (domyślnie), *edns0* (domyślnie) lub *noedns0*, *aaflag* lub *noaaflag* (domyślnie), *adflag* lub *noadflag* (domyślnie). Flagi `flags` *dnssec* i *nsid* nie mogą być używane razem z *noedns0*, ponieważ obie wymagają *edns0*. Pamiętaj, że wartości muszą być podawane wyłącznie małymi literami; wartości zapisane wielkimi literami lub w formacie mieszanym nie są obsługiwane.
- Umiędzynarodowione nazwy domen nie są obsługiwane; zamiast tego użyj nazw zakodowanych w IDNA.
- Dane wyjściowe są obiektem zawierającym informacje o rekordzie DNS na podstawie podanych parametrów (zobacz więcej szczegółów).

Przykłady:

```
net.dns.get[192.0.2.0,example.com,DNSKEY,3,3,tcp,"cdflag,rdflag,nsid"]

net.dns.get[,198.51.100.1,PTR,,,,"cdflag,rdflag,nsid"]
net.dns.get[,1.100.51.198.in-addr.arpa,PTR,,,,"cdflag,rdflag,nsid"]

net.dns.get[,2a00:1450:400f:800::200e,PTR,,,,"cdflag,rdflag,nsid"]
net.dns.get[,e.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.0.f.0.0.4.0.5.4.1.0.0.a.2.ip6.arpa,PTR,,,,"cdflag,rdfla
```

nvml.device.count

 Liczba urządzeń GPU.
 Zwracana wartość: *Integer*.

Więcej informacji można znaleźć w pliku readme wtyczki NVIDIA GPU.

nvml.device.decoder.utilization[<deviceUUID>]

 Wykorzystanie dekodera urządzenia GPU w procentach.
 Zwracana wartość: *Integer*.

Parametr:

- **deviceUUID** - UUID urządzenia GPU.

Aby uzyskać więcej informacji, zobacz plik readme wtyczki NVIDIA GPU.

nvml.device.ecc.mode[<deviceUUID>]

 Informacje o trybie ECC urządzenia GPU (bieżący, oczekujący).
 Zwracana wartość: *JSON*.

Parametr:

- **deviceUUID** - UUID urządzenia GPU.

Więcej informacji można znaleźć w pliku readme wtyczki NVIDIA GPU.

nvml.device.encoder.stats.get[<deviceUUID>]

 Statystyki enkodera urządzenia GPU.
 Zwracana wartość: *JSON*.

Parametr:

- **deviceUUID** - UUID urządzenia GPU.

Więcej informacji można znaleźć w pliku readme wtyczki NVIDIA GPU.

nvml.device.encoder.utilization[<deviceUUID>]

 Wykorzystanie enkodera urządzenia GPU w procentach.
 Zwracana wartość: *Integer*.

Parametr:

- **deviceUUID** — UUID urządzenia GPU.

Więcej informacji można znaleźć w pliku readme wtyczki NVIDIA GPU.

nvml.device.energy.consumption[<deviceUUID>]

 Całkowite zużycie energii urządzenia GPU w milidżulach (mJ) od ostatniego przeładowania sterownika.
 Zwracana wartość: *Integer*.

Parametr:

- **deviceUUID** — UUID urządzenia GPU.

Więcej informacji można znaleźć w pliku readme wtyczki NVIDIA GPU.

nvml.device.errors.memory[<deviceUUID>]

 Informacje o błędach pamięci ECC urządzenia GPU (skorygowane, nieskorygowane).
 Zwracana wartość: *JSON*.

Parametr:

- **deviceUUID** — UUID urządzenia GPU.

Więcej informacji można znaleźć w pliku readme wtyczki NVIDIA GPU.

nvml.device.errors.register[<deviceUUID>]

 Informacje o błędach rejestru ECC urządzenia GPU (skorygowane, nieskorygowane).
 Wartość zwracana: *JSON*.

Parametr:

- **deviceUUID** - UUID urządzenia GPU.

Aby uzyskać więcej informacji, zobacz plik readme wtyczki NVIDIA GPU.

nvml.device.fan.speed.avg[<deviceUUID>]

 Średnia prędkość wentylatora urządzenia GPU jako wartość procentowa maksymalnej prędkości.
 Zwracana wartość: *Integer*.

Parametr:

- **deviceUUID** — UUID urządzenia GPU.

Więcej informacji można znaleźć w pliku readme wtyczki NVIDIA GPU.

nvml.device.get

 Wykryte procesory GPU z UUID i nazwą.
 Zwracana wartość: *JSON*.

Aby uzyskać więcej informacji, zobacz plik readme wtyczki NVIDIA GPU.

nvml.device.graphics.frequency[<deviceUUID>]

 Częstotliwość zegara grafiki urządzenia GPU w MHz.
 Wartość zwracana: *Integer*.

Parametr:

- **deviceUUID** — UUID urządzenia GPU.

Więcej informacji można znaleźć w pliku readme wtyczki NVIDIA GPU.

nvml.device.memory.fb.get[<deviceUUID>]

 Statystyki pamięci framebuffer urządzenia GPU (całkowita, zarezerwowana, wolna, używana).
 Zwracana wartość: *JSON*.

Parametr:

- **deviceUUID** - UUID urządzenia GPU.

Aby uzyskać więcej informacji, zobacz plik readme wtyczki NVIDIA GPU.

nvml.device.memory.bar1.get[<deviceUUID>]

 Statystyki pamięci BAR1 urządzenia GPU (całkowita, wolna, używana).
 Zwracana wartość: *JSON*.

Parametr:

- **deviceUUID** - UUID urządzenia GPU.

Więcej informacji można znaleźć w pliku readme wtyczki NVIDIA GPU.

nvml.device.memory.frequency[<deviceUUID>]

 Częstotliwość taktowania pamięci urządzenia GPU w MHz.
 Zwracana wartość: *Integer*.

Parametr:

- **deviceUUID** - UUID urządzenia GPU.

Więcej informacji można znaleźć w pliku readme wtyczki NVIDIA GPU.

nvml.device.pci.utilization[<deviceUUID>]

 Wykorzystanie PCI urządzenia GPU (przepustowość nadawania/odbioru w KBps).
 Zwracana wartość: *JSON*.

Parametr:

- **deviceUUID** - UUID urządzenia GPU.

Aby uzyskać więcej informacji, zobacz plik readme wtyczki NVIDIA GPU.

nvml.device.performance.state[<deviceUUID>]

 Stan wydajności urządzenia GPU.
 Zwracana wartość: *Integer*.

Parametr:

- **deviceUUID** — UUID urządzenia GPU.

Więcej informacji można znaleźć w pliku readme wtyczki NVIDIA GPU.

nvml.device.power.limit[<deviceUUID>]

 Limit mocy urządzenia GPU w miliwatach.
 Zwracana wartość: *Liczba całkowita*.

Parametr:

- **deviceUUID** — UUID urządzenia GPU.

Więcej informacji można znaleźć w pliku readme wtyczki NVIDIA GPU.

nvml.device.power.usage[<deviceUUID>]

 Bieżące zużycie energii urządzenia GPU w miliwatach.
 Zwracana wartość: *Integer*.

Parametr:

- **deviceUUID** — UUID urządzenia GPU.

Więcej informacji można znaleźć w pliku readme wtyczki NVIDIA GPU.

nvml.device.serial[<deviceUUID>]

 Numer seryjny urządzenia GPU.
 Zwracana wartość: *String*.

Parametr:

- **deviceUUID** — UUID urządzenia GPU.

Więcej informacji można znaleźć w pliku readme wtyczki NVIDIA GPU.

nvml.device.sm.frequency[<deviceUUID>]

 Częstotliwość zegara multiprocesora strumieniowego urządzenia GPU w MHz.
 Zwracana wartość: *Integer*.

Parametr:

- **deviceUUID** — UUID urządzenia GPU.

Więcej informacji można znaleźć w pliku readme wtyczki NVIDIA GPU.

nvml.device.temperature[<deviceUUID>]

 Temperatura urządzenia GPU w stopniach Celsjusza.
 Zwracana wartość: *Integer*.

Parametr:

- **deviceUUID** — UUID urządzenia GPU.

Więcej informacji można znaleźć w pliku readme wtyczki NVIDIA GPU.

nvml.device.utilization[<deviceUUID>]

 Statystyki wykorzystania urządzenia GPU (wykorzystanie GPU/pamięci jako wartość procentowa).
 Zwracana wartość: *JSON*.

Parametr:

- **deviceUUID** — UUID urządzenia GPU.

Więcej informacji można znaleźć w pliku readme wtyczki NVIDIA GPU.

nvml.device.video.frequency[<deviceUUID>]

 Częstotliwość zegara wideo urządzenia GPU w MHz.
 Zwracana wartość: *Integer*.

Parametr:

- **deviceUUID** - UUID urządzenia GPU.

Więcej informacji można znaleźć w pliku readme wtyczki NVIDIA GPU.

nvml.system.driver.version

 Wersja sterownika NVIDIA.
 Zwracana wartość: *String*.

Więcej informacji można znaleźć w pliku readme wtyczki NVIDIA GPU.

nvml.version

 Wersja biblioteki NVML.
 Zwracana wartość: *String*.

Więcej informacji można znaleźć w pliku readme wtyczki NVIDIA GPU.

oracle.diskgroups.stats[connString,<user>,<password>,<service>,<diskgroup>]

 Zwraca statystyki grup dysków Automatic Storage Management (ASM).
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **connString** - może to być:
  - URI - jeśli nie znaleziono sesji o podanej nazwie, a `Plugins.Oracle.ResolveTNS` jest ustawione na false. Jeśli zawiera schemat (np. ”tcp://”), port (np. 1521) lub oba te elementy, opcja ResolveTNS nie będzie brana pod uwagę i mimo to zostanie potraktowane jako URI;
  - nazwa sesji - jeśli taka nazwa została znaleziona w pliku konfiguracyjnym wtyczki;
  - klucz TNS - jeśli opcja ResolveTNS jest ustawiona na true i nie zachodzi żaden z powyższych warunków;
  - wartość TNS - jeśli zaczyna się od nawiasu otwierającego „(” (początkowe spacje są ignorowane). W takim przypadku opcja ResolveTNS nie jest brana pod uwagę.

- **user** - nazwa użytkownika Oracle; obsługuje dołączenie jednej z opcji logowania `as sysdba`, `as sysoper`, `as sysasm`, `as sysbackup`, `as sysdg`, `as syskm` lub `as sysrac` w formacie `user as sysdba` (wielkość liter w opcji logowania nie ma znaczenia; na końcu nie może występować spacja).
- **password** - hasło Oracle;
- **service** - nazwa usługi Oracle;
- **diskgroup** - nazwa grupy dysków ASM, dla której ma zostać wykonane zapytanie.

oracle.diskgroups.discovery[connString,<user>,<password>,<service>]

 Zwraca listę grup dyskowych ASM. Używane w odkrywaniu niskiego poziomu.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **connString** — może to być:
  - URI — jeśli nie znaleziono sesji o podanej nazwie, a `Plugins.Oracle.ResolveTNS` jest ustawione na false. Jeśli zawiera schemat (np. ”tcp://”), port (np. 1521) lub oba, opcja ResolveTNS nie będzie brana pod uwagę i mimo to będzie traktowane jako URI;
  - nazwa sesji — jeśli taka nazwa została znaleziona w pliku konfiguracyjnym wtyczki;
  - klucz TNS — jeśli opcja ResolveTNS jest ustawiona na true i nie zachodzi żaden z powyższych warunków;
  - wartość TNS — jeśli zaczyna się od nawiasu otwierającego „(” (początkowe spacje są ignorowane). W takim przypadku opcja ResolveTNS nie jest brana pod uwagę.
- **user** — nazwa użytkownika Oracle; obsługuje dołączenie jednej z opcji logowania `as sysdba`, `as sysoper`, `as sysasm`, `as sysbackup`, `as sysdg`, `as syskm` lub `as sysrac` w formacie `user as sysdba` (wielkość liter w opcji logowania nie ma znaczenia, nie może ona zawierać końcowej spacji).
- **password** — hasło Oracle;
- **service** — nazwa usługi Oracle.

oracle.archive.info[connString,<user>,<password>,<service>,<destination>]

 Statystyki logów archiwalnych.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **connString** - może to być:
  - URI - jeśli nie znaleziono sesji o podanej nazwie, a `Plugins.Oracle.ResolveTNS` jest ustawione na false. Jeśli zawiera schemat (np. ”tcp://”), port (np. 1521) lub oba te elementy, opcja ResolveTNS nie będzie brana pod uwagę i mimo to zostanie potraktowane jako URI;
  - nazwa sesji - jeśli taka nazwa została znaleziona w pliku konfiguracyjnym wtyczki;
  - klucz TNS - jeśli opcja ResolveTNS jest ustawiona na true i nie ma zastosowania żaden z powyższych warunków;
  - wartość TNS - jeśli zaczyna się od nawiasu otwierającego „(“ (początkowe spacje są ignorowane). W takim przypadku opcja ResolveTNS nie jest brana pod uwagę.
- **user** - nazwa użytkownika Oracle; obsługuje dołączenie jednej z opcji logowania `as sysdba`, `as sysoper`, `as sysasm`, `as sysbackup`, `as sysdg`, `as syskm` lub `as sysrac` w formacie `user as sysdba` (wielkość liter w opcji logowania nie ma znaczenia; na końcu nie może występować spacja).
- **password** - hasło Oracle;
- **service** - nazwa usługi Oracle;
- **destination** - nazwa miejsca docelowego, które ma zostać odpytane.

oracle.cdb.info[connString,<user>,<password>,<service>,<database>]

 Informacje o bazach danych kontenerów (CDB).
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **connString** — może to być:
  - URI — jeśli nie znaleziono sesji o podanej nazwie, a `Plugins.Oracle.ResolveTNS` jest ustawione na false. Jeśli zawiera schemat (np. ”tcp://”), port (np. 1521) lub oba, opcja ResolveTNS nie będzie brana pod uwagę i mimo to zostanie potraktowane jako URI;
  - nazwa sesji — jeśli taka nazwa zostanie znaleziona w pliku konfiguracyjnym wtyczki;
  - klucz TNS — jeśli opcja ResolveTNS jest ustawiona na true i nie ma zastosowania żaden z powyższych warunków;
  - wartość TNS — jeśli zaczyna się od nawiasu otwierającego „(” (początkowe spacje są ignorowane). W takim przypadku opcja ResolveTNS nie jest brana pod uwagę.
- **user** — nazwa użytkownika Oracle; obsługuje dołączenie jednej z opcji logowania `as sysdba`, `as sysoper`, `as sysasm`, `as sysbackup`, `as sysdg`, `as syskm` lub `as sysrac` w formacie `user as sysdba` (opcja logowania nie rozróżnia wielkości liter i nie może zawierać końcowej spacji).
- **password** — hasło Oracle;
- **service** — nazwa usługi Oracle;
- **database** — nazwa bazy danych, która ma zostać odpytana.

oracle.custom.query[connString,<user>,<password>,<service>,queryName,<args...>]

 Wynik niestandardowego zapytania.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **connString** - może to być:
  - URI - jeśli nie znaleziono sesji o podanej nazwie, a `Plugins.Oracle.ResolveTNS` jest ustawione na false. Jeśli zawiera schemat (np. ”tcp://”), port (np. 1521) lub oba te elementy, opcja ResolveTNS nie będzie brana pod uwagę i mimo to zostanie potraktowane jako URI;
  - nazwa sesji - jeśli taka nazwa została znaleziona w pliku konfiguracyjnym wtyczki;
  - klucz TNS - jeśli opcja ResolveTNS jest ustawiona na true i nie ma zastosowania żaden z powyższych warunków;
  - wartość TNS - jeśli zaczyna się od nawiasu otwierającego “(“ (początkowe spacje są ignorowane). W takim przypadku opcja ResolveTNS nie jest brana pod uwagę.
- **user** - nazwa użytkownika Oracle; obsługuje dołączenie jednej z opcji logowania `as sysdba`, `as sysoper`, `as sysasm`, `as sysbackup`, `as sysdg`, `as syskm` lub `as sysrac` w formacie `user as sysdba` (opcja logowania nie rozróżnia wielkości liter i nie może zawierać końcowej spacji).
- **password** - hasło Oracle;
- **service** - nazwa usługi Oracle;
- **queryName** - nazwa niestandardowego zapytania; musi odpowiadać nazwie pliku SQL bez rozszerzenia;
- **args** - jeden lub kilka argumentów oddzielonych przecinkami, przekazywanych do zapytania.

Uwagi: - Zwracane dane są automatycznie konwertowane do formatu JSON. - Należy unikać bezpośredniego zwracania JSON z zapytań, ponieważ ulegnie on uszkodzeniu, gdy wtyczka spróbuje ponownie przekonwertować go do formatu JSON.

oracle.datafiles.stats[connString,<user>,<password>,<service>]

 Zwraca statystyki plików danych.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **connString** — może to być:
  - URI — jeśli nie znaleziono sesji o podanej nazwie, a `Plugins.Oracle.ResolveTNS` jest ustawione na false. Jeśli zawiera schemat (np. „tcp://”), port (np. 1521) lub oba te elementy, opcja ResolveTNS nie będzie brana pod uwagę i mimo to zostanie potraktowane jako URI;
  - nazwa sesji — jeśli taka nazwa została znaleziona w pliku konfiguracyjnym wtyczki;
  - klucz TNS — jeśli opcja ResolveTNS jest ustawiona na true i nie ma zastosowania żaden z powyższych warunków;
  - wartość TNS — jeśli zaczyna się od nawiasu otwierającego „(” (początkowe spacje są ignorowane). W takim przypadku opcja ResolveTNS nie jest brana pod uwagę.
- **user** — nazwa użytkownika Oracle; obsługuje dołączenie jednej z opcji logowania `as sysdba`, `as sysoper`, `as sysasm`, `as sysbackup`, `as sysdg`, `as syskm` lub `as sysrac` w formacie `user as sysdba` (wielkość liter w opcji logowania nie ma znaczenia; na końcu nie może występować spacja).
- **password** — hasło Oracle;
- **service** — nazwa usługi Oracle.

oracle.db.discovery[connString,<user>,<password>,<service>]

 Zwraca listę baz danych. Używane w low-level discovery.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **connString** — może to być:
  - URI — jeśli nie znaleziono sesji o podanej nazwie, a `Plugins.Oracle.ResolveTNS` jest ustawione na false. Jeśli zawiera schemat (np. ”tcp://”), port (np. 1521) lub oba, opcja ResolveTNS nie będzie brana pod uwagę i mimo to zostanie potraktowane jako URI;
  - nazwa sesji — jeśli taka nazwa została znaleziona w pliku konfiguracyjnym wtyczki;
  - klucz TNS — jeśli opcja ResolveTNS jest ustawiona na true i nie ma zastosowania żaden z powyższych warunków;
  - wartość TNS — jeśli zaczyna się od nawiasu otwierającego „(” (początkowe spacje są ignorowane). W takim przypadku opcja ResolveTNS nie jest brana pod uwagę.
- **user** — nazwa użytkownika Oracle; obsługuje dołączenie jednej z opcji logowania `as sysdba`, `as sysoper`, `as sysasm`, `as sysbackup`, `as sysdg`, `as syskm` lub `as sysrac` w formacie `user as sysdba` (wielkość liter w opcji logowania nie ma znaczenia; na końcu nie może występować spacja).
- **password** — hasło Oracle;
- **service** — nazwa usługi Oracle.

oracle.fra.stats[connString,<user>,<password>,<service>]

 Zwraca statystyki Fast Recovery Area (FRA).
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **connString** - może to być:
  - URI - jeśli nie znaleziono sesji o podanej nazwie, a `Plugins.Oracle.ResolveTNS` jest ustawione na false. Jeśli zawiera schemat (np. ”tcp://”), port (np. 1521) lub oba te elementy, opcja ResolveTNS nie będzie brana pod uwagę i mimo to zostanie potraktowane jako URI;
  - nazwa sesji - jeśli taka nazwa została znaleziona w pliku konfiguracyjnym wtyczki;
  - klucz TNS - jeśli opcja ResolveTNS jest ustawiona na true i nie ma zastosowania żaden z powyższych warunków;
  - wartość TNS - jeśli zaczyna się od nawiasu otwierającego „(” (początkowe spacje są ignorowane). W takim przypadku opcja ResolveTNS nie jest brana pod uwagę.
- **user** - nazwa użytkownika Oracle; obsługuje dołączenie jednej z opcji logowania `as sysdba`, `as sysoper`, `as sysasm`, `as sysbackup`, `as sysdg`, `as syskm` lub `as sysrac` w formacie `user as sysdba` (opcja logowania nie rozróżnia wielkości liter i nie może zawierać końcowej spacji).
- **password** - hasło Oracle;
- **service** - nazwa usługi Oracle.

oracle.instance.info[connString,<user>,<password>,<service>]

 Statystyki instancji.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **connString** - może to być:
  - URI - jeśli nie znaleziono sesji o podanej nazwie, a `Plugins.Oracle.ResolveTNS` jest ustawione na false. Jeśli zawiera schemat (np. ”tcp://”), port (np. 1521) lub oba te elementy, opcja ResolveTNS nie będzie brana pod uwagę i mimo to zostanie potraktowane jako URI;
  - nazwa sesji - jeśli taka nazwa została znaleziona w pliku konfiguracyjnym wtyczki;
  - klucz TNS - jeśli opcja ResolveTNS jest ustawiona na true i żaden z powyższych warunków nie ma zastosowania;
  - wartość TNS - jeśli zaczyna się od nawiasu otwierającego „(“ (początkowe spacje są ignorowane). W takim przypadku opcja ResolveTNS nie jest brana pod uwagę.
- **user** - nazwa użytkownika Oracle; obsługuje dołączenie jednej z opcji logowania `as sysdba`, `as sysoper`, `as sysasm`, `as sysbackup`, `as sysdg`, `as syskm` lub `as sysrac` w formacie `user as sysdba` (wielkość liter w opcji logowania nie ma znaczenia; na końcu nie może występować spacja).
- **password** - hasło Oracle;
- **service** - nazwa usługi Oracle.

oracle.pdb.info[connString,<user>,<password>,<service>,<database>]

 Informacje o bazach danych Pluggable Database (PDB).
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **connString** — może to być:
  - URI — jeśli nie znaleziono sesji o podanej nazwie, a `Plugins.Oracle.ResolveTNS` jest ustawione na false. Jeśli zawiera schemat (np. „tcp://”), port (np. 1521) lub oba te elementy, opcja ResolveTNS nie będzie brana pod uwagę i mimo to zostanie potraktowane jako URI;
  - nazwa sesji — jeśli taka nazwa została znaleziona w pliku konfiguracyjnym wtyczki;
  - klucz TNS — jeśli opcja ResolveTNS jest ustawiona na true i nie ma zastosowania żaden z powyższych warunków;
  - wartość TNS — jeśli zaczyna się od nawiasu otwierającego „(” (początkowe spacje są ignorowane). W takim przypadku opcja ResolveTNS nie jest brana pod uwagę.
- **user** — nazwa użytkownika Oracle; obsługuje dołączenie jednej z opcji logowania `as sysdba`, `as sysoper`, `as sysasm`, `as sysbackup`, `as sysdg`, `as syskm` lub `as sysrac` w formacie `user as sysdba` (opcja logowania nie rozróżnia wielkości liter i nie może zawierać końcowej spacji).
- **password** — hasło Oracle;
- **service** — nazwa usługi Oracle;
- **database** — nazwa bazy danych, do której zostanie wykonane zapytanie.

oracle.pdb.discovery[connString,<user>,<password>,<service>]

 Zwraca listę PDB. Używane do odkrywania niskiego poziomu.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **connString** - może to być:
  - URI - jeśli nie znaleziono sesji o podanej nazwie, a `Plugins.Oracle.ResolveTNS` jest ustawione na false. Jeśli zawiera schemat (np. ”tcp://”), port (np. 1521) lub oba, opcja ResolveTNS nie będzie brana pod uwagę i mimo to zostanie potraktowane jako URI;
  - nazwa sesji - jeśli taka nazwa została znaleziona w pliku konfiguracyjnym wtyczki;
  - klucz TNS - jeśli opcja ResolveTNS jest ustawiona na true i żaden z powyższych warunków nie ma zastosowania;
  - wartość TNS - jeśli zaczyna się od nawiasu otwierającego „(“ (początkowe spacje są ignorowane). W takim przypadku opcja ResolveTNS nie jest brana pod uwagę.

- **user** - nazwa użytkownika Oracle; obsługuje dołączenie jednej z opcji logowania `as sysdba`, `as sysoper`, `as sysasm`, `as sysbackup`, `as sysdg`, `as syskm` lub `as sysrac` w formacie `user as sysdba` (opcja logowania nie rozróżnia wielkości liter i nie może zawierać końcowej spacji).
- **password** - hasło Oracle;
- **service** - nazwa usługi Oracle.

oracle.pga.stats[connString,<user>,<password>,<service>]

 Zwraca statystyki Program Global Area (PGA).
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **connString** — może to być:
  - URI — jeśli nie znaleziono sesji o podanej nazwie, a `Plugins.Oracle.ResolveTNS` jest ustawione na false. Jeśli zawiera schemat (np. „tcp://"), port (np. 1521) lub oba, opcja ResolveTNS nie będzie brana pod uwagę i mimo to zostanie potraktowane jako URI;
  - nazwa sesji — jeśli taka nazwa została znaleziona w pliku konfiguracyjnym wtyczki;
  - klucz TNS — jeśli opcja ResolveTNS jest ustawiona na true i nie ma zastosowania żaden z powyższych warunków;
  - wartość TNS — jeśli zaczyna się od nawiasu otwierającego „(" (początkowe spacje są ignorowane). W takim przypadku opcja ResolveTNS nie jest brana pod uwagę.
- **user** — nazwa użytkownika Oracle; obsługuje dołączenie jednej z opcji logowania `as sysdba`, `as sysoper`, `as sysasm`, `as sysbackup`, `as sysdg`, `as syskm` lub `as sysrac` w formacie `user as sysdba` (wielkość liter w opcji logowania nie ma znaczenia; na końcu nie może występować spacja).
- **password** — hasło Oracle;
- **service** — nazwa usługi Oracle.

oracle.ping[connString,<user>,<password>,<service>]

 Sprawdza, czy można ustanowić połączenie z Oracle.
 Zwracana wartość: *1* - połączenie zostało nawiązane pomyślnie; *0* - połączenie jest zerwane (jeśli występuje jakikolwiek błąd, w tym problemy z AUTH i konfiguracją).

Parametry:

- **connString** - może to być:
  - URI - jeśli nie znaleziono sesji o podanej nazwie, a `Plugins.Oracle.ResolveTNS` jest ustawione na false. Jeśli zawiera schemat (np. "tcp://"), port (np. 1521) lub oba, opcja ResolveTNS nie będzie brana pod uwagę i mimo to zostanie potraktowane jako URI;
  - nazwa sesji - jeśli taka nazwa została znaleziona w pliku konfiguracyjnym wtyczki;
  - klucz TNS - jeśli opcja ResolveTNS jest ustawiona na true i nie ma zastosowania żaden z powyższych warunków;
  - wartość TNS - jeśli zaczyna się od nawiasu otwierającego "(" (początkowe spacje są ignorowane). W takim przypadku opcja ResolveTNS nie jest brana pod uwagę.
- **user** - nazwa użytkownika Oracle; obsługuje dołączenie jednej z opcji logowania `as sysdba`, `as sysoper`, `as sysasm`, `as sysbackup`, `as sysdg`, `as syskm` lub `as sysrac` w formacie `user as sysdba` (wielkość liter w opcji logowania nie ma znaczenia; nie może ona zawierać końcowej spacji).
- **password** - hasło Oracle;
- **service** - nazwa usługi Oracle.

Przykłady:

```
oracle.ping[tcp://127.0.0.1:1521,ZABBIX_MON,zabbix,xe]
oracle.ping[localhost,ZABBIX_MON,zabbix,xe]
oracle.ping[zbx_tns_example,ZABBIX_MON,zabbix,xe]
oracle.ping["(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=localhost)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=x
```

oracle.proc.stats[connString,<user>,<password>,<service>]

 Zwraca statystyki procesów.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **connString** - może to być:
  - URI - jeśli nie znaleziono sesji o podanej nazwie, a `Plugins.Oracle.ResolveTNS` jest ustawione na false. Jeśli zawiera schemat (np. "tcp://"), port (np. 1521) lub oba te elementy, opcja ResolveTNS nie będzie brana pod uwagę i mimo to zostanie potraktowane jako URI;
  - nazwa sesji - jeśli taka nazwa została znaleziona w pliku konfiguracyjnym wtyczki;
  - klucz TNS - jeśli opcja ResolveTNS jest ustawiona na true i nie ma zastosowania żaden z powyższych warunków;
  - wartość TNS - jeśli zaczyna się od nawiasu otwierającego „(" (początkowe spacje są ignorowane). W takim przypadku opcja ResolveTNS nie jest brana pod uwagę.

- **user** - nazwa użytkownika Oracle; obsługuje dołączenie jednej z opcji logowania `as sysdba`, `as sysoper`, `as sysasm`, `as sysbackup`, `as sysdg`, `as syskm` lub `as sysrac` w formacie `user as sysdba` (wielkość liter w opcji logowania nie ma znaczenia; nie może ona zawierać końcowej spacji).
- **password** - hasło Oracle;
- **service** - nazwa usługi Oracle.

oracle.redolog.info[connString,<user>,<password>,<service>]

 Informacje o pliku dziennika z pliku kontrolnego.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **connString** - może to być:
  - URI - jeśli nie znaleziono sesji o podanej nazwie, a `Plugins.Oracle.ResolveTNS` jest ustawione na false. Jeśli zawiera schemat (np. ”tcp://”), port (np. 1521) lub oba, opcja ResolveTNS nie będzie brana pod uwagę i mimo to zostanie potraktowane jako URI;
  - nazwa sesji - jeśli taka nazwa została znaleziona w pliku konfiguracyjnym wtyczki;
  - klucz TNS - jeśli opcja ResolveTNS jest ustawiona na true i nie ma zastosowania żaden z powyższych warunków;
  - wartość TNS - jeśli zaczyna się od nawiasu otwierającego „(” (początkowe spacje są ignorowane). W takim przypadku opcja ResolveTNS nie jest brana pod uwagę.
- **user** - nazwa użytkownika Oracle; obsługuje dołączenie jednej z opcji logowania `as sysdba`, `as sysoper`, `as sysasm`, `as sysbackup`, `as sysdg`, `as syskm` lub `as sysrac` w formacie `user as sysdba` (wielkość liter w opcji logowania nie ma znaczenia, nie może ona zawierać końcowej spacji).
- **password** - hasło Oracle;
- **service** - nazwa usługi Oracle.

oracle.sga.stats[connString,<user>,<password>,<service>]

 Zwraca statystyki System Global Area (SGA).
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **connString** — może to być:
  - URI — jeśli nie znaleziono sesji o podanej nazwie, a `Plugins.Oracle.ResolveTNS` jest ustawione na false. Jeśli zawiera schemat (np. „tcp://”), port (np. 1521) lub oba te elementy, opcja ResolveTNS nie będzie brana pod uwagę i mimo to zostanie potraktowane jako URI;
  - nazwa sesji — jeśli taka nazwa została znaleziona w pliku konfiguracyjnym wtyczki;
  - klucz TNS — jeśli opcja ResolveTNS jest ustawiona na true i nie ma zastosowania żaden z powyższych warunków;
  - wartość TNS — jeśli zaczyna się od nawiasu otwierającego „(” (początkowe spacje są ignorowane). W takim przypadku opcja ResolveTNS nie jest brana pod uwagę.
- **user** — nazwa użytkownika Oracle; obsługuje dołączenie jednej z opcji logowania `as sysdba`, `as sysoper`, `as sysasm`, `as sysbackup`, `as sysdg`, `as syskm` lub `as sysrac` w formacie `user as sysdba` (wielkość liter w opcji logowania nie ma znaczenia, na końcu nie może występować spacja).
- **password** — hasło Oracle;
- **service** — nazwa usługi Oracle.

oracle.sessions.stats[connString,<user>,<password>,<service>,<lockMaxTime>]

 Zwraca statystyki sesji.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **connString** — może to być:
  - URI — jeśli nie znaleziono sesji o podanej nazwie, a `Plugins.Oracle.ResolveTNS` jest ustawione na false. Jeśli zawiera schemat (np. „tcp://”), port (np. 1521) lub oba te elementy, opcja ResolveTNS nie będzie brana pod uwagę i mimo to zostanie potraktowane jako URI;
  - nazwa sesji — jeśli taka nazwa została znaleziona w pliku konfiguracyjnym wtyczki;
  - klucz TNS — jeśli opcja ResolveTNS jest ustawiona na true i nie ma zastosowania żaden z powyższych warunków;
  - wartość TNS — jeśli zaczyna się od nawiasu otwierającego „(” (początkowe spacje są ignorowane). W takim przypadku opcja ResolveTNS nie jest brana pod uwagę.
- **user** — nazwa użytkownika Oracle; obsługuje dołączenie jednej z opcji logowania `as sysdba`, `as sysoper`, `as sysasm`, `as sysbackup`, `as sysdg`, `as syskm` lub `as sysrac` w formacie `user as sysdba` (opcja logowania nie rozróżnia wielkości liter i nie może zawierać końcowej spacji).
- **password** — hasło Oracle;
- **service** — nazwa usługi Oracle;
- **lockMaxTime** — maksymalny czas trwania blokady sesji w sekundach, po którego przekroczeniu sesja jest liczona jako długotrwale zablokowana. Wartość domyślna: 600 sekund.

oracle.sys.metrics[connString,<user>,<password>,<service>,<duration>]

 Zwraca zestaw wartości metryk systemowych.
 Wartość zwracana: *obiekt JSON*.

Parametry:

- **connString** - może to być:
  - URI - jeśli nie znaleziono sesji o podanej nazwie, a `Plugins.Oracle.ResolveTNS` jest ustawione na false. Jeśli zawiera schemat (np. ”tcp://”), port (np. 1521) lub oba te elementy, opcja ResolveTNS nie będzie brana pod uwagę i mimo to zostanie potraktowane jako URI;
  - nazwa sesji - jeśli taka nazwa została znaleziona w pliku konfiguracyjnym wtyczki;
  - klucz TNS - jeśli opcja ResolveTNS jest ustawiona na true i nie ma zastosowania żaden z powyższych warunków;
  - wartość TNS - jeśli zaczyna się od nawiasu otwierającego „(” (początkowe spacje są ignorowane). W takim przypadku opcja ResolveTNS nie jest brana pod uwagę.
- **user** - nazwa użytkownika Oracle; obsługuje dołączenie jednej z opcji logowania `as sysdba`, `as sysoper`, `as sysasm`, `as sysbackup`, `as sysdg`, `as syskm` lub `as sysrac` w formacie `user as sysdba` (wielkość liter w opcji logowania nie ma znaczenia; nie może ona zawierać końcowej spacji).
- **password** - hasło Oracle;
- **service** - nazwa usługi Oracle;
- **duration** - interwał przechwytywania (w sekundach) wartości metryk systemowych. Możliwe wartości: *60* — długi czas trwania (domyślnie), *15* — krótki czas trwania.

oracle.sys.params[connString,<user>,<password>,<service>]

 Zwraca zestaw wartości parametrów systemowych.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **connString** — może to być:
  - URI — jeśli nie znaleziono sesji o podanej nazwie, a `Plugins.Oracle.ResolveTNS` jest ustawione na false. Jeśli zawiera schemat (np. „tcp://”), port (np. 1521) lub oba te elementy, opcja ResolveTNS nie będzie brana pod uwagę i mimo to zostanie potraktowane jako URI;
  - nazwa sesji — jeśli taka nazwa została znaleziona w pliku konfiguracyjnym wtyczki;
  - klucz TNS — jeśli opcja ResolveTNS jest ustawiona na true i nie ma zastosowania żaden z powyższych warunków;
  - wartość TNS — jeśli zaczyna się od nawiasu otwierającego „(” (początkowe spacje są ignorowane). W takim przypadku opcja ResolveTNS nie jest brana pod uwagę.
- **user** — nazwa użytkownika Oracle; obsługuje dołączenie jednej z opcji logowania: `as sysdba`, `as sysoper`, `as sysasm`, `as sysbackup`, `as sysdg`, `as syskm` lub `as sysrac` w formacie `user as sysdba` (wielkość liter w opcji logowania nie ma znaczenia; na końcu nie może występować spacja).
- **password** — hasło Oracle;
- **service** — nazwa usługi Oracle.

oracle.ts.stats[connString,<user>,<password>,<service>,<tablespace>,<type>,<conname>]

 Zwraca statystyki tablespace’ów.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **connString** - może to być:
  - URI - jeśli nie znaleziono sesji o podanej nazwie, a `Plugins.Oracle.ResolveTNS` jest ustawione na false. Jeśli zawiera schemat (np. ”tcp://”), port (np. 1521) lub oba te elementy, opcja ResolveTNS nie będzie brana pod uwagę i mimo to zostanie potraktowane jako URI;
  - nazwa sesji - jeśli taka nazwa została znaleziona w pliku konfiguracyjnym wtyczki;
  - klucz TNS - jeśli opcja ResolveTNS jest ustawiona na true i nie zachodzi żaden z powyższych warunków;
  - wartość TNS - jeśli zaczyna się od nawiasu otwierającego “(” (początkowe spacje są ignorowane). W takim przypadku opcja ResolveTNS nie jest brana pod uwagę.
- **user** - nazwa użytkownika Oracle; obsługuje dołączenie jednej z opcji logowania `as sysdba`, `as sysoper`, `as sysasm`, `as sysbackup`, `as sysdg`, `as syskm` lub `as sysrac` w formacie `user as sysdba` (wielkość liter w opcji logowania nie ma znaczenia, nie może ona zawierać końcowej spacji).
- **password** - hasło Oracle;
- **service** - nazwa usługi Oracle;
- **tablespace** - nazwa tablespace’u, dla którego ma zostać wykonane zapytanie. Wartość domyślna (jeśli pozostawiono puste i ustawiono `type`):
  - ”TEMP” (jeśli `type` jest ustawione na ”TEMPORARY”);
  - ”USERS” (jeśli `type` jest ustawione na ”PERMANENT”).
- **type** - typ tablespace’u, dla którego ma zostać wykonane zapytanie. Wartość domyślna (jeśli ustawiono `tablespace`): ”PERMANENT”.
- **conname** - nazwa kontenera, dla którego wymagane są informacje.

Jeśli `tablespace`, `type` lub `conname` zostanie pominięte, pozycja zwróci statystyki tablespace'ów dla wszystkich pasujących kontenerów (w tym PDB i CDB).

oracle.ts.discovery[connString,<user>,<password>,<service>]

 Zwraca listę tablespace'ów. Używane w low-level discovery.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **connString** - może to być:
  - URI - jeśli nie znaleziono sesji o podanej nazwie, a `Plugins.Oracle.ResolveTNS` jest ustawione na false. Jeśli zawiera schemat (np. "tcp://"), port (np. 1521) lub oba, opcja ResolveTNS nie będzie brana pod uwagę i mimo to zostanie potraktowane jako URI;
  - nazwa sesji - jeśli taka nazwa została znaleziona w pliku konfiguracyjnym wtyczki;
  - klucz TNS - jeśli opcja ResolveTNS jest ustawiona na true i nie ma zastosowania żaden z powyższych warunków;
  - wartość TNS - jeśli zaczyna się od nawiasu otwierającego "(" (początkowe spacje są ignorowane). W takim przypadku opcja ResolveTNS nie jest brana pod uwagę.
- **user** - nazwa użytkownika Oracle; obsługuje dołączenie jednej z opcji logowania `as sysdba`, `as sysoper`, `as sysasm`, `as sysbackup`, `as sysdg`, `as syskm` lub `as sysrac` w formacie `user as sysdba` (wielkość liter w opcji logowania nie ma znaczenia, nie może ona zawierać końcowej spacji).
- **password** - hasło Oracle;
- **service** - nazwa usługi Oracle.

oracle.user.info[connString,<user>,<password>,<service>,<username>]

 Zwraca informacje o użytkowniku Oracle.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **connString** - może to być:
  - URI - jeśli nie znaleziono sesji o podanej nazwie, a `Plugins.Oracle.ResolveTNS` jest ustawione na false. Jeśli zawiera schemat (np. "tcp://"), port (np. 1521) lub oba, opcja ResolveTNS nie będzie brana pod uwagę i mimo to zostanie potraktowane jako URI;
  - nazwa sesji - jeśli taka nazwa została znaleziona w pliku konfiguracyjnym wtyczki;
  - klucz TNS - jeśli opcja ResolveTNS jest ustawiona na true i nie zachodzi żaden z powyższych warunków;
  - wartość TNS - jeśli zaczyna się od nawiasu otwierającego „(" (początkowe spacje są ignorowane). W takim przypadku opcja ResolveTNS nie jest brana pod uwagę.
- **user** - nazwa użytkownika Oracle; obsługuje dołączenie jednej z opcji logowania `as sysdba`, `as sysoper`, `as sysasm`, `as sysbackup`, `as sysdg`, `as syskm` lub `as sysrac` w formacie `user as sysdba` (wielkość liter w opcji logowania nie ma znaczenia; nie może ona zawierać końcowej spacji).
- **password** - hasło Oracle;
- **service** - nazwa usługi Oracle;
- **username** - nazwa użytkownika, dla którego potrzebne są informacje. Nazwy użytkowników zapisane małymi literami nie są obsługiwane. Domyślnie: bieżący użytkownik.

oracle.version[connString,<user>,<password>,<service>]

 Zwraca wersję serwera bazy danych.
 Wartość zwracana: *String*.

Parametry:

- **connString** - może to być:
  - URI - jeśli nie znaleziono sesji o podanej nazwie, a `Plugins.Oracle.ResolveTNS` jest ustawione na false. Jeśli zawiera schemat (np. "tcp://"), port (np. 1521) lub oba, opcja ResolveTNS nie będzie brana pod uwagę i mimo to zostanie potraktowane jako URI;
  - nazwa sesji - jeśli taka nazwa została znaleziona w pliku konfiguracyjnym wtyczki;
  - klucz TNS - jeśli opcja ResolveTNS jest ustawiona na true i nie ma zastosowania żaden z powyższych warunków;
  - wartość TNS - jeśli zaczyna się od nawiasu otwierającego „(" (początkowe spacje są ignorowane). W takim przypadku opcja ResolveTNS nie jest brana pod uwagę.
- **user** - nazwa użytkownika Oracle; obsługuje dołączenie jednej z opcji logowania `as sysdba`, `as sysoper`, `as sysasm`, `as sysbackup`, `as sysdg`, `as syskm` lub `as sysrac` w formacie `user as sysdba` (opcja logowania nie rozróżnia wielkości liter i nie może zawierać końcowej spacji).
- **password** - hasło Oracle;
- **service** - nazwa usługi Oracle.

pgsql.autovacuum.count[uri,<username>,<password>,<database name>]

 Liczba procesów roboczych autovacuum.
 Zwracana wartość: *Integer*.

Parametry:

- **uri** — URI lub nazwa sesji;

- **username, password** — dane uwierzytelniające PostgreSQL;
- **database name** — nazwa bazy danych (jeśli pominięto, używana jest wartość Plugins.PostgreSQL.Default.Database z pliku postgresql.conf).

pgsql.archive[uri,<username>,<password>,<database name>]

 Informacje o zarchiwizowanych plikach.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **uri** - URI lub nazwa sesji;
- **username, password** - dane uwierzytelniające PostgreSQL;
- **database name** - nazwa bazy danych (jeśli pominięto, używana jest wartość Plugins.PostgreSQL.Default.Database z postgresql.conf).

pgsql.bgwriter[uri,<username>,<password>,<database name>]

 Łączna liczba checkpointów dla klastra bazy danych, z podziałem według typu checkpointu.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **uri** - URI lub nazwa sesji;
- **username, password** - poświadczenia PostgreSQL;
- **database name** - nazwa bazy danych (jeśli pominięto, używana jest wartość Plugins.PostgreSQL.Default.Database z pliku postgresql.conf).

pgsql.cache.hit[uri,<username>,<password>,<database name>]

 Współczynnik trafień pamięci podręcznej bufora PostgreSQL.
 Zwracana wartość: *Float*.

Parametry:

- **uri** — URI lub nazwa sesji;
- **username, password** — dane uwierzytelniające PostgreSQL;
- **database name** — nazwa bazy danych (jeśli pominięto, używana jest wartość Plugins.PostgreSQL.Default.Database z pliku postgresql.conf).

pgsql.connections[uri,<username>,<password>,<database name>]

 Zwraca połączenia według typu.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **uri** — URI lub nazwa sesji;
- **username, password** — dane uwierzytelniające PostgreSQL;
- **database name** — nazwa bazy danych (jeśli pominięto, używana jest wartość Plugins.PostgreSQL.Default.Database z pliku postgresql.conf).

pgsql.custom.query[uri,<username>,<password>,queryName,<args...>]

 Zwraca wynik niestandardowego zapytania.
 Wartość zwracana: *obiekt JSON*.

Parametry:

- **uri** - URI lub nazwa sesji;
- **username, password** - dane uwierzytelniające PostgreSQL;
- **queryName** - nazwa niestandardowego zapytania; musi odpowiadać nazwie pliku SQL bez rozszerzenia;
- **args** - jeden lub kilka argumentów oddzielonych przecinkami, przekazywanych do zapytania.

pgsql.db.age[uri,<username>,<password>,<database name>]

 Wiek najstarszego FrozenXID bazy danych.
 Zwracana wartość: *Integer*.

Parametry:

- **uri** — URI lub nazwa sesji;
- **username, password** — dane uwierzytelniające PostgreSQL;
- **database name** — nazwa bazy danych (jeśli pominięto, używana jest wartość Plugins.PostgreSQL.Default.Database z pliku postgresql.conf).

pgsql.db.bloating_tables[uri,<username>,<password>,<database name>]

 Liczba tabel z nadmiernym rozrostem w każdej bazie danych.
 Zwracana wartość: *Integer*.

Parametry:

- **uri** - URI lub nazwa sesji;
- **username, password** - poświadczenia PostgreSQL;
- **database name** - nazwa bazy danych (jeśli pominięto, używana jest wartość Plugins.PostgreSQL.Default.Database z pliku postgresql.conf).

pgsql.db.discovery[uri,<username>,<password>,<database name>]

 Lista baz danych PostgreSQL. Używana do niskopoziomowego wykrywania.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **uri** - URI lub nazwa sesji;
- **username, password** - dane uwierzytelniające PostgreSQL;
- **database name** - nazwa bazy danych (jeśli pominięto, używana jest wartość Plugins.PostgreSQL.Default.Database z postgresql.conf).

pgsql.db.size[uri,<username>,<password>,<database name>]

 Rozmiar bazy danych w bajtach.
 Zwracana wartość: *Integer*.

Parametry:

- **uri** - URI lub nazwa sesji;
- **username, password** - poświadczenia PostgreSQL;
- **database name** - nazwa bazy danych (jeśli pominięto, używana jest wartość Plugins.PostgreSQL.Default.Database z pliku postgresql.conf).

pgsql.dbstat[uri,<username>,<password>,<database name>]

 Zbiera statystyki dla każdej bazy danych. Używane do odkrywania niskiego poziomu.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **uri** — URI lub nazwa sesji;
- **username, password** — poświadczenia PostgreSQL;
- **database name** — nazwa bazy danych (jeśli pominięto, używana jest wartość Plugins.PostgreSQL.Default.Database z postgresql.conf).

pgsql.dbstat.sum[uri,<username>,<password>,<database name>]

 Podsumowane dane dla wszystkich baz danych w klastrze.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **uri** — URI lub nazwa sesji;
- **username, password** — poświadczenia PostgreSQL;
- **database name** — nazwa bazy danych (jeśli pominięto, używana jest wartość Plugins.PostgreSQL.Default.Database z pliku postgresql.conf).

pgsql.locks[uri,<username>,<password>,<database name>]

 Informacje o przyznanych blokadach dla każdej bazy danych. Używane do odkrywania niskiego poziomu.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **uri** — URI lub nazwa sesji;
- **username, password** — dane uwierzytelniające PostgreSQL;
- **database name** — nazwa bazy danych (jeśli pominięto, używana jest wartość Plugins.PostgreSQL.Default.Database z postgresql.conf).

pgsql.oldest.xid[uri,<username>,<password>,<database name>]

 Wiek najstarszego XID.
 Zwracana wartość: *Integer*.

Parametry:

- **uri** — URI lub nazwa sesji;
- **username, password** — dane uwierzytelniające PostgreSQL;
- **database name** — nazwa bazy danych (jeśli pominięto, używana jest wartość Plugins.PostgreSQL.Default.Database z pliku postgresql.conf).

pgsql.ping[uri,<username>,<password>,<database name>]

 Sprawdza, czy połączenie jest aktywne.
 Zwracana wartość: *1* - połączenie jest aktywne; *0* - połączenie jest zerwane (jeśli występuje jakikolwiek błąd, w tym problemy z AUTH i konfiguracją).

Parametry:

- **uri** - URI lub nazwa sesji;
- **username, password** - poświadczenia PostgreSQL;
- **database name** - nazwa bazy danych (jeśli pominięto, używana jest wartość Plugins.PostgreSQL.Default.Database z pliku postgresql.conf).

pgsql.queries[uri,<username>,<password>,<database name>,time period]

 Metryki zapytań według czasu wykonania.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **uri** - URI lub nazwa sesji;
- **username, password** - dane uwierzytelniające PostgreSQL;
- **database name** - nazwa bazy danych (jeśli pominięto, używana jest wartość Plugins.PostgreSQL.Default.Database z pliku postgresql.conf);
- **time period** - limit czasu wykonania dla liczby wolnych zapytań (musi być dodatnią liczbą całkowitą).

pgsql.replication.count[uri,<username>,<password>]

 Liczba serwerów standby.
 Zwracana wartość: *Integer*.

Parametry:

- **uri** - URI lub nazwa sesji;
- **username, password** - poświadczenia PostgreSQL.

pgsql.replication.process[uri,<username>,<password>]

 Opóźnienie flush, opóźnienie zapisu i opóźnienie odtwarzania dla każdego procesu nadawcy.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **uri** - URI lub nazwa sesji;
- **username, password** - dane uwierzytelniające PostgreSQL.

pgsql.replication.process.discovery[uri,<username>,<password>]

 Odkrywanie nazw procesów replikacji.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **uri** - URI lub nazwa sesji;
- **username, password** - poświadczenia PostgreSQL.

pgsql.replication.recovery_role[uri,<username>,<password>]

 Status odzyskiwania.
 Zwracana wartość: *0* - tryb master; *1* - odzyskiwanie jest nadal w toku (tryb standby).

Parametry:

- **uri** - URI lub nazwa sesji;
- **username, password** - dane uwierzytelniające PostgreSQL.

pgsql.replication.status[uri,<username>,<password>]

 Status replikacji.
 Zwracana wartość: *0* - streaming jest wyłączony; *1* - streaming jest włączony; *2* - tryb master.

Parametry:

- **uri** - URI lub nazwa sesji;
- **username, password** - dane uwierzytelniające PostgreSQL.

pgsql.replication_lag.b[uri,<username>,<password>]

 Opóźnienie replikacji w bajtach.
 Zwracana wartość: *Integer*.

Parametry:

- **uri** - URI lub nazwa sesji;
- **username, password** - poświadczenia PostgreSQL.

pgsql.replication_lag.sec[uri,<username>,<password>]

 Opóźnienie replikacji w sekundach.
 Zwracana wartość: *Integer*.

Parametry:

- **uri** - URI lub nazwa sesji;
- **username, password** - dane uwierzytelniające PostgreSQL.

pgsql.uptime[uri,<username>,<password>,<database name>]

 Czas działania PostgreSQL w milisekundach.
 Zwracana wartość: *Float*.

Parametry:

- **uri** — URI lub nazwa sesji;
- **username, password** — dane uwierzytelniające PostgreSQL;
- **database name** — nazwa bazy danych (jeśli pominięto, używana jest wartość Plugins.PostgreSQL.Default.Database z postgresql.conf).

pgsql.version[uri,<username>,<password>,<database name>]

 Zwraca wersję PostgreSQL.
 Wartość zwracana: *String*.

Parametry:

- **uri** - URI lub nazwa sesji;
- **username, password** - dane uwierzytelniające PostgreSQL;
- **database name** - nazwa bazy danych (jeśli pominięto, używana jest wartość Plugins.PostgreSQL.Default.Database z postgresql.conf).

pgsql.wal.stat[uri,<username>,<password>,<database name>]

 Statystyki WAL.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **uri** — URI lub nazwa sesji;
- **username, password** — dane uwierzytelniające PostgreSQL;
- **database name** — nazwa bazy danych (jeśli pominięto, używana jest wartość Plugins.PostgreSQL.Default.Database z pliku postgresql.conf).

redis.config[connString,<password>,<pattern>]

 Pobiera parametry konfiguracyjne instancji Redis pasujące do wzorca.
 Zwracana wartość: *JSON* - jeśli użyto wzorca w stylu glob; pojedyncza wartość - jeśli wzorzec nie zawierał żadnego znaku wieloznacznego.

Parametry:

- **connString** - URI lub nazwa sesji;
- **password** - hasło Redis;
- **pattern** - wzorzec w stylu glob (domyślnie *).

Komentarz:

- Ostrzeżenie dotyczące bezpieczeństwa: `redis.config` uruchamia polecenie Redis `CONFIG GET` i może zwracać wrażliwe parametry konfiguracyjne (na przykład `requirepass`, `masterauth`, ustawienia związane z TLS oraz inne sekrety). Użycie domyślnego wzorca (`*`) lub szerokich wzorców może ujawnić te sekrety każdemu, kto ma uprawnienia do przeglądania wartości pozycji w Zabbix.

redis.info[connString,<password>,<section>]

 Pobiera dane wyjściowe polecenia INFO.
 Wartość zwracana: *JSON* — dane wyjściowe są serializowane do formatu JSON.

Parametry:

- **connString** — URI lub nazwa sesji;
- **password** — hasło Redis;
- **section** — sekcja informacji (domyślnie *default*).

redis.ping[connString,<password>]

 Sprawdza, czy połączenie jest aktywne, czy nie.
 Zwracana wartość: *1* - połączenie jest aktywne; *0* - połączenie jest zerwane (jeśli wystąpi jakikolwiek błąd, w tym problemy z AUTH i konfiguracją).

Parametry:

- **connString** - URI lub nazwa sesji;
- **password** - hasło Redis.

redis.slowlog.count[connString,<password>]

 Liczba wpisów w logu wolnych operacji od momentu uruchomienia Redis.
 Zwracana wartość: *Integer*.

Parametry:

- **connString** — URI lub nazwa sesji;
- **password** — hasło Redis.

smart.attribute.discovery

 Zwraca listę atrybutów urządzenia S.M.A.R.T.
 Zwracana wartość: *obiekt JSON*.

Uwagi:

- Zwracane są następujące makra i ich wartości: {#NAME}, {#DISKTYPE}, {#ID}, {#ATTRNAME}, {#THRESH};
- Obsługiwane są typy dysków HDD, SSD i NVME. Dyski mogą występować samodzielnie lub być połączone w RAID. W przypadku RAID do {#NAME} zostanie dodany dodatkowy element, np.: {"{#NAME}": "/dev/sda cciss,2"}.

smart.disk.discovery[<type>]

 Zwraca listę urządzeń S.M.A.R.T.
 Zwracana wartość: *obiekt JSON*.

Parametr:

- **type** - określa wartość, według której mają być skanowane dyski. Możliwe wartości: *id*, *name* (domyślnie). *id* nie jest obsługiwane w systemie Windows i po wybraniu tej wartości zostanie zwrócony błąd

Uwagi:

- Zwracane są następujące makra i ich wartości: {#NAME}, {#DISKTYPE}, {#MODEL}, {#SN}, {#PATH}, {#ATTRIBUTES}, {#RAIDTYPE};
- Obsługiwane są typy dysków HDD, SSD i NVME. Jeśli dysk nie należy do RAID, {#RAIDTYPE} będzie puste. {#NAME} będzie zawierać dodatkowy element w przypadku RAID, np.: {"{#NAME}": "/dev/sda cciss,2"}.

smart.disk.get[<path>,<raid type>]

 Zwraca wszystkie dostępne właściwości urządzeń S.M.A.R.T.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **path** - ścieżka dysku; jako wartości można użyć makra {#PATH};
- **raid_type** - typ RAID; jako wartości można użyć makra {#RAID}

Uwagi:

- Obsługiwane są dyski typu HDD, SSD i NVME. Dyski mogą działać samodzielnie lub być połączone w RAID;
- Dane obejmują wersję smartctl i argumenty wywołania oraz dodatkowe pola:
disk_name - zawiera nazwę z wymaganymi dodatkami do wykrywania RAID, np.: {"disk_name": "/dev/sda cciss,2"}
disk_type - zawiera typ dysku: HDD, SSD lub NVME, np.: {"disk_type": "ssd"};
- Jeśli nie określono parametrów, pozycja zwróci informacje o wszystkich dyskach.

systemd.unit.get[nazwa jednostki,<interface>]

 Zwraca wszystkie właściwości jednostki systemd.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **nazwa jednostki** - nazwa jednostki (możesz chcieć użyć makra {#UNIT.NAME} w prototypie pozycji, aby wykryć nazwę);
- **interface** - typ interfejsu jednostki, możliwe wartości: *Unit* (domyślnie), *Service*, *Socket*, *Device*, *Mount*, *Automount*, *Swap*, *Target*, *Path*.

Komentarze:

- Ta pozycja jest obsługiwana tylko na platformie Linux;
- LoadState, ActiveState i UnitFileState dla interfejsu Unit są zwracane jako tekst i liczba całkowita: `"ActiveState":{"state":1,"tex`

systemd.unit.info[nazwa jednostki,<właściwość>,<interfejs>]

 Informacja o jednostce systemd.
 Zwracana wartość: *String*.

Parametry:

- **nazwa jednostki** - nazwa jednostki (możesz chcieć użyć makra {#UNIT.NAME} w prototypie pozycji, aby wykryć nazwę);
- **właściwość** - właściwość jednostki (np. ActiveState (domyślnie), LoadState, Description);
- **interfejs** - typ interfejsu jednostki (np. Unit (domyślnie), Socket, Service).

Uwagi:

- Ta pozycja jest obsługiwana tylko na platformie Linux;
- Ta pozycja umożliwia pobranie określonej właściwości z określonego typu interfejsu, jak opisano w dbus API.

Przykłady:

```
systemd.unit.info["{#UNIT.NAME}"] #zbiera informacje o stanie aktywności (active, reloading, inactive, fai
systemd.unit.info["{#UNIT.NAME}",LoadState] #zbiera informacje o stanie załadowania wykrytych jednostek sy
systemd.unit.info[mysqld.service,Id] #pobiera techniczną nazwę usługi (mysqld.service)
systemd.unit.info[mysqld.service,Description] #pobiera opis usługi (MySQL Server)
systemd.unit.info[mysqld.service,ActiveEnterTimestamp] #pobiera ostatni czas przejścia usługi do stanu act
systemd.unit.info[dbus.socket,NConnections,Socket] #zbiera liczbę połączeń z tej jednostki gniazda
```

systemd.unit.discovery[<type>]

 Lista jednostek systemd i ich szczegółów. Używane do odkrywania niskiego poziomu.
 Zwracana wartość: *obiekt JSON*.

Parametr:

- **type** — możliwe wartości: *all*, *automount*, *device*, *mount*, *path*, *service* (domyślnie), *socket*, *swap*, *target*.

Ta pozycja jest obsługiwana tylko na platformie Linux.

web.certificate.get[hostname,<port>,<address>]

 Weryfikuje certyfikaty i zwraca szczegóły certyfikatu.
 Wartość zwracana: *obiekt JSON*.

Parametry:

- **hostname** — może być adresem IP lub nazwą DNS.
Może zawierać schemat URL (*https* tylko), ścieżkę (zostanie zignorowana) oraz port.
Jeśli port zostanie podany zarówno w pierwszym, jak i w drugim parametrze, ich wartości muszą być zgodne.
Jeśli określono address (3. parametr), hostname jest używany wyłącznie do SNI i weryfikacji nazwy hosta;
- **port** — numer portu (domyślnie 443 dla HTTPS);
- **address** — może być adresem IP lub nazwą DNS. Jeśli zostanie określony, będzie używany do połączenia, a hostname (1. parametr) będzie używany do SNI i weryfikacji hosta. W przypadku gdy 1. parametr jest adresem IP, a 3. parametr jest nazwą DNS, 1. parametr będzie używany do połączenia, a 3. parametr będzie używany do SNI i weryfikacji hosta.

Uwagi:

- Ta pozycja staje się nieobsługiwana, jeśli miejsce docelowe określone w konfiguracji hosta nie istnieje, jest niedostępne lub jeśli uzgadnianie TLS zakończy się błędem innym niż nieprawidłowy certyfikat;
- Obecnie rozszerzenie X.509 AIA (Authority Information Access), listy CRL i OCSP (w tym OCSP stapling) oraz Certificate Transparency nie są obsługiwane;
- Pola odpowiedzi JSON:
  - *x509*: zawiera szczegóły certyfikatu X.509.
    - *version*: wersja X.509 (np. 3).
    - *serial_number*: numer seryjny certyfikatu.
    - *signature_algorithm*: algorytm użyty do podpisania certyfikatu (np. `SHA256-RSA`).
    - *issuer*: wystawca certyfikatu.
    - *not_before*: data rozpoczęcia ważności certyfikatu.
    - *not_after*: data wygaśnięcia certyfikatu.
    - *subject*: podmiot certyfikatu.
    - *public_key_algorithm*: algorytm użyty dla klucza publicznego (np. `RSA`).
    - *alternative_names*: alternatywne nazwy podmiotu (jeśli występują), w przeciwnym razie `null`.
  - result: zawiera wynik weryfikacji.
    - *value*: status weryfikacji (zobacz możliwe wartości poniżej).
    - *message*: szczegółowy komunikat weryfikacji (np. `"certificate verified successfully"`).
  - *sha1_fingerprint*: odcisk SHA-1 certyfikatu.
  - *sha256_fingerprint*: odcisk SHA-256 certyfikatu.
- Pole `$.result.value` wskazuje wynik weryfikacji certyfikatu. Możliwe wartości obejmują:
  - *valid* – certyfikat jest prawidłowy i zaufany.
  - *valid-but-self-signed* – certyfikat jest prawidłowy, ale samopodpisany, co oznacza, że jego subject odpowiada issuer.
  - *invalid* – certyfikat jest nieprawidłowy z powodu problemu, takiego jak wygaśnięcie, niepoprawna nazwa hosta lub nieznany urząd podpisujący.

Przykład:

```
web.certificate.get[example.com,443]
```

Odpowiedź JSON:

```
{
  "x509": {
    "version": 3,
    "serial_number": "0ad893bafa68b0b7fb7a404f06ecaf9a",
    "signature_algorithm": "ECDSA-SHA384",
    "issuer": "CN=DigiCert Global G3 TLS ECC SHA384 2020 CA1,O=DigiCert Inc,C=US",
    "not_before": {
      "value": "Jan 15 00:00:00 2025 GMT",
      "timestamp": 1736899200
    },
    "not_after": {
      "value": "Jan 15 23:59:59 2026 GMT",
      "timestamp": 1768521599
    },
    "subject": "CN=*.example.com,O=Internet Corporation for Assigned Names and Numbers,L=Los Angeles,ST=Ca
    "public_key_algorithm": "ECDSA",
    "alternative_names": [
      "*.example.com",
      "example.com"
    ]
  },
  "result": {
    "value": "valid",
    "message": "certificate verified successfully"
  },
  "sha1_fingerprint": "310db7af4b2bc9040c8344701aca08d0c69381e3",
  "sha256_fingerprint": "455943cf819425761d1f950263ebf54755d8d684c25535943976f488bc79d23b"
}
```


2 Windows agent Zabbix

Przegląd

Pozycje agenta Zabbix dla systemu Windows są przedstawione na dwóch listach:

- Pozycje współdzielone — klucze pozycji współdzielone z agentem Zabbix dla systemów UNIX;
- Pozycje specyficzne dla Windows — klucze pozycji obsługiwane **tylko** w systemie Windows.

Należy pamiętać, że wszystkie klucze pozycji obsługiwane przez agent Zabbix w systemie Windows są również obsługiwane przez nowej generacji agent Zabbix 2. Zobacz dodatkowe klucze pozycji, których można używać wyłącznie z agentem 2.

Zobacz także: Minimalne uprawnienia dla pozycji Windows

Wspólne pozycje

Poniższa tabela zawiera pozycje agenta Zabbix, które są obsługiwane w systemie Windows i są współdzielone z agentem Zabbix dla systemów UNIX:

- Klucz pozycji jest linkiem do pełnych informacji o pozycji agenta Zabbix dla systemów UNIX
- Uwzględniono komentarze do pozycji istotne dla systemu Windows

Item key	Description	Item group
log	Monitorowanie pliku dziennika. Ta pozycja nie jest obsługiwana dla dziennika zdarzeń Windows. Parametr `persistent_dir` nie jest obsługiwany w systemie Windows.	Monitorowanie logów
log.count	Liczba dopasowanych wierszy w monitorowanym pliku dziennika. Ta pozycja nie jest obsługiwana dla dziennika zdarzeń Windows. Parametr `persistent_dir` nie jest obsługiwany w systemie Windows.	
logrt	Monitorowanie rotowanego pliku dziennika. Ta pozycja nie jest obsługiwana dla dziennika zdarzeń Windows. Parametr `persistent_dir` nie jest obsługiwany w systemie Windows.	
logrt.count	Liczba dopasowanych wierszy w monitorowanym, rotowanym pliku dziennika. Ta pozycja nie jest obsługiwana dla dziennika zdarzeń Windows. Parametr `persistent_dir` nie jest obsługiwany w systemie Windows.	

Item key	Description	Item group
modbus.get	Odczytuje dane Modbus.	Modbus
net.dns	Sprawdza, czy usługa DNS działa. Parametry `ip`, `timeout` i `count` są ignorowane w systemie Windows, chyba że używany jest Zabbix agent 2.	Sieć
net.dns.perf	Sprawdza wydajność usługi DNS. Parametry `ip`, `timeout` i `count` są ignorowane w systemie Windows, chyba że używany jest Zabbix agent 2.	
net.dns.record	Wykonuje zapytanie DNS. Parametry `ip`, `timeout` i `count` są ignorowane w systemie Windows, chyba że używany jest Zabbix agent 2.	
net.if.discovery	Lista interfejsów sieciowych. Niektóre wersje systemu Windows (na przykład Server 2008) mogą wymagać zainstalowania najnowszych aktualizacji, aby obsługiwać znaki spoza ASCII w nazwach interfejsów.	
net.if.in	Statystyki ruchu przychodzącego na interfejsie sieciowym. W systemie Windows pozycja pobiera wartości z 64-bitowych liczników, jeśli są dostępne. 64-bitowe liczniki statystyk interfejsów zostały wprowadzone w systemach Windows Vista i Windows Server 2008. Jeśli 64-bitowe liczniki nie są dostępne, agent używa liczników 32-bitowych. Obsługiwane są wielobajtowe nazwy interfejsów w systemie Windows. Opisy interfejsów sieciowych w systemie Windows można uzyskać za pomocą pozycji net.if.discovery lub net.if.list.	
net.if.out	Statystyki ruchu wychodzącego na interfejsie sieciowym. W systemie Windows pozycja pobiera wartości z 64-bitowych liczników, jeśli są dostępne. 64-bitowe liczniki statystyk interfejsów zostały wprowadzone w systemach Windows Vista i Windows Server 2008. Jeśli 64-bitowe liczniki nie są dostępne, agent używa liczników 32-bitowych. Obsługiwane są wielobajtowe nazwy interfejsów w systemie Windows. Opisy interfejsów sieciowych w systemie Windows można uzyskać za pomocą pozycji net.if.discovery lub net.if.list.	
net.if.total	Suma statystyk ruchu przychodzącego i wychodzącego na interfejsie sieciowym. W systemie Windows pozycja pobiera wartości z 64-bitowych liczników, jeśli są dostępne. 64-bitowe liczniki statystyk interfejsów zostały wprowadzone w systemach Windows Vista i Windows Server 2008. Jeśli 64-bitowe liczniki nie są dostępne, agent używa liczników 32-bitowych. Opisy interfejsów sieciowych w systemie Windows można uzyskać za pomocą pozycji net.if.discovery lub net.if.list.	
net.tcp.listen	Sprawdza, czy ten port TCP jest w stanie LISTEN.	
net.tcp.port	Sprawdza, czy możliwe jest nawiązanie połączenia TCP z określonym portem.	
net.tcp.service	Sprawdza, czy usługa działa i akceptuje połączenia TCP. Sprawdzanie LDAP i HTTPS w systemie Windows jest obsługiwane tylko przez Zabbix agent 2.	
net.tcp.service.perf	Sprawdza wydajność usługi TCP. Sprawdzanie LDAP i HTTPS w systemie Windows jest obsługiwane tylko przez Zabbix agent 2.	
net.tcp.socket.count	Zwraca liczbę gniazd TCP pasujących do parametrów. Ta pozycja jest obsługiwana w systemie Linux przez Zabbix agent, ale w systemie Windows jest obsługiwana tylko przez Zabbix agent 2 w 64-bitowym systemie Windows.	
net.udp.service	Sprawdza, czy usługa działa i odpowiada na żądania UDP.	
net.udp.service.perf	Sprawdza wydajność usługi UDP.	
net.udp.socket.count	Zwraca liczbę gniazd UDP pasujących do parametrów. Ta pozycja jest obsługiwana w systemie Linux przez Zabbix agent, ale w systemie Windows jest obsługiwana tylko przez Zabbix agent 2 w 64-bitowym systemie Windows.	
proc.get	Lista procesów systemu operacyjnego i ich parametrów. Parametr `cmdline` nie jest obsługiwany w systemie Windows.	Procesy
proc.num	Liczba procesów. W systemie Windows obsługiwane są tylko parametry `name` i `user`.	
system.cpu.discovery	Lista wykrytych procesorów/rdzeni CPU.	System

Item key	Description	Item group
system.cpu.load	Obciążenie CPU. Po uruchomieniu procesu collectora w Zabbix agent inicjalizowane są następujące liczniki wydajności, które są później używane przez tę pozycję: `\System\Processor Queue Length`	
system.cpu.num	Liczba procesorów.	
system.cpu.util	Procent wykorzystania CPU. Wartość jest pobierana przy użyciu licznika wydajności *Processor Time*. Należy pamiętać, że od systemu Windows 8 Menedżer zadań pokazuje wykorzystanie CPU na podstawie licznika wydajności *Processor Utility*, podczas gdy w poprzednich wersjach był to licznik *Processor Time* (zobacz więcej szczegółów). *system* jest jedynym parametrem `type` obsługiwanym w systemie Windows.	
system.hostname	Nazwa hosta systemu. Wartość tej pozycji jest pobierana w systemie Windows za pomocą funkcji GetComputerName() (dla **netbios**), GetComputerNameExA() (dla **fqdn**) lub gethostname() (dla **host**). Zobacz także bardziej szczegółowy opis.	
system.localtime	Czas systemowy.	
system.run	Uruchamia określone polecenie na hoście.	
system.sw.arch	Informacje o architekturze oprogramowania.	
system.sw.os	Informacje o systemie operacyjnym.	
system.sw.os.get	Szczegółowe informacje o systemie operacyjnym (wersja, typ, nazwa dystrybucji, wersja główna i pomocnicza itd.).	
system.swap.size	Rozmiar przestrzeni wymiany w bajtach lub jako procent całości. Parametr typu `pused` jest obsługiwany w systemie Linux przez Zabbix agent, ale w systemie Windows jest obsługiwany tylko przez Zabbix agent 2. Należy pamiętać, że ten klucz może raportować nieprawidłowy rozmiar/procent przestrzeni wymiany na zwirtualizowanych platformach Windows (VMware ESXi, VirtualBox). W takim przypadku można użyć klucza `perf_counter[\700(_Total)\702]`, aby uzyskać prawidłowy procent przestrzeni wymiany.	
system.uname	Identyfikacja systemu. W systemie Windows wartość tej pozycji jest pobierana z klas WMI Win32_OperatingSystem i Win32_Processor. Nazwa systemu operacyjnego (wraz z edycją) może być przetłumaczona na język wyświetlania użytkownika. W niektórych wersjach systemu Windows zawiera symbole znaków towarowych i dodatkowe spacje.	
system.uptime	Czas działania systemu w sekundach.	
vfs.dir.count	Liczba wpisów w katalogu. W systemie Windows dowiązania symboliczne do katalogów są pomijane, a dowiązania twarde są liczone tylko raz.	Wirtualne systemy plików
vfs.dir.get	Lista wpisów w katalogu. W systemie Windows dowiązania symboliczne do katalogów są pomijane, a dowiązania twarde są liczone tylko raz.	
vfs.dir.size	Rozmiar katalogu. W systemie Windows wszelkie dowiązania symboliczne są pomijane, a dowiązania twarde są uwzględniane tylko raz.	
vfs.file.cksum	Suma kontrolna pliku obliczana algorytmem UNIX cksum.	
vfs.file.contents	Pobieranie zawartości pliku.	
vfs.file.exists	Sprawdza, czy plik istnieje. W systemie Windows podwójne cudzysłowy muszą być poprzedzone znakiem ucieczki backslash '\', a cały klucz pozycji musi być ujęty w podwójne cudzysłowy podczas używania narzędzia wiersza poleceń do wywoływania zabbix_get.exe lub agent2. Należy pamiętać, że pozycja może stać się nieobsługiwana w systemie Windows, jeśli katalog jest wyszukiwany wewnątrz nieistniejącego katalogu, np. `vfs.file.exists[C:\no\dir,dir]` (gdzie „no" nie istnieje).	
vfs.file.get	Zwraca informacje o pliku. Obsługiwane typy plików w systemie Windows: zwykły plik, katalog, dowiązanie symboliczne	
vfs.file.md5sum	Suma kontrolna MD5 pliku.	
vfs.file.owner	Pobiera właściciela pliku.	

Item key	Description	Item group
vfs.file.regexp	Pobiera ciąg znaków z pliku.	
vfs.file.regmatch	Znajduje ciąg znaków w pliku.	
vfs.file.size	Rozmiar pliku.	
vfs.file.time	Informacje o czasie pliku. W systemie Windows XP `vfs.file.time[file,change]` może być równe `vfs.file.time[file,access]`.	
vfs.fs.discovery	Lista zamontowanych systemów plików wraz z ich typem i opcjami montowania. Makro {#FSLABEL} jest obsługiwane w systemie Windows.	
vfs.fs.get	Lista zamontowanych systemów plików wraz z ich typem, dostępną przestrzenią dyskową, statystykami inode i opcjami montowania. Makro {#FSLABEL} jest obsługiwane w systemie Windows.	
vfs.fs.size	Przestrzeń dyskowa w bajtach lub jako procent całości.	
vm.memory.size	Rozmiar pamięci w bajtach lub jako procent całości.	Pamięć wirtualna
web.page.get	Pobiera zawartość strony internetowej.	Monitorowanie WWW
web.page.perf	Czas ładowania pełnej strony internetowej.	
web.page.regexp	Znajduje ciąg znaków na stronie internetowej.	
agent.hostmetadata	Metadane hosta agenta.	Zabbix
agent.hostname	Nazwa hosta agenta.	
agent.ping	Sprawdzenie dostępności agenta.	
agent.variant	Wariant agenta Zabbix (Zabbix agent lub Zabbix agent 2).	
agent.version	Wersja agenta Zabbix.	
zabbix.stats	Zwraca zdalnie zestaw wewnętrznych metryk Zabbix server lub proxy.	
zabbix.stats	Zwraca zdalnie liczbę monitorowanych pozycji w kolejce, które są opóźnione na Zabbix server lub proxy.	

Pozycje specyficzne dla systemu Windows

Tabela zawiera szczegółowe informacje o kluczach pozycji, które są obsługiwane **wyłącznie** przez agenta Zabbix dla systemu Windows.

Pozycje specyficzne dla systemu Windows są czasami przybliżonym odpowiednikiem podobnej pozycji agenta, na przykład `proc_info`, obsługiwana w systemie Windows, w przybliżeniu odpowiada pozycji `proc.mem`, nieobsługiwanej w systemie Windows.

Klucz pozycji jest łączem do pełnych informacji o kluczu pozycji.

Klucz pozycji	Opis	Grupa pozycji
eventlog	Monitorowanie dziennika zdarzeń systemu Windows.	Monitorowanie logów
eventlog.count	Liczba wierszy w dzienniku zdarzeń systemu Windows.	
net.if.list	Lista interfejsów sieciowych (obejmuje typ interfejsu, stan, adres IPv4, opis).	Sieć
perf_counter	Wartość dowolnego licznika wydajności systemu Windows.	Liczniki wydajności
perf_counter_en	Wartość dowolnego licznika wydajności systemu Windows w języku angielskim.	
perf_instance.discovery	Lista instancji obiektów liczników wydajności systemu Windows.	
perf_instance_en.discovery	Lista instancji obiektów liczników wydajności systemu Windows, wykrytych przy użyciu nazw obiektów w języku angielskim.	
proc_info	Różne informacje o określonym procesie lub procesach.	Procesy
registry.data	Zwraca dane dla określonej nazwy wartości w kluczu Rejestru systemu Windows.	Rejestr
registry.get	Lista wartości lub kluczy Rejestru systemu Windows znajdujących się pod podanym kluczem.	
service.discovery	Lista usług systemu Windows.	Usługi
service.info	Informacje o usłudze.	
services	Wykaz usług.	
vm.vmemory.size	Rozmiar pamięci wirtualnej w bajtach lub jako wartość procentowa całkowitej pamięci.	Pamięć wirtualna
wmi.get	Wykonuje zapytanie WMI i zwraca pierwszy wybrany obiekt.	WMI
wmi.getall	Wykonuje zapytanie WMI i zwraca całą odpowiedź.	

Szczegóły klucza pozycji

Parametry bez nawiasów ostrych są obowiązkowe. Parametry oznaczone nawiasami ostrymi **< >** są opcjonalne.

eventlog[name,<regexp>,<severity>,<source>,<eventid>,<maxlines>,<mode>]

 Monitorowanie dziennika zdarzeń.
 Zwracana wartość: *Log*.

Parametry:

- **name** - nazwa kanału dziennika zdarzeń (*Log Name* w GUI Podglądu zdarzeń);
- **regexp** - wyrażenie regularne opisujące wymagany wzorzec (z uwzględnieniem wielkości liter);
- **severity** - wyrażenie regularne opisujące poziom ważności (bez uwzględniania wielkości liter). Ten parametr akceptuje wyrażenie regularne oparte na następujących wartościach: ”Information”, ”Warning”, ”Error”, ”Critical”, ”Verbose” (w systemie Windows Vista lub nowszym).
- **source** - wyrażenie regularne opisujące identyfikator źródła (bez uwzględniania wielkości liter);
- **eventid** - wyrażenie regularne opisujące identyfikator(y) zdarzeń (z uwzględnieniem wielkości liter);
- **maxlines** - maksymalna liczba nowych linii na sekundę, które agent wyśle do serwer Zabbix lub proxy. Ten parametr nadpisuje wartość ’MaxLinesPerSecond’ w zabbix_agentd.conf.
- **mode** - możliwe wartości: *all* (domyślnie) lub *skip* - pomija przetwarzanie starszych danych (dotyczy tylko nowo utworzonych pozycji).

Uwagi:

- Pozycja musi być skonfigurowana jako active check;
- agent nie może wysyłać zdarzeń z dziennika ”Forwarded events”;
- Obsługiwany jest Windows Eventing 6.0;
- Wybranie dla tej pozycji typu type of information innego niż Log spowoduje utratę lokalnego znacznika czasu, a także informacji o poziomie ważności i źródle dziennika;
- Zobacz także dodatkowe informacje o monitorowaniu logów.

Przykłady:

```
eventlog[Application]
eventlog[Microsoft-Windows-Application-Experience/Program-Compatibility-Assistant]
eventlog[Security,,"Failure Audit",,^(529|680)$]
eventlog[System,,"Warning|Error"]
eventlog[System,,,,^1$]
eventlog[Windows PowerShell,,,,,,skip]
eventlog[System,,,,@TWOSHORT] #tutaj odwołano się do niestandardowego wyrażenia regularnego o nazwie `TWOS
```

eventlog.count[name,<regexp>,<severity>,<source>,<eventid>,<maxproclines>,<mode>]

 Liczba wierszy w dzienniku zdarzeń systemu Windows.
 Zwracana wartość: *Integer*.

Parametry:

- **name** - nazwa kanału dziennika zdarzeń (*Log Name* w GUI Podglądu zdarzeń);
- **regexp** - wyrażenie regularne opisujące wymagany wzorzec (z uwzględnieniem wielkości liter);
- **severity** - wyrażenie regularne opisujące poziom ważności (bez uwzględniania wielkości liter). Ten parametr akceptuje wyrażenie regularne oparte na następujących wartościach: ”Information”, ”Warning”, ”Error”, ”Critical”, ”Verbose” (w systemie Windows Vista lub nowszym).
- **source** - wyrażenie regularne opisujące identyfikator źródła (bez uwzględniania wielkości liter);
- **eventid** - wyrażenie regularne opisujące identyfikator(y) zdarzeń (z uwzględnieniem wielkości liter);
- **maxproclines** - maksymalna liczba nowych wierszy na sekundę, które agent będzie analizował (nie może przekraczać 10000). Wartość domyślna to 10*’MaxLinesPerSecond’ w zabbix_agentd.conf.
- **mode** - możliwe wartości: *all* (domyślnie) lub *skip* - pomiń przetwarzanie starszych danych (dotyczy tylko nowo utworzonych pozycji).

Uwagi:

- Pozycja musi być skonfigurowana jako sprawdzanie aktywne;
- agent nie może wysyłać zdarzeń z dziennika ”Forwarded events”;
- Obsługiwany jest Windows Eventing 6.0;
- Wybranie dla tej pozycji typu informacji innego niż Log (type of information) spowoduje utratę lokalnego znacznika czasu, a także informacji o ważności i źródle dziennika;
- Zobacz także dodatkowe informacje o monitorowaniu logów.

Przykłady:

```
eventlog.count[System,,"Warning|Error"]
eventlog.count[Windows PowerShell,,,,,,skip]
```

net.if.list

 Lista interfejsów sieciowych (zawiera typ interfejsu, status, adres IPv4, opis).
 Zwracana wartość: *Tekst*.

Uwagi:

- Obsługiwane są nazwy interfejsów wielobajtowych;
- Wyłączone interfejsy nie są wyświetlane;
- Włączanie/wyłączanie niektórych komponentów może zmienić ich kolejność w nazwie interfejsu systemu Windows;
- Niektóre wersje systemu Windows (na przykład Server 2008) mogą wymagać zainstalowania najnowszych aktualizacji, aby obsługiwać znaki spoza ASCII w nazwach interfejsów.

perf_counter[counter,<interval>]

 Wartość dowolnego licznika wydajności systemu Windows.
 Zwracana wartość: *Integer*, *float*, *string* lub *text* (w zależności od żądania).

Parametry:

- **counter** — ścieżka do licznika;
- **interval** — ostatnie N sekund do przechowywania wartości średniej. `interval` musi mieścić się w zakresie od 1 do 900 sekund (włącznie), a wartość domyślna to 1.

Uwagi:

- Ta pozycja obsługuje ścieżki UNC, co może stanowić zagrożenie bezpieczeństwa;
- `interval` jest używany dla liczników wymagających więcej niż jednej próbki (takich jak wykorzystanie CPU), dlatego sprawdzenie za każdym razem zwraca wartość średnią z ostatnich „interval" sekund;
- Do uzyskania listy dostępnych liczników można użyć Monitora wydajności.
- Zobacz także: Liczniki wydajności systemu Windows.

perf_counter_en[counter,<interval>]

 Wartość dowolnego licznika wydajności systemu Windows w języku angielskim.
 Zwracana wartość: *Integer*, *float*, *string* lub *text* (w zależności od żądania).

Parametry:

- **counter** — ścieżka do licznika w języku angielskim;
- **interval** — ostatnie N sekund do przechowywania wartości średniej. Wartość `interval` musi mieścić się w zakresie od 1 do 900 sekund (włącznie), a wartość domyślna to 1.

Uwagi:

- Ta pozycja obsługuje ścieżki UNC, co może stanowić zagrożenie bezpieczeństwa;
- `interval` jest używany dla liczników wymagających więcej niż jednej próbki (takich jak użycie CPU), dlatego sprawdzenie za każdym razem zwraca wartość średnią z ostatnich „interval" sekund;
- Ta pozycja jest obsługiwana tylko w systemach **Windows Server 2008/Vista** i nowszych;
- Listę angielskich ciągów można znaleźć, przeglądając następujący klucz rejestru: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wir NT\CurrentVersion\Perflib\009`.

perf_instance.discovery[object]

 Lista instancji obiektów liczników wydajności systemu Windows. Używana do odkrywania niskiego poziomu.
 Zwracana wartość: *obiekt JSON*.

Parametr:

- **object** — nazwa obiektu (zlokalizowana).

perf_instance_en.discovery[object]

 Lista instancji obiektów liczników wydajności systemu Windows, wykrywanych przy użyciu nazw obiektów w języku angielskim. Używane do odkrywania niskiego poziomu.
 Zwracana wartość: *obiekt JSON*.

Parametr:

- **object** - nazwa obiektu (w języku angielskim).

proc_info[process,<attribute>,<type>]

 Różne informacje o określonym procesie(-ach).
 Wartość zwracana: *Float*.

Parametry:

- **process** — nazwa procesu;
- **attribute** — żądany atrybut procesu;
- **type** — typ reprezentacji (ma znaczenie, gdy istnieje więcej niż jeden proces o tej samej nazwie)

Uwagi:

- Obsługiwane są następujące `attributes`:
vmsize (domyślnie) — rozmiar pamięci wirtualnej procesu w KB
wkset — rozmiar zestawu roboczego procesu (ilość pamięci fizycznej używanej przez proces) w KB
pf — liczba błędów strony
ktime — czas jądra procesu w milisekundach
utime — czas użytkownika procesu w milisekundach
io_read_b — liczba bajtów odczytanych przez proces podczas operacji wejścia/wyjścia
io_read_op — liczba operacji odczytu wykonanych przez proces
io_write_b — liczba bajtów zapisanych przez proces podczas operacji wejścia/wyjścia
io_write_op — liczba operacji zapisu wykonanych przez proces
io_other_b — liczba bajtów przesłanych przez proces podczas operacji innych niż odczyt i zapis
io_other_op — liczba operacji wejścia/wyjścia wykonanych przez proces, innych niż odczyt i zapis
gdiobj — liczba obiektów GDI używanych przez proces
userobj — liczba obiektów USER używanych przez proces;
- Prawidłowe `types` to:
avg (domyślnie) — wartość średnia dla wszystkich procesów o nazwie <process>
min — wartość minimalna spośród wszystkich procesów o nazwie <process>
max — wartość maksymalna spośród wszystkich procesów o nazwie <process>
sum — suma wartości dla wszystkich procesów o nazwie <process>;
- W systemie 64-bitowym do poprawnego działania tej pozycji wymagany jest 64-bitowy agent Zabbix.

Przykłady:

```
proc_info[iexplore.exe,wkset,sum] #pobierz ilość pamięci fizycznej zajmowanej przez wszystkie procesy Inte
proc_info[iexplore.exe,pf,avg] #pobierz średnią liczbę błędów strony dla procesów Internet Explorer
```

registry.data[key,<value name>]

 Zwraca dane dla określonej nazwy wartości w kluczu Rejestru Windows.
 Zwracana wartość: *Integer*, *string* lub *text* (w zależności od typu wartości)

Parametry:

- **key** - klucz rejestru wraz z kluczem głównym; dozwolone są skróty kluczy głównych (np. HKLM);
- **value name** - nazwa wartości rejestru w kluczu (domyślnie pusty ciąg ""); Jeśli nazwa wartości nie zostanie podana, zwracana jest wartość domyślna.

Uwagi:

- Obsługiwane skróty kluczy głównych:
HKCR - HKEY_CLASSES_ROOT
HKCC - HKEY_CURRENT_CONFIG
HKCU - HKEY_CURRENT_USER
HKCULS - HKEY_CURRENT_USER_LOCAL_SETTINGS
HKLM - HKEY_LOCAL_MACHINE
HKPD - HKEY_PERFORMANCE_DATA
HKPN - HKEY_PERFORMANCE_NLSTEXT
HKPT - HKEY_PERFORMANCE_TEXT
HKU - HKEY_USERS
- Klucze zawierające spacje muszą być ujęte w podwójny cudzysłów.

Przykłady:

```
registry.data["HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting"] #zwraca dane wartoś
registry.data["HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting","EnableZip"] #zwraca dane wartości
```

registry.get[key,<mode>,<name regexp>]

 Lista wartości lub kluczy Rejestru Windows znajdujących się w podanym kluczu.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **key** - klucz rejestru wraz z kluczem głównym; dozwolone są skróty kluczy głównych (np. HKLM) (pełną listę skrótów można znaleźć w komentarzach dla registry.data[]);
- **mode** - możliwe wartości:
values (domyślnie) lub *keys*;
- **name regexp** - wykrywaj tylko wartości, których nazwy pasują do wyrażenia regularnego (domyślnie - wykrywane są wszystkie wartości). Dozwolone tylko z *values* jako `mode`.

Klucze zawierające spacje muszą być ujęte w podwójny cudzysłów.

Przykłady:

```
registry.get[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall,values,"^DisplayName|DisplayVersion$
JSON będzie zawierał szczegóły klucza, ostatniego podklucza, nazwy wartości, typu wartości i danych wartoś
registry.get[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall,values] #zwraca dane wszystkich wart
JSON będzie zawierał szczegóły klucza, ostatniego podklucza, nazwy wartości, typu wartości i danych wartoś
```

```
registry.get[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall,keys] #zwraca wszystkie podklucze te
JSON będzie zawierał szczegóły klucza i ostatniego podklucza.
```

service.discovery

 Lista usług Windows. Używana do odkrywania niskiego poziomu.
 Zwracana wartość: *obiekt JSON*.

service.info[service,<param>]

 Informacje o usłudze.
 Wartość zwracana: *Integer* - gdy `param` to *state*, *startup*; *String* - gdy `param` to *displayname*, *path*, *user*; *Text* - gdy `param` to *description*
Dokładnie dla *state*: 0 - uruchomiona, 1 - wstrzymana, 2 - oczekiwanie na uruchomienie, 3 - oczekiwanie na wstrzymanie, 4 - oczekiwanie na wznowienie, 5 - oczekiwanie na zatrzymanie, 6 - zatrzymana, 7 - nieznany, 255 - brak takiej usługi
Dokładnie dla *startup*: 0 - automatyczny, 1 - automatyczny opóźniony, 2 - ręczny, 3 - wyłączony, 4 - nieznany, 5 - automatyczny start wyzwalany, 6 - automatyczny opóźniony start wyzwalany, 7 - ręczny start wyzwalany

Parametry:

- **service** - rzeczywista nazwa usługi lub jej nazwa wyświetlana widoczna w przystawce MMC Services;
- **param** - *state* (domyślnie), *displayname*, *path*, *user*, *startup* lub *description*.

Uwagi:

- Pozycje takie jak `service.info[service,state]` i `service.info[service]` zwrócą te same informacje;
- Tylko gdy `param` to *state*, ta pozycja zwraca wartość dla nieistniejących usług (255).

Przykłady:

```
service.info[SNMPTRAP] - stan usługi SNMPTRAP;
service.info[SNMP Trap] - stan tej samej usługi, ale z podaną nazwą wyświetlaną;
service.info[EventLog,startup] - typ uruchamiania usługi EventLog
```

services[<type>,<state>,<exclude>]

 Lista usług.
 Zwracana wartość: *0* - jeśli pusta; *Text* - lista usług rozdzielonych znakiem nowej linii.

Parametry:

- **type** - *all* (domyślnie), *automatic*, *manual* lub *disabled*;
- **state** - *all* (domyślnie), *stopped*, *started*, *start_pending*, *stop_pending*, *running*, *continue_pending*, *pause_pending* lub *paused*;
- **exclude** - usługi, które należy wykluczyć z wyniku. Wykluczane usługi powinny być podane w podwójnych cudzysłowach, rozdzielone przecinkami, bez spacji.

Przykłady:

```
services[,started] #zwraca listę uruchomionych usług;
services[automatic, stopped] #zwraca listę zatrzymanych usług, które powinny być uruchomione;
services[automatic, stopped, "service1,service2,service3"] #zwraca listę zatrzymanych usług, które powinny
```

vm.vmemory.size[<type>]

 Rozmiar pamięci wirtualnej w bajtach lub jako procent całości.
 Zwracana wartość: *Integer* - dla bajtów; *float* - dla wartości procentowej.

Parametr:

- **type** - możliwe wartości: *available* (dostępna pamięć wirtualna), *pavailable* (dostępna pamięć wirtualna, w procentach), *pused* (używana pamięć wirtualna, w procentach), *total* (całkowita pamięć wirtualna, domyślnie) lub *used* (używana pamięć wirtualna)

Komentarze:

- Monitorowanie statystyk pamięci wirtualnej opiera się na:
  - Całkowitej pamięci wirtualnej w systemie Windows (całkowita pamięć fizyczna + rozmiar pliku stronicowania);
  - Maksymalnej ilości pamięci, którą agent Zabbix może przydzielić;
  - Bieżącym limicie pamięci przydzielonej dla systemu lub agent Zabbix, w zależności od tego, która wartość jest mniejsza.

Przykład:

```
vm.vmemory.size[pavailable] #zwraca dostępną pamięć wirtualną, w procentach
```

wmi.get[<namespace>,<query>]

 Wykonuje zapytanie WMI i zwraca pierwszy wybrany obiekt.
 Wartość zwracana: *Integer*, *float*, *string* lub *text* (w zależności od żądania).

Parametry:

- **namespace** - przestrzeń nazw WMI;
- **query** - zapytanie WMI zwracające pojedynczy obiekt.

Zapytania WMI są wykonywane przy użyciu WQL.

Przykład:

```
wmi.get[root\cimv2,select status from Win32_DiskDrive where Name like '%PHYSICALDRIVE0%'] #zwraca status p
```

wmi.getall[<namespace>,<query>]

 Wykonuje zapytanie WMI i zwraca całą odpowiedź. Może być używane do odkrywania niskiego poziomu.
 Wartość zwracana: *obiekt JSON*

Parametry:

- **namespace** — przestrzeń nazw WMI;
- **query** — zapytanie WMI.

Uwagi:

- Zapytania WMI są wykonywane przy użyciu WQL.
- Preprocessing JSONPath może być używany do wskazywania bardziej szczegółowych wartości w zwróconym JSON.

Przykład:

```
wmi.getall[root\cimv2,select * from Win32_DiskDrive where Name like '%PHYSICALDRIVE%'] #zwraca informacje
```

Monitorowanie usług Windows

Ten samouczek zawiera instrukcje krok po kroku dotyczące konfiguracji monitorowania usług Windows. Zakłada się, że serwer Zabbix i agent są skonfigurowane i działają poprawnie.

Krok 1

Pobierz nazwę usługi.

Nazwę usługi można uzyskać, przechodząc do przystawki MMC Services i otwierając właściwości usługi. Na karcie *General* powinno być widoczne pole o nazwie „Service name". Następująca po nim wartość to nazwa, której użyjesz podczas konfigurowania pozycji do monitorowania. Na przykład, jeśli chcesz monitorować usługę „workstation", nazwa usługi może być następująca: **lanmanworkstation**.

Krok 2

Skonfiguruj pozycję do monitorowania usługi.

Pozycja `service.info[service,<param>]` pobiera informacje o określonej usłudze. W zależności od potrzebnych informacji należy określić opcję `param`, która przyjmuje następujące wartości: *displayname*, *state*, *path*, *user*, *startup* lub *description*. Wartością domyślną jest *state*, jeśli `param` nie zostanie określony (`service.info[service]`).

Typ zwracanej wartości zależy od wybranego `param`: integer dla *state* i *startup*; character string dla *displayname*, *path* i *user*; text dla *description*.

Przykład:

- *Klucz:* `service.info[lanmanworkstation]`
- *Typ informacji:* Numeryczny (bez znaku)

Pozycja `service.info[lanmanworkstation]` pobierze informacje o stanie usługi jako wartość liczbową. Aby odwzorować wartość liczbową na reprezentację tekstową we frontendzie („0" jako „Running", „1" jako „Paused" itd.), można skonfigurować mapowanie wartości na hoście, na którym skonfigurowano pozycję. Aby to zrobić, należy albo podłączyć szablon *Windows services by Zabbix agent* lub *Windows services by Zabbix agent active* do hosta, albo skonfigurować na hoście nową mapę wartości opartą na mapie wartości *Windows service state* skonfigurowanej we wspomnianych szablonach.

Należy pamiętać, że oba wspomniane szablony mają skonfigurowaną regułę wykrywania, która będzie automatycznie wykrywać usługi. Jeśli nie jest to pożądane, można wyłączyć regułę wykrywania na poziomie hosta po podłączeniu szablonu do hosta.

Wykrywanie usług Windows

Wykrywanie niskiego poziomu zapewnia sposób na automatyczne tworzenie pozycji, wyzwalaczy i wykresów dla różnych obiektów na komputerze. Zabbix może automatycznie rozpocząć monitorowanie usług Windows na komputerze, bez potrzeby znajomości

dokładnej nazwy usługi ani ręcznego tworzenia pozycji dla każdej usługi. Filtr może zostać użyty do generowania rzeczywistych pozycji, wyzwalaczy i wykresów tylko dla interesujących usług.

2 SNMP agent

Przegląd

Możesz chcieć używać monitorowania SNMP na urządzeniach takich jak drukarki, przełączniki sieciowe, routery czy UPS-y, które zwykle mają włączoną obsługę SNMP i na których próba skonfigurowania kompletnych systemów operacyjnych oraz agentów Zabbix byłaby niepraktyczna.

Aby można było pobierać dane udostępniane przez agenty SNMP na tych urządzeniach, serwer Zabbix musi być wstępnie skonfigurowany z obsługą SNMP przez podanie flagi `--with-net-snmp`. Zaleca się również zainstalowanie plików MIB, aby mieć pewność, że wartości pozycji są wyświetlane w prawidłowym formacie. Bez plików MIB mogą występować problemy z formatowaniem, takie jak wyświetlanie wartości w formacie HEX zamiast UTF-8 lub odwrotnie.

Kontrole SNMP są wykonywane wyłącznie przez protokół UDP.

Demony serwera Zabbix i proxy zapisują w logach wiersze podobne do poniższego, jeśli otrzymają nieprawidłową odpowiedź SNMP:

```
SNMP response from host "gateway" does not contain all of the requested variable bindings
```

Chociaż nie obejmują one wszystkich problematycznych przypadków, są przydatne do identyfikowania poszczególnych urządzeń SNMP, dla których należy wyłączyć żądania łączone.

Serwer/proxy Zabbix ponowi próbę maksymalnie 5 razy dla pozycji SNMP `walk` i `get`. Mechanizm ponawiania nie ma zastosowania do błędów rozwiązywania DNS.

W przypadku starszych kontroli SNMP (pojedynczy numer OID lub ciąg znaków) serwer/proxy Zabbix ponowi próbę co najmniej jeden raz po nieudanej próbie zapytania: albo za pomocą mechanizmu ponawiania biblioteki SNMP, albo za pomocą wewnętrznego mechanizmu przetwarzania łączonego.

Warning:
Jeśli monitorujesz urządzenia SNMPv3, upewnij się, że msgAuthoritativeEngineID (znane również jako snmpEngineID lub "Engine ID") nigdy nie jest współdzielone przez dwa urządzenia. Zgodnie z RFC 2571 (sekcja 3.1.1.1) musi być unikalne dla każdego urządzenia.

Warning:
RFC3414 wymaga, aby urządzenia SNMPv3 zachowywały swoje engineBoots. Niektóre urządzenia tego nie robią, co powoduje, że ich komunikaty SNMP są odrzucane jako nieaktualne po ponownym uruchomieniu. W takiej sytuacji pamięć podręczna SNMP musi zostać ręcznie wyczyszczona na serwerze/proxy (za pomocą -R snmp_cache_reload) albo serwer/proxy musi zostać ponownie uruchomiony.

Note:
Zabbix buforuje mapowania SNMPv3 EngineID → IP i ponownie wykorzystuje zapisane w pamięci podręcznej EngineID przy kolejnych kontrolach zamiast każdorazowo wysyłać zapytanie sondujące, co zmniejsza ruch sieciowy. Jeśli EngineID nie może zostać użyte ponownie, zostanie wykoniona ponowna próba z zapytaniem sondującym w celu wykrycia nowego EngineID.

Konfigurowanie monitorowania SNMP

Aby rozpocząć monitorowanie urządzenia za pomocą SNMP, należy wykonać następujące kroki:

Krok 1

Ustal ciąg SNMP (lub OID) pozycji, którą chcesz monitorować.

Aby uzyskać listę ciągów SNMP, użyj polecenia **snmpwalk** (części oprogramowania net-snmp, które powinno być zainstalowane w ramach instalacji Zabbix) lub równoważnego narzędzia:

```
snmpwalk -v 2c -c public <host IP> .
```

Ponieważ '2c' oznacza tutaj wersję SNMP, możesz również zastąpić ją wartością '1', aby wskazać SNMP Version 1 na urządzeniu.

Powinno to zwrócić listę ciągów SNMP i ich ostatnią wartość. Jeśli tak się nie stanie, możliwe jest, że SNMP 'community' różni się od standardowego 'public'; w takim przypadku trzeba ustalić, jaka ona jest.

Następnie możesz przejrzeć listę, aż znajdziesz ciąg, który chcesz monitorować, np. jeśli chcesz monitorować bajty przychodzące do przełącznika na porcie 3, użyj ciągu `IF-MIB::ifHCInOctets.3` z tego wiersza:

```
IF-MIB::ifHCInOctets.3 = Counter64: 3409739121
```

Możesz teraz użyć polecenia **snmpget**, aby ustalić numeryczny OID dla 'IF-MIB::ifHCInOctets.3':

```
snmpget -v 2c -c public -On <host IP> IF-MIB::ifHCInOctets.3
```

Zwróć uwagę, że ostatnia liczba w ciągu to numer portu, który chcesz monitorować. Zobacz także: Indeksy dynamiczne.

Powinno to zwrócić coś podobnego do poniższego:

```
.1.3.6.1.2.1.31.1.1.1.6.3 = Counter64: 3472126941
```

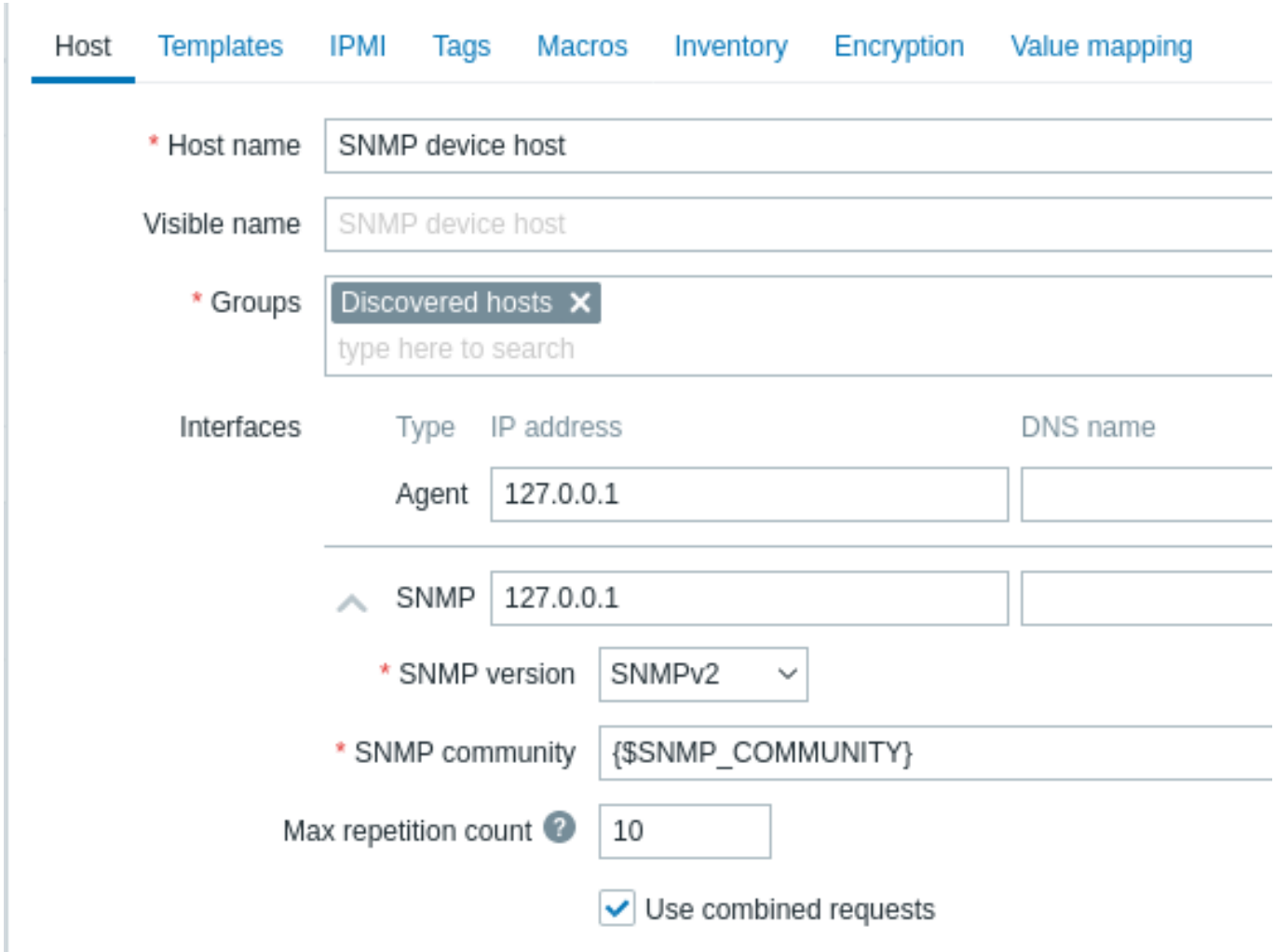
Ponownie, ostatnia liczba w OID to numer portu.

Note:
Niektóre z najczęściej używanych OID-ów SNMP są automatycznie tłumaczone na reprezentację numeryczną przez Zabbix.

W ostatnim przykładzie powyżej typ wartości to "Counter64", co wewnętrznie odpowiada typowi ASN_COUNTER64. Pełna lista obsługiwanych typów to ASN_COUNTER, ASN_COUNTER64, ASN_UINTEGER, ASN_UNSIGNED64, ASN_INTEGER, ASN_INTEGER64, ASN_FLOAT, ASN_DOUBLE, ASN_TIMETICKS, ASN_GAUGE, ASN_IPADDRESS, ASN_OCTET_STR oraz ASN_OBJECT_ID. Typy te w przybliżeniu odpowiadają wartościom "Counter32", "Counter64", "UInteger32", "INTEGER", "Float", "Double", "Timeticks", "Gauge32", "IpAddress", "OCTET STRING", "OBJECT IDENTIFIER" w danych wyjściowych **snmpget**, ale mogą być również wyświetlane jako "STRING", "Hex-STRING", "OID" i inne, w zależności od obecności wskazówki wyświetlania.

Krok 2

Utwórz host odpowiadający urządzeniu.



Dodaj interfejs SNMP dla hosta:

- Wprowadź adres IP/nazwę DNS oraz numer portu.
- Wybierz *wersję SNMP* z listy rozwijanej.

- Dodaj poświadczenia interfejsu zależnie od wybranej wersji SNMP:
  - SNMPv1, v2 wymagają tylko community (zwykle 'public').
  - SNMPv3 wymaga bardziej szczegółowych opcji (patrz poniżej).
- Określ wartość maksymalnej liczby powtórzeń (domyślnie: 10) dla natywnych zbiorczych żądań SNMP (GetBulkRequest-PDUs); tylko dla pozycji `discovery[]` i `walk[]` w SNMPv2 i v3. Pamiętaj, że ustawienie zbyt wysokiej wartości może spowodować przekroczenie limitu czasu sprawdzania agent SNMP.
- Zaznacz pole wyboru *Użyj żądań łączonych*, aby zezwolić na przetwarzanie łączone żądań SNMP (niezwiązane z natywnymi zbiorczymi żądaniami SNMP „walk" i „get").

Parametr SNMPv3	Opis
Nazwa kontekstu	Wprowadź nazwę kontekstu, aby zidentyfikować pozycja w podsieci SNMP. Makra użytkownika są rozwijane w tym polu.
Nazwa bezpieczeństwa	Wprowadź nazwę bezpieczeństwa. Makra użytkownika są rozwijane w tym polu.
Poziom bezpieczeństwa	Wybierz poziom bezpieczeństwa: **noAuthNoPriv** — nie są używane ani protokoły uwierzytelniania, ani prywatności **AuthNoPriv** — używany jest protokół uwierzytelniania, protokół prywatności nie jest używany **AuthPriv** — używane są zarówno protokoły uwierzytelniania, jak i prywatności
Protokół uwierzytelniania	Wybierz protokół uwierzytelniania — *MD5*, *SHA1*; w net-snmp 5.8 i nowszych także *SHA224*, *SHA256*, *SHA384* lub *SHA512*.
Hasło uwierzytelniania	Wprowadź hasło uwierzytelniania. Makra użytkownika są rozwijane w tym polu.
Protokół prywatności	Wybierz protokół prywatności — *DES*, *AES128*, *AES192*, *AES256*, *AES192C* (Cisco) lub *AES256C* (Cisco). Zobacz uwagi dotyczące obsługi protokołu prywatności
Hasło prywatności	Wprowadź hasło prywatności. Makra użytkownika są rozwijane w tym polu.

W przypadku nieprawidłowych poświadczeń SNMPv3 (nazwa bezpieczeństwa, protokół/hasło uwierzytelniania, protokół prywatności):

- Zabbix otrzymuje błąd ERROR z net-snmp, z wyjątkiem nieprawidłowego *Hasła prywatności*, w którym to przypadku Zabbix otrzymuje błąd TIMEOUT z net-snmp.
- Dostępność interfejsu SNMP zmieni się na czerwoną (niedostępny).

Note:
Zmiany w *Protokole uwierzytelniania*, *Haśle uwierzytelniania*, *Protokole prywatności* lub *Haśle prywatności*, wprowadzone bez zmiany *Nazwy bezpieczeństwa*, są zwykle stosowane automatycznie po zaktualizowaniu odpowiedniego interfejsu SNMPv3 w Zabbix. W przypadkach, gdy *Nazwa bezpieczeństwa* również zostanie zmieniona, wszystkie parametry zostaną zaktualizowane natychmiast.

Możesz użyć jednego z dostarczonych szablonów SNMP, który automatycznie doda zestaw pozycji. Przed użyciem szablonu sprawdź, czy jest on zgodny z hostem.

Kliknij *Dodaj*, aby zapisać host.

Obsługa protokołów prywatności

W zależności od systemu operacyjnego i konfiguracji net-snmp niektóre protokoły prywatności mogą nie być dostępne:

- W niektórych nowszych systemach operacyjnych (na przykład RHEL9) obsługa DES została usunięta z pakietu net-snmp.
- Protokoły szyfrowania AES192 i silniejsze nie są obsługiwane od razu po instalacji w systemach operacyjnych starszych niż RHEL 8, CentOS 8, Oracle Linux 8, Debian 12, Ubuntu LTS 22.04, openSUSE Leap 15.5.

Aby sprawdzić, czy biblioteka net-snmp obsługuje AES192+, użyj jednej z poniższych opcji:

1. `net-snmp-config`:

```
net-snmp-config --configure-options
```

Jeśli dane wyjściowe zawierają `--enable-blumenthal-aes`, AES192+ jest obsługiwane.

Pamiętaj, że net-snmp-config jest częścią pakietu deweloperskiego dla SNMP (libsnmp-dev dla Debian/Ubuntu, net-snmp-devel dla CentOS/RHEL/OL/SUSE) i może nie być domyślnie zainstalowany.

2. `snmpget`:

```
snmpget -v 3 -x AES-256
```

Jeśli dane wyjściowe zawierają `Invalid privacy protocol specified after -3x flag: AES-256`, AES192+ nie jest obsługiwane. Jeśli dane wyjściowe zawierają `No hostname specified.`, AES192+ nie jest obsługiwane.

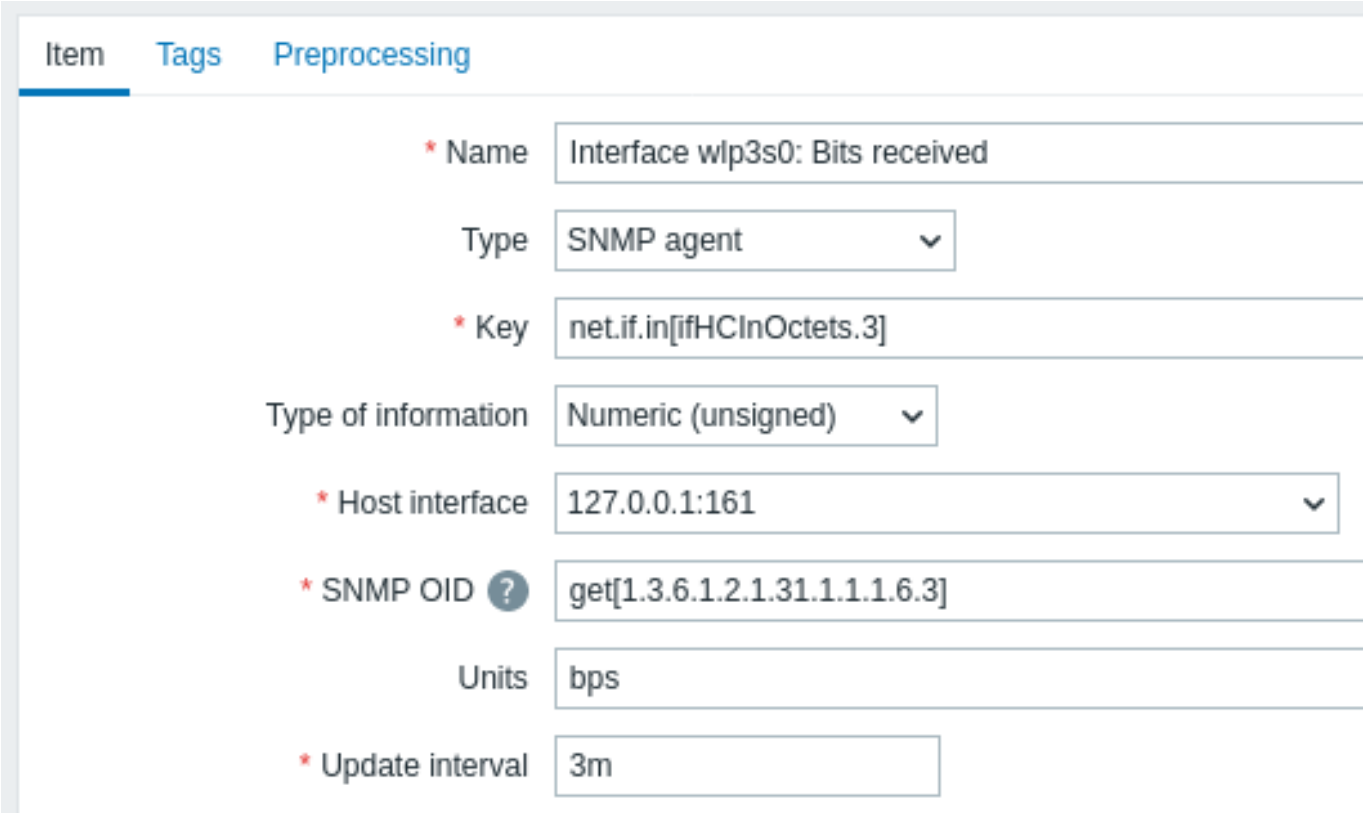
Jeśli biblioteka net-snmp nie obsługuje protokołów AES192 i wyższych, skompiluj ponownie net-snmp z opcją `--enable-blumenthal-aes`, a następnie skompiluj ponownie serwer Zabbix, podając opcję `--with-net-snmp=/home/user/yourcustomnetsnmp/bin/net-snmp-co`

Krok 3

Utwórz pozycję do monitorowania.

Teraz wróć do Zabbix i kliknij *Pozycje* dla hosta SNMP, którego utworzyłeś wcześniej. W zależności od tego, czy podczas tworzenia hosta użyto szablonu, czy nie, zobaczysz albo listę pozycji SNMP powiązanych z hostem, albo po prostu pustą listę. Załóżmy, że zamierzasz samodzielnie utworzyć pozycję, korzystając z informacji, które właśnie zebrałeś za pomocą snmpwalk i snmpget, więc kliknij *Utwórz pozycję*.

Wypełnij wymagane parametry w formularzu nowej pozycji:



Parametr	Opis
Nazwa	Wprowadź nazwę pozycji.
Typ	Wybierz tutaj **agent SNMP**.
Klucz	Wprowadź klucz o sensownej nazwie.
Interfejs hosta	Upewnij się, że wybrano interfejs SNMP, np. przełącznika/routera.

Parametr	Opis
SNMP OID	Użyj jednego z obsługiwanych formatów, aby wprowadzić wartość(-ci) OID: **walk[OID1,OID2,...]** - pobiera poddrzewo wartości. Na przykład: `walk[1.3.6.1.2.1.2.2.1.2,1.3.6.1.2.1.2.2.1.3]`. Ta opcja wykorzystuje natywne żądania zbiorcze SNMP (GetBulkRequest-PDUs) asynchronicznie. Ustawienia limitu czasu dla tej pozycji można skonfigurować w formularzu konfiguracji pozycji. Rozważ ustawienie niskiej wartości limitu czasu, aby uniknąć długich opóźnień, jeśli urządzenie jest nieosiągalne, ponieważ zostanie wykonanych do 5 ponowień, jeśli wcześniejsze próby przekroczą limit czasu lub zakończą się niepowodzeniem (np. 3-sekundowy limit czasu może skutkować 15-sekundowym czasem oczekiwania). Możesz użyć tej pozycji jako pozycji nadrzędnej, a pozycje zależne mogą wyodrębniać dane z pozycji nadrzędnej za pomocą przetwarzania wstępnego. Możliwe jest określenie wielu OID w jednym przebiegu snmp walk, na przykład `walk[OID1,OID2,...]`, aby asynchronicznie przetwarzać po jednym OID naraz. Jeśli żądanie zbiorcze nie zwróci wyników, podejmowana jest próba pobrania pojedynczego rekordu bez użycia żądania zbiorczego. Nazwy MIB są obsługiwane jako parametry; dlatego `walk[1.3.6.1.2.1.2.2.1.2]` i `walk[ifDescr]` zwrócą ten sam wynik. Jeśli określono kilka OID/MIB, tj. `walk[ifDescr,ifType,ifPhysAddress]`, wynik będzie listą połączoną. Żądania GetBulk są używane z interfejsami SNMPv2 i v3, a GetNext z interfejsami SNMPv1; parametr maksymalnej liczby powtórzeń dla żądań zbiorczych jest konfigurowany na poziomie interfejsu. Parametr maksymalnej liczby powtórzeń wpływa na żądania zbiorcze, określając maksymalną liczbę OID zwracanych w jednej odpowiedzi zbiorczej. Wyższa wartość skutkuje większymi odpowiedziami zbiorczymi, zmniejszając liczbę wymaganych transmisji. Jednak nie wszystkie urządzenia mogą obsługiwać bardzo wysokie wartości, co może powodować problemy. Ta pozycja zwraca dane wyjściowe narzędzia snmpwalk z parametrami -Oe -Ot -On. Możesz użyć tej pozycji jako pozycji nadrzędnej w wykrywaniu SNMP. **get[OID]** - pobiera *pojedynczą* wartość asynchronicznie. Na przykład: `get[1.3.6.1.2.1.31.1.1.1.6.3]` Ustawienia limitu czasu dla tej pozycji można skonfigurować w formularzu konfiguracji pozycji. Rozważ ustawienie niskiej wartości limitu czasu, aby uniknąć długich opóźnień, jeśli urządzenie jest nieosiągalne, ponieważ zostanie wykonanych do 5 ponowień, jeśli wcześniejsze próby przekroczą limit czasu lub zakończą się niepowodzeniem (np. 3-sekundowy limit czasu może skutkować 15-sekundowym czasem oczekiwania). **OID** - (starszy sposób) wprowadź pojedynczy tekstowy lub numeryczny OID, aby synchronicznie pobrać pojedynczą wartość, opcjonalnie połączoną z innymi wartościami. Na przykład: `1.3.6.1.2.1.31.1.1.1.6.3`. Dla tej opcji limit czasu sprawdzania pozycji będzie równy wartości ustawionej w pliku konfiguracyjnym serwera. **Zaleca się** używanie pozycji `walk[OID]` i `get[OID]` dla lepszej wydajności. Wszystkie pozycje `walk[OID]` i `get[OID]` są wykonywane asynchronicznie — nie jest wymagane otrzymanie odpowiedzi na jedno żądanie przed rozpoczęciem innych kontroli. Rozwiązywanie DNS również odbywa się asynchronicznie. Maksymalna współbieżność kontroli asynchronicznych wynosi 1000 (określona przez MaxConcurrentChecksPerPoller). Liczba asynchronicznych odpytywaczy SNMP jest określana przez parametr StartSNMPPollers. Zwróć uwagę, że dla statystyk ruchu sieciowego zwracanych przez dowolną z metod należy dodać krok *Zmiana na sekundę* na karcie *Przetwarzanie wstępne*; w przeciwnym razie otrzymasz wartość skumulowaną z urządzenia SNMP zamiast ostatniej zmiany.

Wszystkie obowiązkowe pola wejściowe są oznaczone czerwoną gwiazdką.

Teraz zapisz pozycję i przejdź do *Monitorowanie* > *Najnowsze dane*, aby zobaczyć dane SNMP.

Przykład 1

Ogólny przykład:

Parametr	Opis
OID	1.2.3.45.6.7.8.0 (lub .1.2.3.45.6.7.8.0)
Key	<Unikalny ciąg znaków używany jako odniesienie do wyzwalaczy> Na przykład „my_param”.

Zwróć uwagę, że OID może być podany zarówno w postaci numerycznej, jak i tekstowej. Jednak w niektórych przypadkach tekstowy OID musi zostać przekonwertowany do postaci numerycznej. W tym celu można użyć narzędzia snmpget:

```
snmpget -On localhost public enterprises.ucdavis.memory.memTotalSwap.0
```

Przykład 2

Monitorowanie czasu działania:

Parametr	Opis
OID	MIB::sysUpTime.0
Key	router.uptime
Typ wartości	Float
Jednostki	uptime
Krok przetwarzania wstępnego: Mnożnik niestandardowy	0.01

Natywne żądania zbiorcze SNMP

Pozycja **walk[OID1,OID2,...]** umożliwia użycie natywnej funkcjonalności SNMP do żądań zbiorczych (GetBulkRequest-PDUs), dostępnej w wersjach SNMP 2/3.

Żądanie GetBulk w SNMP wykonuje wiele żądań GetNext i zwraca wynik w jednej odpowiedzi. Może to być używane zarówno dla zwykłych pozycji SNMP, jak i dla wykrywania SNMP, aby zminimalizować liczbę wymian z siecią.

Pozycja SNMP **walk[OID1,OID2,...]** może być używana jako pozycja nadrzędna, która zbiera dane w jednym żądaniu, wraz z pozycjami zależnymi, które analizują odpowiedź w razie potrzeby przy użyciu preprocessing.

Należy pamiętać, że użycie natywnych żądań zbiorczych SNMP nie jest związane z opcją łączenia żądań SNMP, która jest własnym sposobem Zabbix na łączenie wielu żądań SNMP (zobacz następną sekcję).

Dla zbiorczych pozycji SNMP zostanie wykonanych maksymalnie pięć ponowień, aby uniknąć niepowodzenia, jeśli jeden z pakietów zostanie utracony. Limit czasu dla pozycji SNMP z `get` i `walk` (ustawiany w formularzu konfiguracji pozycji) jest ustawiany dla całej sesji. Limit czasu jest stosowany niezależnie od tego, czy dane zostały pobrane w całości; jeśli dane zostaną odebrane częściowo (na przykład dane zostaną pomyślnie zebrane tylko dla jednego z wielu OID), pozycja stanie się nieobsługiwana z komunikatem „Only partial data received”. Jeśli limit czasu zostanie osiągnięty, nastąpi ponowienie, limit czasu zostanie zresetowany, a ostatnie żądanie zostanie wysłane ponownie, co pozwoli kontynuować sesję od ostatniego żądania, jeśli pojedynczy pakiet został utracony lub dotarł zbyt późno. Rozważ ustawienie niskiej wartości limitu czasu, aby uniknąć długich opóźnień, jeśli urządzenie jest nieosiągalne, ponieważ zostanie wykonanych do 5 ponowień, jeśli wcześniejsze przekroczą limit czasu lub zakończą się niepowodzeniem (np. 3-sekundowy limit czasu może skutkować 15-sekundowym czasem oczekiwania).

Wewnętrzne działanie przetwarzania łączonego

serwer Zabbix i proxy mogą odpytywać urządzenia SNMP o wiele wartości w jednym żądaniu. Wpływa to na kilka typów pozycji SNMP:

- zwykłe pozycje SNMP
- pozycje SNMP z dynamicznymi indeksami
- reguły niskopoziomowego wykrywania SNMP

Wszystkie pozycje SNMP na pojedynczym interfejsie o identycznych parametrach są planowane do odpytywania w tym samym czasie. Pierwsze dwa typy pozycji są pobierane przez pollery partiami po maksymalnie 128 pozycji, natomiast reguły niskopoziomowego wykrywania są przetwarzane pojedynczo, tak jak wcześniej.

Na niższym poziomie wykonywane są dwa rodzaje operacji służących do odpytywania wartości: pobieranie wielu określonych obiektów oraz przechodzenie drzewa OID.

Do „pobierania” używane jest GetRequest-PDU z maksymalnie 128 powiązaniami zmiennych. Do „przechodzenia” używane jest GetNextRequest-PDU dla SNMPv1, a dla SNMPv2 i SNMPv3 używane jest GetBulkRequest z polem „max-repetitions” o wartości maksymalnie 128.

W związku z tym korzyści z przetwarzania łączonego dla każdego typu pozycji SNMP przedstawiają się następująco:

- zwykłe pozycje SNMP korzystają z usprawnień „pobierania”;
- pozycje SNMP z dynamicznymi indeksami korzystają zarówno z usprawnień „pobierania”, jak i „przechodzenia”: „pobieranie” jest używane do weryfikacji indeksów, a „przechodzenie” do budowania pamięci podręcznej;
- reguły niskopoziomowego wykrywania SNMP korzystają z usprawnień „przechodzenia”.

Istnieje jednak problem techniczny polegający na tym, że nie wszystkie urządzenia są w stanie zwrócić 128 wartości na żądanie. Niektóre zawsze zwracają prawidłową odpowiedź, ale inne albo odpowiadają błędem „tooBig(1)”, albo nie odpowiadają wcale, gdy potencjalna odpowiedź przekracza pewien limit.

Aby znaleźć optymalną liczbę obiektów do odpytywania dla danego urządzenia, Zabbix stosuje następującą strategię. Zaczyna ostrożnie od odpytywania 1 wartości w żądaniu. Jeśli to się powiedzie, odpytywane są 2 wartości w żądaniu. Jeśli to ponownie się powiedzie, odpytywane są 3 wartości w żądaniu, a następnie proces jest kontynuowany w podobny sposób przez mnożenie liczby odpytywanych obiektów przez 1,5, co daje następującą sekwencję rozmiarów żądań: 1, 2, 3, 4, 6, 9, 13, 19, 28, 42, 63, 94, 128.

Jednak gdy urządzenie odmówi zwrócenia prawidłowej odpowiedzi (na przykład dla 42 zmiennych), Zabbix robi dwie rzeczy.

Po pierwsze, dla bieżącej partii pozycji zmniejsza o połowę liczbę obiektów w pojedynczym żądaniu i odpytuje 21 zmiennych. Jeśli urządzenie działa, to zapytanie powinno zadziałać w zdecydowanej większości przypadków, ponieważ wiadomo, że 28 zmiennych działało, a 21 to znacznie mniej. Jeśli jednak to również się nie powiedzie, Zabbix wraca do odpytywania wartości pojedynczo. Jeśli nadal się nie powiedzie, oznacza to, że urządzenie zdecydowanie nie odpowiada i rozmiar żądania nie jest problemem.

Drugą rzeczą, jaką Zabbix robi dla kolejnych partii pozycji, jest rozpoczęcie od ostatniej pomyślnej liczby zmiennych (28 w naszym przykładzie) i dalsze zwiększanie rozmiaru żądań o 1 aż do osiągnięcia limitu. Na przykład, zakładając, że największy rozmiar odpowiedzi to 32 zmienne, kolejne żądania będą miały rozmiary 29, 30, 31, 32 i 33. Ostatnie żądanie zakończy się niepowodzeniem i Zabbix nigdy więcej nie wyśle żądania o rozmiarze 33. Od tego momentu Zabbix będzie odpytywać to urządzenie o maksymalnie 32 zmienne.

Jeśli duże zapytania zawodzą przy tej liczbie zmiennych, może to oznaczać jedną z dwóch rzeczy. Nie da się dokładnie określić kryteriów, których urządzenie używa do ograniczania rozmiaru odpowiedzi, ale staramy się to przybliżyć za pomocą liczby zmiennych. Pierwsza możliwość jest taka, że ta liczba zmiennych znajduje się blisko rzeczywistego limitu rozmiaru odpowiedzi urządzenia w ogólnym przypadku: czasami odpowiedź jest mniejsza od limitu, a czasami go przekracza. Druga możliwość jest taka, że pakiet UDP w jednym z kierunków po prostu został utracony. Z tych powodów, jeśli Zabbix otrzyma nieudane zapytanie, zmniejsza maksymalną liczbę zmiennych, aby spróbować wejść głębiej w bezpieczny zakres pracy urządzenia, ale robi to najwyżej dwa razy.

W powyższym przykładzie, jeśli zapytanie z 32 zmiennymi akurat się nie powiedzie, Zabbix zmniejszy tę liczbę do 31. Jeśli to również się nie powiedzie, Zabbix zmniejszy tę liczbę do 30. Jednak Zabbix nie zmniejszy tej liczby poniżej 30, ponieważ założy, że dalsze niepowodzenia wynikają z utraty pakietów UDP, a nie z limitu urządzenia.

Jeśli jednak urządzenie nie potrafi poprawnie obsługiwać żądań łączonych z innych powodów i opisana powyżej heurystyka nie działa, dla każdego interfejsu dostępne jest ustawienie „Use combined requests”, które pozwala wyłączyć żądania łączone dla tego urządzenia.

Jeśli żądania łączone powodują częściowe lub nieprawidłowo sformowane odpowiedzi, które skutkują błędnymi obliczeniami wartości na sekundę (delta) (na przykład pozornymi skokami liczników interfejsu), wyłącz opcję *Use combined requests* dla danego interfejsu, aby wymusić osobne zapytania dla każdej pozycji; często zapobiega to fałszywym skokom. Alternatywnie rozważ użycie asynchronicznych pozycji `get[]` lub `walk[]`, które są wykonywane asynchronicznie i nie podlegają grupowaniu według interfejsu przez opcję *Use combined requests* — mogą być używane zamiast starszych synchronicznych kontroli OID, aby uniknąć problemów związanych z żądaniami łączonymi. Szukaj wpisów w logach serwera/proxy podobnych do pokazanego w sekcji Przegląd, aby pomóc w identyfikacji urządzeń, których dotyczy problem.

Dodatkowo, jeśli interfejs często staje się niedostępny, może być konieczne zwiększenie parametru `UnavailableDelay` w plikach konfiguracyjnych serwera Zabbix lub proxy Zabbix, aby zmniejszyć częstotliwość żądań. Pozycje mogą stać się nieobsługiwane, jeśli podczas wykrywania lub przejść OID zostaną odebrane częściowe dane.

1 Indeksy dynamiczne

Przegląd

Chociaż możesz znaleźć wymagany numer indeksu (na przykład interfejsu sieciowego) wśród OID SNMP, czasami nie można całkowicie polegać na tym, że numer indeksu zawsze pozostanie taki sam.

Numery indeksów mogą być dynamiczne — mogą zmieniać się w czasie, a w konsekwencji twoja pozycja może przestać działać.

Aby uniknąć takiej sytuacji, można zdefiniować OID, który uwzględnia możliwość zmiany numeru indeksu.

Na przykład, jeśli chcesz pobrać wartość indeksu do dołączenia do **ifInOctets**, która odpowiada interfejsowi **GigabitEthernet0/1** na urządzeniu Cisco, użyj następującego OID:

```
ifInOctets["index","ifDescr","GigabitEthernet0/1"]
```

Składnia

Używana jest specjalna składnia dla OID:

<OID danych>["index","<bazowy OID indeksu>","<szukany ciąg znaków>"]

Parametr	Opis
OID danych	Główny OID używany do pobierania danych dla pozycji.
index	Metoda przetwarzania. Obecnie obsługiwana jest jedna metoda: **index** – wyszukuje indeks i dołącza go do OID danych
bazowy OID indeksu	Ten OID zostanie odczytany w celu uzyskania wartości indeksu odpowiadającej ciągowi znaków.
szukany ciąg znaków	Ciąg znaków używany do dokładnego dopasowania wartości podczas wyszukiwania. Wielkość liter ma znaczenie.

Przykład

Pobieranie użycia pamięci procesu *apache*.

Jeśli używana jest ta składnia OID:

```
HOST-RESOURCES-MIB::hrSWRunPerfMem["index","HOST-RESOURCES-MIB::hrSWRunPath", "/usr/sbin/apache2"]
```

numer indeksu zostanie wyszukany tutaj:

```
...
HOST-RESOURCES-MIB::hrSWRunPath.5376 = STRING: "/sbin/getty"
HOST-RESOURCES-MIB::hrSWRunPath.5377 = STRING: "/sbin/getty"
HOST-RESOURCES-MIB::hrSWRunPath.5388 = STRING: "/usr/sbin/apache2"
HOST-RESOURCES-MIB::hrSWRunPath.5389 = STRING: "/sbin/sshd"
...
```

Teraz mamy indeks 5388. Indeks zostanie dołączony do OID danych, aby otrzymać interesującą nas wartość:

```
HOST-RESOURCES-MIB::hrSWRunPerfMem.5388 = INTEGER: 31468 KBytes
```

Buforowanie wyszukiwania indeksów

Gdy żądana jest dynamiczna pozycja indeksu, Zabbix pobiera i buforuje całą tabelę SNMP pod bazowym OID dla indeksu, nawet jeśli dopasowanie zostałoby znalezione wcześniej. Jest to wykonywane na wypadek, gdyby inna pozycja odwoływała się później do tego samego bazowego OID — Zabbix wyszuka wtedy indeks w pamięci podręcznej, zamiast ponownie odpyt ywać monitorowany host. Należy pamiętać, że każdy proces pollera używa oddzielnej pamięci podręcznej.

We wszystkich kolejnych operacjach pobierania wartości weryfikowany jest tylko znaleziony indeks. Jeśli nie uległ zmianie, pobierana jest wartość. Jeśli uległ zmianie, pamięć podręczna jest przebudowywana — każdy poller, który napotka zmieniony indeks, ponownie przechodzi przez tabelę SNMP indeksu.

2 Specjalne OID

Niektóre z najczęściej używanych OID SNMP są automatycznie tłumaczone przez Zabbix na reprezentację numeryczną. Na przykład **ifIndex** jest tłumaczone na **1.3.6.1.2.1.2.2.1.1**, a **ifIndex.0** jest tłumaczone na **1.3.6.1.2.1.2.2.1.1.0**.

Tabela zawiera listę specjalnych OID.

Specjalny OID	Identyfikator	Opis
ifIndex	1.3.6.1.2.1.2.2.1.1	Unikalna wartość dla każdego interfejsu.
ifDescr	1.3.6.1.2.1.2.2.1.2	Ciąg tekstowy zawierający informacje o interfejsie. Ten ciąg powinien zawierać nazwę producenta, nazwę produktu oraz wersję interfejsu sprzętowego.
ifType	1.3.6.1.2.1.2.2.1.3	Typ interfejsu, rozróżniany zgodnie z protokołem(ami) fizycznym(i)/łącza bezpośrednio „poniżej" warstwy sieciowej w stosie protokołów.
ifMtu	1.3.6.1.2.1.2.2.1.4	Rozmiar największego datagramu, który może zostać wysłany/odebrany przez interfejs, określony w oktetach.
ifSpeed	1.3.6.1.2.1.2.2.1.5	Szacunkowa bieżąca przepustowość interfejsu w bitach na sekundę.
ifPhysAddress	1.3.6.1.2.1.2.2.1.6	Adres interfejsu na warstwie protokołu bezpośrednio 'poniżej' warstwy sieciowej w stosie protokołów.

Specjalny OID	Identyfikator	Opis
ifAdminStatus	1.3.6.1.2.1.2.2.1.7	Bieżący administracyjny stan interfejsu.
ifOperStatus	1.3.6.1.2.1.2.2.1.8	Bieżący operacyjny stan interfejsu.
ifInOctets	1.3.6.1.2.1.2.2.1.10	Łączna liczba oktetów odebranych przez interfejs, w tym znaków ramkowania.
ifInUcastPkts	1.3.6.1.2.1.2.2.1.11	Liczba pakietów unicast podsieci dostarczonych do protokołu wyższej warstwy.
ifInNUcastPkts	1.3.6.1.2.1.2.2.1.12	Liczba pakietów nie-unicast (tj. rozgłoszeniowych podsieci lub multicastowych podsieci) dostarczonych do protokołu wyższej warstwy.
ifInDiscards	1.3.6.1.2.1.2.2.1.13	Liczba pakietów przychodzących, które zostały wybrane do odrzucenia, mimo że nie wykryto błędów, które uniemożliwiałyby ich dostarczenie do protokołu wyższej warstwy. Jednym z możliwych powodów odrzucenia takiego pakietu może być zwolnienie miejsca w buforze.
ifInErrors	1.3.6.1.2.1.2.2.1.14	Liczba pakietów przychodzących zawierających błędy uniemożliwiające ich dostarczenie do protokołu wyższej warstwy.
ifInUnknownProtos	1.3.6.1.2.1.2.2.1.15	Liczba pakietów odebranych przez interfejs, które zostały odrzucone z powodu nieznanego lub nieobsługiwanego protokołu.
ifOutOctets	1.3.6.1.2.1.2.2.1.16	Łączna liczba oktetów wysłanych z interfejsu, w tym znaków ramkowania.
ifOutUcastPkts	1.3.6.1.2.1.2.2.1.17	Łączna liczba pakietów, których wysłania zażądały protokoły wyższej warstwy i które nie były adresowane do adresu multicast lub broadcast na tej podwarstwie, w tym tych, które zostały odrzucone lub niewysłane.
ifOutNUcastPkts	1.3.6.1.2.1.2.2.1.18	Łączna liczba pakietów, których wysłania zażądały protokoły wyższej warstwy i które były adresowane do adresu multicast lub broadcast na tej podwarstwie, w tym tych, które zostały odrzucone lub niewysłane.
ifOutDiscards	1.3.6.1.2.1.2.2.1.19	Liczba pakietów wychodzących, które zostały wybrane do odrzucenia, mimo że nie wykryto błędów, które uniemożliwiałyby ich transmisję. Jednym z możliwych powodów odrzucenia takiego pakietu może być zwolnienie miejsca w buforze.
ifOutErrors	1.3.6.1.2.1.2.2.1.20	Liczba pakietów wychodzących, które nie mogły zostać przesłane z powodu błędów.
ifOutQLen	1.3.6.1.2.1.2.2.1.21	Długość kolejki pakietów wyjściowych (w pakietach).

3 pliki MIB

Wprowadzenie

MIB oznacza bazę informacji zarządzania (Management Information Base). Pliki MIB umożliwiają używanie tekstowej reprezentacji OID (Object Identifier). Podczas monitorowania urządzeń SNMP za pomocą Zabbix można używać surowych OID, ale jeśli wygodniej jest używać reprezentacji tekstowej, należy zainstalować pliki MIB.

Na przykład

`ifHCOutOctets`

jest tekstową reprezentacją OID

`1.3.6.1.2.1.31.1.1.1.10`

Instalacja plików MIB

W systemach opartych na Debianie:

```
apt install snmp-mibs-downloader
download-mibs
```

W systemach opartych na RedHat:

```
dnf install net-snmp-libs
```

Włączanie plików MIB

W systemach opartych na RedHat pliki MIB powinny być domyślnie włączone. W systemach opartych na Debian należy edytować plik `/etc/snmp/snmp.conf` i zakomentować linię `mibs :`

```
# Ponieważ pakiety snmp są dostarczane bez plików MIB z powodów licencyjnych, ładowanie
# plików MIB jest domyślnie wyłączone. Jeśli dodano pliki MIB, można ponownie włączyć
# ich ładowanie, zakomentowując poniższą linię.
mibs :
```

Testowanie plików MIB

Testowanie SNMP MIB można wykonać za pomocą narzędzia `snmpwalk`. Jeśli nie jest ono zainstalowane, skorzystaj z poniższych instrukcji.

W systemach opartych na Debianie:

```
apt install snmp
```

W systemach opartych na RedHat:

```
dnf install net-snmp-utils
```

Następnie poniższe polecenie nie powinno zwracać błędu podczas odpytywania urządzenia sieciowego:

```
$ snmpwalk -v 2c -c public <NETWORK DEVICE IP> ifInOctets
IF-MIB::ifInOctets.1 = Counter32: 176137634
IF-MIB::ifInOctets.2 = Counter32: 0
IF-MIB::ifInOctets.3 = Counter32: 240375057
IF-MIB::ifInOctets.4 = Counter32: 220893420
[...]
```

Używanie MIB-ów w Zabbixie

Najważniejsze, o czym należy pamiętać, to fakt, że procesy Zabbix nie są informowane o zmianach wprowadzonych w plikach MIB. Dlatego po każdej zmianie należy ponownie uruchomić serwer lub proxy Zabbix, na przykład:

```
systemctl restart zabbix-server
```

Po tym zmiany wprowadzone w plikach MIB zaczną obowiązywać.

Używanie niestandardowych plików MIB

Istnieją standardowe pliki MIB dostarczane z każdą dystrybucją GNU/Linux. Jednak niektórzy producenci urządzeń udostępniają własne.

Załóżmy, że chcesz użyć pliku MIB CISCO-SMI. Poniższe instrukcje pobiorą go i zainstalują:

```
wget ftp://ftp.cisco.com/pub/mibs/v2/CISCO-SMI.my -P /tmp
mkdir -p /usr/local/share/snmp/mibs
grep -q '^mibdirs +/usr/local/share/snmp/mibs' /etc/snmp/snmp.conf 2>/dev/null || echo "mibdirs +/usr/loca
cp /tmp/CISCO-SMI.my /usr/local/share/snmp/mibs
```

Teraz powinno być możliwe jego użycie. Spróbuj przetłumaczyć nazwę obiektu *ciscoProducts* z pliku MIB na OID:

```
snmptranslate -IR -On CISCO-SMI::ciscoProducts
.1.3.6.1.4.1.9.1
```

Jeśli zamiast OID otrzymasz błędy, upewnij się, że wszystkie poprzednie polecenia zostały wykonane bez błędów.

Tłumaczenie nazwy obiektu zadziałało, więc możesz już używać niestandardowego pliku MIB. Zwróć uwagę na prefiks nazwy MIB (*CISCO-SMI::*) użyty w zapytaniu. Będzie on potrzebny zarówno podczas korzystania z narzędzi wiersza poleceń, jak i Zabbix.

Nie zapomnij zrestartować serwera/proxy Zabbix przed użyciem tego pliku MIB w Zabbix.

Attention:
Pamiętaj, że pliki MIB mogą mieć zależności. Oznacza to, że jeden MIB może wymagać innego. Aby spełnić te zależności, musisz zainstalować wszystkie powiązane pliki MIB.

3 Pułapki SNMP

Przegląd

Odbieranie pułapek SNMP jest przeciwieństwem odpytywania urządzeń z włączonym SNMP.

W tym przypadku informacje są wysyłane z urządzenia z włączonym SNMP do snmptrapd i są zbierane lub „przechwytywane” przez serwer Zabbix lub proxy Zabbix z pliku.

Zwykle pułapki są wysyłane po wystąpieniu zmiany jakiegoś warunku, a agent łączy się z serwerem na porcie 162 (w przeciwieństwie do portu 161 po stronie agenta, który jest używany do zapytań). Korzystanie z pułapek może umożliwić wykrycie krótkotrwałych problemów występujących pomiędzy kolejnymi odpytywaniami, które mogłyby zostać pominięte przez dane z zapytań.

Odbieranie pułapek SNMP w Zabbix zostało zaprojektowane do współpracy z **snmptrapd** oraz z jednym z mechanizmów przekazywania pułapek do Zabbix — skryptem Bash lub Perl albo SNMPTT.

Note:
Najprostszym sposobem skonfigurowania monitorowania pułapek po skonfigurowaniu Zabbix jest użycie rozwiązania opartego na skrypcie Bash, ponieważ Perl i SNMPTT często nie są dostępne we współczesnych dystrybucjach i wymagają bardziej złożonej konfiguracji. Jednak to rozwiązanie wykorzystuje skrypt skonfigurowany jako `traphandle`. Aby uzyskać lepszą wydajność w systemach produkcyjnych, użyj rozwiązania z osadzonym Perlem (skrypt z opcją do `perl` lub SNMPTT).

Przebieg odbierania pułapki:

1. `snmptrapd` odbiera pułapkę
2. `snmptrapd` przekazuje pułapkę do skryptu odbierającego (Bash, Perl) lub do SNMPTT
3. Odbiornik analizuje, formatuje i zapisuje pułapkę do pliku
4. Moduł SNMP trapper Zabbix odczytuje i analizuje plik pułapek
5. Dla każdej pułapki Zabbix znajduje wszystkie pozycje „SNMP trapper" z interfejsami hosta pasującymi do adresu odebranej pułapki. Należy pamiętać, że podczas dopasowywania używane jest tylko wybrane „IP" lub „DNS" w interfejsie hosta.
6. Dla każdej znalezionej pozycji pułapka jest porównywana z wyrażeniem regularnym w `snmptrap[regexp]`. Pułapka jest ustawiana jako wartość **wszystkich** dopasowanych pozycji. Jeśli nie zostanie znaleziona żadna pasująca pozycja, a istnieje pozycja `snmptrap.fallback`, pułapka jest ustawiana jako jej wartość.
7. Jeśli pułapka nie została ustawiona jako wartość żadnej pozycji, Zabbix domyślnie zapisuje niedopasowaną pułapkę w logu. (Jest to konfigurowane przez opcję „Log unmatched SNMP traps" w Administration > General > Other.)

Uwagi dotyczące przełączenia awaryjnego HA

Podczas przełączania węzła wysokiej dostępności (HA) Zabbix będzie kontynuował przetwarzanie od ostatniego rekordu w ramach ostatniego znacznika czasu ISO 8601; jeśli ten sam rekord nie zostanie znaleziony, do określenia ostatniej pozycji zostanie użyty tylko znacznik czasu.

Konfigurowanie pułapek SNMP

Ten typ pozycji wymaga następującej konfiguracji frontend.

1. Utwórz interfejs SNMP dla swojego hosta

- W *Data collection* > *Hosts* utwórz/edytuj host, a w polu *Interfaces* dodaj interfejs typu „SNMP", podając adres IP lub DNS.

Adres z każdej odebranej pułapki będzie porównywany z adresami IP i DNS wszystkich interfejsów SNMP w celu znalezienia odpowiadających hostów.

2. Skonfiguruj pozycję

- W *Data collection* > *Hosts* utwórz/edytuj wymaganą pozycję.
- W polu *Key* użyj jednego z kluczy pułapek SNMP:

Key		
Description	Return value	Comments
snmptrap[regexp] Przechwytuje wszystkie pułapki SNMP pasujące do wyrażenia regularnego określonego w **regexp**. Jeśli regexp nie jest określone, przechwytuje dowolną pułapkę. **snmptrap.fallback**	Pułapka SNMP	Tę pozycję można ustawić tylko dla interfejsów SNMP. Makra użytkownika i globalne wyrażenia regularne są obsługiwane w parametrze tego klucza pozycji.

Key		
Przechwytuje wszystkie pułapki SNMP, które nie zostały przechwycone przez żaden z elementów snmptrap[] dla tego interfejsu.	Pułapka SNMP	Tę pozycję można ustawić tylko dla interfejsów SNMP.

Note:
Dopasowywanie wielowierszowych wyrażeń regularnych nie jest obecnie obsługiwane.

- Ustaw *Type of information* na „Log”, aby znaczniki czasu były analizowane. Inne formaty, takie jak „Numeric”, są również akceptowalne, ale mogą wymagać niestandardowej obsługi pułapek.

Konfigurowanie monitorowania pułapek SNMP

Konfigurowanie serwera/proxy Zabbix

Aby odczytywać pułapki, serwer lub proxy Zabbix musi być skonfigurowany tak, aby uruchamiał proces SNMP trapper i wskazywał plik pułapek, do którego zapisuje SNMPTT lub odbiornik pułapek Bash/Perl. W tym celu edytuj plik konfiguracyjny (zabbix_server.conf lub zabbix_proxy.conf):

```
StartSNMPTrapper=1
SNMPTrapperFile=[TRAP FILE]
```

Warning:
Jeśli używany jest parametr systemd **PrivateTmp** , ten plik najprawdopodobniej nie będzie działał w */tmp*.

Konfigurowanie odbiornika pułapek Bash

Wymagania: tylko snmptrapd.

Skrypt odbiornika pułapek Bash script może być używany do przekazywania pułapek do serwera Zabbix z snmptrapd przy użyciu pliku trapper. Aby go skonfigurować, dodaj opcję `traphandle` do pliku konfiguracyjnego snmptrapd (`snmptrapd.conf`), zobacz przykład.

Note:
Aby zastosować zmiany w konfiguracji snmptrapd, może być konieczne jego ponowne uruchomienie.

Konfigurowanie odbiornika trapów Perl

Wymagania: Perl, Net-SNMP skompilowany z opcją --enable-embedded-perl (domyślnie od Net-SNMP 5.4)

Odbiornik trapów Perl (plik znajduje się w misc/snmptrap/zabbix_trap_receiver.pl) może być używany do przekazywania trapów bezpośrednio do serwera Zabbix z snmptrapd. Aby go skonfigurować:

- dodaj skrypt Perl do pliku konfiguracyjnego snmptrapd (snmptrapd.conf), na przykład:

```
perl do "[FULL PATH TO PERL RECEIVER SCRIPT]";
```

- skonfiguruj odbiornik, na przykład:

```
$SNMPTrapperFile = '[TRAP FILE]';
$DateTimeFormat = '[DATE TIME FORMAT]';
```

Note:
Aby zastosować zmiany w konfiguracji, może być konieczne ponowne uruchomienie snmptrapd.

Note:
Jeśli nazwa skryptu nie jest ujęta w cudzysłów, snmptrapd odmówi uruchomienia i wyświetli komunikaty podobne do poniższych:


```
Regexp modifiers "/l" and "/a" are mutually exclusive at (eval 2) line 1, at end of line
Regexp modifier "/l" may not appear twice at (eval 2) line 1, at end of line
```

Konfigurowanie SNMPTT

Na początku należy skonfigurować snmptrapd tak, aby używał SNMPTT.

> **Note:**
> Aby uzyskać najlepszą wydajność, SNMPTT należy skonfigurować jako daemon z użyciem **snmptthandler-embedded** do przekazywania do niego trapów. Zobacz instrukcje dotyczące konfigurowania SNMPTT.

Gdy SNMPTT jest skonfigurowany do odbierania trapów, skonfiguruj `snmptt.ini`:

1. włącz użycie modułu Perl z pakietu NET-SNMP:

```
net_snmp_perl_enable = 1
```

2. zapisuj trapy do pliku trapów, który będzie odczytywany przez Zabbix:

```
log_enable = 1
log_file = [TRAP FILE]
```

3. ustaw format daty i czasu:

```
date_time_format = %Y-%m-%dT%H:%M:%S%z
```

> **Warning:**
> Pakiet "net-snmp-perl" został usunięty w RHEL 8.0-8.2; ponownie dodany w RHEL 8.3. Więcej informacji można znaleźć w sekcji known issues.

Teraz sformatuj trapy tak, aby Zabbix mógł je rozpoznawać (edytuj snmptt.conf):

1. Każda instrukcja FORMAT powinna zaczynać się od "ZBXTRAP [address]", gdzie [address] będzie porównywany z adresami IP i DNS interfejsów SNMP w Zabbix. Na przykład:

```
EVENT coldStart .1.3.6.1.6.3.1.1.5.1 "Status Events" Normal
FORMAT ZBXTRAP $aA Device reinitialized (coldStart)
```

2. Więcej informacji o formacie trapów SNMP znajduje się poniżej.

> **Attention:**
> Nie używaj nieznanych trapów — Zabbix nie będzie w stanie ich rozpoznać. Nieznane trapy można obsłużyć, definiując ogólne zdarzenie w snmptt.conf:

> `EVENT general .* "General event" Normal`

Format pułapki SNMP

Wszystkie niestandardowe odbiorniki pułapek Perl oraz konfiguracja pułapek SNMPTT muszą formatować pułapkę w następujący sposób:

```
[timestamp] [the trap, part 1] ZBXTRAP [address] [the trap, part 2]
```

gdzie

- [timestamp] - znacznik czasu w formacie "%Y-%m-%dT%H:%M:%S%z"
- ZBXTRAP - nagłówek wskazujący, że w tym wierszu rozpoczyna się nowa pułapka
- [address] - adres IP używany do znalezienia hosta dla tej pułapki

Należy pamiętać, że "ZBXTRAP" oraz "[address]" zostaną usunięte z wiadomości podczas przetwarzania. Jeśli pułapka będzie sformatowana inaczej, Zabbix może parsować pułapki w nieoczekiwany sposób.

Przykładowa pułapka:

```
2024-01-11T15:28:47+0200 .1.3.6.1.6.3.1.1.5.3 Normal "Status Events" localhost - ZBXTRAP 192.168.1.1 Link
```

Spowoduje to utworzenie następującej pułapki dla interfejsu SNMP z IP=192.168.1.1:

```
2024-01-11T15:28:47+0200 .1.3.6.1.6.3.1.1.5.3 Normal "Status Events"
localhost - Link down on interface 2. Admin state: 1. Operational state: 2
```

Wymagania systemowe

Note:
Zaleca się zainstalowanie plików MIB, aby zapewnić, że wartości pozycji będą wyświetlane w prawidłowym formacie. Bez plików MIB mogą wystąpić problemy z formatowaniem, takie jak wyświetlanie wartości w formacie HEX zamiast UTF-8 lub odwrotnie.

Obsługa dużych plików

Zabbix obsługuje duże pliki dla plików SNMP trapper. Maksymalny rozmiar pliku, jaki Zabbix może odczytać, wynosi 2^63 (8 EiB). Należy pamiętać, że system plików może narzucać niższy limit rozmiaru pliku.

Rotacja logów

Zabbix nie zapewnia żadnego systemu rotacji logów — powinno to być obsługiwane przez użytkownika. Rotacja logów powinna najpierw zmienić nazwę starego pliku, a dopiero później go usunąć, aby żadne trapy nie zostały utracone:

1. Zabbix otwiera plik trapów w ostatniej znanej lokalizacji i przechodzi do kroku 3.
2. Zabbix sprawdza, czy aktualnie otwarty plik został poddany rotacji, porównując numer inode z numerem inode zdefiniowanego pliku trapów. Jeśli żaden plik nie jest otwarty, Zabbix resetuje ostatnią lokalizację i przechodzi do kroku 1.
3. Zabbix odczytuje dane z aktualnie otwartego pliku i ustawia nową lokalizację.
4. Nowe dane są analizowane. Jeśli był to plik po rotacji, plik zostaje zamknięty i następuje powrót do kroku 2.
5. Jeśli nie było nowych danych, Zabbix usypia się na 1 sekundę i wraca do kroku 2.

System plików

Ze względu na implementację pliku pułapki, Zabbix wymaga, aby system plików obsługiwał i-węzły w celu rozróżniania plików (informacje są pobierane za pomocą wywołania stat()).

Przykłady konfiguracji z użyciem różnych wersji protokołu SNMP

Ten przykład wykorzystuje `snmptrapd` oraz skrypt odbiornika Bash do przekazywania trapów do serwera Zabbix.

Konfiguracja:

1. Skonfiguruj Zabbix tak, aby uruchamiał SNMP trapper i ustaw plik trapów. Dodaj do `zabbix_server.conf`:

```
StartSNMPTrapper=1
SNMPTrapperFile=/var/lib/zabbix/snmptraps/snmptraps.log
```

2. Pobierz skrypt Bash do `/usr/sbin/zabbix_trap_handler.sh`:

```
curl -o /usr/sbin/zabbix_trap_handler.sh https://raw.githubusercontent.com/zabbix/zabbix-docker/trunk/Dock
```

W razie potrzeby dostosuj zmienną `ZABBIX_TRAPS_FILE` w skrypcie. Aby użyć wartości domyślnej, najpierw utwórz katalog nadrzędny:

```
mkdir -p /var/lib/zabbix/snmptraps
```

3. Dodaj następujący wpis do `snmtrapd.conf` (zobacz działający przykład)

```
traphandle default /bin/bash /usr/sbin/zabbix_trap_handler.sh
```

Note:
Może być konieczne ponowne uruchomienie `snmptrapd`, aby wczytał zmiany w swojej konfiguracji.

4. Utwórz pozycję SNMP TEST (pamiętaj o początkowych wymaganiach konfiguracyjnych):

Typ: SNMP trap
Typ informacji: Log Interfejs hosta: SNMP 127.0.0.1
Klucz: `snmptrap["linkUp"]`
Format czasu logu: yyyyMMdd.hhmmss

Zwróć uwagę, że używany jest format daty i czasu ISO 8601.

5. Następnie skonfigurujemy `snmptrapd` dla wybranej wersji protokołu SNMP i wyślemy testowe trapy za pomocą narzędzia `snmptrap`.

SNMPv1, SNMPv2

Protokoły SNMPv1 i SNMPv2 opierają się na uwierzytelnianiu za pomocą „community string”. W poniższym przykładzie użyjemy „secret” jako community string. Musi ona być ustawiona na tę samą wartość u nadawców trapów SNMP.

Należy pamiętać, że mimo iż SNMPv2 jest nadal szeroko używany w środowiskach produkcyjnych, nie oferuje żadnego szyfrowania ani rzeczywistego uwierzytelniania nadawcy. Dane są przesyłane jawnym tekstem, dlatego te wersje protokołu powinny być używane wyłącznie w bezpiecznych środowiskach, takich jak sieć prywatna, i nigdy nie powinny być używane przez sieć publiczną ani sieć podmiotu trzeciego.

Wersja SNMP 1 nie jest obecnie praktycznie używana, ponieważ nie obsługuje liczników 64-bitowych i jest uznawana za przestarzały protokół.

Aby włączyć odbieranie trapów SNMPv1 lub SNMPv2, należy dodać następujący wiersz do `snmptrapd.conf`. Zastąp „secret" community string SNMP skonfigurowanym u nadawców trapów SNMP:

```
authCommunity log,execute,net secret
```

Następnie możemy wysłać testowy trap za pomocą `snmptrap`. W tym przykładzie użyjemy popularnego OID „link up":

```
snmptrap -v 2c -c secret localhost '' linkUp.0
```

SNMPv3

SNMPv3 rozwiązuje problemy bezpieczeństwa SNMPv1/v2 i zapewnia uwierzytelnianie oraz szyfrowanie. Można używać MD5 lub wielu metod uwierzytelniania SHA oraz DES/wielu wariantów AES jako szyfru.

Aby włączyć odbieranie SNMPv3, dodaj następujące wiersze do `snmptrapd.conf`:

```
createUser -e 0x8000000001020304 traptest SHA mypassword AES
authuser log,execute traptest
```

Attention:
Zwróć uwagę na słowo kluczowe „execute", które pozwala wykonywać skrypty dla tego modelu bezpieczeństwa użytkownika.

```
snmptrap -v 3 -n "" -a SHA -A mypassword -x AES -X mypassword -l authPriv -u traptest -e 0x800000000102030
```

Warning:
Jeśli chcesz używać silnych metod szyfrowania, takich jak AES192 lub AES256, użyj net-snmp od wersji 5.8. Może być konieczne ponowne skompilowanie go z opcją `configure: --enable-blumenthal-aes`. Starsze wersje net-snmp nie obsługują AES192/AES256. Zobacz także: Strong Authentication or Encryption.

Weryfikacja

W obu przykładach zobaczysz podobne wiersze w `/var/lib/zabbix/snmptraps/snmptraps.log`:

```
2024-01-30T10:04:23+0200 ZBXTRAP 127.0.0.1
UDP: [127.0.0.1]:56585->[127.0.0.1]:162
DISMAN-EVENT-MIB::sysUpTimeInstance = 2538834
SNMPv2-MIB::snmpTrapOID.0 = IF-MIB::linkUp.0
```

Wartość pozycji w Zabbix będzie następująca:

```
2024-01-30 10:04:23 2024-01-30 10:04:21

2024-01-30T10:04:21+0200 UDP: [127.0.0.1]:56585->[127.0.0.1]:162
DISMAN-EVENT-MIB::sysUpTimeInstance = 2538834
SNMPv2-MIB::snmpTrapOID.0 = IF-MIB::linkUp.0
```

Przykład z użyciem Perla:

```
2024-01-30T11:42:54+0200 ZBXTRAP 127.0.0.1
PDU INFO:
  receivedfrom                   UDP: [127.0.0.1]:58649->[127.0.0.1]:162
  notificationtype               TRAP
  version                        1
  community                      public
  errorstatus                    0
  transactionid                  1
  requestid                      2101882550
  messageid                      0
  errorindex                     0
VARBINDS:
```

```
DISMAN-EVENT-MIB::sysUpTimeInstance type=67 value=Timeticks: (457671) 1:16:16.71
SNMPv2-MIB::snmpTrapOID.0       type=6  value=OID: IF-MIB::linkUp.0
```

Zobacz także

- Artykuł na blogu Zabbix o pułapkach SNMP
- Konfigurowanie snmptrapd (oficjalna dokumentacja net-snmp)
- Konfigurowanie snmptrapd do odbierania powiadomień SNMPv3 (oficjalna dokumentacja net-snmp)

4 Kontrole IPMI

Przegląd

W Zabbix można monitorować stan i dostępność urządzeń Intelligent Platform Management Interface (IPMI). Aby wykonywać kontrole IPMI, serwer Zabbix musi być wcześniej skonfigurowany z obsługą IPMI.

IPMI to standaryzowany interfejs do zdalnego zarządzania systemami komputerowymi w trybie „lights-out" lub „out-of-band". Umożliwia monitorowanie stanu sprzętu bezpośrednio z tak zwanych kart zarządzania „out-of-band", niezależnie od systemu operacyjnego oraz od tego, czy maszyna jest w ogóle włączona.

Monitorowanie IPMI w Zabbix działa tylko dla urządzeń obsługujących IPMI (HP iLO, DELL DRAC, IBM RSA, Sun SSP itd.).

Proces menedżera IPMI planuje kontrole IPMI wykonywane przez pollery IPMI. host jest zawsze odpytywany tylko przez jeden poller IPMI naraz, co zmniejsza liczbę otwartych połączeń do kontrolerów BMC. Dzięki temu można bezpiecznie zwiększać liczbę pollerów IPMI bez obaw o przeciążenie kontrolerów BMC. Proces menedżera IPMI jest uruchamiany automatycznie, gdy uruchomiony zostanie co najmniej jeden poller IPMI.

Zobacz także znane problemy dotyczące kontroli IPMI.

Konfiguracja

Konfiguracja hosta

Aby przetwarzać kontrole IPMI, host musi być skonfigurowany. Należy dodać interfejs IPMI z odpowiednim adresem IP i numerem portu oraz zdefiniować parametry uwierzytelniania IPMI.

Więcej informacji można znaleźć w sekcji konfiguracja hostów.

Konfiguracja serwera

Domyślnie serwer Zabbix nie jest skonfigurowany do uruchamiania żadnych procesów odpytywania IPMI, dlatego wszelkie dodane pozycje IPMI nie będą działać. Aby to zmienić, otwórz jako root plik konfiguracyjny serwera Zabbix (zabbix_server.conf) i znajdź następujący wiersz:

```
# StartIPMIPollers=0
```

Odkomentuj go i ustaw liczbę procesów odpytywania na przykład na 3, tak aby wyglądał następująco:

```
StartIPMIPollers=3
```

Zapisz plik, a następnie uruchom ponownie zabbix_server.

Konfiguracja pozycji

Podczas konfigurowania pozycji na poziomie hosta:

- Wybierz „IPMI agent" jako *Typ*
- Wprowadź klucz pozycji, który jest unikalny w obrębie hosta (na przykład `ipmi.fan.rpm`)
- W polu *Interfejs hosta* wybierz odpowiedni interfejs IPMI (adres IP i port). Pamiętaj, że interfejs IPMI musi istnieć na hoście.
- Określ *Czujnik IPMI* (na przykład „FAN MOD 1A RPM" w Dell Poweredge), z którego ma być pobierana metryka. Domyślnie należy podać identyfikator czujnika. Możliwe jest również użycie prefiksów przed wartością:
  - `id:` — aby określić identyfikator czujnika;
  - `name:` — aby określić pełną nazwę czujnika. Może to być przydatne w sytuacjach, gdy czujniki można rozróżnić tylko przez podanie pełnej nazwy.
- Wybierz odpowiedni typ informacji („Numeryczny (zmiennoprzecinkowy)" w tym przypadku; dla czujników dyskretnych — „Numeryczny (bez znaku)"), jednostki (najprawdopodobniej „rpm") oraz wszelkie inne wymagane atrybuty pozycji

Obsługiwane testy

Agent IPMI obsługuje wbudowaną pozycję **ipmi.get**, która zwraca informacje związane z czujnikami IPMI i może być używana do wykrywania czujników IPMI.
Wartość zwracana: *obiekt JSON*

Timeout i zakończenie sesji

Timeouty komunikatów IPMI oraz liczba ponowień są zdefiniowane w bibliotece OpenIPMI. Ze względu na obecną konstrukcję OpenIPMI nie ma możliwości skonfigurowania tych wartości w Zabbix, ani na poziomie interfejsu, ani pozycja.

Timeout bezczynności sesji IPMI dla LAN wynosi 60 +/-3 sekundy. Obecnie nie jest możliwe zaimplementowanie okresowego wysyłania polecenia Activate Session przy użyciu OpenIPMI. Jeśli z Zabbix do określonego BMC nie są wykonywane żadne kontrole pozycja IPMI przez czas dłuższy niż timeout sesji skonfigurowany w BMC, to następna kontrola IPMI po upływie tego timeoutu zakończy się timeoutem z powodu timeoutów pojedynczych komunikatów, ponowień lub błędu odbioru. Następnie otwierana jest nowa sesja i inicjowane jest pełne ponowne skanowanie BMC. Może zostać otwarty nowy port UDP do zarządzania nową sesją. Bezczynność jest definiowana jako brak zarówno żądań wychodzących, jak i odpowiedzi przychodzących. Jeśli chcesz uniknąć niepotrzebnych ponownych skanowań BMC, zaleca się ustawienie interwału odpytywania pozycja IPMI poniżej timeoutu bezczynności sesji IPMI skonfigurowanego w BMC.

Uwagi dotyczące dyskretnych sensorów IPMI

Aby znaleźć sensory na hoście, uruchom serwer Zabbix z włączonym **DebugLevel=4**. Odczekaj kilka minut i znajdź rekordy wykrywania sensorów w pliku logu serwera Zabbix:

```
$ grep 'Added sensor' zabbix_server.log
8358:20130318:111122.170 Added sensor: host:'192.168.1.12:623' id_type:0 id_sz:7 id:'CATERR' reading_type:
8358:20130318:111122.170 Added sensor: host:'192.168.1.12:623' id_type:0 id_sz:15 id:'CPU Therm Trip' read
8358:20130318:111122.171 Added sensor: host:'192.168.1.12:623' id_type:0 id_sz:17 id:'System Event Log' re
8358:20130318:111122.171 Added sensor: host:'192.168.1.12:623' id_type:0 id_sz:17 id:'PhysicalSecurity' re
8358:20130318:111122.171 Added sensor: host:'192.168.1.12:623' id_type:0 id_sz:14 id:'IPMI Watchdog' readi
8358:20130318:111122.171 Added sensor: host:'192.168.1.12:623' id_type:0 id_sz:16 id:'Power Unit Stat' rea
8358:20130318:111122.171 Added sensor: host:'192.168.1.12:623' id_type:0 id_sz:16 id:'P1 Therm Ctrl %' rea
8358:20130318:111122.172 Added sensor: host:'192.168.1.12:623' id_type:0 id_sz:16 id:'P1 Therm Margin' rea
8358:20130318:111122.172 Added sensor: host:'192.168.1.12:623' id_type:0 id_sz:13 id:'System Fan 2' readin
8358:20130318:111122.172 Added sensor: host:'192.168.1.12:623' id_type:0 id_sz:13 id:'System Fan 3' readin
8358:20130318:111122.172 Added sensor: host:'192.168.1.12:623' id_type:0 id_sz:14 id:'P1 Mem Margin' readi
8358:20130318:111122.172 Added sensor: host:'192.168.1.12:623' id_type:0 id_sz:17 id:'Front Panel Temp' re
8358:20130318:111122.173 Added sensor: host:'192.168.1.12:623' id_type:0 id_sz:15 id:'Baseboard Temp' read
8358:20130318:111122.173 Added sensor: host:'192.168.1.12:623' id_type:0 id_sz:9 id:'BB +5.0V' reading_typ
8358:20130318:111122.173 Added sensor: host:'192.168.1.12:623' id_type:0 id_sz:14 id:'BB +3.3V STBY' readi
8358:20130318:111122.173 Added sensor: host:'192.168.1.12:623' id_type:0 id_sz:9 id:'BB +3.3V' reading_typ
8358:20130318:111122.173 Added sensor: host:'192.168.1.12:623' id_type:0 id_sz:17 id:'BB +1.5V P1 DDR3' re
8358:20130318:111122.173 Added sensor: host:'192.168.1.12:623' id_type:0 id_sz:17 id:'BB +1.1V P1 Vccp' re
8358:20130318:111122.174 Added sensor: host:'192.168.1.12:623' id_type:0 id_sz:14 id:'BB +1.05V PCH' readi
```

Do dekodowania typów i stanów sensorów IPMI dostępna jest kopia specyfikacji IPMI 2.0 (proszę zauważyć, że nie są planowane dalsze aktualizacje specyfikacji IPMI).

Pierwszym parametrem, od którego należy zacząć, jest ”reading_type”. Użyj ”Table 42-1, Event/Reading Type Code Ranges” ze specyfikacji, aby zdekodować kod ”reading_type”. Większość sensorów w naszym przykładzie ma ”reading_type:0x1”, co oznacza sensor typu ”threshold”. ”Table 42-3, Sensor Type Codes” pokazuje, że ”type:0x1” oznacza sensor temperatury, ”type:0x2” — sensor napięcia, ”type:0x4” — wentylator itd. Sensory progowe są czasami nazywane sensorami ”analogowymi”, ponieważ mierzą ciągłe parametry, takie jak temperatura, napięcie, obroty na minutę.

Inny przykład — sensor z ”reading_type:0x3”. ”Table 42-1, Event/Reading Type Code Ranges” mówi, że kody typu odczytu 02h-0Ch oznaczają sensor ”Generic Discrete”. Sensory dyskretne mają do 15 możliwych stanów (innymi słowy — do 15 znaczących bitów). Na przykład dla sensora ’CATERR’ z ”type:0x7” ”Table 42-3, Sensor Type Codes” pokazuje, że ten typ oznacza ”Processor”, a znaczenie poszczególnych bitów jest następujące: 00h (bit najmniej znaczący) — IERR, 01h — Thermal Trip itd.

W naszym przykładzie jest kilka sensorów z ”reading_type:0x6f”. Dla tych sensorów ”Table 42-1, Event/Reading Type Code Ranges” zaleca użycie ”Table 42-3, Sensor Type Codes” do dekodowania znaczenia bitów. Na przykład sensor ’Power Unit Stat’ ma typ ”type:0x9”, co oznacza ”Power Unit”. Przesunięcie 00h oznacza ”PowerOff/Power Down”. Innymi słowy, jeśli bit najmniej znaczący ma wartość 1, to serwer jest wyłączony. Aby sprawdzić ten bit, można użyć funkcji `bitand` z maską ’1’. Wyrażenie wyzwalacza może wyglądać następująco:

```
bitand(last(/www.example.com/Power Unit Stat,#1),1)=1
```

aby ostrzegać o wyłączeniu zasilania serwera.

Uwagi dotyczące nazw czujników dyskretnych w OpenIPMI-2.0.16, 2.0.17, 2.0.18 i 2.0.19

Nazwy czujników dyskretnych w OpenIPMI-2.0.16, 2.0.17 i 2.0.18 często mają na końcu dodane dodatkowe ”0” (lub inną cyfrę albo literę). Na przykład, podczas gdy `ipmitool` i OpenIPMI-2.0.19 wyświetlają nazwy czujników jako ”PhysicalSecurity” lub ”CATERR”, w OpenIPMI-2.0.16, 2.0.17 i 2.0.18 nazwy te to odpowiednio ”PhysicalSecurity0” lub ”CATERR0”.

Podczas konfigurowania pozycji IPMI w serwerze Zabbix z użyciem OpenIPMI-2.0.16, 2.0.17 i 2.0.18 należy używać tych nazw zakończonych na ”0” w polu *IPMI sensor* pozycji agenta IPMI. Gdy serwer Zabbix zostanie zaktualizowany do nowej dystrybucji Linuksa, która używa OpenIPMI-2.0.19 (lub nowszej), pozycje z tymi dyskretnymi czujnikami IPMI staną się ”NOT SUPPORTED”. Należy zmienić ich nazwy *IPMI sensor* (usunąć końcowe ’0’) i odczekać pewien czas, aż ponownie staną się ”Enabled”.

Uwagi dotyczące jednoczesnej dostępności czujnika progowego i czujnika dyskretnego

Niektóre agenty IPMI udostępniają zarówno czujnik progowy, jak i czujnik dyskretny pod tą samą nazwą. Zawsze preferowany jest czujnik progowy.

Uwagi dotyczące zakończenia połączenia

Jeśli kontrole IPMI nie są wykonywane (z dowolnego powodu: wszystkie pozycje IPMI hosta są wyłączone/nieobsługiwane, host jest wyłączony/usunięty, host jest w trybie konserwacji itp.), połączenie IPMI zostanie zakończone przez serwer Zabbix lub proxy w ciągu 3 do 4 godzin, w zależności od czasu uruchomienia serwera/proxy Zabbix.

5 Proste testy

Przegląd

Proste testy są zwykle używane do zdalnego monitorowania usług bez użycia agenta.

Należy pamiętać, że agent Zabbix nie jest wymagany do prostych testów. Za przetwarzanie prostych testów odpowiada serwer/proxy Zabbix (nawiązywanie połączeń zewnętrznych itp.).

Przykłady użycia prostych testów:

```
net.tcp.service[ftp,,155]
net.tcp.service[http]
net.tcp.service.perf[http,,8080]
net.udp.service.perf[ntp]
```

Note:
Pola *Nazwa użytkownika* i *Hasło* (ograniczone do 255 znaków) w konfiguracji pozycji prostego testu są używane dla pozycji monitorowania VMware; w pozostałych przypadkach są ignorowane.

Obsługiwane testy

Klucze pozycji są wymienione bez opcjonalnych parametrów i dodatkowych informacji. Kliknij klucz pozycji, aby zobaczyć pełne szczegóły.

Zobacz także klucze pozycji monitorowania VMware.

Klucz pozycji	Opis
icmpping	Dostępność hosta za pomocą ICMP ping.
icmppingloss	Procent utraconych pakietów.
icmppingretry	Dostępność hosta za pomocą ICMP ping z ponowieniami.
icmppingsec	Czas odpowiedzi ICMP ping.
net.tcp.service	Sprawdza, czy usługa jest uruchomiona i akceptuje połączenia TCP.
net.tcp.service.perf	Sprawdza wydajność usługi TCP.
net.udp.service	Sprawdza, czy usługa jest uruchomiona i odpowiada na żądania UDP.
net.udp.service.perf	Sprawdza wydajność usługi UDP.

Szczegóły klucza pozycji

Parametry bez nawiasów ostrych są obowiązkowe. Parametry oznaczone nawiasami ostrymi **< >** są opcjonalne.

icmpping[<target>,<packets>,<interval>,<size>,<timeout>,<options>]

 Dostępność hosta za pomocą ICMP ping.
 Zwracana wartość: *0* - ICMP ping nie powiódł się; *1* - ICMP ping zakończył się powodzeniem.

Parametry:

- **target** - adres IP hosta lub nazwa DNS;
- **packets** - liczba pakietów;
- **interval** - czas między kolejnymi pakietami w milisekundach;
- **size** - rozmiar pakietu w bajtach;

- **timeout** - limit czasu w milisekundach;
- **options** - używane do zezwolenia na przekierowanie: jeśli puste (wartość domyślna), odpowiedzi przekierowane są traktowane jako niedostępność hosta docelowego; jeśli ustawione na *allow_redirect*, odpowiedzi przekierowane są traktowane jako dostępność hosta docelowego.

Zobacz także tabelę wartości domyślnych.

Przykład:

```
icmpping[,4] #Jeśli zostanie zwrócony co najmniej jeden z czterech pakietów, pozycja zwróci 1.
```

icmppingloss[<target>,<packets>,<interval>,<size>,<timeout>,<options>]

 Procent utraconych pakietów.
 Zwracana wartość: *Float*.

Parametry:

- **target** - adres IP hosta lub nazwa DNS;
- **packets** - liczba pakietów;
- **interval** - czas między kolejnymi pakietami w milisekundach;
- **size** - rozmiar pakietu w bajtach;
- **timeout** - limit czasu w milisekundach;
- **options** - używane do zezwolenia na przekierowanie: jeśli puste (wartość domyślna), odpowiedzi przekierowane są traktowane jako niedostępność hosta docelowego; jeśli ustawione na *allow_redirect*, odpowiedzi przekierowane są traktowane jako dostępność hosta docelowego.

Zobacz także tabelę wartości domyślnych.

icmppingretry[<target>,<retries>,<backoff>,<size>,<timeout>,<options>]

 Dostępność hosta za pomocą ICMP ping z ponowieniami. Jeśli pierwszy pakiet zakończy się powodzeniem, dalsze próby są wstrzymywane; jeśli pakiet nie powiedzie się, próby są ponawiane aż do osiągnięcia maksymalnej liczby prób określonej w parametrze `retries`. Ta pozycja jest przydatna do zmniejszenia liczby pakietów wysyłanych przez sieć.
 Wartość zwracana: *0* - ICMP ping nie powiódł się; *1* - ICMP ping zakończył się powodzeniem.

Parametry:

- **target** - adres IP lub nazwa DNS hosta;
- **retries** - liczba ponowień próby pingowania celu, bez uwzględnienia pierwszej próby (0 lub więcej; domyślnie 1);
- **backoff** - wartość, przez którą mnożony jest czas oczekiwania przy każdym kolejnym żądaniu (zakres 1.0-5.0; domyślnie 1.0);
- **size** - rozmiar pakietu w bajtach;
- **timeout** - limit czasu w milisekundach;
- **options** - używane do zezwalania na przekierowanie: jeśli puste (wartość domyślna), odpowiedzi przekierowane są traktowane jako niedostępność hosta docelowego; jeśli ustawione na *allow_redirect*, odpowiedzi przekierowane są traktowane jako dostępność hosta docelowego.

Zobacz także tabelę wartości domyślnych.

icmppingsec[<target>,<packets>,<interval>,<size>,<timeout>,<mode>,<options>]

 Czas odpowiedzi ping ICMP (w sekundach).
 Zwracana wartość: *Float*.

Parametry:

- **target** - adres IP lub nazwa DNS hosta;
- **packets** - liczba pakietów;
- **interval** - czas między kolejnymi pakietami w milisekundach;
- **size** - rozmiar pakietu w bajtach;
- **timeout** - limit czasu w milisekundach;
- **mode** - możliwe wartości: *min*, *max* lub *avg* (domyślnie);
- **options** - używane do zezwolenia na przekierowanie: jeśli puste (wartość domyślna), odpowiedzi przekierowane są traktowane jako niedostępność hosta docelowego; jeśli ustawione na *allow_redirect*, odpowiedzi przekierowane są traktowane jako dostępność hosta docelowego.

Uwagi:

- Pakiety utracone lub takie, dla których upłynął limit czasu, nie są uwzględniane w obliczeniach;
- Jeśli host jest niedostępny (osiągnięto limit czasu), pozycja zwróci 0;
- Jeśli zwracana wartość jest mniejsza niż 0.0001 sekundy, wartość zostanie ustawiona na 0.0001 sekundy;
- Zobacz także tabelę wartości domyślnych.

net.tcp.service[service,<ip>,<port>]

 Sprawdza, czy usługa działa i akceptuje połączenia TCP.
 Zwracana wartość: *0* - usługa jest niedostępna; *1* - usługa działa.

Parametry:

- **service** - możliwe wartości: *ssh*, *ldap*, *smtp*, *ftp*, *http*, *pop*, *nntp*, *imap*, *tcp*, *https*, *telnet* (zobacz szczegóły);
- **ip** - adres IP lub nazwa DNS (domyślnie używany jest IP/DNS hosta);
- **port** - numer portu (domyślnie używany jest standardowy numer portu usługi).

Uwagi:

- Należy pamiętać, że dla usługi *tcp* podanie portu jest obowiązkowe;
- Te testy mogą powodować dodatkowe komunikaty w plikach dziennika demonów systemowych (zwykle rejestrowane są sesje SMTP i SSH);
- Sprawdzanie szyfrowanych protokołów (takich jak IMAP na porcie 993 lub POP na porcie 995) nie jest obecnie obsługiwane. Jako obejście należy użyć `net.tcp.service[tcp,<ip>,port]` do takich testów.

Przykład:

```
net.tcp.service[ftp,,45] #Ta pozycja może być użyta do testowania dostępności serwera FTP na porcie TCP 45
```

Attention:
Jeśli SELinux działa w trybie enforced, niestandardowe proste testy TCP/UDP mogą być blokowane przez politykę. Aby zweryfikować i zezwolić na nowe połączenie wychodzące, sprawdź odmowy w audycie: używając `grep denied /var/log/audit/audit.log`

net.tcp.service.perf[service,<ip>,<port>]

 Sprawdza wydajność usługi TCP.
 Wartość zwracana: *Float*: *0.000000* - usługa jest niedostępna; *seconds* - liczba sekund poświęconych na połączenie z usługą.

Parametry:

- **service** - możliwe wartości: *ssh*, *ldap*, *smtp*, *ftp*, *http*, *pop*, *nntp*, *imap*, *tcp*, *https*, *telnet* (zobacz szczegóły);
- **ip** - adres IP lub nazwa DNS (domyślnie używany jest IP/DNS hosta);
- **port** - numer portu (domyślnie używany jest standardowy numer portu usługi).

Uwagi:

- Należy pamiętać, że w przypadku usługi *tcp* podanie portu jest obowiązkowe;
- Sprawdzanie szyfrowanych protokołów (takich jak IMAP na porcie 993 lub POP na porcie 995) nie jest obecnie obsługiwane. Jako obejście należy użyć `net.tcp.service[tcp,<ip>,port]` do takich kontroli.

Przykład:

```
net.tcp.service.perf[ssh] #Ta pozycja może być użyta do testowania szybkości początkowej odpowiedzi serwer
```

net.udp.service[service,<ip>,<port>]

 Sprawdza, czy usługa działa i odpowiada na żądania UDP.
 Zwracana wartość: *0* - usługa jest niedostępna; *1* - usługa działa.

Parametry:

- **service** - możliwe wartości: *ntp* (zobacz szczegóły);
- **ip** - adres IP lub nazwa DNS (domyślnie używany jest IP/DNS hosta);
- **port** - numer portu (domyślnie używany jest standardowy numer portu usługi).

Przykład:

```
net.udp.service[ntp,,45] #Ta pozycja może być użyta do testowania dostępności usługi NTP na porcie UDP 45.
```

net.udp.service.perf[service,<ip>,<port>]

 Sprawdza wydajność usługi UDP.
 Zwracana wartość: *Float*: *0.000000* - usługa jest niedostępna; *seconds* - liczba sekund oczekiwania na odpowiedź z usługi.

Parametry:

- **service** - możliwe wartości: *ntp* (zobacz szczegóły);
- **ip** - adres IP lub nazwa DNS (domyślnie używany jest IP/DNS hosta);
- **port** - numer portu (domyślnie używany jest standardowy numer portu usługi).

Przykład:

```
net.udp.service.perf[ntp] #Ta pozycja może być użyta do testowania czasu odpowiedzi usługi NTP.
```

Attention:
Do obsługi SourceIP w prostych kontrolach LDAP (np. `net.tcp.service[ldap]`) wymagana jest wersja OpenLDAP 2.6.1 lub nowsza.

Przetwarzanie limitu czasu

Elastyczne limity czasu pozycji, mimo że są obsługiwane dla prostych testów, nie mają zastosowania do pozycji `icmpping*` i VMware. Zobacz Obsługa elastycznych limitów czasu.

Pingi ICMP

Zabbix używa zewnętrznego narzędzia **fping** do przetwarzania pingów ICMP (**icmpping**, **icmppingloss**, **icmppingretry**, **icmppingsec**).

Instalacja

fping nie jest dołączony do Zabbix i musi zostać zainstalowany osobno:

- Różne platformy oparte na Uniksie mają pakiet fping w swoich domyślnych repozytoriach, ale nie jest on preinstalowany. W takim przypadku można użyć menedżera pakietów do zainstalowania fping.
- Zabbix udostępnia pakiety fping dla RHEL i jego pochodnych. Należy pamiętać, że pakiety te są dostarczane bez oficjalnego wsparcia.
- fping można również skompilować ze źródeł.

Konfiguracja

Określ lokalizację fping w parametrze *FpingLocation* pliku konfiguracyjnego serwera/proxy Zabbix (lub parametrze *Fping6Location* w przypadku używania adresów IPv6).

fping powinien być wykonywalny dla użytkownika, z uprawnieniami którego działa serwer/proxy Zabbix, a użytkownik ten powinien mieć wystarczające uprawnienia.

Zobacz także: Znane problemy dotyczące przetwarzania prostych testów przy użyciu wersji fping starszych niż 3.10.

Wartości domyślne

Wartości domyślne, limity i opis wartości parametrów sprawdzania ICMP:

Parametr	Jednostka	Opis	Flaga fping	Wartości domyślne ustawiane przez		Dozwolone limity przez Zabbix	
				fping	**Zabbix**	**min**	**max**
packets	liczba	Liczba pakietów żądania wysyłanych do celu	-C		3	1	10000
interval	milisekundy	Czas oczekiwania między kolejnymi pakietami do pojedynczego celu	-p	1000		20	bez ograniczeń
size	bajty	Rozmiar pakietu w bajtach 56 bajtów na x86, 68 bajtów na x86_64	-b	56 lub 68		24	65507
timeout	milisekundy	**fping v3.x** - limit czasu oczekiwania po wysłaniu ostatniego pakietu, zależny od flagi *-C* **fping v4.x** - indywidualny limit czasu dla każdego pakietu	-t	**fping v3.x** - 500 **fping v4.x** i nowsze - dziedziczone z flagi *-p*, ale nie więcej niż 2000		50	bez ograniczeń

Parametr	Jednostka	Opis	Flaga fping	Wartości domyślne ustaw-iane przez		Dozwolone limity przez Zabbix	
retries	liczba	Liczba prób pingowania celu, nie licząc pierwszej próby	-r	3	1	0	bez ograniczeń
backoff factor	liczba	Wartość, przez którą mnożony jest czas oczekiwania przy każdym kolejnym żądaniu	-B	1.5	1.0	1.0	5.0

Wartości domyślne mogą się nieznacznie różnić w zależności od platformy i wersji.

Dodatkowo Zabbix używa opcji fping *-i interval ms* (nie należy mylić z parametrem pozycji *interval* wymienionym w tabeli powyżej, który odpowiada opcji fping *-p*) oraz *-S source IP address* (lub *-I* w starszych wersjach fping). Opcje te są wykrywane automatycznie przez uruchamianie sprawdzeń z różnymi kombinacjami opcji. Zabbix próbuje wykryć minimalną wartość w milisekundach, której fping pozwala użyć z opcją *-i*, testując 3 wartości: 0, 1 i 10. Wartość, która jako pierwsza zakończy się powodzeniem, jest następnie używana w kolejnych sprawdzeniach ICMP. Proces ten jest wykonywany indywidualnie przez każdy proces ICMP pinger.

Automatycznie wykryte opcje fping są unieważniane co godzinę i wykrywane ponownie przy następnej próbie wykonania sprawdzenia ICMP. Ustaw DebugLevel>=4, aby wyświetlić szczegóły tego procesu w pliku dziennika serwera lub proxy.

Zabbix zapisuje adresy IP do sprawdzenia przez dowolny z kluczy *icmpping** do pliku tymczasowego, który jest następnie przekazywany do fping. Jeśli pozycje mają różne parametry klucza, tylko te z identycznymi parametrami klucza są zapisywane do jednego pliku. Wszystkie adresy IP zapisane w jednym pliku będą sprawdzane przez fping równolegle, dlatego proces ICMP pinger Zabbix będzie zużywał stałą ilość czasu niezależnie od liczby adresów IP w pliku.

1 Klucze pozycji monitorowania VMware

Lista kluczy pozycji monitorowania VMware została przeniesiona do sekcji Monitorowanie VMware.

6 Monitorowanie plików dziennika

Przegląd

Zabbix może być używany do scentralizowanego monitorowania i analizy plików dziennika z obsługą lub bez obsługi rotacji logów.

Powiadomienia mogą być używane do ostrzegania użytkowników, gdy plik dziennika zawiera określone ciągi znaków lub wzorce ciągów.

Aby monitorować plik dziennika, musisz mieć:

- działający Zabbix agent na hoście
- skonfigurowaną pozycję monitorowania logów

Attention:
Limit rozmiaru monitorowanego pliku dziennika zależy od obsługi dużych plików.

Konfiguracja

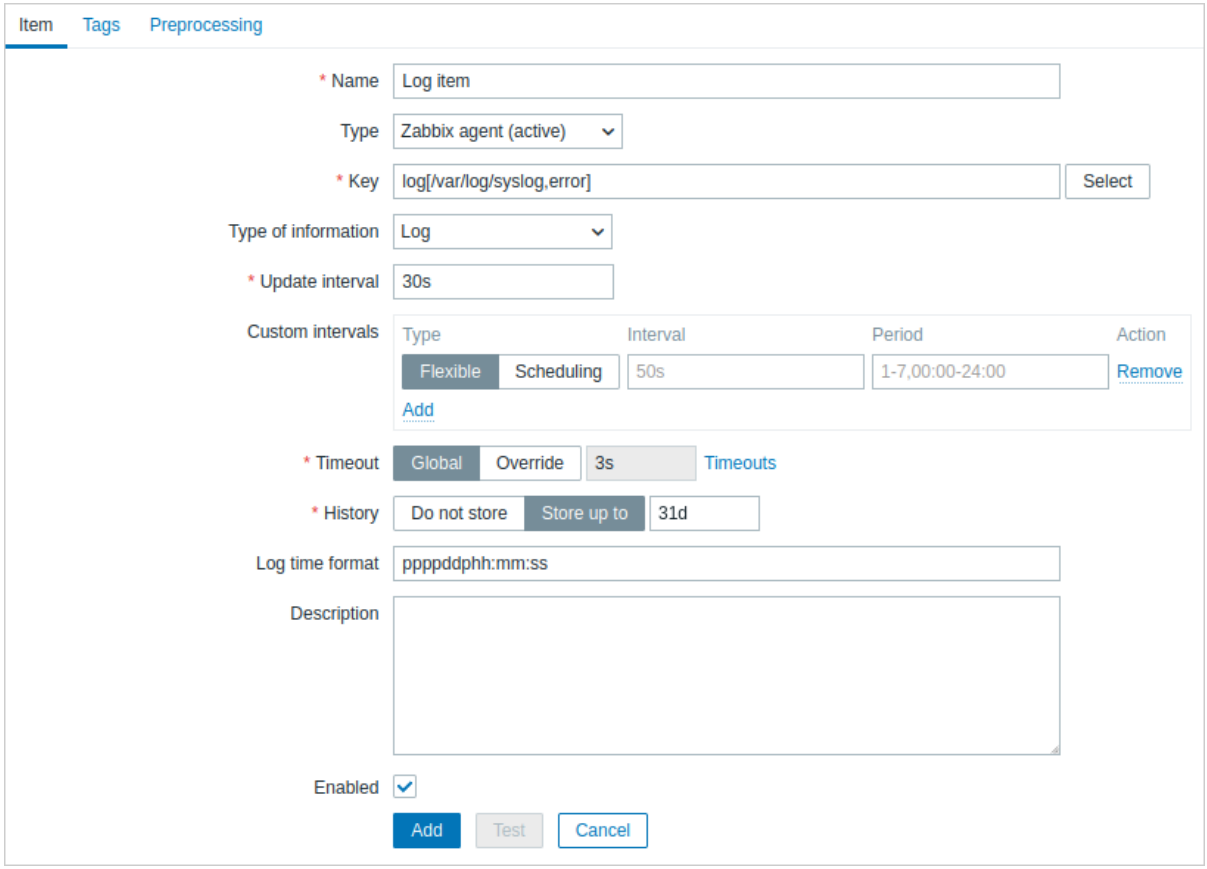
Zweryfikuj parametry agent

Upewnij się, że w pliku konfiguracyjnym agent:

- parametr `Hostname` odpowiada nazwie hosta we frontend.
- serwery w parametrze `ServerActive` są określone do przetwarzania aktywnych kontroli.

Konfiguracja pozycji

Skonfiguruj pozycję monitorowania logów item.



Wszystkie wymagane pola wejściowe są oznaczone czerwoną gwiazdką.

W przypadku pozycji monitorowania logów należy wprowadzić:

Type	Wybierz tutaj **Zabbix agent (active)**.
Key	Użyj jednego z następujących kluczy pozycji: **log[]** lub **logrt[]**: Te dwa klucze pozycji umożliwiają monitorowanie logów i filtrowanie wpisów logów za pomocą wyrażenia regularnego zawartości, jeśli zostało podane. Na przykład: `log[/var/log/syslog,error]`. Upewnij się, że plik ma uprawnienia do odczytu dla użytkownika 'zabbix', w przeciwnym razie status pozycji zostanie ustawiony na 'unsupported'. **log.count[]** lub **logrt.count[]**: Te dwa klucze pozycji umożliwiają zwrócenie tylko liczby pasujących wierszy. Szczegółowe informacje o używaniu tych kluczy pozycji i ich parametrów można znaleźć w sekcji kluczy obsługiwanych Zabbix agent item.
Type of information	Wypełniane automatycznie: Dla pozycji log[] lub logrt[] - `Log`; Dla pozycji log.count[] lub logrt.count[] - `Numeric (unsigned)`. W przypadku opcjonalnego użycia parametru `output` można ręcznie wybrać odpowiedni typ informacji inny niż `Log`. Należy pamiętać, że wybranie typu informacji innego niż Log spowoduje utratę lokalnego znacznika czasu.
Update interval (in sec)	Parametr określa, jak często Zabbix agent będzie sprawdzać, czy w pliku logu zaszły jakiekolwiek zmiany. Ustawienie wartości 1 sekundy zapewni otrzymywanie nowych rekordów tak szybko, jak to możliwe.

Log time format	W tym polu można opcjonalnie określić wzorzec do analizowania znacznika czasu w wierszu logu. Obsługiwane symbole zastępcze: * **y**: *Rok (1970-2038)* * **M**: *Miesiąc (01-12)* * **d**: *Dzień (01-31)* * **h**: *Godzina (00-23)* * **m**: *Minuta (00-59)* * **s**: *Sekunda (00-59)* Jeśli pole pozostanie puste, znacznik czasu zostanie ustawiony na 0 w czasie Unix, co odpowiada 1 stycznia 1970 roku. Na przykład rozważmy następujący wiersz z pliku logu Zabbix agent: " 23480:20100328:154718.045 Zabbix agent started. Zabbix 1.8.2 (revision 11211)." Rozpoczyna się on od sześciu pozycji znakowych dla PID, po których następują data, czas i pozostała część komunikatu. Format czasu logu dla tego wiersza to "ppppppp:yyyyMMdd:hhmmss". Należy pamiętać, że znaki "p" i ":" są symbolami zastępczymi i mogą być dowolnymi znakami z wyjątkiem "yMdhms".

Ważne uwagi

- serwer i agent przechowują informacje o rozmiarze monitorowanego pliku dziennika oraz czasie ostatniej modyfikacji (dla logrt) w dwóch licznikach. Dodatkowo:
  - agent używa również wewnętrznie numerów inode (w systemach UNIX/GNU/Linux), indeksów plików (w systemie Microsoft Windows) oraz sum MD5 z pierwszych 512 bajtów pliku dziennika, aby usprawnić podejmowanie decyzji, gdy pliki dziennika są obcinane i rotowane.
  - W systemach UNIX/GNU/Linux zakłada się, że systemy plików, na których przechowywane są pliki dziennika, raportują numery inode, które mogą być używane do śledzenia plików.
  - W systemie Microsoft Windows agent Zabbix określa typ systemu plików, na którym znajdują się pliki dziennika, i używa:
    * W systemach plików NTFS 64-bitowych indeksów plików.
    * W systemach plików ReFS (tylko od Microsoft Windows Server 2012) 128-bitowych identyfikatorów plików.
    * W systemach plików, w których indeksy plików się zmieniają (np. FAT32, exFAT), używany jest algorytm awaryjny, aby przyjąć rozsądne podejście w niepewnych warunkach, gdy rotacja plików dziennika skutkuje wieloma plikami dziennika z tym samym czasem ostatniej modyfikacji.
  - Numery inode, indeksy plików i sumy MD5 są zbierane wewnętrznie przez agent Zabbix. Nie są one przesyłane do serwera Zabbix i są tracone po zatrzymaniu agenta Zabbix.
  - Nie należy modyfikować czasu ostatniej modyfikacji pliku dziennika (na przykład za pomocą `touch`) ani zastępować monitorowanego pliku dziennika przez skopiowanie pliku z powrotem pod jego oryginalną nazwą (powoduje to utworzenie nowego inode). W obu przypadkach Zabbix może potraktować plik jako inny plik i odczytać go ponownie od początku, co może spowodować zduplikowane alerty.
  - Jeśli istnieje kilka pasujących plików dziennika dla pozycji `logrt[]`, a agent Zabbix śledzi najnowszy z nich i ten najnowszy plik dziennika zostanie usunięty, zapisywany jest komunikat ostrzegawczy `"there are no files matching "<regexp mask>" in "<directory>"`. agent Zabbix ignoruje pliki dziennika z czasem modyfikacji mniejszym niż najnowszy czas modyfikacji widziany przez agenta dla sprawdzanej pozycji `logrt[]`.
- agent rozpoczyna odczyt pliku dziennika od miejsca, w którym zakończył poprzednim razem.
- Liczba bajtów już przeanalizowanych (licznik rozmiaru) oraz czas ostatniej modyfikacji (licznik czasu) są przechowywane w bazie danych Zabbix i przesyłane do agenta, aby zapewnić, że agent rozpocznie odczyt pliku dziennika od tego miejsca w przypadkach, gdy agent został właśnie uruchomiony lub otrzymał pozycje, które były wcześniej wyłączone albo nieobsługiwane. Jednak jeśli agent otrzymał z serwera niezerowy licznik rozmiaru, ale pozycja logrt[] lub logrt.count[] nie może znaleźć pasujących plików, licznik rozmiaru jest resetowany do 0, aby analizować od początku, jeśli pliki pojawią się później.
- Za każdym razem, gdy plik dziennika staje się mniejszy niż licznik rozmiaru dziennika znany agentowi, licznik jest resetowany do zera, a agent rozpoczyna odczyt pliku dziennika od początku, uwzględniając licznik czasu.
- Jeśli w katalogu znajduje się kilka pasujących plików z tym samym czasem ostatniej modyfikacji, agent próbuje poprawnie przeanalizować wszystkie pliki dziennika z tym samym czasem modyfikacji i uniknąć pomijania danych lub analizowania tych samych danych dwukrotnie, chociaż nie można tego zagwarantować we wszystkich sytuacjach. agent nie zakłada żadnego konkretnego schematu rotacji plików dziennika ani go nie określa. W przypadku wielu plików dziennika z tym samym czasem ostatniej modyfikacji agent będzie przetwarzał je w malejącej kolejności leksykograficznej. Dlatego w przypadku niektórych schematów rotacji pliki dziennika będą analizowane i raportowane w ich oryginalnej kolejności. W przypadku innych schematów rotacji oryginalna kolejność plików dziennika nie zostanie zachowana, co może prowadzić do raportowania pasujących rekordów plików dziennika w zmienionej kolejności (problem nie występuje, jeśli pliki dziennika mają różne czasy ostatniej modyfikacji).
- agent Zabbix przetwarza nowe rekordy pliku dziennika raz na *Update interval* sekund.
- agent Zabbix nie wysyła więcej niż **maxlines** pliku dziennika na sekundę. Limit zapobiega przeciążeniu zasobów sieci i CPU

oraz zastępuje wartość domyślną dostarczaną przez parametr **MaxLinesPerSecond** w pliku konfiguracyjnym agenta.

- Aby znaleźć wymagany ciąg, Zabbix przetworzy 10 razy więcej nowych linii niż ustawiono w MaxLinesPerSecond. Dlatego na przykład, jeśli pozycja `log[]` lub `logrt[]` ma *Update interval* równy 1 sekundzie, domyślnie agent przeanalizuje nie więcej niż 200 rekordów pliku dziennika i wyśle nie więcej niż 20 pasujących rekordów do serwera Zabbix podczas jednego sprawdzenia. Zwiększając **MaxLinesPerSecond** w pliku konfiguracyjnym agenta lub ustawiając parametr **maxlines** w kluczu pozycji, można zwiększyć limit maksymalnie do 10000 analizowanych rekordów pliku dziennika i 1000 pasujących rekordów wysyłanych do serwera Zabbix podczas jednego sprawdzenia. Jeśli *Update interval* jest ustawiony na 2 sekundy, limity dla jednego sprawdzenia będą 2 razy wyższe niż przy *Update interval* równym 1 sekundzie.
- Dodatkowo wartości log i log.count są zawsze ograniczone do 50% rozmiaru bufora wysyłania agenta, nawet jeśli nie ma w nim wartości innych niż logi. Aby więc wartości **maxlines** zostały wysłane w jednym połączeniu (a nie w kilku połączeniach), parametr BufferSize agenta musi mieć wartość co najmniej maxlines x 2. agent Zabbix może przesyłać dane podczas zbierania logów i w ten sposób zwalniać bufor, natomiast agent Zabbix 2 zatrzyma zbieranie logów do czasu przesłania danych i zwolnienia bufora, co jest wykonywane asynchronicznie.
- Przy braku pozycji logów cały rozmiar bufora agenta jest używany dla wartości innych niż logi. Gdy pojawiają się wartości logów, zastępują one starsze wartości inne niż logi w razie potrzeby, do wyznaczonego poziomu 50%.
- Dla rekordów pliku dziennika dłuższych niż 256kB tylko pierwsze 256kB jest dopasowywane do wyrażenia regularnego, a reszta rekordu jest ignorowana. Jednak jeśli agent Zabbix zostanie zatrzymany podczas przetwarzania długiego rekordu, wewnętrzny stan agenta zostanie utracony i długi rekord może zostać przeanalizowany ponownie i inaczej po ponownym uruchomieniu agenta.
- Uwaga specjalna dotycząca separatorów ścieżek "\": jeśli file_format ma wartość "file\.log", nie powinien istnieć katalog "file", ponieważ nie da się jednoznacznie określić, czy "." jest znakiem specjalnym poprzedzonym znakiem ucieczki, czy pierwszym symbolem nazwy pliku.
- Wyrażenia regularne dla `logrt` są obsługiwane tylko w nazwie pliku; dopasowywanie wyrażeń regularnych dla katalogu nie jest obsługiwane.
- Na platformach UNIX pozycja `logrt[]` staje się NOTSUPPORTED, jeśli katalog, w którym oczekuje się znalezienia plików dziennika, nie istnieje.
- W systemie Microsoft Windows, jeśli katalog nie istnieje, pozycja nie stanie się NOTSUPPORTED (na przykład jeśli nazwa katalogu jest błędnie wpisana w kluczu pozycji).
- Brak plików dziennika dla pozycji `logrt[]` nie powoduje, że staje się ona NOTSUPPORTED. Błędy odczytu plików dziennika dla pozycji `logrt[]` są zapisywane jako ostrzeżenia w pliku dziennika agenta Zabbix, ale nie powodują, że pozycja staje się NOTSUPPORTED.
- Plik dziennika agenta Zabbix może być pomocny w ustaleniu, dlaczego pozycja `log[]` lub `logrt[]` stała się NOTSUPPORTED. Zabbix może monitorować plik dziennika swojego agenta, z wyjątkiem sytuacji, gdy DebugLevel=4 lub DebugLevel=5.
- Wyszukiwanie znaku zapytania za pomocą wyrażenia regularnego, np. \?, może skutkować fałszywie dodatnimi wynikami, jeśli plik tekstowy zawiera symbole NUL, ponieważ są one zastępowane przez "?" przez Zabbix, aby kontynuować przetwarzanie linii aż do znaku nowej linii.

Wyodrębnianie pasującej części wyrażenia regularnego

Czasami możemy chcieć wyodrębnić z pliku docelowego tylko interesującą wartość, zamiast zwracać cały wiersz po znalezieniu dopasowania wyrażenia regularnego.

Pozycje logów mają możliwość wyodrębniania żądanych wartości z dopasowanych wierszy. Jest to realizowane za pomocą dodatkowego parametru **output** w pozycjach `log` i `logrt`.

Użycie parametru „output" pozwala wskazać „grupę przechwytującą" dopasowania, która może nas interesować.

Na przykład

```
log[/path/to/the/file,"large result buffer allocation.*Entries: ([0-9]+)",,,,\1]
```

powinno umożliwić zwrócenie liczby wpisów znalezionej w treści:

```
Fr Feb 07 2014 11:07:36.6690 */ Thread Id 1400 (GLEWF) large result
buffer allocation - /Length: 437136/Entries: 5948/Client Ver: >=10/RPC
ID: 41726453/User: AUser/Form: CFG:ServiceLevelAgreement
```

Zwrócona zostanie tylko liczba, ponieważ **\1** odnosi się do pierwszej i jedynej grupy przechwytującej: **([0-9]+)**.

Dzięki możliwości wyodrębnienia i zwrócenia liczby, wartość ta może zostać użyta do definiowania wyzwalaczy.

Używanie parametru maxdelay

Parametr `maxdelay` w pozycjach logów pozwala ignorować niektóre starsze linie z plików logów, aby najnowsze linie zostały przeanalizowane w czasie `maxdelay` sekund.

Warning:
Ustawienie `maxdelay` > 0 może prowadzić do **ignorowania ważnych wpisów pliku logu i pominięcia alertów**. Należy używać go ostrożnie, na własne ryzyko i tylko wtedy, gdy jest to konieczne.

Domyślnie pozycje do monitorowania logów śledzą wszystkie nowe linie pojawiające się w plikach logów. Istnieją jednak aplikacje, które w pewnych sytuacjach zaczynają zapisywać ogromną liczbę komunikatów do swoich plików logów. Na przykład, jeśli baza danych lub serwer DNS jest niedostępny, takie aplikacje zalewają pliki logów tysiącami niemal identycznych komunikatów o błędach, dopóki normalne działanie nie zostanie przywrócone. Domyślnie wszystkie te komunikaty będą sumiennie analizowane, a pasujące linie wysyłane do serwer zgodnie z konfiguracją w pozycjach `log` i `logrt`.

Wbudowana ochrona przed przeciążeniem składa się z konfigurowalnego parametru `maxlines` (chroni serwer przed zbyt dużą liczbą przychodzących pasujących linii logów) oraz limitu 10*'maxlines' (chroni CPU i operacje I/O host przed przeciążeniem przez agent podczas jednego sprawdzenia). Mimo to wbudowana ochrona ma 2 problemy. Po pierwsze, duża liczba potencjalnie mało informacyjnych komunikatów jest raportowana do serwer i zajmuje miejsce w bazie danych. Po drugie, ze względu na ograniczoną liczbę linii analizowanych na sekundę agent może pozostawać w tyle za najnowszymi wpisami logów przez wiele godzin. Jest bardzo prawdopodobne, że wolisz szybciej otrzymać informację o bieżącej sytuacji w plikach logów, zamiast przez wiele godzin przedzierać się przez stare wpisy.

Rozwiązaniem obu problemów jest użycie parametru `maxdelay`. Jeśli ustawiono `maxdelay` > 0, podczas każdego sprawdzenia mierzona jest liczba przetworzonych bajtów, liczba pozostałych bajtów oraz czas przetwarzania. Na podstawie tych wartości agent oblicza szacowane opóźnienie — ile sekund zajęłaby analiza wszystkich pozostałych wpisów w pliku logu.

Jeśli opóźnienie nie przekracza `maxdelay`, agent kontynuuje analizę pliku logu jak zwykle.

Jeśli opóźnienie jest większe niż `maxdelay`, agent **ignoruje fragment pliku logu, „przeskakując" nad nim** do nowej szacowanej pozycji, tak aby pozostałe linie mogły zostać przeanalizowane w czasie `maxdelay` sekund.

Należy pamiętać, że agent nawet nie wczytuje ignorowanych linii do bufora, lecz oblicza przybliżoną pozycję, do której ma przeskoczyć w pliku.

Fakt pomijania linii pliku logu jest zapisywany w pliku logu agent w następujący sposób:

```
14287:20160602:174344.206 item:"logrt["/home/zabbix32/test[0-9].log",ERROR,,1000,,,120.0]"
logfile:"/home/zabbix32/test1.log" skipping 679858 bytes
(from byte 75653115 to byte 76332973) to meet maxdelay
```

Liczba „to byte" jest przybliżona, ponieważ po „przeskoku" agent dostosowuje pozycję w pliku do początku linii logu, która może znajdować się dalej w pliku lub wcześniej.

W zależności od tego, jak szybkość przyrastania pliku ma się do szybkości analizowania pliku logu, możesz nie obserwować żadnych „przeskoków", obserwować je rzadko lub często, duże lub małe „przeskoki", a nawet mały „przeskok" przy każdym sprawdzeniu. Wahania obciążenia systemu i opóźnienia sieci również wpływają na obliczanie opóźnienia, a tym samym na „przeskakiwanie" do przodu w celu dotrzymania parametru `maxdelay`.

Nie zaleca się ustawiania `maxdelay` < `update interval` (może to skutkować częstymi małymi „przeskokami").

Uwagi dotyczące obsługi rotacji plików dziennika typu „copytruncate"

`logrt` z opcją `copytruncate` zakłada, że różne pliki dziennika zawierają różne rekordy (co najmniej ich znaczniki czasu są różne), dlatego sumy MD5 początkowych bloków (do pierwszych 512 bajtów) będą różne. Dwa pliki z takimi samymi sumami MD5 początkowych bloków oznaczają, że jeden z nich jest oryginałem, a drugi — kopią.

`logrt` z opcją `copytruncate` dokłada starań, aby poprawnie przetwarzać kopie plików dziennika bez zgłaszania duplikatów. Nie zaleca się jednak takich sytuacji, jak tworzenie wielu kopii plików dziennika z tym samym znacznikiem czasu, rotacja plików dziennika częściej niż interwał aktualizacji pozycji logrt[], czy częste ponowne uruchamianie agent. agent stara się obsługiwać wszystkie te sytuacje w rozsądnie poprawny sposób, jednak nie można zagwarantować dobrych rezultatów we wszystkich okolicznościach.

Uwagi dotyczące trwałych plików dla pozycji log*[]

Przeznaczenie plików trwałych

Po uruchomieniu Zabbix agent otrzymuje listę aktywnych testów z serwera Zabbix lub proxy. Dla metryk log*[] otrzymuje rozmiar przetworzonego logu oraz czas modyfikacji, aby ustalić, od którego miejsca rozpocząć monitorowanie pliku logu. W zależności od rzeczywistego rozmiaru pliku logu i czasu modyfikacji zgłaszanego przez system plików agent decyduje, czy kontynuować monitorowanie pliku logu od rozmiaru przetworzonego logu, czy ponownie przeanalizować plik logu od początku.

Działający agent utrzymuje większy zestaw atrybutów do śledzenia wszystkich monitorowanych plików logów pomiędzy kolejnymi testami. Ten stan przechowywany w pamięci jest tracony po zatrzymaniu agenta.

Nowy opcjonalny parametr **persistent_dir** określa katalog do przechowywania tego stanu pozycja log[], log.count[], logrt[] lub logrt.count[] w pliku. Stan pozycji log jest odtwarzany z pliku trwałego po ponownym uruchomieniu Zabbix agent.

Podstawowym przypadkiem użycia jest monitorowanie pliku logu znajdującego się w systemie plików z kopią lustrzaną. Do pewnego momentu plik logu jest zapisywany na obu kopiach lustrzanych. Następnie kopie lustrzane są rozdzielane. Na aktywnej kopii plik logu nadal rośnie, otrzymując nowe wpisy. Zabbix agent analizuje go i wysyła do serwera rozmiar przetworzonych logów oraz czas modyfikacji. Na pasywnej kopii plik logu pozostaje bez zmian, znacznie w tyle za aktywną kopią. Później system operacyjny i Zabbix agent są ponownie uruchamiane z pasywnej kopii. Rozmiar przetworzonego logu i czas modyfikacji, które Zabbix agent otrzymuje z serwera, mogą nie być prawidłowe w sytuacji na pasywnej kopii. Aby kontynuować monitorowanie pliku logu od miejsca, w którym agent zakończył pracę w momencie rozdzielenia kopii lustrzanej systemu plików, agent odtwarza swój stan z pliku trwałego.

Działanie agenta z trwałym plikiem

Przy uruchomieniu agent Zabbix nic nie wie o trwałych plikach. Dopiero po otrzymaniu listy aktywnych kontroli z serwera Zabbix (proxy) agent widzi, że niektóre pozycje logów powinny być wspierane przez trwałe pliki w określonych katalogach.

Podczas działania agenta trwałe pliki są otwierane do zapisu (za pomocą fopen(filename, ”w”)) i nadpisywane najnowszymi danymi. Prawdopodobieństwo utraty danych trwałego pliku, jeśli nadpisywanie i rozdzielenie kopii lustrzanej systemu plików nastąpią w tym samym czasie, jest bardzo małe, nie stosuje się tu żadnej specjalnej obsługi. Po zapisie do trwałego pliku NIE jest wymuszana synchronizacja z nośnikiem danych (fsync() nie jest wywoływane).

Nadpisanie najnowszymi danymi następuje po pomyślnym zgłoszeniu pasującego rekordu pliku logu lub metadanych (przetworzony rozmiar logu i czas modyfikacji) do serwera Zabbix. Może to następować nawet przy każdym sprawdzeniu pozycji, jeśli plik logu stale się zmienia.

Podczas zamykania agenta nie są wykonywane żadne specjalne działania.

Po otrzymaniu listy aktywnych testów agent oznacza przestarzałe pliki trwałe do usunięcia. Plik trwały staje się przestarzały, jeśli:

1. Odpowiadająca mu pozycja logu nie jest już monitorowana.
2. Pozycja logu zostanie przekonfigurowana z inną lokalizacją **persistent_dir** niż wcześniej.

Usuwanie jest wykonywane z opóźnieniem 24 godzin, ponieważ pliki logów w stanie NOTSUPPORTED nie są uwzględniane na liście aktywnych testów, ale mogą później ponownie przejść do stanu SUPPORTED i ich pliki trwałe będą przydatne.

Jeśli agent zostanie zatrzymany przed upływem 24 godzin, przestarzałe pliki nie zostaną usunięte, ponieważ agent Zabbix nie otrzymuje już z serwera Zabbix informacji o ich lokalizacji.

Warning:
Przekonfigurowanie **persistent_dir** pozycji logu z powrotem na starą lokalizację **persistent_dir** podczas gdy agent jest zatrzymany, bez usunięcia starego pliku trwałego przez użytkownika, spowoduje odtworzenie stanu agenta ze starego pliku trwałego, co doprowadzi do pominiętych komunikatów lub fałszywych alertów.

Nazewnictwo i lokalizacja plików trwałych

Zabbix agent rozróżnia aktywne sprawdzenia na podstawie ich kluczy. Na przykład, logrt[/home/zabbix/test.log] i logrt[/home/zabbix/test.log,] to różne pozycje. Zmiana pozycji logrt[/home/zabbix/test.log„,10] we frontendzie na logrt[/home/zabbix/test.log„,2 spowoduje usunięcie pozycji logrt[/home/zabbix/test.log„,10] z listy aktywnych sprawdzeń agenta i utworzenie pozycji logrt[/home/zabbix/test.log„,20] (niektóre atrybuty są przenoszone podczas modyfikacji we frontendzie/serwerze, ale nie w agencie).

Nazwa pliku składa się z sumy MD5 klucza pozycji z dołączoną długością klucza pozycji, aby zmniejszyć możliwość kolizji. Na przykład, stan pozycji logrt[/home/zabbix50/test.log„„„„„/home/zabbix50/agent_private] będzie przechowywany w pliku trwałym c963ade4008054813bbc0a650bb8e09266.

Wiele pozycji log może używać tej samej wartości **persistent_dir**.

persistent_dir jest określany z uwzględnieniem specyficznych układów systemu plików, punktów montowania, opcji montowania oraz konfiguracji dublowania pamięci masowej — plik trwały powinien znajdować się w tym samym dublowanym systemie plików co monitorowany plik logu.

Jeśli katalog **persistent_dir** nie może zostać utworzony lub nie istnieje, albo prawa dostępu dla Zabbix agent nie pozwalają na tworzenie/zapis/odczyt/usuwanie plików, pozycja log stanie się NOTSUPPORTED.

Jeśli prawa dostępu do plików trwałej pamięci masowej zostaną usunięte podczas działania agent lub wystąpią inne błędy (np. brak miejsca na dysku), błędy są zapisywane w pliku dziennika agent, ale pozycja dziennika nie staje się NOTSUPPORTED.

Obciążenie wejścia/wyjścia

Plik trwały pozycji jest aktualizowany po pomyślnym wysłaniu każdego pakietu danych (zawierającego dane pozycji) do serwera. Na przykład domyślna wartość `BufferSize` wynosi 100. Jeśli pozycja logu znajdzie 70 pasujących rekordów, to pierwsze 50 rekordów zostanie wysłanych w jednym pakiecie, plik trwały zostanie zaktualizowany, następnie pozostałe 20 rekordów zostanie wysłanych (być może z pewnym opóźnieniem, gdy zgromadzi się więcej danych) w drugim pakiecie, a plik trwały zostanie zaktualizowany ponownie.

Działania, jeśli komunikacja między agent a serwerem nie powiedzie się

Każda pasująca linia z kontroli pozycji `log[]` i `logrt[]` oraz wynik każdej kontroli pozycji `log.count[]` i `logrt.count[]` wymaga wolnego miejsca w wydzielonym obszarze 50% bufora wysyłania agenta. Elementy bufora są regularnie wysyłane do serwera (lub proxy), a miejsca w buforze ponownie stają się wolne.

Dopóki w wydzielonym obszarze logów bufora wysyłania agenta są wolne miejsca i komunikacja między agent a serwerem (lub proxy) nie działa, wyniki monitorowania logów są gromadzone w buforze wysyłania. Pomaga to ograniczyć skutki krótkotrwałych problemów z komunikacją.

Podczas dłuższych problemów z komunikacją wszystkie miejsca przeznaczone na logi zostają zajęte i podejmowane są następujące działania:

- kontrole pozycji `log[]` i `logrt[]` są zatrzymywane. Po przywróceniu komunikacji i gdy w buforze dostępne są wolne miejsca, kontrole są wznawiane od poprzedniej pozycji. Żadne pasujące linie nie zostają utracone, są jedynie raportowane później.
- kontrole `log.count[]` i `logrt.count[]` są zatrzymywane, jeśli `maxdelay = 0` (domyślnie). Zachowanie jest podobne jak w przypadku pozycji `log[]` i `logrt[]`, jak opisano powyżej. Należy pamiętać, że może to wpływać na wyniki `log.count[]` i `logrt.count[]`: na przykład jedna kontrola zlicza 100 pasujących linii w pliku logu, ale ponieważ w buforze nie ma wolnych miejsc, kontrola zostaje zatrzymana. Po przywróceniu komunikacji agent zlicza te same 100 pasujących linii, a także 70 nowych pasujących linii. Agent wysyła teraz count = 170, tak jakby zostały znalezione podczas jednej kontroli.
- kontrole `log.count[]` i `logrt.count[]` z `maxdelay > 0`: jeśli podczas kontroli nie wystąpił „skok", zachowanie jest podobne do opisanego powyżej. Jeśli nastąpił „skok" ponad liniami pliku logu, zachowywana jest pozycja po „skoku", a zliczony wynik jest odrzucany. W ten sposób agent próbuje nadążyć za rosnącym plikiem logu nawet w przypadku problemów z komunikacją.

Obsługa błędów kompilacji i błędów wykonania wyrażeń regularnych

Jeśli wyrażenie regularne używane w pozycji `log[]`, `logrt[]`, `log.count[]` lub `logrt.count[]` nie może zostać skompilowane przez bibliotekę PCRE lub PCRE2, wówczas pozycja przechodzi w stan NOTSUPPORTED z komunikatem o błędzie. Aby kontynuować monitorowanie pozycji logu, należy poprawić wyrażenie regularne.

Jeśli wyrażenie regularne skompiluje się pomyślnie, ale zakończy się błędem podczas działania (dla niektórych lub wszystkich rekordów logu), wówczas pozycja logu pozostaje obsługiwana, a monitorowanie jest kontynuowane. Błąd wykonania jest zapisywany w pliku logu agenta Zabbix (bez rekordu z pliku logu).

Częstotliwość logowania jest ograniczona do jednego błędu wykonania na sprawdzenie, aby agent Zabbix mógł monitorować własny plik logu. Na przykład, jeśli analizowanych jest 10 rekordów, a 3 rekordy kończą się błędem wykonania regexp, w logu agenta tworzony jest jeden wpis.

Wyjątek: jeśli `MaxLinesPerSecond=1` i interwał aktualizacji=1 (do analizy na jedno sprawdzenie dozwolony jest tylko 1 rekord), wówczas błędy wykonania regexp nie są zapisywane w logu.

zabbix_agentd zapisuje klucz pozycji w przypadku błędu wykonania, a zabbix_agent2 zapisuje ID pozycji, aby ułatwić identyfikację, która pozycja logu powoduje błędy wykonania. W przypadku błędów wykonania zaleca się przeprojektowanie wyrażenia regularnego.

7 Pozycje obliczane

Przegląd

Pozycja obliczana umożliwia utworzenie obliczenia na podstawie wartości niektórych istniejących pozycji. Na przykład możesz chcieć obliczyć średnią godzinową wartości jakiejś pozycji albo obliczyć wartość łączną dla grupy pozycji. Właśnie do tego służy pozycja obliczana.

Obliczenia mogą wykorzystywać zarówno:

- pojedyncze wartości poszczególnych pozycji
- złożony filtr do wyboru wielu pozycji do agregacji (zobacz obliczenia agregujące po szczegóły)

Pozycje obliczane są sposobem tworzenia wirtualnych źródeł danych. Wszystkie obliczenia są wykonywane wyłącznie przez serwer Zabbix. Wartości są okresowo obliczane na podstawie użytego wyrażenia arytmetycznego.

Wynikowe dane są przechowywane w bazie danych Zabbix tak jak dla każdej innej pozycji; zapisywane są zarówno wartości historii, jak i trendów, a także mogą być generowane wykresy.

Note:
Jeśli wynik obliczenia jest wartością zmiennoprzecinkową, zostanie obcięty do liczby całkowitej, jeśli typ informacji pozycji obliczanej to *Numeric (unsigned)*.
Ponadto, jeśli w pamięci podręcznej nie ma aktualnych danych i w funkcji nie zdefiniowano okresu odpytywania, Zabbix domyślnie cofnie się maksymalnie o jeden tydzień wstecz, aby odpytać bazę danych o wartości historyczne.

Pozycje obliczane współdzielą swoją składnię z wyrażeniami wyzwalaczy. Jeśli znasz wyrażenia wyzwalaczy, możesz myśleć o pozycjach obliczanych jak o funkcjach analizujących pewne wartości, ale bez porównania z progiem.

W pozycjach obliczanych dozwolone jest porównywanie ze stringami. Do pozycji obliczanych można odwoływać się za pomocą makr lub innych encji tak samo jak do każdego innego typu pozycji.

Aby używać pozycji obliczanych, wybierz typ pozycji **Calculated**.

Konfigurowalne pola

Klucz jest unikalnym identyfikatorem pozycji (w obrębie hosta). Możesz utworzyć dowolną nazwę klucza, używając obsługiwanych symboli.

Definicję obliczenia należy wprowadzić w polu **Formula**. Nie ma powiązania między formułą a kluczem. Parametry klucza nie są w żaden sposób używane w formule.

Składnia prostej formuły jest następująca:

```
function(/host/key,<parameter1>,<parameter2>,...)
```

gdzie:

Element	Opis
`function`	Jedna z obsługiwanych funkcji: last, min, max, avg, count itp.
`host`	Host pozycji używanej do obliczeń. Bieżący host można pominąć (tj. jak w `function(//key,parameter,...)`).
`key`	Klucz pozycji używanej do obliczeń. Pozycje zwracające wartości z binarnym lub JSON typem danych nie są obsługiwane.
`parameter(s)`	Parametry funkcji, jeśli są wymagane. Obsługiwane są sufiksy czasu oraz sufiksy rozmiaru pamięci.

Attention:
Makra użytkownika w formule zostaną rozwinięte, jeśli są używane do odwołania do parametru funkcji, parametru filtra pozycji lub stałej. Makra użytkownika NIE zostaną rozwinięte, jeśli odwołują się do funkcji, nazwy hosta, klucza pozycji, parametru klucza pozycji lub operatora.

Bardziej złożona formuła może wykorzystywać kombinację funkcji, operatorów i nawiasów. Możesz używać wszystkich funkcji i operatorów obsługiwanych w wyrażeniach wyzwalaczy. Logika i priorytet operatorów są dokładnie takie same.

W przeciwieństwie do wyrażeń wyzwalaczy, Zabbix przetwarza pozycje obliczane zgodnie z interwałem aktualizacji pozycji, a nie po otrzymaniu nowej wartości.

Wszystkie pozycje, do których odwołują się funkcje historii w formule pozycji obliczanej, muszą istnieć i zbierać dane. Ponadto, jeśli zmienisz klucz pozycji, do której istnieje odwołanie, musisz ręcznie zaktualizować wszystkie formuły używające tego klucza.

Pozycja obliczana może stać się nieobsługiwana w kilku przypadkach:

- pozycje, do których istnieje odwołanie
  - nie zostały znalezione
  - są wyłączone
  - należą do wyłączonego hosta
  - są nieobsługiwane (z wyjątkiem funkcji nodata() oraz operatorów z nieznanymi wartościami)
- brak danych do obliczenia funkcji
- dzielenie przez zero
- użyto nieprawidłowej składni

Przykłady użycia

Przykład 1

Obliczanie procentu wolnego miejsca na dysku dla '/'.

Użycie funkcji **last**:

```
100*last(//vfs.fs.size[/,free])/last(//vfs.fs.size[/,total])
```

Zabbix pobierze najnowsze wartości wolnego i całkowitego miejsca na dysku oraz obliczy wartość procentową zgodnie z podaną formułą.

Przykład 2

Obliczanie 10-minutowej średniej liczby wartości przetwarzanych przez Zabbix.

Użycie funkcji **avg**:

```
avg(/Zabbix Server/zabbix[wcache,values],10m)
```

Należy pamiętać, że intensywne używanie pozycji obliczanych z długimi okresami czasu może wpływać na wydajność serwera Zabbix.

Przykład 3

Obliczanie całkowitej przepustowości na eth0.

Suma dwóch funkcji:

```
last(//net.if.in[eth0,bytes])+last(//net.if.out[eth0,bytes])
```

Przykład 4

Obliczanie procentowego udziału ruchu przychodzącego.

Bardziej złożone wyrażenie:

```
100*last(//net.if.in[eth0,bytes])/(last(//net.if.in[eth0,bytes])+last(//net.if.out[eth0,bytes]))
```

Zobacz także: Przykłady obliczeń agregowanych

1 Obliczenia agregowane

Przegląd

Obliczenia agregujące są typem pozycji obliczanej, który umożliwia zbieranie informacji z kilku pozycji przez serwer Zabbix, a następnie obliczanie wartości zagregowanej, w zależności od użytej funkcji agregującej.

Obliczenia agregujące nie wymagają uruchomionego agenta na monitorowanym hoście.

Składnia

Aby pobrać agregaty, użyj jednej z obsługiwanych funkcji agregujących: `avg`, `max`, `min`, `sum` itd. Następnie dodaj funkcję **foreach** jako jedyny parametr oraz jej filtr pozycji, aby wybrać wymagane pozycje:

```
aggregate_function(function_foreach(/host/key?[group="host group"],timeperiod))
```

Funkcja **foreach** (np. *avg_foreach*, *count_foreach* itd.) zwraca jedną wartość agregowaną dla każdej wybranej pozycji. Pozycje są wybierane przy użyciu filtra pozycji (`/host/key?[group="host group"]`) z historii pozycji. Więcej informacji znajduje się w sekcji funkcje foreach.

Jeśli niektóre pozycje nie mają danych dla żądanego okresu, są ignorowane podczas obliczeń. Jeśli żadna pozycja nie ma danych, funkcja zwróci błąd.

Alternatywnie możesz podać kilka pozycji jako parametry agregacji:

```
aggregate_function(function(/host/key,parameter),function(/host2/key2,parameter),...)
```

Zwróć uwagę, że `function` musi tutaj być funkcją historii/trendów.

Note:
Jeśli agregacja daje wartość zmiennoprzecinkową, zostanie ona obcięta do liczby całkowitej, jeśli typ informacji agregowanej pozycji to *Numeric (unsigned)*.

Makra użytkownika i makra wykrywania niskopoziomowego są obsługiwane w:

- parametrach klucza pozycji
- parametrach funkcji
- warunkach filtra (nazwa grupy hostów i nazwa tagu)
- stałych wyrażenia

Obliczenie agregatu może stać się nieobsługiwane, jeśli:

- nie znaleziono żadnej z odwoływanych pozycji (co może się zdarzyć, jeśli klucz pozycji jest nieprawidłowy, żadna z pozycji nie istnieje lub wszystkie uwzględnione grupy są nieprawidłowe)
- brak danych do obliczenia funkcji

Przykłady użycia

Przykłady kluczy dla obliczeń agregujących.

Przykład 1

Całkowita przestrzeń dyskowa grupy hostów „MySQL Servers”.

```
sum(last_foreach(/*/vfs.fs.size[/,total]?[group="MySQL Servers"]))
```

Przykład 2

Suma najnowszych wartości wszystkich pozycji pasujących do net.if.in[*] na hoście.

```
sum(last_foreach(/host/net.if.in[*]))
```

Przykład 3

Średnie obciążenie procesora dla grupy hostów „MySQL Servers”.

```
avg(last_foreach(/*/system.cpu.load[,avg1]?[group="MySQL Servers"]))
```

Przykład 4

5-minutowa średnia liczby zapytań na sekundę dla grupy hostów „MySQL Servers”.

```
avg(avg_foreach(/*/mysql.qps?[group="MySQL Servers"],5m))
```

Przykład 5

Średnie obciążenie CPU na wszystkich hostach w wielu grupach hostów, które mają określone tagi.

```
avg(last_foreach(/*/system.cpu.load?[(group="Servers A" or group="Servers B" or group="Servers C") and (ta
```

Przykład 6

Obliczenie używane na sumach najnowszych wartości pozycji dla całej grupy hostów.

```
sum(last_foreach(/*/net.if.out[eth0,bytes]?[group="video"])) / sum(last_foreach(/*/nginx_stat.sh[active]?[
```

Przykład 7

Łączna liczba niewspieranych pozycji w grupie hostów „Zabbix servers”.

```
sum(last_foreach(/*/zabbix[host,,items_unsupported]?[group="Zabbix servers"]))
```

Przykład 8

Suma najnowszych wyników liczbowych kontroli DNS dla wszystkich hostów. Pokazana forma pozycji to `net.dns[192.0.2.0,example.com,` jako przykład jednego z możliwych kluczy.

```
sum(last_foreach(/*/net.dns[*,*,*]))
```

Zwróć uwagę, że symbole wieloznaczne muszą odpowiadać liczbie parametrów w kluczu (tutaj `net.dns` ma trzy parametry: ip, name, type).

Przykłady poprawnej/niepoprawnej składni

Wyrażenia (w tym wywołania funkcji) nie mogą być używane jako parametry funkcji historii, trendów ani foreach function. Jednak same te funkcje mogą być używane w innych (niehistorycznych) parametrach funkcji.

Wyrażenie	Przykład
Poprawne	`avg(last(/host/key1),last(/host/key2)*10,last(/host/key1)*100)` `max(avg(avg_foreach(/*/system.cpu.load?[group="Servers A"],5m)),avg(avg_foreach(/*/system.cpu.load?[group="Servers B"],5m)),avg(avg_foreach(/*/system.cpu.load?[group="Servers C"],5m)))`

Niepoprawne	`sum(/host/key,10+2)`
	`sum(/host/key, avg(10,2))`
	`sum(/host/key,last(/host/key2))`

Zwróć uwagę, że w wyrażeniu takim jak:

```
sum(sum_foreach(//resptime[*],5m))/sum(count_foreach(//resptime[*],5m))
```

nie można zagwarantować, że obie części równania zawsze będą miały ten sam zestaw wartości. Podczas obliczania jednej części wyrażenia może nadejść nowa wartość dla żądanego okresu, a wtedy druga część wyrażenia będzie miała inny zestaw wartości.

8 Kontrole wewnętrzne

Przegląd

Kontrole wewnętrzne umożliwiają monitorowanie wewnętrznych procesów Zabbix. Innymi słowy, można monitorować to, co dzieje się z serwer Zabbix lub Zabbix proxy.

Kontrole wewnętrzne są obliczane:

- na serwer Zabbix — jeśli host jest monitorowany przez serwer
- na Zabbix proxy — jeśli host jest monitorowany przez proxy

Kontrole wewnętrzne są przetwarzane przez serwer lub proxy niezależnie od statusu konserwacji hosta.

Aby użyć tej pozycji, wybierz typ pozycji **Zabbix internal**.

Note:
Kontrole wewnętrzne są przetwarzane przez pollery Zabbix.

Wydajność

Używanie niektórych wewnętrznych pozycji może negatywnie wpływać na wydajność. Są to następujące pozycje:

- `zabbix[host,,items]`
- `zabbix[host,,items_unsupported]`
- `zabbix[hosts]`
- `zabbix[items]`
- `zabbix[items_unsupported]`
- `zabbix[queue,,]`
- `zabbix[requiredperformance]`
- `zabbix[stats,,,queue,,]`
- `zabbix[triggers]`

Dotyczy to również sekcji frontend Informacje o systemie oraz Kolejka.

Obsługiwane kontrole

Klucze pozycji są wymienione bez parametrów konfigurowalnych i dodatkowych informacji. Kliknij klucz pozycji, aby zobaczyć pełne szczegóły.

Item key	Opis
zabbix[boottime]	Czas uruchomienia procesu serwera Zabbix lub Zabbix proxy w sekundach.
zabbix[cluster,discovery,nodes]	Wykrywa węzły klastra wysokiej dostępności.
zabbix[connector_queue]	Liczba wartości umieszczonych w kolejce connector.
zabbix[discovery_queue]	Liczba kontroli sieciowych umieszczonych w kolejce wykrywania.
zabbix[host,,items]	Liczba włączonych pozycji (obsługiwanych i nieobsługiwanych) na hoście.
zabbix[host,,items_unsupported]	Liczba włączonych nieobsługiwanych pozycji na hoście.
zabbix[host,,maintenance]	Bieżący stan konserwacji hosta.
zabbix[host,active_agent,available]	Dostępność aktywnych kontroli agent na hoście.
zabbix[host,discovery,interfaces]	Szczegóły wszystkich skonfigurowanych interfejsów hosta w frontendzie Zabbix.
zabbix[host,,available]	Dostępność głównego interfejsu określonego typu kontroli na hoście.
zabbix[hosts]	Liczba monitorowanych hostów.
zabbix[items]	Liczba włączonych pozycji (obsługiwanych i nieobsługiwanych).
zabbix[items_unsupported]	Liczba nieobsługiwanych pozycji.
zabbix[java,,]	Informacje o Zabbix Java gateway.
zabbix[lld_queue]	Liczba wartości umieszczonych w kolejce przetwarzania wykrywania niskiego poziomu.
zabbix[preprocessing]	Statystyki wartości odebranych przez menedżera przetwarzania wstępnego.
zabbix[preprocessing_queue]	Liczba wartości umieszczonych w kolejce przetwarzania wstępnego.
zabbix[process,,,]	Procent czasu, jaki określony proces Zabbix lub grupa procesów (identyfikowana przez <type> i <mode>) spędziła w stanie <state>.

Item key	Opis
zabbix[proxy„]	Informacje o Zabbix proxy.
zabbix[proxy,discovery]	Lista Zabbix proxy.
zabbix[proxy group„available]	Liczba proxy online w grupie proxy.
zabbix[proxy group„pavailable]	Procent proxy online w grupie proxy.
zabbix[proxy group„proxies]	Lista Zabbix proxy w grupie proxy.
zabbix[proxy group„state]	Stan grupy proxy.
zabbix[proxy group,discovery]	Zwraca listę grup proxy z danymi konfiguracyjnymi i danymi czasu rzeczywistego.
zabbix[proxy_buffer,buffer,]	Zwraca statystyki użycia bufora pamięci proxy.
zabbix[proxy_buffer,state,changes]	Zwraca liczbę zmian stanu między trybami bufora dysk/pamięć od uruchomienia.
zabbix[proxy_buffer,state,current]	Zwraca bieżący stan pracy, w którym przechowywane są nowe dane.
zabbix[proxy_history]	Liczba wartości w tabeli historii proxy oczekujących na wysłanie do serwera.
zabbix[queue„]	Liczba monitorowanych pozycji w kolejce, które są opóźnione co najmniej o <from> sekund, ale mniej niż o <to> sekund.
zabbix[rcache„]	Statystyki dostępności pamięci podręcznej konfiguracji Zabbix.
zabbix[requiredperformance]	Wymagana wydajność serwera Zabbix lub Zabbix proxy, wyrażona jako oczekiwana liczba nowych wartości na sekundę.
zabbix[stats„]	Zwraca wewnętrzne metryki serwera Zabbix lub proxy. Jeśli określono <ip> i <port>, metryki są pobierane ze zdalnej instancji; w przeciwnym razie z instancji lokalnej.
zabbix[stats„,queue„]	Zwraca wewnętrzne metryki kolejki serwera Zabbix lub proxy. Jeśli określono <ip> i <port>, metryki są pobierane ze zdalnej instancji; w przeciwnym razie z instancji lokalnej.
zabbix[tcache„]	Statystyki efektywności pamięci podręcznej funkcji trendów Zabbix.
zabbix[triggers]	Liczba włączonych wyzwalaczy w bazie danych Zabbix, ze wszystkimi pozycjami włączonymi na włączonych hostach.
zabbix[uptime]	Czas działania procesu serwera Zabbix lub proxy w sekundach.
zabbix[vcache,buffer,]	Statystyki dostępności pamięci podręcznej wartości Zabbix.
zabbix[vcache,cache,]	Statystyki efektywności pamięci podręcznej wartości Zabbix.
zabbix[version]	Wersja serwera Zabbix lub proxy.
zabbix[vmware,buffer,]	Statystyki dostępności pamięci podręcznej vmware Zabbix.
zabbix[vps,written]	Łączna liczba wartości historii zapisanych do bazy danych.
zabbix[wcache„]	Statystyki i dostępność pamięci podręcznej zapisu Zabbix.

Szczegóły klucza pozycji

- Parametry bez nawiasów ostrych są obowiązkowe i muszą być użyte *dokładnie w tej postaci* (na przykład „host” i „available” w `zabbix[host,<type>,available]`).
- Parametry ujęte w nawiasy ostre **< >** muszą zostać zastąpione prawidłową wartością. Jeśli parametr ma wartość domyślną, można go pominąć.
- Wartości dla pozycji i parametrów pozycji oznaczonych jako „not supported on proxy” mogą być pobierane tylko wtedy, gdy host jest monitorowany przez serwer. Z kolei wartości oznaczone jako „not supported on server” mogą być pobierane tylko wtedy, gdy host jest monitorowany przez proxy.

zabbix[boottime]

 Czas uruchomienia procesu serwera Zabbix lub procesu Zabbix proxy w sekundach.
 Zwracana wartość: *Integer*.

zabbix[cluster,discovery,nodes]

 Wykrywa węzły klastra wysokiej dostępności.
 Zwracana wartość: *obiekt JSON*.

Uwagi:

- Ta pozycja może być używana w wykrywaniu niskiego poziomu.
- Zwracane pola w większości odpowiadają właściwościom obiektu węzła wysokiej dostępności.
- Dodatkowe pola:
  - `db_timestamp` — bieżący czas serwera (znacznik czasu Unix) uwzględniony w odpowiedzi
  - `lastaccess_age` — liczba sekund od ostatniego heartbeat węzła (db_timestamp - lastaccess)
  - `status` — stan węzła:
    - 0 — zapasowy
    - 1 — zatrzymany ręcznie

    * 2 — niedostępny
    * 3 — aktywny

Przykład zwracanych wartości:

```
[
  {
    "id": "ckvupihk70001z8mkpw5cg0u3",
    "name": "zabbix-prod-01",
    "status": 3,
    "address": "10.0.4.12:10051",
    "port": 10051,
    "lastaccess": 1756115995,
    "db_timestamp": 1756116000,
    "lastaccess_age": 5
  },
  {
    "id": "ckvx2a9k70004b1nq2hz9d7f",
    "name": "zabbix-standby-02",
    "status": 0,
    "address": "10.0.4.13:10051",
    "port": 10051,
    "lastaccess": 1756115550,
    "db_timestamp": 1756116000,
    "lastaccess_age": 450
  },
  {
    "id": "ckw0bq3l70007y4r1a0m5kz8",
    "name": "zabbix-backup-eu1",
    "status": 1,
    "address": "backup.example.com:10051",
    "port": 10051,
    "lastaccess": 1756105080,
    "db_timestamp": 1756116000,
    "lastaccess_age": 10920
  }
]
```

zabbix[connector_queue]

 Liczba wartości umieszczonych w kolejce connector queue.
 Zwracana wartość: *Integer*.

zabbix[discovery_queue]

 Liczba kontroli sieciowych umieszczonych w kolejce wykrywania.
 Wartość zwracana: *Integer*.

zabbix[host,„items]

 Liczba włączonych pozycji (obsługiwanych i nieobsługiwanych) na hoście.
 Zwracana wartość: *Integer*.

zabbix[host,„items_unsupported]

 Liczba włączonych nieobsługiwanych pozycji na hoście.
 Zwracana wartość: *Integer*.

zabbix[host,„maintenance]

 Bieżący status konserwacji hosta.
 Zwracane wartości: *0* - stan normalny; *1* - konserwacja z gromadzeniem danych; *2* - konserwacja bez gromadzenia danych.

Uwagi:

- Ta pozycja jest zawsze przetwarzana przez serwer Zabbix niezależnie od lokalizacji hosta (na serwerze lub proxy). Proxy nie otrzyma tej pozycji wraz z danymi konfiguracyjnymi.
- Drugi parametr musi być pusty i jest zarezerwowany do wykorzystania w przyszłości.

zabbix[host,active_agent,available]

 Dostępność aktywnych kontroli agenta na hoście.
 Zwracane wartości: *0* - nieznana; *1* - dostępny; *2* - niedostępny.

zabbix[host,discovery,interfaces]

 Szczegóły wszystkich skonfigurowanych interfejsów hosta w Zabbix frontend.
 Zwracana wartość: *obiekt JSON*.

Uwagi:

- Ta pozycja może być używana w odkrywaniu niskiego poziomu.
- Ta pozycja nie jest obsługiwana przez Zabbix proxy.

zabbix[host,<type>,available]

 Dostępność głównego interfejsu określonego typu kontroli na hoście.
 Zwracane wartości: *0* - nieznana; *1* - dostępny; *2* - niedostępny.

Parametry:

- **type** - *agent*, *snmp*, *ipmi* lub *jmx*.

Uwagi:

- Wartość pozycji jest obliczana zgodnie z parametrami konfiguracyjnymi dotyczącymi nieosiągalności/niedostępności hosta.

zabbix[hosts]

 Liczba monitorowanych hostów.
 Zwracana wartość: *Integer*.

zabbix[items]

 Liczba włączonych pozycji (obsługiwanych i nieobsługiwanych).
 Zwracana wartość: *Integer*.

zabbix[items_unsupported]

 Liczba nieobsługiwanych pozycji.
 Zwracana wartość: *Integer*.

zabbix[java,,<param>]

 Informacje o Zabbix Java gateway.
 Zwracane wartości: *1* - jeśli <param> to *ping*; *wersja Java gateway* - jeśli <param> to *version* (na przykład: ”8.0.0”).

Parametry:

- **param** - *ping* lub *version*.

Uwagi:

- Ta pozycja może być używana do sprawdzania dostępności Java gateway przy użyciu funkcji wyzwalacza `nodata()`.
- Drugi parametr musi być pusty i jest zarezerwowany do wykorzystania w przyszłości.

zabbix[lld_queue]

 Liczba wartości umieszczonych w kolejce przetwarzania wykrywania niskiego poziomu.
 Zwracana wartość: *Integer*.

Uwagi:

- Ta pozycja może być używana do monitorowania długości kolejki przetwarzania wykrywania niskiego poziomu.

zabbix[preprocessing]

 Statystyki wartości otrzymanych przez menedżera preprocessing:

- *queued* — liczba i rozmiar wartości oczekujących w kolejce, które wymagają preprocessing (licznik)
- *direct* — liczba i rozmiar wartości oczekujących w kolejce, które nie wymagają preprocessing (licznik)
- *queue* — liczba wartości umieszczonych w kolejce preprocessing (to samo co `zabbix[preprocessing_queue]`)

Zwracana wartość: *JSON*.

Przykład zwracanych wartości:

```
{"data":
    {
    "queued": {
        "count": 106,
        "size": 58620
    },
    "direct": {
        "count": 395,
        "size": 33843
    },
    "queue": 0
    }
}
```

zabbix[preprocessing_queue]

 Liczba wartości umieszczonych w kolejce przetwarzania wstępnego.
 Zwracana wartość: *Integer*.

Uwagi:

- Ta pozycja może być używana do monitorowania długości kolejki przetwarzania wstępnego.

zabbix[process,<type>,<mode>,<state>]

 Procent czasu, jaki określony proces Zabbix lub grupa procesów (identyfikowana przez <type> i <mode>) spędziła w stanie <state>. Jest on obliczany tylko dla ostatniej minuty.
 Wartość zwracana: *Float*.

Parametry:

- **type** - dla procesów serwera: *agent poller*, *alert manager*, *alert syncer*, *alerter*, *availability manager*, *browser poller*, *configuration syncer*, *configuration syncer worker*, *connector manager*, *connector worker*, *discovery manager*, *discovery worker*, *escalator*, *ha manager*, *history poller*, *history syncer*, *housekeeper*, *http agent poller*, *http poller*, *icmp pinger*, *internal poller* *ipmi manager*, *ipmi poller*, *java poller*, *lld manager*, *lld worker*, *odbc poller*, *poller*, *preprocessing manager*, *preprocessing worker*, *proxy group manager*, *proxy poller*, *self-monitoring*, *service manager*, *snmp poller*, *snmp trapper*, *task manager*, *timer*, *trapper*, *trigger housekeeper*, *unreachable poller*, *vmware collector*;
dla procesów proxy: *agent poller*, *availability manager*, *browser poller*, *configuration syncer*, *data sender*, *discovery manager*, *discovery worker*, *history syncer*, *housekeeper*, *http agent poller*, *http poller*, *icmp pinger*, *internal poller ipmi manager*, *ipmi poller*, *java poller*, *odbc poller*, *poller*, *preprocessing manager*, *preprocessing worker*, *self-monitoring*, *snmp poller*, *snmp trapper*, *task manager*, *trapper*, *unreachable poller*, *vmware collector*;
- **mode** - *avg* - wartość średnia dla wszystkich procesów danego typu (domyślnie);
count - zwraca liczbę forków dla danego typu procesu, nie należy podawać <state>;
max - wartość maksymalna;
min - wartość minimalna;
<*process number*> - numer procesu (od 1 do liczby wstępnie utworzonych instancji; na przykład, jeśli uruchomione są 4 procesy trapper, wartość mieści się w zakresie od 1 do 4);
- **state** - *busy* - proces jest w stanie zajętości, na przykład przetwarza żądanie (domyślnie);
idle - proces jest w stanie bezczynności i nic nie robi.

Uwagi:

- Jeśli <mode> jest numerem procesu Zabbix, który nie jest uruchomiony (na przykład przy 5 uruchomionych pollerach dla <mode> podano 6), taka pozycja stanie się nieobsługiwana.
- Wartości minimalna i maksymalna odnoszą się do procentu wykorzystania pojedynczego procesu. Zatem jeśli w grupie 3 pollerów procenty wykorzystania dla poszczególnych procesów wynosiły 2, 18 i 66, *min* zwróci 2, a *max* zwróci 66.
- Procesy raportują, co robią, do pamięci współdzielonej, a proces self-monitoring podsumowuje te dane co sekundę. Zmiany stanu (busy/idle) są rejestrowane przy zmianie — dlatego proces, który staje się zajęty, rejestruje taki stan i nie zmienia ani nie aktualizuje stanu, dopóki nie stanie się bezczynny. Zapewnia to poprawne zarejestrowanie nawet całkowicie zawieszonych procesów jako 100% busy.
- Obecnie „busy" oznacza „nie śpi", ale w przyszłości mogą zostać wprowadzone dodatkowe stany — oczekiwanie na blokady, wykonywanie zapytań do bazy danych itd. Należy pamiętać, że asynchroniczne pollery są uznawane za busy, jeśli osiągnęły limit ustawiony przez parametr konfiguracyjny MaxConcurrentChecksPerPoller server/proxy.
- W systemie Linux i większości innych systemów rozdzielczość wynosi 1/100 sekundy.

Przykłady:

```
zabbix[process,poller,avg,busy] #średni czas, jaki procesy poller spędziły na wykonywaniu czegoś w ciągu c
zabbix[process,"icmp pinger",max,busy] #maksymalny czas spędzony na wykonywaniu czegoś przez dowolny proce
zabbix[process,"history syncer",2,busy] #czas spędzony na wykonywaniu czegoś przez proces history syncer n
zabbix[process,trapper,count] #liczba aktualnie uruchomionych procesów trapper
```

zabbix[proxy,<name>,<param>]

 Informacje o proxy Zabbix.
 Zwracana wartość: *Integer*.

Parametry:

- **name** - nazwa proxy;
- **param** - *lastaccess* - znacznik czasu ostatniej wiadomości heartbeat otrzymanej od proxy;
delay - jak długo zebrane wartości pozostają niewysłane; obliczane jako „opóźnienie proxy" + („bieżący czas serwera" - „proxy lastaccess"), gdzie „opóźnienie proxy" to różnica między bieżącym czasem proxy a znacznikiem czasu najstarszej niewysłanej wartości na proxy.

Uwagi:

- Ta pozycja jest zawsze przetwarzana przez serwer Zabbix niezależnie od lokalizacji hosta (na serwerze lub proxy).
- Funkcja `fuzzytime()` może być użyta do sprawdzenia dostępności proxy.

Przykład:

```
zabbix[proxy,"Germany",lastaccess] #znacznik czasu ostatniej wiadomości heartbeat otrzymanej od proxy "Ger
```

zabbix[proxy,discovery]

 Lista proxy Zabbix zawierająca nazwę, tryb, szyfrowanie, kompresję, wersję, czas ostatniego połączenia, liczbę hostów, liczbę pozycji, wymaganą liczbę wartości na sekundę (vps), status wersji (aktualna/przestarzała/niewspierana), limity czasu według typu pozycji, nazwę grupy proxy (jeśli proxy należy do grupy), stan (nieznany/offline/online).
 Wartość zwracana: *obiekt JSON*.

zabbix[proxy group,<name>,available]

 Liczba proxy online w grupie proxy.
 Wartość zwracana: *Integer*.

Parametry:

- **name** - nazwa grupy proxy.

zabbix[proxy group,<name>,pavailable]

 Procent proxy online w grupie proxy.
 Zwracana wartość: *Float*.

Parametry:

- **name** — nazwa grupy proxy.

zabbix[proxy group,<name>,proxies]

 Lista proxy Zabbix w grupie proxy z nazwą, trybem, szyfrowaniem, kompresją, wersją, czasem ostatniej aktywności, liczbą hostów, liczbą pozycji, wymaganą liczbą wartości na sekundę (vps), statusem wersji (current/outdated/unsupported), limitami czasu, nazwą grupy proxy, stanem (unknown/offline/online).
 Zwracana wartość: *JSON*.

Parametry:

- **name** - nazwa grupy proxy.

zabbix[proxy group,<name>,state]

 Stan grupy proxy.
 Zwracana wartość: *0* - nieznany; *1* - offline; *2* - odzyskiwanie; *3* - online; *4* - pogarszanie się.

Parametry:

- **name** - nazwa grupy proxy.

zabbix[proxy group,discovery]

 Zwraca listę grup proxy z danymi konfiguracyjnymi i danymi czasu rzeczywistego. Dane konfiguracyjne obejmują nazwę grupy proxy, opóźnienie przełączenia awaryjnego oraz minimalną wymaganą liczbę proxy online. Dane czasu rzeczywistego obejmują stan grupy proxy (szczegóły w komentarzach), liczbę proxy online oraz procent proxy online.
 Wartość zwracana: *JSON*.

Komentarze:

- Ta pozycja nie zwraca proxy nienależących do żadnej grupy.
- Jeśli dla ”failover_delay” lub ”min_online” występuje nieprawidłowa wartość, zgłaszana jest specjalna wartość *-1*, aby to zasygnalizować. Nieprawidłowe wartości mogą wystąpić, jeśli do konfiguracji używane są makra i nie można ich rozwinąć do prawidłowej wartości.
- Stan grupy proxy jest raportowany jako liczba całkowita: *0* - nieznany; *1* - offline; *2* - odzyskiwanie; *3* - online; *4* - pogarszanie.

Przykład wartości zwracanych:

```
{
    "groups": [
       { "name": "Riga", "failover_delay": 60, "min_online": 1 },
       { "name": "Tokyo", "failover_delay": 60, "min_online": 2 },
       { "name": "Porto Alegre", "failover_delay": 60, "min_online": 3 }
    ],
    "details": {
        "Riga": { "state": 3, "available": 10, "pavailable": 20 },
        "Tokyo": { "state": 3, "available": 10, "pavailable": 20 },
        "Porto Alegre": { "state": 1, "available": 0, "pavailable": 0 }
    }
}
```

zabbix[proxy_buffer,buffer,<mode>]

 Statystyki użycia bufora pamięci proxy.
 Zwracane wartości: *Integer* (dla rozmiaru); *Float* (dla wartości procentowej).

Parametry:

- **mode**: *total* - całkowity rozmiar bufora (może być używany do sprawdzenia, czy bufor pamięci jest włączony);
free - rozmiar wolnego bufora;
pfree - procent wolnego bufora;
used - rozmiar używanego bufora;
pused - procent używanego bufora.

Uwagi:

- Zwraca błąd „Proxy memory buffer is disabled”, gdy bufor pamięci jest wyłączony;
- Ta pozycja nie jest obsługiwana na serwerze Zabbix.

zabbix[proxy_buffer,state,changes]

 Zwraca liczbę zmian stanu między trybami bufora dysk/pamięć od momentu uruchomienia.
 Zwracane wartości: *Integer*; *0* - bufor pamięci jest wyłączony.

Uwagi:

- Częste zmiany stanu wskazują, że należy zwiększyć rozmiar lub wiek bufora pamięci.
- Jeśli stan bufora pamięci jest monitorowany rzadko (na przykład raz na minutę), bufor może zmienić swój stan bez zarejestrowania tego faktu.

zabbix[proxy_buffer,state,current]

 Zwraca bieżący stan roboczy, w którym przechowywane są nowe dane.
 Zwracane wartości: *0* - dysk; *1* - pamięć.

Uwagi:

- „0” jest również zwracane, gdy bufor pamięci jest wyłączony.

zabbix[proxy_history]

 Liczba wartości w tabeli historii proxy oczekujących na wysłanie do serwer.
 Zwracane wartości: *Integer*.

Komentarze:

- Ta pozycja nie jest obsługiwana na serwerze Zabbix.

zabbix[queue,<from>,<to>]

 Liczba monitorowanych pozycji w kolejce, które są opóźnione co najmniej o <from> sekund, ale mniej niż o <to> sekund.
 Zwracana wartość: *Integer*.

Parametry:

- **from** — opóźnienie co najmniej o (domyślnie 6 sekund);
- **to** — opóźnienie co najwyżej o (domyślnie nieskończoność).

Uwagi:

- Sufiksy czasu (s,m,h,d,w) są obsługiwane w parametrach.

> **Attention:**
> Proxy Zabbix nie uwzględnia okresów konserwacji; szczegóły znajdują się w sekcji Obliczanie kolejek podczas konserwacji.

zabbix[rcache,<cache>,<mode>]

 Statystyki dostępności pamięci podręcznej konfiguracji Zabbix.
 Zwracane wartości: *Integer* (dla rozmiaru); *Float* (dla wartości procentowej).

Parametry:

- **cache** - *buffer*;
- **mode** - *total* - całkowity rozmiar bufora;
free - rozmiar wolnego bufora;
pfree - procent wolnego bufora;
used - rozmiar używanego bufora;
pused - procent używanego bufora.

zabbix[requiredperformance]

 Wymagana wydajność serwera Zabbix lub proxy Zabbix, wyrażona jako oczekiwana liczba nowych wartości na sekundę.
 Zwracana wartość: *Float*.

Komentarze:

- W przybliżeniu odpowiada „Required server performance, new values per second” w *Raporty* > *Informacje o systemie*.

zabbix[stats,<ip>,<port>]

 Zwraca wewnętrzne metryki serwera lub proxy Zabbix. Jeśli określono <ip> i <port>, metryki są pobierane ze zdalnej instancji; w przeciwnym razie z instancji lokalnej.
 Zwracane wartości: *obiekt JSON*.

Parametry:

- **ip** — lista IP/DNS/masek sieciowych serwerów/proxy, które mają być odpytywane zdalnie (domyślnie 127.0.0.1);
- **port** — port serwera/proxy, który ma być odpytywany zdalnie (domyślnie 10051).

Uwagi:

- Żądanie statystyk będzie akceptowane tylko z adresów wymienionych w parametrze 'StatsAllowedIP' server/proxy na instancji docelowej.
- Ta pozycja zwraca wybrany zestaw wewnętrznych metryk. Szczegóły znajdują się w Zdalne monitorowanie statystyk Zabbix.

zabbix[stats,<ip>,<port>,queue,<from>,<to>]

 Zwraca metryki wewnętrznej kolejki (zob. `zabbix[queue,<from>,<to>]`) serwera lub proxy Zabbix. Jeśli określono <ip> i <port>, metryki są pobierane ze zdalnej instancji; w przeciwnym razie z instancji lokalnej.
 Wartości zwracane: *obiekt JSON*.

Parametry:

- **ip** - lista IP/DNS/masek sieciowych serwerów/proxy, które mają być odpytywane zdalnie (domyślnie 127.0.0.1);
- **port** - port serwera/proxy, który ma być odpytywany zdalnie (domyślnie 10051);
- **from** - opóźnienie co najmniej o (domyślnie 6 sekund);
- **to** - opóźnienie co najwyżej o (domyślnie nieskończoność).

Komentarze:

- Żądanie statystyk będzie akceptowane wyłącznie z adresów wymienionych w parametrze 'StatsAllowedIP' instancji docelowej server/proxy.
- Wybrany zestaw metryk wewnętrznych jest zwracany przez tę pozycję. Szczegóły znajdują się w Zdalne monitorowanie statystyk Zabbix.

Attention:
Proxy Zabbix nie uwzględnia okresów konserwacji; szczegóły znajdują się w sekcji Obliczanie kolejek podczas konserwacji.

zabbix[tcache,cache,<parameter>]

 Statystyki efektywności pamięci podręcznej funkcji trendów Zabbix.
 Zwracane wartości: *Integer* (dla rozmiaru); *Float* (dla wartości procentowej).

Parametry:

- **parameter** - *all* - łączna liczba żądań do pamięci podręcznej (domyślnie);
hits - trafienia pamięci podręcznej;
phits - procent trafień pamięci podręcznej;
misses - chybienia pamięci podręcznej;
pmisses - procent chybień pamięci podręcznej;
items - liczba elementów w pamięci podręcznej;
requests - liczba żądań w pamięci podręcznej;
pitems - procent elementów w pamięci podręcznej względem sumy elementów i żądań w pamięci podręcznej. Niski procent najprawdopodobniej oznacza, że rozmiar pamięci podręcznej można zmniejszyć.

Uwagi:

- Ta pozycja nie jest obsługiwana przez Zabbix proxy.

zabbix[triggers]

 Liczba włączonych wyzwalaczy w bazie danych Zabbix, ze wszystkimi pozycjami włączonymi na włączonych hostach.
 Zwracana wartość: *Integer*.

Komentarze:

- Ta pozycja nie jest obsługiwana przez Zabbix proxy.

zabbix[uptime]

 Czas działania procesu serwera lub proxy Zabbix w sekundach.
 Zwracana wartość: *Integer*.

zabbix[vcache,buffer,<mode>]

 Statystyki dostępności pamięci podręcznej wartości Zabbix.
 Zwracane wartości: *Integer* (dla rozmiaru); *Float* (dla wartości procentowej).

Parametry:

- **mode** - *total* - całkowity rozmiar bufora;
free - rozmiar wolnego bufora;
pfree - procent wolnego bufora;
used - rozmiar używanego bufora;
pused - procent używanego bufora.

Uwagi:

- Ta pozycja nie jest obsługiwana przez Zabbix proxy.

zabbix[vcache,cache,<parameter>]

 Statystyki efektywności pamięci podręcznej wartości Zabbix.
 Zwracana wartość: *Integer*. Jeśli <parameter> jest ustawiony na *mode*, zwracana wartość to: *0* - tryb normalny; *1* - tryb niskiej pamięci.

Parametry:

- **parameter** - *requests* - całkowita liczba żądań;
hits - liczba trafień pamięci podręcznej (wartości historii pobrane z pamięci podręcznej);
misses - liczba chybień pamięci podręcznej (wartości historii pobrane z bazy danych);
mode - tryb działania pamięci podręcznej wartości.

Uwagi:

- Po włączeniu trybu niskiej pamięci pamięć podręczna wartości pozostanie w tym stanie przez 24 godziny, nawet jeśli problem, który wyzwolił ten tryb, zostanie rozwiązany wcześniej.
- Możesz użyć tego klucza z krokiem przetwarzania wstępnego *Change per second*, aby uzyskać statystyki wartości na sekundę.
- Ta pozycja nie jest obsługiwana przez Zabbix proxy.

zabbixversion

 Wersja serwera lub proxy Zabbix.
 Zwracana wartość: *String*. Na przykład: `8.0.0`.

zabbix[vmware,buffer,<mode>]

 Statystyki dostępności pamięci podręcznej vmware Zabbix.
 Zwracane wartości: *Integer* (dla rozmiaru); *Float* (dla wartości procentowej).

Parametry:

- **mode** - *total* - całkowity rozmiar bufora;
free - rozmiar wolnego bufora;
pfree - procent wolnego bufora;
used - rozmiar używanego bufora;
pused - procent używanego bufora.

zabbix[vps,written]

 Łączna liczba wartości historii zapisanych do bazy danych.
 Zwracana wartość: *Integer*.

zabbix[wcache,<cache>,<mode>]

 Statystyki i dostępność pamięci podręcznej zapisu Zabbix.
 Zwracane wartości: *Integer* (dla liczby/rozmiaru); *Float* (dla wartości procentowej).

Parametry:

- **cache** - *values*, *history*, *index* lub *trend*;
- **mode** - (z *values*) *all* (domyślnie) - całkowita liczba wartości przetworzonych przez serwer/proxy Zabbix, z wyjątkiem nieobsługiwanych pozycji (licznik);
float - liczba przetworzonych wartości zmiennoprzecinkowych (licznik);
uint - liczba przetworzonych wartości typu unsigned integer (licznik);
str - liczba przetworzonych wartości znakowych/łańcuchowych (licznik);
log - liczba przetworzonych wartości logów (licznik);
text - liczba przetworzonych wartości tekstowych (licznik);
bin - liczba przetworzonych wartości binarnych (licznik);
json - liczba przetworzonych wartości JSON (licznik);
not supported - liczba przypadków, gdy przetwarzanie pozycji spowodowało przejście pozycji do stanu nieobsługiwanego lub utrzymanie tego stanu (licznik);
(z pamięcią podręczną *history*, *index*, *trend*) *pfree* (domyślnie) - procent wolnego bufora;
total - całkowity rozmiar bufora;
free - rozmiar wolnego bufora;
used - rozmiar używanego bufora;
pused - procent używanego bufora.

Uwagi:

- Parametr pamięci podręcznej `trend` nie jest obsługiwany przez Zabbix proxy.
- Pamięć podręczna historii jest używana do przechowywania wartości pozycji. Niska wartość wskazuje na problemy z wydajnością po stronie bazy danych.
- Pamięć podręczna indeksu historii jest używana do indeksowania wartości przechowywanych w pamięci podręcznej historii.
- Po zapełnieniu, a następnie wyczyszczeniu pamięci podręcznej historii, pamięć podręczna indeksu historii nadal będzie przechowywać część danych. Takie zachowanie jest oczekiwane i pomaga systemowi działać wydajniej, ponieważ pozwala uniknąć dodatkowego przetwarzania wymaganego do ciągłej zmiany rozmiaru pamięci.
- Pamięć podręczna trendów przechowuje agregaty dla bieżącej godziny dla wszystkich pozycji, które otrzymują dane.
- Możesz użyć klucza zabbix[wcache,values] wraz z krokiem preprocessing *Change per second*, aby uzyskać statystyki wartości na sekundę.

9 Kontrole SSH

Przegląd

Kontrole SSH są wykonywane jako monitorowanie bezagentowe. Agent Zabbix nie jest wymagany do kontroli SSH.

Aby wykonywać kontrole SSH, serwer Zabbix musi być wcześniej skonfigurowany z obsługą SSH2 (libssh lub libssh2). Zobacz także: Wymagania.

Attention:
Począwszy od RHEL 8, obsługiwany jest tylko libssh. W przypadku innych dystrybucji zalecane jest używanie libssh zamiast libssh2.

Konfiguracja

Uwierzytelnianie za pomocą hasła

Kontrole SSH udostępniają dwie metody uwierzytelniania — parę użytkownik/hasło oraz metodę opartą na pliku klucza.

Jeśli nie zamierzasz używać kluczy, nie jest wymagana żadna dodatkowa konfiguracja, poza podlinkowaniem biblioteki libssh lub libssh2 do Zabbix, jeśli kompilujesz ze źródeł.

Uwierzytelnianie za pomocą pliku klucza

Aby używać uwierzytelniania opartego na kluczach dla pozycji SSH, wymagane są określone zmiany w konfiguracji serwera.

Otwórz plik konfiguracyjny serwera Zabbix (*zabbix_server.conf*) jako `root` i znajdź następującą linię:

```
##### SSHKeyLocation=
```

Odkomentuj ją i ustaw pełną ścieżkę do katalogu, w którym będą znajdować się klucze publiczny i prywatny:

```
SSHKeyLocation=/home/zabbix/.ssh
```

Zapisz plik, a następnie uruchom ponownie serwer Zabbix.

Ścieżka */home/zabbix* oznacza tutaj katalog domowy konta użytkownika *zabbix*, a *.ssh* to katalog, w którym domyślnie klucze publiczny i prywatny zostaną wygenerowane przez polecenie ssh-keygen wewnątrz katalogu domowego.

Zazwyczaj pakiety instalacyjne serwera Zabbix z różnych dystrybucji systemów operacyjnych tworzą konto użytkownika *zabbix* z katalogiem domowym w innej lokalizacji, na przykład */var/lib/zabbix* (jak w przypadku kont systemowych).

Przed wygenerowaniem kluczy możesz przenieść katalog domowy do */home/zabbix*, aby odpowiadał parametrowi konfiguracyjnemu serwera Zabbix `SSHKeyLocation`, wspomnianemu powyżej.

Note:
Poniższe kroki można pominąć, jeśli konto *zabbix* zostało dodane ręcznie zgodnie z sekcją instalacji. W takim przypadku katalog domowy konta *zabbix* najprawdopodobniej już znajduje się w */home/zabbix*.

Aby zmienić katalog domowy konta użytkownika *zabbix*, należy zatrzymać wszystkie procesy robocze, które go używają:

```
systemctl stop zabbix-agent
systemctl stop zabbix-server
```

Aby zmienić lokalizację katalogu domowego z próbą jego przeniesienia (jeśli istnieje), należy wykonać następujące polecenie:

```
usermod -m -d /home/zabbix zabbix
```

Możliwe jest również, że katalog domowy nie istniał w starej lokalizacji, więc należy go utworzyć w nowej lokalizacji. Bezpieczna próba wykonania tego wygląda następująco:

```
test -d /home/zabbix || mkdir /home/zabbix
```

Aby mieć pewność, że wszystko jest odpowiednio zabezpieczone, można dodatkowo wykonać polecenia ustawiające uprawnienia do katalogu domowego:

```
chown zabbix:zabbix /home/zabbix
chmod 700 /home/zabbix
```

Wcześniej zatrzymane procesy można teraz ponownie uruchomić:

```
systemctl start zabbix-agent
systemctl start zabbix-server
```

Teraz można wykonać kroki generowania kluczy publicznego i prywatnego za pomocą następujących poleceń (dla lepszej czytelności znaki zachęty powłoki zostały zakomentowane):

```
sudo -u zabbix ssh-keygen -t rsa
##### Generating public/private rsa key pair.
##### Enter file in which to save the key (/home/zabbix/.ssh/id_rsa):
/home/zabbix/.ssh/id_rsa
##### Enter passphrase (empty for no passphrase):
<Leave empty>
##### Enter same passphrase again:
<Leave empty>
##### Your identification has been saved in /home/zabbix/.ssh/id_rsa.
##### Your public key has been saved in /home/zabbix/.ssh/id_rsa.pub.
##### The key fingerprint is:
##### 90:af:e4:c7:e3:f0:2e:5a:8d:ab:48:a2:0c:92:30:b9 zabbix@it0
##### The key's randomart image is:
##### +--[ RSA 2048]----+
##### |                 |
##### |        .        |
##### |      o          |
##### | .     o         |
##### |+     . S        |
##### |.+   o =         |
##### |E .   * =        |
##### |=o . ..* .       |
##### |... oo.o+        |
##### +-----------------+
```

Note:
Klucze publiczny i prywatny (*id_rsa.pub* oraz *id_rsa*) zostały domyślnie wygenerowane w katalogu */home/zabbix/.ssh*, co odpowiada parametrowi konfiguracyjnemu serwera Zabbix `SSHKeyLocation`.

Attention:
Typy kluczy inne niż ”rsa” mogą być obsługiwane przez narzędzie ssh-keygen i serwery SSH, ale mogą nie być obsługiwane przez libssh2 używane przez Zabbix.

Formularz konfiguracji powłoki

Ten krok należy wykonać tylko raz dla każdego hosta, który będzie monitorowany za pomocą kontroli SSH.

Korzystając z poniższych poleceń, plik klucza **publicznego** można zainstalować na zdalnym hoście *10.10.10.10*, tak aby kontrole SSH mogły być wykonywane przy użyciu konta *root* (dla lepszej czytelności znaki zachęty wiersza poleceń zostały zakomentowane):

```
sudo -u zabbix ssh-copy-id root@10.10.10.10
##### The authenticity of host '10.10.10.10 (10.10.10.10)' can't be established.
##### RSA key fingerprint is 38:ba:f2:a4:b5:d9:8f:52:00:09:f7:1f:75:cc:0b:46.
##### Are you sure you want to continue connecting (yes/no)?
yes
##### Warning: Permanently added '10.10.10.10' (RSA) to the list of known hosts.
##### root@10.10.10.10's password:
<Enter root password>
##### Now try logging into the machine, with "ssh 'root@10.10.10.10'",
##### and check to make sure that only the key(s) you wanted were added.
```

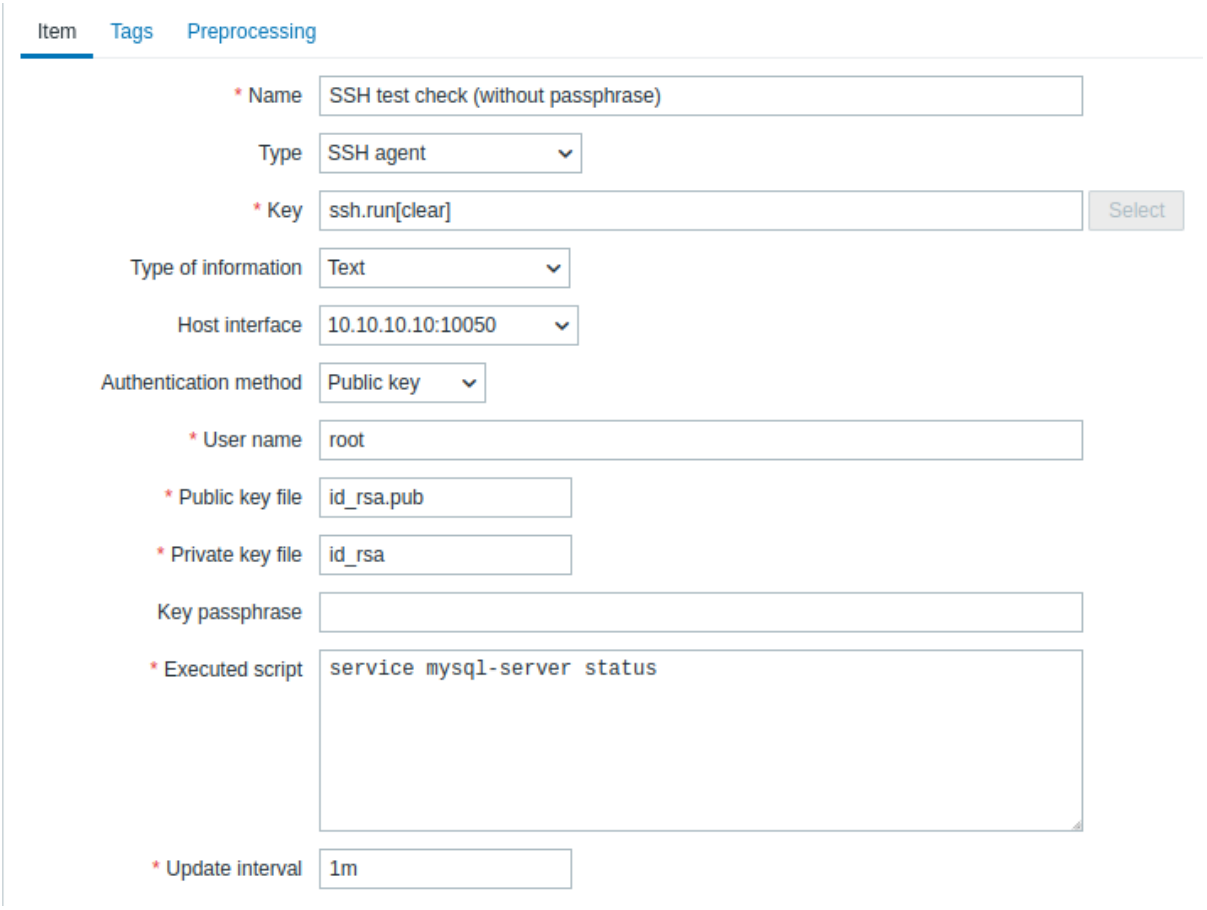
Teraz można sprawdzić logowanie SSH przy użyciu domyślnego klucza prywatnego (*/home/zabbix/.ssh/id_rsa*) dla konta użytkownika *zabbix*:

```
sudo -u zabbix ssh root@10.10.10.10
```

Jeśli logowanie powiedzie się, część konfiguracyjna w powłoce jest zakończona i zdalną sesję SSH można zamknąć.

Konfiguracja pozycji

Rzeczywiste polecenie(-a) do wykonania należy umieścić w polu *Executed script* w konfiguracji pozycji. Wiele poleceń można wykonać jedno po drugim, umieszczając je w nowej linii. W takim przypadku zwracane wartości również będą sformatowane jako wielowierszowe.



Wszystkie obowiązkowe pola wejściowe są oznaczone czerwoną gwiazdką.

Pola wymagające określonych informacji dla pozycji SSH to:

Parameter	Description	Comments
Type	Wybierz tutaj **SSH agent**.	

Parameter	Description	Comments

Key	Unikalny (dla każdego hosta) klucz pozycji w formacie **ssh.run[unikalny krótki opis,<ip>,<port>,<encoding>,<ssh options>,<subsystem>]**	**unikalny krótki opis** jest wymagany i powinien być unikalny dla każdej pozycji SSH na danym hoście.
		
		Domyślny port to 22, a nie port określony w interfejsie, do którego przypisana jest ta pozycja.
		
		ssh options umożliwia przekazanie dodatkowych opcji SSH w formacie *key1=value1;key2=value2,value3*. Wiele wartości dla jednego klucza można przekazać, oddzielając je przecinkiem (w takim przypadku parametr musi być quoted); wiele kluczy opcji można przekazać, oddzielając je średnikiem.
		
		Obsługiwane są następujące klucze opcji: `KexAlgorithms`, `HostkeyAlgorithms`, `Ciphers`, `MACs`, `PubkeyAcceptedKeyTypes`. Obsługa klucza opcji i wartości zależy od biblioteki SSH (na przykład `PubkeyAcceptedKeyTypes` jest obsługiwane tylko z libssh); jeśli opcja nie jest obsługiwana, zostanie zwrócony błąd, a pozycja stanie się nieobsługiwana.
		
		Należy pamiętać, że znak "+" do dołączania ustawień szyfrów oraz "!" do wyłączania określonych ustawień szyfrów (jak w GnuTLS i OpenSSL) nie są obsługiwane.
		
		Przykłady:
		=>
		`ssh.run[KexAlgorithms,127.0.0.1,,,Ciphers=aes128`
		=>
		`ssh.run[KexAlgorithms,,,,"KexAlgorithms=diffie-h`
		=>
		`ssh.run[PubkeyAcceptedKeyTypes,127.0.0.1,,,Pubke`
		
		subsystem umożliwia przekazanie podsystemu SSH, ograniczając połączenie SSH do określonych operacji dozwolonych przez podsystem (np. transfer plików przy użyciu SFTP lub zarządzanie urządzeniami sieciowymi przy użyciu NETCONF). Należy pamiętać, że użycie podsystemu może również wymagać zastosowania określonej składni skryptu w parametrze *Executed script*.
		
		Przykłady:
		=>
		`ssh.run[SFTPBackup,192.0.2.18,,,,sftp]`
		=>
		`ssh.run[Cisco1234,192.0.2.18,,,,netconf]`

Authentication method	Jedna z metod: "Password" lub "Public key".	
User name	Nazwa użytkownika (do 255 znaków) do uwierzytelniania na zdalnym hoście. Wymagane.	
Public key file	Nazwa pliku klucza publicznego, jeśli *Authentication method* to "Public key". Wymagane.	Przykład: *id_rsa.pub* - domyślna nazwa pliku klucza publicznego generowanego przez polecenie ssh-keygen.
Private key file	Nazwa pliku klucza prywatnego, jeśli *Authentication method* to "Public key". Wymagane.	Przykład: *id_rsa* - domyślna nazwa pliku klucza prywatnego.

Parameter	Description	Comments
Password or *Key passphrase*	Hasło (do 255 znaków) do uwierzytelniania lub Hasło klucza **jeśli** zostało użyte dla klucza prywatnego.	Pozostaw pole *Key passphrase* puste, jeśli hasło klucza nie było używane. Zobacz także known issues dotyczące użycia hasła klucza.

Executed script	Wykonywane polecenie(-a) powłoki przy użyciu zdalnej sesji SSH.	Wartość zwracana przez wykonywane polecenie(-a) powłoki jest ograniczona do 16MB (wliczając końcowe białe znaki, które są obcinane); obowiązują również database limits.
		
		Należy pamiętać, że biblioteka libssh2 może obcinać wykonywalne skrypty do ~32kB.
		
		Przykłady:
		`date +%s`
		`systemctl status mysql-server`
		`ps auxww | grep httpd | wc -l`
		
		Przykład (dla podsystemu NETCONF):
		`<rpc>`
		`<get-software-information/>`
		`</rpc>`
		`]]>]]>`
		`<rpc>`
		`<close-session/>`
		`</rpc>`
		`]]>]]>`

10 Kontrole Telnet

Przegląd

Kontrole Telnet są wykonywane jako monitorowanie bez agent. Zabbix agent nie jest wymagany do kontroli Telnet.

Konfigurowalne pola

Rzeczywiste polecenie(-a) do wykonania należy umieścić w polu **Executed script** w konfiguracji pozycji.
Wiele poleceń można wykonać jedno po drugim, umieszczając je w nowej linii. W takim przypadku zwracana wartość również będzie sformatowana jako wielowierszowa.

Obsługiwane znaki, którymi może kończyć się znak zachęty powłoki:

- $
- #
- >
- %

Note:
Linia znaku zachęty telnet zakończona jednym z tych znaków zostanie usunięta ze zwracanej wartości, ale tylko dla pierwszego polecenia na liście poleceń, tj. tylko na początku sesji telnet.

Key	Description
telnet.run[<unique short description>,<ip>,<port>,<encoding>]	Uruchamia polecenie na zdalnym urządzeniu przy użyciu połączenia telnet

Attention:
Jeśli sprawdzenie telnet zwraca wartość zawierającą znaki spoza ASCII i w kodowaniu innym niż UTF8, wówczas parametr *<encoding>* klucza powinien zostać odpowiednio określony. Więcej informacji można znaleźć na stronie encoding of returned values.

11 Kontrole zewnętrzne

Przegląd

Sprawdzenie zewnętrzne to sprawdzenie wykonywane przez serwer Zabbix poprzez uruchomienie skryptu powłoki lub pliku binarnego. Jednak gdy hosty są monitorowane przez proxy Zabbix, sprawdzenia zewnętrzne są wykonywane przez proxy.

Sprawdzenia zewnętrzne nie wymagają uruchomionego agenta na monitorowanym hoście.

Składnia klucza pozycji jest następująca:

```
script[<parameter1>,<parameter2>,...]
```

Gdzie:

ARGUMENT	DEFINITION
script	Nazwa skryptu powłoki lub pliku binarnego.
parameter(s)	Opcjonalne parametry wiersza poleceń.

Jeśli nie chcesz przekazywać żadnych parametrów do skryptu, możesz użyć:

```
script[] or
script
```

serwer Zabbix lub proxy wyszuka katalog określony dla skryptów zewnętrznych i wykona polecenie (zobacz parametr `ExternalScripts` w pliku konfiguracyjnym Zabbix server/proxy). Polecenie zostanie wykonane z uprawnieniami tego samego użytkownika co serwer/proxy Zabbix, dlatego wszelkie uprawnienia dostępu lub zmienne środowiskowe powinny być w razie potrzeby obsłużone w skrypcie opakowującym. Uprawnienia do polecenia również muszą pozwalać temu użytkownikowi na jego wykonanie. Do wykonania dostępne są tylko polecenia znajdujące się w określonym katalogu.

Warning:
Nie należy nadużywać sprawdzeń zewnętrznych, ponieważ każdy skrypt wymaga uruchomienia procesu fork przez serwer/proxy Zabbix, a uruchamianie wielu skryptów może znacząco obniżyć wydajność Zabbix.

Przykład użycia

Wykonanie skryptu **check_oracle.sh** z pierwszym parametrem '-h'. Drugi parametr zostanie zastąpiony adresem IP lub nazwą DNS, w zależności od wyboru we właściwościach hosta.

```
check_oracle.sh["-h","{HOST.CONN}"]
```

Zakładając, że host jest skonfigurowany do używania adresu IP, serwer/proxy Zabbix wykona:

```
check_oracle.sh '-h' '192.168.1.4'
```

Wynik kontroli zewnętrznej

Wartością zwracaną kontroli zewnętrznej jest standardowe wyjście wraz ze standardowym wyjściem błędów generowanym przez kontrolę.

Attention:
Pozycja zwracająca tekst (informacja typu znakowego, log lub tekst) nie stanie się nieobsługiwana w przypadku standardowego wyjścia błędów.

Wartość zwracana jest ograniczona do 16 MB (włącznie z końcowymi białymi znakami, które są obcinane); obowiązują również ograniczenia bazy danych.

Jeśli żądany skrypt nie zostanie znaleziony lub serwer/proxy Zabbix nie ma uprawnień do jego wykonania, pozycja stanie się nieobsługiwana i zostanie wyświetlony odpowiedni komunikat o błędzie.

W przypadku przekroczenia limitu czasu pozycja stanie się nieobsługiwana, zostanie wyświetlony odpowiedni komunikat o błędzie, a proces utworzony dla skryptu zostanie zakończony.

12 Pozycje trapper

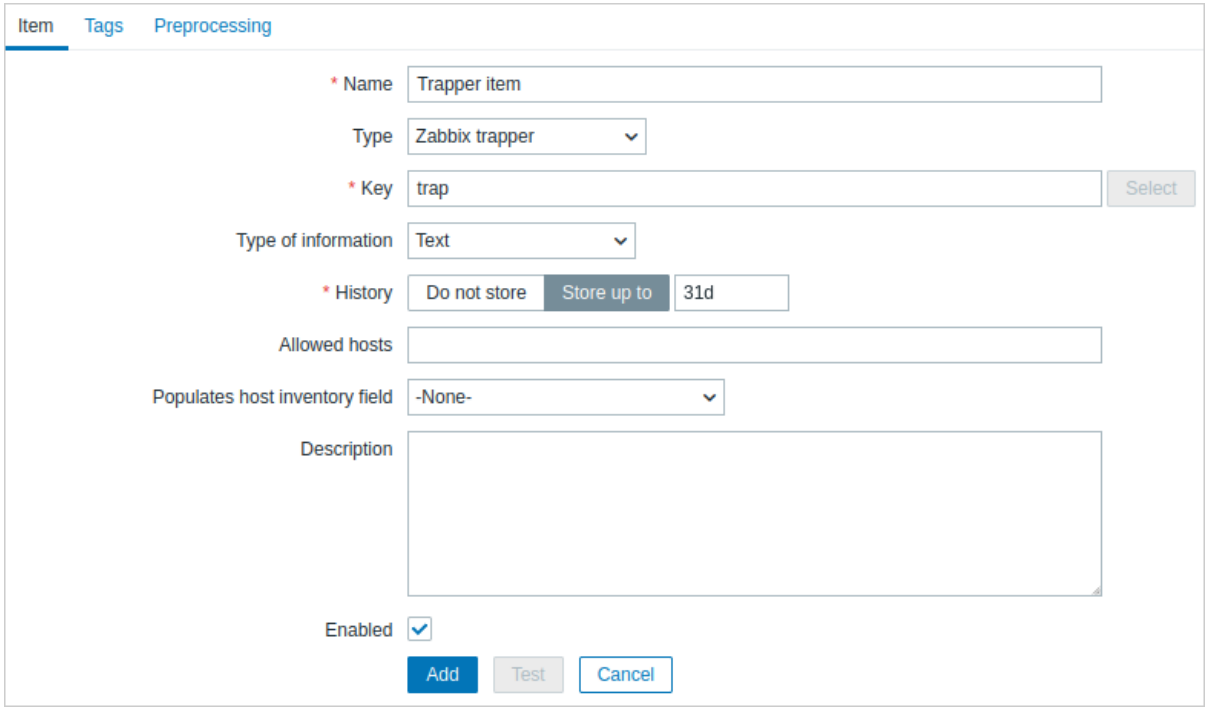
Przegląd

Pozycje trapper akceptują dane przychodzące zamiast je odpytywać. Jest to przydatne w przypadku wszelkich danych, które chcesz wysyłać do Zabbix.

Konfiguracja

Aby skonfigurować pozycję trapper:

1. Przejdź do *Data collection* → *Hosts*.
2. Kliknij *Items* w wierszu hosta.
3. Kliknij *Create item*.
4. Wprowadź parametry pozycji w formularzu konfiguracji.



Wszystkie wymagane pola wejściowe są oznaczone czerwoną gwiazdką.

Pola wymagające podania określonych informacji dla pozycji trapper to:

Type	Wybierz „Zabbix trapper”.
Key	Wprowadź klucz, który będzie używany do rozpoznawania pozycji podczas wysyłania danych do serwera Zabbix.
Type of information	Wybierz typ informacji, który będzie odpowiadał formatowi wysyłanych danych.
Allowed hosts	Lista adresów IP rozdzielonych przecinkami (opcjonalnie w notacji CIDR) lub nazw DNS. Jeśli parametr jest określony, połączenia przychodzące będą akceptowane tylko od hostów wymienionych tutaj. Jeśli obsługa IPv6 jest włączona, wtedy „127.0.0.1”, „::127.0.0.1”, „::ffff:127.0.0.1” są traktowane jednakowo, a „::/0” pozwoli na dowolny adres IPv4 lub IPv6. „0.0.0.0/0” może być użyte do zezwolenia na dowolny adres IPv4. Zwróć uwagę, że „adresy IPv6 zgodne z IPv4” (prefiks 0000::/96) są obsługiwane, ale ich użycie jest odradzane przez RFC4291. Przykład: 127.0.0.1, 192.168.1.0/24, 192.168.3.1-255, 192.168.1-10.1-255, ::1,2001:db8::/32, mysqlserver1, zabbix.example.com, {HOST.HOST} Obsługiwane są spacje, makra użytkownika oraz makra hosta {HOST.HOST}, {HOST.NAME}, {HOST.IP}, {HOST.DNS}, {HOST.CONN}.

Note:
Przed wysłaniem wartości może być konieczne odczekanie do 60 sekund po zapisaniu pozycji, aż serwer Zabbix uwzględni zmiany po aktualizacji pamięci podręcznej konfiguracji.

Wysyłanie danych

Wysyłanie danych do serwera lub proxy Zabbix jest możliwe przy użyciu narzędzia Zabbix sender lub protokołu Zabbix sender. Wysyłanie danych do serwera Zabbix jest również możliwe przy użyciu metody API `history.push`.

Zabbix sender

Aby wysłać dane do serwera lub proxy Zabbix przy użyciu narzędzia Zabbix sender, możesz uruchomić następujące polecenie, aby wysłać „wartość testową”:

```
zabbix_sender -z <server IP address> -p 10051 -s "New host" -k trap -o "test value"
```

Aby wysłać „wartość testową”, używane są następujące opcje polecenia:

- `-z` — określa adres IP serwera Zabbix
- `-p` — określa numer portu serwera Zabbix (domyślnie 10051)
- `-s` — określa hosta (upewnij się, że używasz technicznej, a nie widocznej nazwy hosta)
- `-k` — określa klucz pozycji skonfigurowanej w pozycji trapper
- `-o` — określa wartość do wysłania

Attention:
Proces Zabbix trapper nie rozwija makr użytych w kluczu pozycji podczas sprawdzania istnienia odpowiedniego klucza pozycji dla docelowego hosta.

Więcej informacji o komunikacji między Zabbix sender a serwerem lub proxy Zabbix można znaleźć w sekcji *protokół Zabbix sender*.

history.push

Aby wysłać dane do serwera Zabbix za pomocą metody API `history.push`, można wykonać następujące żądanie HTTP POST zawierające przykładowe wartości testowe:

```
curl --request POST \
  --url 'https://example.com/zabbix/api_jsonrpc.php' \
  --header 'Authorization: Bearer 0424bd59b807674191e7d77572075f33' \
  --header 'Content-Type: application/json-rpc' \
  --data '{"jsonrpc":"2.0","method":"history.push","params":[{"itemid":10600,"value":"test value 1"},{"ite
```

Jeśli żądanie jest poprawne, odpowiedź zwrócona przez API może wyglądać następująco:

```
{
    "jsonrpc": "2.0",
    "result": {
        "response": "success",
        "data": [
            {
                "itemid": "10600"
            },
            {
                "itemid": "10601",
                "error": "Item is disabled."
            },
            {
                "error": "No permissions to referred object or it does not exist."
            }
        ]
    },
    "id": 1
}
```

Błędy w danych odpowiedzi wskazują, że wysyłanie danych dla określonych pozycji nie przeszło walidacji przez serwer Zabbix. Może się tak zdarzyć z następujących powodów:

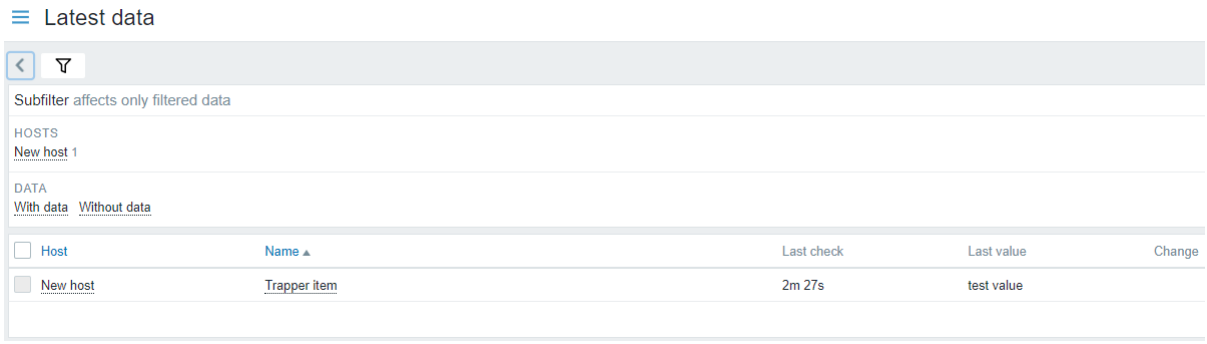
- użytkownik wysyłający dane nie ma uprawnień *read* do hosta danej pozycji;
- host jest wyłączony lub znajduje się w trybie maintenance bez zbierania danych;
- pozycja nie istnieje lub nie została jeszcze uwzględniona w pamięci podręcznej konfiguracji serwera;
- pozycja jest wyłączona lub jej typ jest inny niż Zabbix trapper lub HTTP agent (z włączonym trappingiem);
- adres IP lub DNS użytkownika nie jest ustawiony na liście *Allowed hosts* pozycji;
- inna pozycja ma wartość z duplikującym się znacznikiem czasu na poziomie nanosekund.

Brak błędów oznacza, że wysłane wartości zostały przyjęte do przetwarzania, które obejmuje preprocessing (jeśli występuje), przetwarzanie wyzwalaczy oraz zapis do bazy danych. Należy pamiętać, że przetwarzanie przyjętej wartości również może się nie powieść (na przykład podczas preprocessing), co spowoduje odrzucenie wartości.

Więcej informacji o pracy z Zabbix API można znaleźć w sekcji API.

Wyświetlanie danych

Po wysłaniu danych możesz przejść do *Monitoring* → *Najnowsze dane*, aby zobaczyć wynik:



Note:
Jeśli zostanie wysłana pojedyncza wartość liczbowa, wykres danych pokaże poziomą linię po lewej i prawej stronie punktu czasowego tej wartości.

13 Monitorowanie JMX

Przegląd

Monitorowanie JMX może być używane do monitorowania liczników JMX aplikacji Java.

Monitorowanie JMX ma natywne wsparcie w Zabbix w postaci demona Zabbix o nazwie „Zabbix Java gateway".

Aby pobrać wartość konkretnego licznika JMX na hoście, serwer Zabbix odpytuje **Java gateway** Zabbix, który z kolei używa API zarządzania JMX do zdalnego odpytywania interesującej aplikacji.

Więcej szczegółów oraz informacje o konfiguracji można znaleźć w sekcji Zabbix Java gateway.

Warning:
Komunikacja między Java gateway a monitorowaną aplikacją JMX nie powinna być blokowana przez zaporę sieciową.

Włączanie zdalnego monitorowania JMX dla aplikacji Java

Aplikacja Java nie wymaga instalacji żadnego dodatkowego oprogramowania, ale musi zostać uruchomiona z opcjami wiersza poleceń podanymi poniżej, aby obsługiwać zdalne monitorowanie JMX.

Jako absolutne minimum, jeśli chcesz po prostu rozpocząć monitorowanie prostej aplikacji Java na lokalnym hoście bez wymuszonych zabezpieczeń, uruchom ją z następującymi opcjami:

```
java \
-Dcom.sun.management.jmxremote \
-Dcom.sun.management.jmxremote.port=12345 \
-Dcom.sun.management.jmxremote.authenticate=false \
-Dcom.sun.management.jmxremote.ssl=false \
-Dcom.sun.management.jmxremote.registry.ssl=false \
-jar /path/to/your/application.jar
```

Spowoduje to, że Java będzie nasłuchiwać przychodzących połączeń JMX na porcie 12345, wyłącznie z lokalnego hosta, oraz nie będzie wymagać uwierzytelniania ani SSL.

Jeśli chcesz zezwolić na połączenia na innym interfejsie, ustaw parametr -Djava.rmi.server.hostname na adres IP tego interfejsu.

Jeśli chcesz bardziej rygorystycznie podejść do kwestii bezpieczeństwa, masz do dyspozycji wiele innych opcji Java. Na przykład kolejny przykład uruchamia aplikację z bardziej wszechstronnym zestawem opcji i udostępnia ją w szerszej sieci, a nie tylko na lokalnym hoście.

```
java \
-Djava.rmi.server.hostname=192.168.3.14 \
```

```
-Dcom.sun.management.jmxremote \
-Dcom.sun.management.jmxremote.port=12345 \
-Dcom.sun.management.jmxremote.authenticate=true \
-Dcom.sun.management.jmxremote.password.file=/etc/java-6-openjdk/management/jmxremote.password \
-Dcom.sun.management.jmxremote.access.file=/etc/java-6-openjdk/management/jmxremote.access \
-Dcom.sun.management.jmxremote.ssl=true \
-Dcom.sun.management.jmxremote.registry.ssl=true \
-Djavax.net.ssl.keyStore=$YOUR_KEY_STORE \
-Djavax.net.ssl.keyStorePassword=$YOUR_KEY_STORE_PASSWORD \
-Djavax.net.ssl.trustStore=$YOUR_TRUST_STORE \
-Djavax.net.ssl.trustStorePassword=$YOUR_TRUST_STORE_PASSWORD \
-Dcom.sun.management.jmxremote.ssl.need.client.auth=true \
-jar /path/to/your/application.jar
```

Większość (jeśli nie wszystkie) z tych ustawień można określić w pliku `$JRE/lib/management/management.properties` (lub tam, gdzie ten plik znajduje się w twoim systemie).

Zwróć uwagę, że jeśli chcesz używać SSL, musisz zmodyfikować skrypt startup.sh, dodając opcje `-Djavax.net.ssl.*` do Java gateway, aby wiedział, gdzie znaleźć magazyny kluczy i zaufania.

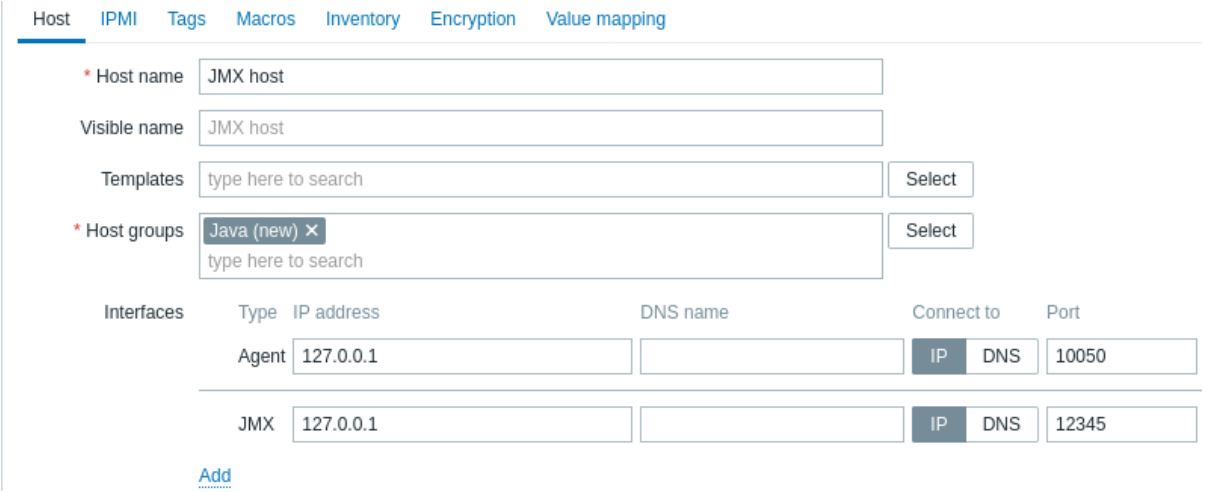
Szczegółowy opis znajduje się w Monitoring and Management Using JMX.

Konfigurowanie interfejsów JMX i pozycji w frontend Zabbix

Gdy Java gateway jest uruchomiony, serwer wie, gdzie go znaleźć, a aplikacja Java została uruchomiona z obsługą zdalnego monitorowania JMX, nadszedł czas, aby skonfigurować interfejsy i pozycje w GUI Zabbix.

Konfigurowanie interfejsu JMX

Zacznij od utworzenia interfejsu typu JMX na interesującym Cię hoście.

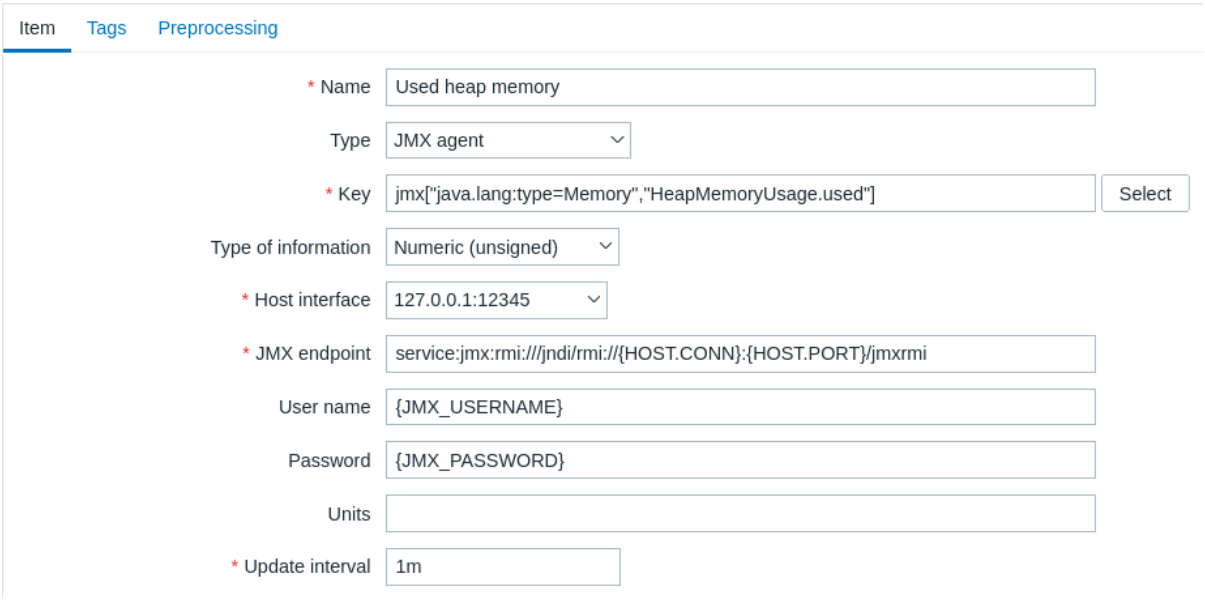


Wszystkie obowiązkowe pola wejściowe są oznaczone czerwoną gwiazdką.

Dodawanie pozycji JMX agent

Dla każdego licznika JMX, który chcesz monitorować, dodaj pozycję **JMX agent** powiązaną z tym interfejsem.

Klucz na poniższym zrzucie ekranu to `jmx["java.lang:type=Memory","HeapMemoryUsage.used"]`.



Wszystkie wymagane pola wejściowe są oznaczone czerwoną gwiazdką.

Pola wymagające określonych informacji dla pozycji JMX to:

Type	Ustaw tutaj **JMX agent**.
Key	Klucz pozycji `jmx[]` zawiera trzy parametry: **nazwa obiektu** — nazwa obiektu MBean **nazwa atrybutu** — nazwa atrybutu MBean z opcjonalnymi nazwami pól danych złożonych oddzielonymi kropkami **unikalny krótki opis** — unikalny opis, który pozwala na istnienie wielu pozycji JMX z tą samą nazwą obiektu i nazwą atrybutu na hoście (opcjonalnie) Poniżej znajduje się więcej szczegółów dotyczących kluczy pozycji JMX. Możesz wykrywać MBean i atrybuty MBean za pomocą pozycji low-level discovery `jmx.discovery[]`.
JMX endpoint	Możesz określić niestandardowy punkt końcowy JMX. Upewnij się, że parametry połączenia punktu końcowego JMX są zgodne z interfejsem JMX. Można to osiągnąć, używając makr {HOST.*}, tak jak w domyślnym punkcie końcowym JMX. Obsługiwane są makra {HOST.*} oraz makra użytkownika.
User name	Podaj nazwę użytkownika (do 255 znaków), jeśli w aplikacji Java skonfigurowano uwierzytelnianie. Obsługiwane są makra użytkownika.
Password	Podaj hasło (do 255 znaków), jeśli w aplikacji Java skonfigurowano uwierzytelnianie. Obsługiwane są makra użytkownika.

Jeśli chcesz monitorować licznik logiczny, który przyjmuje wartość „true” albo „false”, ustaw typ informacji na „Numeric (unsigned)” i wybierz krok przetwarzania wstępnego „Boolean to decimal” na karcie Preprocessing. Serwer będzie przechowywać wartości logiczne odpowiednio jako 1 lub 0.

Klucze pozycji JMX bardziej szczegółowo

Proste atrybuty

Nazwa obiektu MBean jest po prostu ciągiem znaków, który definiujesz w swojej aplikacji Java. Z kolei nazwa atrybutu może być bardziej złożona. Jeśli atrybut zwraca prymitywny typ danych (liczbę całkowitą, ciąg znaków itp.), nie ma się czym martwić — klucz będzie wyglądał tak:

`jmx[com.example:Type=Hello,weight]`

W tym przykładzie nazwa obiektu to „com.example:Type=Hello”, nazwa atrybutu to „weight”, a typ zwracanej wartości powinien prawdopodobnie być ustawiony na „Numeric (float)”.

Atrybuty zwracające dane złożone

Sytuacja staje się bardziej skomplikowana, gdy atrybut zwraca dane złożone. Na przykład: nazwa atrybutu to ”apple” i zwraca on hash reprezentujący jego parametry, takie jak ”weight”, ”color” itp. Klucz może wyglądać następująco:

`jmx[com.example:Type=Hello,apple.weight]`

W ten sposób nazwa atrybutu i klucz hash są rozdzielane przy użyciu symbolu kropki. Analogicznie, jeśli atrybut zwraca zagnieżdżone dane złożone, poszczególne części są rozdzielane kropką:

```
jmx[com.example:Type=Hello,fruits.apple.weight]
```

Atrybuty zwracające dane tabelaryczne

Atrybuty danych tabelarycznych składają się z jednego lub wielu atrybutów złożonych. Jeśli taki atrybut zostanie określony w parametrze nazwy atrybutu, wówczas wartość tej pozycji zwróci kompletną strukturę atrybutu w formacie JSON. Wartości poszczególnych elementów wewnątrz atrybutu danych tabelarycznych można pobrać za pomocą preprocessing.

Przykład atrybutu danych tabelarycznych:

```
jmx[com.example:type=Hello,foodinfo]
```

Wartość pozycji:

```
[
  {
    "a": "apple",
    "b": "banana",
    "c": "cherry"
  },
  {
    "a": "potato",
    "b": "lettuce",
    "c": "onion"
  }
]
```

Problem z kropkami

Jak dotąd wszystko dobrze. Ale co, jeśli nazwa atrybutu lub klucz hash zawiera symbol kropki? Oto przykład:

```
jmx[com.example:Type=Hello,all.fruits.apple.weight]
```

To problem. Jak powiedzieć Zabbixowi, że nazwa atrybutu to „all.fruits”, a nie tylko „all”? Jak odróżnić kropkę, która jest częścią nazwy, od kropki, która oddziela nazwę atrybutu od kluczy hash?

Jest to możliwe, wystarczy poprzedzić kropki będące częścią nazwy ukośnikiem odwrotnym:

```
jmx[com.example:Type=Hello,all\.fruits.apple.weight]
```

W ten sam sposób, jeśli klucz hash zawiera kropkę, należy ją poprzedzić znakiem ucieczki:

```
jmx[com.example:Type=Hello,all\.fruits.apple.total\.weight]
```

Inne problemy

Znak ukośnika odwrotnego w nazwie atrybutu powinien być poprzedzony znakiem ucieczki:

```
jmx[com.example:type=Hello,c:\\documents]
```

Aby obsłużyć wszelkie inne znaki specjalne w kluczu pozycji JMX, zobacz sekcję dotyczącą formatu klucza pozycji section.

To właściwie wszystko. Życzymy udanego monitorowania JMX!

Nieprymitywne typy danych

Możliwa jest praca z niestandardowymi MBeanami zwracającymi nieprymitywne typy danych, które przesłaniają metodę **toString()**.

Używanie niestandardowego endpointu z JBoss EAP 6.4

Niestandardowe endpointy umożliwiają pracę z różnymi protokołami transportowymi innymi niż domyślne RMI.

Aby zilustrować tę możliwość, spróbujmy skonfigurować monitorowanie JBoss EAP 6.4 jako przykład. Najpierw przyjmijmy kilka założeń:

- Masz już zainstalowany Zabbix Java gateway. Jeśli nie, możesz to zrobić zgodnie z dokumentacją.
- Zabbix serwer i Java gateway są zainstalowane z prefiksem `/usr/local/`
- JBoss jest już zainstalowany w `/opt/jboss-eap-6.4/` i działa w trybie standalone
- Załóżmy, że wszystkie te komponenty działają na tym samym hoście
- Firewall i SELinux są wyłączone (lub odpowiednio skonfigurowane)

Wprowadźmy kilka prostych ustawień w pliku zabbix_server.conf:

```
JavaGateway=127.0.0.1
StartJavaPollers=5
```

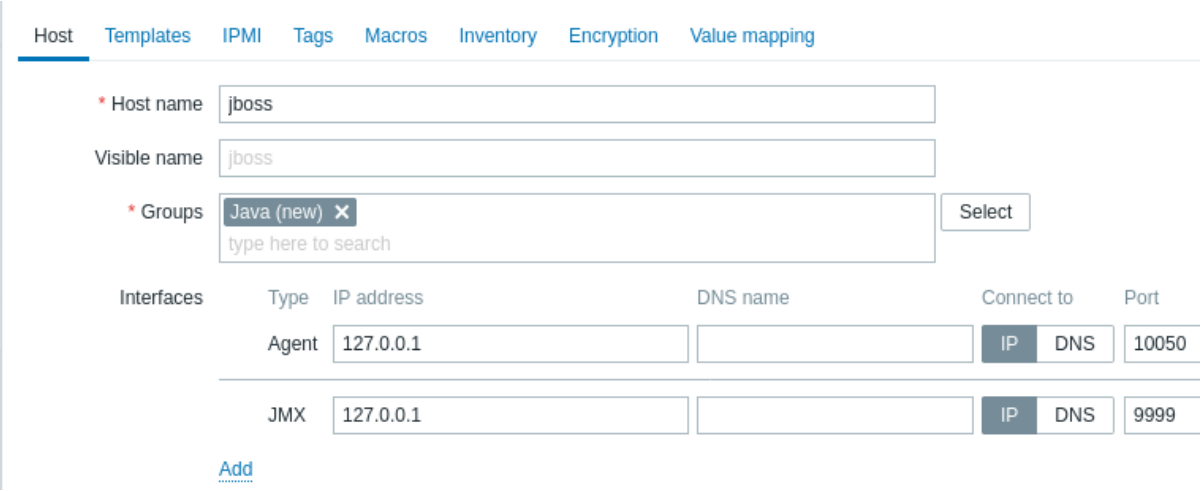
A w pliku konfiguracyjnym `zabbix_java/settings.sh` (lub `zabbix_java_gateway.conf`):

```
START_POLLERS=5
```

Sprawdź, czy JBoss nasłuchuje na swoim standardowym porcie zarządzania:

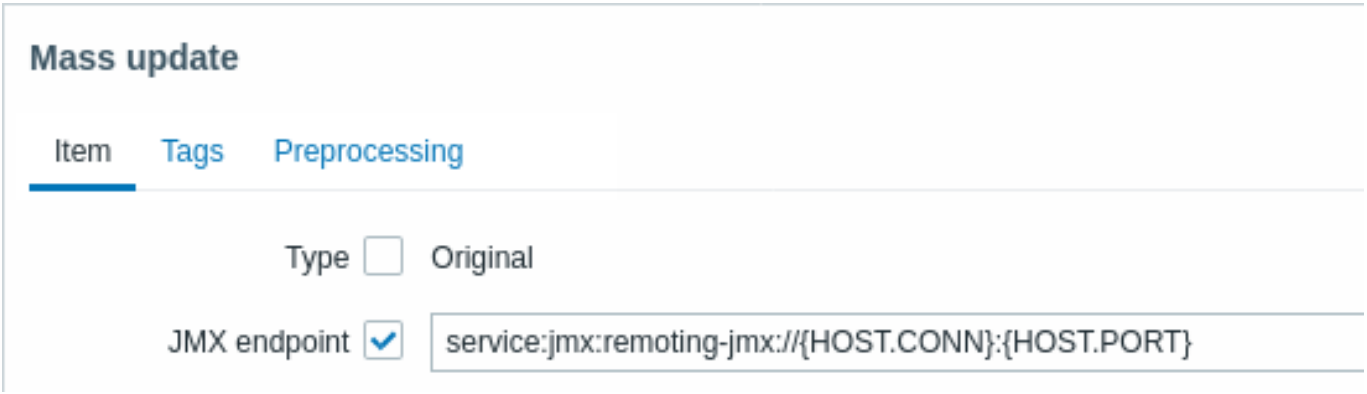
```
$ netstat -natp | grep 9999
tcp        0      0 127.0.0.1:9999          0.0.0.0:*               LISTEN      10148/java
```

Teraz utwórzmy w Zabbix host z interfejsem JMX 127.0.0.1:9999.



Ponieważ wiemy, że ta wersja JBoss używa protokołu JBoss Remoting zamiast RMI, możemy odpowiednio zbiorczo zaktualizować parametr endpointu JMX dla pozycji w naszym szablonie JMX:

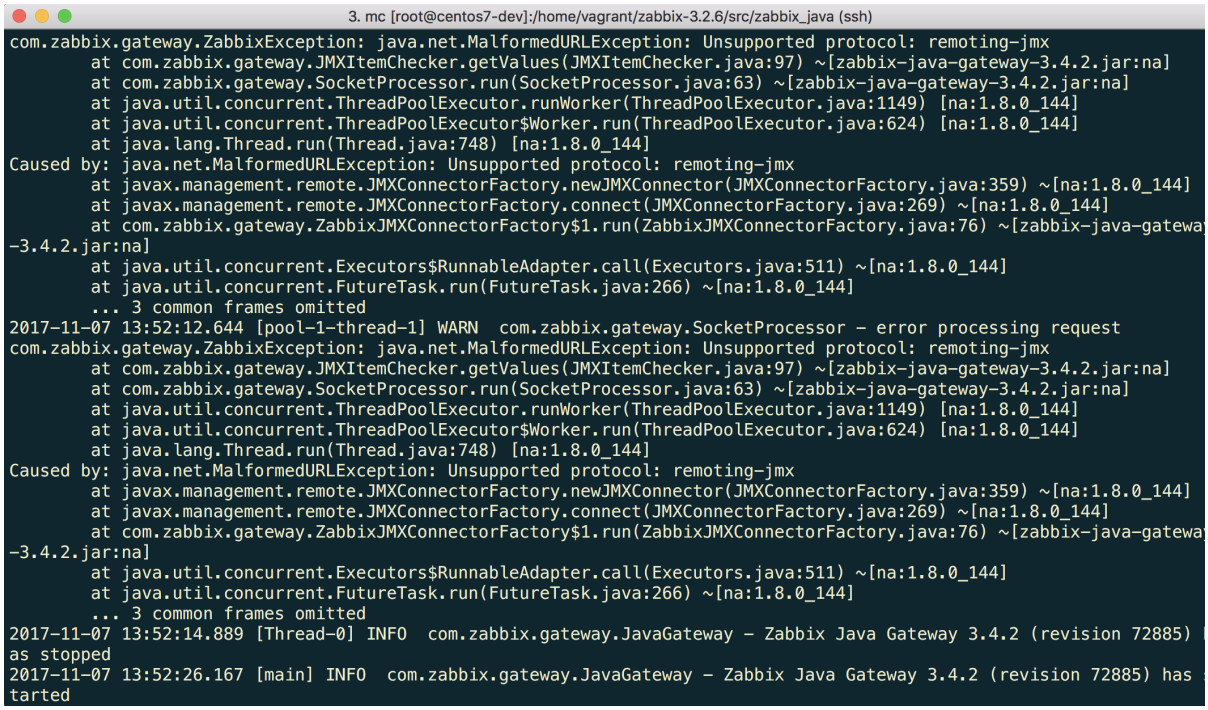
```
service:jmx:remoting-jmx://{HOST.CONN}:{HOST.PORT}
```



Zaktualizujmy pamięć podręczną konfiguracji:

```
/usr/local/sbin/zabbix_server -R config_cache_reload
```

Zwróć uwagę, że na początku możesz napotkać błąd.



„Unsupported protocol: remoting-jmx" oznacza, że Java gateway nie wie, jak pracować z określonym protokołem. Można to naprawić przez utworzenie pliku `~/needed_modules.txt` z następującą zawartością:

```
jboss-as-remoting
jboss-logging
jboss-logmanager
jboss-marshalling
jboss-remoting
jboss-sasl
jcl-over-slf4j
jul-to-slf4j-stub
log4j-jboss-logmanager
remoting-jmx
slf4j-api
xnio-api
xnio-nio
```

a następnie wykonanie polecenia:

```
for i in $(cat ~/needed_modules.txt); do find /opt/jboss-eap-6.4 -iname "${i}*.jar" -exec cp '{}' /usr/loc
```

W ten sposób Java gateway będzie miał wszystkie niezbędne moduły do pracy z jmx-remoting. Pozostaje zrestartować Java gateway, chwilę odczekać i, jeśli wszystko zostało wykonane poprawnie, zobaczyć, że dane monitorowania JMX zaczną napływać do Zabbix (zobacz także: Latest data).

14 Monitorowanie ODBC

Przegląd

Monitorowanie ODBC odpowiada typowi pozycji **Monitor bazy danych** w frontendzie Zabbix.

ODBC to pośredniczące API języka programowania C służące do uzyskiwania dostępu do systemów zarządzania bazami danych (DBMS). Koncepcja ODBC została opracowana przez firmę Microsoft, a później przeniesiona na inne platformy.

Zabbix może wykonywać zapytania do dowolnej bazy danych obsługiwanej przez ODBC. W tym celu Zabbix nie łączy się bezpośrednio z bazami danych, lecz korzysta z interfejsu ODBC i sterowników skonfigurowanych w ODBC. Pozwala to na bardziej efektywne monitorowanie różnych baz danych do wielu celów (na przykład sprawdzanie określonych kolejek bazy danych, statystyk użycia itp.).

Zabbix obsługuje unixODBC, które jest jedną z najczęściej używanych implementacji API ODBC typu open source.

Attention:
Zobacz także: znane problemy dotyczące kontroli ODBC.

Instalacja unixODBC

Zalecanym sposobem instalacji unixODBC jest użycie domyślnych repozytoriów pakietów systemu operacyjnego Linux. W najpopularniejszych dystrybucjach Linux unixODBC jest domyślnie dołączony do repozytorium pakietów. Jeśli pakiety nie są dostępne, pliki źródłowe można pobrać ze strony głównej unixODBC: http://www.unixodbc.org/download.html.

Aby zainstalować unixODBC, użyj menedżera pakietów odpowiedniego dla wybranego systemu:

```
##### Dla systemów Ubuntu/Debian:
apt install unixodbc unixodbc-dev

##### Dla systemów opartych na RedHat/Fedora:
dnf install unixODBC unixODBC-devel

##### Dla systemów opartych na SUSE:
zypper in unixODBC-devel
```

Attention:
Pakiet `unixodbc-dev` lub `unixODBC-devel` jest wymagany do skompilowania Zabbix z obsługą unixODBC. Aby włączyć obsługę ODBC, Zabbix należy skompilować z następującą opcją konfiguracji:

`--with-unixodbc[=ARG] # Użyj sterownika ODBC z pakietem unixODBC.`

Instalowanie sterowników unixODBC

Sterownik bazy danych unixODBC powinien być zainstalowany dla bazy danych, która będzie monitorowana. Listę obsługiwanych baz danych i sterowników można znaleźć na stronie głównej unixODBC: http://www.unixodbc.org/drivers.html.

Note:
W niektórych dystrybucjach Linuksa sterowniki baz danych są dołączone do repozytoriów pakietów.

MySQL

Aby zainstalować sterownik bazy danych MySQL dla unixODBC, użyj menedżera pakietów odpowiedniego dla wybranego systemu:

```
##### Dla systemów Ubuntu/Debian:
apt install odbc-mariadb

##### Dla systemów opartych na RedHat/Fedora:
dnf install mariadb-connector-odbc

##### Dla systemów opartych na SUSE:
zypper install mariadb-connector-odbc
```

Aby zainstalować sterownik bazy danych bez użycia menedżera pakietów, zapoznaj się z dokumentacją MySQL dla `mysql-connector-odbc` lub z dokumentacją MariaDB dla `mariadb-connector-odbc`.

PostgreSQL

Aby zainstalować sterownik bazy danych PostgreSQL dla unixODBC, użyj menedżera pakietów odpowiedniego dla wybranego systemu:

```
##### Dla systemów Ubuntu/Debian:
apt install odbc-postgresql

##### Dla systemów opartych na RedHat/Fedora:
dnf install postgresql-odbc

##### Dla systemów opartych na SUSE:
zypper install psqlODBC
```

Aby zainstalować sterownik bazy danych bez użycia menedżera pakietów, zapoznaj się z dokumentacją PostgreSQL.

Oracle

Aby zainstalować sterownik bazy danych unixODBC, zapoznaj się z dokumentacją Oracle.

MSSQL

Aby zainstalować sterownik bazy danych MSSQL unixODBC, użyj menedżera pakietów odpowiedniego dla wybranego systemu:

```
##### Dla systemów Ubuntu/Debian:
apt install tdsodbc

##### Dla systemów opartych na RedHat/Fedora (pakiety EPEL: https://docs.fedoraproject.org/en-US/epel/):
dnf install epel-release
dnf install freetds

##### Dla systemów opartych na SUSE:
zypper install libtdsodbc0
```

Aby zainstalować sterownik bazy danych bez użycia menedżera pakietów, zapoznaj się z przewodnikiem użytkownika FreeTDS.

Konfigurowanie unixODBC

Aby skonfigurować unixODBC, należy edytować pliki `odbcinst.ini` i `odbc.ini`. Lokalizację tych plików można sprawdzić, wykonując następujące polecenie:

```
odbcinst -j
```

Wynik polecenia powinien zawierać informacje podobne do poniższych:

```
unixODBC 2.3.9
DRIVERS............: /etc/odbcinst.ini
SYSTEM DATA SOURCES: /etc/odbc.ini
FILE DATA SOURCES..: /etc/ODBCDataSources
```

odbcinst.ini

Plik `odbcinst.ini` zawiera listę zainstalowanych sterowników baz danych ODBC. Jeśli plik `odbcinst.ini` nie istnieje, należy utworzyć go ręcznie.

```
[TEST_MYSQL]
Description=ODBC for MySQL
Driver=/usr/lib/libmyodbc5.so
FileUsage=1
```

Parameter	Description
TEST_MYSQL	Nazwa sterownika bazy danych.
Description	Opis sterownika bazy danych.
Driver	Lokalizacja biblioteki sterownika bazy danych.
FileUsage	Określa, czy sterownik bazy danych obsługuje połączenie z serwerem bazy danych bez obsługi dostępu do plików lokalnych (0); obsługuje odczyt danych z plików (1); obsługuje zapis danych do plików (2).
Threading	Poziom serializacji wątków. Obsługiwane dla PostgreSQL. Od wersji 1.6, jeśli menedżer sterowników został zbudowany z obsługą wątków, można dodać kolejny wpis sterownika.

odbc.ini

Plik `odbc.ini` służy do konfigurowania źródeł danych. Należy pamiętać, że lista obsługiwanych parametrów zależy od sterownika bazy danych (na przykład bazy danych Oracle mogą używać parametru ServerName zamiast Server itd.).

```
[TEST_MYSQL]
Description=MySQL Test Database
Driver=mysql
Server=127.0.0.1
User=root
Password=
Port=3306
Socket=
Database=zabbix
```

Parameter	Description
TEST_MYSQL	Nazwa źródła danych (DSN).
Description	Opis źródła danych.

Parameter	Description
Driver	Nazwa sterownika bazy danych (zgodnie z określeniem w `odbcinst.ini`).
Server	IP/DNS serwera bazy danych.
User	Użytkownik bazy danych używany do połączenia.
Password	Hasło użytkownika bazy danych.
Port	Port połączenia z bazą danych.
Socket	Gniazdo połączenia z bazą danych.
Database	Nazwa bazy danych.

Aby poznać inne możliwe opcje parametrów konfiguracyjnych, zobacz dokumentację MySQL.

Plik `odbc.ini` dla PostgreSQL może zawierać dodatkowe parametry:

```
[TEST_PSQL]
Description=PostgreSQL Test Database
Driver=postgresql
Username=zbx_test
Password=zabbix
Servername=127.0.0.1
Database=zabbix
Port=5432
ReadOnly=No
Protocol=8.0+
ShowOidColumn=No
FakeOidIndex=No
RowVersioning=No
ShowSystemTables=No
Fetch=Yes
BoolsAsChar=Yes
SSLmode=Require
ConnSettings=
```

Parametr	Opis
ReadOnly	Określa, czy połączenie z bazą danych zezwala wyłącznie na operacje odczytu (zapytania `SELECT`) i ogranicza modyfikacje (instrukcje `INSERT`, `UPDATE` i `DELETE`); przydatne w scenariuszach, w których dane powinny pozostać niezmienione.
Protocol	Wersja protokołu backend PostgreSQL (ignorowana w przypadku używania połączeń SSL).
ShowOidColumn	Określa, czy uwzględniać Object ID (OID) w SQLColumns.
FakeOidIndex	Określa, czy tworzyć sztuczny unikalny indeks dla OID.
RowVersioning	Określa, czy włączyć aplikacjom możliwość wykrywania, czy dane zostały zmodyfikowane przez innych użytkowników podczas próby aktualizacji wiersza. Należy pamiętać, że ten parametr może przyspieszyć proces aktualizacji, ponieważ przy aktualizacji wiersza nie trzeba określać każdej pojedynczej kolumny w klauzuli `WHERE`.
ShowSystemTables	Określa, czy sterownik bazy danych powinien traktować tabele systemowe jako zwykłe tabele w SQLTables; jest to przydatne ze względu na dostępność, ponieważ umożliwia wgląd w tabele systemowe.
Fetch	Określa, czy sterownik powinien automatycznie używać declare cursor/fetch do obsługi instrukcji `SELECT` i utrzymywać pamięć podręczną 100 wierszy.
BoolsAsChar	Steruje mapowaniem typów logicznych. Jeśli ustawiono wartość "Yes", wartości logiczne są mapowane na `SQL_CHAR`; w przeciwnym razie są mapowane na `SQL_BIT`.
SSLmode	Określa tryb SSL dla połączenia.
ConnSettings	Dodatkowe ustawienia wysyłane do backend podczas nawiązywania połączenia.

Testowanie połączenia ODBC

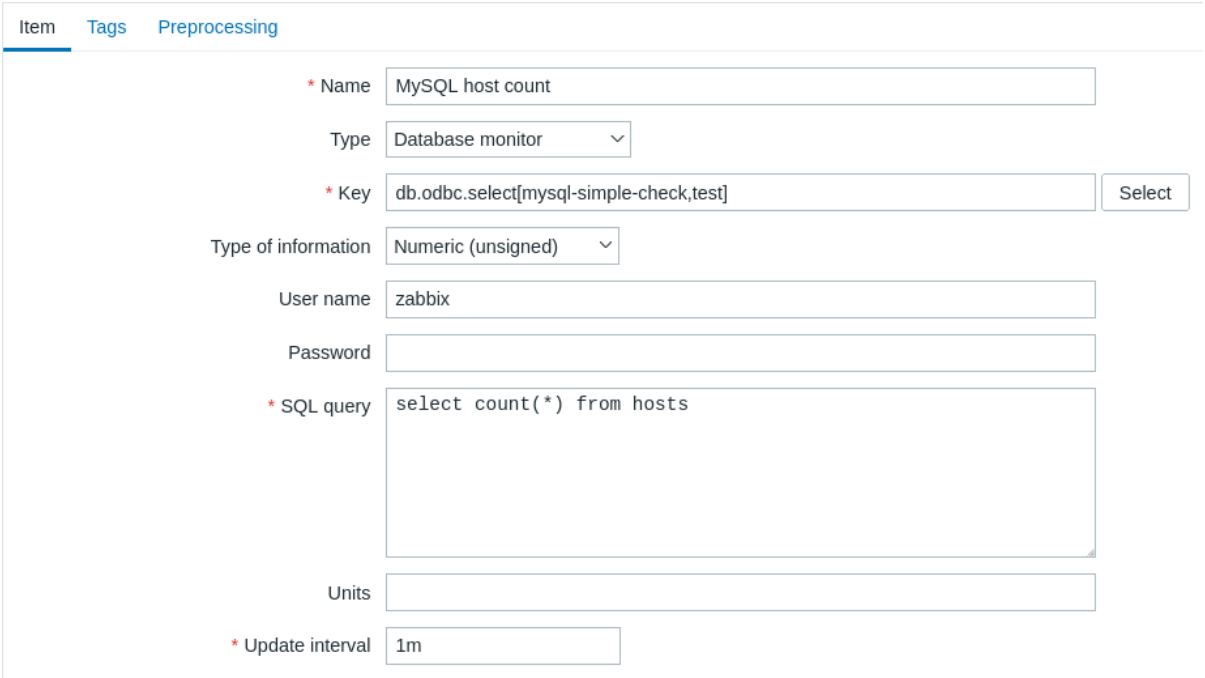
Aby sprawdzić, czy połączenie ODBC działa poprawnie, można użyć narzędzia `isql` (dołączonego do pakietu `unixODBC`):

```
isql test
+---------------------------------------+
| Connected!                            |
|                                       |
```

```
| sql-statement                          |
| help [tablename]                       |
| quit                                   |
|                                        |
+----------------------------------------+
```

Konfiguracja pozycji w frontendzie Zabbix

Skonfiguruj pozycję monitorowania **Database monitoring** item.



Wszystkie wymagane pola wejściowe są oznaczone czerwoną gwiazdką.

Dla pozycji monitorowania bazy danych należy określić:

Type	Wybierz tutaj ”Database monitor”.
Key	Wprowadź jeden z obsługiwanych kluczy pozycji: **db.odbc.select[]** - ta pozycja zwraca jedną wartość (pierwszą kolumnę pierwszego wiersza wyniku zapytania SQL); **db.odbc.get[]** - ta pozycja zwraca wiele wierszy/kolumn w formacie JSON; **db.odbc.discovery[]** - ta pozycja zwraca dane wykrywania niskiego poziomu.
User name	Wprowadź nazwę użytkownika bazy danych (do 255 znaków). Ten parametr jest opcjonalny, jeśli nazwa użytkownika bazy danych jest określona w pliku `odbc.ini`. Jeśli używany jest connection string, a pole *User name* nie jest puste, zostanie on dołączony do connection string jako `UID=<user>`.
Password	Wprowadź hasło użytkownika bazy danych (do 255 znaków). Ten parametr jest opcjonalny, jeśli hasło jest określone w pliku `odbc.ini`. Jeśli używany jest connection string, a pole *Password* nie jest puste, zostanie on dołączony do connection string jako `PWD=<password>`. Znaki specjalne są obsługiwane w tym polu. Hasło zostanie dołączone do connection string po nazwie użytkownika, na przykład jako `UID=<username>;PWD=P?;)*word`. Aby przetestować wynikowy ciąg, możesz uruchomić następujące polecenie: `isql -v -k 'Driver=libmaodbc.so;Database=zabbix;UID=zabbix;PWD=P?;)*word'`
SQL query	Wprowadź zapytanie SQL. Zwróć uwagę, że w przypadku `db.odbc.select[]` zapytanie musi zwracać tylko jedną wartość.
Type of information	Wybierz tutaj typ informacji, który będzie zwracany przez zapytanie. Jeśli typ informacji zostanie wybrany nieprawidłowo, pozycja stanie się nieobsługiwana.

Ważne uwagi

- Pozycje monitorowania bazy danych staną się nieobsługiwane, jeśli w konfiguracji serwera lub proxy nie zostaną uruchomione żadne procesy *odbc poller*. Aby aktywować pollery ODBC, ustaw parametr `StartODBCPollers` w pliku konfiguracyjnym Zabbix server lub, w przypadku kontroli wykonywanych przez proxy, w pliku konfiguracyjnym Zabbix proxy.
- Wartość parametru *Timeout* w formularzu konfiguracji pozycji jest używana jako limit czasu logowania ODBC oraz limit czasu wykonania zapytania. Należy pamiętać, że te ustawienia limitu czasu mogą zostać zignorowane, jeśli zainstalowany sterownik ODBC ich nie obsługuje.
- Polecenie SQL musi zwracać zestaw wyników, jak każde zapytanie używające instrukcji `select`. Składnia zapytania będzie zależeć od systemu RDBMS, który będzie je przetwarzał. Składnia żądania do procedury składowanej musi rozpoczynać się od słowa kluczowego `call`.

Szczegóły klucza pozycji

Parametry bez nawiasów ostrych są obowiązkowe. Parametry oznaczone nawiasami ostrymi **< >** są opcjonalne.

db.odbc.select[<unikalny krótki opis>,<dsn>,<connection string>]

 Zwraca jedną wartość, czyli pierwszą kolumnę pierwszego wiersza wyniku zapytania SQL.
 Wartość zwracana: Zależy od zapytania SQL.

Parametry:

- **unikalny krótki opis** — unikalny krótki opis identyfikujący pozycja (do użycia w wyzwalaczach itp.);
- **dsn** — nazwa źródła danych (zgodnie z definicją w `odbc.ini`);
- **connection string** — ciąg połączenia (może zawierać argumenty specyficzne dla sterownika).

Uwagi:

- Chociaż `dsn` i `connection string` są parametrami opcjonalnymi, wymagany jest co najmniej jeden z nich; jeśli zdefiniowano oba, `dsn` zostanie zignorowany.
- Jeśli zapytanie zwraca więcej niż jedną kolumnę, odczytywana jest tylko pierwsza kolumna. Jeśli zapytanie zwraca więcej niż jeden wiersz, odczytywany jest tylko pierwszy wiersz.

db.odbc.get[<unique short description>,<dsn>,<connection string>]

 Przekształca wynik zapytania SQL w tablicę JSON.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **unique short description** - unikalny krótki opis identyfikujący pozycję (do użycia w wyzwalaczach itp.);
- **dsn** - nazwa źródła danych (zgodnie z definicją w `odbc.ini`);
- **connection string** - ciąg połączenia (może zawierać argumenty specyficzne dla sterownika).

Uwagi:

- Chociaż `dsn` i `connection string` są parametrami opcjonalnymi, wymagany jest co najmniej jeden z nich; jeśli zdefiniowano oba, `dsn` zostanie zignorowany.
- Może zostać zwróconych wiele wierszy/kolumn w formacie JSON. Ta pozycja może być używana jako pozycja nadrzędna, która zbiera wszystkie dane w jednym wywołaniu systemowym, podczas gdy przetwarzanie wstępne JSONPath może być używane w pozycjach zależnych do wyodrębniania poszczególnych wartości. Więcej informacji można znaleźć w przykładzie zwracanego formatu używanego w wykrywaniu niskopoziomowym.

Przykład:

```
# Połączenie dla sterownika MySQL ODBC 5:
db.odbc.get[MySQL example,,"Driver=/usr/local/lib/libmyodbc5a.so;Database=master;Server=127.0.0.1;Port=330
```

db.odbc.discovery[<unikalny krótki opis>,<dsn>,<connection string>]

 Przekształca wynik zapytania SQL w tablicę JSON, używaną do niskopoziomowego wykrywania. Nazwy kolumn z wyniku zapytania są przekształcane w nazwy makr niskopoziomowego wykrywania sparowane z wartościami wykrytych pól. Makra te mogą być używane podczas tworzenia prototypów pozycji, wyzwalaczy itp.
 Wartość zwracana: *obiekt JSON*.

Parametry:

- **unikalny krótki opis** — unikalny krótki opis identyfikujący pozycję (do użycia w wyzwalaczach itp.);
- **dsn** — nazwa źródła danych (zgodnie z definicją w `odbc.ini`);
- **connection string** — ciąg połączenia (może zawierać argumenty specyficzne dla sterownika).

Uwagi:

- Chociaż `dsn` i `connection string` są parametrami opcjonalnymi, wymagany jest co najmniej jeden z nich; jeśli zdefiniowano oba, `dsn` zostanie zignorowany.

Komunikaty o błędach

Komunikaty o błędach ODBC są podzielone na pola, aby dostarczyć szczegółowych informacji. Na przykład komunikat o błędzie może wyglądać tak:

```
Cannot execute ODBC query: [SQL_ERROR]:[42601][7][ERROR: syntax error at or near ";"; Error while executin
```

- "`Cannot execute ODBC query`" — komunikat Zabbix
- "`[SQL_ERROR]`" — kod zwrotny ODBC
- "`[42601]`" — SQLState
- "`[7]`" — natywny kod błędu
- "`[ERROR: syntax error at or near ";"; Error while executing the query]`" — natywny komunikat błędu

Należy pamiętać, że długość komunikatu o błędzie jest ograniczona do 2048 bajtów, więc komunikat może zostać obcięty. Jeśli istnieje więcej niż jeden rekord diagnostyczny ODBC, Zabbix próbuje je połączyć (oddzielając je znakiem |) w zakresie dozwolonym przez limit długości.

15 Pozycje zależne

Przegląd

Zdarzają się sytuacje, gdy jedna pozycja zbiera jednocześnie wiele metryk lub gdy bardziej sensowne jest równoczesne zbieranie powiązanych metryk, na przykład:

- wykorzystanie CPU poszczególnych rdzeni
- przychodzący/wychodzący/całkowity ruch sieciowy

Aby umożliwić zbiorcze pobieranie metryk i ich jednoczesne użycie w kilku powiązanych pozycjach, Zabbix obsługuje pozycje zależne. Pozycje zależne są zależne od pozycji nadrzędnej, która zbiera ich dane jednocześnie, w ramach jednego zapytania. Nowa wartość pozycji nadrzędnej automatycznie uzupełnia wartości pozycji zależnych. Pozycje zależne nie mogą mieć innego interwału aktualizacji niż pozycja nadrzędna.

Opcje preprocessing w Zabbix mogą być używane do wyodrębnienia części potrzebnej dla pozycji zależnej z danych pozycji nadrzędnej.

Preprocessing jest zarządzany przez proces `preprocessing manager` wraz z wątkami roboczymi wykonującymi kroki preprocessing. Wszystkie wartości z preprocessing, otrzymane od różnych mechanizmów zbierania danych, przechodzą przez preprocessing manager przed dodaniem do pamięci podręcznej historii. Między mechanizmami zbierania danych (pollerami, trapperami itp.) a procesem preprocessing wykorzystywana jest komunikacja IPC oparta na gniazdach.

Kroki preprocessing oraz przetwarzanie pozycji zależnych są wykonywane przez Zabbix serwer lub Zabbix proxy (jeśli host jest monitorowany przez proxy).

Pozycje dowolnego typu, nawet pozycje zależne, mogą być ustawione jako pozycje nadrzędne. Dodatkowe poziomy pozycji zależnych mogą być używane do wyodrębniania mniejszych części z wartości istniejącej pozycji zależnej.

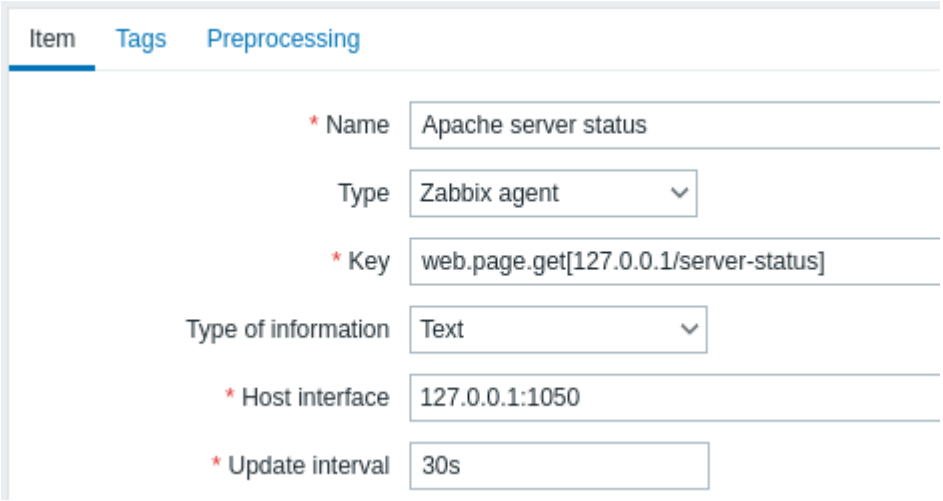
Ograniczenia

- Dozwolone są tylko zależności w obrębie tego samego hosta (szablonu)
- Prototyp pozycji może zależeć od innego prototypu pozycji lub zwykłej pozycji z tego samego hosta
- Zależna pozycja na hoście z główną pozycją z szablonu nie zostanie wyeksportowana do XML

Konfiguracja pozycji

Pozycja zależna zależy od swojej pozycji nadrzędnej pod względem danych. Dlatego najpierw musi zostać skonfigurowana (lub istnieć) **pozycja nadrzędna**:

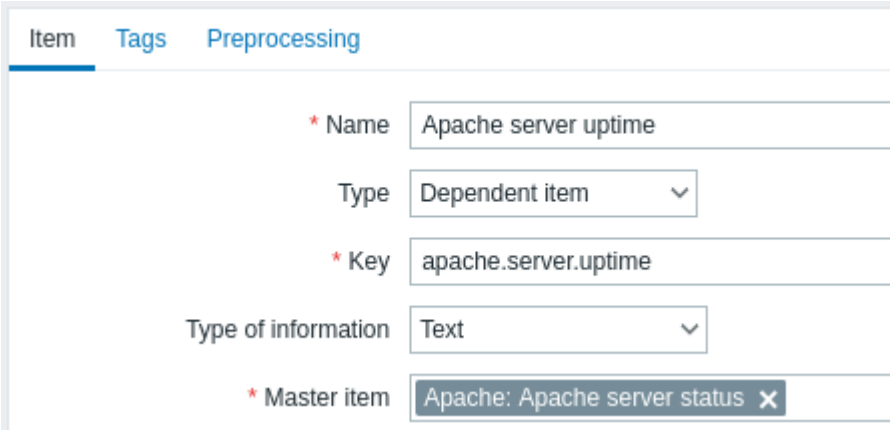
- Przejdź do: *Data collection* → *Hosts*
- Kliknij *Items* w wierszu hosta
- Kliknij *Create item*
- Wprowadź parametry pozycji w formularzu



Wszystkie obowiązkowe pola wejściowe są oznaczone czerwoną gwiazdką.

Kliknij *Add*, aby zapisać pozycję nadrzędną.

Następnie możesz skonfigurować **pozycję zależną**.

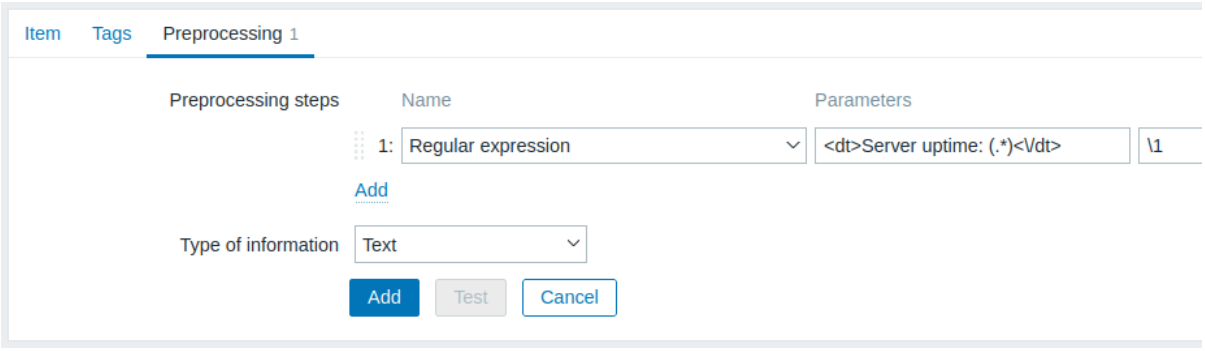


Wszystkie obowiązkowe pola wejściowe są oznaczone czerwoną gwiazdką.

Pola wymagające określonych informacji dla pozycji zależnych to:

Type	Wybierz tutaj **Dependent item**.
Key	Wprowadź klucz, który będzie używany do rozpoznawania pozycji.
Master item	Wybierz pozycję nadrzędną. Wartość pozycji nadrzędnej zostanie użyta do wypełnienia wartości pozycji zależnej.
Type of information	Wybierz typ informacji, który będzie odpowiadał formatowi danych, które będą przechowywane.

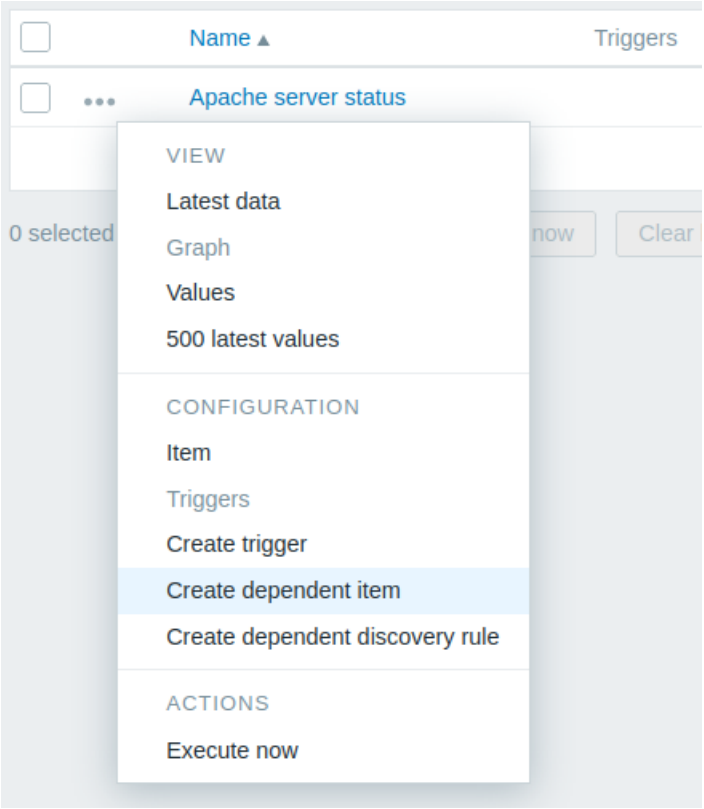
Możesz użyć przetwarzania wstępnego wartości pozycji, aby wyodrębnić wymaganą część wartości pozycji nadrzędnej.



Bez przetwarzania wstępnego wartość pozycji zależnej będzie dokładnie taka sama jak wartość pozycji nadrzędnej.

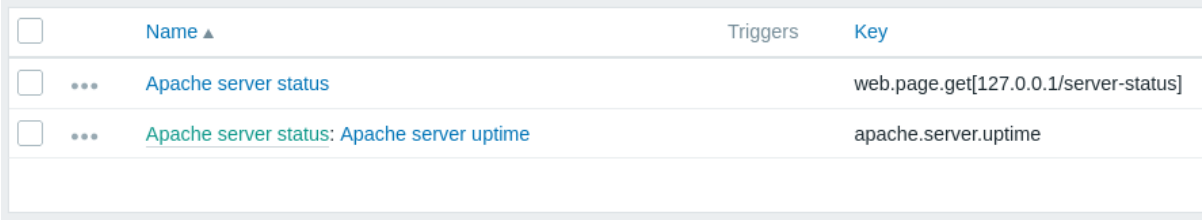
Kliknij *Add*, aby zapisać pozycję zależną.

Skrót umożliwiający szybsze utworzenie pozycji zależnej jest dostępny po kliknięciu przycisku ••• na liście pozycji i wybraniu *Create dependent item*.



Wyświetlanie

Na liście pozycji pozycje zależne są wyświetlane z nazwą nadrzędnej pozycji jako prefiksem.



Jeśli nadrzędna pozycja zostanie usunięta, wszystkie jej pozycje zależne również zostaną usunięte.

16 Agent HTTP

Przegląd

Ten typ pozycji umożliwia odpytywanie danych przy użyciu protokołu HTTP/HTTPS. Możliwe jest również trapowanie przy użyciu narzędzia Zabbix sender lub protokołu Zabbix sender (do wysyłania danych do serwera lub proxy Zabbix), albo przy użyciu metody API `history.push` (do wysyłania danych do serwera Zabbix).

Kontrole pozycji HTTP są wykonywane przez serwer Zabbix. Jednak gdy hosty są monitorowane przez proxy Zabbix, kontrole pozycji HTTP są wykonywane przez proxy.

Kontrole pozycji HTTP nie wymagają uruchomionego agenta na monitorowanym hoście.

HTTP agent obsługuje zarówno HTTP, jak i HTTPS. Zabbix może opcjonalnie podążać za przekierowaniami (zobacz opcję *Follow redirects* poniżej). Maksymalna liczba przekierowań jest na stałe ustawiona na 10 (przy użyciu opcji cURL CURLOPT_MAXREDIRS).

> **Attention:**
> Serwer/proxy Zabbix musi być wstępnie skonfigurowany z obsługą cURL (libcurl).

Kontrole HTTP są wykonywane asynchronicznie — nie jest wymagane odebranie odpowiedzi na jedno żądanie przed rozpoczęciem innych kontroli. Rozwiązywanie DNS również odbywa się asynchronicznie.

Maksymalna współbieżność kontroli asynchronicznych wynosi 1000 (zdefiniowana przez MaxConcurrentChecksPerPoller).

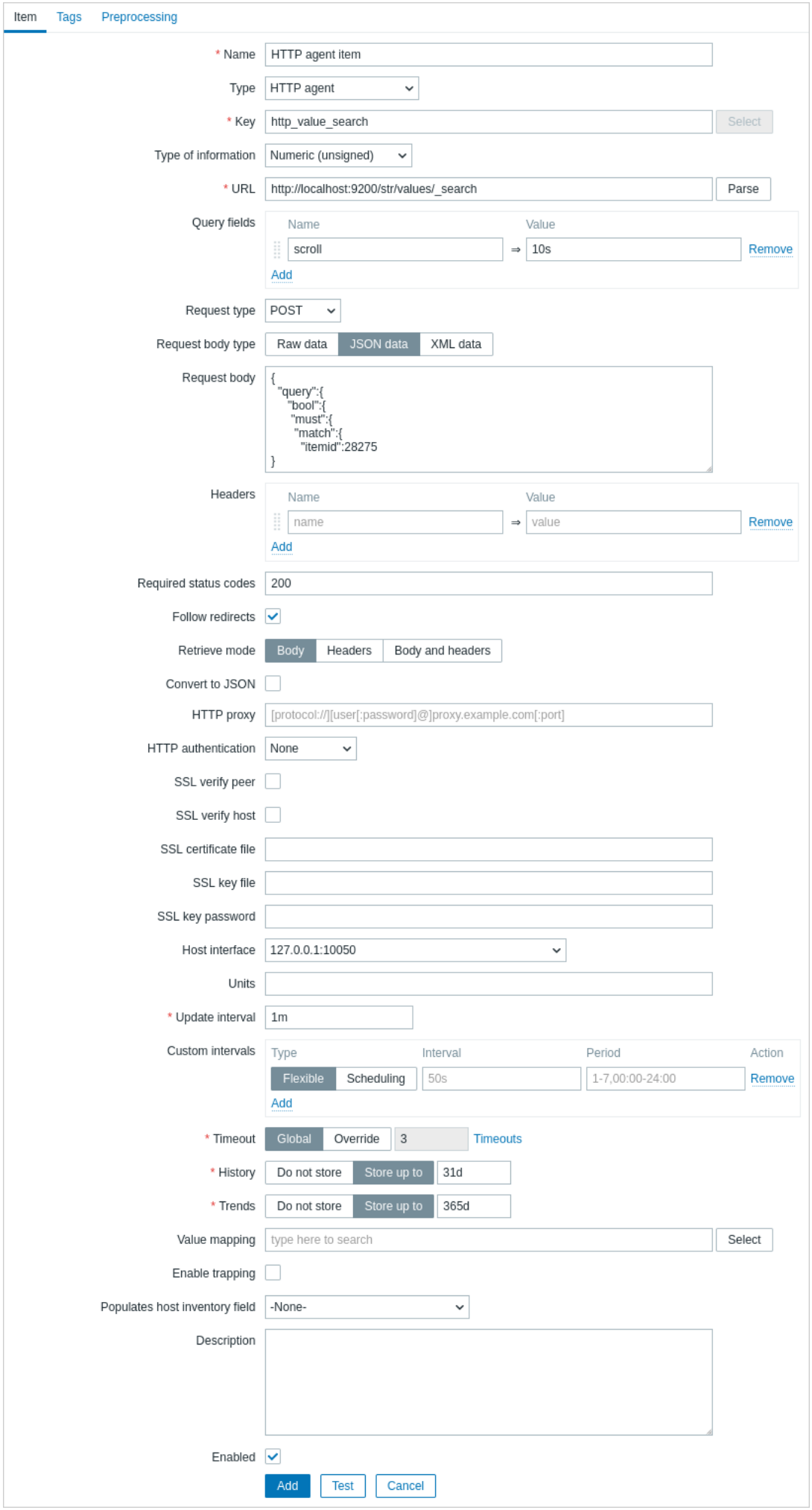
Liczba asynchronicznych pollerów HTTP agent jest definiowana przez parametr StartHTTPAgentPollers.

Funkcja trwałych połączeń cURL została dodana do kontroli HTTP agent od wersji Zabbix 7.0.

Konfiguracja

Aby skonfigurować pozycję HTTP:

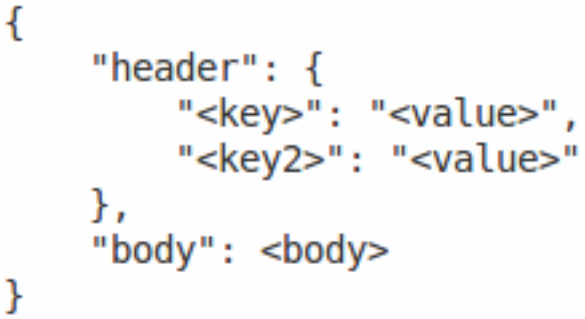
- Przejdź do: *Data collection* → *Hosts*
- Kliknij *Items* w wierszu hosta
- Kliknij *Create item*
- Wprowadź parametry pozycji w formularzu


Item
Tags
Preprocessing
* Name
HTTP agent item
Type
HTTP agent
* Key
http_value_search
Select
Type of information
Numeric (unsigned)
* URL
http://localhost:9200/str/values/_search
Parse
Query fields
Name
Value
scroll
⇒
10s
Remove
Add
Request type
POST
Request body type
Raw data
JSON data
XML data
Request body
{
"query":{
"bool":{
"must":{
"match":{
"itemid":28275
}
Headers
Name
Value
name
⇒
value
Remove
Add
Required status codes
200
Follow redirects
Retrieve mode
Body
Headers
Body and headers
Convert to JSON
HTTP proxy
[protocol://][user[:password]@]proxy.example.com[:port]
HTTP authentication
None
SSL verify peer
SSL verify host
SSL certificate file
SSL key file
SSL key password
Host interface
127.0.0.1:10050
Units
* Update interval
1m
Custom intervals
Type
Interval
Period
Action
Flexible
Scheduling
50s
1-7,00:00-24:00
Remove
Add
* Timeout
Global
Override
3
Timeouts
* History
Do not store
Store up to
31d
* Trends
Do not store
Store up to
365d
Value mapping
type here to search
Select
Enable trapping
Populates host inventory field
-None-
Description
Enabled
Add
Test
Cancel

Wszystkie obowiązkowe pola wejściowe są oznaczone czerwoną gwiazdką.

Pola wymagające określonych informacji dla pozycji HTTP to:

Parameter	Description
Type	Wybierz tutaj **HTTP agent**.
Key	Wprowadź unikalny klucz pozycji.
URL	Adres URL, z którym ma zostać nawiązane połączenie i z którego mają zostać pobrane dane. Na przykład: https://www.example.com http://www.example.com/download Nazwy domen mogą być podawane przy użyciu znaków Unicode. Podczas wykonywania sprawdzenia HTTP są one automatycznie konwertowane z punycode do ASCII. Przycisk *Parse* może zostać użyty do oddzielenia opcjonalnych pól zapytania (takich jak ?name=Admin&password=mypassword) od adresu URL, przenosząc atrybuty i wartości do *Query fields* w celu automatycznego kodowania URL. Limit wynosi 2048 znaków. Obsługiwane makra: {HOST.IP}, {HOST.CONN}, {HOST.DNS}, {HOST.HOST}, {HOST.NAME}, {HOST.PORT}, {ITEM.ID}, {ITEM.KEY}, {ITEM.KEY.ORIG}, makra użytkownika, makra niskopoziomowego wykrywania. Ustawia to opcję cURL CURLOPT_URL.
Query fields	Zmienne dla adresu URL (patrz wyżej). Określane jako pary atrybut-wartość. Wartości są automatycznie kodowane URL. Wartości z makr są rozwijane, a następnie automatycznie kodowane URL. Obsługiwane makra: {HOST.IP}, {HOST.CONN}, {HOST.DNS}, {HOST.HOST}, {HOST.NAME}, {HOST.PORT}, {ITEM.ID}, {ITEM.KEY}, {ITEM.KEY.ORIG}, makra użytkownika, makra niskopoziomowego wykrywania. Ustawia to opcję cURL CURLOPT_URL.
Request type	Wybierz typ metody żądania: *GET*, *POST*, *PUT* lub *HEAD*
Request body type	Wybierz typ treści żądania: **Raw data** - niestandardowa treść żądania HTTP; makra są podstawiane, ale nie jest wykonywane kodowanie **JSON data** - treść żądania HTTP w formacie JSON. Makra mogą być używane jako string, number, true i false; makra używane jako string muszą być ujęte w podwójne cudzysłowy. Wartości z makr są rozwijane, a następnie automatycznie poprzedzane znakami ucieczki. Jeśli w nagłówkach nie określono ”Content-Type”, domyślnie zostanie użyte ”Content-Type: application/json” **XML data** - treść żądania HTTP w formacie XML. Makra mogą być używane jako węzeł tekstowy, atrybut lub sekcja CDATA. Wartości z makr są rozwijane, a następnie automatycznie poprzedzane znakami ucieczki w węźle tekstowym i atrybucie. Jeśli w nagłówkach nie określono ”Content-Type”, domyślnie zostanie użyte ”Content-Type: application/xml”
Request body	Wprowadź treść żądania. Obsługiwane makra: {HOST.IP}, {HOST.CONN}, {HOST.DNS}, {HOST.HOST}, {HOST.NAME}, {HOST.PORT}, {ITEM.ID}, {ITEM.KEY}, {ITEM.KEY.ORIG}, makra użytkownika, makra niskopoziomowego wykrywania.
Headers	Niestandardowe nagłówki HTTP, które zostaną wysłane podczas wykonywania żądania. Określane jako pary atrybut-wartość. Obsługiwane makra: {HOST.IP}, {HOST.CONN}, {HOST.DNS}, {HOST.HOST}, {HOST.NAME}, {HOST.PORT}, {ITEM.ID}, {ITEM.KEY}, {ITEM.KEY.ORIG}, makra użytkownika, makra niskopoziomowego wykrywania. Ustawia to opcję cURL CURLOPT_HTTPHEADER.
Required status codes	Lista oczekiwanych kodów statusu HTTP. Jeśli Zabbix otrzyma kod, którego nie ma na liście, pozycja stanie się nieobsługiwana. Jeśli pole jest puste, sprawdzenie nie jest wykonywane. Na przykład: 200,201,210-299 Obsługiwane makra na liście: makra użytkownika, makra niskopoziomowego wykrywania. Wykorzystuje to opcję cURL CURLINFO_RESPONSE_CODE.
Follow redirects	Zaznacz pole wyboru, aby podążać za przekierowaniami HTTP. Ustawia to opcję cURL CURLOPT_FOLLOWLOCATION.
Retrieve mode	Wybierz część odpowiedzi, która ma zostać pobrana: **Body** - tylko treść **Headers** - tylko nagłówki **Body and headers** - treść i nagłówki

Parameter	Description
Convert to JSON	Nagłówki są zapisywane jako pary atrybut-wartość pod kluczem "header", jeśli *Retrieve mode* nie jest ustawione na *Body*. Jeśli zostanie napotkane 'Content-Type: application/json', treść zostanie zapisana jako obiekt; w przeciwnym razie zostanie zapisana jako string, na przykład: 
HTTP proxy	Możesz określić używany serwer proxy HTTP, korzystając z formatu `[protocol://][username[:password]@]proxy.example.com[:port]`. Opcjonalny prefiks `protocol://` może zostać użyty do określenia alternatywnych protokołów proxy (np. https, socks4, socks5; zobacz documentation; obsługa prefiksu protokołu została dodana w cURL 7.21.7). Jeśli nie określono protokołu, proxy będzie traktowany jako proxy HTTP. Jeśli określisz niewłaściwy protokół, połączenie zakończy się niepowodzeniem, a pozycja stanie się nieobsługiwana. Domyślnie zostanie użyty port 1080. Jeśli określono, proxy nadpisze zmienne środowiskowe związane z proxy, takie jak http_proxy, HTTPS_PROXY. Jeśli nie określono, proxy nie nadpisze zmiennych środowiskowych związanych z proxy. Wprowadzona wartość jest przekazywana „tak jak jest"; nie jest wykonywana żadna kontrola poprawności. *Uwaga*: w przypadku proxy HTTP obsługiwane jest tylko proste uwierzytelnianie. Obsługiwane makra: {HOST.IP}, {HOST.CONN}, {HOST.DNS}, {HOST.HOST}, {HOST.NAME}, {HOST.PORT}, {ITEM.ID}, {ITEM.KEY}, {ITEM.KEY.ORIG}, makra użytkownika, makra niskopoziomowego wykrywania. Ustawia to opcję cURL CURLOPT_PROXY.
HTTP authentication	Wybierz opcję uwierzytelniania: **None** - bez uwierzytelniania; **Basic** - używane jest uwierzytelnianie podstawowe; **NTLM** - używane jest uwierzytelnianie NTLM (Windows NT LAN Manager); **Kerberos** - używane jest uwierzytelnianie Kerberos (zobacz także: Configuring Kerberos with Zabbix); **Digest** - używane jest uwierzytelnianie Digest. Ustawia to opcję cURL CURLOPT_HTTPAUTH.
User name	Wprowadź nazwę użytkownika (do 255 znaków). To pole jest dostępne, jeśli *HTTP authentication* jest ustawione na Basic, NTLM, Kerberos lub Digest. Obsługiwane są makra użytkownika i makra niskopoziomowego wykrywania.
Password	Wprowadź hasło użytkownika (do 255 znaków). To pole jest dostępne, jeśli *HTTP authentication* jest ustawione na Basic, NTLM, Kerberos lub Digest. Obsługiwane są makra użytkownika i makra niskopoziomowego wykrywania.
SSL verify peer	Zaznacz pole wyboru, aby weryfikować certyfikat SSL serwera WWW. Certyfikat serwera zostanie automatycznie pobrany z systemowej lokalizacji urzędu certyfikacji (CA). Możesz zastąpić lokalizację plików CA za pomocą parametru konfiguracyjnego serwera lub proxy Zabbix SSLCALocation. Ustawia to opcję cURL CURLOPT_SSL_VERIFYPEER.
SSL verify host	Zaznacz pole wyboru, aby zweryfikować, czy pole Common Name lub Subject Alternate Name certyfikatu serwera WWW jest zgodne. Ustawia to opcję cURL CURLOPT_SSL_VERIFYHOST.
SSL certificate file	Nazwa pliku certyfikatu SSL używanego do uwierzytelniania klienta. Plik certyfikatu musi być w formacie PEM[1]. Jeśli plik certyfikatu zawiera również klucz prywatny, pozostaw pole pliku klucza SSL puste. Jeśli klucz jest zaszyfrowany, podaj hasło w polu hasła klucza SSL. Katalog zawierający ten plik jest określany przez parametr konfiguracyjny serwera lub proxy Zabbix SSLCertLocation. Obsługiwane makra: {HOST.IP}, {HOST.CONN}, {HOST.DNS}, {HOST.HOST}, {HOST.NAME}, {HOST.PORT}, {ITEM.ID}, {ITEM.KEY}, {ITEM.KEY.ORIG}, makra użytkownika, makra niskopoziomowego wykrywania. Ustawia to opcję cURL CURLOPT_SSLCERT.

Parameter	Description
SSL key file	Nazwa pliku klucza prywatnego SSL używanego do uwierzytelniania klienta. Plik klucza prywatnego musi być w formacie PEM[1]. Katalog zawierający ten plik jest określany przez parametr konfiguracyjny serwera lub proxy Zabbix SSLKeyLocation. Obsługiwane makra: {HOST.IP}, {HOST.CONN}, {HOST.DNS}, {HOST.HOST}, {HOST.NAME}, {HOST.PORT}, {ITEM.ID}, {ITEM.KEY}, {ITEM.KEY.ORIG}, makra użytkownika, makra niskopoziomowego wykrywania. Ustawia to opcję cURL CURLOPT_SSLKEY.
SSL key password	Hasło do pliku klucza prywatnego SSL. Obsługiwane makra: makra użytkownika, makra niskopoziomowego wykrywania. Ustawia to opcję cURL CURLOPT_KEYPASSWD.
Timeout	Zabbix nie poświęci więcej niż ustawiony czas na przetwarzanie adresu URL (1-600 sekund). W praktyce parametr ten określa maksymalny czas na nawiązanie połączenia z adresem URL oraz maksymalny czas wykonania żądania HTTP. Dlatego Zabbix nie poświęci więcej niż 2 x *Timeout* sekund na jedno sprawdzenie. Ustawia to opcję cURL CURLOPT_TIMEOUT. Więcej informacji o parametrze *Timeout* można znaleźć w general item attributes.
Enable trapping	Po zaznaczeniu tego pola wyboru pozycja będzie również działać jako pozycja trapper i będzie akceptować dane wysyłane do serwera lub proxy Zabbix za pomocą narzędzia Zabbix sender lub protocol Zabbix sender, albo będzie akceptować dane wysyłane do serwera Zabbix za pomocą metody API `history.push`. Więcej informacji o wysyłaniu danych można znaleźć tutaj: Trapper items.
Allowed hosts	Widoczne tylko wtedy, gdy zaznaczone jest pole wyboru *Enable trapping*. Lista adresów IP rozdzielonych przecinkami, opcjonalnie w notacji CIDR, lub nazw DNS. Jeśli określono, połączenia przychodzące będą akceptowane tylko od hostów wymienionych tutaj. Jeśli obsługa IPv6 jest włączona, wtedy '127.0.0.1', '::127.0.0.1', '::ffff:127.0.0.1' są traktowane jednakowo, a '::/0' pozwoli na dowolny adres IPv4 lub IPv6. '0.0.0.0/0' może zostać użyte do zezwolenia na dowolny adres IPv4. Zwróć uwagę, że „adresy IPv6 zgodne z IPv4" (prefiks 0000::/96) są obsługiwane, ale przestarzałe według RFC4291. Przykład: 127.0.0.1, 192.168.1.0/24, 192.168.3.1-255, 192.168.1-10.1-255, ::1,2001:db8::/32, mysqlserver1, zabbix.example.com, {HOST.HOST} Spacje i user macros są dozwolone w tym polu. Makra hosta: {HOST.HOST}, {HOST.NAME}, {HOST.IP}, {HOST.DNS}, {HOST.CONN} są dozwolone w tym polu.

Note:
Jeśli pole *HTTP proxy* pozostanie puste, innym sposobem użycia proxy HTTP jest ustawienie zmiennych środowiskowych związanych z proxy.
Dla HTTP - ustaw zmienną środowiskową `http_proxy` dla użytkownika serwera Zabbix. Na przykład: `http_proxy=http://proxy_ip:proxy_port`.
Dla HTTPS - ustaw zmienną środowiskową `HTTPS_PROXY`. Na przykład: `HTTPS_PROXY=http://proxy_ip:proxy_port`. Więcej szczegółów jest dostępnych po uruchomieniu polecenia powłoki: *# man curl*.

Attention:
[1] Zabbix obsługuje wyłącznie pliki certyfikatów i kluczy prywatnych w formacie PEM. Jeśli dane certyfikatu i klucza prywatnego są zapisane w pliku w formacie PKCS #12 (zwykle z rozszerzeniem *.p12 lub *.pfx), możesz wygenerować z niego plik PEM za pomocą następujących poleceń:

```
openssl pkcs12 -in ssl-cert.p12 -clcerts -nokeys -out ssl-cert.pem
openssl pkcs12 -in ssl-cert.p12 -nocerts -nodes  -out ssl-cert.key
```

Przykłady

Przykład 1

Wysyłaj proste żądania GET, aby pobierać dane z usług takich jak Elasticsearch:

- Utwórz pozycja GET z adresem URL: `localhost:9200/?pretty`
- Zwróć uwagę na odpowiedź:

```
{
  "name" : "YQ2VAY-",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "kH4CYqh5QfqgeTsjh2F9zg",
  "version" : {
    "number" : "6.1.3",
    "build_hash" : "af51318",
    "build_date" : "2018-01-26T18:22:55.523Z",
    "build_snapshot" : false,
    "lucene_version" : "7.1.0",
    "minimum_wire_compatibility_version" : "5.6.0",
    "minimum_index_compatibility_version" : "5.0.0"
  },
  "tagline" : "You know, for search"
}
```

- Teraz wyodrębnij numer wersji za pomocą kroku wstępnego przetwarzania JSONPath: `$.version.number`

Przykład 2

Wysyłaj proste żądania POST, aby pobierać dane z usług takich jak Elasticsearch:

- Utwórz pozycję POST z adresem URL: `http://localhost:9200/str/values/_search?scroll=10s`
- Skonfiguruj następującą treść POST, aby uzyskać obciążenie procesora (średnia 1-minutowa na rdzeń)

```
{
    "query": {
        "bool": {
            "must": [{
                "match": {
                    "itemid": 28275
                }
            }],
            "filter": [{
                "range": {
                    "clock": {
                        "gt": 1517565836,
                        "lte": 1517566137
                    }
                }
            }]
        }
    }
}
```

- Otrzymano:

```
{
    "_scroll_id": "DnF1ZXJ5VGhlbkZldGNoBQAAAAAAAAAkFllRMlZBWS1UU1pxTmdEeGVwQjRBTFEAAAAAAAAAJRZZUTJWQVk
    "took": 18,
    "timed_out": false,
    "_shards": {
        "total": 5,
        "successful": 5,
        "skipped": 0,
        "failed": 0
    },
    "hits": {
        "total": 1,
        "max_score": 1.0,
        "hits": [{
            "_index": "dbl",
            "_type": "values",
            "_id": "dqX9VWEBV6sEKSMyk6sw",
            "_score": 1.0,
            "_source": {
```

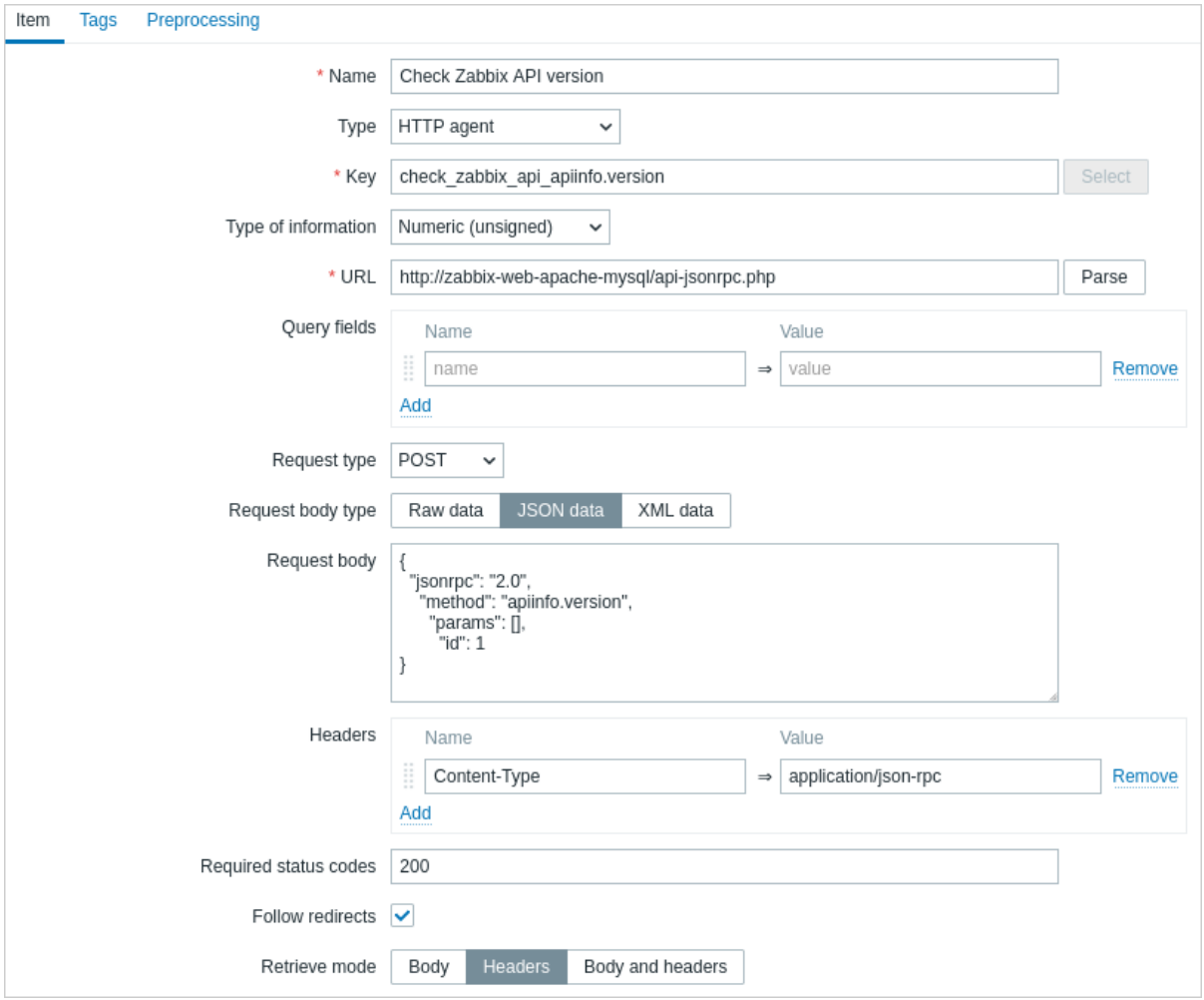
```
                    "itemid": 28275,
                    "value": "0.138750",
                    "clock": 1517566136,
                    "ns": 25388713,
                    "ttl": 604800
                }
            }]
        }
    }
```


- Teraz użyj kroku preprocessing JSONPath, aby uzyskać wartość pozycji: `$.hits.hits[0]._source.value`

Przykład 3

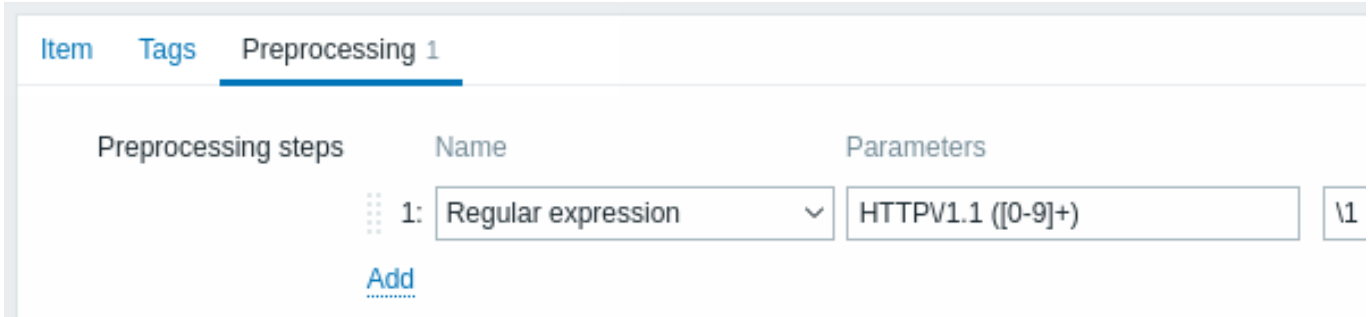
Sprawdzanie, czy API Zabbix działa, przy użyciu apiinfo.version.

- Konfiguracja pozycji:

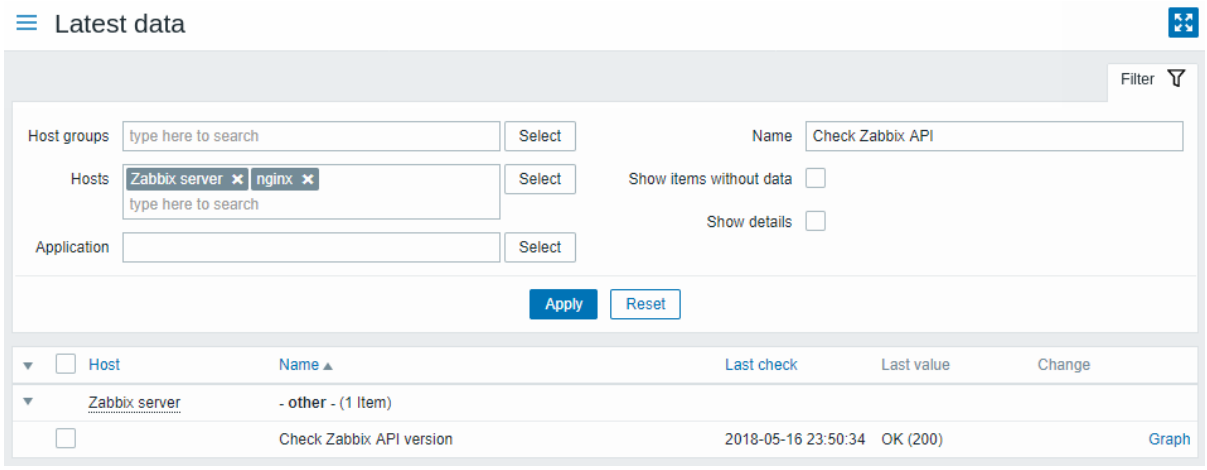


Zwróć uwagę na użycie metody POST z danymi JSON, ustawienie nagłówków żądania oraz żądanie zwrócenia tylko nagłówków:

- Wstępne przetwarzanie wartości pozycji za pomocą wyrażenia regularnego w celu uzyskania kodu HTTP:



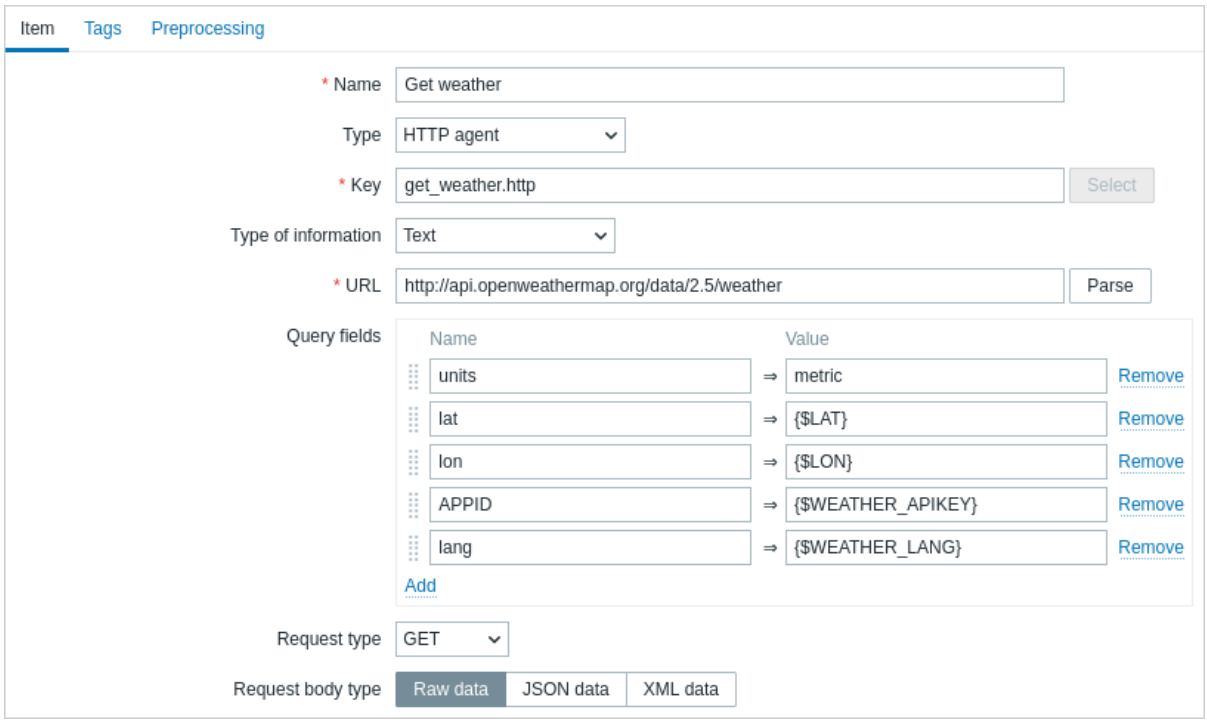
- Sprawdzanie wyniku w *Najnowszych danych*:



Przykład 4

Pobieranie informacji o pogodzie przez połączenie z publiczną usługą Openweathermap.

- Skonfiguruj master item do zbiorczego pobierania danych w pojedynczym JSON:



Zwróć uwagę na użycie makr w polach zapytania. Informacje o tym, jak je wypełnić, znajdziesz w API Openweathermap.

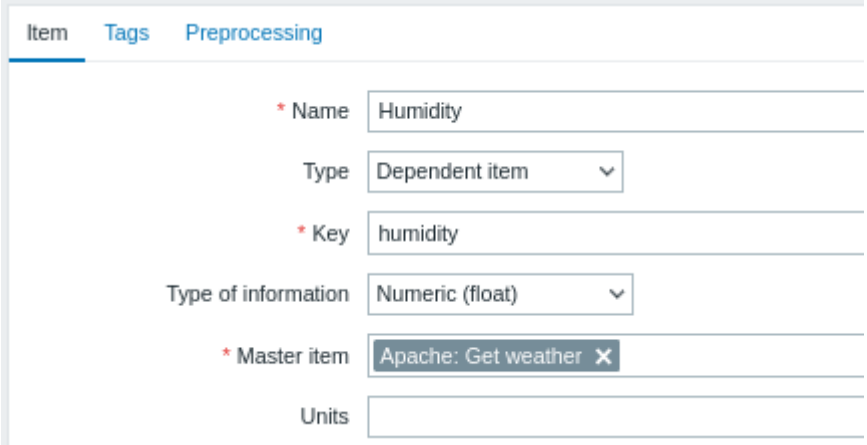
Przykładowy JSON zwrócony w odpowiedzi przez HTTP agent:

```
{
    "body": {
        "coord": {
            "lon": 40.01,
            "lat": 56.11
        },
        "weather": [{
            "id": 801,
            "main": "Clouds",
            "description": "few clouds",
            "icon": "02n"
        }],
        "base": "stations",
        "main": {
            "temp": 15.14,
            "pressure": 1012.6,
            "humidity": 66,
```

```
            "temp_min": 15.14,
            "temp_max": 15.14,
            "sea_level": 1030.91,
            "grnd_level": 1012.6
        },
        "wind": {
            "speed": 1.86,
            "deg": 246.001
        },
        "clouds": {
            "all": 20
        },
        "dt": 1526509427,
        "sys": {
            "message": 0.0035,
            "country": "RU",
            "sunrise": 1526432608,
            "sunset": 1526491828
        },
        "id": 487837,
        "name": "Stavrovo",
        "cod": 200
    }
}
```

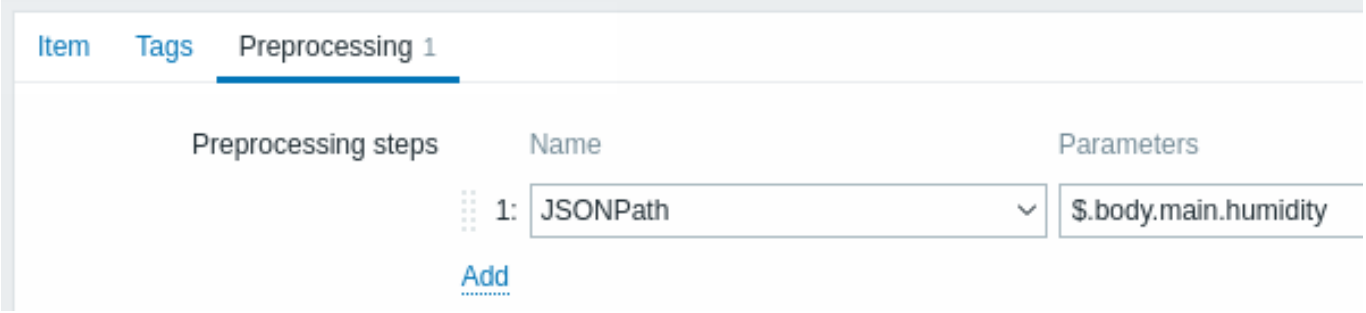

Następnym zadaniem jest skonfigurowanie pozycji zależnych, które wyodrębniają dane z JSON.

- Skonfiguruj przykładową pozycję zależną dla wilgotności:

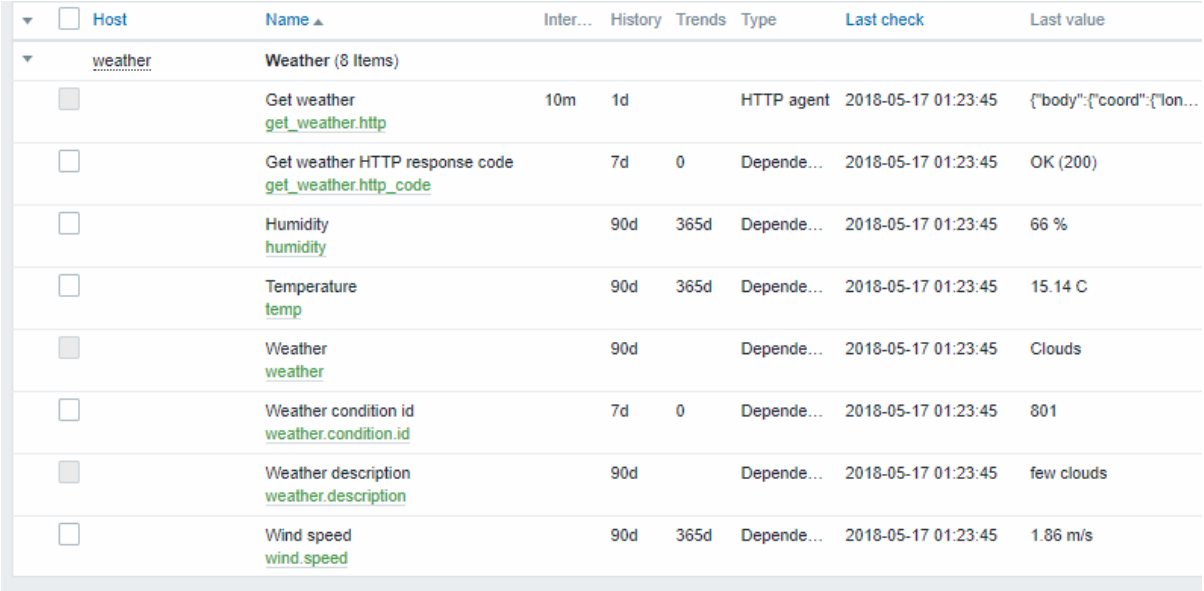


Pozostałe metryki pogodowe, takie jak „Temperature”, dodaje się w ten sam sposób.

- Przykładowe przetwarzanie wstępne wartości pozycji zależnej z użyciem JSONPath:



- Sprawdź wynik danych pogodowych w *Latest data*:

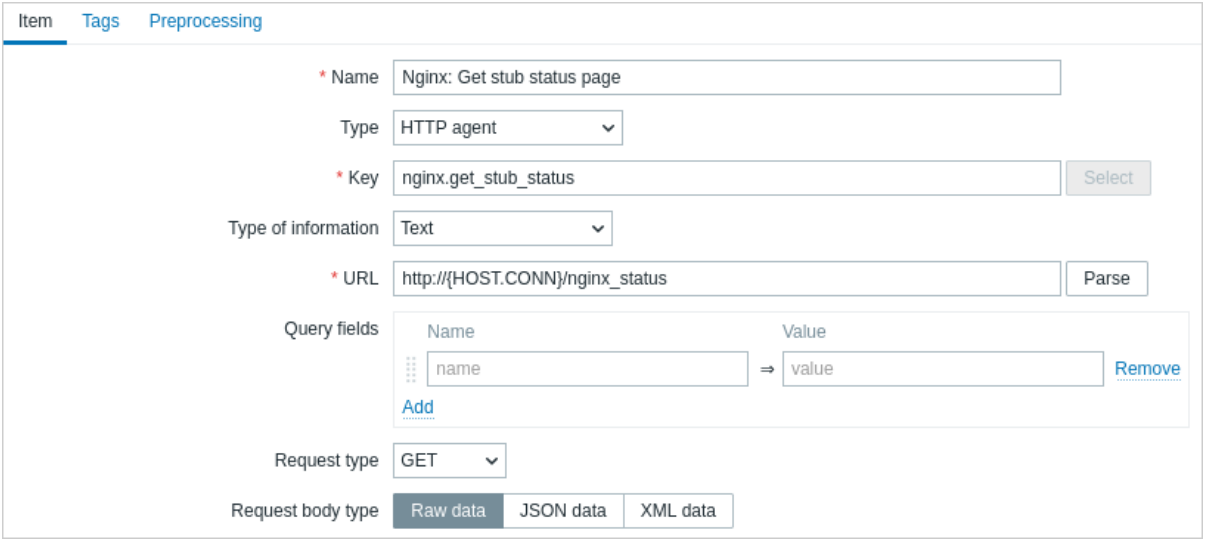


Host	Name ▲	Inter...	History	Trends	Type	Last check	Last value
weather	**Weather** (8 Items)						
	Get weather get_weather.http	10m	1d		HTTP agent	2018-05-17 01:23:45	{"body":{"coord":{"lon...
	Get weather HTTP response code get_weather.http_code		7d	0	Depende...	2018-05-17 01:23:45	OK (200)
	Humidity humidity		90d	365d	Depende...	2018-05-17 01:23:45	66 %
	Temperature temp		90d	365d	Depende...	2018-05-17 01:23:45	15.14 C
	Weather weather		90d		Depende...	2018-05-17 01:23:45	Clouds
	Weather condition id weather.condition.id		7d	0	Depende...	2018-05-17 01:23:45	801
	Weather description weather.description		90d		Depende...	2018-05-17 01:23:45	few clouds
	Wind speed wind.speed		90d	365d	Depende...	2018-05-17 01:23:45	1.86 m/s

Przykład 5

Łączenie ze stroną statusu Nginx i zbiorcze pobieranie jego metryk.

- Skonfiguruj Nginx zgodnie z oficjalnym przewodnikiem.
- Skonfiguruj główną pozycję do zbiorczego zbierania danych:

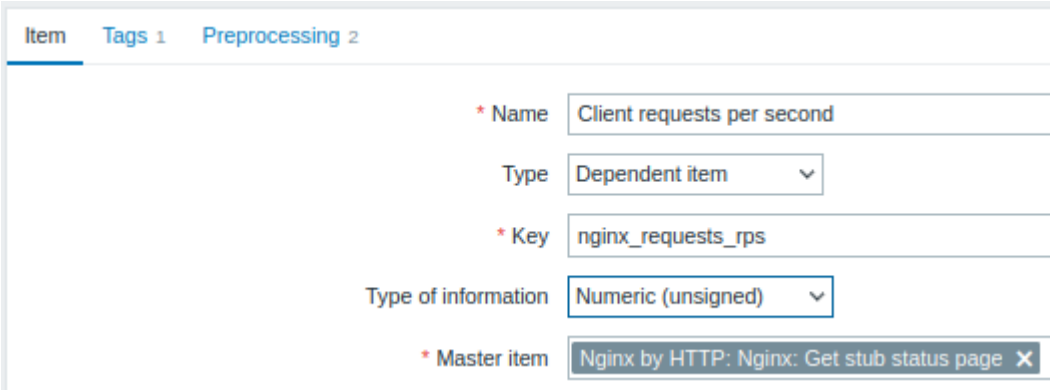


Przykładowe dane wyjściowe statusu stub Nginx:

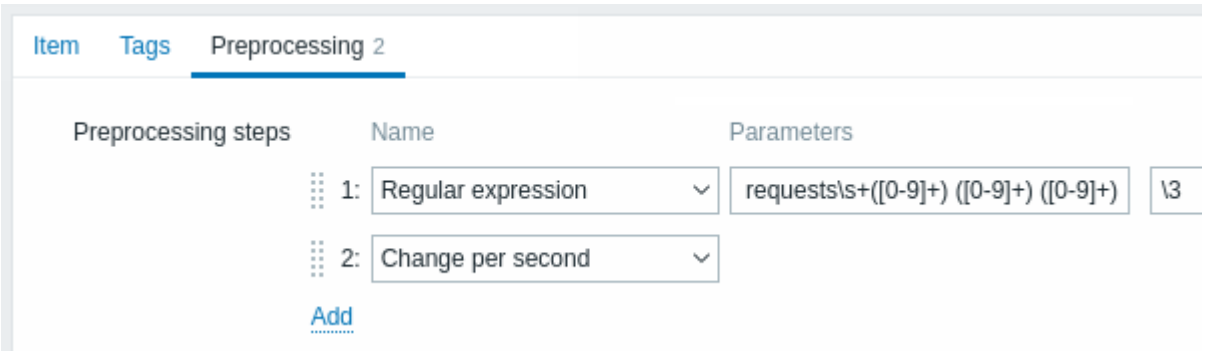
```
Active connections: 1 Active connections:
server accepts handled requests
 52 52 52
Reading: 0 Writing: 1 Waiting: 0
```

Następnym zadaniem jest skonfigurowanie pozycji zależnych, które wyodrębniają dane.

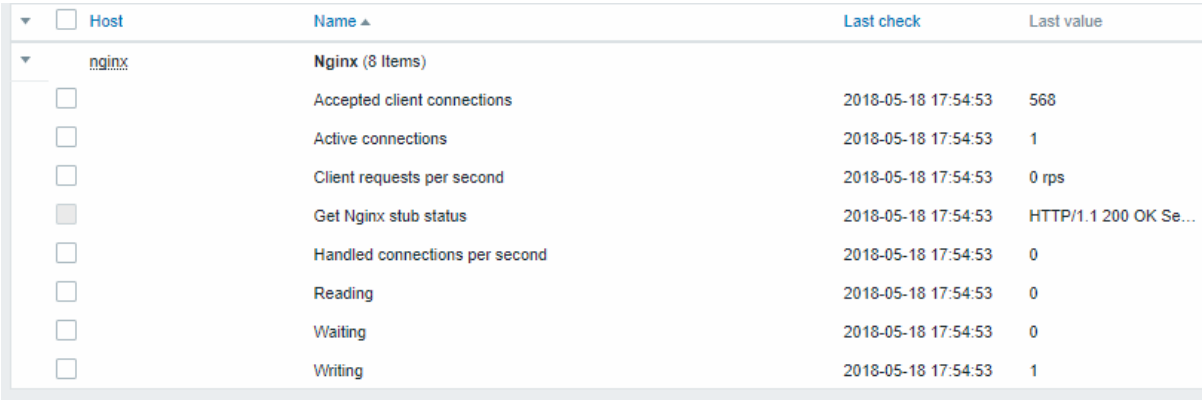
- Skonfiguruj przykładową pozycję zależną dla liczby żądań na sekundę:



- Przykładowe wstępne przetwarzanie wartości pozycji zależnej za pomocą wyrażenia regularnego `server accepts handled requests\s+([0-9]+) ([0-9]+) ([0-9]+)`:



- Sprawdź pełny wynik z modułu stub w *Najnowsze dane*:



17 Kontrole Prometheus

Przegląd

Zabbix może odpytywać metryki udostępniane w formacie linii Prometheus.

Aby rozpocząć zbieranie danych Prometheus, wymagane są dwa kroki:

- główna pozycja HTTP wskazująca odpowiedni endpoint danych, np. `https://<prometheus host>/metrics`
- pozycje zależne używające opcji preprocessing Prometheus do odpytywania wymaganych danych z metryk zebranych przez główną pozycję

Dostępne są dwie opcje preprocessing danych Prometheus:

- *Wzorzec Prometheus* - używany w zwykłych pozycjach do odpytywania danych Prometheus
- *Prometheus do JSON* - używany w zwykłych pozycjach oraz do wykrywania niskopoziomowego. W tym przypadku odpytywane dane Prometheus są zwracane w formacie JSON.

Przetwarzanie zbiorcze

Przetwarzanie zbiorcze jest obsługiwane dla zależnych pozycji. Aby włączyć buforowanie i indeksowanie, wstępne przetwarzanie *Prometheus pattern* musi być **pierwszym** krokiem wstępnego przetwarzania. Jeśli *Prometheus pattern* jest pierwszym krokiem wstępnego przetwarzania, przeanalizowane dane Prometheus są buforowane i indeksowane według pierwszego warunku

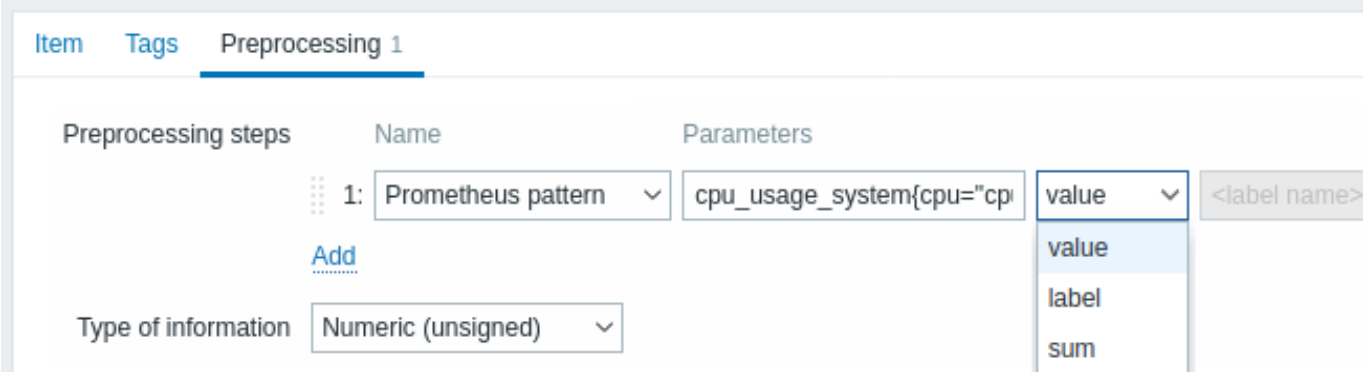
`<label>==<value>` w kroku wstępnego przetwarzania *Prometheus pattern*. Ta pamięć podręczna jest ponownie wykorzystywana podczas przetwarzania innych zależnych pozycji w tej partii. Aby uzyskać optymalną wydajność, pierwsza etykieta powinna być tą, która ma najwięcej różnych wartości.

Jeśli przed pierwszym krokiem trzeba wykonać inne wstępne przetwarzanie, należy je przenieść albo do pozycji nadrzędnej, albo do nowej zależnej pozycji, która będzie używana jako pozycja nadrzędna dla zależnych pozycji.

Konfiguracja

Zakładając, że masz skonfigurowaną nadrzędną pozycję HTTP, musisz utworzyć pozycję zależną, która używa kroku preprocessing Prometheus:

- Wprowadź ogólne parametry pozycji zależnej w formularzu konfiguracji
- Przejdź do zakładki Preprocessing
- Wybierz opcję preprocessing Prometheus (*Prometheus pattern* lub *Prometheus to JSON*)



Następujące parametry są specyficzne dla opcji preprocessing *Prometheus pattern*:

Parametr	Opis	Przykłady
Pattern	Aby zdefiniować wymagany wzorzec danych, możesz użyć języka zapytań podobnego do języka zapytań Prometheus (zobacz tabelę porównawczą), np.: <metric name> - wybór według nazwy metryki {__name__="<metric name>"} - wybór według nazwy metryki {__name__=~"<regex>"} - wybór według nazwy metryki pasującej do wyrażenia regularnego {<label name>="<label value>",...} - wybór według nazwy etykiety {<label name>=~"<regex>",...} - wybór według nazwy etykiety pasującej do wyrażenia regularnego {__name__=~".*"}==<value> - wybór według wartości metryki Lub kombinację powyższych: <metric name>{<label1 name>="<label1 value>",<label2 name>=~"<regex>",...}==<value> Wartość etykiety może być dowolną sekwencją znaków UTF-8, ale znaki ukośnika odwrotnego, podwójnego cudzysłowu i znaku nowej linii muszą być poprzedzone znakiem ucieczki jako \\, \" i \n; pozostałe znaki nie powinny być poprzedzane znakiem ucieczki.	*wmi_os_physical_memory_free_bytes* *cpu_usage_system{cpu="cpu-total"}* *cpu_usage_system{cpu=~".*"}* *cpu_usage_system{cpu="cpu-total",host=~".*"}* *wmi_service_state{name="dhcp"}==1* *wmi_os_timezone{timezone=~".*"}==1*

Parametr	Opis	Przykłady
Result processing	Określ, czy ma zostać zwrócona wartość, etykieta, czy ma zostać zastosowana odpowiednia funkcja (jeśli wzorzec pasuje do kilku wierszy i wynik wymaga agregacji): **value** - zwróć wartość metryki (błąd, jeśli dopasowano wiele wierszy) **label** - zwróć wartość etykiety określonej w polu *Label* (błąd, jeśli dopasowano wiele metryk) **sum** - zwróć sumę wartości **min** - zwróć wartość minimalną **max** - zwróć wartość maksymalną **avg** - zwróć wartość średnią **count** - zwróć liczbę wartości To pole jest dostępne tylko dla opcji *Prometheus pattern*.	Zobacz także poniższe przykłady użycia parametrów.
Output	Zdefiniuj nazwę etykiety (opcjonalnie). W takim przypadku zostanie zwrócona wartość odpowiadająca nazwie etykiety. To pole jest dostępne tylko dla opcji *Prometheus pattern*, jeśli w polu *Result processing* wybrano 'Label'.	

Przykłady użycia parametrów

1. Najczęstszym przypadkiem użycia jest zwrócenie **wartości**. Aby zwrócić wartość `/var/db` z:

   `node_disk_usage_bytes{path="/var/cache"} 2.1766144e+09<br> node_disk_usage_bytes{path="/var/db"} 20480<br> node_disk_usage_bytes{path="/var/dpkg"} 8192<br> node_disk_usage_bytes{path="/var/empty"} 4096`

użyj następujących parametrów:

- *Pattern* - `node_disk_usage_bytes{path="/var/db"}`
- *Result processing* - wybierz 'value'

2. Możesz być także zainteresowany **średnią** wartością wszystkich parametrów `node_disk_usage_bytes`:

- *Pattern* - `node_disk_usage_bytes`
- *Result processing* - wybierz 'avg'

3. Chociaż Prometheus obsługuje tylko dane liczbowe, popularne jest stosowanie obejścia, które pozwala również zwrócić odpowiedni opis tekstowy. Można to osiągnąć za pomocą filtra i określenia etykiety. Tak więc, aby zwrócić wartość etykiety 'color' z

   `elasticsearch_cluster_health_status{cluster="elasticsearch",color="green"} 1<br> elasticsearch_cluster 0<br> elasticsearch_cluster_health_status{cluster="elasticsearch",color="yellow"} 0`

użyj następujących parametrów:

- *Pattern* - `elasticsearch_cluster_health_status {cluster="elasticsearch"} == 1`
- *Result processing* - wybierz 'label'
- *Label* - określ 'color'

Filtr (oparty na wartości liczbowej '1') dopasuje odpowiedni wiersz, a etykieta zwróci opis stanu kondycji (obecnie 'green', ale potencjalnie także 'red' lub 'yellow').

Prometheus do JSON

Dane z Prometheus mogą być używane do wykrywania niskiego poziomu. W takim przypadku potrzebne są dane w formacie JSON, a opcja przetwarzania wstępnego *Prometheus do JSON* zwróci dokładnie taki format.

Aby uzyskać więcej informacji, zobacz Wykrywanie przy użyciu danych Prometheus.

Porównanie języków zapytań

Poniższa tabela przedstawia różnice i podobieństwa między PromQL a językiem zapytań wstępnego przetwarzania Prometheus w Zabbixie.

Selektor wektora chwilowego PromQL		Wstępne przetwarzanie Prometheus w Zabbixie
Różnice		
Cel zapytania	Serwer Prometheus	Zwykły tekst w formacie ekspozycji Prometheus
Zwraca	Wektor chwilowy	Wartość metryki lub etykiety (wzorzec Prometheus) Tablica metryk dla pojedynczej wartości w JSON (Prometheus do JSON)
Operatory dopasowania etykiet	**=**, **!=**, **=~**, **!~**	**=**, **!=**, **=~**, **!~**
Wyrażenie regularne używane przy dopasowaniu etykiety lub nazwy metryki	RE2	PCRE
Operatory porównania	Zobacz listę	Do filtrowania wartości obsługiwany jest tylko operator **==** (równe)
Podobieństwa		
Wybór według nazwy metryki równej ciągowi znaków	<metric name> lub {__name__="<metric name>"}	<metric name> lub {__name__="<metric name>"}
Wybór według nazwy metryki pasującej do wyrażenia regularnego	{__name__=~"<regex>"}	{__name__=~"<regex>"}
Wybór według wartości <label name> równej ciągowi znaków	{<label name>="<label value>",...}	{<label name>="<label value>",...}
Wybór według wartości <label name> pasującej do wyrażenia regularnego	{<label name>=~"<regex>",...}	{<label name>=~"<regex>",...}
Wybór według wartości równej ciągowi znaków	{__name__=~".*"} == <value>	{__name__=~".*"} == <value>

18 Pozycje skryptowe

Przegląd

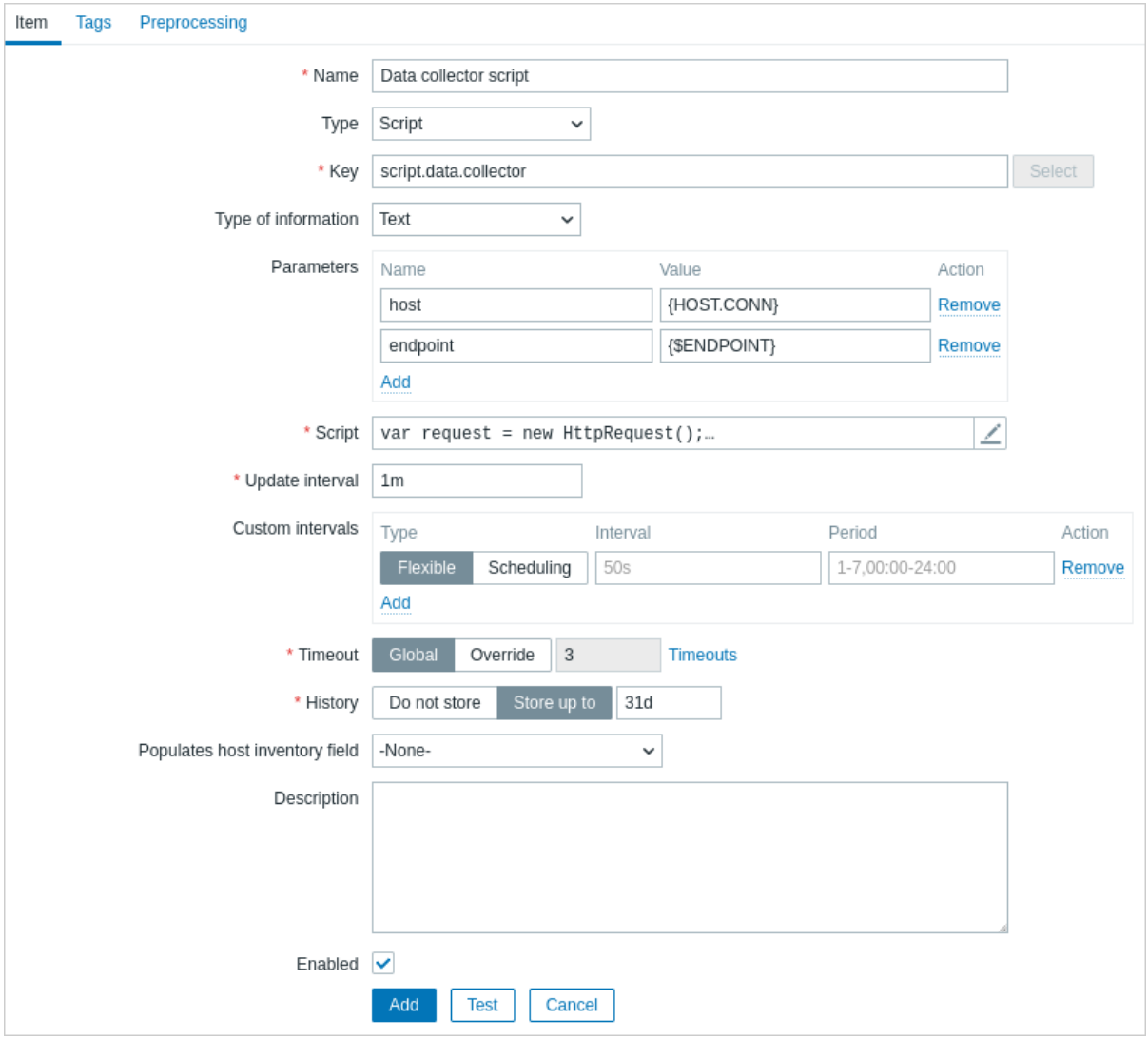
Pozycje skryptowe mogą być używane do zbierania danych przez wykonywanie zdefiniowanego przez użytkownika kodu JavaScript z możliwością pobierania danych przez HTTP/HTTPS. Oprócz skryptu można określić opcjonalną listę parametrów (par nazw i wartości) oraz limit czasu.

Ten typ pozycji może być przydatny w scenariuszach zbierania danych, które wymagają wielu kroków lub złożonej logiki. Na przykład pozycja skryptowa może być skonfigurowana tak, aby wykonać wywołanie HTTP, następnie w pewien sposób przetworzyć dane otrzymane w pierwszym kroku i przekazać przekształconą wartość do drugiego wywołania HTTP.

Pozycje skryptowe są przetwarzane przez pollery serwera lub proxy Zabbix.

Konfiguracja

W polu *Typ* formularza konfiguracji pozycji wybierz Script, a następnie wypełnij wymagane pola.



Wszystkie obowiązkowe pola wejściowe są oznaczone czerwoną gwiazdką.

Pola wymagające określonych informacji dla pozycji typu Script to:

Pole	Opis
Key	Wprowadź unikalny klucz, który będzie używany do identyfikacji pozycji.
Parameters	Określ zmienne przekazywane do skryptu jako pary atrybut-wartość. Obsługiwane są makra użytkownika. Aby sprawdzić, które wbudowane makra są obsługiwane, wyszukaj „Script-type item” w tabeli obsługiwanych makr.
Script	Wprowadź kod JavaScript w modalnym edytorze, który otwiera się po kliknięciu w pole parametru lub ikonę ołówka obok niego. Kod ten musi zawierać logikę zwracania wartości metryki. Kod ma dostęp do wszystkich parametrów oraz wszystkich dodatkowych obiektów JavaScript dodanych przez Zabbix. Zobacz także: Przewodnik po JavaScript.
Timeout	Limit czasu wykonywania JavaScript (1-600 s; jego przekroczenie spowoduje zwrócenie błędu). Pamiętaj, że w zależności od skryptu wyzwolenie limitu czasu może potrwać dłużej. Więcej informacji o parametrze *Timeout* znajdziesz w sekcji ogólnych atrybutów pozycji.

Przykłady

Proste zbieranie danych

Pobierz zawartość *https://www.example.com/release_notes*:

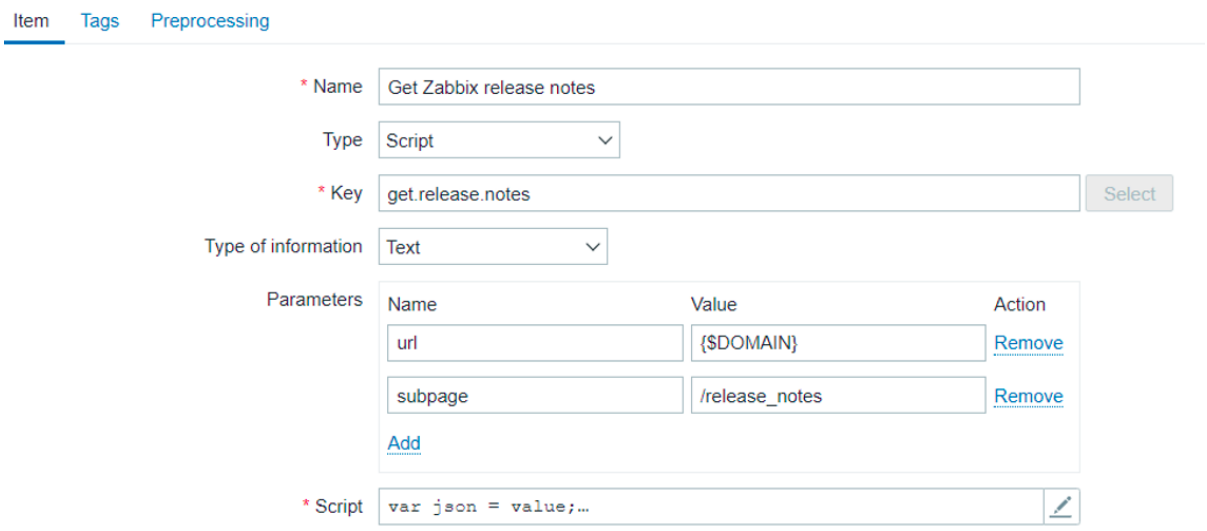
- Utwórz pozycję typu „Script”.
- W polu *Script* wprowadź:

```
var request = new HttpRequest();
return request.get("https://www.example.com/release_notes");
```

Zbieranie danych z użyciem parametrów

Pobierz zawartość określonej strony i wykorzystaj parametry:

- Utwórz pozycję typu ”Script” z dwoma parametrami:
  - **url : {$DOMAIN}** (makro użytkownika {$DOMAIN} powinno być zdefiniowane, najlepiej na poziomie hosta)
  - **subpage : /release_notes**



- W polu *Script* wprowadź:

```
var obj = JSON.parse(value);
var url = obj.url;
var subpage = obj.subpage;
var request = new HttpRequest();
return request.get(url + subpage);
```

Wiele żądań HTTP

Pobierz zawartość zarówno *https://www.example.com*, jak i *https://www.example.com/release_notes*:

- Utwórz pozycję typu „Script”.
- W polu *Script* wprowadź:

```
var request = new HttpRequest();
return request.get("https://www.example.com") + request.get("https://www.example.com/release_notes");
```

Logowanie

Dodaj wpis „Log test” do logu serwera Zabbix i w odpowiedzi odbierz wartość pozycji „1”:

- Utwórz pozycję typu „Script”.
- W polu *Script* wprowadź:

```
Zabbix.log(3, 'Log test');
return 1;
```

19 Pozycje przeglądarki

Przegląd

Pozycje przeglądarki umożliwiają monitorowanie złożonych witryn internetowych i aplikacji webowych przy użyciu przeglądarki.

> **Attention:**
> Obsługa pozycji przeglądarki jest obecnie eksperymentalna.

Pozycje przeglądarki zbierają dane przez wykonywanie kodu JavaScript zdefiniowanego przez użytkownika oraz pobieranie danych przez HTTP/HTTPS. Ta pozycja może symulować takie działania związane z przeglądarką, jak klikanie, wprowadzanie tekstu, przechodzenie między stronami internetowymi oraz inne interakcje użytkownika z witrynami internetowymi lub aplikacjami webowymi.

Oprócz skryptu można określić opcjonalną listę parametrów (par nazw i wartości) oraz limit czasu.

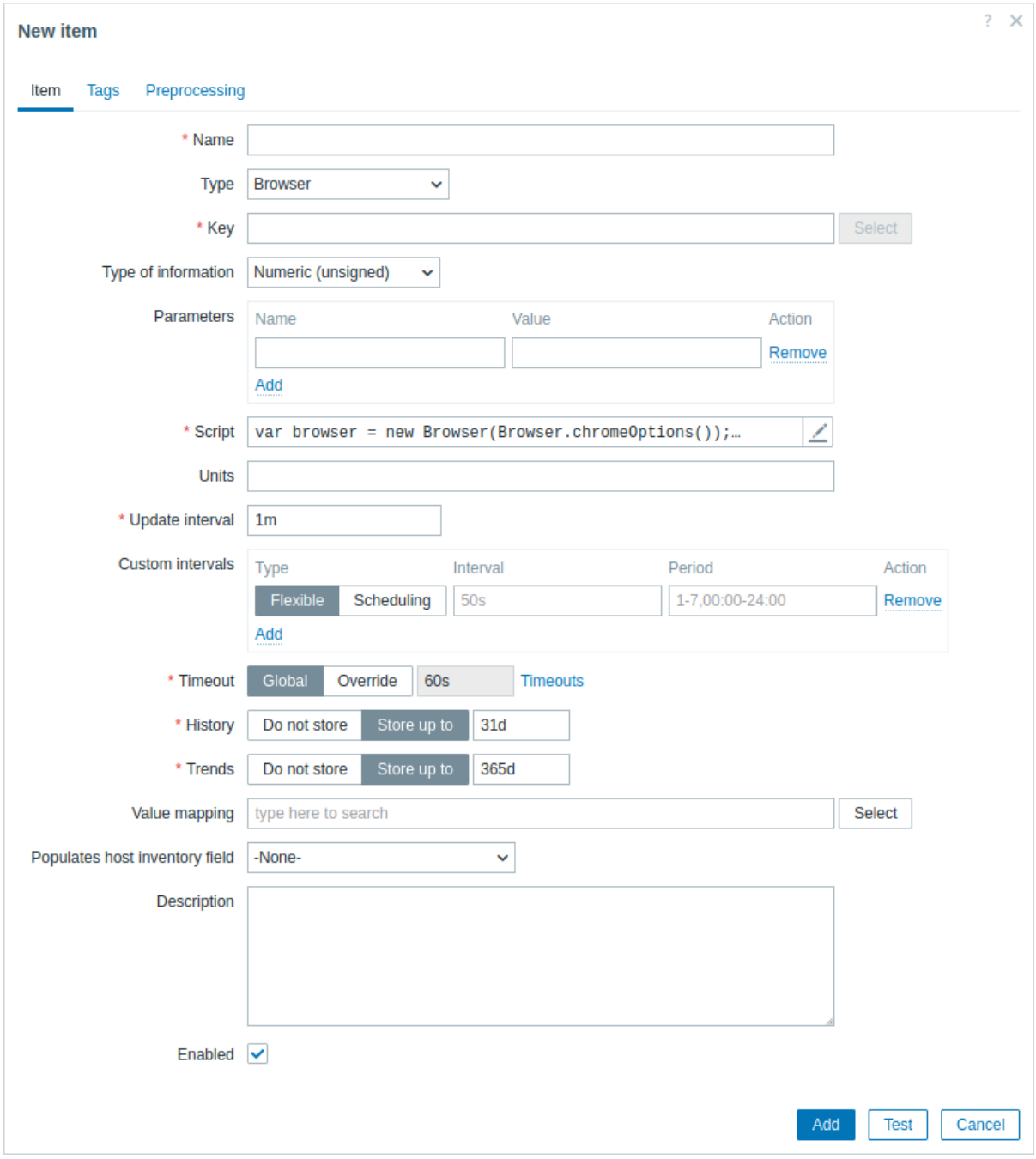
Attention:
Pozycja częściowo implementuje standard W3C WebDriver standard z użyciem Selenium Server lub zwykłego WebDrivera (na przykład ChromeDriver) jako punktu końcowego testów webowych. Aby pozycja działała, ustaw punkt końcowy w parametrze `WebDriverURL` pliku konfiguracyjnego Zabbix server/proxy (jeśli używasz ChromeDrivera, zobacz Security Considerations). Aby uzyskać lepszą wydajność, rozważ użycie dedykowanego serwera dla środowiska testów webowych.

Kontrole pozycji przeglądarki są wykonywane i przetwarzane przez pollery przeglądarki Zabbix server lub proxy. W razie potrzeby możesz dostosować liczbę wstępnie tworzonych instancji pollerów przeglądarki w parametrze `StartBrowserPollers` pliku konfiguracyjnego Zabbix server/proxy.

Do monitorowania złożonych witryn internetowych i aplikacji webowych dostępny jest szablon Website by Browser jako gotowy szablon.

Konfiguracja

W polu *Type* formularza konfiguracji pozycji wybierz Browser, a następnie wypełnij wymagane pola.



Wszystkie obowiązkowe pola wejściowe są oznaczone czerwoną gwiazdką.

Pola wymagające określonych informacji dla pozycji Browser to:

Field	Description
Key	Wprowadź unikalny klucz, który będzie używany do identyfikacji pozycji.
Parameters	Określ zmienne, które mają zostać przekazane do skryptu jako pary atrybut-wartość. Obsługiwane są makra użytkownika. Aby sprawdzić, które wbudowane makra są obsługiwane, wyszukaj frazę "Browser-type item" w tabeli obsługiwanych makr.
Script	Wprowadź kod JavaScript w modalnym edytorze, który otwiera się po kliknięciu w pole parametru lub ikonę ołówka obok niego. Kod ten musi zawierać logikę zwracania wartości metryki. Kod ma dostęp do wszystkich parametrów, wszystkich dodatkowych obiektów JavaScript oraz obiektów JavaScript pozycji Browser dodanych przez Zabbix. Zobacz także: Przewodnik po JavaScript.
Timeout	Limit czasu wykonania JavaScript (1-600 s; jego przekroczenie spowoduje zwrócenie błędu). Należy pamiętać, że w zależności od skryptu wyzwolenie limitu czasu może potrwać dłużej. Więcej informacji o parametrze *Timeout* można znaleźć w sekcji ogólnych atrybutów pozycji.

Przykłady

Przykład konfiguracji Zabbix do monitorowania stron internetowych przy użyciu szablonu *Website by Browser* można znaleźć w Monitor websites with Browser items.

Domyślny skrypt

Poniższy skrypt:

1. Inicjalizuje sesję przeglądarki.
2. Przechodzi pod określony adres URL.
3. Zbiera wpisy wydajności i statystyki sesji, a następnie zwraca je jako ciąg JSON.

W polu *Skrypt* wprowadź:

```
var browser = new Browser(Browser.chromeOptions());

try {
    browser.navigate("http://example.com");
    browser.collectPerfEntries();
}
finally {
    return JSON.stringify(browser.getResult());
}
```

Inicjalizacja przeglądarki z niestandardowymi capabilities

Poniższy skrypt:

1. Inicjalizuje sesję przeglądarki dla dostępnej przeglądarki na podstawie pierwszej pasującej przeglądarki zgodnie z kolejnością określoną w skrypcie.
2. Definiuje capabilities przeglądarki, w tym strategię ładowania strony oraz opcje specyficzne dla każdej przeglądarki, takie jak tryb headless dla przeglądarek Chrome, Firefox i Microsoft Edge.

W polu *Script* wprowadź:

```
var browser = new Browser({
    "capabilities":{
        "firstMatch":[
            {
                "browserName":"chrome",
                "pageLoadStrategy":"normal",
                "goog:chromeOptions":{
                    "args":[
                        "--headless=new"
                    ]
                }
            },
            {
                "browserName":"firefox",
                "pageLoadStrategy":"normal",
                "moz:firefoxOptions":{
                    "args":[
```

```
                    "--headless"
                ]
            }
        },
        {
            "browserName":"MicrosoftEdge",
            "pageLoadStrategy":"normal",
            "ms:edgeOptions":{
                "args":[
                    "--headless=new"
                ]
            }
        },
        {
            "browserName":"safari",
            "pageLoadStrategy":"normal"
        }
    ]
  }
});
```

Inicjalizacja przeglądarki z GUI

Domyślnie sesje przeglądarki (z wyjątkiem Safari) są inicjalizowane w trybie headless, co oznacza, że graficzny interfejs użytkownika (GUI) przeglądarki nie jest wyświetlany.

Poniższy skrypt inicjalizuje sesję przeglądarki z włączonym GUI.

Pamiętaj, że jeśli WebDriver nie może zlokalizować pliku binarnego przeglądarki, możesz ręcznie określić ścieżkę.

```
var opts = Browser.chromeOptions();
opts.capabilities.alwaysMatch['goog:chromeOptions'].args = [];

// Aby zainicjalizować sesję Firefox z GUI, odkomentuj poniższe linie:
// var opts = Browser.firefoxOptions();
// opts.capabilities.alwaysMatch['moz:firefoxOptions'].binary = 'usr/bin/firefox';
// opts.capabilities.alwaysMatch['moz:firefoxOptions'].args = [];

// Aby zainicjalizować sesję Microsoft Edge z GUI, odkomentuj poniższe linie:
// var opts = Browser.edgeOptions();
// opts.capabilities.alwaysMatch['ms:edgeOptions'].binary = 'usr/bin/microsoft-edge';
// opts.capabilities.alwaysMatch['ms:edgeOptions'].args = [];

var browser = new Browser(opts);
```

> **Note:**
> Jeśli testy są uruchamiane na zdalnym serwerze lub w kontenerze, możesz użyć klienta Virtual Network Computing (VNC), aby połączyć się z serwerem VNC tej maszyny. Pozwala to zdalnie wyświetlać GUI przeglądarki i wchodzić z nim w interakcję.

Wykonywanie zrzutów ekranu

Poniższy skrypt:

1. Inicjalizuje sesję przeglądarki.
2. Ustawia rozmiar obszaru roboczego przeglądarki w celu określenia rozmiaru zrzutu ekranu (określonego jako parametry, patrz poniżej).
3. Przechodzi do adresu URL (określonego jako parametr, patrz poniżej).
4. Zbiera statystyki sesji, wykonuje zrzut ekranu i dodaje go do zebranych statystyk.
5. Obsługuje błędy, przechwytując komunikaty o błędach i zrzut ekranu.
6. Zwraca zebrane wyniki jako ciąg JSON.

Skrypt używa również parametrów z formularza konfiguracji pozycji:

- webURL - http://example.com
- width - 1920
- height - 1080

W polu *Script* wprowadź:

```
var browser, result;

var browser = new Browser(Browser.chromeOptions());

try {
    var params = JSON.parse(value); // Parse the JSON string containing parameters passed from Zabbix.

    browser.setScreenSize(Number(params.width), Number(params.height))

    browser.navigate(params.webURL);

    result = browser.getResult();
    result.screenshot = browser.getScreenshot();
}
catch (err) {
    if (!(err instanceof BrowserError)) {
        browser.setError(err.message);
    }
    result = browser.getResult();
    result.error.screenshot = browser.getScreenshot();
}
finally {
    return JSON.stringify(result);
}
```

Sprawdzenie logowania do Zabbix

Poniższy skrypt:

1. Inicjalizuje sesję przeglądarki.
2. Przechodzi do strony (określonej jako parametr, patrz poniżej).
3. Wprowadza nazwę użytkownika i hasło (określone jako parametry, patrz poniżej).
4. Wyszukuje i klika przycisk logowania.
5. Wyszukuje i klika przycisk wylogowania.
6. Zbiera dane wydajności przed logowaniem i po nim, a także po wylogowaniu.
7. Obsługuje błędy przez przechwytywanie komunikatów o błędach i zrzutu ekranu.
8. Zwraca zebrane wyniki jako ciąg JSON.

Skrypt używa również parametrów z formularza konfiguracji pozycji:

- webURL - http://{HOST.CONN}/index.php
- username - {$USERNAME}
- password - {$PASSWORD}

W polu *Script* wprowadź:

```
var browser, result;

browser = new Browser(Browser.chromeOptions());

try {
    var params = JSON.parse(value); // Parse the JSON string containing parameters passed from Zabbix.

    browser.navigate(params.webURL);
    browser.collectPerfEntries("open page");

    var el = browser.findElement("xpath", "//input[@id='name']");
    if (el === null) {
        throw Error("cannot find name input field");
    }
    el.sendKeys(params.username);

    el = browser.findElement("xpath", "//input[@id='password']");
    if (el === null) {
        throw Error("cannot find password input field");
```

```
    }
    el.sendKeys(params.password);

    el = browser.findElement("xpath", "//button[@id='enter']");
    if (el === null) {
        throw Error("cannot find login button");
    }
    el.click();

    browser.collectPerfEntries("login");

    el = browser.findElement("link text", "Sign out");
    if (el === null) {
        throw Error("cannot find logout button");
    }
    el.click();

    browser.collectPerfEntries("logout");

    result = browser.getResult();
}
catch (err) {
    if (!(err instanceof BrowserError)) {
        browser.setError(err.message);
    }
    result = browser.getResult();
    result.error.screenshot = browser.getScreenshot();
}
finally {
    return JSON.stringify(result);
}
```

Znajdowanie linków

Poniższy skrypt:

1. Inicjalizuje sesję przeglądarki.
2. Definiuje funkcję usuwania zduplikowanych elementów z tablicy (zobacz krok 5).
3. Przechodzi do strony (określonej przez parametry, patrz poniżej).
4. Znajduje linki na stronie.
5. Usuwa zduplikowane linki, aby zapewnić ich unikalność.
6. Wyodrębnia tylko linki zaczynające się od ”http”.
7. Formatuje wyodrębnione linki do określonej struktury.
8. Obsługuje błędy przez przechwytywanie komunikatów o błędach i zrzutu ekranu.
9. Zwraca zebrane wyniki jako ciąg JSON.

Skrypt używa również parametrów z formularza konfiguracji pozycji:

- scheme - {$WEBSITE.SCHEME}
- domain - {$WEBSITE.DOMAIN}
- path - {$WEBSITE.PATH}

W polu *Script* wprowadź:

```
var browser, result;

browser = new Browser(Browser.chromeOptions());

try {
    var params = JSON.parse(value);  // Parse the JSON string containing parameters passed from Zabbix.

    function uniq(a) {
        return a.sort().filter(function (item, pos, ary) {
            return !pos || item != ary[pos - 1];
        });
    }
```

```
    browser.navigate(params.scheme + '://' + params.domain + params.path);

    var el = browser.findElements("link text", "");
    var links = [];
    for (var n = 0; n < el.length; n++) {
        links.push(el[n].getAttribute('href'));
    }

    links = uniq(links);

    result = [];
    for (i = 0; i < links.length; i++) {
        if (links[i].match(/^http.*/)) {
            var row = {};
            row["{#URL}"] = links[i];
            result.push(row);
        }
    }
}
catch (err) {
    if (!(err instanceof BrowserError)) {
        browser.setError(err.message);
    }
    result = browser.getResult();
    result.error.screenshot = browser.getScreenshot();
}
finally {
    return JSON.stringify(result);
}
```

4 Historia i trendy

Przegląd

Historia i trendy to dwa sposoby przechowywania zebranych danych w Zabbix.

Podczas gdy historia przechowuje każdą zebraną wartość, trendy przechowują uśrednione informacje w ujęciu godzinowym i dlatego zużywają mniej zasobów.

Przechowywanie historii

Możesz ustawić, przez ile dni historia będzie przechowywana:

- we formularzu właściwości pozycji
- podczas masowej aktualizacji pozycji
- podczas konfigurowania zadań housekeepera

Wszelkie starsze dane zostaną usunięte przez housekeeper.

Ogólne, zdecydowane zalecenie jest takie, aby przechowywać historię przez możliwie najmniejszą liczbę dni i w ten sposób nie przeciążać bazy danych dużą liczbą wartości historycznych.

Zamiast przechowywać długą historię, możesz dłużej przechowywać dane trendów. Na przykład możesz przechowywać historię przez 14 dni, a trendy przez 5 lat.

Dobre wyobrażenie o tym, ile miejsca wymagają dane historii w porównaniu z danymi trendów, można uzyskać, odwołując się do strony dotyczącej rozmiaru bazy danych.

Przy krótszym okresie przechowywania historii nadal będzie można przeglądać starsze dane na wykresach, ponieważ do wyświetlania starszych danych wykresy będą używać wartości trendów.

> **Attention:**
> Jeśli historia jest ustawiona na '0', pozycja będzie aktualizować tylko pozycje zależne i inwentarz. Żadne funkcje wyzwalaczy nie będą obliczane, ponieważ obliczanie wyzwalaczy opiera się wyłącznie na danych historii.

Note:
Jako alternatywny sposób zachowania historii rozważ użycie funkcji eksportu historii modułów ładowalnych.

Przechowywanie trendów

Trendy to wbudowany mechanizm redukcji danych historycznych, który przechowuje minimalną, maksymalną, średnią oraz całkowitą liczbę wartości dla każdej godziny dla numerycznych typów danych.

Możesz ustawić, przez ile dni trendy będą przechowywane:

- we formularzu właściwości pozycji
- podczas masowej aktualizacji pozycji
- podczas konfigurowania zadań Housekeepera

Trendy zwykle mogą być przechowywane znacznie dłużej niż historia. Wszelkie starsze dane zostaną usunięte przez housekeeper.

Serwer Zabbix gromadzi dane trendów w czasie działania w pamięci podręcznej trendów, w miarę napływu danych. Serwer zapisuje trendy z **poprzedniej godziny** każdej pozycji do bazy danych (gdzie frontend może je znaleźć) w następujących sytuacjach:

- serwer otrzymuje pierwszą wartość pozycji z bieżącej godziny
- do końca bieżącej godziny pozostało 5 minut lub mniej, a nadal nie ma żadnych wartości pozycji z bieżącej godziny
- serwer zatrzymuje się

Aby zobaczyć trendy na wykresie, należy poczekać co najmniej do początku następnej godziny (jeśli pozycja jest aktualizowana często) i co najwyżej do końca następnej godziny (jeśli pozycja jest aktualizowana rzadko), czyli maksymalnie 2 godziny.

Gdy serwer zapisuje pamięć podręczną trendów i w bazie danych istnieją już trendy dla tej godziny (na przykład serwer został uruchomiony ponownie w połowie godziny), serwer musi używać instrukcji aktualizacji zamiast prostych instrukcji wstawiania. Dlatego w większych instalacjach, jeśli wymagane jest ponowne uruchomienie, zaleca się zatrzymanie serwera pod koniec jednej godziny i uruchomienie go na początku następnej godziny, aby uniknąć nakładania się danych trendów.

Tabele historii w żaden sposób nie uczestniczą w generowaniu trendów.

Attention:
Jeśli dla trendów ustawiono wartość „0”, serwer Zabbix w ogóle nie oblicza ani nie przechowuje trendów.

Note:
Trendy są obliczane i przechowywane z użyciem tego samego typu danych co oryginalne wartości. W rezultacie obliczenia wartości średniej dla wartości typu unsigned są zaokrąglane, a im mniejszy jest przedział wartości, tym mniej precyzyjny będzie wynik. Na przykład, jeśli pozycja ma wartości 0 i 1, wartość średnia wyniesie 0, a nie 0,5.
Ponadto ponowne uruchomienie serwera może spowodować utratę precyzji obliczeń wartości średniej dla typu unsigned w bieżącej godzinie.

5 Parametry użytkownika

Przegląd

Czasami możesz chcieć uruchomić sprawdzenie agenta, które nie jest wstępnie zdefiniowane w Zabbix. W takich przypadkach z pomocą przychodzą parametry użytkownika.

Możesz napisać polecenie, które pobiera potrzebne dane, i umieścić je w parametrze użytkownika w pliku konfiguracyjnym agenta (parametr konfiguracyjny 'UserParameter').

Parametr użytkownika ma następującą składnię:

```
UserParameter=<key>,<command>
```

Jak widać, parametr użytkownika zawiera również klucz. Klucz będzie potrzebny podczas konfigurowania pozycji. Wprowadź wybrany przez siebie klucz, do którego łatwo będzie się odwołać (musi być unikalny w obrębie hosta).

Uruchom ponownie agent lub użyj opcji kontroli w czasie wykonywania agenta, aby wczytać nowy parametr, np.:

```
zabbix_agentd -R userparameter_reload
```

Następnie podczas konfigurowania pozycji wprowadź klucz, aby odwołać się do polecenia z parametru użytkownika, które ma zostać wykonane.

Parametry użytkownika to polecenia wykonywane przez agent Zabbix. Należy pamiętać, że przed etapami wstępnego przetwarzania wartości pozycji może zostać zwrócone do 16 MB danych.

W systemach operacyjnych UNIX jako interpreter wiersza poleceń używany jest **/bin/sh**. Parametry użytkownika podlegają limitowi czasu sprawdzenia agenta; jeśli limit czasu zostanie osiągnięty, rozwidlony proces parametru użytkownika zostanie zakończony.

Zobacz także:

- Samouczek krok po kroku dotyczący korzystania z parametrów użytkownika
- Wykonywanie poleceń

Przykłady prostych parametrów użytkownika

Proste polecenie:

```
UserParameter=ping,echo 1
```

agent będzie zawsze zwracał '1' dla pozycji z kluczem 'ping'.

Bardziej złożony przykład:

```
UserParameter=mysql.ping,mysqladmin -uroot ping | grep -c alive
```

agent zwróci '1', jeśli serwer MySQL działa, w przeciwnym razie '0'.

Elastyczne parametry użytkownika

Elastyczne parametry użytkownika akceptują parametry wraz z kluczem. Dzięki temu elastyczny parametr użytkownika może stanowić podstawę do utworzenia kilku pozycji.

Elastyczne parametry użytkownika mają następującą składnię:

```
UserParameter=key[*],command
```

Parametr	Opis
Key	Unikalny klucz pozycji. [*] określa, że ten klucz akceptuje parametry w nawiasach kwadratowych. Parametry są podawane podczas konfigurowania pozycji.
Command	Polecenie, które ma zostać wykonane w celu obliczenia wartości klucza. *Tylko dla elastycznych parametrów użytkownika*: W poleceniu można używać odwołań pozycyjnych $1...$9, aby odwołać się do odpowiedniego parametru w kluczu pozycji. Zabbix analizuje parametry ujęte w [ ] klucza pozycji i odpowiednio podstawia $1,...,$9 w poleceniu. $0 zostanie zastąpione oryginalnym poleceniem (przed rozwinięciem $0,...,$9), które ma zostać uruchomione. Odwołania pozycyjne są interpretowane niezależnie od tego, czy są ujęte w podwójne (") czy pojedyncze (') cudzysłowy. Aby użyć odwołań pozycyjnych bez zmian, należy podać podwójny znak dolara — na przykład awk '{print $$2}'. W takim przypadku $$2 podczas wykonywania polecenia faktycznie zostanie zamienione na $2.

Attention:
Odwołania pozycyjne ze znakiem $ są wyszukiwane i zastępowane przez Zabbix agent tylko dla elastycznych parametrów użytkownika. Dla prostych parametrów użytkownika takie przetwarzanie odwołań jest pomijane i dlatego żadne cytowanie znaku $ nie jest konieczne.

Attention:
Niektóre znaki domyślnie nie są dozwolone w parametrach użytkownika. Pełną listę znaków można znaleźć w UnsafeUserParameters.

Przykład 1

Coś bardzo prostego:

```
UserParameter=ping[*],echo $1
```

Możemy zdefiniować nieograniczoną liczbę pozycji do monitorowania, wszystkie w formacie ping[coś].

- ping[0] - zawsze zwróci '0'
- ping[aaa] - zawsze zwróci 'aaa'

Przykład 2

Dodajmy więcej sensu!

```
UserParameter=mysql.ping[*],mysqladmin -u$1 -p$2 ping | grep -c alive
```

Ten parametr może być używany do monitorowania dostępności bazy danych MySQL. Możemy przekazać nazwę użytkownika i hasło:

```
mysql.ping[zabbix,our_password]
```

Przykład 3

Ile linii w pliku pasuje do wyrażenia regularnego?

```
UserParameter=wc[*],grep -c "$2" $1
```

Ten parametr może być używany do obliczania liczby linii w pliku.

```
wc[/etc/passwd,root]
wc[/etc/services,zabbix]
```

Wynik polecenia

Wartością zwracaną przez polecenie jest standardowe wyjście wraz ze standardowym wyjściem błędów wygenerowanym przez polecenie.

> **Attention:**
> Pozycja zwracająca tekst (informacje typu znakowego, log lub tekstowego) nie stanie się nieobsługiwana w przypadku standardowego wyjścia błędów.

Wartość zwracana jest ograniczona do 16 MB (włącznie z końcowymi białymi znakami, które są obcinane); obowiązują również ograniczenia bazy danych.

Parametry użytkownika zwracające tekst (informacje typu znakowego, log lub tekstowego) mogą również zwracać białe znaki. W przypadku nieprawidłowego wyniku pozycja stanie się nieobsługiwana.

1 Rozszerzanie agentów Zabbix

Ten samouczek zawiera instrukcje krok po kroku dotyczące rozszerzania funkcjonalności agenta Zabbix przy użyciu parametru użytkownika.

Krok 1

Napisz skrypt lub polecenie wiersza poleceń, aby pobrać wymagany parametr.

Na przykład możemy użyć następującego polecenia, aby uzyskać całkowitą liczbę zapytań wykonanych przez serwer MySQL:

```
mysqladmin -uroot status | cut -f4 -d":" | cut -f1 -d"S"
```

Po wykonaniu polecenie zwraca całkowitą liczbę zapytań SQL.

Krok 2

Dodaj polecenie do zabbix_agentd.conf:

```
UserParameter=mysql.questions,mysqladmin -uroot status | cut -f4 -d":" | cut -f1 -d"S"
```

mysql.questions jest unikalnym identyfikatorem. Może to być dowolny prawidłowy identyfikator klucza, na przykład *queries*.

Przetestuj ten parametr, używając agenta Zabbix z flagą "-t" (jeśli jest uruchamiany jako root, pamiętaj jednak, że agent może mieć inne uprawnienia po uruchomieniu jako demon):

```
zabbix_agentd -t mysql.questions
```

Krok 3

Przeładuj parametry użytkownika z pliku konfiguracyjnego, uruchamiając:

```
zabbix_agentd -R userparameter_reload
```

Możesz także ponownie uruchomić agent zamiast używać polecenia runtime control.

Przetestuj parametr za pomocą narzędzia zabbix_get.

Krok 4

Dodaj nową pozycję z kluczem Key=mysql.questions do monitorowanego hosta. Typ pozycji musi być ustawiony na Zabbix Agent lub Zabbix Agent (active).

Pamiętaj, że typ zwracanych wartości musi być poprawnie ustawiony na serwerze Zabbix. W przeciwnym razie Zabbix ich nie zaakceptuje.

6 Liczniki wydajności systemu Windows

Przegląd

Możesz skutecznie monitorować liczniki wydajności systemu Windows za pomocą klucza *perf_counter[]*.

Na przykład:

```
perf_counter["\Processor(0)\Interrupts/sec"]
```

lub

```
perf_counter["\Processor(0)\Interrupts/sec", 10]
```

Aby uzyskać więcej informacji o użyciu tego klucza lub jego odpowiednika dostępnego wyłącznie w języku angielskim, `perf_counter_en`, zobacz klucze pozycji specyficzne dla systemu Windows.

Aby uzyskać pełną listę liczników wydajności dostępnych do monitorowania, możesz uruchomić:

```
typeperf -qx
```

Możesz również użyć wykrywania niskiego poziomu do wykrywania wielu instancji obiektów liczników wydajności systemu Windows i zautomatyzować tworzenie pozycji perf_counter dla obiektów z wieloma instancjami.

Reprezentacja numeryczna

Windows utrzymuje numeryczne reprezentacje (indeksy) nazw obiektów i liczników wydajności. Zabbix obsługuje te reprezentacje numeryczne jako parametry w kluczach pozycji `perf_counter`, `perf_counter_en` oraz w parametrach konfiguracyjnych `PerfCounter`, `PerfCounterEn`.

Nie zaleca się jednak ich używania, chyba że możesz zagwarantować, że Twoje indeksy numeryczne są mapowane na poprawne ciągi znaków na określonych hostach. Jeśli chcesz utworzyć przenośne pozycje, które działają na różnych hostach z różnymi zlokalizowanymi wersjami Windows, możesz użyć klucza `perf_counter_en` lub parametru konfiguracyjnego `PerfCounterEn`, które pozwalają używać nazw angielskich niezależnie od ustawień regionalnych systemu.

Aby znaleźć odpowiedniki numeryczne, uruchom **regedit**, a następnie znajdź *Counter* w *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\009*.

Wpis rejestru zawiera informacje takie jak poniżej:

```
1
1847
2
System
4
Memory
6
% Processor Time
10
File Read Operations/sec
12
File Write Operations/sec
14
File Control Operations/sec
16
File Read Bytes/sec
18
File Write Bytes/sec
....
```

Tutaj możesz znaleźć odpowiadające numery dla każdej części tekstowej licznika wydajności, jak w '\System\% Processor Time':

```
System → 2
% Processor Time → 6
```

Następnie możesz użyć tych numerów, aby przedstawić ścieżkę w postaci liczbowej:

\2\6

Parametry licznika wydajności

Możesz wdrożyć niektóre parametry PerfCounter do monitorowania liczników wydajności systemu Windows.

Na przykład możesz dodać je do pliku konfiguracyjnego agenta Zabbix:

```
PerfCounter=UserPerfCounter1,"\Memory\Page Reads/sec",30
or
PerfCounter=UserPerfCounter2,"\4\24",30
```

Po skonfigurowaniu tych parametrów możesz następnie po prostu użyć *UserPerfCounter1* lub *UserPerfCounter2* jako kluczy do utworzenia odpowiednich pozycji.

Pamiętaj, aby po wprowadzeniu zmian w pliku konfiguracyjnym zrestartować agent Zabbix.

7 Aktualizacja masowa

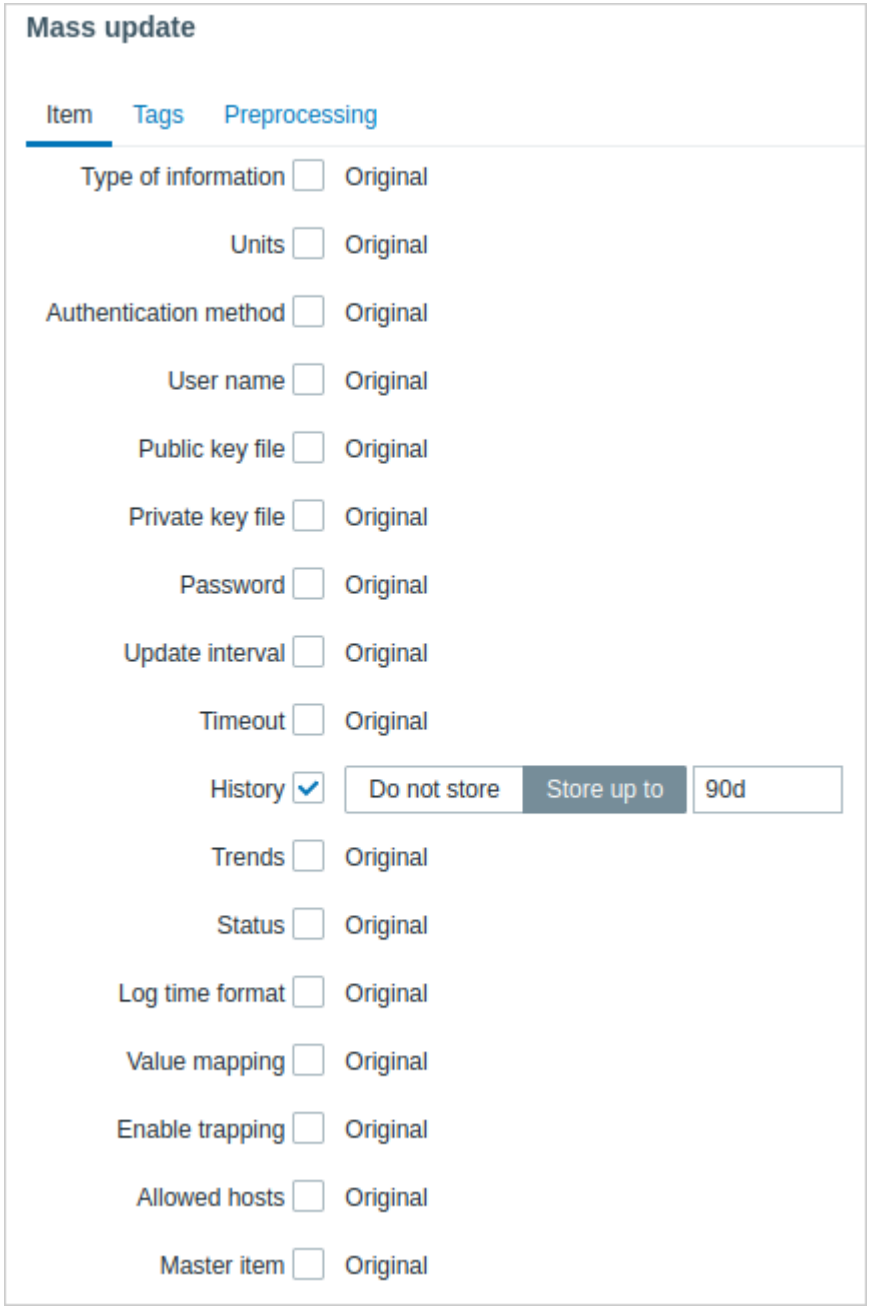
Przegląd

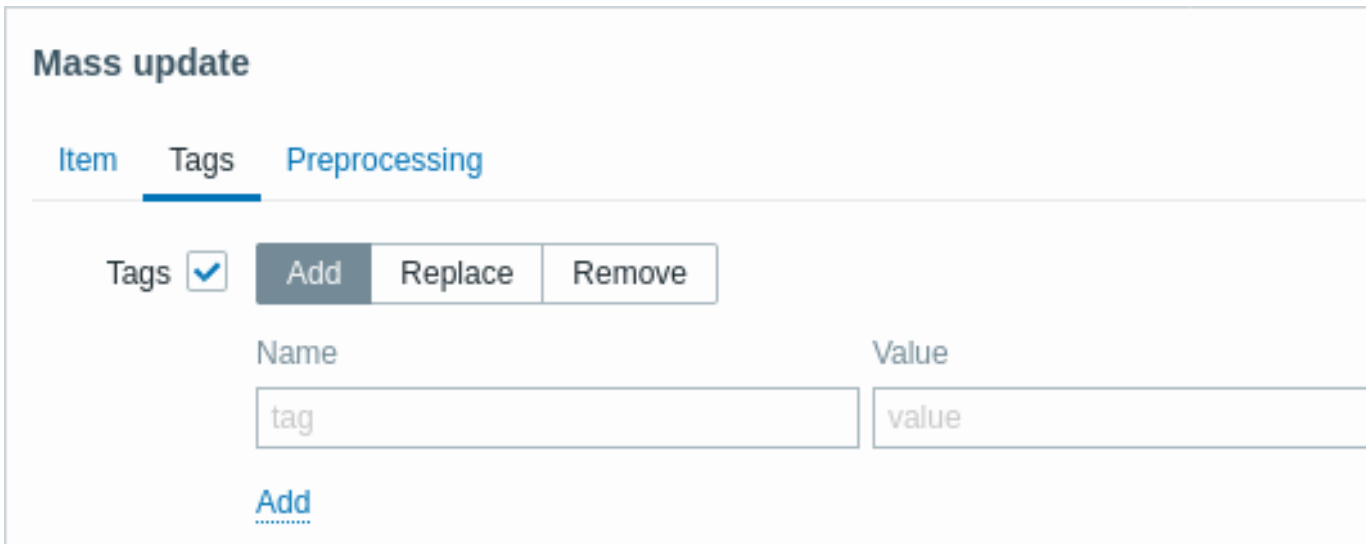
Czasami możesz chcieć zmienić jakiś atrybut dla wielu pozycji jednocześnie. Zamiast otwierać każdą pojedynczą pozycję do edycji, możesz w tym celu użyć funkcji masowej aktualizacji.

Używanie aktualizacji masowej

Aby masowo zaktualizować niektóre pozycje, wykonaj następujące czynności:

- Zaznacz pola wyboru pozycji do zaktualizowania na liście
- Kliknij *Mass update* pod listą
- Przejdź do karty z wymaganymi atrybutami (*Item*, *Tags* lub *Preprocessing*)
- Zaznacz pola wyboru atrybutów do zaktualizowania
- Wprowadź nowe wartości atrybutów



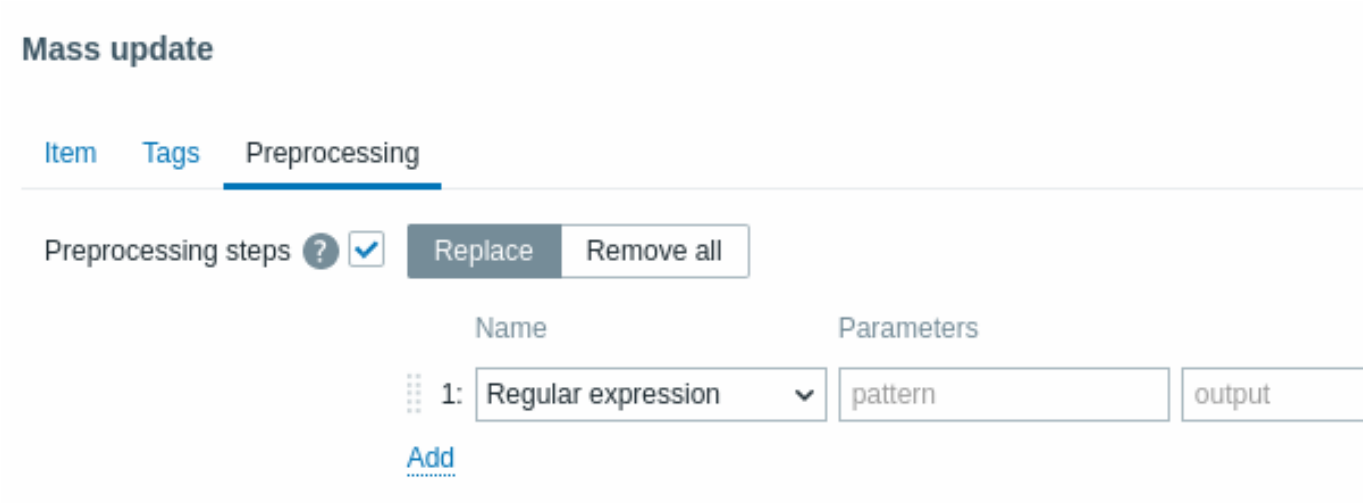


Opcja *Tags* umożliwia:

- *Add* — dodanie określonych tagów do pozycji (tagi o tej samej nazwie, ale różnych wartościach nie są uznawane za „duplikaty" i mogą zostać dodane do tej samej pozycji).
- *Replace* — usunięcie określonych tagów i dodanie tagów z nowymi wartościami

- *Remove* — usunięcie określonych tagów z pozycji

W tagach obsługiwane są makra użytkownika, makra {INVENTORY.*}, {HOST.HOST}, {HOST.NAME}, {HOST.CONN}, {HOST.DNS}, {HOST.IP}, {HOST.PORT} oraz {HOST.ID}.



Zaznacz pole wyboru obok *Preprocessing steps*, aby włączyć aktualizację masową kroków przetwarzania wstępnego.

Aktualizacja masowa *Preprocessing* umożliwia:

- *Replace* — zastąpienie istniejących kroków przetwarzania wstępnego w pozycjach krokami przetwarzania wstępnego określonymi poniżej
- *Remove all* — usunięcie wszystkich kroków przetwarzania wstępnego z pozycji

Po zakończeniu kliknij *Update*.

8 Mapowanie wartości

Przegląd

Mapowanie wartości umożliwia skonfigurowanie bardziej przyjaznej dla użytkownika reprezentacji otrzymanych wartości przy użyciu mapowań między wartościami numerycznymi/tekstowymi a ich reprezentacjami tekstowymi.

Na przykład, gdy wartość pozycji to „0” lub „1”, mapowania wartości mogą zostać użyte do przedstawienia tych wartości w bardziej przyjazny dla użytkownika sposób:

- 0 → Niedostępne
- 1 → Dostępne

Mapowania wartości dla typów kopii zapasowych danych mogą zostać skonfigurowane następująco:

- F → Pełna
- D → Różnicowa
- I → Przyrostowa

Zakresy wartości dla napięcia mogą zostać skonfigurowane następująco:

- <=209 → Niskie
- 210-230 → OK
- >=231 → Wysokie

Mapowanie wartości jest używane w frontendzie Zabbix oraz w powiadomieniach wysyłanych przez typy mediów.

Attention:
Podstawienie otrzymanej wartości skonfigurowaną reprezentacją jest wykonywane zarówno w frontendzie Zabbix, jak i na serwerze; jednak serwer obsługuje podstawienie tylko w następujących przypadkach:

- podczas wypełniania inwentarza hosta;
- podczas rozwijania obsługiwanych makr {ITEM.VALUE}, {ITEM.LASTVALUE}, {EVENT.OPDATA} oraz {EVENT.CAUSE.OPDATA}.

Mapowania wartości są konfigurowane w szablonach lub hostach. Po skonfigurowaniu są dostępne dla wszystkich pozycji w odpowiednim szablonie lub hoście. Podczas konfigurowania pozycji należy podać nazwę wcześniej skonfigurowanego mapowania wartości w parametrze *Mapowanie wartości*.

Note:
Nie ma dziedziczenia mapowań wartości — hosty i szablony nie dziedziczą mapowań wartości z podłączonych szablonów. Pozycje szablonu na hoście będą nadal używać mapowań wartości skonfigurowanych w szablonie.

Note:
Mapowania wartości mogą być używane z pozycjami mającymi typ informacji *Numeric (unsigned)*, *Numeric (float)* oraz *Character*.

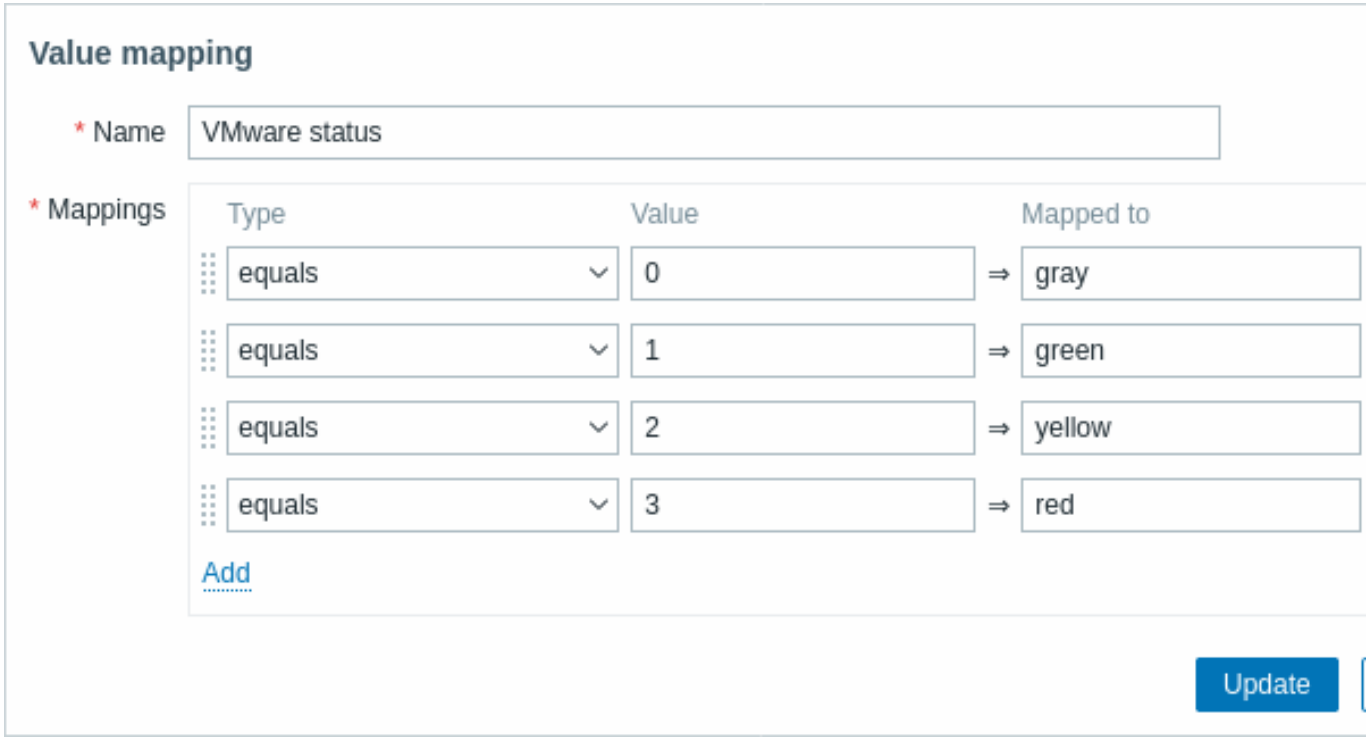
Mapowania wartości są eksportowane/importowane wraz z odpowiednim szablonem lub hostem. Mogą również być masowo aktualizowane przy użyciu formularzy masowej aktualizacji hosta i szablonu.

Konfiguracja

Aby skonfigurować mapowanie wartości, wykonaj następujące kroki:

1. Otwórz formularz konfiguracji hosta lub szablonu.

2. Na karcie *Mapowanie wartości* kliknij *Dodaj*, aby dodać nowe mapowanie wartości, lub kliknij nazwę istniejącego mapowania, aby je edytować.



Parametry mapowania wartości:

Parametr	Opis
Nazwa	Unikalna nazwa zestawu mapowań wartości.
Mapowania	Poszczególne reguły mapowania wartości numerycznych/ciągów znaków na reprezentacje tekstowe. Mapowanie jest stosowane zgodnie z kolejnością reguł, którą można zmieniać przez przeciąganie.

Parametr	Opis
Typ	Typ mapowania: **równa się** - równe wartości zostaną zmapowane; **jest większe lub równe** - równe lub większe wartości zostaną zmapowane; **jest mniejsze lub równe** - równe lub mniejsze wartości zostaną zmapowane; **w zakresie** - wartości z zakresu zostaną zmapowane; zakres jest wyrażany jako <number1>-<number2> lub <number>; obsługiwanych jest wiele zakresów (na przykład 1-10,101-110,201); **regexp** - wartości odpowiadające wyrażeniu regularnemu zostaną zmapowane (globalne wyrażenia regularne nie są obsługiwane); **domyślne** - wszystkie pozostałe wartości zostaną zmapowane, inne niż te ze zdefiniowanymi mapowaniami. W przypadku mapowania zakresów obsługiwane są tylko numeryczne typy wartości (*jest większe lub równe*, *jest mniejsze lub równe*, *w zakresie*).
Wartość	Wartość przychodząca (może zawierać zakres lub wyrażenie regularne, w zależności od typu mapowania).
Mapowane na	Reprezentacja tekstowa (do 64 znaków) dla wartości przychodzącej.

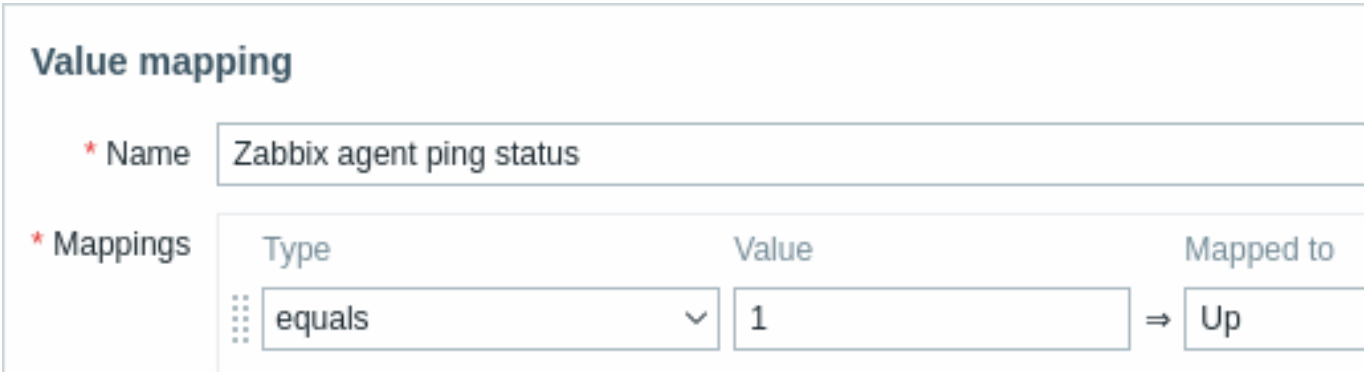
Wszystkie obowiązkowe pola wejściowe są oznaczone czerwoną gwiazdką.

Podczas wyświetlania mapowania wartości na liście widoczne są tylko pierwsze trzy mapowania, a trzy kropki wskazują, że istnieją kolejne mapowania.



Przykład mapowania wartości

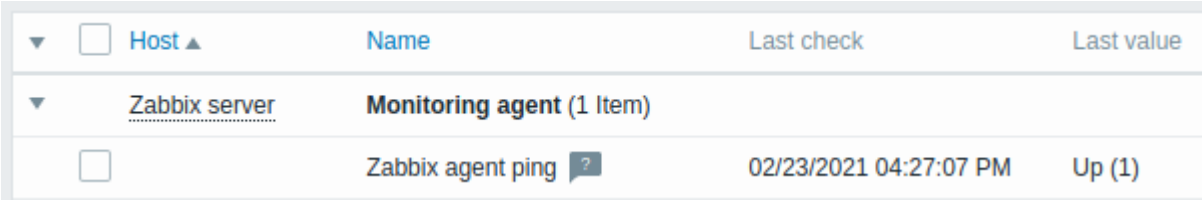
Jedna ze wstępnie zdefiniowanych pozycji agenta, *Zabbix agent ping*, używa mapowania wartości na poziomie szablonu „Zabbix agent ping status” do wyświetlania swoich wartości.



W formularzu konfiguracji pozycji można znaleźć odwołanie do tego mapowania wartości w polu *Mapowanie wartości*:

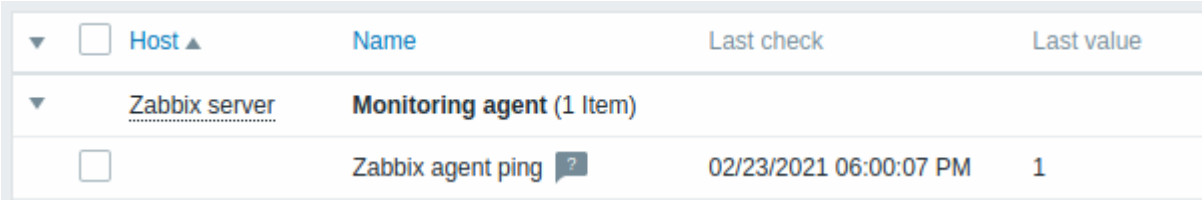


To mapowanie jest używane w sekcji *Monitoring* → *Najnowsze dane* do wyświetlania „Up” (z surową wartością w nawiasach).



Note:
W sekcji *Najnowsze dane* wyświetlane wartości są skracane do 20 znaków. Jeśli używane jest mapowanie wartości, to skrócenie nie jest stosowane do zmapowanej wartości, lecz tylko do surowej wartości (wyświetlanej w nawiasach).

Bez wstępnie zdefiniowanego mapowania wartości widoczne byłoby tylko „1”, co mogłoby być trudne do zrozumienia.



9 Kolejka

Przegląd

Kolejka wyświetla pozycje oczekujące na odświeżenie. Kolejka jest tylko **logiczną** reprezentacją danych. W Zabbix nie ma kolejki IPC ani żadnego innego mechanizmu kolejkowania.

Pozycje monitorowane przez proxy są również uwzględniane w kolejce — będą liczone jako oczekujące w okresie aktualizacji danych historycznych proxy.

W kolejce wyświetlane są tylko pozycje z zaplanowanymi czasami odświeżania. Oznacza to, że następujące typy pozycji są wykluczone z kolejki:

- aktywne pozycje log, logrt i event log agenta Zabbix
- pozycje SNMP trap
- pozycje trapper
- pozycje monitorowania WWW
- pozycje zależne

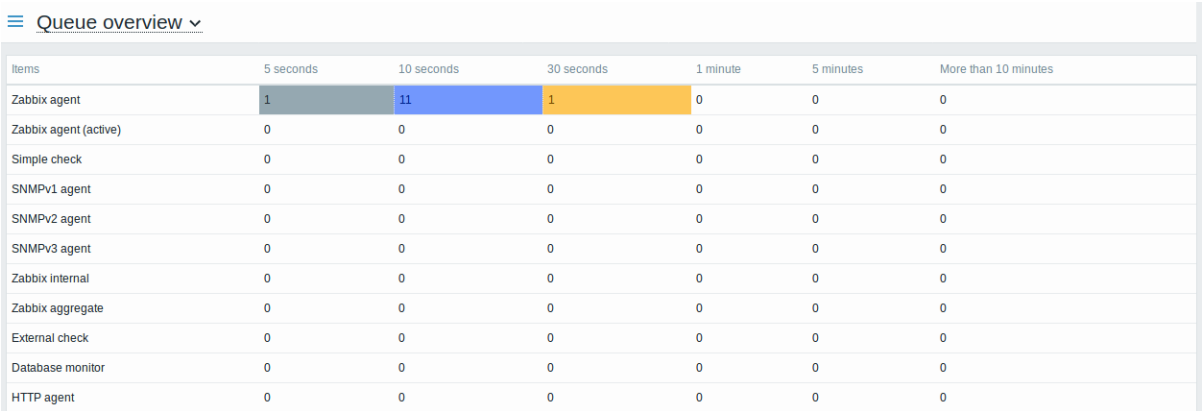
Statystyki pokazywane przez kolejkę są dobrym wskaźnikiem wydajności serwera Zabbix.

Kolejka jest pobierana bezpośrednio z serwera Zabbix przy użyciu protokołu JSON. Informacje są dostępne tylko wtedy, gdy serwer Zabbix jest uruchomiony.

Attention:
Pozycje nie są uwzględniane w kolejce, jeśli interfejs pozycji staje się niedostępny z powodu problemów z połączeniem lub nieprawidłowego działania agenta.

Odczytywanie kolejki

Aby odczytać kolejkę, przejdź do *Administration* > *Queue* > *Queue overview*.



Obraz tutaj jest ogólnie „ok”, więc możemy założyć, że serwer działa prawidłowo.

Kolejka pokazuje niektóre pozycje oczekujące do 30 sekund. Dobrze byłoby wiedzieć, jakie to pozycje.

Aby to sprawdzić, wybierz *Queue details* z rozwijanego menu w tytule. Teraz możesz zobaczyć listę tych opóźnionych pozycji.

Queue details

Scheduled check	Delayed by	Host	Name	Proxy
2019-09-02 11:46:40	58s	My host	CPU idle time	Remote proxy
2019-09-02 11:46:41	57s	My host	CPU interrupt time	Remote proxy
2019-09-02 11:46:42	56s	My host	CPU iowait time	Remote proxy
2019-09-02 11:46:43	55s	My host	CPU nice time	Remote proxy
2019-09-02 11:46:44	54s	My host	CPU softirq time	Remote proxy
2019-09-02 11:46:45	53s	My host	CPU steal time	Remote proxy
2019-09-02 11:46:46	52s	My host	CPU system time	Remote proxy

Mając te szczegóły, może być możliwe ustalenie, dlaczego te pozycje są opóźnione.

W przypadku jednej lub dwóch opóźnionych pozycji prawdopodobnie nie ma powodów do niepokoju. Mogą zostać zaktualizowane za sekundę. Jednak jeśli widzisz wiele pozycji opóźnionych zbyt długo, może to oznaczać poważniejszy problem.

Zobacz także: Wyrównywanie stref czasowych podczas używania scheduling intervals.

Queue overview

Items	5 seconds	10 seconds	30 seconds	1 minute	5 minutes	More than 10 minutes
Zabbix agent	0	1	1	26	0	0
Zabbix agent (active)	0	0	0	0	0	0
Simple check	0	0	0	0	0	0
SNMPv1 agent	0	0	0	0	0	0
SNMPv2 agent	0	0	0	0	0	0
SNMPv3 agent	0	0	0	0	0	0
Zabbix internal	0	0	0	0	0	0
Zabbix aggregate	0	0	0	0	0	0
External check	0	0	0	0	0	0
Database monitor	0	0	0	0	0	0
HTTP agent	0	0	0	0	0	0
IPMI agent	0	0	0	0	0	0
SSH agent	0	0	0	0	0	0
TELNET agent	0	0	0	0	0	0
JMX agent	0	0	0	0	0	0
Calculated	0	0	0	0	0	0

Pozycja kolejki

Specjalna wewnętrzna pozycja **zabbix[queue,<from>,<to>]** może być używana do monitorowania stanu kolejki w Zabbix. Zwraca liczbę pozycji opóźnionych o ustawiony czas. Więcej informacji można znaleźć w sekcji Pozycje wewnętrzne.

10 Cache wartości

Przegląd

Aby znacznie przyspieszyć obliczanie wyrażeń wyzwalaczy, pozycji obliczanych oraz niektórych makr, serwer Zabbix obsługuje opcję pamięci podręcznej wartości.

Ta pamięć podręczna w pamięci operacyjnej może być używana do uzyskiwania dostępu do danych historycznych zamiast wykonywania bezpośrednich wywołań SQL do bazy danych. Jeśli wartości historyczne nie są obecne w pamięci podręcznej, brakujące wartości są pobierane z bazy danych, a pamięć podręczna jest odpowiednio aktualizowana.

Wartości pozycji pozostają w pamięci podręcznej wartości do momentu, gdy:

- pozycja zostanie usunięta (wartości z pamięci podręcznej są usuwane po następnej synchronizacji konfiguracji);
- wartość pozycji znajdzie się poza zakresem czasu lub liczby określonym w wyrażeniu wyzwalacza/obliczanej pozycji (wartość z pamięci podręcznej jest usuwana po odebraniu nowej wartości);
- zakres czasu lub liczby określony w wyrażeniu wyzwalacza/obliczanej pozycji zostanie zmieniony tak, że do obliczeń wymagane będzie mniej danych (niepotrzebne wartości z pamięci podręcznej są usuwane po 24 godzinach).

Note:
Stan pamięci podręcznej wartości można obserwować za pomocą opcji runtime control serwera `diaginfo` (lub `diaginfo=valuecache`) oraz sprawdzając sekcję z informacjami diagnostycznymi pamięci podręcznej wartości. Może to być przydatne przy określaniu błędnie skonfigurowanych wyzwalaczy lub obliczanych pozycji.

Aby włączyć funkcjonalność pamięci podręcznej wartości, w pliku konfiguracji serwera Zabbix obsługiwany jest opcjonalny parametr **ValueCacheSize**.

Do monitorowania pamięci podręcznej wartości obsługiwane są dwie wewnętrzne pozycje: **zabbix[vcache,buffer,<mode>]** oraz **zabbix[vcache,cache,<parameter>]**. Więcej szczegółów można znaleźć w sekcji pozycje wewnętrzne.

11 Wykonaj teraz

Przegląd

Opcja *Wykonaj teraz* umożliwia natychmiastowe wykonywanie kontroli pasywnych.

Pobieranie wartości pozycji w Zabbix odbywa się zgodnie ze skonfigurowanymi interwałami aktualizacji. Niektóre pozycje (np. reguły wykrywania niskopoziomowego) mają długie interwały i może być konieczne natychmiastowe pobranie nowej wartości — na przykład w celu wykrycia zmian w wykrywalnych zasobach.

Opcja *Wykonaj teraz* jest obsługiwana dla następujących typów pozycji:

- agent Zabbix (pasywny)
- Kontrola prosta
- agent SNMP (v1/v2/v3)
- Wewnętrzny Zabbix
- Kontrola zewnętrzna
- Monitor bazy danych
- agent HTTP
- agent IPMI
- agent SSH
- agent TELNET
- agent JMX
- Obliczana
- Pozycja zależna
- Skrypt
- Przeglądarka

Jeśli pozycja jest typu „Pozycja zależna”, jej pozycja nadrzędna również musi być jednym z powyższych typów.

Konfiguracja

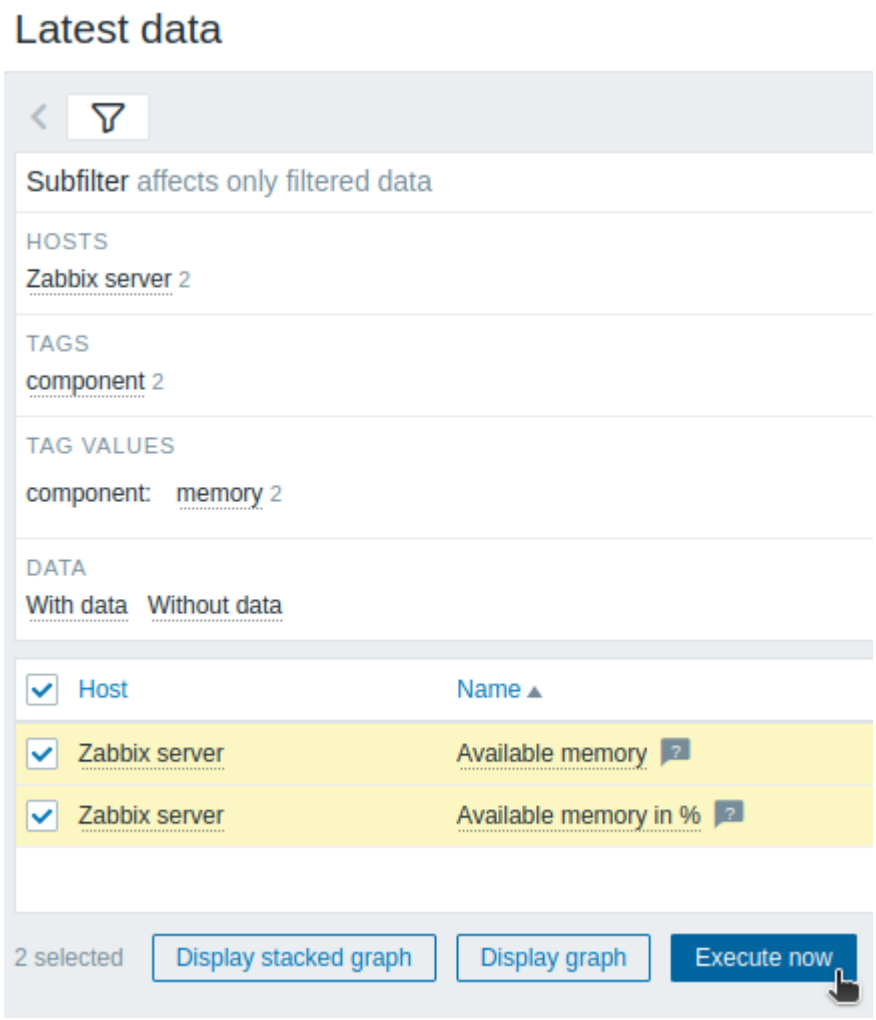
Możesz wykonywać pasywne sprawdzenia z poziomu:

- *Monitoring* > *Najnowsze dane*
- *Zbieranie danych* > *Hosty* > *Pozycje* lub *Odkrywanie*
- menu pozycji
- Podczas edycji pozycji lub reguł wykrywania niskiego poziomu (w ich formularzach konfiguracyjnych)

Attention:
Sprawdzenie musi istnieć w pamięci podręcznej konfiguracji, aby mogło zostać wykonane; zobacz także CacheUpdateFrequency. Pamięć podręczna **nie jest aktualizowana** przed wykonaniem sprawdzenia, więc ostatnie zmiany w konfiguracji pozycji lub reguły wykrywania niskiego poziomu nie zostaną uwzględnione. Aby testować pozycje lub reguły LLD, które są tworzone lub zostały właśnie utworzone, możesz zamiast tego użyć opcji Test.

Na przykład, aby wykonać pasywne sprawdzenie w *Monitoring* > *Najnowsze dane*:

1. Wybierz pozycje; możesz wykonać sprawdzenie dla wielu pozycji jednocześnie.
2. Kliknij *Wykonaj teraz*.



Note:
W sekcji *Najnowsze dane* użytkownicy mogą używać opcji *Wykonaj teraz* dla pozycji na hostach, do których mają uprawnienia odczyt-zapis, albo uprawnienia tylko do odczytu oraz włączoną dla swojej roli akcję Invoke "Execute now" on read-only hosts.

12 Ograniczanie kontroli agenta

Przegląd

Możesz kontrolować, których kluczy pozycji agent Zabbix lub agent 2 może używać albo których nie może używać podczas wykonywania kontroli pozycji, zdalnych poleceń lub skryptów.

Aby to zrobić, użyj tych parametrów konfiguracji agenta do zdefiniowania reguł zezwalania/odrzucania:

- `AllowKey=<pattern>`
- `DenyKey=<pattern>`

`<pattern>` musi zawierać pojedynczy klucz pozycji i obsługuje symbole wieloznaczne (`*`). Symbol wieloznaczny dopasowuje dowolną liczbę dowolnych znaków w swoim położeniu i może być używany do dopasowywania kluczy pozycji lub parametrów (np. `vfs.file.*[*]`).

Attention:
Aby zwiększyć bezpieczeństwo, zaleca się używanie dokładnych kluczy pozycji zamiast symboli wieloznacznych. Szczegóły znajdują się w sekcji Zabezpieczanie reguł zezwalania/odrzucania.

W przeciwieństwie do innych parametrów konfiguracji agenta możesz określić nieograniczoną liczbę parametrów `AllowKey` lub `DenyKey`.

Ważne uwagi

- Wszystkie pozycje `system.run` są domyślnie wyłączone (nawet gdy `DenyKey` jest puste), tak jakby `DenyKey=system.run[*]`

było ustawione jako ostatnia reguła. Z tego powodu możesz zezwolić na określone pozycje system.run bez jawnego zabraniania innych pozycji system.run.

- Pozycja określona w AllowKey musi być również określona w DenyKey (z wyjątkiem pozycji system.run); w przeciwnym razie agent Zabbix **nie uruchomi się**.
- Jeśli to możliwe, używaj AllowKey, aby zezwalać tylko na wymagane pozycje i zabraniać wszystkiego innego. Niektóre klucze mogą zostać wykorzystane do odczytu niezamierzonych plików poprzez przechodzenie po ścieżkach (np. vfs.file.contents["../../../../etc/passwd"]), a nowe wersje agenta Zabbix mogą wprowadzać klucze nieobjęte regułami DenyKey.
- Konfiguracja AllowKey i DenyKey nie wpływa na parametry agenta HostnameItem, HostMetadataItem ani HostInterfaceItem.
- Zabronione pozycje stają się nieobsługiwane bez żadnych wskazówek ani komunikatów o błędach; na przykład:
  - Parametr wiersza poleceń agenta Zabbix --print (-p) nie pokaże kluczy zabronionych pozycji.
  - Parametr wiersza poleceń agenta Zabbix --test (-t) zwróci „Unsupported item key." dla kluczy zabronionych pozycji.
  - Gdy rejestrowanie jest włączone (LogRemoteCommands=1), plik dziennika agenta Zabbix nie będzie rejestrować zabronionych zdalnych poleceń.

Kolejność reguł zezwalania/odmawiania

Możesz określić nieograniczoną liczbę reguł AllowKey lub DenyKey, jednak ich kolejność ma znaczenie.

- Reguły są oceniane jedna po drugiej, od góry do dołu.
- Gdy klucz pozycji pasuje do reguły, zostaje odpowiednio dozwolony lub zabroniony, a ocena reguł zostaje zatrzymana.

Na przykład podczas oceny vfs.file.contents[/etc/passwd] reguły są przetwarzane w następujący sposób:

```
AllowKey=vfs.file.contents[/tmp/app.log]    # Wzorzec klucza pozycji nie pasuje, agent przechodzi do nastę
AllowKey=vfs.file.contents[/etc/passwd]     # Wzorzec klucza pozycji pasuje; agent zezwala na sprawdzenie
DenyKey=vfs.file.*[*]                       # Agent ignoruje regułę, ponieważ ocena została zatrzymana.
```

Poniższa kolejność reguł spowoduje odmowę sprawdzenia pozycji:

```
DenyKey=vfs.file.*[*]                       # Wzorzec klucza pozycji pasuje; agent odmawia sprawdzenia poz
AllowKey=vfs.file.contents[/etc/passwd]     # Agent ignoruje regułę, ponieważ ocena została zatrzymana.
AllowKey=vfs.file.contents[/tmp/app.log]    # Agent ignoruje regułę, ponieważ ocena została zatrzymana.
```

Przykłady

Poniższe przykłady pokazują typowe wzorce konfiguracji dla AllowKey i DenyKey.

Zezwalanie na określone kontrole i polecenia

Zezwól tylko na dwie kontrole pozycji vfs.file i dwa polecenia system.run:

```
AllowKey=vfs.file.contents[/tmp/app.log]
AllowKey=vfs.file.size[/tmp/app.log]
AllowKey=system.run[/usr/bin/uptime]
AllowKey=system.run[/usr/bin/df -h /]
DenyKey=vfs.file.*[*]
```

Note:
Ustawienie DenyKey=system.run[*] nie jest konieczne, ponieważ wszystkie pozostałe polecenia system.run są domyślnie zabronione.

Zezwalanie na skrypty

Zezwól agentowi Zabbix na wykonywanie skryptów na hostach wszystkimi dostępnymi metodami:

- Skrypty globalne, które mogą być wykonywane we frontendzie lub przez API (ta metoda zawsze używa klucza system.run[myscript.sh])
- Zdalne polecenia z operacji akcji (ta metoda zawsze używa klucza system.run[myscript.sh,nowait])
- Pozycje agenta Zabbix system.run ze skryptem, na przykład:
  - system.run[myscript.sh]
  - system.run[myscript.sh,wait]
  - system.run[myscript.sh,nowait]

```
AllowKey=system.run[myscript.sh,*]
```

Aby kontrolować parametr `wait/nowait`, należy ustawić inną regułę. Na przykład można zezwolić tylko na pozycje `system.run[myscript.s` wykluczając w ten sposób inne metody:

```
AllowKey=system.run[myscript.sh,wait]
```

Zabezpieczanie reguł allow/deny

Ten przykład pokazuje, jak zabezpieczyć zbyt liberalne reguły `AllowKey` lub `DenyKey`.

Rozważ następujące reguły:

```
AllowKey=system.run["C:\Program^ Files\Zabbix^ Agent^ 2\scripts\test.bat*"]
DenyKey=vfs.file.*
DenyKey=system.cpu.load[*]
```

Note:
W systemie Windows spacje w ścieżce należy poprzedzać znakiem daszka (^).

Te reguły zawierają symbol wieloznaczny (*), który może zostać niewłaściwie wykorzystany:

- Skrypt `test.bat` może zostać uruchomiony z dowolnymi argumentami, w tym niezamierzonymi.
- Wzorzec `vfs.file.*` dopasowuje tylko klucze pozycji bez parametrów; jednak wszystkie pozycje `vfs.file` wymagają parametrów.
- Wzorzec `system.cpu.load[*]` dopasowuje tylko klucze pozycji z parametrami; jednak pozycje `system.cpu.load` nie wymagają parametrów.

Aby zabezpieczyć te reguły, jawnie zezwól na wykonywanie `test.bat` tylko z określonymi argumentami oraz zabroń poprawnych wzorców kluczy pozycji; na przykład:

```
AllowKey=system.run["C:\Program^ Files\Zabbix^ Agent^ 2\scripts\test.bat status"]
AllowKey=system.run["C:\Program^ Files\Zabbix^ Agent^ 2\scripts\test.bat version"]
DenyKey=vfs.file.*[*]
DenyKey=system.cpu.load
DenyKey=system.cpu.load[*]
```

Możesz przetestować reguły, uruchamiając następujące polecenia, które zwrócą `ZBX_NOTSUPPORTED`.

```
cd "C:\Program Files\Zabbix Agent 2"
zabbix_agent2.exe -t system.run["C:\Program^ Files\Zabbix^ Agent^ 2\scripts\test.bat debug"]
zabbix_agent2.exe -t vfs.file.size["C:\ProgramData\MyApp\config.ini"]
zabbix_agent2.exe -t vfs.file.contents["C:\Windows\System32\drivers\etc\hosts"]
zabbix_agent2.exe -t system.cpu.load
zabbix_agent2.exe -t system.cpu.load[all,avg1]
```

Przykłady wzorców

Poniższa tabela pokazuje, jak dopasowywane są wzorce kluczy pozycji:

- Klucz pasuje do wzorca tylko wtedy, gdy spełnia **wszystkie** warunki w kolumnie *Dopasowania*.
- Parametry muszą być w całości ujęte w nawiasy kwadratowe (np. `vfs.file.contents[*` i `vfs.file.contents*utf8]` są nieprawidłowymi wzorcami).

Wzorzec	Dopasowania	Przykłady
*	Dowolny klucz z parametrami lub bez parametrów	

vfs.file.*	Klucz zaczyna się od `vfs.file.`
	Brak parametrów
		Pasuje:
		`vfs.file.size`
		`vfs.file.contents`
		
		Nie pasuje:
		`vfs.file.contents[]`
		`vfs.file.size[/var/log/app.log]`

Wzorzec	Dopasowania	Przykłady

`vfs.*.contents`	Klucz zaczyna się od `vfs.`
	Klucz kończy się na `.contents`
	Brak parametrów
		Pasuje:
		`vfs..contents`
		`vfs.mount.point.file.contents`
		
		Nie pasuje:
		`vfs.contents`
		`vfs.file.contents[]`

`vfs.file.*[*]`	Klucz zaczyna się od `vfs.file.`
	Dowolne lub puste parametry
		Pasuje
		`vfs.file.get.custom[]`
		`vfs.file.size[/var/log/app.log, utf8]`
		
		Nie pasuje:
		`vfs.file.get.custom`

`vfs.file.contents`	Klucz to `vfs.file.contents`
	Brak parametrów
		Pasuje:
		`vfs.file.contents`
		
		Nie pasuje:
		`vfs.file.contents[/etc/passwd]`

`vfs.file.contents[]`	Klucz to `vfs.file.contents[]`
	Puste parametry
		Pasuje:
		`vfs.file.contents[]`
		
		Nie pasuje:
		`vfs.file.contents`

`vfs.file.contents[*]`	Klucz to `vfs.file.contents`
	Dowolne lub puste parametry
		Pasuje:
		`vfs.file.contents[/path/to/file]`
		
		Nie pasuje:
		`vfs.file.contents`

`vfs.file.contents[/etc/passwd,*]`	Klucz to `vfs.file.contents`
	Pierwszy parametr to `/etc/passwd`
	Dowolny lub pusty drugi parametr
		Pasuje:
		`vfs.file.contents[/etc/passwd,]`
		`vfs.file.contents[/etc/passwd,utf8]`
		
		Nie pasuje:
		`vfs.file.contents[]`
		`vfs.file.contents[/etc/passwd]`

`vfs.file.contents[*passwd*]`	Klucz to `vfs.file.contents`
	Pierwszy parametr zawiera `passwd`
	Brak drugiego parametru
		Pasuje:
		`vfs.file.contents[/etc/passwd]`
		
		Nie pasuje:
		`vfs.file.contents[/etc/passwd,]`
		`vfs.file.contents[/etc/passwd,utf8]`

`vfs.file.contents[*passwd*,*]`	Klucz to `vfs.file.contents`
	Pierwszy parametr zawiera `passwd`
	Dowolny lub pusty drugi parametr
		Pasuje:
		`vfs.file.contents[/etc/passwd,]`
		`vfs.file.contents[/etc/passwd,utf8]`
		
		Nie pasuje:
		`vfs.file.contents[/etc/passwd]`
		`vfs.file.contents[/tmp/test]`

`vfs.file.contents[/etc/passwd,utf8]`	Klucz to `vfs.file.contents`
	Pierwszy parametr to `/etc/passwd`
	Drugi parametr to `utf8`
		Pasuje:
		`vfs.file.contents[/etc/passwd,utf8]`
		
		Nie pasuje:
		`vfs.file.contents[/etc/passwd,]`
		`vfs.file.contents[/etc/passwd,utf16]`

3 Wykrywanie problemów za pomocą wyzwalaczy

Wykrywanie problemów w Zabbix opiera się na **wyzwalaczach**.

Wyzwalacz opisuje warunek problemu, umożliwiając Zabbix reakcję, jeśli problem wystąpi.

Pełny proces wykrywania problemów wygląda następująco:

1. Upewnij się, że masz pozycję zbierającą dane.
2. Zdefiniuj wyzwalacz dla tej pozycji. Bez wyzwalacza Zabbix tylko zbiera dane, ale nigdy na nie nie reaguje.
3. Obserwuj wykryte problemy:
    - W *Monitoring* > *Problems*
    - W widżecie *Problems* widget
4. Otrzymuj powiadomienia, wykonuj zdalne polecenia (jeśli zostały zdefiniowane).

Pamiętaj, że oficjalne szablony Zabbix zawierają wstępnie zdefiniowane wyzwalacze. Zobacz przewodnik dotyczący stosowania szablonu do monitorowania systemu Linux.

Czym jest „wyzwalacz”?

Wyzwalacz opisuje *warunek problemu* za pomocą wyrażenia wyzwalacza.

Warunek problemu, gdy wystąpi w rzeczywistości, oznacza, że wyzwalacz „uruchamia się” (w Zabbix tworzony jest problem).

Warunek problemu może być oparty na najnowszej wartości, wartości średniej, wykrytym ciągu znaków i wielu innych funkcjach. Wyzwalaczy nie można tworzyć dla pozycji zwracających wartości o typie danych binary lub JSON.

Proste wyrażenie wyzwalacza oblicza funkcję (na przykład `max()` dla wartości maksymalnej) dla danych określonych w nawiasach (zwykle pozycja danych i okno czasowe), a następnie porównuje wynik tego obliczenia z progiem.

Na przykład:

```
max(/host/vfs.fs.size[/,free],5m)<10G
```

Ten wyzwalacz uruchamia się, jeśli wolne miejsce na dysku, mierzone przez 5 minut, stale utrzymuje się poniżej 10 GB.

Wyzwalacz może mieć następujące stany:

Stan wyzwalacza	Opis	W Zabbix
OK	Wyrażenie wyzwalacza zostało obliczone jako „0” (lub FALSE)	Nie utworzono problemu Problem został rozwiązany (jeśli istniał)
Problem	Wyrażenie wyzwalacza zostało obliczone jako „1” (lub TRUE)	Utworzono problem

Czasami obliczenie wyrażenia wyzwalacza nie jest z jakiegoś powodu możliwe. Zobacz Nieznany stan wyrażenia.

Inne materiały:

- Przykłady wyzwalaczy
- Konfigurowanie wyzwalacza
- Najlepsze praktyki

Częstotliwość obliczeń

Wyzwalacz jest przeliczany za każdym razem, gdy serwer Zabbix otrzyma **nową wartość**, która jest częścią wyrażenia. Po otrzymaniu nowej wartości każda funkcja uwzględniona w wyrażeniu jest przeliczana (nie tylko ta, która otrzymała nową wartość).

Dodatkowo wyzwalacz jest przeliczany co 30 sekund (przez history syncer), jeśli wyrażenie zawiera:

- funkcje daty i czasu
- funkcję nodata()

Wyzwalacze zawierające wyłącznie funkcje trend są oceniane raz na najmniejszy okres czasu w wyrażeniu. Podczas gdy wiele funkcji wyzwalaczy używa danych historii wartości pozycji, funkcje trendów używają danych trendów.

1 Przykłady wyzwalaczy

Ta strona zawiera zbiór przykładów wyzwalaczy.

Przykłady są posortowane według przypadków użycia:

- Niedostępny host

- Niedostępny proxy
- Niedostępny klaster SMTP
- Nieosiągalny host
- Nieoczekiwany restart
- Zmiany w ważnych plikach
- Zmiany w zapytaniu DNS
- Niezgodne oprogramowanie na różnych hostach
- Niezsynchronizowane zegary
- Nieaktualny agent
- Niestabilny interfejs
- Wysoki ruch przychodzący
- Mało miejsca na dysku
- Mało miejsca na dysku (próg dynamiczny)
- Wysokie obciążenie CPU
- Porównanie obciążenia CPU
- Długoterminowe porównanie obciążenia CPU
- Ciąg znaków zawierający znaki specjalne

Wykrywanie niedostępnego hosta

```
max(/host/zabbix[host,agent,available],5m)=0
```

Ten wyzwalacz uruchamia się, jeśli agent Zabbix na hoście jest niedostępny przez 5 minut.
 Funkcja: `max`
 Pozycja danych: `zabbix[host,agent,available]`

Alternatywnie:

```
nodata(/host/agent.ping,5m)=1
```

Ten wyzwalacz uruchamia się, jeśli przez 5 minut nie odebrano żadnych danych od agenta Zabbix.
 Funkcja: `nodata`
 Pozycja danych: `agent.ping`

Wykrywanie niedostępnego proxy

```
fuzzytime(/host/zabbix[proxy,{$PROXY_NAME},lastaccess],1m)=0
```

Ten wyzwalacz uruchamia się, jeśli dane proxy Zabbix są opóźnione względem czasu serwera Zabbix o 1 minutę.
 Funkcja: `fuzzytime`
 Pozycja danych: `zabbix[proxy,{$PROXY_NAME},lastaccess]`

Wykrywanie niedostępnego klastra SMTP

```
last(/smtp1.example.com/net.tcp.service[smtp])=0 and last(/smtp2.example.com/net.tcp.service[smtp])=0
```

Ten wyzwalacz uruchamia się, jeśli oba serwery SMTP są niedostępne.
 Funkcja: `last`
 Pozycja danych: `net.tcp.service`

Wykrywanie nieosiągalnego hosta

```
count(/host/icmpping,30m,,"0")>5
```

Ten wyzwalacz uruchamia się, jeśli host jest nieosiągalny przez ping więcej niż 5 razy w ciągu ostatnich 30 minut.
 Funkcja: `count`
 Pozycja danych: `icmpping`

Wykrywanie nieoczekiwanego restartu

```
change(/host/system.uptime)<0
```

Ten wyzwalacz uruchamia się, jeśli zostanie wykryta ujemna zmiana wartości czasu działania systemu (co wskazuje na restart).
 Funkcja: `change`
 Pozycja danych: `system.uptime`

Wykrywanie zmian w ważnych plikach

```
last(/host/vfs.file.cksum[/etc/passwd],#1)<>last(/host/vfs.file.cksum[/etc/passwd],#2)
```

Ten wyzwalacz uruchamia się, jeśli plik `/etc/passwd` został zmieniony. Wyrażenie jest prawdziwe, gdy poprzednia suma kontrolna `/etc/passwd` różni się od najnowszej. Podobne wyrażenia mogą być przydatne do monitorowania zmian w ważnych plikach, takich jak `/etc/passwd`, `/etc/inetd.conf`, `/kernel` itd.
 Funkcja: `last`
 Pozycja danych: `vfs.file.cksum`

Wykrywanie zmian w zapytaniu DNS

```
last(/Zabbix server/net.dns.record[192.0.2.0,{$WEBSITE_NAME},{$DNS_RESOURCE_RECORD_TYPE},2,1])<>"{$WEBSITE
```

Zwróć uwagę na cudzysłowy wokół drugiego operandu.

Ten wyzwalacz uruchamia się, jeśli wynik zapytania nie jest równy temu, co zwykle zwraca:

```
example.com             MX       0 mail.example.com
```

Funkcja: last
 Pozycja danych: net.dns.record[192.0.2.0,{$WEBSITE_NAME},{$DNS_RESOURCE_RECORD_TYPE},2,1], z makrami zdefiniowanymi jako:

```
{$WEBSITE_NAME} = example.com
{$DNS_RESOURCE_RECORD_TYPE} = MX
```

Wykrywanie niezgodnego oprogramowania na różnych hostach

```
last(/host/vfs.file.contents[/etc/os-release])<>last(/host2/vfs.file.contents[/etc/os-release])
```

Ten wyzwalacz uruchamia się, jeśli wersja Ubuntu jest różna na różnych hostach. Zwróć uwagę, że operandami są tutaj funkcje zwracające ciągi znaków.
 Funkcja: last
 Pozycja danych: vfs.file.contents

Wykrywanie niezsynchronizowanych zegarów

```
fuzzytime(/host/system.localtime,10s)=0
```

Wyzwalacz uruchamia się, jeśli lokalny czas klienta i czas serwera Zabbix różnią się o więcej niż 10 sekund.
 Funkcja: fuzzytime
 Pozycja danych: system.localtime

Należy pamiętać, że system.localtime musi być skonfigurowana jako sprawdzenie pasywne dla agenta Zabbix; w Zabbix agent 2 może być skonfigurowana jako sprawdzenie aktywne.

Wykrywanie nieaktualnego agent

```
find(/host/agent.version,,"like","beta")=1
```

Ten wyzwalacz uruchamia się, jeśli Zabbix agent ma wersję beta. Zabbix agent wymaga aktualizacji.
 Funkcja: find
 Pozycja danych: agent.version

Wykrywanie niestabilnego interfejsu

```
changecount(/host/vfs.file.contents["/sys/class/net/eth0/operstate"],1h)>5
```

Ten wyzwalacz uruchamia się, jeśli stan operacyjny (up/down/unknown) interfejsu eth0 zmienił się więcej niż 5 razy w ciągu godziny.
 Funkcja: changecount
 Pozycja danych: vfs.file.contents

Wykrywanie wysokiego ruchu przychodzącego

```
min(/host/net.if.in[eth0,bytes],5m)>100K
```

Ten wyzwalacz uruchamia się, jeśli liczba odebranych bajtów na eth0 w ciągu ostatnich pięciu minut była zawsze większa niż 100 kilobajtów. Prawdopodobnie ktoś pobiera duży plik.
 Funkcja: min
 Pozycja danych: net.if.in[eth0,bytes]

Wykrywanie małej ilości wolnego miejsca na dysku

```
max(/host/vfs.fs.size[/,free],5m)<10G
```

Wyzwalacz uruchamia się, jeśli ilość wolnego miejsca na dysku jest stale (przez 5 minut) poniżej 10 GB.

Można również zdefiniować wyrażenie odzyskiwania:

```
min(/host/vfs.fs.size[/,free],10m)>40G
```

Problem zostaje **rozwiązany** dopiero wtedy, gdy ilość wolnego miejsca na dysku jest stale (przez 10 minut) powyżej 40 GB.
 Funkcja: min
 Pozycja danych: vfs.fs.size

Wykrywanie małej ilości wolnego miejsca na dysku (próg dynamiczny)

```
last(/template/hrStorageFree[{#SNMPVALUE}])<last(/template/hrStorageSize[{#SNMPVALUE}])*0.1
```

Wyzwalacz uruchamia się, jeśli ilość wolnego miejsca w pamięci masowej (w jednostkach alokacji) spadnie poniżej 10 procent. Zwróć uwagę na użycie wartości innej pozycji do uzyskania adaptacyjnego progu wyzwalacza, mającego zastosowanie do wykrytej pamięci masowej o różnej wielkości. Funkcja: last

Wykrywanie wysokiego obciążenia CPU

```
last(/host/system.cpu.load[all,avg1])>5
```

Wyzwalacz uruchamia się, gdy średnie obciążenie procesora przekracza 5 przez jedną minutę.

Warianty:

```
min(/host/system.cpu.load[all,avg1],5m)>2 and time()<060000
```

```
min(/host/system.cpu.load[all,avg1],5m)>2 and not (dayofweek()=7 and time()>230000) and not (dayofweek()=1
```

Takie wyzwalacze analizują dane z 5 minut i uruchamiają się tylko wtedy, gdy obciążenie CPU nigdy nie spada poniżej 2. Dodatkowo te wyzwalacze uruchamiają się:

- tylko w nocy (00:00-06:00)
- o dowolnej porze z wyjątkiem 2 godzin podczas zmiany tygodnia (niedziela, 23:00 - poniedziałek, 01:00)

```
(last(/host/system.cpu.load[all,avg1])>5) + (last(/host2/system.cpu.load[all,avg1])>5) + (last(/host3/syst
```

Ten wyzwalacz uruchamia się, jeśli obciążenie procesora jest zbyt wysokie na co najmniej dwóch z trzech hostów.
 Funkcje: `last`, `min`, `dayofweek`, `time`
 Pozycja danych: `system.cpu.load`

Porównanie obciążeń CPU

```
avg(/Zabbix server/system.cpu.load,1h)/avg(/Zabbix server/system.cpu.load,1h:now-1d)>2
```

Wyzwalacz uruchamia się, jeśli średnie obciążenie dzisiaj przekracza średnie obciążenie z tej samej godziny wczoraj (z użyciem przesunięcia czasu `now-1d`) ponad dwukrotnie.
 Funkcja: `avg`
 Pozycja danych: `system.cpu.load`

Porównanie długoterminowego obciążenia CPU

```
trendavg(/host/system.cpu.load,1M:now/M)>1.1*trendavg(/host/system.cpu.load,1M:now/M-1M)
```

Ten wyzwalacz uruchamia się, jeśli obciążenie CPU na hoście wzrosło w ostatnim miesiącu o więcej niż 10%
 Funkcja: `trendavg`
 Pozycja danych: `system.cpu.load`

Możesz również użyć pola Nazwa zdarzenia w konfiguracji wyzwalacza, aby zbudować zrozumiały komunikat alertu, na przykład aby otrzymać coś takiego

```
"Obciążenie serwera Exchange wzrosło o 24% w lipcu (0.69) w porównaniu do czerwca (0.56)"
```

nazwa zdarzenia musi być zdefiniowana jako:

```
Load of {HOST.HOST} server increased by {{?100*trendavg(//system.cpu.load,1M:now/M)/trendavg(//system.cpu.
```

Przy tego rodzaju problemie przydatne jest również zezwolenie na ręczne zamykanie w konfiguracji wyzwalacza.

Wykrywanie ciągu zawierającego znaki specjalne

```
last(/host/vfs.file.contents[/tmp/hello])={$HELLO_MACRO}
```

Wyzwalacz uruchamia się, jeśli zawartość `/tmp/hello` jest równa ciągowi zdefiniowanemu w `{$HELLO_MACRO}`:

```
{$HELLO_MACRO} = \" //hello ?\"
```

Alternatywnie można porównać bezpośrednio do ciągu:

```
last(/Zabbix server/vfs.file.contents[/tmp/hello])="\\\" //hello ?\\\""
```

Zwróć uwagę, że znaki specjalne (\\ i ") są poprzedzone znakiem ucieczki, gdy ciąg jest porównywany bezpośrednio.

Funkcja: `last`
 Pozycja danych: `vfs.file.contents`

2 Konfigurowanie wyzwalacza

Ta strona opisuje, jak skonfigurować wyzwalacz w frontendzie Zabbix.

Należy pamiętać, że oficjalne szablony Zabbix zawierają wstępnie zdefiniowane wyzwalacze. Zobacz przewodnik dotyczący stosowania szablonu do monitorowania systemu Linux. Możliwe jest również masowe aktualizowanie skonfigurowanych wyzwalaczy.

Inne materiały:

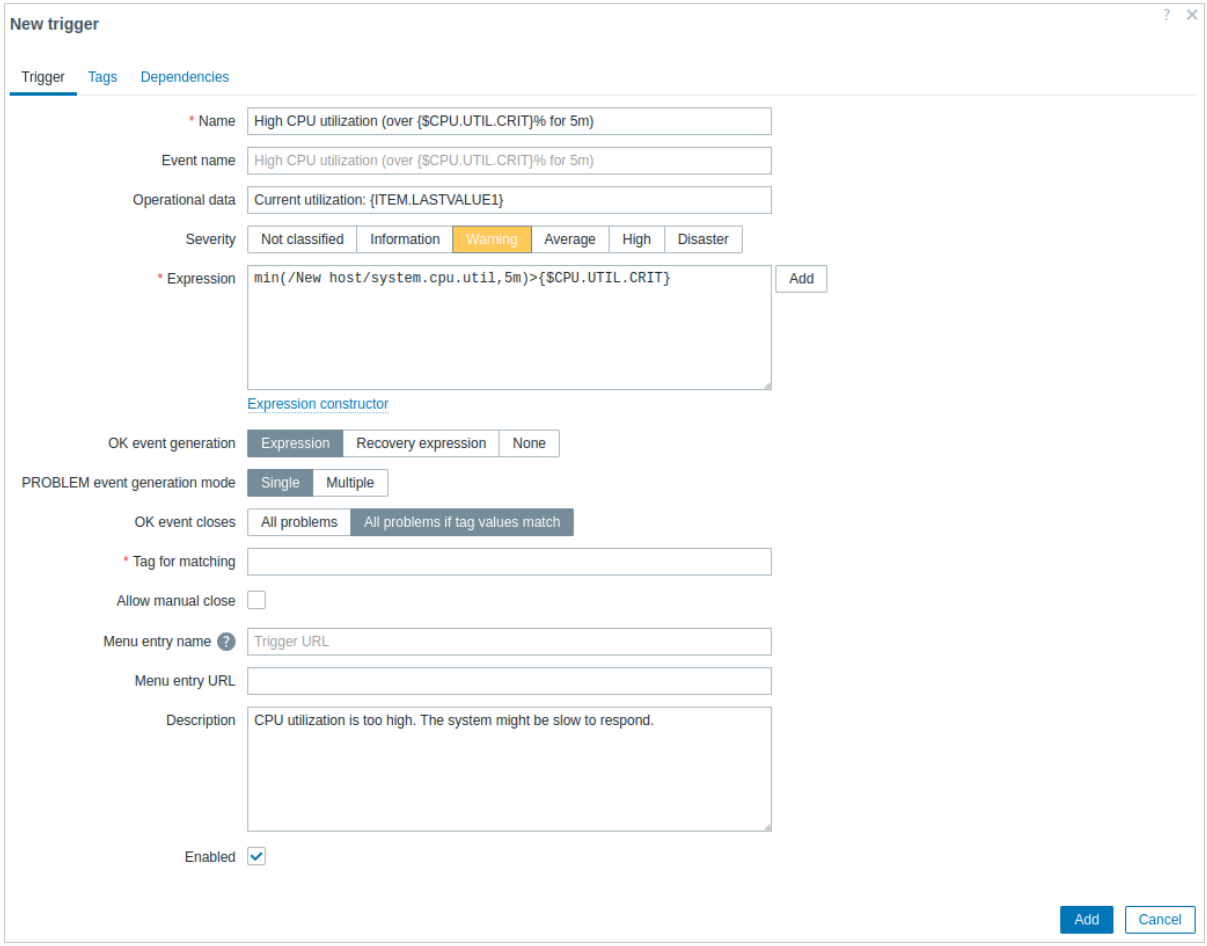
- Wykrywanie problemów za pomocą wyzwalaczy (ogólne wprowadzenie)
- Przykłady wyzwalaczy (według przypadku użycia)
- Wyrażenie wyzwalacza (szczegóły składni)
- Najlepsze praktyki

Konfiguracja

Aby skonfigurować wyzwalacz, wykonaj następujące czynności:

- Przejdź do: *Zbieranie danych* > *Hosty*
- Kliknij *Wyzwalacze* w wierszu hosta
- Kliknij *Utwórz wyzwalacz* po prawej stronie (lub nazwę wyzwalacza, aby edytować istniejący wyzwalacz)
- Wprowadź parametry wyzwalacza w formularzu

Karta **Wyzwalacz** zawiera wszystkie podstawowe atrybuty wyzwalacza.

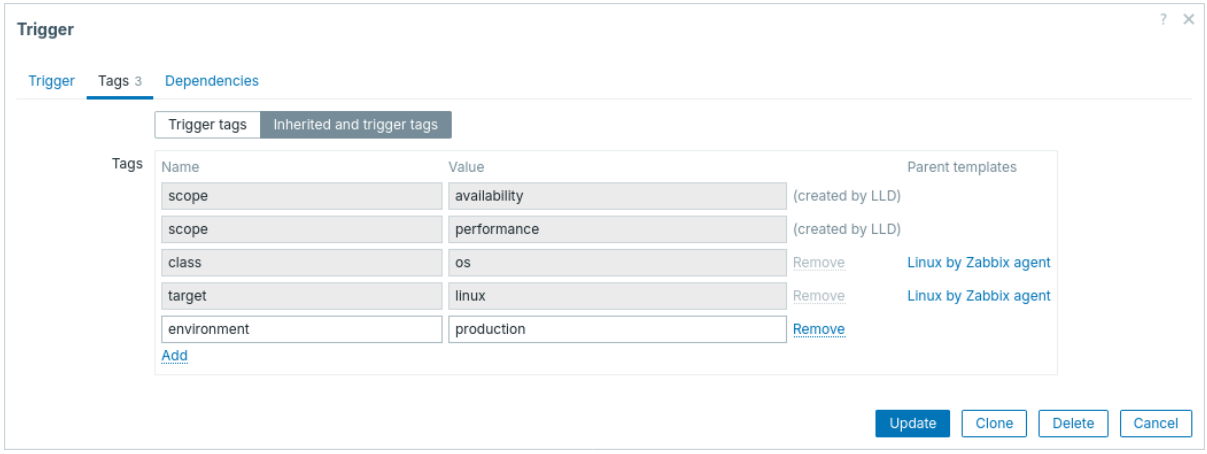


Wszystkie obowiązkowe pola wejściowe są oznaczone czerwoną gwiazdką.

Parameter	Description
Name	Nazwa wyzwalacza. Obsługiwane makra to: {HOST.HOST}, {HOST.NAME}, {HOST.PORT}, {HOST.CONN}, {HOST.DNS}, {HOST.IP}, {ITEM.VALUE}, {ITEM.VALUE.AGE}, {ITEM.VALUE.DATE}, {ITEM.VALUE.TIME}, {ITEM.VALUE.TIMESTAMP}, {ITEM.LASTVALUE}, {ITEM.LASTVALUE.AGE}, {ITEM.LASTVALUE.DATE}, {ITEM.LASTVALUE.TIME}, {ITEM.LASTVALUE.TIMESTAMP}, {ITEM.LOG.*} oraz makra użytkownika {$MACRO}. Makra **$1, $2...$9** mogą być używane do odwoływania się do pierwszej, drugiej... dziewiątej stałej wyrażenia. *Uwaga*: makra $1-$9 zostaną poprawnie rozwinięte, jeśli odnoszą się do stałych w stosunkowo prostych, bezpośrednich wyrażeniach. Na przykład nazwa „Obciążenie procesora powyżej $1 na {HOST.NAME}" automatycznie zmieni się na „Obciążenie procesora powyżej 5 na New host", jeśli wyrażenie ma postać last(/New host/system.cpu.load[percpu,avg1])>5.
Event name	Jeśli zdefiniowano, ta nazwa będzie używana do utworzenia nazwy zdarzenia problemu. Domyślnie nazwa zdarzenia jest taka sama jak nazwa wyzwalacza. Nazwa zdarzenia może być używana do tworzenia znaczących alertów zawierających dane problemu (zobacz przykład). Obsługiwany jest ten sam zestaw makr co w nazwie wyzwalacza, dodatkowo {TIME}, {TIMESTAMP} oraz makra wyrażeń {?EXPRESSION}.

Parameter	Description
Operational data	Dane operacyjne pozwalają definiować dowolne ciągi znaków wraz z makrami. Makra będą dynamicznie rozwijane do danych czasu rzeczywistego w *Monitorowanie* > *Problemy*. Podczas gdy makra w nazwie wyzwalacza (patrz wyżej) zostaną rozwinięte do swoich wartości w momencie wystąpienia problemu i staną się podstawą statycznej nazwy problemu, makra w danych operacyjnych zachowują możliwość dynamicznego wyświetlania najnowszych informacji. Jeśli na poziomie wyzwalacza nie skonfigurowano danych operacyjnych, zostaną wyświetlone najnowsze wartości wszystkich pozycji z wyrażenia. Obsługiwany jest ten sam zestaw makr co w nazwie wyzwalacza.
Severity	Ustaw wymagany poziom ważności wyzwalacza, klikając przyciski.
Expression	Logiczne wyrażenie używane do definiowania warunków problemu. Obsługiwane są sufiksy czasu oraz sufiksy rozmiaru pamięci. Problem jest tworzony po spełnieniu wszystkich warunków zawartych w wyrażeniu, tj. gdy wyrażenie przyjmie wartość TRUE. Problem zostanie rozwiązany, gdy tylko wyrażenie przyjmie wartość FALSE, chyba że w *Wyrażeniu odzyskiwania* określono dodatkowe warunki odzyskiwania.
OK event generation	Opcje generowania zdarzeń OK: **Expression** - zdarzenia OK są generowane na podstawie tego samego wyrażenia co zdarzenia problemu; **Recovery expression** - zdarzenia OK są generowane, jeśli wyrażenie problemu przyjmie wartość FALSE, a wyrażenie odzyskiwania przyjmie wartość TRUE; **None** - w takim przypadku wyzwalacz nigdy samodzielnie nie powróci do stanu OK.
Recovery expression	Logiczne wyrażenie (opcjonalne) definiujące dodatkowe warunki, które muszą zostać spełnione, zanim problem zostanie rozwiązany, po tym jak pierwotne wyrażenie problemu zostało już ocenione jako FALSE. Wyrażenie odzyskiwania jest przydatne w przypadku histerezy wyzwalacza. **Nie** jest możliwe rozwiązanie problemu wyłącznie za pomocą wyrażenia odzyskiwania, jeśli wyrażenie problemu nadal ma wartość TRUE. To pole jest dostępne tylko wtedy, gdy dla *Generowania zdarzeń OK* wybrano opcję „Recovery expression”.
PROBLEM event generation mode	Tryb generowania zdarzeń problemu: **Single** - pojedyncze zdarzenie jest generowane, gdy wyzwalacz po raz pierwszy przejdzie do stanu „Problem”; **Multiple** - zdarzenie jest generowane przy *każdej* ocenie wyzwalacza jako „Problem”.
OK event closes	Wybierz, co zamyka zdarzenie OK: **All problems** - wszystkie problemy tego wyzwalacza; **All problems if tag values match** - tylko te problemy wyzwalacza, których wartości tagów zdarzeń są zgodne.
Tag for matching	Wprowadź nazwę tagu zdarzenia używaną do korelacji zdarzeń. To pole jest wyświetlane, jeśli dla właściwości *OK event closes* wybrano opcję „All problems if tag values match”, i w takim przypadku jest obowiązkowe.
Allow manual close	Zaznacz, aby zezwolić na ręczne zamykanie zdarzeń problemu generowanych przez ten wyzwalacz. Ręczne zamykanie jest możliwe podczas potwierdzania zdarzeń problemu.
Menu entry name	Jeśli nie jest puste, wprowadzona tutaj nazwa (do 64 znaków) jest używana w kilku miejscach frontend jako etykieta dla adresu URL wyzwalacza określonego w parametrze *Menu entry URL*. Jeśli pole jest puste, używana jest domyślna nazwa *Trigger URL*. Obsługiwany jest ten sam zestaw makr co w nazwie wyzwalacza, dodatkowo {EVENT.ID}, {HOST.ID} oraz {TRIGGER.ID}.
Menu entry URL	Jeśli nie jest puste, wprowadzony tutaj adres URL (do 2048 znaków) jest dostępny jako odnośnik w menu zdarzenia w kilku miejscach frontend, na przykład po kliknięciu nazwy problemu w *Monitorowanie* > *Problemy* lub w widżecie pulpitu *Problemy*. Obsługiwany jest ten sam zestaw makr co w nazwie wyzwalacza, dodatkowo {EVENT.ID}, {HOST.ID} oraz {TRIGGER.ID}. Uwaga: makra użytkownika z tajnymi wartościami nie będą rozwijane w adresie URL.
Description	Pole tekstowe używane do podania dodatkowych informacji o tym wyzwalaczu. Może zawierać instrukcje dotyczące rozwiązania konkretnego problemu, dane kontaktowe odpowiedzialnego personelu itp. Obsługiwany jest ten sam zestaw makr co w nazwie wyzwalacza.
Enabled	Odznaczenie tego pola wyłączy wyzwalacz, jeśli będzie to wymagane. Problemy wyłączonego wyzwalacza nie są już wyświetlane w frontend, ale nie są usuwane.

Karta **Tagi** umożliwia definiowanie tagów na poziomie wyzwalacza. Wszystkie problemy tego wyzwalacza zostaną oznaczone wartościami wprowadzonymi tutaj.



Dodatkowo opcja *Inherited and trigger tags* umożliwia wyświetlenie tagów zdefiniowanych na poziomie szablonu, jeśli wyzwalacz pochodzi z tego szablonu. Jeśli istnieje wiele szablonów z tym samym tagiem, tagi te są wyświetlane jednokrotnie, a nazwy szablonów są oddzielone przecinkami. Wyzwalacz nie „dziedziczy" ani nie wyświetla tagów na poziomie hosta.

Parameter	Description
Name/Value	Ustaw własne tagi do oznaczania zdarzeń wyzwalacza. Tagi są parą nazwy tagu i wartości. Możesz użyć samej nazwy lub połączyć ją z wartością. Wyzwalacz może mieć kilka tagów o tej samej nazwie, ale różnych wartościach. W tagach zdarzeń obsługiwane są makra użytkownika, makra użytkownika z kontekstem, makra wykrywania niskopoziomowego oraz funkcje makr z `{{ITEM.VALUE}}`, `{{ITEM.LASTVALUE}}`. Makra wykrywania niskopoziomowego mogą być używane wewnątrz kontekstu makra. Makro {TRIGGER.ID} jest obsługiwane w wartościach tagów wyzwalacza. Może być przydatne do identyfikowania wyzwalaczy utworzonych z prototypów wyzwalaczy i na przykład do tłumienia problemów z tych wyzwalaczy podczas konserwacji. Jeśli całkowita długość rozwiniętej wartości przekracza 255, zostanie ona obcięta do 255 znaków. Zobacz wszystkie makra obsługiwane dla tagów zdarzeń. Tagi zdarzeń mogą być używane do korelacji zdarzeń, w warunkach akcji, a także będą widoczne w *Monitorowanie* > *Problemy* lub w widżecie *Problemy*.

Karta **Zależności** zawiera wszystkie zależności wyzwalacza.

Kliknij *Dodaj*, aby dodać nową zależność.

Note:
Możesz również skonfigurować wyzwalacz, otwierając istniejący, naciskając przycisk *Klonuj*, a następnie zapisując go pod inną nazwą.

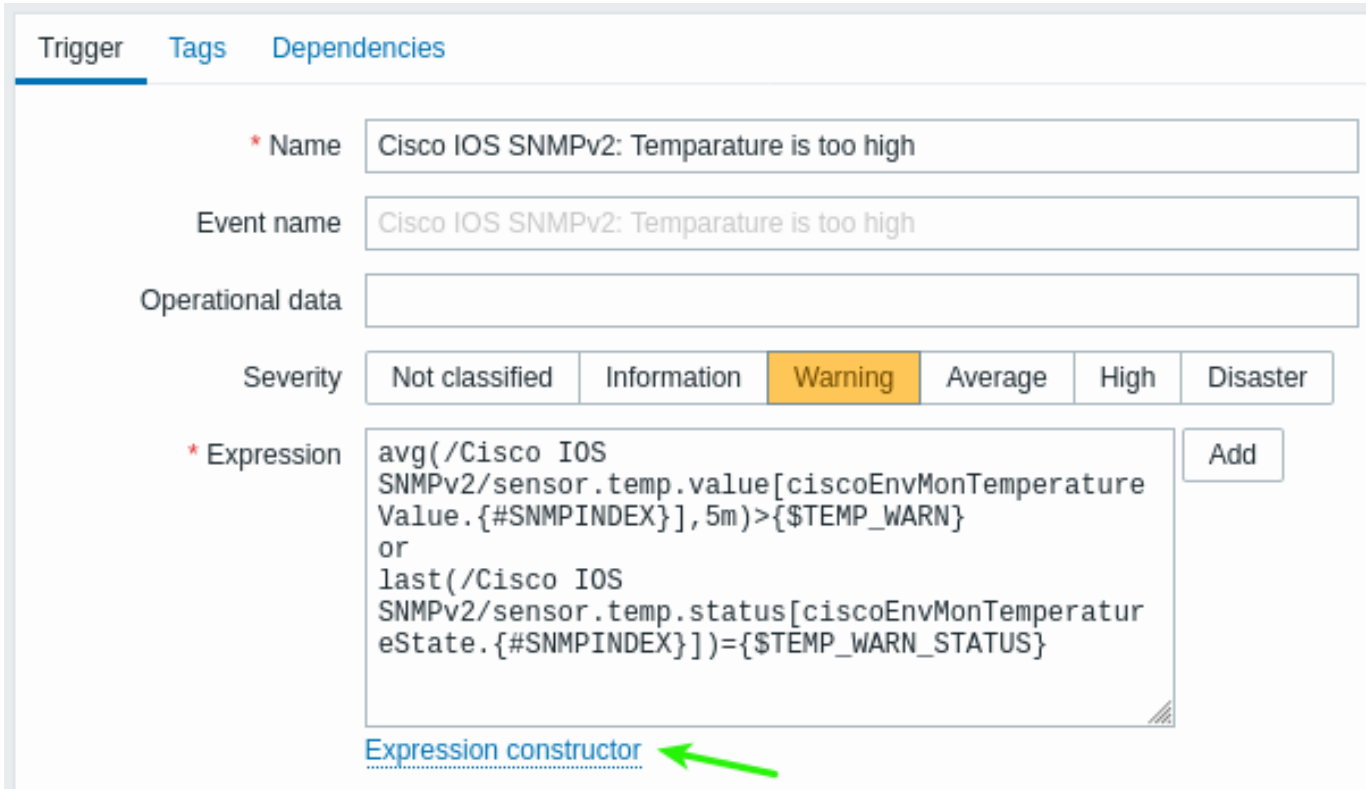
Testowanie wyrażenia wyzwalacza

Możliwe jest przetestowanie, jaki byłby wynik wyrażenia w zależności od otrzymanej wartości.

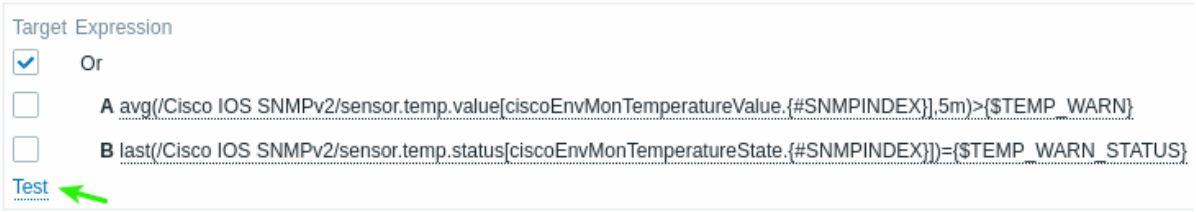
Jako przykład wykorzystano następujące wyrażenie z oficjalnego szablonu:

```
avg(/Cisco IOS SNMPv2/sensor.temp.value[ciscoEnvMonTemperatureValue.{#SNMPINDEX}],5m)>{$TEMP_WARN}
or
last(/Cisco IOS SNMPv2/sensor.temp.status[ciscoEnvMonTemperatureState.{#SNMPINDEX}])={$TEMP_WARN_STATUS}
```

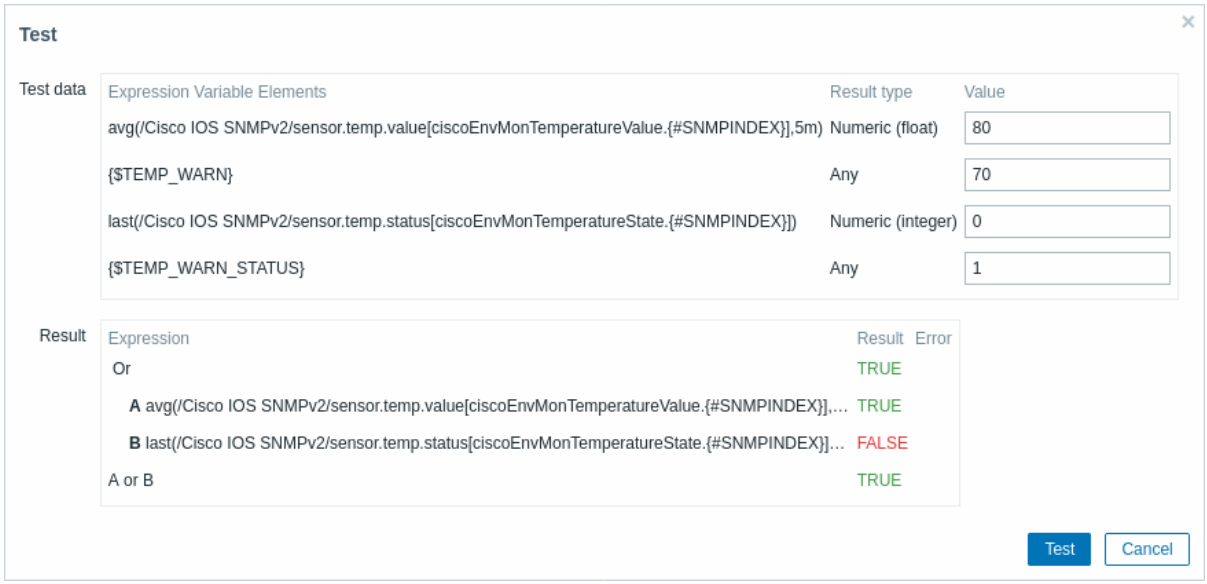
Aby przetestować wyrażenie, kliknij *Expression constructor* pod polem wyrażenia.



W oknie Expression constructor wyświetlane są wszystkie pojedyncze wyrażenia. Aby otworzyć okno testowania, kliknij *Test* pod listą wyrażeń.



W oknie testowania możesz wprowadzić przykładowe wartości („80”, „70”, „0”, „1” w tym przykładzie), a następnie sprawdzić wynik wyrażenia, klikając przycisk *Test*.



Można zobaczyć wynik poszczególnych wyrażeń, jak również całego wyrażenia.

„TRUE” oznacza, że określone wyrażenie jest prawdziwe. W tym konkretnym przypadku A wartość „80” jest większa niż określona wartość {$TEMP_WARN}, czyli „70” w tym przykładzie. Zgodnie z oczekiwaniami pojawia się wynik „TRUE”.

„FALSE” oznacza, że określone wyrażenie jest fałszywe. W tym konkretnym przypadku B wartość {$TEMP_WARN_STATUS} „1” musi być równa określonej wartości, czyli „0” w tym przykładzie. Zgodnie z oczekiwaniami pojawia się wynik „FALSE”.

Wybrany typ wyrażenia to „OR”. Jeśli co najmniej jeden z określonych warunków (w tym przypadku A lub B) ma wartość TRUE, wynik końcowy również będzie miał wartość TRUE. Oznacza to, że bieżąca wartość przekracza wartość ostrzegawczą i wystąpił problem.

3 Wyrażenie wyzwalacza

Przegląd

Ta strona opisuje składnię wyrażeń wyzwalaczy oraz szczegóły ich obliczania.

Składnia prostego wyrażenia jest następująca:

```
function(/host/item,time_period)<operator><constant>
```

W tym wyrażeniu pierwszy operand (po lewej stronie operatora) to funkcja z jej parametrami w nawiasach (zwykle pozycja danych i okres czasu).

Funkcja służy do analizowania odebranych danych w ustawionym okresie czasu, czego wynikiem jest obliczona wartość.

Ta wartość jest następnie porównywana z drugim operandem przy użyciu operatora. W tym przykładzie drugi operand jest stałą, ale może to być również inna funkcja.

Na przykład:

```
min(/Zabbix server/net.if.in[eth0,bytes],5m)>100K
```

Ten wyzwalacz uruchamia się, jeśli liczba odebranych bajtów na `eth0` w ciągu ostatnich pięciu minut była cały czas większa niż 100 kilobajtów. W takim przypadku wyrażenie ma wartość prawda i tworzony jest problem.

Wyrażenia wyzwalaczy są niezwykle elastyczne. W bardziej złożonych wyrażeniach można łączyć wiele funkcji, operatorów i stałych.

Zobacz także:

- Przykłady wyzwalaczy
- Wykrywanie problemów za pomocą wyzwalaczy (ogólne wprowadzenie)

Funkcje

Funkcje umożliwiają analizę zebranych wartości, na przykład obliczenie średniej lub znalezienie określonego ciągu znaków.

Kliknij odpowiednią grupę funkcji, aby zobaczyć więcej szczegółów.

Grupa funkcji	Funkcje
Funkcje agregujące	avg, bucket_percentile, count, histogram_quantile, item_count, kurtosis, mad, max, min, skewness, stddevpop, stddevsamp, sum, sumofsquares, varpop, varsamp
Funkcje foreach	avg_foreach, bucket_rate_foreach, count_foreach, exists_foreach, last_foreach, max_foreach, min_foreach, sum_foreach
Funkcje bitowe	bitand, bitlshift, bitnot, bitor, bitrshift, bitxor
Funkcje daty i czasu	date, dayofmonth, dayofweek, now, time
Funkcje historii	change, changecount, count, countunique, find, first, firstclock, fuzzytime, last, lastclock, logeventid, logseverity, logsource, logtimestamp, monodec, monoinc, nodata, percentile, rate
Funkcje trendów	baselinedev, baselinewma, trendavg, trendcount, trendmax, trendmin, trendstl, trendsum
Funkcje matematyczne	abs, acos, asin, atan, atan2, avg, cbrt, ceil, cos, cosh, cot, degrees, e, exp, expm1, floor, log, log10, max, min, mod, pi, power, radians, rand, round, signum, sin, sinh, sqrt, sum, tan, truncate
Funkcje operatorów	between, in

Grupa funkcji	Funkcje
Funkcje predykcyjne	forecast, timeleft
Funkcje ciągów znaków	ascii, bitlength, bytelength, char, concat, insert, jsonpath, left, length, ltrim, mid, repeat, replace, right, rtrim, trim, xmlxpath

O ile nie określono inaczej, te funkcje są obsługiwane w:

- Wyrażeniach wyzwalaczy
- Pozycjach obliczanych
- Makrach wyrażeń

Funkcje foreach są obsługiwane tylko dla obliczeń agregujących.

Zazwyczaj funkcje zwracają wartości liczbowe do porównania. Jeśli zwracają ciągi znaków, porównanie jest możliwe za pomocą operatorów **=** i **<>** (zobacz przykład Wykrywanie niezgodnego oprogramowania na różnych hostach).

Parametry funkcji

Parametry funkcji pozwalają określić:

- klucz pozycji (jako `/host/key`) dla funkcji odwołujących się do historii pozycji hosta
- okres czasu (oraz inne parametry specyficzne dla funkcji)
- inne wyrażenia

Klucz pozycji

Pozycja, do której następuje odwołanie, musi być w obsługiwanym stanie (z wyjątkiem funkcji **nodata()**, która jest obliczana również dla nieobsługiwanych pozycji).

Pominięcie nazwy hosta w pierwszym parametrze (tj. jak w `function(//key,parameter,...)`) jest obsługiwane tylko w określonych kontekstach:

- W formule pozycji obliczanych
- W makrach wyrażeń, które mogą być używane w:
  - polu *Nazwa zdarzenia*
  - nazwie wykresu
  - etykiecie elementów mapy „Host" i „Trigger" map elements

W tych kontekstach można również użyć makra `{HOST.HOST}`. Makro `{HOST.HOST<1-9>}` może być użyte w przypadku pola *Nazwa zdarzenia* oraz elementu mapy „Trigger", aby odwołać się do określonej pozycji w wyrażeniu wyzwalacza. Gdy nazwa hosta jest pominięta lub zastąpiona przez `{HOST.HOST}` w tych kontekstach, odwołanie wskazuje na pierwszą pozycję w wyrażeniu wyzwalacza lub na pierwszą pozycję na wykresie. Poza tymi obsługiwanymi kontekstami pominięcie nazwy hosta w wyrażeniach wyzwalaczy spowoduje błąd. Zobacz przykład Compare long-term CPU loads, aby zobaczyć ilustrację użycia podwójnego ukośnika w makrach Nazwy zdarzenia.

Okres czasu

Parametry specyficzne dla funkcji są umieszczane po kluczu pozycji i oddzielane od klucza pozycji przecinkiem.

Większość funkcji numerycznych akceptuje **okres czasu** jako parametr. Pozwala on określić interesujący nas przedział. Może być podany jako okres czasu (30s, 10m, 1h) lub jako zakres wartości (#5 - dla pięciu najnowszych wartości).

Możesz użyć sekund lub sufiksów czasu, aby wskazać okres czasu. Jeśli parametr jest poprzedzony znakiem kratki, ma inne znaczenie:

Expression	Description
sum(/host/key,**10m)**	Suma wartości z ostatnich 10 minut.
sum(/host/key,**#10)**	Suma ostatnich dziesięciu wartości.

Parametry ze znakiem kratki mają inne znaczenie w przypadku funkcji **last** — oznaczają N-tą poprzednią wartość, więc przy wartościach 30, 70, 20, 60, 50 (od najnowszej do najstarszej):

- `last(/host/key,#2)` zwróci '70'
- `last(/host/key,#5)` zwróci '50'

Okres czasu jest mierzony do chwili „teraz” — gdzie „teraz” oznacza czas ostatniego przeliczenia wyzwalacza (zobacz Częstotliwość obliczania); „teraz” nie jest czasem „teraz” serwera.

Okres czasu określa jedno z poniższych:

- Uwzględnienie wszystkich wartości pomiędzy „teraz-okres czasu” a „teraz” (lub, przy przesunięciu czasu, pomiędzy „teraz-przesunięcie czasu-okres czasu” a „teraz-przesunięcie_czasu”)
- Uwzględnienie nie więcej niż liczby wartości określonej przez num z przeszłości, aż do „teraz”
  - Jeśli dla określonego okresu czasu lub liczby num dostępnych jest 0 wartości — wówczas wyzwalacz lub obliczana pozycja korzystająca z tej funkcji staje się nieobsługiwana

Zwróć uwagę, że:

- Jeśli w wyzwalaczu używana jest tylko jedna funkcja (odwołująca się do historii danych), „teraz” zawsze oznacza ostatnio otrzymaną wartość. Na przykład, jeśli ostatnia wartość została odebrana godzinę temu, okres czasu będzie traktowany jako kończący się na tej ostatniej wartości sprzed godziny.
- Nowy wyzwalacz jest obliczany natychmiast po odebraniu pierwszej wartości (funkcje historii); dla funkcji date and time oraz nodata() zostanie obliczony w ciągu 30 sekund. W ten sposób wyzwalacz zostanie obliczony, nawet jeśli od jego utworzenia być może nie upłynął jeszcze ustawiony okres czasu (na przykład jedna godzina). Wyzwalacz zostanie również obliczony po pierwszej wartości, nawet jeśli zakres czasu został ustawiony, na przykład, na dziesięć najnowszych wartości.

Przesunięcie czasu

Opcjonalne przesunięcie czasu jest obsługiwane przy użyciu czasu lub liczby wartości jako parametru funkcji. Ten parametr umożliwia odwoływanie się do danych z okresu czasu w przeszłości.

Przesunięcie czasu zaczyna się od `now` — określającego bieżący czas, po którym następuje `+N<time unit>` lub `-N<time unit>` — aby dodać lub odjąć N jednostek czasu.

Na przykład `avg(/host/key,1h:now-1d)` zwróci wartość średnią dla jednej godziny sprzed jednego dnia.

> **Attention:**
> Przesunięcie czasu określone w miesiącach (M) i latach (y) jest obsługiwane tylko dla funkcji trendów. Inne funkcje obsługują sekundy (s), minuty (m), godziny (h), dni (d) i tygodnie (w).

Przesunięcie czasu z bezwzględnymi okresami czasu

Bezwzględne okresy czasu są obsługiwane w parametrze przesunięcia czasu, na przykład od północy do północy dla dnia, od poniedziałku do niedzieli dla tygodnia, od pierwszego do ostatniego dnia miesiąca dla miesiąca.

Przesunięcie czasu dla bezwzględnych okresów czasu zaczyna się od `now` — określającego bieżący czas, po którym może następować dowolna liczba operacji na czasie: `/<time unit>` — definiuje początek i koniec jednostki czasu, na przykład od północy do północy dla dnia, `+N<time unit>` lub `-N<time unit>` — aby dodać lub odjąć N jednostek czasu.

Należy pamiętać, że wartość przesunięcia czasu może być większa lub równa 0, podczas gdy minimalna wartość okresu czasu wynosi 1.

Parameter	Description
1d:now/d	Wczoraj
1d:now/d+1d	Dzisiaj
2d:now/d+1d	Ostatnie 2 dni
1w:now/w	Poprzedni tydzień
1w:now/w+1w	Bieżący tydzień

Inne wyrażenia

Parametry funkcji mogą zawierać inne wyrażenia, jak w poniższej składni:

```
min(min(/host/key,1h),min(/host2/key2,1h)*10)
```

Należy pamiętać, że inne wyrażenia nie mogą być używane, jeśli funkcja odwołuje się do historii pozycji. Na przykład poniższa składnia **nie** jest dozwolona:

~~`min(/host/key,#5*10)`~~

Chociaż inne wyrażenia wyzwalaczy jako parametry funkcji są w wyzwalaczach ograniczone do funkcji nieodwołujących się do historii, to ograniczenie nie ma zastosowania w pozycjach obliczanych.

Operatory

Następujące operatory są obsługiwane dla wyzwalaczy **(w malejącej kolejności priorytetu wykonywania)**:

Priorytet	Operator	Definicja	**Uwagi dotyczące wartości nieznanych**	Wymuś rzutowanie operandu na float [1]
1	**-**	Jednoargumentowy minus	**-**Unknown → Unknown	Tak
2	**not**	Logiczne NOT	**not** Unknown → Unknown	Tak
3	*	Mnożenie	0 * Unknown → Unknown (tak, Unknown, a nie 0 - aby nie utracić Unknown w operacjach arytmetycznych) 1.2 * Unknown → Unknown	Tak
	/	Dzielenie	Unknown / 0 → error Unknown / 1.2 → Unknown 0.0 / Unknown → Unknown	Tak
4	+	Dodawanie arytmetyczne	1.2 + Unknown → Unknown	Tak
	-	Odejmowanie arytmetyczne	1.2 - Unknown → Unknown	Tak
5	<	Mniejsze niż. Operator jest zdefiniowany jako: A<B ⇔ (A<B-0.000001)	1.2 < Unknown → Unknown	Tak
	<=	Mniejsze niż lub równe. Operator jest zdefiniowany jako: A<=B ⇔ (A≤B+0.000001)	Unknown <= Unknown → Unknown	Tak
	>	Większe niż. Operator jest zdefiniowany jako: A>B ⇔ (A>B+0.000001)		Tak
	>=	Większe niż lub równe. Operator jest zdefiniowany jako: A>=B ⇔ (A≥B-0.000001)		Tak
6	=	Równe. Operator jest zdefiniowany jako: A=B ⇔ (A≥B-0.000001) and (A≤B+0.000001)		Nie [1]

Priorytet	Operator	Definicja	**Uwagi dotyczące wartości nieznanych**	Wymuś rzutowanie operandu na float [1]
	<>	Różne. Operator jest zdefiniowany jako: A<>B ⇔ (A<B-0.000001) or (A>B+0.000001)		Nie [1]
7	**and**	Logiczne AND	0 **and** Unknown → 0 1 **and** Unknown → Unknown Unknown **and** Unknown → Unknown	Tak
8	**or**	Logiczne OR	1 **or** Unknown → 1 0 **or** Unknown → Unknown Unknown **or** Unknown → Unknown	Tak

[1] Operand typu string jest nadal rzutowany na wartość numeryczną, jeśli:

- drugi operand jest numeryczny
- na operandzie użyto operatora innego niż **=** lub **<>**

(Jeśli rzutowanie się nie powiedzie - operand numeryczny jest rzutowany na operand typu string i oba operandy są porównywane jako stringi.)

Operatory **not**, **and** i **or** rozróżniają wielkość liter i muszą być zapisane małymi literami. Muszą też być otoczone spacjami lub nawiasami.

Wszystkie operatory, z wyjątkiem jednoargumentowego **-** i **not**, mają lewostronną łączność. Jednoargumentowe **-** i **not** nie są łączne (co oznacza, że należy używać **-(-1)** i **not (not 1)** zamiast **--1** i **not not 1**).

Wynik obliczenia:

- operatory **<**, **<=**, **>**, **>=**, **=**, **<>** zwracają '1' w wyrażeniu wyzwalacza, jeśli określona relacja jest prawdziwa, oraz '0', jeśli jest fałszywa. Jeśli co najmniej jeden operand ma wartość Unknown, wynikiem jest Unknown;
- **and** dla znanych operandów zwraca '1', jeśli oba jego operandy są różne od '0'; w przeciwnym razie zwraca '0'; dla nieznanych operandów **and** zwraca '0' tylko wtedy, gdy jeden operand jest równy '0'; w przeciwnym razie zwraca 'Unknown';
- **or** dla znanych operandów zwraca '1', jeśli którykolwiek z jego operandów jest różny od '0'; w przeciwnym razie zwraca '0'; dla nieznanych operandów **or** zwraca '1' tylko wtedy, gdy jeden operand jest różny od '0'; w przeciwnym razie zwraca 'Unknown';
- wynik operatora negacji logicznej **not** dla znanego operandu wynosi '0', jeśli wartość jego operandu jest różna od '0'; '1', jeśli wartość jego operandu jest równa '0'. Dla nieznanego operandu **not** zwraca 'Unknown'.

Nieznany stan wyrażenia

Możliwe jest, że w wyrażeniu wyzwalacza pojawi się nieznany operand, gdy:

- używana jest nieobsługiwana pozycja
- obliczenie funkcji dla obsługiwanej pozycji kończy się błędem

W takim przypadku wyrażenie wyzwalacza jest zazwyczaj obliczane jako `Unknown` (ponieważ nie może zostać obliczone)

Możliwe jest otrzymywanie powiadomień o wyzwalaczach w stanie nieznanym.

Wyjątki

Pomimo obecności nieznanego operandu, wyrażenia wyzwalacza mogą w niektórych przypadkach zostać obliczone do znanego wyniku (Problem/OK):

- Funkcja `nodata()` jest obliczana niezależnie od tego, czy wskazana pozycja jest obsługiwana, czy nie.
- Wyrażenia z AND/OR mogą zostać obliczone do znanego wyniku w dwóch przypadkach:
  - **Przypadek 1**: „`1 or some_function(unsupported_item1) or some_function(unsupported_item2) or ...`" jest obliczane do znanego wyniku ('1' lub „Problem"),
  - **Przypadek 2**: „`0 and some_function(unsupported_item1) and some_function(unsupported_item2) and ...`" jest obliczane do znanego wyniku ('0' lub „OK").

- Jeśli obliczenie funkcji dla obsługiwanej pozycji kończy się błędem, wartość funkcji staje się `Unknown` i bierze udział jako nieznany operand w dalszym obliczaniu wyrażenia.

Nieznane operandy mogą „zniknąć" tylko w wyrażeniach logicznych, jak opisano powyżej. W wyrażeniach arytmetycznych nieznane operandy zawsze prowadzą do wyniku `Unknown` (z wyjątkiem dzielenia przez 0).

Attention:
Nieznany stan wyrażenia nie zmienia stanu wyzwalacza (Problem/OK). Dlatego jeśli stan wyzwalacza był „Problem" (zobacz Przypadek 1), pozostaje on w stanie problemu nawet wtedy, gdy znana część zostanie rozwiązana ('1' zmieni się na '0'), ponieważ wyrażenie jest teraz obliczane jako `Unknown`, a to nie zmienia stanu wyzwalacza.

Jeśli wyrażenie wyzwalacza z kilkoma nieobsługiwanymi pozycjami zostanie obliczone jako `Unknown`, komunikat o błędzie w frontend odnosi się do ostatniej obliczanej nieobsługiwanej pozycji.

Buforowanie wartości

Wartości wymagane do obliczania wyzwalaczy są buforowane przez serwer Zabbix. Z tego powodu obliczanie wyzwalaczy przez pewien czas po ponownym uruchomieniu serwera powoduje większe obciążenie bazy danych.

Bufor wartości nie jest czyszczony po usunięciu wartości historii pozycja (ręcznie lub przez housekeeper), dlatego serwer będzie używać wartości z pamięci podręcznej, dopóki nie będą one starsze niż okresy czasu zdefiniowane w funkcjach wyzwalaczy lub dopóki serwer nie zostanie ponownie uruchomiony.

Note:
Jeśli w pamięci podręcznej nie ma aktualnych danych i w funkcji nie zdefiniowano okresu odpytywania, Zabbix domyślnie cofnie się maksymalnie o tydzień, aby odpytać bazę danych o wartości historyczne.

1 Funkcje agregujące

O ile nie podano inaczej, wszystkie wymienione tutaj funkcje są obsługiwane w:

- Wyrażeniach wyzwalaczy
- Pozycjach obliczanych
- Makrach wyrażeń

Funkcje agregujące mogą działać na:

- historii pozycji, na przykład `min(/host/key,1h)`
- funkcjach foreach jako jedynym parametrze, na przykład `min(last_foreach(/*/key))` (tylko w pozycjach obliczanych; nie można używać w wyzwalaczach)

Funkcje są wymienione bez dodatkowych informacji. Kliknij funkcję, aby zobaczyć pełne szczegóły.

Function	Description
avg	Średnia wartość pozycji w zdefiniowanym okresie oceny.
bucket_percentile	Oblicza percentyl na podstawie kubełków histogramu.
count	Liczba wartości w tablicy zwróconej przez funkcję foreach.
histogram_quantile	Oblicza φ-kwantyl na podstawie kubełków histogramu.
item_count	Liczba istniejących pozycji w konfiguracji, które spełniają kryteria filtra.
kurtosis	„Spiczastość" rozkładu prawdopodobieństwa zebranych wartości w zdefiniowanym okresie oceny.
mad	Mediana odchyleń bezwzględnych zebranych wartości w zdefiniowanym okresie oceny.
max	Najwyższa wartość pozycji w zdefiniowanym okresie oceny.
min	Najniższa wartość pozycji w zdefiniowanym okresie oceny.
skewness	Asymetria rozkładu prawdopodobieństwa zebranych wartości w zdefiniowanym okresie oceny.
stddevpop	Odchylenie standardowe populacji zebranych wartości w zdefiniowanym okresie oceny.
stddevsamp	Odchylenie standardowe próby zebranych wartości w zdefiniowanym okresie oceny.
sum	Suma zebranych wartości w zdefiniowanym okresie oceny.
sumofsquares	Suma kwadratów zebranych wartości w zdefiniowanym okresie oceny.
varpop	Wariancja populacji zebranych wartości w zdefiniowanym okresie oceny.
varsamp	Wariancja próby zebranych wartości w zdefiniowanym okresie oceny.

Wspólne parametry

- `/host/key` to wspólny obowiązkowy pierwszy parametr dla funkcji odwołujących się do historii pozycji hosta

- `(sec|#num)<:time shift>` to wspólny drugi parametr dla funkcji odwołujących się do historii pozycji hosta, gdzie:
  - **sec** — maksymalny okres obliczania w sekundach (mogą być używane sufiksy czasu), lub
  - **#num** — maksymalny zakres obliczania w ostatnio zebranych wartościach (jeśli jest poprzedzony znakiem kratki)
  - **time shift** (opcjonalnie) pozwala przesunąć punkt obliczania wstecz w czasie. Zobacz więcej szczegółów dotyczących określania przesunięcia czasu.

Szczegóły funkcji

Kilka ogólnych uwag dotyczących parametrów funkcji:

- Parametry funkcji są oddzielane przecinkiem
- Opcjonalne parametry funkcji (lub części parametrów) są oznaczone przez < >
- Parametry specyficzne dla danej funkcji są opisane przy każdej funkcji
- Parametry `/host/key` oraz `(sec|#num)<:time shift>` nigdy nie mogą być ujmowane w cudzysłów

avg(/host/key,(sec|#num)<:time shift>)

Średnia wartość pozycji w zdefiniowanym okresie obliczania.
 Obsługiwane typy wartości: *Float*, *Integer*.
 Obsługiwane funkcje foreach: *avg_foreach*, *count_foreach*, *exists_foreach*, *last_foreach*, *max_foreach*, *min_foreach*, *sum_foreach*.

Parametry: zobacz wspólne parametry.

Przesunięcie czasu jest przydatne, gdy zachodzi potrzeba porównania bieżącej wartości średniej ze średnią wartością sprzed pewnego czasu.

Przykłady:

```
avg(/host/key,1h) #średnia wartość z ostatniej godziny do teraz
avg(/host/key,1h:now-1d) #średnia wartość z jednej godziny w przedziale od 25 godzin temu do 24 godzin tem
avg(/host/key,#5) #średnia wartość z pięciu najnowszych wartości
avg(/host/key,#5:now-1d) #średnia wartość z pięciu najnowszych wartości z wyłączeniem wartości otrzymanych
```

bucket_percentile(item filter,time period,percentage)

Oblicza percentyl z bucketów histogramu.

Parametry:

- **item filter** - zobacz item filter;
- **time period** - zobacz time period;
- **percentage** - wartość procentowa (0-100).

Uwagi:

- Obsługiwane tylko w pozycjach obliczanych;
- Ta funkcja jest aliasem dla `histogram_quantile(percentage/100, bucket_rate_foreach(item filter, time period, 1))`.

count(func_foreach(item filter,<time period>),<operator>,<pattern>)

Liczba wartości w tablicy zwróconej przez funkcję foreach.
 Obsługiwane funkcje foreach: *avg_foreach*, *count_foreach*, *exists_foreach*, *last_foreach*, *max_foreach*, *min_foreach*, *sum_foreach*.

Parametry:

- **func_foreach** - funkcja foreach, dla której ma zostać policzona liczba zwróconych wartości. Szczegóły znajdują się w opisie funkcji foreach. Należy pamiętać, że count_foreach i bucket_rate_foreach obsługują dodatkowe parametry.
- **item filter** - zobacz item filter;
- **time period** - zobacz time period;
- **operator** (musi być ujęty w podwójny cudzysłów). Obsługiwane `operators`:
eq - równe
ne - różne od
gt - większe niż
ge - większe lub równe
lt - mniejsze niż
le - mniejsze lub równe
like - pasuje, jeśli zawiera wzorzec (z uwzględnieniem wielkości liter)
bitand - bitowe AND
regexp - dopasowanie z uwzględnieniem wielkości liter do wyrażenia regularnego podanego w `pattern`
iregexp - dopasowanie bez uwzględniania wielkości liter do wyrażenia regularnego podanego w `pattern`
- **pattern** - wymagany wzorzec (argumenty tekstowe muszą być ujęte w podwójny cudzysłów); obsługiwany, jeśli *operator* jest określony w trzecim parametrze.

Uwagi:

- Użycie **count()** z funkcją foreach powiązaną z historią (max_foreach, avg_foreach itp.) może mieć wpływ na wydajność, podczas gdy użycie **exists_foreach()**, które działa wyłącznie na danych konfiguracyjnych, nie będzie miało takiego efektu.
- Opcjonalnych parametrów *operator* lub *pattern* nie można pozostawić pustych po przecinku, można je jedynie całkowicie pominąć.

- Gdy jako trzeci parametr użyto *bitand*, czwarty parametr `pattern` można podać jako dwie liczby rozdzielone znakiem '/': **number_to_compare_with/mask**. count() oblicza „bitowe AND" z wartości i *mask*, a następnie porównuje wynik z *number_to_compare_with*. Jeśli wynik „bitowego AND" jest równy *number_to_compare_with*, wartość jest zliczana.
Jeśli *number_to_compare_with* i *mask* są równe, wystarczy podać tylko *mask* (bez '/').
- Gdy jako trzeci parametr użyto *regexp* lub *iregexp*, czwarty parametr `pattern` może być zwykłym lub globalnym (zaczynającym się od '@') wyrażeniem regularnym. W przypadku globalnych wyrażeń regularnych rozróżnianie wielkości liter jest dziedziczone z ustawień globalnego wyrażenia regularnego. Na potrzeby dopasowania regexp wartości zmiennoprzecinkowe będą zawsze reprezentowane z 4 cyframi dziesiętnymi po '.'. Należy również pamiętać, że w przypadku dużych liczb różnica między reprezentacją dziesiętną (przechowywaną w bazie danych) a binarną (używaną przez serwer Zabbix) może wpływać na 4. cyfrę dziesiętną.

Przykłady:

```
count(max_foreach(/*/net.if.in[*],1h)) #liczba pozycji net.if.in, które otrzymały dane w ciągu ostatniej g
count(last_foreach(/*/vfs.fs.size[*,pused]),"gt",95) #liczba systemów plików z wykorzystaniem ponad 95% mi
```

histogram_quantile(quantile,bucket1,value1,bucket2,value2,...)

Oblicza φ-kwantyl na podstawie kubełków histogramu.
 Obsługiwana funkcja foreach: *bucket_rate_foreach*.

Parametry:

- **quantile** — 0 ≤ φ ≤ 1;
- **bucketN, valueN** — ręcznie wprowadzone pary (>=2) parametrów lub odpowiedź bucket_rate_foreach.

Uwagi:

- Obsługiwane tylko w pozycjach obliczanych;
- Funkcjonalnie odpowiada funkcji 'histogram_quantile' w PromQL;
- Zwraca -1, jeśli wartości ostatniego kubełka 'Infinity' ("+*inf*") są równe 0.

Przykłady:

```
histogram_quantile(0.75,1.0,last(/host/rate_bucket[1.0]),"+Inf",last(/host/rate_bucket[Inf]))
histogram_quantile(0.5,bucket_rate_foreach(//item_key,30s))
```

item_count(item filter)

Liczba istniejących pozycji w konfiguracji, które spełniają kryteria filtra.
 Obsługiwany typ wartości: *Integer*.

Parametr:

- **item filter** — kryteria wyboru pozycji; umożliwia odwoływanie się według grupy hostów, hosta, klucza pozycji i tagów. Obsługiwane są symbole wieloznaczne. Więcej informacji znajduje się w filtrze pozycji.

Uwagi:

- Obsługiwane tylko w pozycjach obliczanych;
- Działa jako alias funkcji *count(exists_foreach(item_filter))*.

Przykłady:

```
item_count(/*/agent.ping?[group="Host group 1"]) #liczba hostów z pozycją *agent.ping* w "Host group 1"
```

kurtosis(/host/key,(sec|#num)<:przesunięcie czasu>)

„Spiczastość" rozkładu prawdopodobieństwa wartości zebranych w zdefiniowanym okresie obliczania. Zobacz także: Kurtosis.
 Obsługiwane typy wartości: *Float*, *Integer*.
 Obsługiwana funkcja foreach: *last_foreach*.

Parametry: zobacz wspólne parametry.

Przykład:

```
kurtosis(/host/key,1h) #kurtoza za ostatnią godzinę do teraz
```

mad(/host/key,(sec|#num)<:time shift>)

Odchylenie medianowe w zebranych wartościach w zdefiniowanym okresie obliczania. Zobacz także: Odchylenie medianowe.
 Obsługiwane typy wartości: *Float*, *Integer*.
 Obsługiwana funkcja foreach: *last_foreach*.

Parametry: zobacz wspólne parametry.

Przykład:

```
mad(/host/key,1h) #odchylenie medianowe dla ostatniej godziny do teraz
```

max(/host/key,(sek|#num)<:przesunięcie czasu>)

Najwyższa wartość pozycji w zdefiniowanym okresie obliczania.
 Obsługiwane typy wartości: *Float*, *Integer*.
 Obsługiwane funkcje foreach: *avg_foreach*, *count_foreach*, *exists_foreach*, *last_foreach*, *max_foreach*, *min_foreach*, *sum_foreach*.

Parametry: zobacz wspólne parametry.

Przykład:

```
max(/host/key,1h) - min(/host/key,1h) #oblicza różnicę między wartościami maksymalną i minimalną w ciągu c
```

min(/host/key,(sek|#num)<:przesunięcie czasu>)

Najniższa wartość pozycji w zdefiniowanym okresie obliczeniowym.
 Obsługiwane typy wartości: *Float*, *Integer*.
 Obsługiwane funkcje foreach: *avg_foreach*, *count_foreach*, *exists_foreach*, *last_foreach*, *max_foreach*, *min_foreach*, *sum_foreach*.

Parametry: zobacz wspólne parametry.

Przykład:

```
max(/host/key,1h) - min(/host/key,1h) #oblicza różnicę między wartościami maksymalną i minimalną w ciągu c
```

skewness(/host/key,(sec|#num)<:time shift>)

Asymetria rozkładu prawdopodobieństwa zebranych wartości w zdefiniowanym okresie obliczania. Zobacz także: Skewness.
 Obsługiwane typy wartości: *Float*, *Integer*.
 Obsługiwana funkcja foreach: *last_foreach*.

Parametry: zobacz wspólne parametry.

Przykład:

```
skewness(/host/key,1h) #asymetria dla ostatniej godziny do teraz
```

stddevpop(/host/key,(sec|#num)<:time shift>)

Odchylenie standardowe populacji w zebranych wartościach w zdefiniowanym okresie obliczania. Zobacz także: Odchylenie standardowe.
 Obsługiwane typy wartości: *Float*, *Integer*.
 Obsługiwana funkcja foreach: *last_foreach*.

Parametry: zobacz wspólne parametry.

Przykład:

```
stddevpop(/host/key,1h) #odchylenie standardowe populacji dla ostatniej godziny do teraz
```

stddevsamp(/host/key,(sec|#num)<:time shift>)

Odchylenie standardowe z próby dla zebranych wartości w zdefiniowanym okresie obliczania. Zobacz także: Odchylenie standardowe.
 Obsługiwane typy wartości: *Float*, *Integer*.
 Obsługiwana funkcja foreach: *last_foreach*.

Parametry: zobacz wspólne parametry.

Do działania tej funkcji wymagane są co najmniej dwie wartości danych.

Przykład:

```
stddevsamp(/host/key,1h) #odchylenie standardowe z próby dla ostatniej godziny do chwili obecnej
```

sum(/host/key,(sec|#num)<:time shift>)

Suma zebranych wartości w zdefiniowanym okresie obliczania.
 Obsługiwane typy wartości: *Float*, *Integer*.
 Obsługiwane funkcje foreach: *avg_foreach*, *count_foreach*, *exists_foreach*, *last_foreach*, *max_foreach*, *min_foreach*, *sum_foreach*.

Parametry: zobacz wspólne parametry.

Przykład:

```
sum(/host/key,1h) #suma wartości z ostatniej godziny do teraz
```

sumofsquares(/host/key,(sec|#num)<:time shift>)

Suma kwadratów zebranych wartości w zdefiniowanym okresie obliczania.
 Obsługiwane typy wartości: *Float*, *Integer*.
 Obsługiwana funkcja foreach: *last_foreach*.

Parametry: zobacz wspólne parametry.

Przykład:

```
sumofsquares(/host/key,1h) #suma kwadratów za ostatnią godzinę do teraz
```

varpop(/host/key,(sec|#num)<:time shift>)

Wariancja populacji zebranych wartości w zdefiniowanym okresie obliczania. Zobacz także: Wariancja.
 Obsługiwane typy wartości: *Float*, *Integer*.
 Obsługiwana funkcja foreach: *last_foreach*.

Parametry: zobacz wspólne parametry.

Przykład:

```
varpop(/host/key,1h) #wariancja populacji za ostatnią godzinę do teraz
```

varsamp(/host/key,(sec|#num)<:time shift>)

Wariancja z próby zebranych wartości w zdefiniowanym okresie obliczania. Zobacz także: Variance.
 Obsługiwane typy wartości: *Float*, *Integer*.
 Obsługiwana funkcja foreach: *last_foreach*.

Parametry: zobacz wspólne parametry.

Do działania tej funkcji wymagane są co najmniej dwie wartości danych.

Przykład:

```
varsamp(/host/key,1h) #wariancja z próby dla ostatniej godziny do teraz
```

Zobacz wszystkie obsługiwane funkcje.

Funkcje foreach

Przegląd

Funkcje foreach są używane w obliczeniach agregujących do zwracania jednej wartości zagregowanej dla każdej pozycji wybranej przez użyty **filtr pozycji**. Zwracana jest tablica wartości.

Attention:
Funkcje foreach są obsługiwane wyłącznie w ramach pozycji obliczanych jako część formuł obliczeń agregujących. Nie można ich wywoływać w zwykłych kluczach pozycji ani w wyrażeniach wyzwalaczy poza tym kontekstem.

Na przykład funkcja *avg_foreach* zwróci tablicę wartości, gdzie każda wartość jest *średnią* wartością historyczną wybranej pozycji w określonym przedziale czasu.

Filtr pozycji jest częścią składni używanej przez funkcje foreach. W filtrze pozycji obsługiwane jest użycie symboli wieloznacznych, dzięki czemu wymagane pozycje można wybierać w bardzo elastyczny sposób.

Obsługiwane funkcje

Function	Description
avg_foreach	Zwraca średnią wartość dla każdej pozycji.
bucket_rate_foreach	Zwraca pary (górna granica koszyka, wartość współczynnika) odpowiednie do użycia w funkcji histogram_quantile(), gdzie „górna granica koszyka” jest wartością parametru klucza pozycji zdefiniowanego przez <parameter number> parametr.
count_foreach	Zwraca liczbę wartości dla każdej pozycji.
exists_foreach	Zwraca „1” dla każdej włączonej pozycji.
last_foreach	Zwraca ostatnią wartość dla każdej pozycji.
max_foreach	Zwraca maksymalną wartość dla każdej pozycji.
min_foreach	Zwraca minimalną wartość dla każdej pozycji.
sum_foreach	Zwraca sumę wartości dla każdej pozycji.

Składnia funkcji

Funkcje foreach obsługują dwa wspólne parametry: `filtr pozycji` (szczegóły poniżej) oraz `okres czasu`:

```
foreach_function(item filter,time period)
```

Na przykład:

```
avg_foreach(/*/mysql.qps?[group="MySQL Servers"],5m)
```

zwróci pięciominutową średnią dla każdej pozycji „mysql.qps” w grupie serwerów MySQL.

Należy pamiętać, że niektóre funkcje obsługują dodatkowe parametry.

Składnia filtra pozycji

Filtr pozycji:

`/host/key[parameters]?[conditions]`

składa się z czterech części, gdzie:

- host - nazwa hosta
- key - klucz pozycji (bez parametrów)
- parameters - parametry klucza pozycji
- conditions - warunki oparte na grupie hostów i/lub tagach pozycji (w postaci wyrażenia)

Spacje są dozwolone wyłącznie wewnątrz wyrażenia warunków.

Użycie symbolu wieloznacznego

- Symbol wieloznaczny może być użyty do zastąpienia nazwy hosta, klucza pozycji lub pojedynczego parametru klucza pozycji.
- Albo host, albo klucz pozycji musi być określony bez symbolu wieloznacznego. Dlatego `/host/*` i `/*/key` są poprawnymi filtrami, ale `/*/*` jest nieprawidłowy.
- Symbol wieloznaczny nie może być użyty dla *części* nazwy hosta, klucza pozycji ani parametru klucza pozycji.
- Symbol wieloznaczny nie dopasowuje więcej niż jednego parametru klucza pozycji. Dlatego symbol wieloznaczny musi być określony osobno dla każdego parametru (tj. `key[abc,*,*]`).

Wyrażenie warunków

Wyrażenie warunków obsługuje:

- operandy:
  - group - grupa hostów
  - tag - tag pozycji
  - `"<text>"` - stała tekstowa, ze znakiem ucieczki \ do poprzedzania " i \
- operatory porównania ciągów znaków z rozróżnianiem wielkości liter: =, <>
- operatory logiczne: `and`, `or`, `not`
- grupowanie za pomocą nawiasów: ( )

Ujęcie stałych tekstowych w cudzysłów jest obowiązkowe. Obsługiwane jest tylko pełne porównanie ciągów znaków z rozróżnianiem wielkości liter.

Warning:
Podczas określania tagów w filtrze (tj. `tag="tagname:value"`), dwukropek ":" jest używany jako separator. Wszystko po nim jest traktowane jako wartość tagu. Dlatego obecnie nie jest obsługiwane określanie nazwy tagu zawierającej ":".

Przykłady

Można użyć złożonego filtra odwołującego się do klucza pozycji, grupy hostów i tagów, co ilustrują poniższe przykłady:

Przykład składni	Opis
`/host/key[abc,*]`	Dopasowuje podobne pozycje na tym hoście.
`/*/key`	Dopasowuje tę samą pozycję dowolnego hosta.
`/*/key?[group="ABC" and tag="tagname:value"]`	Dopasowuje tę samą pozycję dowolnego hosta z grupy ABC mającego tagi 'tagname:value'.
`/*/key[a,*,c]?[(group="ABC" and tag="Tag1") or (group="DEF" and (tag="Tag2" or tag="Tag3:value"))]`	Dopasowuje podobne pozycje dowolnego hosta z grupy ABC lub DEF z odpowiednimi tagami.

Wszystkie pozycje, do których istnieją odwołania, muszą istnieć i zbierać dane. W obliczeniach uwzględniane są tylko włączone pozycje na włączonych hostach. Pozycje w stanie nieobsługiwanym nie są uwzględniane.

Attention:
Jeśli klucz pozycji, do której istnieje odwołanie, zostanie zmieniony, filtr musi zostać zaktualizowany ręcznie.

Określenie nadrzędnej grupy hostów obejmuje grupę nadrzędną oraz wszystkie zagnieżdżone grupy hostów wraz z ich pozycjami.

Okres czasu

Drugi parametr pozwala określić okres czasu dla agregacji. Okres czasu może być wyrażony wyłącznie jako czas; liczba wartości (poprzedzona prefiksem **#**) nie jest obsługiwana.

Dla wygody w tym parametrze można używać obsługiwanych symboli jednostek, na przykład „5m” (pięć minut) zamiast „300s” (300 sekund) lub „1d” (jeden dzień) zamiast „86400” (86400 sekund).

W przypadku funkcji *last_foreach* okres czasu jest parametrem opcjonalnym (obsługiwanym od Zabbix 7.0), który można pominąć:

```
last_foreach(/*/key?[group="host group"])
```

Okres czasu nie jest obsługiwany przez funkcję *exists_foreach*.

Dodatkowe parametry

bucket_rate_foreach

Trzeci opcjonalny parametr jest obsługiwany przez funkcję *bucket_rate_foreach*:

```
bucket_rate_foreach(item filter,time period,<parameter number>)
```

gdzie <parameter number> to pozycja wartości „bucket” w kluczu pozycji. Na przykład, jeśli wartość „bucket” w myItem[aaa,0.2] to „0.2”, to jej pozycja wynosi 2.

Domyślna wartość <parameter number> to „1”.

count_foreach

Trzeci i czwarty opcjonalny parametr są obsługiwane przez funkcję *count_foreach*:

```
count_foreach(item filter,time period,<operator>,<pattern>)
```

Gdzie:

- **operator** to operator warunkowy dla wartości pozycji (musi być ujęty w podwójny cudzysłów). Obsługiwane `operators`:
eq - równe
ne - nierówne
gt - większe
ge - większe lub równe
lt - mniejsze
le - mniejsze lub równe
like - pasuje, jeśli zawiera wzorzec (z rozróżnianiem wielkości liter)
bitand - bitowe AND
regexp - dopasowanie z rozróżnianiem wielkości liter do wyrażenia regularnego podanego w `pattern`
iregexp - dopasowanie bez rozróżniania wielkości liter do wyrażenia regularnego podanego w `pattern`
- **pattern** to wymagany wzorzec (argumenty tekstowe muszą być ujęte w podwójny cudzysłów); obsługiwany, jeśli *operator* jest określony w trzecim parametrze.

Uwagi:

- Opcjonalnych parametrów *operator* lub *pattern* nie można pozostawić pustych po przecinku, można je tylko całkowicie pominąć.
- Gdy jako trzeci parametr użyto *bitand*, czwarty parametr `pattern` można określić jako dwie liczby rozdzielone znakiem '/': **number_to_compare_with/mask**. count_foreach() oblicza „bitowe AND” z wartości i *mask* oraz porównuje wynik z *number_to_compare_with*. Jeśli wynik „bitowego AND” jest równy *number_to_compare_with*, wartość jest zliczana.
Jeśli *number_to_compare_with* i *mask* są równe, wystarczy podać tylko *mask* (bez '/').
- Gdy jako trzeci parametr użyto *regexp* lub *iregexp*, czwarty parametr `pattern` może być zwykłym lub globalnym (zaczynającym się od '@') wyrażeniem regularnym. W przypadku globalnych wyrażeń regularnych rozróżnianie wielkości liter jest dziedziczone z ustawień globalnych wyrażeń regularnych. Na potrzeby dopasowania regexp wartości zmiennoprzecinkowe będą zawsze przedstawiane z 4 cyframi dziesiętnymi po '.'. Należy również pamiętać, że w przypadku dużych liczb różnica między reprezentacją dziesiętną (przechowywaną w bazie danych) a binarną (używaną przez serwer Zabbix) może wpływać na 4. cyfrę dziesiętną.

Więcej szczegółów i przykładów użycia funkcji foreach można znaleźć w sekcji obliczenia agregowane.

Zachowanie zależne od dostępności

Poniższa tabela ilustruje, jak każda funkcja zachowuje się w przypadkach ograniczonej dostępności hosta/pozycji oraz danych historycznych.

Function	Disabled host	Unavailable host with data	Unavailable host without data	Disabled item	Unsupported item	Data retrieval error (SQL)
avg_foreach	ignoruj	zwróć średnią	ignoruj	ignoruj	ignoruj	ignoruj
bucket_rate_foreach	ignoruj	zwróć bucket rate	ignoruj	ignoruj	ignoruj	ignoruj
count_foreach	ignoruj	zwróć liczbę	0	ignoruj	ignoruj	ignoruj
exists_foreach	ignoruj	1	1	ignoruj	1	n/d
last_foreach	ignoruj	zwróć ostatnią wartość	ignoruj	ignoruj	ignoruj	ignoruj
max_foreach	ignoruj	zwróć maksimum	ignoruj	ignoruj	ignoruj	ignoruj

Function	Disabled host	Unavailable host with data	Unavailable host without data	Disabled item	Unsupported item	Data retrieval error (SQL)
min_foreach	ignoruj	zwróć minimum	ignoruj	ignoruj	ignoruj	ignoruj
sum_foreach	ignoruj	zwróć sumę	ignoruj	ignoruj	ignoruj	ignoruj

Jeśli pozycja jest *ignorowana*, nic nie jest dodawane do agregacji.

2 Funkcje bitowe

Wszystkie wymienione tutaj funkcje są obsługiwane w:

- Wyrażeniach wyzwalaczy
- Pozycjach obliczanych
- Makrach wyrażeń

Funkcje są wymienione bez dodatkowych informacji. Kliknij funkcję, aby zobaczyć pełne szczegóły.

Function	Description
bitand	Wartość „bitowego AND” wartości pozycji i maski.
bitlshift	Bitowe przesunięcie w lewo wartości pozycji.
bitnot	Wartość „bitowego NOT” wartości pozycji.
bitor	Wartość „bitowego OR” wartości pozycji i maski.
bitrshift	Bitowe przesunięcie w prawo wartości pozycji.
bitxor	Wartość „bitowego wykluczającego OR” wartości pozycji i maski.

Szczegóły funkcji

Kilka ogólnych uwag dotyczących parametrów funkcji:

- Parametry funkcji są oddzielane przecinkiem
- Wyrażenia są akceptowane jako parametry
- Opcjonalne parametry funkcji (lub części parametrów) są oznaczone przez < >

bitand(value,mask)

Wartość operacji „bitwise AND” wartości pozycji i maski.
 Obsługiwane typy wartości: *Integer*.

Parametry:

- **value** — wartość do sprawdzenia;
- **mask** (wymagane) — 64-bitowa liczba całkowita bez znaku (0 - 18446744073709551615).

Chociaż porównanie jest wykonywane bitowo, wszystkie wartości muszą być podawane i są zwracane w postaci dziesiętnej. Na przykład sprawdzenie 3. bitu wykonuje się przez porównanie do 4, a nie 100.

Przykłady:

```
bitand(last(/host/key),12)=8 or bitand(last(/host/key),12)=4 #ustawiony 3. lub 4. bit, ale nie oba jednocz
bitand(last(/host/key),20)=16 #3. bit nie jest ustawiony, a 5. bit jest ustawiony
```

bitlshift(value,bits to shift)

Przesunięcie bitowe w lewo wartości pozycji.
 Obsługiwane typy wartości: *Integer*.

Parametry:

- **value** - wartość do sprawdzenia;
- **bits to shift** (wymagane) - liczba bitów do przesunięcia.

Chociaż porównanie jest wykonywane w sposób bitowy, wszystkie wartości muszą być podawane i są zwracane w postaci dziesiętnej. Na przykład sprawdzenie 3. bitu odbywa się przez porównanie do 4, a nie 100.

bitnot(value)

Wartość operacji „bitwise NOT” dla wartości pozycji.
 Obsługiwane typy wartości: *Integer*.

Parametr:

- **value** — wartość do sprawdzenia.

Chociaż porównanie jest wykonywane bitowo, wszystkie wartości muszą być podawane i są zwracane w postaci dziesiętnej. Na przykład sprawdzenie 3. bitu odbywa się przez porównanie z 4, a nie 100.

bitor(value,mask)

Wartość operacji „bitwise OR” dla wartości pozycji i maski.
 Obsługiwane typy wartości: *Integer*.

Parametry:

- **value** - wartość do sprawdzenia;
- **mask** (wymagane) - 64-bitowa liczba całkowita bez znaku (0 - 18446744073709551615).

Chociaż porównanie jest wykonywane bitowo, wszystkie wartości muszą być podawane i zwracane w postaci dziesiętnej. Na przykład sprawdzenie 3. bitu wykonuje się przez porównanie z 4, a nie 100.

bitrshift(value,bits to shift)

Przesunięcie bitowe w prawo wartości pozycji.
 Obsługiwane typy wartości: *Integer*.

Parametry:

- **value** - wartość do sprawdzenia;
- **bits to shift** (wymagane) - liczba bitów do przesunięcia.

Chociaż porównanie jest wykonywane w sposób bitowy, wszystkie wartości muszą być podane i są zwracane w postaci dziesiętnej. Na przykład sprawdzenie 3. bitu odbywa się przez porównanie z 4, a nie 100.

bitxor(value,mask)

Wartość operacji „bitowe wykluczające LUB” dla wartości pozycji i maski.
 Obsługiwane typy wartości: *Integer*.

Parametry:

- **value** - wartość do sprawdzenia;
- **mask** (wymagany) - 64-bitowa liczba całkowita bez znaku (0 - 18446744073709551615).

Chociaż porównanie jest wykonywane bitowo, wszystkie wartości muszą być podawane i zwracane w postaci dziesiętnej. Na przykład sprawdzenie 3. bitu odbywa się przez porównanie z wartością 4, a nie 100.

Zobacz wszystkie obsługiwane funkcje.

3 Funkcje daty i czasu

Wszystkie wymienione tutaj funkcje są obsługiwane w:

- Wyrażeniach wyzwalaczy
- Pozycjach obliczanych
- Makrach wyrażeń

Attention:
Funkcje daty i czasu nie mogą być używane samodzielnie w wyrażeniu; w wyrażeniu musi być uwzględniona co najmniej jedna funkcja z innej grupy, odwołująca się do pozycji hosta (z wyjątkiem funkcji nodata()). Szczegółowe informacje o tym, jak funkcje daty i czasu działają w wyrażeniach, można znaleźć w sekcji Czas obliczania.

Funkcje są wymienione bez dodatkowych informacji. Kliknij funkcję, aby zobaczyć pełne szczegóły.

Funkcja	Opis
date	Bieżąca data w formacie YYYYMMDD.
dayofmonth	Dzień miesiąca z zakresu od 1 do 31.
dayofweek	Dzień tygodnia z zakresu od 1 do 7.
now	Liczba sekund od początku epoki (00:00:00 UTC, 1 stycznia 1970).
time	Bieżący czas w formacie HHMMSS.

Szczegóły funkcji

date

Bieżąca data w formacie YYYYMMDD.

Przykład:

`date()<20220101`

dayofmonth

Dzień miesiąca w zakresie od 1 do 31.

Przykład:

`dayofmonth()=1`

dayofweek

Dzień tygodnia w zakresie od 1 do 7 (pon. - 1, niedz. - 7).

Przykład (tylko dni robocze):

`dayofweek()<6`

Przykład (tylko weekend):

`dayofweek()>5`

now

Liczba sekund od Epoki (00:00:00 UTC, 1 stycznia 1970).

Przykład:

`now()<1640998800`

time

Bieżący czas w formacie HHMMSS.

Przykład (tylko pora nocna, 00:00-06:00):

`time()<060000`

Zobacz wszystkie obsługiwane funkcje.

4 Funkcje historii

Wszystkie wymienione tutaj funkcje są obsługiwane w:

- Wyrażeniach wyzwalaczy
- Pozycjach obliczanych
- Makrach wyrażeń

Funkcje są wymienione bez dodatkowych informacji. Kliknij funkcję, aby zobaczyć pełne szczegóły.

Function	Description
change	Wielkość różnicy między poprzednią a najnowszą wartością.
changecount	Liczba zmian między sąsiednimi wartościami w zdefiniowanym okresie obliczania.
count	Liczba wartości w zdefiniowanym okresie obliczania.
countunique	Liczba unikalnych wartości w zdefiniowanym okresie obliczania.
find	Znajdź dopasowanie wartości w zdefiniowanym okresie obliczania.
first	Pierwsza (najstarsza) wartość w zdefiniowanym okresie obliczania.
firstclock	Znacznik czasu pierwszej (najstarszej) wartości w zdefiniowanym okresie obliczania.
fuzzytime	Sprawdź, jak bardzo czas pasywnego agent różni się od czasu serwer/proxy Zabbix.
last	Najnowsza wartość.
lastclock	Znacznik czasu N-tej najnowszej wartości w zdefiniowanym okresie obliczania.
logeventid	Sprawdź, czy identyfikator zdarzenia ostatniego wpisu logu pasuje do wyrażenia regularnego.
logseverity	Poziom ważności logu ostatniego wpisu logu.
logsource	Sprawdź, czy źródło logu ostatniego wpisu logu pasuje do wyrażenia regularnego.
logtimestamp	Znacznik czasu komunikatu logu dla N-tej najnowszej wartości pozycja logu.
monodec	Sprawdź, czy wystąpił monotoniczny spadek wartości.
monoinc	Sprawdź, czy wystąpił monotoniczny wzrost wartości.
nodata	Sprawdź, czy nie odebrano danych.
percentile	P-ty percentyl okresu, gdzie P (wartość procentowa) jest określone przez trzeci parametr.
rate	Średnie tempo wzrostu na sekundę dla monotonicznie rosnącego licznika w zdefiniowanym okresie czasu.

Wspólne parametry

- `/host/key` to wspólny obowiązkowy pierwszy parametr dla funkcji odwołujących się do historii pozycji hosta
- `(sec|#num)<:time shift>` to wspólny drugi parametr dla funkcji odwołujących się do historii pozycji hosta, gdzie:
  - **sec** - maksymalny okres obliczania w sekundach (mogą być używane sufiksy czasu), lub
  - **#num** - maksymalny zakres obliczania w ostatnio zebranych wartościach (jeśli jest poprzedzony znakiem kratki)
  - **time shift** (opcjonalnie) pozwala przesunąć punkt obliczania wstecz w czasie. Zobacz więcej szczegółów dotyczących określania przesunięcia czasu.

Szczegóły funkcji

Kilka ogólnych uwag dotyczących parametrów funkcji:

- Parametry funkcji są oddzielane przecinkiem
- Opcjonalne parametry funkcji (lub części parametrów) są oznaczone za pomocą < >
- Parametry specyficzne dla danej funkcji są opisane przy każdej funkcji
- Parametry `/host/key` oraz `(sec|#num)<:time shift>` nigdy nie mogą być ujmowane w cudzysłów

change(/host/key)

Wielkość różnicy między poprzednią a najnowszą wartością.
 Obsługiwane typy wartości: *Float*, *Integer*, *String*, *Text*, *Log*.
 Dla ciągów znaków zwraca: 0 - wartości są równe; 1 - wartości różnią się.

Parametry: zobacz wspólne parametry.

Uwagi:

- Zostanie obliczona różnica liczbowa, jak pokazano na poniższych przykładowych wartościach wejściowych („poprzednia” i „najnowsza” wartość = różnica):
’1’ i ’5’ = +4
’3’ i ’1’ = −2
’0’ i ’-2.5’ = −2.5.
- W wyzwalaczach funkcja jest przydatna do wykrywania nagłych skoków (lub spadków), resetów liczników oraz przejść stanów liczbowych.
- Zobacz także: abs do porównania.

Przykłady:

```
change(/host/system.uptime)<0 #zmiana czasu działania systemu była ujemna od ostatniej wartości (wskazuje
change(/host/system.cpu.load[all,avg1])>2 #obciążenie CPU (w ciągu jednej minuty) wzrosło o więcej niż 2 c
change(/host/vfs.fs.size[/,free])<-1G #ilość wolnego miejsca na dysku spadła o więcej niż 1 GB między kole
```

changecount(/host/key,(sec|#num)<:time shift>,<mode>)

Liczba zmian między sąsiednimi wartościami w zdefiniowanym okresie obliczania.
 Obsługiwane typy wartości: *Float*, *Integer*, *String*, *Text*, *Log*.

Parametry:

- Zobacz wspólne parametry
- **mode** (musi być ujęty w podwójny cudzysłów) — możliwe wartości: *all* — zliczaj wszystkie zmiany (domyślnie); *dec* — zliczaj spadki; *inc* — zliczaj wzrosty

Uwagi:

- Dla nienumerycznych typów wartości parametr *mode* jest ignorowany.
- W wyzwalaczach przydatne do wykrywania częstych zmian stanu (wskazujących na niestabilność).

Przykłady:

```
changecount(/host/icmpping,10m)>5 #status ping zmienił się więcej niż 5 razy w ciągu 10 minut
changecount(/host/vfs.file.contents["/sys/class/net/eth0/operstate"],1h)>5 #stan operacyjny eth0 zmienił s
changecount(/host/proc.num[httpd],15m)>10 #liczba procesów httpd zmieniła się więcej niż 10 razy w ciągu 1
changecount(/host/key,#10,"inc") #liczba wzrostów wartości (względem wartości sąsiedniej) wśród ostatnich
changecount(/host/key,24h,"dec") #liczba spadków wartości (względem wartości sąsiedniej) w ciągu ostatnich
```

count(/host/key,(sec|#num)<:time shift>,<operator>,<pattern>)

Liczba wartości w zdefiniowanym okresie obliczania.
 Obsługiwane typy wartości: *Float*, *Integer*, *String*, *Text*, *Log*.

Parametry:

- Zobacz wspólne parametry
- **operator** (musi być ujęty w podwójny cudzysłów) Obsługiwane `operatory`:
eq - równe (domyślnie dla integer, float)
ne - nierówne
gt - większe niż
ge - większe lub równe
lt - mniejsze niż
le - mniejsze lub równe
like (domyślnie dla string, text, log) - pasuje, jeśli zawiera wzorzec (z uwzględnieniem wielkości liter)
bitand

- bitowe AND
regexp - dopasowanie z uwzględnieniem wielkości liter do wyrażenia regularnego podanego w `pattern`
iregexp - dopasowanie bez uwzględniania wielkości liter do wyrażenia regularnego podanego w `pattern`
- **pattern** - wymagany wzorzec (argumenty typu string muszą być ujęte w podwójny cudzysłów)

Komentarze:

- Pozycje typu float są dopasowywane z precyzją 2.22e-16.
- *like* nie jest obsługiwany jako operator dla wartości integer.
- *like* i *bitand* nie są obsługiwane jako operatory dla wartości float.
- Dla wartości string, text i log obsługiwane są tylko operatory *eq*, *ne*, *like*, *regexp* i *iregexp*.
- Gdy jako operator używany jest *bitand*, czwarty parametr `pattern` można określić jako dwie liczby rozdzielone znakiem '/': **number_to_compare_with/mask**. count() oblicza „bitowe AND" z wartości i *mask* oraz porównuje wynik z *number_to_compare_with*. Jeśli wynik „bitowego AND" jest równy *number_to_compare_with*, wartość jest zliczana.
Jeśli *number_to_compare_with* i *mask* są równe, wystarczy podać tylko *mask* (bez '/').
- Gdy jako operator używany jest *regexp* lub *iregexp*, czwarty parametr `pattern` może być zwykłym lub globalnym (zaczynającym się od '@') wyrażeniem regularnym. W przypadku globalnych wyrażeń regularnych rozróżnianie wielkości liter jest dziedziczone z ustawień globalnych wyrażeń regularnych. Na potrzeby dopasowania regexp wartości float będą zawsze przedstawiane z 4 cyframi dziesiętnymi po '.'. Należy również pamiętać, że w przypadku dużych liczb różnica między reprezentacją dziesiętną (przechowywaną w bazie danych) a binarną (używaną przez serwer Zabbix) może wpływać na 4. cyfrę po przecinku.

Przykłady:

```
count(/host/icmpping,30m,,"0")>5 #ping has failed more than 5 times in 30 minutes
count(/host/key,10m,"like","error") #the number of values for the last 10 minutes until now that contain '
count(/host/key,10m,,12) #the number of values for the last 10 minutes until now that equal '12'
count(/host/key,10m,"gt",12) #the number of values for the last 10 minutes until now that are over '12'
count(/host/key,#10,"gt",12) #the number of values within the last 10 values until now that are over '12'
count(/host/key,10m:now-1d,"gt",12) #the number of values between 24 hours and 10 minutes and 24 hours ago
count(/host/key,10m,"bitand","6/7") #the number of values for the last 10 minutes until now having '110' (
count(/host/key,10m:now-1d) #the number of values between 24 hours and 10 minutes and 24 hours ago from no
```

countunique(/host/key,(sec|#num)<:time shift>,<operator>,<pattern>)

Liczba unikalnych wartości w zdefiniowanym okresie obliczania.
 Obsługiwane typy wartości: *Float*, *Integer*, *String*, *Text*, *Log*.

Parametry:

- Zobacz wspólne parametry
- **operator** (musi być ujęty w podwójny cudzysłów). Obsługiwane `operators`:
eq - równe (domyślnie dla integer, float)
ne - nierówne
gt - większe niż
ge - większe lub równe
lt - mniejsze niż
le - mniejsze lub równe
like (domyślnie dla string, text, log) - pasuje, jeśli zawiera wzorzec (z rozróżnianiem wielkości liter)
bitand - bitowe AND
regexp - dopasowanie z rozróżnianiem wielkości liter do wyrażenia regularnego podanego w `pattern`
iregexp - dopasowanie bez rozróżniania wielkości liter do wyrażenia regularnego podanego w `pattern`
- **pattern** - wymagany wzorzec (argumenty typu string muszą być ujęte w podwójny cudzysłów)

Uwagi:

- Pozycje typu float są dopasowywane z precyzją 2.22e-16.
- *like* nie jest obsługiwany jako operator dla wartości integer.
- *like* i *bitand* nie są obsługiwane jako operatory dla wartości float.
- Dla wartości string, text i log obsługiwane są tylko operatory *eq*, *ne*, *like*, *regexp* oraz *iregexp*.
- Przy użyciu *bitand* jako operatora, czwarty parametr `pattern` można określić jako dwie liczby rozdzielone znakiem '/': **number_to_compare_with/mask**. countunique() oblicza „bitowe AND" z wartości i *mask*, a następnie porównuje wynik z *number_to_compare_with*. Jeśli wynik „bitowego AND" jest równy *number_to_compare_with*, wartość jest zliczana.
Jeśli *number_to_compare_with* i *mask* są równe, wystarczy podać tylko *mask* (bez '/').
- Przy użyciu *regexp* lub *iregexp* jako operatora, czwarty parametr `pattern` może być zwykłym lub globalnym (zaczynającym się od '@') wyrażeniem regularnym. W przypadku globalnych wyrażeń regularnych rozróżnianie wielkości liter jest dziedziczone z ustawień globalnych wyrażeń regularnych. Na potrzeby dopasowania regexp wartości float będą zawsze przedstawiane z 4 cyframi dziesiętnymi po '.'. Należy również pamiętać, że w przypadku dużych liczb różnica między reprezentacją dziesiętną (przechowywaną w bazie danych) a binarną (używaną przez serwer Zabbix) może wpływać na 4. cyfrę dziesiętną.

Przykłady:

```
countunique(/host/key,10m) #liczba unikalnych wartości z ostatnich 10 minut do teraz
countunique(/host/key,10m,"like","error") #liczba unikalnych wartości z ostatnich 10 minut do teraz, które
countunique(/host/key,10m,,12) #liczba unikalnych wartości z ostatnich 10 minut do teraz równych '12'
countunique(/host/key,10m,"gt",12) #liczba unikalnych wartości z ostatnich 10 minut do teraz większych niż
countunique(/host/key,#10,"gt",12) #liczba unikalnych wartości wśród ostatnich 10 wartości do teraz większ
```

```
countunique(/host/key,10m:now-1d,"gt",12) #liczba unikalnych wartości między 24 godzinami i 10 minutami te
countunique(/host/key,10m,"bitand","6/7") #liczba unikalnych wartości z ostatnich 10 minut do teraz mający
countunique(/host/key,10m:now-1d) #liczba unikalnych wartości między 24 godzinami i 10 minutami temu a 24
```

find(/host/key,(sec|#num)<:time shift>,<operator>,<pattern>)

Znajduje dopasowanie wartości w zdefiniowanym okresie obliczania.
 Obsługiwane typy wartości: *Float*, *Integer*, *String*, *Text*, *Log*.
 Zwraca: 1 - znaleziono; 0 - w przeciwnym razie.

Parametry:

- Zobacz wspólne parametry
- **sec** lub **#num** (opcjonalne) - jeśli nie podano, domyślnie używana jest najnowsza wartość
- **operator** (musi być ujęty w podwójny cudzysłów) Obsługiwane `operatory`:
eq - równe (domyślnie dla integer, float)
ne - nierówne
gt - większe niż
ge - większe lub równe
lt - mniejsze niż
le - mniejsze lub równe
like (domyślnie dla string, text, log) - dopasowuje, jeśli zawiera ciąg znaków podany w `pattern` (z uwzględnieniem wielkości liter)
bitand - bitowe AND
regexp - dopasowanie z uwzględnieniem wielkości liter do wyrażenia regularnego podanego w `pattern`
iregexp - dopasowanie bez uwzględniania wielkości liter do wyrażenia regularnego podanego w `pattern`
- **pattern** - wymagany wzorzec (argumenty typu string muszą być ujęte w podwójny cudzysłów); wyrażenie regularne Perl Compatible Regular Expression (PCRE), jeśli `operator` to *regexp*, *iregexp*

Uwagi:

- Jeśli przetwarzana jest więcej niż jedna wartość, zwracane jest '1', jeśli istnieje co najmniej jedna pasująca wartość.
- *like* nie jest obsługiwany jako operator dla wartości integer.
- *like* i *bitand* nie są obsługiwane jako operatory dla wartości float.
- Dla wartości string, text i log obsługiwane są tylko operatory *eq*, *ne*, *like*, *regexp* i *iregexp*.
- Gdy jako operator użyto *regexp* lub *iregexp*, czwarty parametr `pattern` może być zwykłym lub globalnym (zaczynającym się od '@') wyrażeniem regularnym. W przypadku globalnych wyrażeń regularnych rozróżnianie wielkości liter jest dziedziczone z ustawień globalnego wyrażenia regularnego.

Przykłady:

```
find(/host/key,10m,"like","error") #znajdź wartość zawierającą 'error' w ciągu ostatnich 10 minut do teraz
find(/host/agent.version,,"like","beta")=1 #agent Zabbix ma wersję beta, musi zostać zaktualizowany
find(/host/log[/var/log/nginx/access.log],,"regexp"," 500 ")=1 #znaleziono wewnętrzny błąd serwera WWW
```

first(/host/key,sec<:time shift>)

Pierwsza (najstarsza) wartość w zdefiniowanym okresie obliczania.
 Obsługiwane typy wartości: *Float*, *Integer*, *String*, *Text*, *Log*.

Parametry:

- Zobacz wspólne parametry

Zobacz także last().

Przykład:

```
first(/host/key,1h) #retrieve the oldest value within the last hour until now
```

firstclock(/host/key,sec<:time shift>)

Znacznik czasu najstarszej wartości w zdefiniowanym okresie obliczania.
 Obsługiwane typy wartości: *Float*, *Integer*, *String*, *Text*, *Log*.

Parametry:

- Zobacz wspólne parametry.

Funkcja kończy się błędem, jeśli w podanym okresie nie zebrano żadnych danych.

Zobacz także lastclock().

Przykłady:

```
firstclock(/host/key,1h) #pobierz znacznik czasu najstarszej wartości z ostatniej godziny
firstclock(/host/key,1h:now-24h) #pobierz znacznik czasu najstarszej wartości z ostatniej godziny sprzed d
```

fuzzytime(/host/key,sec)

Sprawdza, jak bardzo czas pasywnego agenta różni się od czasu serwera/proxy Zabbix.
 Obsługiwane typy wartości: *Float*, *Integer*.
 Zwraca: 1 - różnica między wartością pasywnej pozycji (jako znacznik czasu) a znacznikiem czasu serwera/proxy Zabbix (czasem pobrania wartości) jest mniejsza lub równa *sec* sekund; 0 - w przeciwnym razie.

Parametry:

- Zobacz wspólne parametry.

Komentarze:

- Zwykle używane z pozycją 'system.localtime' do sprawdzenia, czy czas lokalny jest zsynchronizowany z czasem lokalnym serwera Zabbix. *Uwaga*: dla agenta Zabbix pozycja 'system.localtime' musi być skonfigurowana jako sprawdzenie pasywne; w Zabbix agent 2 może być skonfigurowana jako sprawdzenie aktywne.
- Może być również używane z kluczem `vfs.file.time[/path/file,modify]` do sprawdzenia, czy plik nie był aktualizowany przez długi czas.
- Ta funkcja nie jest zalecana do użycia w złożonych wyrażeniach wyzwalaczy (z wieloma pozycjami), ponieważ może powodować nieoczekiwane wyniki (różnica czasu będzie mierzona względem najnowszej metryki), np. w `fuzzytime(/Host/system.l or last(/Host/trap)<>0`.

Przykłady:

```
fuzzytime(/host/system.localtime,5m)=0 #czas lokalny klienta różni się od czasu serwera/proxy Zabbix o wię
fuzzytime(/host/system.localtime,5m)=0 and nodata(/host/system.localtime,10m)=0 #czas lokalny klienta różn
```

last(/host/key,<#num<:time shift»)

Najnowsza wartość.
 Obsługiwane typy wartości: *Float*, *Integer*, *String*, *Text*, *Log*.

Parametry:

- Zobacz wspólne parametry
- **#num** (opcjonalnie) — N-ta najnowsza wartość

Uwagi:

- Należy zwrócić uwagę, że okres czasu oznaczony hashem (#N) działa tutaj inaczej niż w przypadku wielu innych funkcji. Na przykład: `last(/host/key)` jest zawsze równe `last(/host/key,#1)`; `last(/host/key,#3)` — trzecia najnowsza wartość (*nie* trzy najnowsze wartości).
- Zabbix nie gwarantuje dokładnej kolejności wartości, jeśli w historii istnieje więcej niż dwie wartości w ciągu jednej sekundy.
- Zobacz także first().

Przykłady:

```
last(/host/key) #retrieve the last value
last(/host/key,#2) #retrieve the previous value
last(/host/key,#1)<>last(/host/key,#2) #last two values differ
```

lastclock(/host/key,<#num<:time shift»)

Znacznik czasu N-tej najnowszej wartości w zdefiniowanym okresie obliczania.
 Obsługiwane typy wartości: *Float*, *Integer*, *String*, *Text*, *Log*.

Parametry:

- Zobacz wspólne parametry;
- **#num** (opcjonalnie) — N-ta najnowsza wartość.

Funkcja kończy się błędem, jeśli w podanym okresie nie zebrano żadnych danych lub nie zebrano N-tej wartości.

Zobacz także firstclock().

Przykłady:

```
lastclock(/host/key) #pobierz znacznik czasu najnowszej wartości
lastclock(/host/key,#2) #pobierz znacznik czasu 2. najnowszej wartości
now()-lastclock(/host/heartbeat.item)>300 #minęło więcej niż 5 minut od aktualizacji pozycji heartbeat
lastclock(/host/system.cpu.load[all,avg1])-lastclock(/host/system.cpu.load[all,avg1],#2)>300 #interwał akt
((now()-lastclock(/host/system.cpu.load[all,avg1])<120 and last(/host/system.cpu.load[all,avg1])>5)) #wart
```

logeventid(/host/key,<#num<:time shift»,<pattern>)

Sprawdza, czy identyfikator zdarzenia ostatniego wpisu logu pasuje do wyrażenia regularnego.
 Obsługiwane typy wartości: *Log*.
 Zwraca: 0 - nie pasuje; 1 - pasuje.

Parametry:

- Zobacz wspólne parametry
- **#num** (opcjonalnie) - N-ta najnowsza wartość
- **pattern** (opcjonalnie) - wyrażenie regularne opisujące wymagany wzorzec, w stylu Perl Compatible Regular Expression (PCRE) (argumenty typu string muszą być ujęte w podwójny cudzysłów)

Przykłady:

```
logeventid(/host/eventlog[Security],,"4625")=1 #znaleziono wpis logu z identyfikatorem pasującym do "4625"
logeventid(/host/eventlog[System],,"6008|41")=1 #znaleziono wpis logu z identyfikatorem pasującym do "6008
```

logseverity(/host/key,<#num<:time shift»)

Poziom ważności ostatniego wpisu logu.
 Obsługiwane typy wartości: *Log*.
 Zwraca: 0 - domyślny poziom ważności; N - poziom ważności (liczba całkowita, przydatne dla dzienników zdarzeń Windows: 1 - Informacja, 2 - Ostrzeżenie, 4 - Błąd, 7 - Audyt niepowodzeń, 8 - Audyt powodzeń, 9 - Krytyczny, 10 - Szczegółowy).

Parametry:

- Zobacz wspólne parametry
- **#num** (opcjonalnie) - N-ta najnowsza wartość

Zabbix pobiera poziom ważności logu z pola **Information** dziennika zdarzeń Windows.

Przykłady:

```
logseverity(/host/log[/var/log/syslog],10m)>3 #a log entry with severity above "3" found
logseverity(/host/eventlog[System],10m)=4 #a log entry with severity equaling "Error" found
```

logsource(/host/key,<#num<:time shift»,<pattern>)

Sprawdza, czy źródło logu ostatniego wpisu logu pasuje do wyrażenia regularnego.
 Obsługiwane typy wartości: *Log*.
 Zwraca: 0 - nie pasuje; 1 - pasuje.

Parametry:

- Zobacz wspólne parametry
- **#num** (opcjonalnie) - N-ta najnowsza wartość
- **pattern** (opcjonalnie) - wyrażenie regularne opisujące wymagany wzorzec, w stylu Perl Compatible Regular Expression (PCRE) (argumenty typu string muszą być ujęte w podwójny cudzysłów)

Zwykle używane dla logów zdarzeń systemu Windows.

Przykłady:

```
logsource(/host/eventlog[Application],,"MSSQLSERVER")=1 #znaleziono wpis logu ze źródłem pasującym do "MSS
logsource(/host/eventlog[System],,"Service Control Manager")=1 #znaleziono wpis logu ze źródłem pasującym
logsource(/host/eventlog[System],,"Service Control Manager")=1 and logeventid(/host/eventlog[System],,"703
```

logtimestamp(/host/key,<#num<:time shift»)

Znacznik czasu komunikatu dziennika dla N-tej najnowszej wartości pozycji dziennika.
 Obsługiwane typy wartości: *Log*.

Parametry:

- Zobacz wspólne parametry;
- **#num** (opcjonalnie) — N-ta najnowsza wartość.

Uwagi:

- Obliczanie przesunięcia czasu opiera się na zegarze wartości pozycji, a nie na znaczniku czasu komunikatu dziennika;
- Funkcja kończy się błędem, jeśli:
  - odebrano pozycję typu innego niż log;
  - w podanym okresie nie zebrano żadnych danych;
  - nie zebrano N-tej wartości;
  - komunikat dziennika nie zawiera wartości znacznika czasu.

Przykłady:

```
logtimestamp(/host/key) #retrieve the timestamp of the latest log message
logtimestamp(/host/key,#2) #retrieve the timestamp of the 2nd latest log message
logtimestamp(/host/key,#3:now-1d) #retrieve the timestamp of the 3rd latest log message a day ago
```

monodec(/host/key,(sec|#num)<:time shift>,<mode>)

Sprawdza, czy nastąpił monotoniczny spadek wartości.
 Obsługiwane typy wartości: *Integer*.
 Zwraca: 1 - jeśli wszystkie elementy w okresie czasu stale maleją; 0 - w przeciwnym razie.

Parametry:

- Zobacz wspólne parametry
- **mode** (musi być ujęty w podwójny cudzysłów) - *weak* (każda wartość jest mniejsza lub taka sama jak poprzednia; domyślnie) lub *strict* (każda wartość zmalała)

Przykłady:

```
monodec(/host/system.swap.size[all,free],60s) + monodec(/host2/system.swap.size[all,free],60s) + monodec(/
monodec(/host/proc.num[nginx],10m,"strict")=1 #liczba procesów nginx monotonicznie malała przez 10 minut
```

monoinc(/host/key,(sec|#num)<:time shift>,<mode>)

Sprawdza, czy wystąpił monotoniczny wzrost wartości.
 Obsługiwane typy wartości: *Integer*.
 Zwraca: 1 - jeśli wszystkie elementy w okresie czasu stale rosną; 0 - w przeciwnym razie.

Parametry:

- Zobacz wspólne parametry
- **mode** (musi być ujęty w podwójny cudzysłów) - *weak* (każda wartość jest większa lub taka sama jak poprzednia; domyślnie) lub *strict* (każda wartość wzrosła)

Przykłady:

```
monoinc(/host/system.localtime,#3,"strict")=0 #lokalny czas systemowy nie wzrastał w sposób ciągły
monoinc(/host/vfs.dir.count[/mnt/data/logs],24h,"weak")=0 #wyzwalacz, jeśli liczba plików pozostawała bez
```

nodata(/host/key,sec,<mode>)

Sprawdza brak otrzymanych danych.
 Obsługiwane typy wartości: *Integer*, *Float*, *Character*, *Text*, *Log*.
 Zwraca: 1 - jeśli w zdefiniowanym przedziale czasu nie otrzymano danych; 0 - w przeciwnym razie.

Parametry:

- Zobacz wspólne parametry
- **sec** - okres nie powinien być krótszy niż 30 sekund, ponieważ proces synchronizacji historii oblicza tę funkcję tylko co 30 sekund; `nodata(/host/key,0)` jest niedozwolone
- **mode** - jeśli ustawiono na *strict* (w podwójnych cudzysłowach), ta funkcja będzie niewrażliwa na dostępność proxy (szczegóły w komentarzach)

Komentarze:

- wyzwalacze 'nodata' monitorowane przez proxy są domyślnie wrażliwe na dostępność proxy - jeśli proxy stanie się niedostępne, wyzwalacze 'nodata' nie uruchomią się natychmiast po przywróceniu połączenia, lecz pominą dane za opóźniony okres. Należy pamiętać, że dla pasywnych proxy tłumienie jest aktywowane, jeśli połączenie zostanie przywrócone po więcej niż 15 sekundach i nie mniej niż 2 sekundy później. Dla aktywnych proxy tłumienie jest aktywowane, jeśli połączenie zostanie przywrócone po więcej niż 15 sekundach. Aby wyłączyć wrażliwość na dostępność proxy, użyj trzeciego parametru, np.: `nodata(/host/key,5m,"strict")`; w takim przypadku funkcja uruchomi się, gdy tylko upłynie okres oceny (pięć minut) bez danych.
- Ta funkcja wyświetli błąd, jeśli w okresie określonym przez 1. parametr:
- nie ma danych i serwer Zabbix został uruchomiony ponownie
- nie ma danych i zakończono konserwację
- nie ma danych i pozycja została dodana lub ponownie włączona.
- Błędy są wyświetlane w kolumnie *Info* w konfiguracji wyzwalacza.
- Ta funkcja może nie działać prawidłowo, jeśli występują różnice czasu między serwerem Zabbix, proxy i agentem. Zobacz także: Wymaganie synchronizacji czasu.

Przykład:

```
nodata(/host/agent.ping,5m)=1 #wyzwalacz, jeśli przez 5 minut nie otrzymano danych od agenta Zabbix
```

percentile(/host/key,(sec|#num)<:time shift>,percentage)

P-ty percentyl okresu, gdzie P (percentage) jest określony przez trzeci parametr.
 Obsługiwane typy wartości: *Float*, *Integer*.

Parametry:

- Zobacz wspólne parametry
- **percentage** - liczba zmiennoprzecinkowa z zakresu od 0 do 100 (włącznie), z maksymalnie 4 cyframi po przecinku

Przykłady:

```
percentile(/host/net.if.in[eth0,bytes],1h,95)>1000000 #95. percentyl wejściowego ruchu sieciowego (bajty/s
percentile(/host/system.cpu.util,5m,95)>80 #95. percentyl procentowego wykorzystania CPU w czasie użytkown
percentile(/host/icmppingsec[192.168.0.2],15m,95)>0.15 #większość pomiarów opóźnienia jest poniżej 150 ms,
percentile(/host/net.if.in[eth0,bytes],1h,50) #oblicz 50. percentyl (wartość mediany) przychodzącego ruchu
(percentile(/host/net.if.in[eth0,bytes],1h,50)+percentile(/host/net.if.in[eth0,bytes],1h,51))/2 #oblicz do
```

rate(/host/key,sec<:time shift>)

Średni przyrost na sekundę w monotonicznie rosnącym liczniku w zdefiniowanym okresie czasu.
 Obsługiwane typy wartości: *Float*, *Integer*.

Parametry:

- Zobacz wspólne parametry

Funkcjonalnie odpowiada funkcji 'rate' w PromQL.

Przykłady:

```
rate(/host/key,30s) #jeśli monotoniczny przyrost w ciągu 30 sekund wynosi 20, ta funkcja zwraca 0.67.
rate(/host/net.if.in[eth0,bytes],5m)>500000 #szybkość ruchu przychodzącego interfejsu na eth0 przekroczyła
rate(/host/app.requests.count,1m)>100 #licznik żądań wzrósł do >100 żądań na sekundę w ostatniej minucie
```

Zobacz wszystkie obsługiwane funkcje.

5 Funkcje trendów

Funkcje trendów, w przeciwieństwie do funkcji historii, używają danych trendów do obliczeń.

Trendy przechowują godzinowe wartości zagregowane. Funkcje trendów używają tych godzinowych średnich, dlatego są przydatne do analizy długoterminowej.

Wyniki funkcji trendów są buforowane, więc wielokrotne wywołania tej samej funkcji z tymi samymi parametrami pobierają informacje z bazy danych tylko raz. Pamięć podręczna funkcji trendów jest kontrolowana przez parametr serwera TrendFunctionCacheSize.

Wyzwalacze odwołujące się **wyłącznie** do funkcji trendów są obliczane raz na najmniejszy okres czasu w wyrażeniu. Na przykład wyzwalacz taki jak

```
trendavg(/host/key,1d:now/d) > 1 or trendavg(/host/key2,1w:now/w) > 2
```

będzie obliczany raz dziennie. Jeśli wyzwalacz zawiera zarówno funkcje trendów, jak i historii (lub funkcje daty i czasu i/lub nodata()), jest obliczany zgodnie ze zwykłymi zasadami.

Wszystkie wymienione tutaj funkcje są obsługiwane w:

- Wyrażeniach wyzwalaczy
- Pozycjach obliczanych
- Makrach wyrażeń

Funkcje są wymienione bez dodatkowych informacji. Kliknij funkcję, aby zobaczyć pełne szczegóły.

Function	Description
baselinedev	Zwraca liczbę odchyleń (według algorytmu stddevpop) między ostatnim okresem danych a tymi samymi okresami danych w poprzednich sezonach.
baselinewma	Oblicza linię bazową przez uśrednianie danych z tego samego przedziału czasowego w wielu równych okresach czasu („sezonach") przy użyciu algorytmu ważonej średniej ruchomej.
trendavg	Średnia wartości trendów w zdefiniowanym okresie czasu.
trendcount	Liczba pomyślnie pobranych wartości historii użytych do obliczenia wartości trendu w zdefiniowanym okresie czasu.
trendmax	Maksimum wartości trendów w zdefiniowanym okresie czasu.
trendmin	Minimum wartości trendów w zdefiniowanym okresie czasu.
trendstl	Zwraca współczynnik anomalii w okresie wykrywania — wartość dziesiętną z zakresu od 0 do 1, która jest równa `((liczba wartości anomalii)/(całkowita liczba wartości))`.
trendsum	Suma wartości trendów w zdefiniowanym okresie czasu.

Wspólne parametry

- `/host/key` to wspólny obowiązkowy pierwszy parametr

- `time period:time shift` to wspólny drugi parametr, gdzie:
  - **time period** - okres czasu (minimum „1h”), zdefiniowany jako <N><time unit>, gdzie `N` - liczba jednostek czasu, `time unit` - h (godzina), d (dzień), w (tydzień), M (miesiąc) lub y (rok).
  - **time shift** - przesunięcie okresu czasu (zobacz przykłady funkcji)

Szczegóły funkcji

Kilka ogólnych uwag dotyczących parametrów funkcji:

- Parametry funkcji są oddzielane przecinkiem
- Opcjonalne parametry funkcji (lub części parametrów) są oznaczane za pomocą < >
- Parametry specyficzne dla danej funkcji są opisane przy każdej funkcji
- Parametry `/host/key` oraz `time period:time shift` nigdy nie mogą być ujmowane w cudzysłów

baselinedev(/host/key,data period:time shift,season unit,num seasons)

Zwraca liczbę odchyleń (według algorytmu stddevpop) między ostatnim okresem danych a tymi samymi okresami danych w poprzednich sezonach.

Parametry:

- Zobacz wspólne parametry
- **data period** - okres zbierania danych w ramach sezonu, zdefiniowany jako <N><time unit>, gdzie:
`N` - liczba jednostek czasu
`time unit` - h (godzina), d (dzień), w (tydzień), M (miesiąc) lub y (rok), musi być równa sezonowi lub od niego mniejsza
- **season unit** - jednostka kalendarzowa definiująca jeden sezon (h, d, w, M, y); nie może być mniejsza niż data period
- **num seasons** - liczba sezonów do oceny

Przykłady:

```
baselinedev(/host/key,1d:now/d,"M",6) #obliczanie liczby odchyleń standardowych (populacyjnych) między pop
baselinedev(/host/key,1h:now/h,"d",10)  #obliczanie liczby populacyjnych odchyleń standardowych między pop
```

baselinewma(/host/key,data period:time shift,season unit,num seasons)

Oblicza linię bazową przez uśrednianie danych z tego samego przedziału czasowego w wielu równych okresach czasu („sezonach”) przy użyciu algorytmu ważonej średniej ruchomej.

Parametry:

- Zobacz wspólne parametry
- **data period** - okres zbierania danych w ramach sezonu, zdefiniowany jako <N><jednostka czasu>, gdzie:
`N` - liczba jednostek czasu
`jednostka czasu` - h (godzina), d (dzień), w (tydzień), M (miesiąc) lub y (rok), musi być równa sezonowi lub od niego mniejsza
Time shift - przesunięcie czasowe, określa przesunięcie okresu czasu, definiuje koniec przedziału zbierania danych w sezonach (zobacz przykłady)
- **season unit** - jednostka kalendarzowa definiująca jeden sezon (h, d, w, M, y); nie może być mniejsza niż data period
- **num seasons** - liczba sezonów do oceny

Przykłady:

```
baselinewma(/host/key,1h:now/h,"d",3) #obliczanie linii bazowej dla tej samej godziny dnia w ostatnich 3 p
baselinewma(/host/key,2h:now/h,"d",3) #obliczanie linii bazowej dla tego samego dwugodzinnego przedziału c
baselinewma(/host/key,1d:now/d,"M",4) #obliczanie linii bazowej dla tego samego dnia miesiąca co „wczoraj”
```

trendavg(/host/key,time period:time shift)

Średnia wartości trendów w zdefiniowanym okresie czasu.

Parametry:

- Zobacz wspólne parametry

Przykłady:

```
trendavg(/host/key,1h:now/h) #średnia dla poprzedniej godziny (np. 12:00-13:00)
trendavg(/host/key,1h:now/h-1h) #średnia sprzed dwóch godzin (11:00-12:00)
trendavg(/host/key,1h:now/h-2h) #średnia sprzed trzech godzin (10:00-11:00)
trendavg(/host/key,1M:now/M-1y) #średnia dla poprzedniego miesiąca rok temu
```

trendcount(/host/key,time period:time shift)

Liczba pomyślnie pobranych wartości historii użytych do obliczenia wartości trendu w zdefiniowanym okresie czasu.

Parametry:

- Zobacz wspólne parametry

Przykłady:

```
trendcount(/host/key,1h:now/h) #liczba wartości dla poprzedniej godziny (np. 12:00-13:00)
trendcount(/host/key,1h:now/h-1h) #liczba wartości sprzed dwóch godzin (11:00-12:00)
trendcount(/host/key,1h:now/h-2h) #liczba wartości sprzed trzech godzin (10:00-11:00)
trendcount(/host/key,1M:now/M-1y) #liczba wartości dla poprzedniego miesiąca rok temu
```

trendmax(/host/key,time period:time shift)

Maksimum w wartościach trendu w zdefiniowanym okresie czasu.

Parametry:

- Zobacz wspólne parametry

Przykłady:

```
trendmax(/host/key,1h:now/h) #maksimum dla poprzedniej godziny (np. 12:00-13:00)
trendmax(/host/key,1h:now/h) - trendmin(/host/key,1h:now/h) → oblicza różnicę między wartościami maksymaln
trendmax(/host/key,1h:now/h-1h) #maksimum sprzed dwóch godzin (11:00-12:00)
trendmax(/host/key,1h:now/h-2h) #maksimum sprzed trzech godzin (10:00-11:00)
trendmax(/host/key,1M:now/M-1y) #maksimum dla poprzedniego miesiąca rok temu
```

trendmin(/host/key,time period:time shift)

Minimum w wartościach trendu w zdefiniowanym okresie czasu.

Parametry:

- Zobacz wspólne parametry

Przykłady:

```
trendmin(/host/key,1h:now/h) #minimum dla poprzedniej godziny (np. 12:00-13:00)
trendmax(/host/key,1h:now/h) - trendmin(/host/key,1h:now/h) → oblicza różnicę między wartościami maksymaln
trendmin(/host/key,1h:now/h-1h) #minimum sprzed dwóch godzin (11:00-12:00)
trendmin(/host/key,1h:now/h-2h) #minimum sprzed trzech godzin (10:00-11:00)
trendmin(/host/key,1M:now/M-1y) #minimum dla poprzedniego miesiąca rok temu
```

trendstl(/host/key,eval period:time shift,detection period,season,<deviations>,<devalg>,<s window>)

Zwraca współczynnik anomalii w okresie wykrywania — wartość dziesiętną z zakresu od 0 do 1, obliczaną jako `((liczba wartości anomalii)/(całkowita liczba wartości))`.

Parametry:

- Zobacz wspólne parametry
- **eval period** - okres czasu, który ma zostać poddany dekompozycji (minimum „1h”), zdefiniowany jako <N><time unit>, gdzie
`N` - liczba jednostek czasu
`time unit` - h (godzina), d (dzień), w (tydzień), M (miesiąc) lub y (rok)
- **detection period** - okres czasu przed końcem eval period, dla którego obliczane są anomalie (minimum „1h”, nie może być dłuższy niż eval period), zdefiniowany jako <N><time unit>, gdzie
`N` - liczba jednostek czasu
`time unit` - h (godzina), d (dzień), w (tydzień)
- **season** - najkrótszy okres czasu, w którym oczekiwany jest powtarzający się wzorzec („sezon”) (minimum „2h”, nie może być dłuższy niż eval period, liczba wpisów w eval period musi być większa niż dwukrotność wynikowej częstotliwości (season/h)), zdefiniowany jako <N><time unit>, gdzie
`N` - liczba jednostek czasu
`time unit` - h (godzina), d (dzień), w (tydzień)
- **deviations** - liczba odchyleń (obliczana przez devalg), przy której wartość jest uznawana za anomalię (może być dziesiętna), (musi być większa lub równa 1, domyślnie 3)
- **devalg** (musi być ujęty w podwójny cudzysłów) - algorytm odchylenia; może to być *stddevpop*, *stddevsamp* lub *mad* (domyślnie)
- **s window** - rozpiętość (w opóźnieniach) okna loess dla ekstrakcji sezonowej (domyślnie 10 * liczba wpisów w eval period + 1)

Przykłady:

```
trendstl(/host/key,100h:now/h,10h,2h) #analizuje ostatnie 100 godzin danych trendu, znajduje współczynnik
trendstl(/host/key,100h:now/h-10h,100h,2h,2.1,"mad") #analizuje okres 100 godzin danych trendu do 10 godzi
trendstl(/host/key,100d:now/d-1d,10d,1d,4,,10) #analizuje 100 dni danych trendu do jednego dnia wstecz, zn
trendstl(/host/key,1M:now/M-1y,1d,2h,,"stddevsamp") #analizuje poprzedni miesiąc sprzed roku, znajduje wsp
```

trendsum(/host/key,time period:time shift)

Suma wartości trendów w zdefiniowanym okresie czasu.

Parametry:

- Zobacz wspólne parametry

Przykłady:

```
trendsum(/host/key,1h:now/h) #suma dla poprzedniej godziny (np. 12:00-13:00)
trendsum(/host/key,1h:now/h-1h) #suma sprzed dwóch godzin (11:00-12:00)
trendsum(/host/key,1h:now/h-2h) #suma sprzed trzech godzin (10:00-11:00)
trendsum(/host/key,1M:now/M-1y) #suma dla poprzedniego miesiąca sprzed roku
```

Zobacz wszystkie obsługiwane funkcje.

6 Funkcje matematyczne

Wszystkie wymienione tutaj funkcje są obsługiwane w:

- Wyrażeniach wyzwalaczy
- Pozycjach obliczanych
- Makrach wyrażeń

Funkcje matematyczne są obsługiwane dla typów wartości float i integer, o ile nie podano inaczej.

Funkcje są wymienione bez dodatkowych informacji. Kliknij funkcję, aby zobaczyć pełne szczegóły.

Function	Description
abs	Wartość bezwzględna wartości.
acos	Arcus cosinus wartości jako kąta wyrażonego w radianach.
asin	Arcus sinus wartości jako kąta wyrażonego w radianach.
atan	Arcus tangens wartości jako kąta wyrażonego w radianach.
atan2	Arcus tangens rzędnej (wartości) i współrzędnej odciętej określony jako kąt wyrażony w radianach.
avg	Średnia wartość wskazanych wartości pozycji.
cbrt	Pierwiastek sześcienny z wartości.
ceil	Zaokrągla wartość w górę do najbliższej większej lub równej liczby całkowitej.
cos	Cosinus wartości, gdzie wartość jest kątem wyrażonym w radianach.
cosh	Cosinus hiperboliczny wartości.
cot	Cotangens wartości, gdzie wartość jest kątem wyrażonym w radianach.
degrees	Konwertuje wartość z radianów na stopnie.
e	Liczba Eulera (2.718281828459045).
exp	Liczba Eulera podniesiona do potęgi wartości.
expm1	Liczba Eulera podniesiona do potęgi wartości minus 1.
floor	Zaokrągla wartość w dół do najbliższej mniejszej lub równej liczby całkowitej.
log	Logarytm naturalny.
log10	Logarytm dziesiętny.
max	Najwyższa wartość spośród wskazanych wartości pozycji.
min	Najniższa wartość spośród wskazanych wartości pozycji.
mod	Reszta z dzielenia.
pi	Stała Pi (3.14159265358979).
power	Potęga wartości.
radians	Konwertuje wartość ze stopni na radiany.
rand	Zwraca losową wartość całkowitą.
round	Zaokrągla wartość do miejsc dziesiętnych.
signum	Zwraca '-1', jeśli wartość jest ujemna, '0', jeśli wartość wynosi zero, '1', jeśli wartość jest dodatnia.
sin	Sinus wartości, gdzie wartość jest kątem wyrażonym w radianach.
sinh	Sinus hiperboliczny wartości, gdzie wartość jest kątem wyrażonym w radianach.
sqrt	Pierwiastek kwadratowy z wartości.
sum	Suma wskazanych wartości pozycji.
tan	Tangens wartości.
truncate	Obcina wartość do miejsc dziesiętnych.

Szczegóły funkcji

Kilka ogólnych uwag dotyczących parametrów funkcji:

- Parametry funkcji są oddzielone przecinkiem
- Wyrażenia są akceptowane jako parametry
- Opcjonalne parametry funkcji (lub części parametrów) są oznaczone przez < >

abs(value)

Wartość bezwzględna (od 0) wartości.

Parametr:

- **value** - wartość do sprawdzenia

Na przykład wartość bezwzględna zarówno „3”, jak i „-3” będzie wynosić „3”.

Przykład:

```
abs(last(/host/key))>10
```

acos(value)

Arcus cosinus wartości jako kąta, wyrażony w radianach.

Parametr:

- **value** - wartość do sprawdzenia

Wartość musi mieścić się w zakresie od -1 do 1. Na przykład arcus cosinus wartości „0.5” będzie wynosił „2.0943951”.

Przykład:

```
acos(last(/host/key))
```

asin(value)

Arcus sinus wartości jako kąt wyrażony w radianach.

Parametr:

- **value** - wartość do sprawdzenia

Wartość musi mieścić się w zakresie od -1 do 1. Na przykład arcus sinus wartości „0.5” będzie wynosić „-0.523598776”.

Przykład:

```
asin(last(/host/key))
```

atan(value)

Arcus tangens wartości jako kąt wyrażony w radianach.

Parametr:

- **value** - wartość do sprawdzenia

Na przykład arcus tangens wartości „1” będzie wynosił „0.785398163”.

Przykład:

```
atan(last(/host/key))
```

atan2(value,abscissa)

Arcus tangens współrzędnych rzędnej (value) i odciętej, określony jako kąt wyrażony w radianach.

Parametry:

- **value** - wartość do sprawdzenia;
- **abscissa** - wartość odciętej.

Na przykład arcus tangens współrzędnych rzędnej i odciętej dla wartości „1” będzie wynosić „2.21429744”.

Przykład:

```
atan2(last(/host/key),2)
```

avg(<value1>,<value2>,...)

Średnia wartość wartości pozycja, do których istnieje odwołanie.

Parametr:

- **valueX** — wartość zwracana przez inną funkcję, która działa na historii pozycji.

Przykład:

```
avg(avg(/host/key,1h),avg(/host2/key2,1h))
```

cbrt(value)

Pierwiastek sześcienny z wartości.

Parametr:

- **value** - wartość do sprawdzenia

Na przykład pierwiastek sześcienny z „64” wyniesie „4”, a z „63” — „3.97905721”.

Przykład:

```
cbrt(last(/host/key))
```

ceil(value)

Zaokrągla wartość w górę do najbliższej większej lub równej liczby całkowitej.

Parametr:

- **value** - wartość do sprawdzenia

Na przykład „2.4” zostanie zaokrąglone w górę do „3”. Zobacz także floor().

Przykład:

```
ceil(last(/host/key))
```

cos(value)

Cosinus wartości, gdzie wartość jest kątem wyrażonym w radianach.

Parametr:

- **value** - wartość do sprawdzenia

Na przykład cosinus wartości „1” będzie wynosił „0.54030230586”.

Przykład:

```
cos(last(/host/key))
```

cosh(value)

Cosinus hiperboliczny wartości. Zwraca wartość jako liczbę rzeczywistą, a nie w notacji naukowej.

Parametr:

- **value** - wartość do sprawdzenia

Na przykład cosinus hiperboliczny wartości „1” wyniesie „1.54308063482”.

Przykład:

```
cosh(last(/host/key))
```

cot(value)

Cotangens wartości, gdzie wartość jest kątem wyrażonym w radianach.

Parametr:

- **value** - wartość do sprawdzenia

Na przykład cotangens wartości „1” będzie wynosił „0.54030230586”.

Przykład:

```
cot(last(/host/key))
```

degrees(value)

Konwertuje wartość z radianów na stopnie.

Parametr:

- **value** - wartość do sprawdzenia

Na przykład wartość „1” po konwersji na stopnie będzie wynosić „57.2957795”.

Przykład:

```
degrees(last(/host/key))
```

e

Liczba Eulera (2.718281828459045).

Przykład:

```
e()
```

exp(value)

Liczba Eulera podniesiona do potęgi wartości.

Parametr:

- **value** - wartość do sprawdzenia

Na przykład liczba Eulera podniesiona do potęgi wartości „2” będzie równa „7.38905609893065”.

Przykład:

```
exp(last(/host/key))
```

expm1(value)

Liczba Eulera podniesiona do potęgi wartości minus 1.

Parametr:

- **value** - wartość do sprawdzenia

Na przykład liczba Eulera podniesiona do potęgi wartości „2” minus 1 będzie równa „6.38905609893065”.

Przykład:

```
expm1(last(/host/key))
```

floor(value)

Zaokrągla wartość w dół do najbliższej mniejszej lub równej liczby całkowitej.

Parametr:

- **value** - wartość do sprawdzenia

Na przykład „2.6” zostanie zaokrąglone w dół do „2”. Zobacz także ceil().

Przykład:

```
floor(last(/host/key))
```

log(value)

Logarytm naturalny.

Parametr:

- **value** - wartość do sprawdzenia

Na przykład logarytm naturalny wartości „2” wyniesie „0.69314718055994529”.

Przykład:

```
log(last(/host/key))
```

log10(value)

Logarytm dziesiętny.

Parametr:

- **value** - wartość do sprawdzenia

Na przykład logarytm dziesiętny wartości „5” wyniesie „0.69897000433”.

Przykład:

```
log10(last(/host/key))
```

max(<value1>,<value2>,...)

Najwyższa wartość spośród wartości referencyjnych pozycji.

Parametr:

- **valueX** - wartość zwracana przez inną funkcję, która działa na historii pozycji.

Przykład:

```
max(avg(/host/key,1h),avg(/host2/key2,1h))
```

min(<value1>,<value2>,...)

Najniższa wartość spośród wartości referencyjnych pozycji.

Parametr:

- **valueX** - wartość zwracana przez inną funkcję, która działa na historii pozycji.

Przykład:

```
min(avg(/host/key,1h),avg(/host2/key2,1h))
```

mod(value,denominator)

Reszta z dzielenia.

Parametry:

- **value** - wartość do sprawdzenia;
- **denominator** - mianownik dzielenia.

Na przykład reszta z dzielenia wartości ’5’ przez mianownik dzielenia ’2’ będzie wynosić ’1’.

Przykład:

```
mod(last(/host/key),2)
```

pi

Stała Pi (3.14159265358979).

Przykład:

```
pi()
```

power(value,power value)

Potęga wartości.

Parametry:

- **value** - wartość do sprawdzenia;
- **power value** - wykładnik potęgi do użycia.

Na przykład trzecia potęga wartości „2” będzie równa „8”.

Przykład:

```
power(last(/host/key),3)
```

radians(value)

Konwertuje wartość ze stopni na radiany.

Parametr:

- **value** - wartość do sprawdzenia

Na przykład wartość „1” po konwersji na radiany będzie wynosić „0.0174532925”.

Przykład:

```
radians(last(/host/key))
```

rand

Zwraca losową wartość całkowitą. Jest to liczba pseudolosowa generowana z użyciem czasu jako ziarna (wystarczająca do celów matematycznych, ale nie do kryptografii).

Przykład:

```
rand()
```

round(value,decimal places)

Zaokrągla wartość do określonej liczby miejsc dziesiętnych.

Parametry:

- **value** - wartość do sprawdzenia;
- **decimal places** - określa liczbę miejsc dziesiętnych do zaokrąglenia (możliwe jest również 0).

Na przykład wartość „2.5482” zaokrąglona do 2 miejsc dziesiętnych będzie wynosić „2.55”.

Przykład:

```
round(last(/host/key),2)
```

signum(value)

Zwraca ’-1’, jeśli wartość jest ujemna, ’0’, jeśli wartość jest równa zero, oraz ’1’, jeśli wartość jest dodatnia.

Parametr:

- **value** - wartość do sprawdzenia.

Przykład:

```
signum(last(/host/key))
```

sin(value)

Sinus wartości, gdzie wartość jest kątem wyrażonym w radianach.

Parametr:

- **value** - wartość do sprawdzenia

Na przykład sinus wartości „1” wyniesie „0.8414709848”.

Przykład:

```
sin(last(/host/key))
```

sinh(value)

Sinus hiperboliczny wartości.

Parametr:

- **value** - wartość do sprawdzenia

Na przykład sinus hiperboliczny wartości „1” wyniesie „1.17520119364”.

Przykład:

```
sinh(last(/host/key))
```

sqrt(value)

Pierwiastek kwadratowy z wartości.
 Ta funkcja zakończy się niepowodzeniem dla wartości ujemnej.

Parametr:

- **value** - wartość do sprawdzenia

Na przykład pierwiastek kwadratowy z wartości „3.5” będzie wynosił „1.87082869339”.

Przykład:

```
sqrt(last(/host/key))
```

sum(<value1>,<value2>,...)

Suma wartości referencyjnych pozycji.

Parametr:

- **valueX** - wartość zwracana przez inną funkcję, która pracuje z historią pozycji.

Przykład:

```
sum(avg(/host/key,1h),avg(/host2/key2,1h))
```

tan(value)

Tangens wartości.

Parametr:

- **value** - wartość do sprawdzenia

Na przykład tangens wartości „1” wyniesie „1.55740772465”.

Przykład:

```
tan(last(/host/key))
```

truncate(value,decimal places)

Obetnij wartość do określonej liczby miejsc dziesiętnych.

Parametry:

- **value** - wartość do sprawdzenia;
- **decimal places** - określ liczbę miejsc dziesiętnych do obcięcia (możliwe jest również 0).

Na przykład wartość „2.5482” obcięta do 2 miejsc dziesiętnych będzie wynosić „2.54”.

Przykład:

```
truncate(last(/host/key),2)
```

Zobacz wszystkie obsługiwane funkcje.

7 Funkcje operatorów

Wszystkie wymienione tutaj funkcje są obsługiwane w:

- Wyrażeniach wyzwalaczy
- Pozycjach obliczanych
- Makrach wyrażeń

Funkcje są wymienione bez dodatkowych informacji. Kliknij funkcję, aby zobaczyć pełne szczegóły.

Function	Description
between	Sprawdza, czy wartość należy do podanego zakresu.
in	Sprawdza, czy wartość jest równa co najmniej jednej z wymienionych wartości.

Szczegóły funkcji

Kilka ogólnych uwag dotyczących parametrów funkcji:

- Parametry funkcji są oddzielone przecinkiem
- Wyrażenia są akceptowane jako parametry

between(value,min,max)

Sprawdza, czy wartość należy do podanego zakresu.
 Obsługiwane typy wartości: *Integer*, *Float*.
 Zwraca: 1 - w zakresie; 0 - w przeciwnym razie.

Parametry:

- **value** - wartość do sprawdzenia;
- **min** - wartość minimalna;
- **max** - wartość maksymalna.

Przykład:

```
between(last(/host/key),1,10)=1 #wyzwalacz, jeśli wartość jest między 1 a 10
```

in(value,value1,value2,...valueN)

Sprawdza, czy wartość jest równa co najmniej jednej z podanych wartości.
 Obsługiwane typy wartości: *Integer*, *Float*, *Character*, *Text*, *Log*.
 Zwraca: 1 - jeśli równa; 0 - w przeciwnym razie.

Parametry:

- **value** - wartość do sprawdzenia;
- **valueX** - podane wartości (wartości tekstowe muszą być ujęte w podwójny cudzysłów).

Wartość jest porównywana z podanymi wartościami jako liczby, jeśli wszystkie te wartości mogą zostać przekonwertowane na wartości liczbowe; w przeciwnym razie jest porównywana jako ciągi znaków.

Przykład:

```
in(last(/host/key),5,10)=1 #wyzwalacz, jeśli ostatnia wartość jest równa 5 lub 10
in("text",last(/host/key),last(/host/key,#2))=1 #wyzwalacz, jeśli "text" jest równe jednej z 2 ostatnich w
```

Zobacz wszystkie obsługiwane funkcje.

8 Funkcje predykcyjne

Wszystkie wymienione tutaj funkcje są obsługiwane w:

- Wyrażeniach wyzwalaczy
- Pozycjach obliczanych
- Makrach wyrażeń

Funkcje są wymienione bez dodatkowych informacji. Kliknij funkcję, aby zobaczyć pełne szczegóły.

Function	Description
forecast	Przyszła wartość, maksimum, minimum, delta lub średnia pozycji.
timeleft	Czas w sekundach potrzebny, aby pozycja osiągnęła określony próg.

Wspólne parametry

- `/host/key` jest wspólnym obowiązkowym pierwszym parametrem dla funkcji odwołujących się do historii pozycji hosta
- `(sec|#num)<:time shift>` jest wspólnym drugim parametrem dla funkcji odwołujących się do historii pozycji hosta, gdzie:
  - **sec** — maksymalny okres obliczania w sekundach (mogą być używane sufiksy czasu), lub
  - **#num** — maksymalny zakres obliczania w ostatnio zebranych wartościach (jeśli jest poprzedzony znakiem kratki)
  - **time shift** (opcjonalnie) pozwala przesunąć punkt obliczania wstecz w czasie. Zobacz więcej szczegółów dotyczących określania przesunięcia czasu.

Szczegóły funkcji

Kilka ogólnych uwag dotyczących parametrów funkcji:

- Parametry funkcji są oddzielane przecinkiem
- Opcjonalne parametry funkcji (lub części parametrów) są oznaczone przez < >
- Parametry specyficzne dla danej funkcji są opisane przy każdej funkcji
- Parametry `/host/key` oraz `(sec|#num)<:time shift>` nigdy nie mogą być ujmowane w cudzysłów

forecast(/host/key,(sec|#num)<:time shift>,time,<fit>,<mode>)

Przyszła wartość, maksimum, minimum, delta lub średnia pozycji.
 Obsługiwane typy wartości: *Float*, *Integer*.

Parametry:

- Zobacz wspólne parametry;
- **time** — horyzont prognozy w sekundach (mogą być używane sufiksy czasu); obsługiwane są wartości ujemne;
- **fit** (opcjonalny; musi być ujęty w podwójny cudzysłów) — funkcja używana do dopasowania danych historycznych. Obsługiwane dopasowania:
linear — funkcja liniowa (domyślnie)
polynomialN — wielomian stopnia N (1 <= N <= 6)
exponential — funkcja wykładnicza
logarithmic — funkcja logarytmiczna
power — funkcja potęgowa
Zwróć uwagę, że *polynomial1* jest równoważne *linear*;
- **mode** (opcjonalny; musi być ujęty w podwójny cudzysłów) — wymagane dane wyjściowe. Obsługiwane tryby:
value — wartość (domyślnie)
max — maksimum
min — minimum
delta — *max-min*
avg — średnia
Zwróć uwagę, że *value* szacuje wartość pozycji w momencie `now + time`; *max*, *min*, *delta* i *avg* analizują oszacowanie wartości pozycji w przedziale między `now` a `now + time`.

Komentarze:

- Jeśli zwracana wartość jest większa niż 1.7976931348623158E+308 lub mniejsza niż -1.7976931348623158E+308, zwracana wartość jest odpowiednio ograniczana do 1.7976931348623158E+308 lub -1.7976931348623158E+308;
- Staje się nieobsługiwana tylko w przypadku nieprawidłowego użycia w wyrażeniu (niewłaściwy typ pozycji, nieprawidłowe parametry), w przeciwnym razie w przypadku błędów zwraca -1;
- Zobacz także dodatkowe informacje o funkcjach predykcyjnych wyzwalaczy.

Przykłady:

```
forecast(/host/key,#10,1h) #prognoza wartości pozycji za godzinę na podstawie ostatnich 10 wartości
forecast(/host/key,1h,30m) #prognoza wartości pozycji za 30 minut na podstawie danych z ostatniej godziny
forecast(/host/key,1h:now-1d,12h) #prognoza wartości pozycji za 12 godzin na podstawie danych z jednej god
forecast(/host/key,1h,10m,"exponential") #prognoza wartości pozycji za 10 minut na podstawie danych z osta
forecast(/host/key,1h,2h,"polynomial3","max") #prognoza maksymalnej wartości, jaką pozycja może osiągnąć w
forecast(/host/key,#2,-20m) #oszacowanie wartości pozycji sprzed 20 minut na podstawie dwóch ostatnich war
```

timeleft(/host/key,(sec|#num)<:przesunięcie czasu>,threshold,<fit>)

Czas w sekundach potrzebny, aby pozycja osiągnęła określony próg.
 Obsługiwane typy wartości: *Float*, *Integer*.

Parametry:

- Zobacz wspólne parametry;
- **threshold** - wartość do osiągnięcia (można używać sufiksów jednostek);
- **fit** (opcjonalny; musi być ujęty w podwójny cudzysłów) - zobacz forecast().

Uwagi:

- Jeśli zwracana wartość jest większa niż 1.7976931348623158E+308, zostanie przycięta do 1.7976931348623158E+308;
- Zwraca 1.7976931348623158E+308, jeśli próg nie może zostać osiągnięty;
- Staje się nieobsługiwana tylko w przypadku nieprawidłowego użycia w wyrażeniu (niewłaściwy typ pozycji, nieprawidłowe parametry), w przeciwnym razie zwraca -1 w przypadku błędów;
- Zobacz także dodatkowe informacje o funkcjach predykcyjnych wyzwalaczy.

Przykłady:

```
timeleft(/host/key,#10,0) #czas do momentu, aż wartość pozycji osiągnie zero na podstawie ostatnich 10 war
timeleft(/host/key,1h,100) #czas do momentu, aż wartość pozycji osiągnie 100 na podstawie danych z ostatni
timeleft(/host/key,1h:now-1d,100) #czas do momentu, aż wartość pozycji osiągnie 100 na podstawie jednej go
timeleft(/host/key,1h,200,"polynomial2") #czas do momentu, aż wartość pozycji osiągnie 200 na podstawie da
```

Zobacz wszystkie obsługiwane funkcje.

Predykcyjne funkcje wyzwalaczy

Przegląd

Czasami pojawiają się oznaki nadchodzącego problemu. Oznaki te można wykryć, aby z wyprzedzeniem podjąć działania zapobiegające problemowi lub przynajmniej zminimalizować jego wpływ.

Zabbix udostępnia narzędzia do przewidywania przyszłego zachowania monitorowanego systemu na podstawie danych historycznych. Narzędzia te są realizowane za pomocą predykcyjnych funkcji wyzwalacza.

Funkcje

Przed ustawieniem wyzwalacza należy określić, czym jest stan problemowy i ile czasu potrzeba na podjęcie działania. Następnie są dwa sposoby skonfigurowania wyzwalacza sygnalizującego potencjalną niepożądaną sytuację. Po pierwsze: wyzwalacz musi zostać uruchomiony, gdy oczekuje się, że system będzie w stanie problemowym po upływie „czasu na działanie". Po drugie: wyzwalacz musi zostać uruchomiony, gdy system osiągnie stan problemowy w czasie krótszym niż „czas na działanie". Odpowiadające funkcje wyzwalacza, których należy użyć, to **forecast** oraz **timeleft**. Należy pamiętać, że podstawowa analiza statystyczna jest zasadniczo identyczna dla obu funkcji. Możesz skonfigurować wyzwalacz w dowolny preferowany sposób, uzyskując podobne wyniki.

Parametry

Obie funkcje używają niemal tego samego zestawu parametrów. Aby uzyskać informacje, skorzystaj z listy obsługiwanych funkcji.

Przedział czasu

Przede wszystkim należy określić historyczny okres, który Zabbix ma analizować, aby przygotować prognozę. Robi się to w znany sposób za pomocą parametru `time period` oraz opcjonalnego przesunięcia czasu, tak jak w przypadku funkcji **avg**, **count**, **delta**, **max**, **min** i **sum**.

Horyzont prognozowania

(tylko **forecast**)
Parametr `time` określa, jak daleko w przyszłość Zabbix powinien ekstrapolować zależności wykryte w danych historycznych. Niezależnie od tego, czy używasz `time_shift`, czy nie, `time` jest zawsze liczone od bieżącego momentu.

Próg do osiągnięcia

(tylko **timeleft**)
Parametr `threshold` określa wartość, którą analizowana pozycja ma osiągnąć, bez względu na to, czy od góry, czy od dołu. Gdy wyznaczymy f(t) (zob. poniżej), należy rozwiązać równanie f(t) = `threshold` i zwrócić pierwiastek, który jest bliżej chwili obecnej i znajduje się na prawo od niej, lub 1.7976931348623158E+308, jeśli taki pierwiastek nie istnieje.

Note:
Gdy wartości pozycji zbliżają się do progu, a następnie go przekraczają, **timeleft** zakłada, że punkt przecięcia jest już w przeszłości, i dlatego przełącza się na następne przecięcie z poziomem `threshold`, jeśli takie istnieje. Zalecaną praktyką jest używanie predykcji jako uzupełnienia zwykłej diagnostyki problemów, a nie jej substytutu.[1]

Funkcje dopasowania

Domyślną funkcją `fit` jest funkcja *liniowa*. Jeśli jednak monitorowany system jest bardziej złożony, masz do wyboru więcej opcji.

`fit`	x = f(t)
linear	$x = a + b*t$
polynomialN[2]	$x = a_0 + a_1*t + a_2*t^2 + ... + a_n*t^n$
exponential	$x = a*exp(b*t)$
logarithmic	$x = a + b*log(t)$
power	$x = a*t^b$

Tryby

(tylko **forecast**) Za każdym razem, gdy funkcja wyzwalacza jest obliczana, pobiera dane z określonego okresu historii i dopasowuje do nich wskazaną funkcję. Tak więc, jeśli dane nieznacznie się różnią, dopasowana funkcja również będzie się nieznacznie różnić. Jeśli po prostu obliczymy wartość dopasowanej funkcji dla określonego momentu w przyszłości, nie będzie wiadomo nic o tym, jak analizowana pozycja ma się zachowywać między teraz a tym przyszłym momentem. Dla niektórych opcji `fit` (takich jak *wielomian*) prosta wartość z przyszłości może być myląca.

`mode`	wynik **forecast**
value	f(now + `time`)
max	$max_{now <= t <= now + time}$ f(t)
min	$min_{now <= t <= now + time}$ f(t)
delta	*max* - *min*
avg	średnia z f(t) (now <= t <= now + `time`) zgodnie z definicją

Szczegóły

Aby uniknąć obliczeń na bardzo dużych liczbach, traktujemy znacznik czasu pierwszej wartości w określonym okresie plus 1 ns jako nowy czas zerowy (aktualny czas epoki jest rzędu 10^9, kwadrat epoki to 10^{18}, precyzja podwójna wynosi około 10^{-16}). 1 ns dodaje się, aby zapewnić wyłącznie dodatnie wartości czasu dla dopasowań *logarytmicznych* i *potęgowych*, które obejmują obliczanie log(t). Przesunięcie czasu nie wpływa na funkcje *liniowe*, *wielomianowe*, *wykładnicze* (poza łatwiejszymi i dokładniejszymi obliczeniami), ale zmienia kształt funkcji *logarytmicznych* i *potęgowych*.

Potencjalne błędy

Funkcje zwracają -1 w następujących sytuacjach:

- określony okres oceny nie zawiera danych;
- wynik operacji matematycznej nie jest zdefiniowany[3];
- komplikacje numeryczne (niestety, dla niektórych zestawów danych wejściowych zakres i precyzja formatu liczb zmiennoprzecinkowych podwójnej precyzji okazują się niewystarczające)[4].

Note:
Nie są zgłaszane żadne ostrzeżenia ani błędy, jeśli wybrane dopasowanie słabo opisuje dostarczone dane lub jeśli danych jest po prostu zbyt mało do dokładnego przewidywania.

Przykłady i obsługa błędów

Aby otrzymać ostrzeżenie, gdy na host zaczyna brakować wolnego miejsca na dysku, możesz użyć wyrażenia wyzwalacza takiego jak to:

```
timeleft(/host/vfs.fs.size[/,free],1h,0)<1h
```

Jednak kod błędu -1 może wejść w grę i wprowadzić wyzwalacz w stan problemu. Ogólnie jest to dobre, ponieważ otrzymujesz ostrzeżenie, że Twoje prognozy nie działają poprawnie i powinieneś przyjrzeć się im dokładniej, aby ustalić przyczynę. Czasami jednak jest to niepożądane, ponieważ -1 może po prostu oznaczać, że w ciągu ostatniej godziny nie uzyskano danych o wolnym miejscu na dysku hosta. Jeśli otrzymujesz zbyt wiele fałszywie dodatnich alertów, rozważ użycie bardziej złożonego wyrażenia wyzwalacza [5]:

```
timeleft(/host/vfs.fs.size[/,free],1h,0)<1h and timeleft(/host/vfs.fs.size[/,free],1h,0)<>-1
```

Sytuacja jest nieco trudniejsza w przypadku **forecast**. Przede wszystkim -1 może, ale nie musi, wprowadzić wyzwalacz w stan problemu w zależności od tego, czy masz wyrażenie takie jak `forecast(/host/item,(...))<...`, czy takie jak `forecast(/host/item,(...))>...`

Ponadto -1 może być prawidłową prognozą, jeśli ujemna wartość pozycji jest czymś normalnym. Jednak prawdopodobieństwo takiej sytuacji w rzeczywistych warunkach jest znikome (zobacz, jak działa operator =). Dlatego dodaj `... or forecast(/host/item,(...))=-` lub `... and forecast(/host/item,(...))<>-1`, jeśli odpowiednio chcesz lub nie chcesz traktować -1 jako problemu.

Przypisy

[1] Na przykład prosty wyzwalacz taki jak `timeleft(/host/item,1h,X) < 1h` może przejść w stan problemu, gdy wartość pozycji zbliża się do X, a następnie nagle powrócić do stanu OK po osiągnięciu wartości X. Jeśli problem polega na tym, że wartość pozycji jest poniżej X, użyj: `last(/host/item) < X or timeleft(/host/item,1h,X) < 1h` Jeśli problem polega na tym, że wartość pozycji jest powyżej X, użyj: `last(/host/item) > X or timeleft(/host/item,1h,X) < 1h`

[2] Stopień wielomianu może wynosić od 1 do 6, *polynomial1* jest równoważny *linear*. Jednak wielomianów wyższego stopnia należy używać ostrożnie. Jeśli okres oceny zawiera mniej punktów niż potrzeba do wyznaczenia współczynników wielomianu, stopień wielomianu zostanie obniżony (np. żądany jest *polynomial5*, ale są tylko 4 punkty, dlatego zostanie dopasowany *polynomial3*).

[3] Na przykład dopasowanie funkcji *exponential* lub *power* obejmuje obliczanie log() wartości pozycji. Jeśli dane zawierają zera lub liczby ujemne, otrzymasz błąd, ponieważ log() jest zdefiniowany tylko dla wartości dodatnich.

[4] Dla dopasowań *linear*, *exponential*, *logarithmic* i *power* wszystkie niezbędne obliczenia można zapisać jawnie. Dla *polynomial* bez dodatkowych kroków można obliczyć tylko *value*. Obliczenie *avg* obejmuje wyznaczenie funkcji pierwotnej wielomianu (analitycznie). Obliczenie *max*, *min* i *delta* obejmuje wyznaczenie pochodnej wielomianu (analitycznie) i znalezienie jej pierwiastków (numerycznie). Rozwiązanie f(t) = 0 obejmuje znalezienie pierwiastków wielomianu (numerycznie).

[5] Jednak w tym przypadku -1 może spowodować, że wyzwalacz wyjdzie ze stanu problemu. Aby zapewnić pełną ochronę, użyj: `timeleft(/host/vfs.fs.size[/,free],1h,0)<1h and ({TRIGGER.VALUE}=0 and timeleft(/host/vfs.fs.size[/,free], or {TRIGGER.VALUE}=1)`

9 Funkcje tekstowe

Wszystkie wymienione tutaj funkcje są obsługiwane w:

- Wyrażeniach wyzwalaczy
- Pozycjach obliczanych
- Makrach wyrażeń

Funkcje są wymienione bez dodatkowych informacji. Kliknij funkcję, aby zobaczyć pełne szczegóły.

Function	Description
ascii	Kod ASCII skrajnie lewego znaku wartości.
bitlength	Długość wartości w bitach.
bytelength	Długość wartości w bajtach.
char	Zwraca znak poprzez interpretację wartości jako kodu ASCII.
concat	Ciąg znaków powstały przez połączenie wartości wskazanych pozycji lub wartości stałych.
insert	Wstawia określone znaki lub spacje do ciągu znaków, zaczynając od określonej pozycji w ciągu.
jsonpath	Zwraca wynik JSONPath.

Function	Description
left	Zwraca skrajnie lewe znaki wartości.
length	Długość wartości w znakach.
ltrim	Usuwa określone znaki z początku ciągu.
mid	Zwraca podciąg N znaków, zaczynając od pozycji znaku określonej przez „start”.
repeat	Powtarza ciąg znaków.
replace	Znajduje wzorzec w wartości i zastępuje go ciągiem replacement.
right	Zwraca skrajnie prawe znaki wartości.
rtrim	Usuwa określone znaki z końca ciągu.
trim	Usuwa określone znaki z początku i końca ciągu.
xmlxpath	Zwraca wynik XML XPath.

Szczegóły funkcji

Kilka ogólnych uwag dotyczących parametrów funkcji:

- Parametry funkcji są oddzielane przecinkiem
- Wyrażenia są akceptowane jako parametry
- Parametry tekstowe muszą być ujęte w podwójny cudzysłów; w przeciwnym razie mogą zostać błędnie zinterpretowane
- Opcjonalne parametry funkcji (lub części parametrów) są oznaczane przez < >

ascii(value)

Kod ASCII skrajnie lewego znaku wartości.
 Obsługiwane typy wartości: *String*, *Text*, *Log*.

Parametr:

- **value** - wartość do sprawdzenia

Na przykład wartość taka jak ’Abc’ zwróci ’65’ (kod ASCII dla ’A’).

Przykład:

```
ascii(last(/host/key))
```

bitlength(value)

Długość wartości w bitach.
 Obsługiwane typy wartości: *String*, *Text*, *Log*, *Integer*.

Parametr:

- **value** - wartość do sprawdzenia

Przykład:

```
bitlength(last(/host/key))
```

bytelength(value)

Długość wartości w bajtach.
 Obsługiwane typy wartości: *String*, *Text*, *Log*, *Integer*.

Parametr:

- **value** - wartość do sprawdzenia

Przykład:

```
bytelength(last(/host/key))
```

char(value)

Zwraca znak poprzez interpretację wartości jako kodu ASCII.
 Obsługiwane typy wartości: *Integer*.

Parametr:

- **value** — wartość do sprawdzenia

Wartość musi mieścić się w zakresie 0–255. Na przykład wartość taka jak „65” (interpretowana jako kod ASCII) zwróci „A”.

Przykład:

```
char(last(/host/key))
```

concat(<value1>,<value2>,...)

Ciąg znaków wynikający z połączenia wartości referencyjnych pozycji lub wartości stałych.
 Obsługiwane typy wartości: *String*, *Text*, *Log*, *Float*, *Integer*.

Parametr:

- **valueX** - wartość zwracana przez jedną z funkcji historii lub wartość stała (ciąg znaków, liczba całkowita lub zmienno-przecinkowa). Musi zawierać co najmniej dwa parametry.

Na przykład wartość taka jak 'Zab' połączona z 'bix' (stały ciąg znaków) zwróci 'Zabbix'.

Przykłady:

```
concat(last(/host/key),"bix")
concat("1 min: ",last(/host/system.cpu.load[all,avg1]),", 15 min: ",last(/host/system.cpu.load[all,avg15])
```

insert(value,start,length,replacement)

Wstawia określone znaki lub spacje do ciągu znaków, zaczynając od wskazanej pozycji w ciągu.
 Obsługiwane typy wartości: *String*, *Text*, *Log*.

Parametry:

- **value** - wartość do sprawdzenia;
- **start** - pozycja początkowa;
- **length** - pozycje do zastąpienia;
- **replacement** - ciąg zastępujący.

Na przykład wartość taka jak 'Zabbbix' zostanie zastąpiona przez 'Zabbix', jeśli 'bb' (pozycja początkowa 3, liczba pozycji do zastąpienia 2) zostanie zastąpione przez 'b'.

Przykład:

```
insert(last(/host/key),3,2,"b")
```

jsonpath(value,path,<default>)

Zwraca wynik JSONPath.
 Obsługiwane typy wartości: *String*, *Text*, *Log*.

Parametry:

- **value** - wartość do sprawdzenia;
- **path** - ścieżka (musi być ujęta w cudzysłów);
- **default** - opcjonalna wartość zapasowa, jeśli zapytanie JSONPath nie zwróci danych. Należy pamiętać, że w przypadku innych błędów zwracane jest niepowodzenie (np. „unsupported construct").

Przykład:

```
jsonpath(last(/host/proc.get[zabbix_agentd,,,summary]),"$..size")
```

left(value,count)

Zwraca skrajnie lewe znaki wartości.
 Obsługiwane typy wartości: *String*, *Text*, *Log*.

Parametry:

- **value** - wartość do sprawdzenia;
- **count** - liczba znaków do zwrócenia.

Na przykład można zwrócić „Zab" z „Zabbix", określając 3 skrajnie lewe znaki do zwrócenia. Zobacz także right().

Przykład:

```
left(last(/host/key),3) #zwraca trzy skrajnie lewe znaki
```

length(value)

Długość wartości w znakach.
 Obsługiwane typy wartości: *String*, *Text*, *Log*.

Parametr:

- **value** - wartość do sprawdzenia.

Przykłady:

```
length(last(/host/key)) #długość najnowszej wartości
length(last(/host/key,#3)) #długość trzeciej najnowszej wartości
length(last(/host/key,#1:now-1d)) #długość najnowszej wartości sprzed jednego dnia
```

ltrim(value,<chars>)

Usuń określone znaki z początku ciągu.
 Obsługiwane typy wartości: *String*, *Text*, *Log*.

Parametry:

- **value** - wartość do sprawdzenia;
- **chars** (opcjonalnie) - określa znaki do usunięcia.

Domyślnie usuwane są białe znaki z początku ciągu (jeśli nie określono opcjonalnych znaków). Zobacz także: rtrim(), trim().

Przykłady:

```
ltrim(last(/host/key)) #usuń białe znaki z początku ciągu
ltrim(last(/host/key),"Z") #usuń dowolne 'Z' z początku ciągu
ltrim(last(/host/key)," Z") #usuń dowolną spację i 'Z' z początku ciągu
```

mid(value,start,length)

Zwraca podciąg N znaków, zaczynając od pozycji znaku określonej przez parametr „start”.
 Obsługiwane typy wartości: *String*, *Text*, *Log*.

Parametry:

- **value** - wartość do sprawdzenia;
- **start** - pozycja początkowa podciągu;
- **length** - liczba pozycji do zwrócenia w podciągu.

Na przykład możliwe jest zwrócenie „abbi” z wartości takiej jak „Zabbix”, jeśli pozycja początkowa wynosi 2, a liczba pozycji do zwrócenia wynosi 4.

Przykład:

```
mid(last(/host/key),2,4)="abbi"
```

repeat(value,count)

Powtórz ciąg znaków.
 Obsługiwane typy wartości: *String*, *Text*, *Log*.

Parametry:

- **value** - wartość do sprawdzenia;
- **count** - liczba powtórzeń.

Przykład:

```
repeat(last(/host/key),2) #powtórz wartość dwa razy
```

replace(value,pattern,replacement)

Znajduje wzorzec w wartości i zastępuje go ciągiem replacement. Wszystkie wystąpienia wzorca zostaną zastąpione.
 Obsługiwane typy wartości: *String*, *Text*, *Log*.

Parametry:

- **value** - wartość do sprawdzenia;
- **pattern** - wzorzec do znalezienia;
- **replacement** - ciąg, którym zostanie zastąpiony wzorzec.

Przykład:

```
replace(last(/host/key),"ibb","abb") #zastępuje wszystkie 'ibb' przez 'abb'
```

right(value,count)

Zwraca skrajnie prawe znaki wartości.
 Obsługiwane typy wartości: *String*, *Text*, *Log*.

Parametry:

- **value** - wartość do sprawdzenia;
- **count** - liczba znaków do zwrócenia.

Na przykład można zwrócić „bix” z „Zabbix”, podając 3 skrajnie prawe znaki do zwrócenia. Zobacz także left().

Przykład:

```
right(last(/host/key),3) #zwraca trzy skrajnie prawe znaki
```

rtrim(value,<chars>)

Usuwa określone znaki z końca ciągu znaków.
 Obsługiwane typy wartości: *String*, *Text*, *Log*.

Parametry:

- **value** - wartość do sprawdzenia;
- **chars** (opcjonalnie) - określa znaki do usunięcia.

Domyślnie usuwane są białe znaki z prawej strony (jeśli nie określono opcjonalnych znaków). Zobacz także: ltrim(), trim().

Przykłady:

```
rtrim(last(/host/key)) #usuń białe znaki z końca ciągu znaków
rtrim(last(/host/key),"x") #usuń wszystkie znaki 'x' z końca ciągu znaków
rtrim(last(/host/key),"x ") #usuń wszystkie znaki 'x' i spacje z końca ciągu znaków
```

trim(value,<chars>)

Usuń określone znaki z początku i końca ciągu znaków.
 Obsługiwane typy wartości: *String*, *Text*, *Log*.

Parametry:

- **value** - wartość do sprawdzenia;
- **chars** (opcjonalnie) - określa znaki do usunięcia.

Domyślnie z obu stron usuwane są białe znaki (jeśli nie określono opcjonalnych znaków). Zobacz także: ltrim(), rtrim().

Przykłady:

```
trim(last(/host/key)) #usuń białe znaki z początku i końca ciągu znaków
trim(last(/host/key),"_") #usuń '_' z początku i końca ciągu znaków
```

xmlxpath(value,path,<default>)

Zwraca wynik XML XPath.
 Obsługiwane typy wartości: *String*, *Text*, *Log*.

Parametry:

- **value** - wartość do sprawdzenia;
- **path** - ścieżka (musi być ujęta w cudzysłów);
- **default** - opcjonalna wartość zastępcza, jeśli zapytanie XML XPath zwróci pusty zbiór węzłów. Nie zostanie zwrócona, jeśli pusty wynik nie jest zbiorem węzłów (tj. pustym ciągiem). W przypadku innych błędów zwracane jest niepowodzenie (np. „invalid expression”).

Przykład:

```
xmlxpath(last(/host/xml_result),"/response/error/status")
```

Zobacz wszystkie obsługiwane funkcje.

4 Najlepsze praktyki dotyczące wyzwalaczy

Wyzwalacze są potężnym narzędziem, ale mogą też powodować niepożądany szum alertów. Aby widzieć więcej rzeczywistych sygnałów, a mniej szumu, postępuj zgodnie z tymi wskazówkami:

1. Zmniejsz czułość wyzwalaczy. Zamiast alertować na podstawie najnowszej wartości (zbyt wysokiej/zbyt niskiej), analizuj średnią z dłuższego okresu, używając funkcji takich jak **avg**, **min** i **max**.
2. Rozważ użycie funkcji **percentile** (ustawionej na 95% lub 5%) w wyzwalaczach, jeśli chcesz uniknąć alertów przy losowych skokach i spadkach.
3. Użyj histerezy, aby uniknąć flappingu wyzwalaczy — częstych zmian stanu wyzwalacza (OK ↔ Problem). Ciągłość stanu problemu można zdefiniować przez dodanie wyrażenia odzyskiwania (oddzielnego warunku rozwiązania problemu).
4. Użyj zależności wyzwalaczy, aby uniknąć alertów, które nie są związane z przyczyną źródłową.
5. Użyj ważności wyzwalacza, aby alertować tylko o poważniejszych problemach.
6. Zdefiniuj okna konserwacji.

Histereza

Czasami potrzebny jest przedział między stanem problemu a stanem odzyskania, zamiast prostego progu. Na przykład, jeśli chcemy zdefiniować wyzwalacz, który zgłasza problem, gdy temperatura w serwerowni przekroczy 20°C, i chcemy, aby pozostawał

on w stanie problemu, dopóki temperatura nie spadnie poniżej 15°C, prosty próg wyzwalacza ustawiony na 20°C nie będzie wystarczający.

Zamiast tego najpierw musimy zdefiniować wyrażenie wyzwalacza dla zdarzenia problemowego (temperatura powyżej 20°C). Następnie musimy zdefiniować dodatkowy warunek odzyskania (temperatura poniżej 15°C). Robi się to przez zdefiniowanie *wyrażenia odzyskania* podczas konfigurowania wyzwalacza.

W tym przypadku odzyskanie po problemie odbywa się w dwóch krokach:

- Najpierw wyrażenie problemowe (temperatura powyżej 20°C) musi zostać obliczone jako FALSE
- Następnie wyrażenie odzyskania (temperatura poniżej 15°C) musi zostać obliczone jako TRUE

Wyrażenie odzyskania jest obliczane dopiero po rozwiązaniu zdarzenia problemowego. Samo ustawienie wyrażenia odzyskania na TRUE nie powoduje rozwiązania problemu, jeśli wyrażenie problemowe nadal ma wartość TRUE!

Przykład

Temperatura w serwerowni jest zbyt wysoka.

Wyrażenie problemu:

```
last(/server/temp)>20
```

Wyrażenie odzyskiwania:

```
last(/server/temp)<=15
```

> **Note:**
> Używanie makra {TRIGGER.VALUE} w wyrażeniu odzyskiwania jest nieefektywne, ponieważ to wyrażenie jest oceniane tylko wtedy, gdy wyzwalacz znajduje się w stanie „Problem”. W konsekwencji podczas obliczania wyrażenia makro {TRIGGER.VALUE} zawsze zostanie rozwinięte do wartości „1” (co oznacza stan „Problem”).

Ważność wyzwalacza

Ważność wyzwalacza może być używana do ograniczenia szumu alertów w przypadku mniej istotnych problemów.

Zobacz wszystkie najlepsze praktyki.

Przegląd

Ważność określa względne znaczenie wyzwalacza.



Przypisanie ważności jest przydatne nie tylko do reprezentacji wizualnej, ale także do unikania powiadomień o błahych problemach.

Ważności wyzwalaczy są używane do:

- Reprezentacji wizualnej (odrębny kolor dla każdego utworzonego problemu, na podstawie oryginalnej ważności wyzwalacza)
- Ograniczania powiadomień na podstawie ważności (zobacz warunki akcji)
- Mediów użytkownika — różne media (kanały powiadomień) dla różnych ważności (na przykład SMS dla wyzwalaczy o ważności *Wysoka* i *Katastrofa* oraz e-mail dla wyzwalaczy o innych ważnościach)
- Dźwięku w alarmach globalnych — różne dźwięki dla różnych ważności

Domyślnie obsługiwane są następujące ważności wyzwalaczy:

Ważność	Kolor	Opis
Niesklasyfikowane	Szary	Może być używana tam, gdzie poziom ważności zdarzenia jest nieznany, nie został określony, nie należy do regularnego zakresu monitorowania itp., na przykład podczas początkowej konfiguracji, jako symbol zastępczy do przyszłej oceny lub jako część procesu integracji.
Informacja	Jasnoniebieski	Może być używana dla zdarzeń informacyjnych, które nie wymagają natychmiastowej uwagi, ale nadal mogą dostarczać cennych informacji.
Ostrzeżenie	Żółty	Może być używana do wskazania potencjalnego problemu, który może wymagać zbadania lub działania, ale nie jest krytyczny.
Średnia	Pomarańczowy	Może być używana do wskazania istotnego problemu, którym należy zająć się stosunkowo szybko, aby zapobiec dalszym problemom.
Wysoka	Jasnoczerwony	Może być używana do wskazania krytycznych problemów, które wymagają natychmiastowej uwagi, aby uniknąć znaczących zakłóceń.

Ważność	Kolor	Opis
Katastrofa	Czerwony	Może być używana do wskazania poważnego incydentu, który wymaga natychmiastowego działania, aby zapobiec na przykład awariom systemu lub utracie danych.

Nazwy i kolory ważności wyzwalaczy można **dostosować** w *Administracja* > *Ogólne* > *Opcje wyświetlania wyzwalaczy*.
Kolory są współdzielone przez wszystkie motywy frontend.

Tłumaczenie niestandardowych nazw poziomów ważności

> **Attention:**
> Jeśli używane są tłumaczenia frontend Zabbix, niestandardowe nazwy poziomów ważności domyślnie zastąpią nazwy przetłumaczone.

Domyślne nazwy poziomów ważności wyzwalaczy są dostępne do tłumaczenia we wszystkich ustawieniach regionalnych.
Jeśli nazwa poziomu ważności zostanie zmieniona, nazwa niestandardowa będzie używana we wszystkich ustawieniach regionalnych i konieczne będzie dodatkowe ręczne tłumaczenie.

Procedura tłumaczenia niestandardowej nazwy poziomu ważności:

- ustaw wymaganą niestandardową nazwę poziomu ważności, na przykład „Important”
- edytuj <frontend_dir>/locale/<required_locale>/LC_MESSAGES/frontend.po
- dodaj 2 linie:

```
msgid "Important"
msgstr "<ciąg tłumaczenia>"
```

i zapisz plik.

- utwórz pliki .mo zgodnie z opisem w <frontend_dir>/locale/README

Tutaj **msgid** powinno odpowiadać nowej niestandardowej nazwie poziomu ważności, a **msgstr** powinno być jej tłumaczeniem w danym języku.

Tę procedurę należy wykonać po każdej zmianie nazwy poziomu ważności.

Zależności wyzwalaczy

Zależności wyzwalaczy mogą być używane do unikania alertów, które nie są związane z główną przyczyną.

Zobacz wszystkie najlepsze praktyki.

Przegląd

Czasami dostępność jednego hosta zależy od innego. Serwer, który znajduje się za routerem, stanie się nieosiągalny, jeśli router przestanie działać. Jeśli dla obu skonfigurowano wyzwalacze, możesz otrzymać powiadomienia o niedostępności dwóch hostów, podczas gdy w rzeczywistości winowajcą był tylko router.

W takich przypadkach przydatne mogą być zależności między hostami. Po ustawieniu zależności powiadomienia dla elementów zależnych mogą zostać wstrzymane, a wysłane zostanie tylko powiadomienie o problemie głównym.

Chociaż Zabbix nie obsługuje bezpośrednio zależności między hostami, mogą one zostać zdefiniowane inną, bardziej elastyczną metodą — zależnościami wyzwalaczy. Wyzwalacz może zależeć od jednego lub większej liczby innych wyzwalaczy.

W naszym prostym przykładzie otwieramy formularz konfiguracji wyzwalacza serwera i ustawiamy, że zależy on od odpowiedniego wyzwalacza routera. Przy takiej zależności wyzwalacz serwera nie zmieni swojego stanu tak długo, jak wyzwalacz, od którego zależy, znajduje się w stanie „PROBLEM” — a więc nie zostaną wykonane żadne zależne akcje i nie zostaną wysłane żadne powiadomienia.

Jeśli zarówno serwer, jak i router są niedostępne i zależność jest ustawiona, Zabbix nie wykona akcji dla zależnego wyzwalacza.

Gdy nadrzędny wyzwalacz znajduje się w stanie PROBLEM, jego zależne wyzwalacze mogą zgłaszać wartości, którym nie można ufać. Dlatego zależne wyzwalacze nie będą oceniane ponownie, dopóki nadrzędny wyzwalacz (router w powyższym przykładzie):

- nie wróci ze stanu „PROBLEM” do stanu „OK”;
- nie zmieni stanu z „PROBLEM” na „UNKNOWN”;
- nie zostanie zamknięty ręcznie, przez korelację lub przy użyciu funkcji date and time i/lub nodata();
- nie zostanie rozwiązany przez wartość pozycja, która nie jest używana w zależnym wyzwalaczu;
- nie zostanie wyłączony, nie będzie miał wyłączonej pozycja lub wyłączonego hosta pozycji

We wszystkich wymienionych powyżej przypadkach zależny wyzwalacz (serwer) zostanie oceniony ponownie dopiero po otrzymaniu dla niego nowej metryki. Oznacza to, że zależny wyzwalacz może nie zostać zaktualizowany natychmiast.

Ponadto:

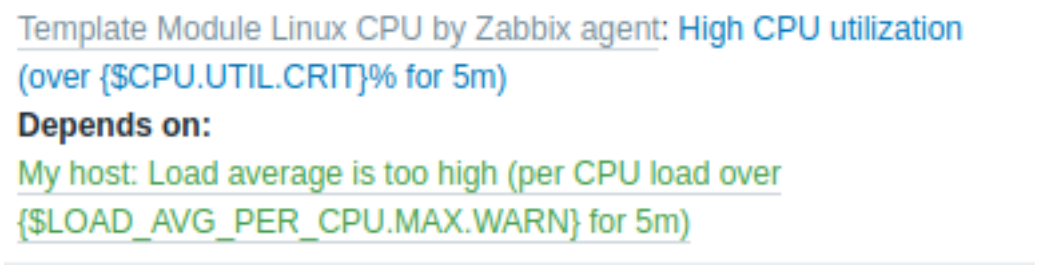
- Zależność wyzwalacza można dodać z dowolnego wyzwalacza hosta do dowolnego innego wyzwalacza hosta, o ile nie prowadzi to do zależności cyklicznej.
- Zależność wyzwalacza można dodać z jednego szablonu do drugiego. Jeśli jakiś wyzwalacz z szablonu A zależy od jakiegoś wyzwalacza z szablonu B, szablon A może być podłączony do hosta (lub innego szablonu) tylko razem z szablonem B, natomiast szablon B może być podłączony do hosta (lub innego szablonu) samodzielnie.
- Zależność wyzwalacza można dodać z wyzwalacza szablonu do wyzwalacza hosta. W takim przypadku podłączenie takiego szablonu do hosta utworzy wyzwalacz hosta, który będzie zależał od tego samego szablonu wyzwalacza, od którego zależał dany wyzwalacz. Pozwala to na przykład utworzyć szablon, w którym niektóre wyzwalacze zależą od wyzwalaczy routera (hosta). Wszystkie hosty podłączone do tego szablonu będą zależne od tego konkretnego routera.
- Zależności wyzwalacza nie można dodać z wyzwalacza hosta do wyzwalacza szablonu.
- Zależność wyzwalacza można dodać z prototypu wyzwalacza do innego prototypu wyzwalacza (w ramach tej samej reguły wykrywania niskiego poziomu) lub rzeczywistego wyzwalacza. Prototyp wyzwalacza nie może zależeć od prototypu wyzwalacza z innej reguły LLD ani od wyzwalacza utworzonego z prototypu wyzwalacza. Prototyp wyzwalacza hosta nie może zależeć od wyzwalacza z szablonu.

Konfiguracja

Aby zdefiniować zależność, otwórz kartę Zależności w formularzu konfiguracji wyzwalacza. Kliknij *Dodaj* w bloku „Zależności" i wybierz jeden lub więcej wyzwalaczy, od których dany wyzwalacz będzie zależny.



Kliknij *Aktualizuj*. Teraz wyzwalacz ma oznaczenie swojej zależności na liście.



Przykład kilku zależności

Na przykład, host znajduje się za Router2, a Router2 znajduje się za Router1.

```
Zabbix - Router1 - Router2 - Host
```

Jeśli Router1 jest niedostępny, to oczywiście host i Router2 również są nieosiągalne, jednak otrzymywanie trzech powiadomień o tym, że host, Router1 i Router2 są niedostępne, jest nadmiarowe.

Dlatego w tym przypadku definiujemy dwie zależności:

```
wyzwalacz „Host is down" zależy od wyzwalacza „Router2 is down"
wyzwalacz „Router2 is down" zależy od wyzwalacza „Router1 is down"
```

Przed zmianą stanu wyzwalacza „Host is down" Zabbix sprawdzi odpowiadające zależności wyzwalacza. Jeśli takie zostaną znalezione i jeden z tych wyzwalaczy jest w stanie **Problem**, stan wyzwalacza nie zostanie zmieniony, akcje nie zostaną wykonane i żadne powiadomienia nie zostaną wysłane.

Zabbix wykonuje to sprawdzenie rekurencyjnie. Jeśli Router1 lub Router2 jest nieosiągalny, wyzwalacz hosta nie zostanie zaktualizowany.

4 Zdarzenia

Przegląd

W Zabbix generowanych jest kilka typów zdarzeń:

- zdarzenia wyzwalaczy — za każdym razem, gdy wyzwalacz zmienia swój stan (*OK→PROBLEM→OK*)
- zdarzenia usług — za każdym razem, gdy usługa zmienia swój stan (*OK→PROBLEM→OK*)
- zdarzenia wykrywania — gdy wykrywane są hosty lub usługi
- zdarzenia autorejestracji — gdy aktywne agenty są automatycznie rejestrowane przez serwer
- zdarzenia wewnętrzne — gdy pozycja/reguła wykrywania niskiego poziomu staje się nieobsługiwana lub wyzwalacz przechodzi w nieznany stan

Zdarzenia są oznaczane znacznikiem czasu i mogą stanowić podstawę działań, takich jak wysyłanie wiadomości e-mail z powiadomieniami itp.

Aby wyświetlić szczegóły zdarzeń we frontendzie, przejdź do *Monitoring* → *Problems*. Tam możesz kliknąć datę i godzinę zdarzenia, aby wyświetlić jego szczegóły.

Więcej informacji jest dostępnych na stronach:

- zdarzenia wyzwalaczy
- inne źródła zdarzeń

1 Generowanie zdarzeń wyzwalacza

Przegląd

Zmiana stanu wyzwalacza jest najczęstszym i najważniejszym źródłem zdarzeń. Za każdym razem, gdy wyzwalacz zmienia swój stan, generowane jest zdarzenie. Zdarzenie zawiera szczegóły zmiany stanu wyzwalacza — kiedy do niej doszło i jaki jest nowy stan.

Wyzwalacze tworzą dwa typy zdarzeń — `Problem` i `OK`.

Zdarzenia problemów

Zdarzenie problemu jest tworzone:

- gdy wyrażenie wyzwalacza zostanie obliczone jako TRUE, jeśli wyzwalacz jest w stanie OK;
- za każdym razem, gdy wyrażenie wyzwalacza zostanie obliczone jako TRUE, jeśli dla wyzwalacza włączone jest generowanie wielu zdarzeń problemów.

Zdarzenia OK

Zdarzenie OK zamyka powiązane zdarzenie(a) problemu i może zostać utworzone przez 3 komponenty:

- wyzwalacze - na podstawie ustawień „Generowanie zdarzenia OK" i „Zdarzenie OK zamyka";
- korelację zdarzeń
- menedżera zadań – gdy zdarzenie jest zamykane ręcznie

Wyzwalacze

Wyzwalacze mają ustawienie „Generowanie zdarzenia OK", które określa, w jaki sposób generowane są zdarzenia OK:

- *Wyrażenie* — zdarzenie OK jest generowane dla wyzwalacza w stanie problemu, gdy jego wyrażenie przyjmuje wartość FALSE. Jest to najprostsze ustawienie, domyślnie włączone.
- *Wyrażenie odzyskiwania* — zdarzenie OK jest generowane dla wyzwalacza w stanie problemu, gdy jego wyrażenie przyjmuje wartość FALSE, a wyrażenie odzyskiwania przyjmuje wartość TRUE. Można tego użyć, jeśli kryteria odzyskiwania wyzwalacza różnią się od kryteriów problemu.
- *Brak* — zdarzenie OK nigdy nie jest generowane. Można tego użyć w połączeniu z generowaniem wielu zdarzeń problemu, aby po prostu wysłać powiadomienie, gdy coś się wydarzy.

Dodatkowo wyzwalacze mają ustawienie „Zdarzenie OK zamyka", które określa, które zdarzenia problemu są zamykane:

- *Wszystkie problemy* — zdarzenie OK zamknie wszystkie otwarte problemy utworzone przez wyzwalacz
- *Wszystkie problemy, jeśli wartości tagów są zgodne* — zdarzenie OK zamknie otwarte problemy utworzone przez wyzwalacz i mające co najmniej jedną pasującą wartość tagu. Tag jest definiowany przez ustawienie wyzwalacza „Tag do dopasowania". Jeśli nie ma żadnych zdarzeń problemu do zamknięcia, zdarzenie OK nie jest generowane. Jest to często nazywane korelacją zdarzeń na poziomie wyzwalacza.

Korelacja zdarzeń

Korelacja zdarzeń (nazywana również globalną korelacją zdarzeń) to sposób konfiguracji niestandardowych reguł zamykania zdarzeń (skutkujących generowaniem zdarzenia OK).

Reguły określają, w jaki sposób nowe zdarzenia problemowe są parowane z istniejącymi zdarzeniami problemowymi, i umożliwiają zamknięcie nowego zdarzenia lub dopasowanych zdarzeń przez wygenerowanie odpowiednich zdarzeń OK.

Jednak korelację zdarzeń należy konfigurować bardzo ostrożnie, ponieważ może ona negatywnie wpływać na wydajność przetwarzania zdarzeń lub, w przypadku błędnej konfiguracji, zamknąć więcej zdarzeń, niż zamierzano (w najgorszym przypadku mogą zostać zamknięte nawet wszystkie zdarzenia problemowe). Kilka wskazówek dotyczących konfiguracji:

1. zawsze ograniczaj zakres korelacji przez ustawienie unikalnego tagu dla zdarzenia kontrolnego (zdarzenia, które jest parowane ze starymi zdarzeniami) i użycie warunku korelacji „tag nowego zdarzenia”
2. nie zapomnij dodać warunku opartego na starym zdarzeniu podczas używania operacji „zamknij stare zdarzenie”, w przeciwnym razie wszystkie istniejące problemy mogą zostać zamknięte
3. unikaj używania popularnych nazw tagów stosowanych przez różne konfiguracje korelacji

Menedżer zadań

Jeśli dla wyzwalacza włączono ustawienie „Allow manual close”, możliwe jest ręczne zamykanie zdarzeń problemowych generowanych przez ten wyzwalacz. Odbywa się to we frontendzie podczas aktualizacji problemu. Zdarzenie nie jest zamykane bezpośrednio — zamiast tego tworzona jest pozycja „close event”, która wkrótce zostanie obsłużona przez menedżera zadań. Menedżer zadań wygeneruje odpowiednie zdarzenie OK, a zdarzenie problemowe zostanie zamknięte.

2 Inne źródła zdarzeń

Zdarzenia usługi

Zdarzenia usługi są generowane tylko wtedy, gdy działania usługi dla tych zdarzeń są włączone. W takim przypadku każda zmiana stanu usługi tworzy nowe zdarzenie:

- Zdarzenie problemu — gdy stan usługi zmienia się z `OK` na `Problem`
- Zdarzenie OK — gdy stan usługi zmienia się z `Problem` na `OK`

Zdarzenie zawiera szczegóły zmiany stanu usługi — kiedy ona nastąpiła i jaki jest nowy stan.

Zdarzenia wykrywania

Zabbix okresowo skanuje zakresy adresów IP zdefiniowane w regułach wykrywania sieci. Częstotliwość sprawdzania można skonfigurować indywidualnie dla każdej reguły. Po wykryciu hosta lub usługi generowane jest zdarzenie wykrywania (lub kilka zdarzeń).

Zabbix generuje następujące zdarzenia:

Zdarzenie	Kiedy jest generowane
Usługa dostępna	Za każdym razem, gdy Zabbix wykryje aktywną usługę.
Usługa niedostępna	Za każdym razem, gdy Zabbix nie może wykryć usługi.
Host dostępny	Jeśli dla adresu IP co najmniej jedna z usług jest w stanie UP.
Host niedostępny	Jeśli wszystkie usługi nie odpowiadają.
Usługa wykryta	Jeśli usługa powróci po okresie niedostępności lub zostanie wykryta po raz pierwszy.
Usługa utracona	Jeśli usługa zostanie utracona po wcześniejszym stanie dostępności.
Host wykryty	Jeśli host powróci po okresie niedostępności lub zostanie wykryty po raz pierwszy.
Host utracony	Jeśli host zostanie utracony po wcześniejszym stanie dostępności.

Zdarzenia aktywnej autorejestracji agenta

Aktywna autorejestracja agenta tworzy zdarzenia w Zabbixie.

Jeśli jest skonfigurowana, zdarzenie aktywnej autorejestracji agenta jest tworzone, gdy wcześniej nieznany aktywny agent żąda testów lub gdy metadane hosta uległy zmianie. Serwer dodaje nowy automatycznie zarejestrowany host, używając otrzymanego adresu IP i portu agenta.

Więcej informacji można znaleźć na stronie aktywna autorejestracja agenta.

Zdarzenia wewnętrzne

Zdarzenia wewnętrzne występują, gdy:

- pozycja zmienia stan z „normalny” na „nieobsługiwany”
- pozycja zmienia stan z „nieobsługiwany” na „normalny”
- reguła wykrywania niskiego poziomu zmienia stan z „normalny” na „nieobsługiwany”
- reguła wykrywania niskiego poziomu zmienia stan z „nieobsługiwany” na „normalny”
- wyzwalacz zmienia stan z „normalny” na „nieznany”
- wyzwalacz zmienia stan z „nieznany” na „normalny”

Celem wprowadzenia zdarzeń wewnętrznych jest umożliwienie użytkownikom otrzymywania powiadomień, gdy wystąpi dowolne zdarzenie wewnętrzne, na przykład gdy pozycja staje się nieobsługiwana i przestaje zbierać dane.

Zdarzenia wewnętrzne są tworzone tylko wtedy, gdy włączone są działania wewnętrzne dla tych zdarzeń. Aby zatrzymać generowanie zdarzeń wewnętrznych (na przykład dla pozycji stających się nieobsługiwanymi), wyłącz wszystkie działania dla zdarzeń wewnętrznych w Alerty → Działania → Działania wewnętrzne.

Note:
Jeśli działania wewnętrzne są wyłączone, a obiekt znajduje się w stanie „nieobsługiwany", zdarzenie odzyskania dla tego obiektu nadal zostanie utworzone.

Jeśli działania wewnętrzne są włączone, a obiekt znajduje się w stanie „nieobsługiwany", zdarzenie odzyskania dla tego obiektu zostanie utworzone, mimo że „zdarzenie problemu" nie zostało utworzone dla tego obiektu.

Zobacz także: Otrzymywanie powiadomień o nieobsługiwanych pozycjach

3 Ręczne zamykanie problemów

Przegląd

Chociaż zazwyczaj zdarzenia problemów są rozwiązywane automatycznie, gdy stan wyzwalacza zmienia się z `Problem` na `OK`, mogą wystąpić przypadki, gdy trudno jest określić, czy problem został rozwiązany za pomocą wyrażenia wyzwalacza. W takich przypadkach problem musi zostać rozwiązany ręcznie.

Na przykład *syslog* może zgłaszać, że niektóre parametry jądra wymagają dostrojenia w celu uzyskania optymalnej wydajności. W takim przypadku problem jest zgłaszany administratorom Linuksa, którzy go naprawiają, a następnie ręcznie zamykają problem.

Problemy mogą być zamykane ręcznie tylko dla wyzwalaczy z włączoną opcją *Allow manual close*.

Gdy problem zostanie „zamknięty ręcznie", Zabbix generuje nowe wewnętrzne zadanie dla serwera Zabbix. Następnie proces *task manager* wykonuje to zadanie i generuje zdarzenie OK, zamykając tym samym zdarzenie problemu.

Wygenerowane zdarzenie *OK* zawiera pełny zestaw tagów zdarzenia określonych dla tego zdarzenia (w tym tagi dziedziczone z szablonów, hostów i wyzwalaczy). Tagi te są dostępne w powiadomieniach oraz w makrach takich jak `{EVENT.RECOVERY.TAGS}` i `{EVENT.RECOVERY.TAGSJSON}`.

Ręczne zamknięcie problemu nie oznacza, że bazowy wyzwalacz nigdy więcej nie przejdzie do stanu *Problem*. Wyrażenie wyzwalacza jest oceniane ponownie i może ponownie skutkować problemem:

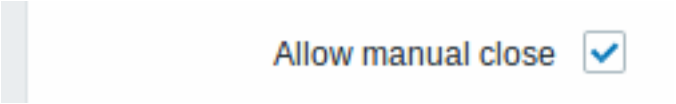
- Gdy nadejdą nowe dane dla dowolnej pozycji uwzględnionej w wyrażeniu wyzwalacza (należy pamiętać, że wartości odrzucone przez krok przetwarzania wstępnego typu throttling nie są uznawane za odebrane i nie spowodują ponownej oceny wyrażenia wyzwalacza);
- Gdy w wyrażeniu używane są funkcje date and time i/lub nodata().

Konfiguracja

Do ręcznego zamknięcia problemu wymagane są dwa kroki.

Konfiguracja wyzwalacza

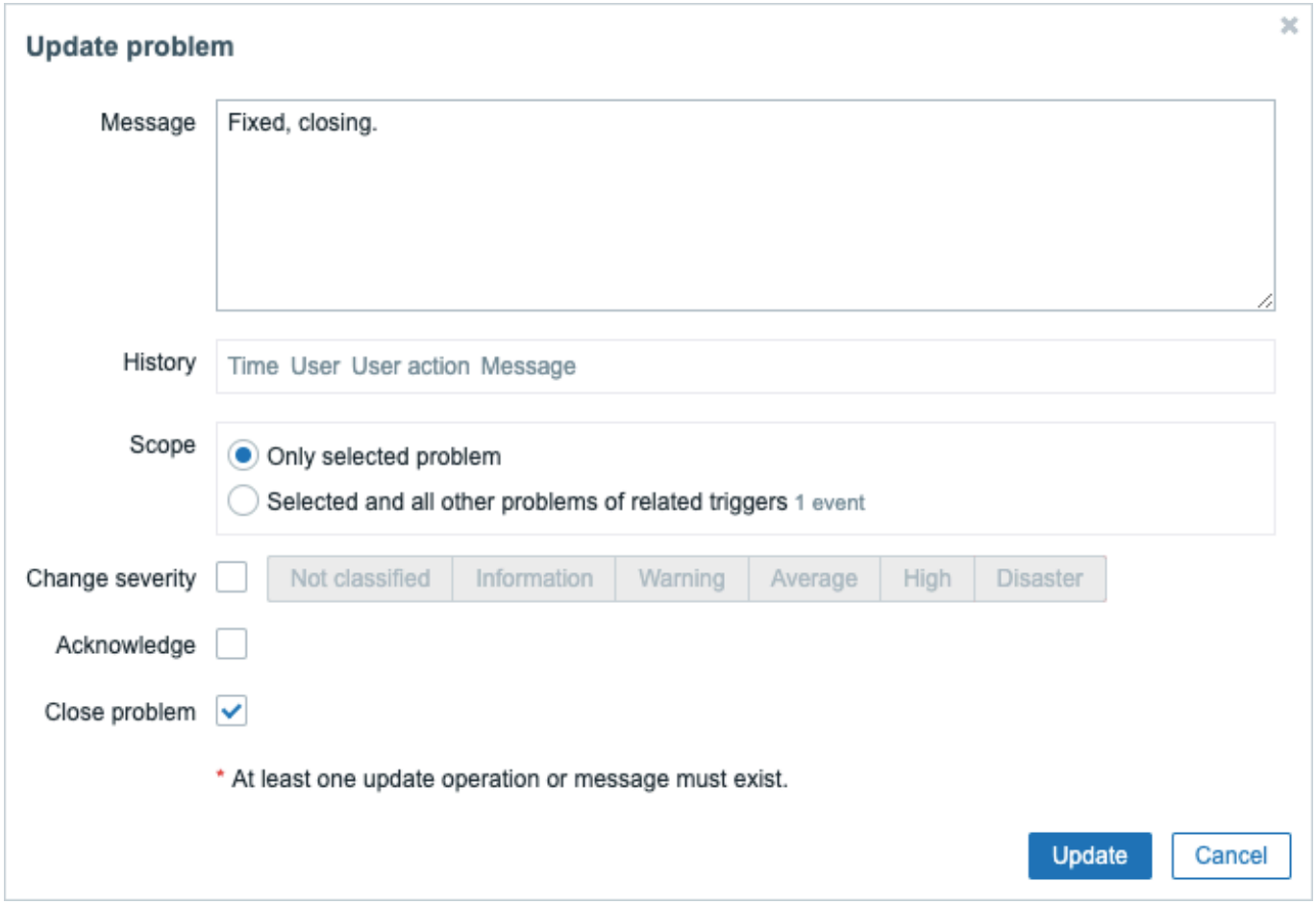
W konfiguracji wyzwalacza włącz opcję *Allow manual close*.



Okno aktualizacji problemu

Jeśli dla wyzwalacza z flagą *Manual close* wystąpi problem, możesz otworzyć wyskakujące okno aktualizacji problemu dla tego problemu i zamknąć problem ręcznie.

Aby zamknąć problem, zaznacz w formularzu opcję *Close problem* i kliknij *Update*.



Wszystkie wymagane pola wejściowe są oznaczone czerwoną gwiazdką.

Żądanie jest przetwarzane przez serwer Zabbix. Zamknięcie problemu zwykle zajmuje kilka sekund. W trakcie tego procesu w *Monitoring* > *Problems* jako status problemu wyświetlane jest *CLOSING*.

Weryfikacja

Można zweryfikować, że problem został zamknięty ręcznie:

- w szczegółach zdarzenia, dostępnych przez *Monitoring* > *Problems*;
- używając makra `{EVENT.UPDATE.HISTORY}` w wiadomościach powiadomień, które dostarczy tę informację.

5 Korelacja zdarzeń

Przegląd

Korelacja zdarzeń umożliwia powiązanie zdarzeń problemowych z ich rozwiązaniem w sposób bardzo precyzyjny i elastyczny.

Korelację zdarzeń można zdefiniować:

- na poziomie wyzwalacza - jeden wyzwalacz może być użyty do powiązania oddzielnych problemów z ich rozwiązaniem
- globalnie - problemy mogą być powiązane z ich rozwiązaniem z innego wyzwalacza/metody odpytywania przy użyciu globalnych reguł korelacji

1 Korelacja zdarzeń oparta na wyzwalaczach

Przegląd

Korelacja zdarzeń oparta na wyzwalaczach pozwala korelować oddzielne problemy zgłaszane przez jeden wyzwalacz.

Chociaż zasadniczo zdarzenie OK może zamknąć wszystkie zdarzenia problemów utworzone przez jeden wyzwalacz, istnieją przypadki, w których potrzebne jest bardziej szczegółowe podejście. Na przykład podczas monitorowania plików dziennika możesz chcieć wykrywać określone problemy w pliku dziennika i zamykać je indywidualnie, a nie wszystkie jednocześnie.

Dotyczy to wyzwalaczy, dla których parametr *PROBLEM event generation mode* jest ustawiony na *Multiple*. Takie wyzwalacze są zwykle używane do monitorowania logów, przetwarzania trapów itp.

W Zabbix możliwe jest powiązanie zdarzeń problemów na podstawie tagów. Tagi są używane do wyodrębniania wartości i tworzenia identyfikacji dla zdarzeń problemów. Dzięki temu problemy mogą być również zamykane indywidualnie na podstawie pasującego tagu.

Innymi słowy, ten sam wyzwalacz może tworzyć oddzielne zdarzenia identyfikowane przez tag zdarzenia. Dlatego zdarzenia problemów mogą być identyfikowane pojedynczo i zamykane oddzielnie na podstawie identyfikacji przez tag zdarzenia.

Jak to działa

Podczas monitorowania logów możesz napotkać wiersze podobne do tych:

```
Wiersz1: Usługa 1 została zatrzymana
Wiersz2: Usługa 2 została zatrzymana
Wiersz3: Usługa 1 została uruchomiona ponownie
Wiersz4: Usługa 2 została uruchomiona ponownie
```

Ideą korelacji zdarzeń jest możliwość dopasowania zdarzenia problemowego z Wiersza1 do rozwiązania z Wiersza3 oraz zdarzenia problemowego z Wiersza2 do rozwiązania z Wiersza4 i zamykania tych problemów jeden po drugim:

```
Wiersz1: Usługa 1 została zatrzymana
Wiersz3: Usługa 1 została uruchomiona ponownie #problem z Wiersza 1 zamknięty

Wiersz2: Usługa 2 została zatrzymana
Wiersz4: Usługa 2 została uruchomiona ponownie #problem z Wiersza 2 zamknięty
```

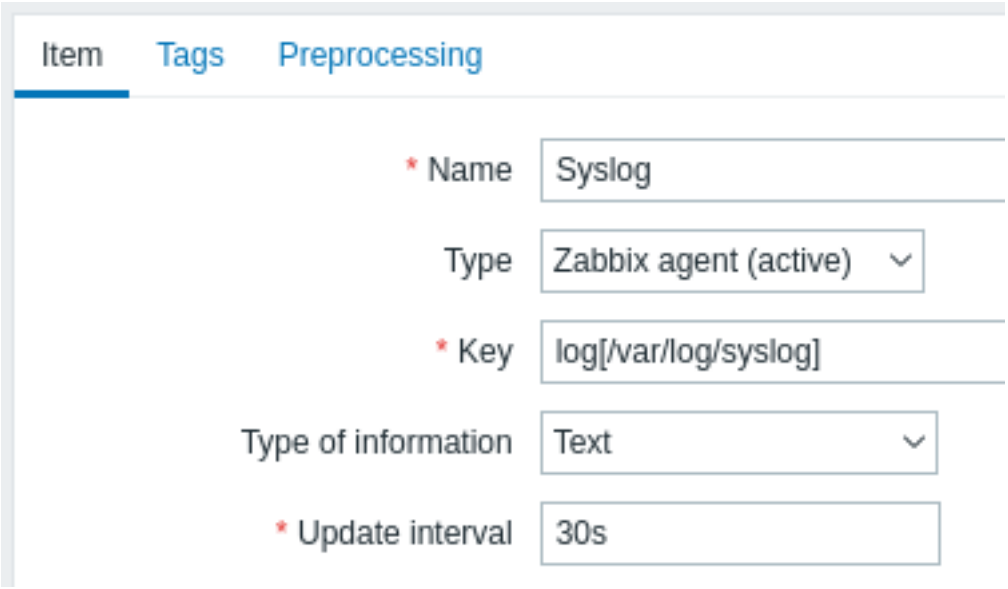
Aby to zrobić, musisz oznaczyć te powiązane zdarzenia tagami, na przykład „Usługa 1" i „Usługa 2". Można to zrobić, stosując wyrażenie regularne do wiersza logu w celu wyodrębnienia wartości tagu. Następnie, gdy zdarzenia są tworzone, otrzymują odpowiednio tagi „Usługa 1" i „Usługa 2", a problem może zostać dopasowany do rozwiązania.

Konfiguracja

Pozycja

Na początek możesz skonfigurować pozycję monitorującą plik dziennika, na przykład:

```
log[/var/log/syslog]
```



Po skonfigurowaniu pozycji odczekaj minutę, aż zmiany konfiguracji zostaną zastosowane, a następnie przejdź do Najnowsze dane, aby upewnić się, że pozycja rozpoczęła zbieranie danych.

Wyzwalacz

Gdy pozycja działa, należy skonfigurować wyzwalacz. Ważne jest, aby zdecydować, które wpisy w pliku dziennika są warte uwagi. Na przykład poniższe wyrażenie wyzwalacza będzie wyszukiwać ciąg znaków 'Stopping', aby sygnalizować potencjalne problemy:

```
find(/My host/log[/var/log/syslog],,"regexp","Stopping")=1
```

Attention:
Aby upewnić się, że każda linia zawierająca ciąg ”Stopping” jest traktowana jako problem, ustaw również opcję *Tryb generowania zdarzeń problemów* w konfiguracji wyzwalacza na ’Multiple’.

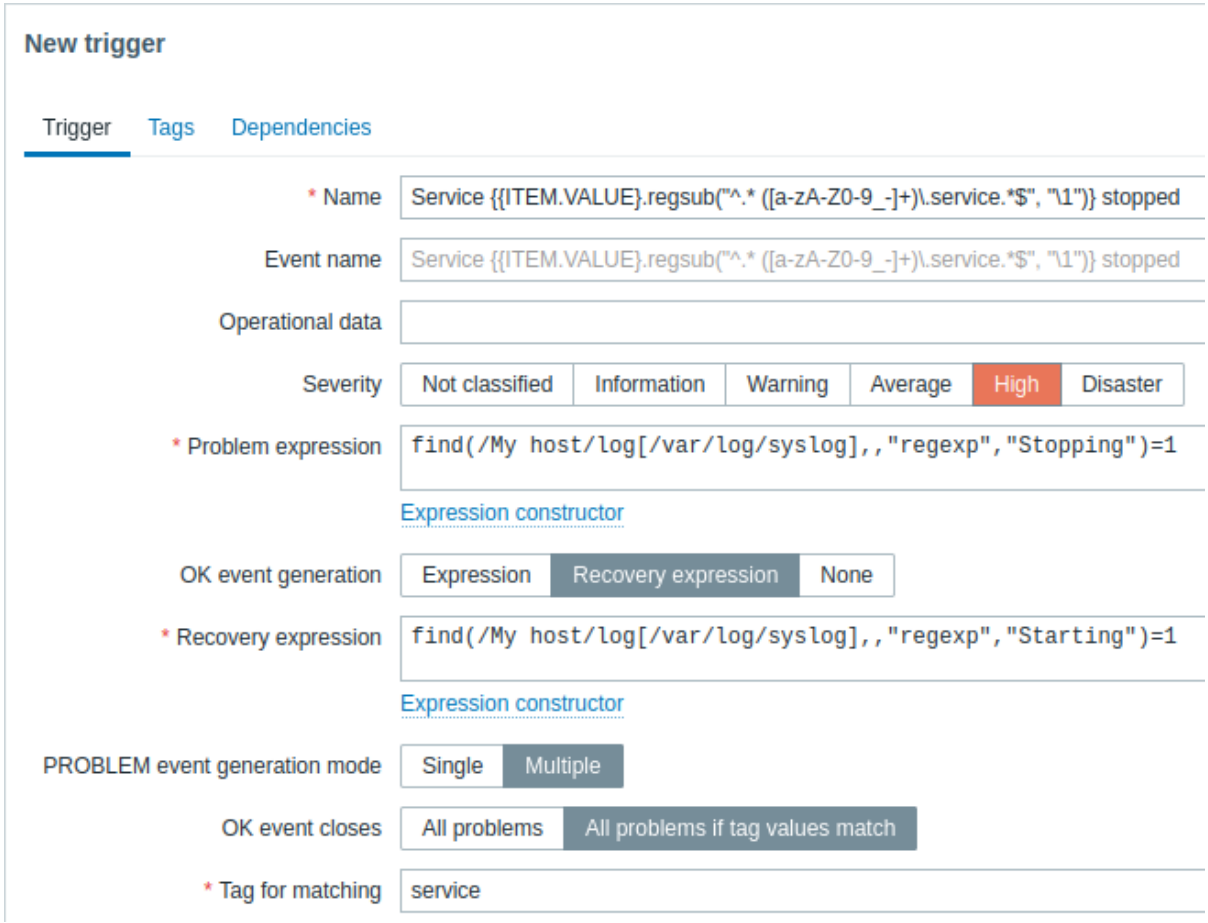
Następnie zdefiniuj wyrażenie odzyskiwania. Poniższe wyrażenie odzyskiwania spowoduje rozwiązanie wszystkich problemów, jeśli zostanie znaleziona linia dziennika zawierająca ciąg ”Starting”:

```
find(/My host/log[/var/log/syslog],,"regexp","Starting")=1
```

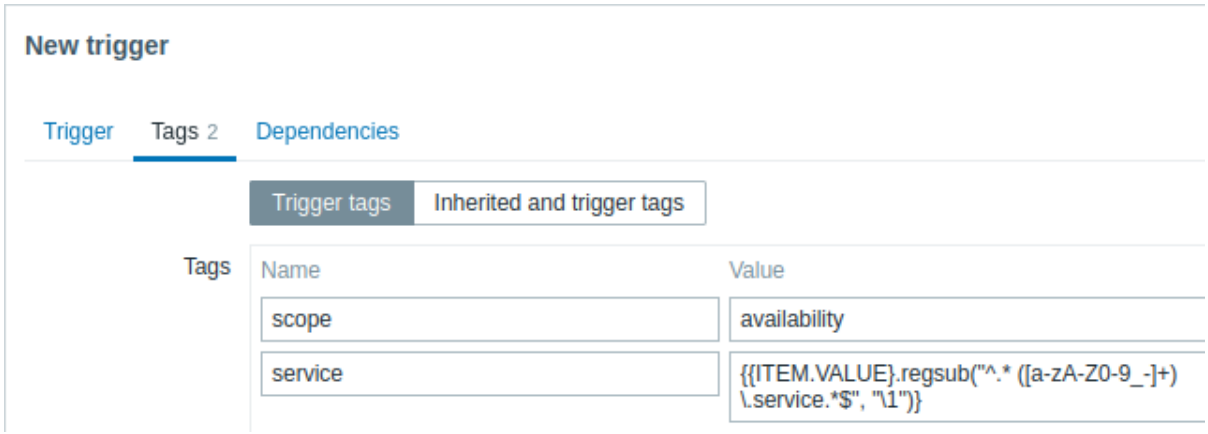
Ponieważ nie tego chcemy, ważne jest, aby w jakiś sposób upewnić się, że zamykane są odpowiadające im główne problemy, a nie po prostu wszystkie problemy. W tym miejscu pomocne może być tagowanie.

Problemy i rozwiązania można dopasować, określając tag w konfiguracji wyzwalacza. Należy wprowadzić następujące ustawienia:

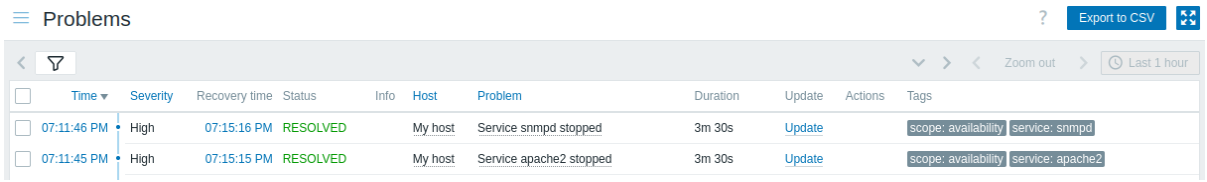
- *Tryb generowania zdarzeń problemów*: Multiple
- *Zdarzenie OK zamyka*: Wszystkie problemy, jeśli wartości tagów są zgodne
- Wprowadź nazwę tagu do dopasowywania zdarzeń



- skonfiguruj tagi, aby wyodrębniać wartości tagów z linii dziennika



Jeśli konfiguracja zakończy się powodzeniem, będzie można zobaczyć zdarzenia problemów otagowane według aplikacji i dopasowane do ich rozwiązania w *Monitoring* → *Problems*.



Warning:
Ponieważ możliwa jest błędna konfiguracja, gdy podobne tagi zdarzeń mogą zostać utworzone dla **niepowiązanych** problemów, zapoznaj się z przypadkami opisanymi poniżej!

- Makra indeksowane zawsze odnoszą się do pola *Expression* w konfiguracji wyzwalacza, a nie do *Recovery expression*. Na przykład w zdarzeniu odzyskiwania **{ITEM.VALUE1}** zostanie rozwinięte do najnowszej wartości pierwszej pozycji **w wyrażeniu problemu** w momencie odzyskiwania. Jeśli wyrażenie odzyskiwania opiera się na innej pozycji, a wartość pozycji z wyrażenia problemu zmieni się do czasu odzyskiwania, zdarzenia otrzymają różne tagi i nie zostaną skorelowane.

- Gdy dwie aplikacje zapisują komunikaty o błędach i odzyskiwaniu do tego samego pliku dziennika, użytkownik może zdecydować się na użycie dwóch tagów *service* w tym samym wyzwalaczu z różnymi wartościami tagów, stosując osobne wyrażenia regularne w wartościach tagów do wyodrębnienia nazw, powiedzmy, usługi A i usługi B z makra {ITEM.VALUE} (np. gdy formaty komunikatów się różnią). Jednak może to nie działać zgodnie z oczekiwaniami, jeśli nie będzie dopasowania do wyrażeń regularnych. Niedopasowane regexpy dadzą puste wartości tagów, a pojedyncza pusta wartość tagu zarówno w zdarzeniach problemów, jak i OK wystarczy do ich skorelowania. Tak więc komunikat odzyskiwania z usługi A może przypadkowo zamknąć komunikat o błędzie z usługi B.
- Rzeczywiste tagi i wartości tagów stają się widoczne dopiero po zadziałaniu wyzwalacza. Jeśli użyte wyrażenie regularne jest nieprawidłowe, zostaje ono po cichu zastąpione ciągiem *UNKNOWN*. Jeśli początkowe zdarzenie problemu z wartością tagu *UNKNOWN* zostanie przeoczone, mogą pojawić się kolejne zdarzenia OK z tą samą wartością tagu *UNKNOWN*, które mogą zamknąć zdarzenia problemów, których nie powinny były zamknąć.
- Jeśli użytkownik używa makra {ITEM.VALUE} bez funkcji makr jako wartości tagu, obowiązuje ograniczenie do 255 znaków. Gdy komunikaty dziennika są długie, a pierwsze 255 znaków nie jest charakterystyczne, może to również skutkować podobnymi tagami zdarzeń dla niepowiązanych problemów.

2 Globalna korelacja zdarzeń

Przegląd

Globalna korelacja zdarzeń pozwala objąć wszystkie metryki monitorowane przez Zabbix i tworzyć korelacje.

Możliwe jest korelowanie zdarzeń utworzonych przez całkowicie różne wyzwalacze i stosowanie do nich wszystkich tych samych operacji. Dzięki tworzeniu inteligentnych reguł korelacji można w praktyce uwolnić się od tysięcy powtarzalnych powiadomień i skupić się na źródłowych przyczynach problemu!

Globalna korelacja zdarzeń to potężny mechanizm, który pozwala uniezależnić się od logiki problemów i ich rozwiązywania opartej na pojedynczym wyzwalaczu. Dotychczas pojedyncze zdarzenie problemu było tworzone przez jeden wyzwalacz i od tego samego wyzwalacza zależało rozwiązanie problemu. Nie mogliśmy rozwiązać problemu utworzonego przez jeden wyzwalacz za pomocą innego wyzwalacza. Jednak dzięki korelacji zdarzeń opartej na tagowaniu zdarzeń jest to możliwe.

Na przykład wyzwalacz logów może zgłaszać problemy aplikacji, podczas gdy wyzwalacz odpytywania może zgłaszać, że aplikacja działa i jest dostępna. Korzystając z tagów zdarzeń, można oznaczyć wyzwalacz logów tagiem *status:down*, a wyzwalacz odpytywania tagiem *status:up*. Następnie w globalnej regule korelacji można powiązać te wyzwalacze i przypisać do tej korelacji odpowiednią operację, taką jak zamykanie starych zdarzeń.

W innym zastosowaniu globalna korelacja może identyfikować podobne wyzwalacze i stosować do nich tę samą operację. Co, jeśli moglibyśmy otrzymywać tylko jedno zgłoszenie problemu dla problemu z portem sieciowym? Nie ma potrzeby zgłaszać ich wszystkich. To również jest możliwe dzięki globalnej korelacji zdarzeń.

Globalna korelacja zdarzeń jest konfigurowana w **regułach korelacji**. Reguła korelacji określa, w jaki sposób nowe zdarzenia problemów są łączone w pary z istniejącymi zdarzeniami problemów oraz co należy zrobić w przypadku dopasowania (zamknąć nowe zdarzenie, zamknąć dopasowane stare zdarzenia przez wygenerowanie odpowiadających im zdarzeń OK). Jeśli problem zostanie zamknięty przez globalną korelację, zostanie to zgłoszone w kolumnie *Info* w *Monitoring* > *Problems*.

Konfigurowanie globalnej korelacji jest dostępne wyłącznie dla użytkowników na poziomie Super Admin.

Attention:
Korelację zdarzeń należy konfigurować bardzo ostrożnie, ponieważ może ona negatywnie wpływać na wydajność przetwarzania zdarzeń lub — w przypadku błędnej konfiguracji — zamknąć więcej zdarzeń, niż zamierzano (w najgorszym przypadku mogą zostać zamknięte nawet wszystkie zdarzenia problemów).

Aby **bezpiecznie** skonfigurować globalną korelację, należy przestrzegać następujących ważnych wskazówek:

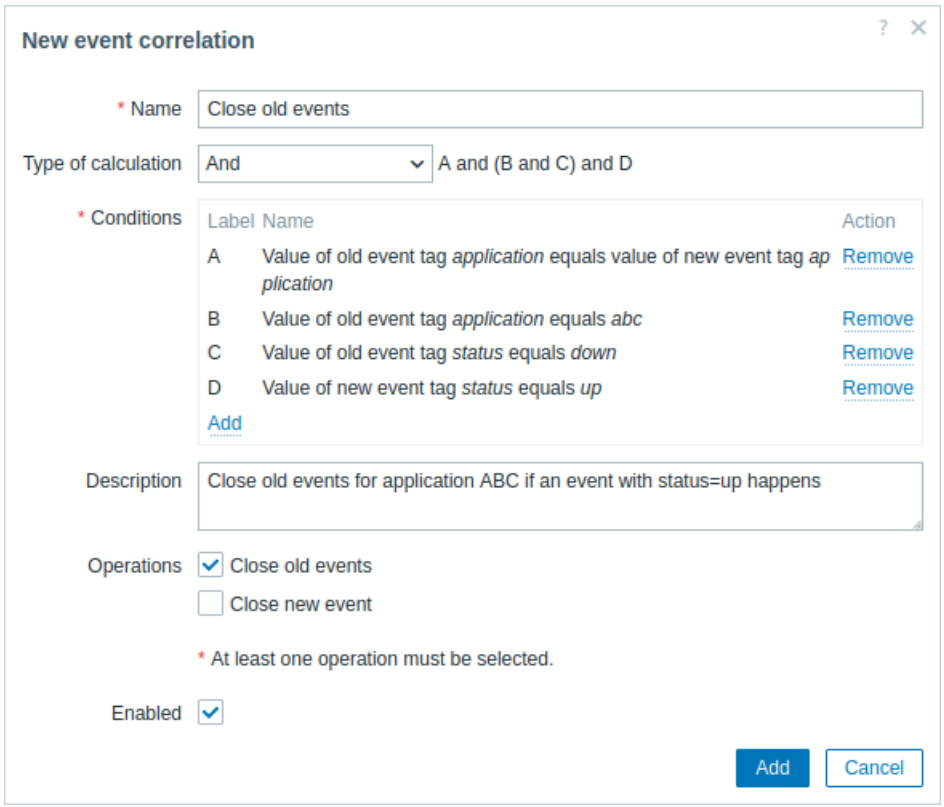
- Ogranicz zakres korelacji. Zawsze ustawiaj unikalny tag dla nowego zdarzenia, które jest łączone w parę ze starymi zdarzeniami, i używaj warunku korelacji *New event tag name*.
- Dodaj jawny warunek starego zdarzenia podczas używania **Close old events**. Zawsze dodawaj co najmniej jeden warunek *Old event* (na przykład *Old event tag name*, *Old event tag value* lub *Event tag pair*) przy wyborze **Close old events** — w przeciwnym razie reguła może dopasować i zamknąć niepowiązane istniejące zdarzenia problemów (w najgorszym przypadku wszystkie problemy). Do dopasowywania wartości środowiska uruchomieniowego (host:port, session id itp.) preferuj **Event tag pair**, a jeśli to możliwe, dodatkowo zawężaj dopasowanie według hosta lub grupy hostów.
- Unikaj używania popularnych nazw tagów, które mogą zostać użyte przez różne konfiguracje korelacji.
- Ogranicz liczbę reguł korelacji do tych, których naprawdę potrzebujesz.

Zobacz także: znane problemy.

Konfiguracja

Aby skonfigurować globalne reguły korelacji zdarzeń:

- Przejdź do *Data collection* > *Event correlation*
- Kliknij *Create event correlation* po prawej stronie (lub nazwę korelacji, aby edytować istniejącą regułę)
- Wprowadź parametry reguły korelacji w formularzu

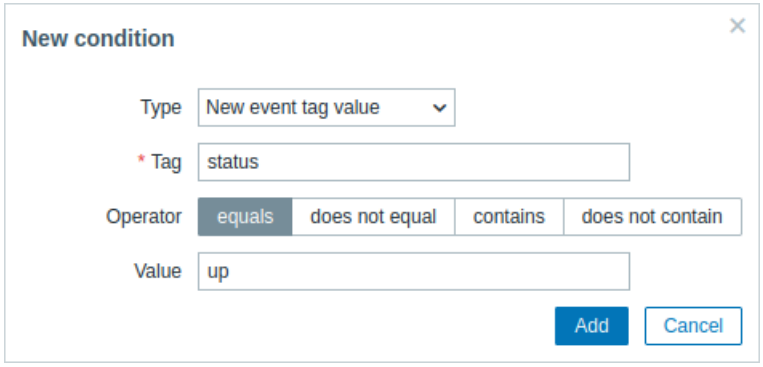


Wszystkie wymagane pola wejściowe są oznaczone czerwoną gwiazdką.

Parameter	Description
Name	Unikalna nazwa reguły korelacji.
Type of calculation	Dostępne są następujące opcje obliczania warunków: **And** - wszystkie warunki muszą być spełnione **Or** - wystarczy, że jeden warunek jest spełniony **And/Or** - AND dla różnych typów warunków oraz OR dla tego samego typu warunku **Custom expression** - zdefiniowana przez użytkownika formuła obliczeniowa do oceny warunków akcji. Musi zawierać wszystkie warunki (reprezentowane jako wielkie litery A, B, C, ...) i może zawierać spacje, tabulatory, nawiasy ( ), **and** (z rozróżnianiem wielkości liter), **or** (z rozróżnianiem wielkości liter), **not** (z rozróżnianiem wielkości liter).

Parameter	Description
Conditions	Lista warunków. Szczegóły dotyczące konfiguracji warunku znajdują się poniżej.
Description	Opis reguły korelacji.
Operations	Zaznacz pole wyboru operacji, która ma zostać wykonana po skorelowaniu zdarzenia. Dostępne są następujące operacje: **Close old events** - zamknij stare zdarzenia, gdy wystąpi nowe zdarzenie. Zawsze dodawaj warunek oparty na starym zdarzeniu podczas używania operacji *Close old events*, w przeciwnym razie wszystkie istniejące problemy mogą zostać zamknięte. **Close new event** - zamknij nowe zdarzenie, gdy wystąpi. **Warning!** Nie pozostawiaj pustych warunków starego/nowego zdarzenia podczas używania *Close old events*/*Close new event*. Jeśli wybierzesz operację *Close old events* bez dodania warunku pasującego do starego zdarzenia, Zabbix może dopasować wszystkie istniejące stare zdarzenia i je zamknąć. Zawsze dodawaj jawny warunek starego zdarzenia (na przykład *Old event tag name* lub *Event tag pair*) podczas używania *Close old events*. Na przykład reguła, która używa tylko *New event condition* oraz operacji *Close old events*, dopasuje wszystkie stare zdarzenia spełniające kryteria starego zdarzenia (których brak) — skutecznie zamykając stare problemy.
Enabled	Jeśli zaznaczysz to pole wyboru, reguła korelacji będzie włączona.

Aby skonfigurować szczegóły nowego warunku, kliknij Add w bloku Conditions. Otworzy się wyskakujące okno, w którym można edytować szczegóły warunku.



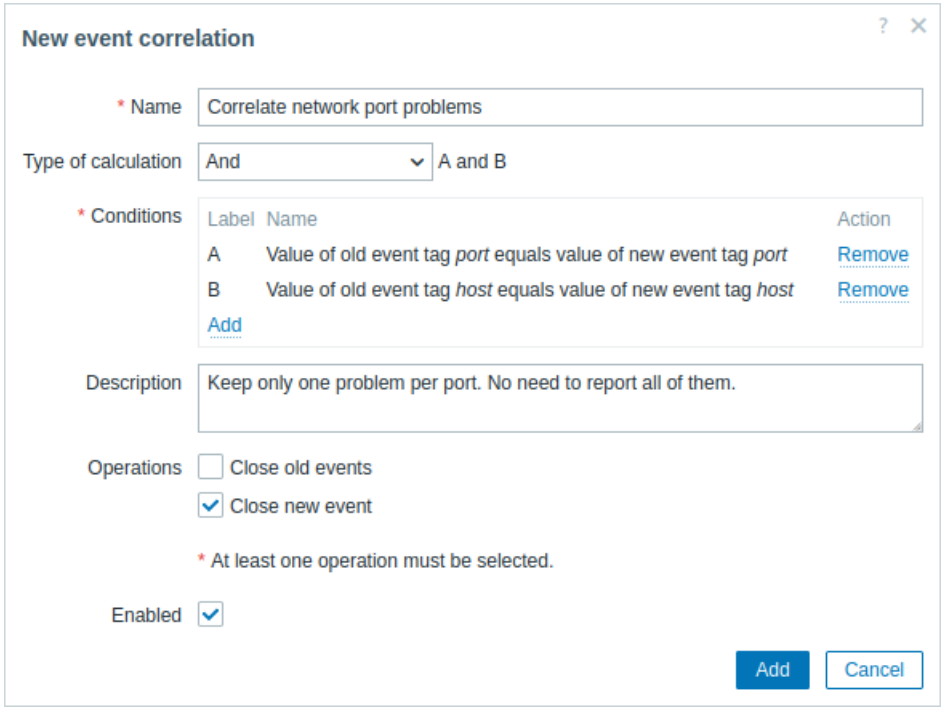
Parameter	Description
New condition	Wybierz warunek do korelacji zdarzeń. *Uwaga:* jeśli nie określono warunku starego zdarzenia, wszystkie stare zdarzenia mogą zostać dopasowane i zamknięte. Podobnie, jeśli nie określono warunku nowego zdarzenia, wszystkie nowe zdarzenia mogą zostać dopasowane i zamknięte. Dostępne są następujące warunki: **Old event tag name** - określ nazwę tagu starego zdarzenia do dopasowania. **New event tag name** - określ nazwę tagu nowego zdarzenia do dopasowania. **New event host group** - określ grupę hostów nowego zdarzenia do dopasowania. **Event tag pair** - określ nazwę tagu nowego zdarzenia i nazwę tagu starego zdarzenia do dopasowania. W takim przypadku dopasowanie nastąpi, jeśli **wartości** tagów w obu zdarzeniach są zgodne. *Nazwy* tagów nie muszą być zgodne. Ta opcja jest przydatna do dopasowywania wartości czasu działania, które mogą nie być znane w momencie konfiguracji (zobacz także Przykład). **Old event tag value** - określ nazwę i wartość tagu starego zdarzenia do dopasowania, używając następujących operatorów: *equals* - ma wartość tagu starego zdarzenia *does not equal* - nie ma wartości tagu starego zdarzenia *contains* - zawiera ciąg w wartości tagu starego zdarzenia *does not contain* - nie zawiera ciągu w wartości tagu starego zdarzenia **New event tag value** - określ nazwę i wartość tagu nowego zdarzenia do dopasowania, używając następujących operatorów: *equals* - ma wartość tagu nowego zdarzenia *does not equal* - nie ma wartości tagu nowego zdarzenia *contains* - zawiera ciąg w wartości tagu nowego zdarzenia *does not contain* - nie zawiera ciągu w wartości tagu nowego zdarzenia

Warning:
Ponieważ możliwa jest błędna konfiguracja, gdy podobne tagi zdarzeń mogą być tworzone dla **niepowiązanych** problemów, zapoznaj się z przypadkami opisanymi poniżej!

- Rzeczywiste tagi i wartości tagów stają się widoczne dopiero po uruchomieniu wyzwalacza. Jeśli użyte wyrażenie regularne jest nieprawidłowe, jest ono po cichu zastępowane ciągiem *UNKNOWN*. Jeśli początkowe zdarzenie problemu z wartością tagu *UNKNOWN* zostanie pominięte, mogą pojawić się kolejne zdarzenia OK z tą samą wartością tagu *UNKNOWN*, które mogą zamknąć zdarzenia problemów, których nie powinny były zamknąć.
- Jeśli użytkownik używa makra {ITEM.VALUE} bez funkcji makr jako wartości tagu, obowiązuje ograniczenie do 255 znaków. Gdy komunikaty logów są długie, a pierwsze 255 znaków jest niespecyficzne, może to również skutkować podobnymi tagami zdarzeń dla niepowiązanych problemów.

Przykład

Zatrzymaj powtarzające się zdarzenia problemów z tego samego portu sieciowego.



Ta globalna reguła korelacji będzie korelować problemy, jeśli wartości tagów *host* i *port* istnieją w wyzwalaczu i są takie same w oryginalnym oraz nowym zdarzeniu.

Operacja zamknie nowe zdarzenia problemów na tym samym porcie sieciowym, pozostawiając otwarty tylko oryginalny problem.

6 Tagowanie

Przegląd

Tagi składają się z nazwy tagu i wartości tagu. Podczas tagowania encji można użyć samej nazwy lub połączyć ją z wartością (na przykład `mysql`, `jira`, `target:mysql`, `service:jira` itd.).

Tagi można definiować dla różnych encji:

- Szablony
- Hosty
- Pozycje
- Scenariusze WWW
- Wyzwalacze
- Usługi
- Pozycje i wyzwalacze szablonów
- Prototypy hostów, pozycji i wyzwalaczy

Na listach *Templates*, *Hosts*, *Items*, *Triggers*, *Web scenarios* oraz ich prototypów kolumna *Tags* wyświetla zarówno zwykłe, jak i dziedziczone tagi. Po najechaniu kursorem na *dziedziczony* tag lub kliknięciu go pojawia się podpowiedź JavaScript z tekstem „Inherited tag". Jeśli dziedziczony tag istnieje również jako zwykły tag, wyświetlany jest inny tekst podpowiedzi zależnie od listy, na której się pojawia (na przykład „Inherited and template tag" na liście templates lub „Inherited and host tag" na liście hosts). W innych miejscach frontend zwykłe i dziedziczone tagi są wyświetlane razem (duplikaty są usuwane), bez ikon i bez dodatkowego tekstu podpowiedzi.

Note:
Zapoznaj się z oficjalnymi wytycznymi Zabbix dotyczącymi ogólnych zaleceń w zakresie definiowania tagów, a także ze szczegółowymi wskazówkami dla szablonów, pozycji, wyzwalaczy oraz reguł wykrywania niskiego poziomu.

Tagi mają wiele zastosowań, przede wszystkim do oznaczania zdarzeń. Gdy encje są otagowane, każde nowe zdarzenie powiązane z otagowaną encją odziedziczy jej tagi. Na przykład:

- w przypadku otagowanych szablonów — każdy problem hosta (utworzony przez wyzwalacze z szablonu) odziedziczy tagi szablonu.
- w przypadku otagowanych hostów — każdy problem hosta odziedziczy tagi hosta.

- w przypadku otagowanych pozycji/scenariuszy WWW — każdy problem pozycji/scenariusza WWW odziedziczy tagi pozycji/scenariusza WWW.
- w przypadku otagowanych wyzwalaczy — każdy problem utworzony przez wyzwalacz odziedziczy tagi wyzwalacza.

Zdarzenie problemu dziedziczy wszystkie tagi z całego łańcucha encji — szablonów, hostów, pozycji/scenariuszy WWW, wyzwalaczy. Identyczne kombinacje `tag:value` (po rozwinięciu makr) są scalane w jedną, co pozwala uniknąć duplikacji.

Zdarzenia odtworzenia wygenerowane przez ręczne zamknięcie również zawierają rozwinięte tagi zdarzenia odziedziczone z szablonów, hostów, pozycji/scenariuszy WWW i wyzwalaczy. Tagi te są dostępne w powiadomieniach oraz za pośrednictwem makr takich jak `{EVENT.RECOVERY.TAGS}` i `{EVENT.RECOVERY.TAGSJSON}`.

Niestandardowe tagi zdarzeń oferują większą elastyczność. Na przykład:

- korelację zdarzeń można skonfigurować na podstawie tagów zdarzeń.
- warunki akcji można skonfigurować na podstawie tagów zdarzeń.
- problemy pozycji mogą być grupowane na podstawie tagów zdarzeń.
- tagi problemów mogą być używane do mapowania problemów na usługi.

Encje mogą być oznaczone tym samym tagiem, ale z różnymi wartościami tagu (na przykład `component:memory` i `component:storage`). Podobnie encja może mieć tag bez wartości oraz ten sam tag z wartością (na przykład `database` i `database:postgresql`). Takie tagi nie są uznawane za duplikaty.

Przykłady użycia

Niektóre typowe przypadki użycia tagowania są następujące:

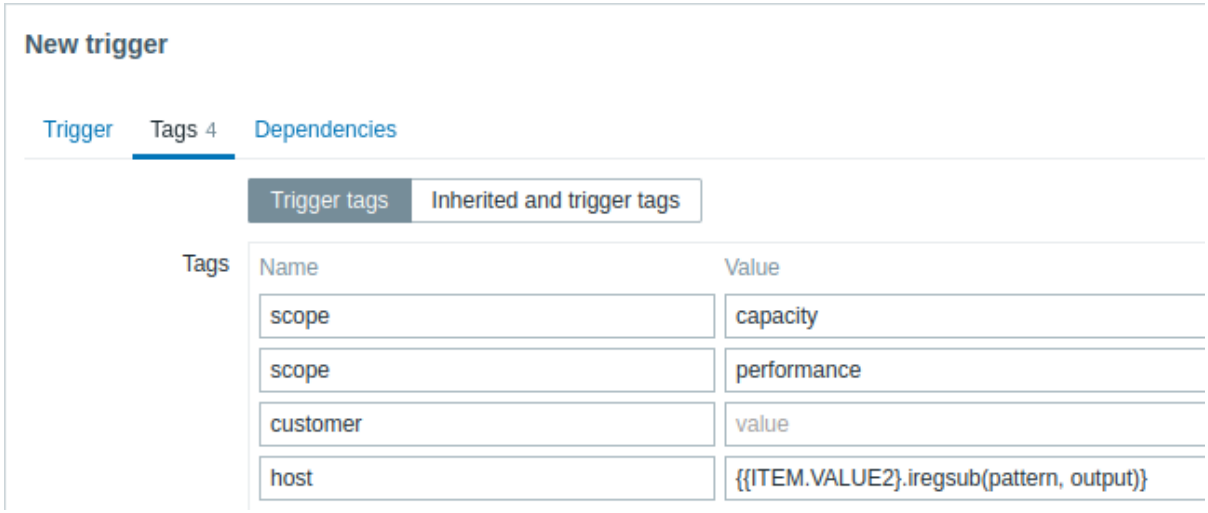
1. Oznaczanie zdarzeń wyzwalaczy:
   - Zdefiniuj tag wyzwalacza (na przykład `scope:performance`).
   - Problemy utworzone przez ten wyzwalacz będą miały tag wyzwalacza.
2. Oznaczanie problemów dziedziczonych z szablonu:
   - Zdefiniuj tag szablonu (na przykład `target:mysql`).
   - Problemy utworzone przez wyzwalacze z tego szablonu będą miały tag szablonu.
3. Oznaczanie problemów hosta:
   - Zdefiniuj tag hosta (na przykład `service:jira`).
   - Problemy utworzone przez wyzwalacze z tego hosta będą miały tag hosta.
4. Filtrowanie powiązanych pozycji:
   - Zdefiniuj tag pozycji (na przykład `component:cpu`).
   - W *Monitoring* > *Latest data* pozycje można filtrować według tagu `component:cpu`.
5. Użycie informacji wyodrębnionych z wartości pozycji jako wartości tagu:
   - Zdefiniuj tag z makrem jako wartością tagu (na przykład `tag-name:{{ITEM.VALUE<N>}.regsub()}`).
   - W *Monitoring* > *Problems* problemy będą miały wartość tagu ustawioną na dane wyodrębnione z wartości pozycji.
6. Identyfikowanie problemów w pliku dziennika i zamykanie ich oddzielnie:
   - Zdefiniuj tag wyzwalacza dla wyzwalacza pozycji monitorowania logów, który będzie wyodrębniał wartości z wartości pozycji przy użyciu makra (na przykład `service:{{ITEM.VALUE<N>}.regsub()}`).
   - W konfiguracji wyzwalacza skonfiguruj korelację zdarzeń:
     - ustaw *PROBLEM event generation mode* na "Multiple";
     - ustaw *OK event closes* na "All problems if tag values match";
     - ustaw tag do dopasowania.
   - Problemy utworzone przez wyzwalacz pozycji logu będą miały tag wyzwalacza i będą zamykane indywidualnie.
7. Filtrowanie powiadomień:
   - Zdefiniuj tagi wyzwalaczy (na przykład `scope:security` dla trigger1 i `scope:availability` dla trigger2).
   - Użyj filtrowania tagów w warunkach akcji, aby otrzymywać powiadomienia tylko o zdarzeniach pasujących do danych tagów.
8. Identyfikowanie problemów w powiadomieniach:
   - Zdefiniuj tagi wyzwalaczy.
   - Użyj makra {EVENT.TAGS} w powiadomieniu o problemie.
   - Powiadomienie o problemie będzie zawierać tagi wyzwalacza, co ułatwi identyfikację, do której aplikacji/usługi należy powiadomienie.
9. Uproszczenie zadań konfiguracyjnych przez użycie tagów szablonu:
   - Zdefiniuj tag wyzwalacza szablonu.
   - Wyzwalacze utworzone z tego wyzwalacza szablonu będą miały jego tag.
10. Tworzenie wyzwalaczy z tagami z wykrywania niskiego poziomu (LLD):
    - Zdefiniuj tag prototypu wyzwalacza z makrem LLD w nazwie lub wartości tagu (na przykład `scope:{#FSNAME}`).
    - Wyzwalacze utworzone z prototypu wyzwalacza będą miały jego tag.
11. Dopasowywanie usług przy użyciu tagów usług:
    - Zdefiniuj tagi usług.
    - Skonfiguruj akcje usług dla usług z pasującymi tagami.

- Dodatkowo użyj tagów usług, aby powiązać usługę z SLA na potrzeby obliczeń SLA.

12. Łączenie usług z problemami przy użyciu tagów problemów usługi:
    - Zdefiniuj tag problemu w konfiguracji usługi (na przykład `target:mysql`).
    - Problemy z pasującym tagiem będą automatycznie korelowane z usługą, a stan usługi będzie się zmieniał zgodnie ze skonfigurowanymi regułami obliczania stanu usługi.
13. Tłumienie problemów, gdy host jest w trybie konserwacji:
    - Zdefiniuj tagi w konfiguracji okresu konserwacji.
    - Problemy ze zdefiniowanymi tagami będą tłumione.
14. Przyznawanie dostępu grupom użytkowników:
    - Zdefiniuj tagi w konfiguracji grupy użytkowników.
    - Użytkownicy w grupie użytkowników będą mogli wyświetlać tylko problemy ze zdefiniowanymi tagami.

Konfiguracja

Tagi można zdefiniować w dedykowanej karcie, na przykład w konfiguracji wyzwalacza:



Obsługa makr

Wbudowane i makra użytkownika w tagach są rozwijane w momencie wystąpienia zdarzenia. Do czasu wystąpienia zdarzenia makra te będą wyświetlane w Zabbix frontend jako nierozwinięte.

Makra niskopoziomowego wykrywania są rozwijane podczas procesu wykrywania.

Następujące makra mogą być używane w nazwach i wartościach tagów wyzwalacza:

- wbudowane makra {ITEM.VALUE}, {ITEM.VALUE.AGE}, {ITEM.VALUE.DATE}, {ITEM.VALUE.TIME}, {ITEM.VALUE.TIMESTAMP}, {ITEM.LASTVALUE}, {ITEM.LASTVALUE.AGE}, {ITEM.LASTVALUE.DATE}, {ITEM.LASTVALUE.TIME}, {ITEM.LASTVALUE.TIMESTAMP}, {HOST.HOST}, {HOST.NAME}, {HOST.CONN}, {HOST.DNS}, {HOST.IP}, {HOST.PORT} oraz {HOST.ID}
- wbudowane makra {INVENTORY.*} (do odwoływania się do wartości inwentarza hosta z jednego lub kilku hostów w wyrażeniu wyzwalacza)
- makra użytkownika oraz makra użytkownika z kontekstem (kontekst może zawierać makra niskopoziomowego wykrywania)
- makra niskopoziomowego wykrywania (tylko w tagach prototypu wyzwalacza)

Następujące makra mogą być używane w nazwach i wartościach tagów szablonu, hosta oraz pozycji/scenariusza WWW:

- wbudowane makra {HOST.HOST}, {HOST.NAME}, {HOST.CONN}, {HOST.DNS}, {HOST.IP}, {HOST.PORT} oraz {HOST.ID}
- wbudowane makra {INVENTORY.*}
- makra użytkownika
- makra niskopoziomowego wykrywania (tylko w tagach prototypu hosta i pozycji)

Następujące makra mogą być używane w powiadomieniach opartych na wyzwalaczach:

- wbudowane makra {EVENT.TAGS} oraz {EVENT.RECOVERY.TAGS} (te makra zostaną rozwinięte do listy tagów zdarzenia lub tagów zdarzenia odzyskania rozdzielonej przecinkami)
- wbudowane makra {EVENT.TAGSJSON} oraz {EVENT.RECOVERY.TAGSJSON} (te makra zostaną rozwinięte do tablicy JSON zawierającej obiekty tagów zdarzenia lub obiekty tagów zdarzenia odzyskania)

Wyodrębnianie podciągów w tagach wyzwalacza

Wyodrębnianie podciągów jest obsługiwane przy wypełnianiu nazwy lub wartości tagu z użyciem funkcji makra. Funkcja stosuje wyrażenie regularne do wartości uzyskanej z obsługiwanego makra. Na przykład:

```
{{ITEM.VALUE}.regsub(pattern, output)}
{{ITEM.VALUE}.iregsub(pattern, output)}

{{#LLDMACRO}.regsub(pattern, output)}
{{#LLDMACRO}.iregsub(pattern, output)}
```

Jeśli nazwa lub wartość tagu po rozwinięciu makra przekracza 255 znaków, zostanie obcięta do 255 znaków.

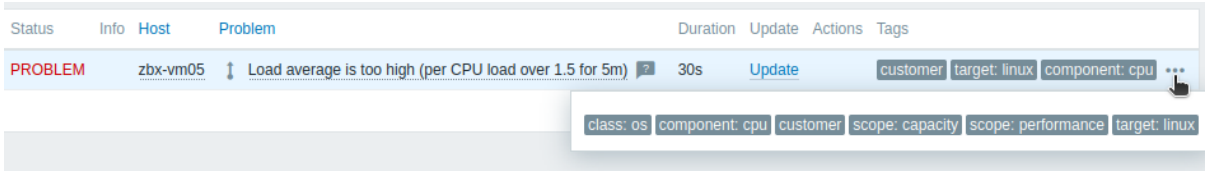
Zobacz także: Używanie funkcji makr w makrach low-level discovery do tagowania zdarzeń.

Wyświetlanie tagów zdarzeń

Tagi, jeśli są zdefiniowane, można wyświetlać przy nowych zdarzeniach w:

- *Monitoring* > *Problems*
- *Monitoring* > *Problems* > *Szczegóły zdarzenia*
- *Dashboards* > widżet *Problems*

Kolejność i liczba wyświetlanych tagów jest określana przez opcje filtrowania *Tag display priority* i *Show tags* w *Monitoring* > *Problems* lub w widżecie pulpitu *Problems*. Należy pamiętać, że można wyświetlić maksymalnie trzy tagi; jeśli tagów jest więcej, najechanie kursorem na trzy kropki powoduje wyświetlenie wszystkich tagów w wyskakującym oknie.



7 Wizualizacja

Użyj paska bocznego, aby uzyskać dostęp do treści w sekcji Wizualizacja.

1 Wykresy

Przegląd

Przy dużej ilości danych napływających do Zabbix użytkownikom znacznie łatwiej jest korzystać z wizualnej reprezentacji tego, co się dzieje, zamiast opierać się wyłącznie na liczbach.

W tym miejscu pojawiają się wykresy. Wykresy pozwalają na pierwszy rzut oka zrozumieć przepływ danych, powiązać problemy, ustalić, kiedy coś się zaczęło, lub przedstawić, kiedy coś może przerodzić się w problem.

Zabbix zapewnia użytkownikom:

- wbudowane proste wykresy dla danych jednej pozycji
- możliwość tworzenia bardziej złożonych niestandardowych wykresów
- szybki dostęp do porównania kilku pozycji w wykresach ad hoc
- nowoczesne, konfigurowalne wektorowe wykresy i wykresy kołowe

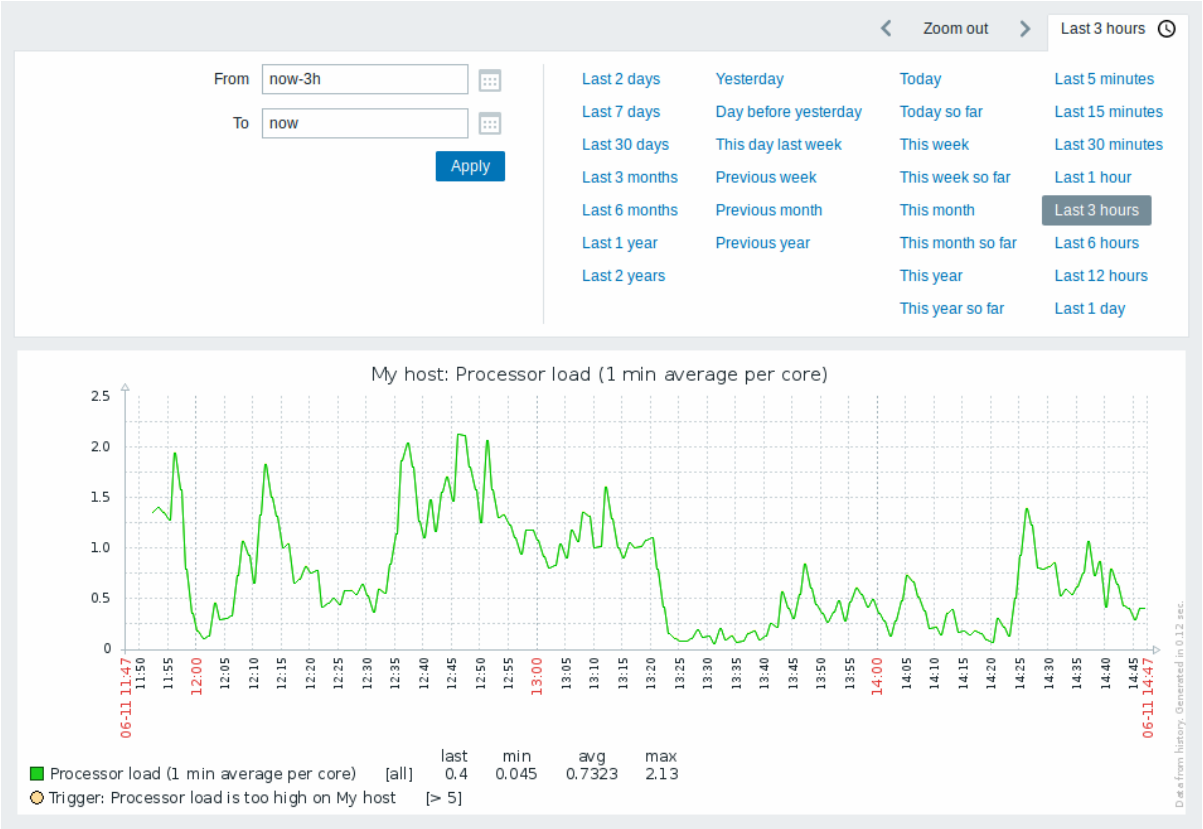
1 Proste wykresy

Przegląd

Proste wykresy służą do wizualizacji danych zbieranych przez pozycje.

Wyświetlanie prostych wykresów nie wymaga od użytkownika żadnej konfiguracji. Są one udostępniane przez Zabbix automatycznie.

Wystarczy przejść do *Monitoring* > *Latest data* i kliknąć link Graph dla odpowiedniej pozycji, a wykres zostanie wyświetlony.



Note:
Proste wykresy są dostępne dla wszystkich pozycji numerycznych. Dla pozycji tekstowych w *Monitoring* > *Latest data* dostępny jest link do historii.

Selektor okresu czasu

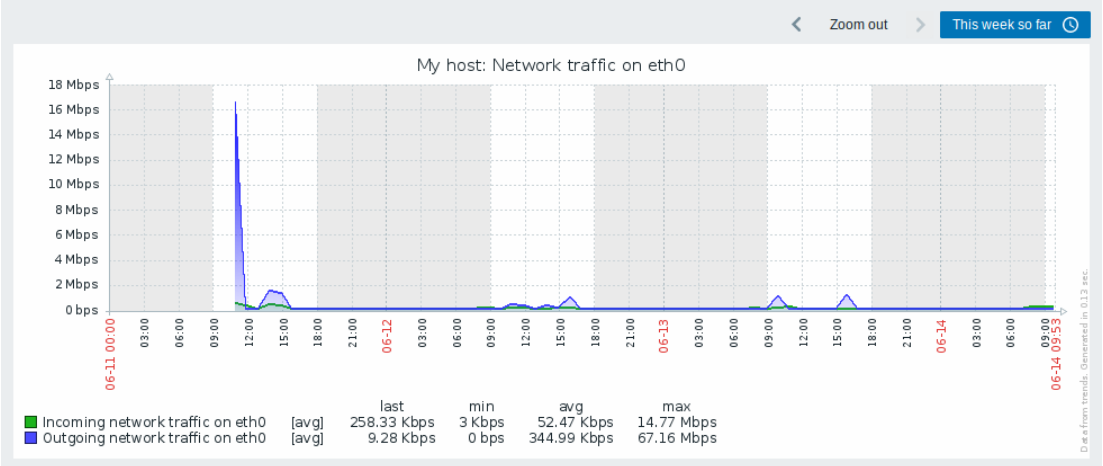
Selektor okresu czasu nad wykresem umożliwia wybór często wymaganych okresów jednym kliknięciem myszy. Więcej informacji można znaleźć w sekcji Selektory okresu czasu i hosta.

Ostatnie dane a dłuższe okresy

Dla bardzo świeżych danych rysowana jest **pojedyncza** linia łącząca każdą otrzymaną wartość. Pojedyncza linia jest rysowana tak długo, jak długo dostępny jest co najmniej jeden poziomy piksel dla jednej wartości.

Dla danych obejmujących dłuższy okres rysowane są **trzy linie** — ciemnozielona pokazuje średnią, natomiast jasnoróżowa i jasnozielona pokazują wartości maksymalne i minimalne w danym momencie. Przestrzeń między wartościami najwyższymi i najniższymi jest wypełniona żółtym tłem.

Czas pracy (dni robocze) jest wyświetlany na wykresach jako białe tło, natomiast czas poza godzinami pracy jest wyświetlany na szaro (w domyślnym motywie frontend *Original blue*).

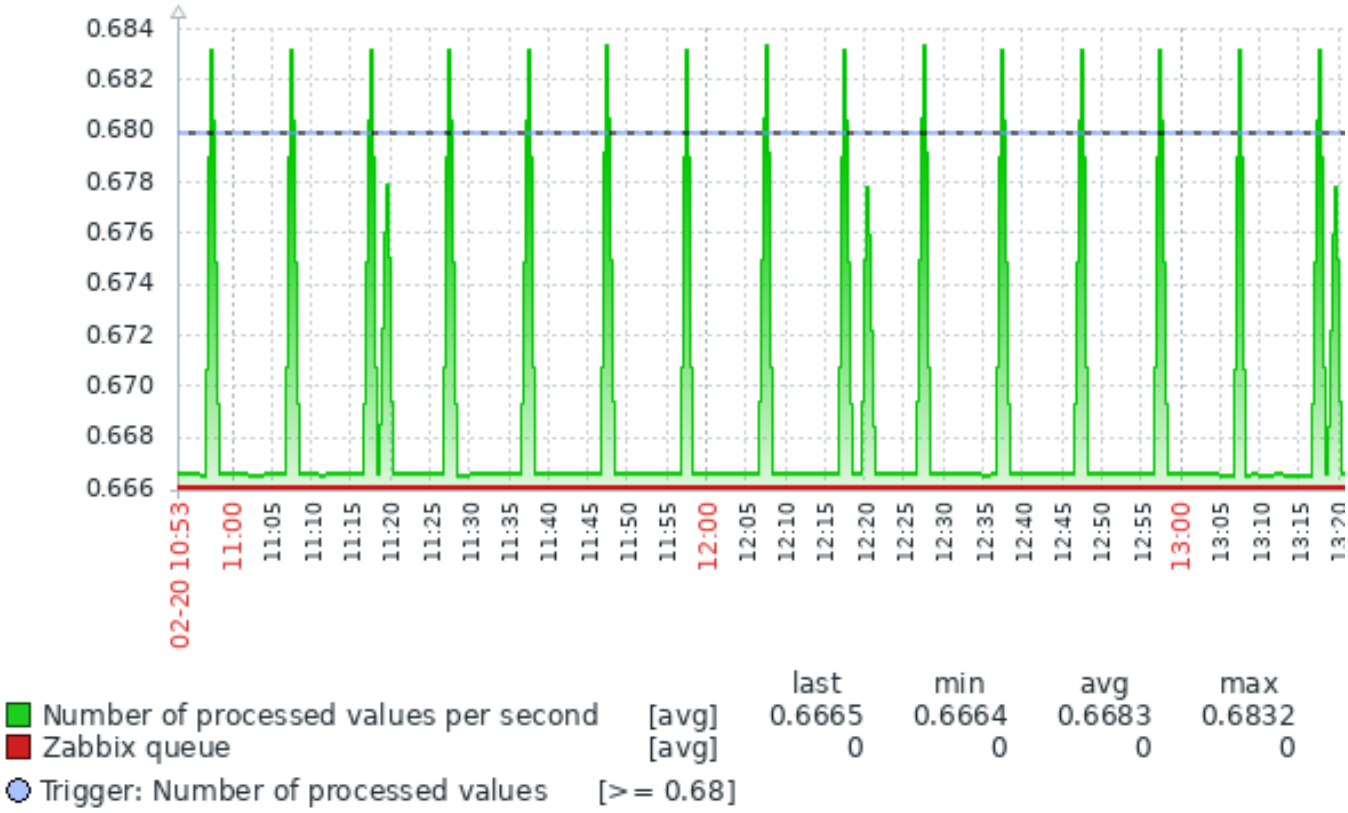


Czas pracy jest zawsze wyświetlany na wykresach prostych, natomiast jego wyświetlanie na wykresach niestandardowych zależy od preferencji użytkownika.

Czas pracy nie jest wyświetlany, jeśli wykres pokazuje okres dłuższy niż 3 miesiące.

Linie wyzwalaczy

Proste wyzwalacze są wyświetlane jako linie z czarnymi kreskami nałożonymi na kolor ważności wyzwalacza — zwróć uwagę na niebieską linię na wykresie oraz informacje o wyzwalaczu wyświetlane w legendzie. Na wykresie mogą być wyświetlane maksymalnie 3 linie wyzwalaczy; jeśli wyzwalaczy jest więcej, priorytet mają wyzwalacze o niższej ważności. Wyzwalacze są zawsze wyświetlane na prostych wykresach, natomiast ich wyświetlanie na wykresach niestandardowych zależy od preferencji użytkownika.



Generowanie z historii/trendów

Wykresy mogą być rysowane na podstawie historii lub trendów pozycji.

Dla użytkowników, którzy mają włączony tryb debugowania frontendu, w prawym dolnym rogu wykresu wyświetlany jest szary, pionowy podpis wskazujący, skąd pochodzą dane.

Na to, czy używana jest historia, czy trendy, wpływa kilka czynników:

- okres przechowywania historii pozycji. Na przykład historia pozycji może być przechowywana przez 14 dni. W takim przypadku wszelkie dane starsze niż czternaście dni będą pochodzić z trendów.
- zagęszczenie danych na wykresie. Jeśli liczba sekund przypadających na poziomy piksel wykresu przekracza 3600/16, wyświetlane są dane trendów (nawet jeśli historia pozycji jest nadal dostępna dla tego samego okresu).
- jeśli trendy są wyłączone, do budowania wykresu używana jest historia pozycji — jeśli jest dostępna dla tego okresu.

Brak danych

W przypadku pozycji z regularnym interwałem aktualizacji na wykresie nic nie jest wyświetlane, jeśli dane pozycji nie są zbierane.

Jednak w przypadku pozycji trapper oraz pozycji z harmonogramowanym interwałem aktualizacji (i regularnym interwałem aktualizacji ustawionym na 0) rysowana jest prosta linia prowadząca do pierwszej zebranej wartości oraz od ostatniej zebranej wartości do końca wykresu; linia znajduje się odpowiednio na poziomie pierwszej/ostatniej wartości.

Przełączanie na surowe wartości

Lista rozwijana w prawym górnym rogu umożliwia przełączenie z prostego wykresu na listy *Wartości/500 najnowszych wartości*. Może to być przydatne do wyświetlania wartości liczbowych składających się na wykres.

Przedstawione tutaj wartości są surowe, tj. nie są używane żadne jednostki ani przetwarzanie końcowe wartości. Mapowanie wartości jest jednak stosowane.

Znane problemy

Zobacz znane problemy dotyczące wykresów.

2 Własne wykresy

Przegląd

Niestandardowe wykresy, jak sama nazwa wskazuje, oferują możliwości dostosowywania.

Podczas gdy proste wykresy dobrze nadają się do wyświetlania danych pojedynczej pozycji, nie oferują możliwości konfiguracji.

Dlatego jeśli chcesz zmienić styl wykresu lub sposób wyświetlania linii albo porównać kilka pozycji, na przykład ruch przychodzący i wychodzący na jednym wykresie, potrzebujesz niestandardowego wykresu.

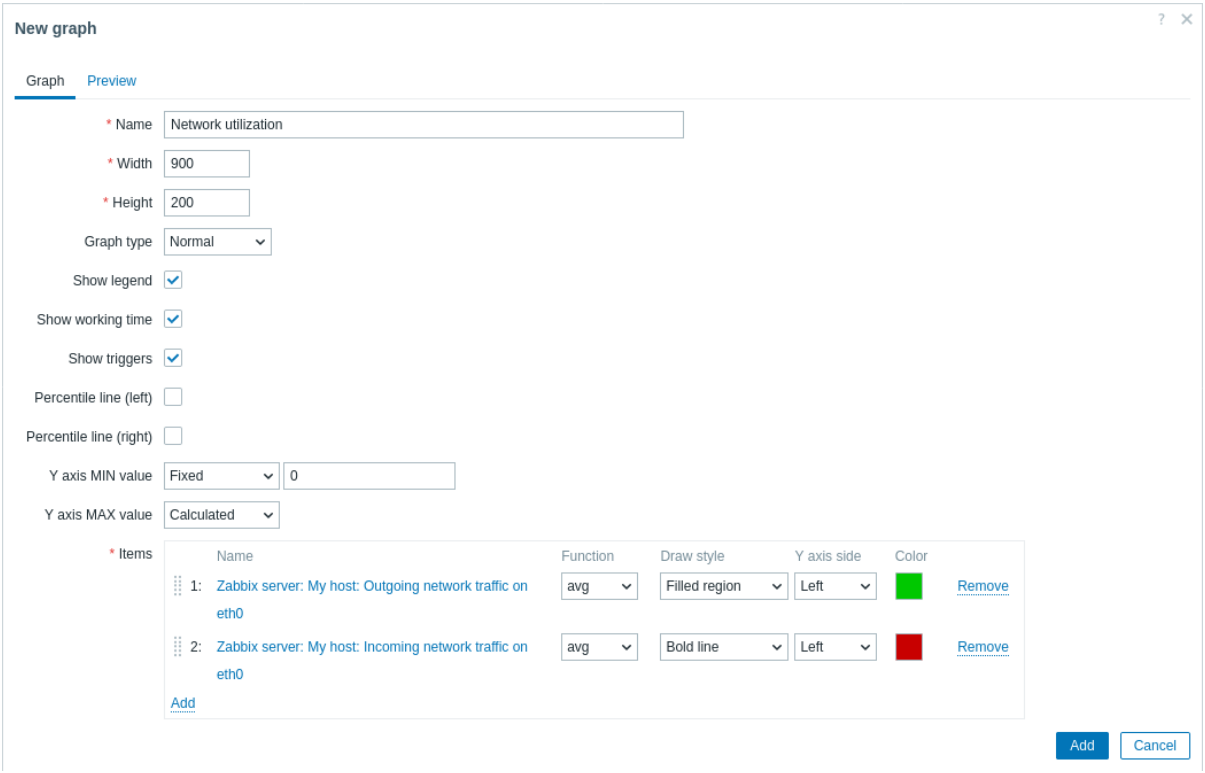
Niestandardowe wykresy są konfigurowane ręcznie.

Można je tworzyć dla jednego hosta lub kilku hostów albo dla pojedynczego szablonu.

Konfigurowanie własnych wykresów

Aby utworzyć własny wykres, wykonaj następujące czynności:

- Przejdź do *Data collection* > *Hosts (lub Templates)*
- Kliknij *Graphs* w wierszu obok wybranego hosta lub szablonu
- Na ekranie Graphs kliknij *Create graph*
- Edytuj atrybuty wykresu



Wszystkie obowiązkowe pola wejściowe są oznaczone czerwoną gwiazdką.

Atrybuty wykresu:

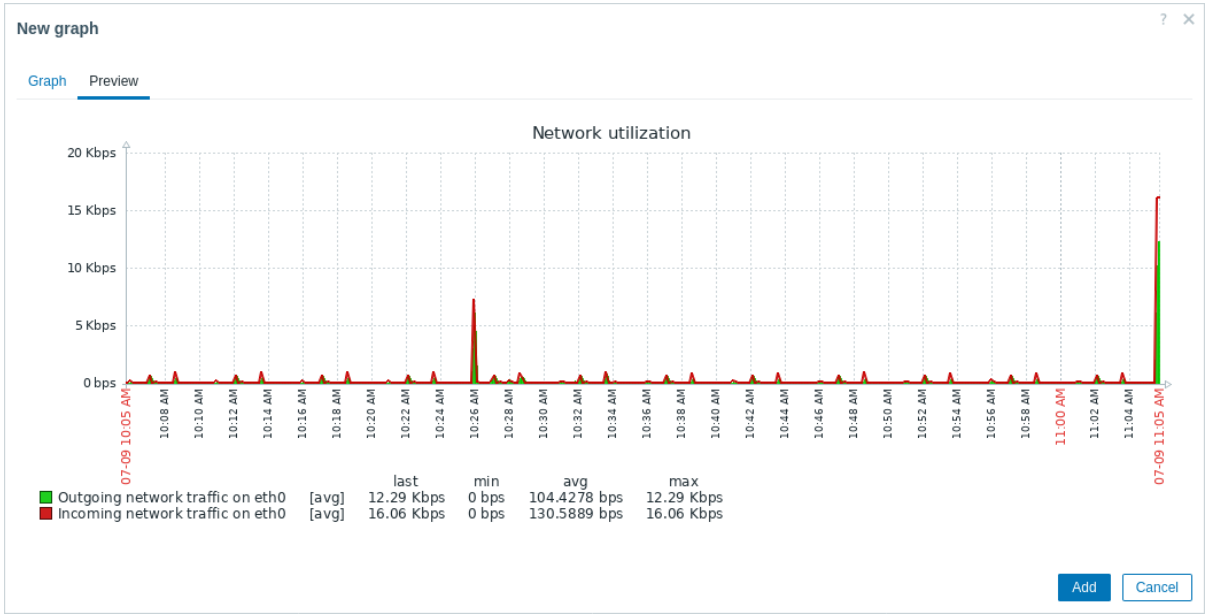
Parameter	Description
Name	Unikalna nazwa wykresu. W tym polu obsługiwane są wyrażenia makr, ale tylko z funkcjami `avg`, `last`, `min` i `max`, z czasem jako parametrem (na przykład `{?avg(/host/key,1h)}`). Makra {HOST.HOST<1-9>} są obsługiwane do użycia wewnątrz tego makra, odwołując się do pierwszego, drugiego, trzeciego itd. hosta na wykresie, na przykład `{?avg(/{HOST.HOST2}/key,1h)}`. Zwróć uwagę, że odwoływanie się do pierwszego hosta za pomocą tego makra jest zbędne, ponieważ do pierwszego hosta można odwołać się niejawnie, na przykład `{?avg(//key,1h)}`.
Width	Szerokość wykresu w pikselach (tylko dla podglądu oraz wykresów kołowych/rozsuniętych).
Height	Wysokość wykresu w pikselach.

Parameter	Description
Graph type	Typ wykresu: **Normal** - zwykły wykres, wartości wyświetlane jako linie **Stacked** - wykres skumulowany, wyświetlane są wypełnione obszary **Pie** - wykres kołowy **Exploded** - „rozsunięty” wykres kołowy, segmenty są wyświetlane jako „wycięte” z koła
Show legend	Zaznaczenie tego pola spowoduje wyświetlenie legendy wykresu.
Show working time	Jeśli wybrane, godziny poza czasem pracy będą pokazane z szarym tłem. Ten parametr nie jest dostępny dla wykresów kołowych i rozsuniętych wykresów kołowych.
Show triggers	Jeśli wybrane, proste wyzwalacze będą wyświetlane jako linie z czarnymi kreskami na kolorze ważności wyzwalacza. Ten parametr nie jest dostępny dla wykresów kołowych i rozsuniętych wykresów kołowych.
Percentile line (left)	Wyświetla percentyl dla lewej osi Y. Jeśli na przykład ustawiony jest percentyl 95%, linia percentyla będzie na poziomie, poniżej którego znajduje się 95 procent wartości. Wyświetlana jako jasna zielona linia. Dostępne tylko dla zwykłych wykresów.
Percentile line (right)	Wyświetla percentyl dla prawej osi Y. Jeśli na przykład ustawiony jest percentyl 95%, linia percentyla będzie na poziomie, poniżej którego znajduje się 95 procent wartości. Wyświetlana jako jasna czerwona linia. Dostępne tylko dla zwykłych wykresów.
Y axis MIN value	Minimalna wartość osi Y: **Calculated** - minimalna wartość osi Y zostanie obliczona automatycznie. **Fixed** - stała minimalna wartość osi Y. **Item** - ostatnia wartość wybranej pozycji będzie wartością minimalną. Ten parametr nie jest dostępny dla wykresów kołowych i rozsuniętych wykresów kołowych.
Y axis MAX value	Maksymalna wartość osi Y: **Calculated** - maksymalna wartość osi Y zostanie obliczona automatycznie. **Fixed** - stała maksymalna wartość osi Y. **Item** - ostatnia wartość wybranej pozycji będzie wartością maksymalną Ten parametr nie jest dostępny dla wykresów kołowych i rozsuniętych wykresów kołowych.
3D view	Włącza styl 3D. Tylko dla wykresów kołowych i rozsuniętych wykresów kołowych.
Items	Pozycje, których dane mają być wyświetlane na tym wykresie. Kliknij *Add*, aby wybrać pozycje. Możesz także wybrać różne opcje wyświetlania (funkcja, styl rysowania, wyświetlanie lewej/prawej osi, kolor).
Sort order (0→100)	Kolejność rysowania. 0 będzie przetwarzane jako pierwsze. Może być użyte do rysowania linii lub obszarów za (lub przed) innymi. Możesz przeciągać i upuszczać pozycje za pomocą ikony na początku wiersza, aby ustawić kolejność sortowania lub określić, która pozycja jest wyświetlana przed inną.
Name	Nazwa wybranej pozycji jest wyświetlana jako link. Kliknięcie linku otwiera listę innych dostępnych pozycji.
Type	Typ (dostępny tylko dla wykresów kołowych i rozsuniętych wykresów kołowych): **Simple** - wartość pozycji jest reprezentowana proporcjonalnie na wykresie kołowym **Graph sum** - wartość pozycji reprezentuje cały wykres kołowy Zwróć uwagę, że kolor pozycji „graph sum” będzie widoczny tylko w takim zakresie, w jakim nie jest zajęty przez pozycje „proportional”.
Function	Wybierz, jakie wartości będą wyświetlane, gdy dla pozycji istnieje więcej niż jedna wartość na pionowy piksel wykresu: **all** - wyświetla wszystkie możliwe wartości (minimalną, maksymalną, średnią) na wykresie. Zwróć uwagę, że dla krótszych okresów to ustawienie nie ma wpływu; dopiero dla dłuższych okresów, gdy zagęszczenie danych w pionowym pikselu wykresu wzrasta, funkcja „all” zaczyna wyświetlać wartości minimalne, maksymalne i średnie. Ta funkcja jest dostępna tylko dla typu wykresu *Normal*. Zobacz także: Generowanie wykresów z historii/trendów. **avg** - wyświetla wartości średnie **last** - wyświetla najnowsze wartości. Ta funkcja jest dostępna tylko wtedy, gdy jako typ wykresu wybrano *Pie/Exploded pie*. **max** - wyświetla wartości maksymalne **min** - wyświetla wartości minimalne

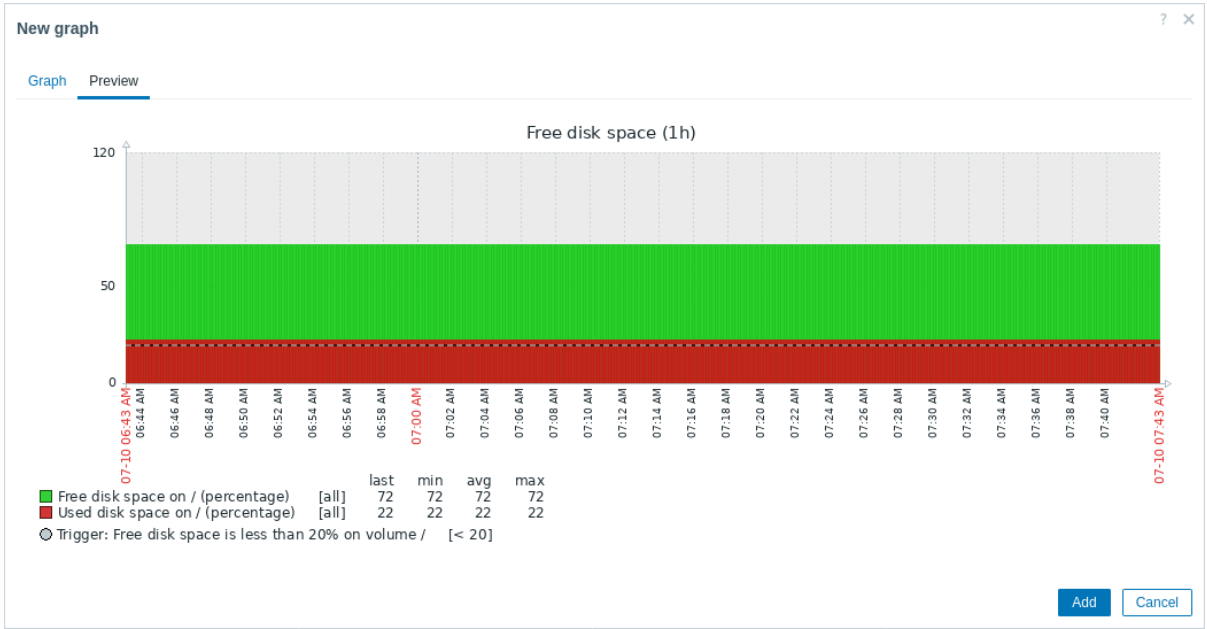
Parameter	Description
Draw style	Wybierz styl rysowania (dostępny tylko dla zwykłych wykresów; dla wykresów skumulowanych zawsze używany jest wypełniony obszar), który ma zostać zastosowany do danych pozycji - *Line*, *Bold line*, *Filled region*, *Dot*, *Dashed line*, *Gradient line*.
Y axis side	Wybierz stronę osi Y, po której mają być wyświetlane dane pozycji - *Left*, *Right*.
Color	Wybierz kolor, który ma zostać zastosowany do danych pozycji.

Podgląd wykresu

Na karcie *Podgląd* wyświetlany jest podgląd wykresu, dzięki czemu możesz od razu zobaczyć, co tworzysz.



Pamiętaj, że podgląd nie będzie wyświetlał żadnych danych dla pozycji szablonu.



W tym przykładzie zwróć uwagę na pogrubioną linię przerywaną przedstawiającą poziom wyzwalacza oraz informacje o wyzwalaczu wyświetlane w legendzie.

Note:
Można wyświetlić nie więcej niż 3 linie wyzwalaczy. Jeśli wyzwalaczy jest więcej, do wyświetlenia priorytetowo wybierane są wyzwalacze o niższym poziomie ważności.

 Jeśli wysokość wykresu jest ustawiona na mniej niż 120 pikseli, w legendzie nie będzie wyświetlany żaden wyzwalacz.

3 Wykresy ad hoc

Przegląd

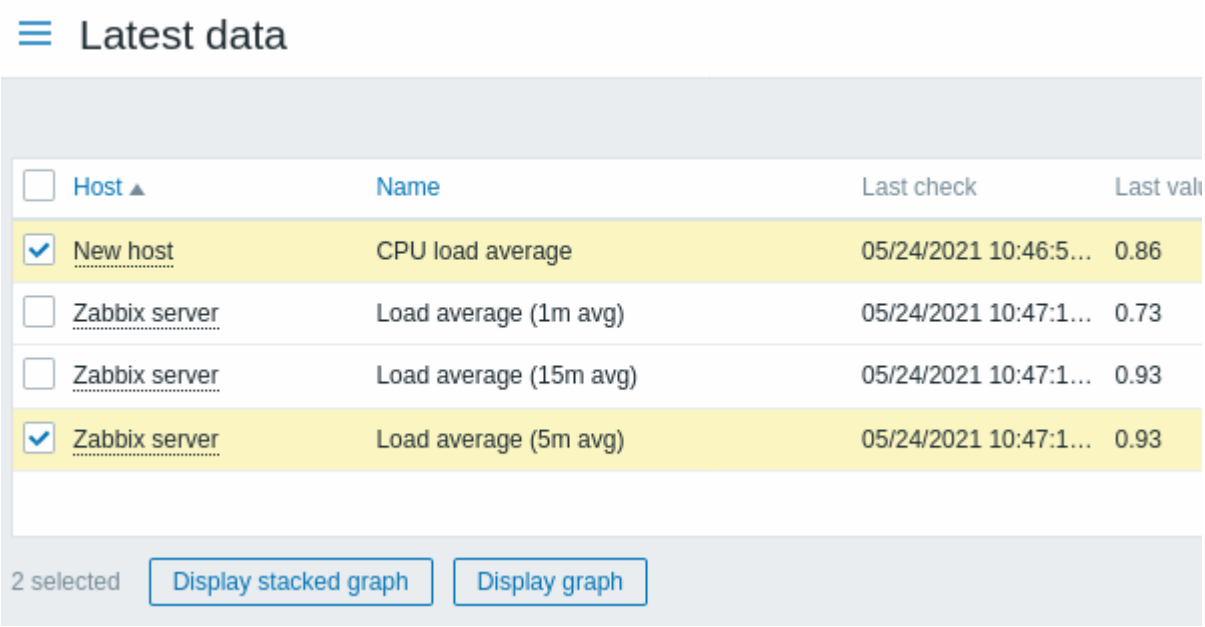
Podczas gdy prosty wykres świetnie nadaje się do uzyskiwania dostępu do danych jednej pozycji, a wykresy niestandardowe oferują opcje dostosowywania, żaden z tych dwóch nie pozwala szybko utworzyć wykresu porównawczego dla wielu pozycji przy niewielkim nakładzie pracy i bez konieczności utrzymania.

Aby rozwiązać ten problem, można w bardzo szybki sposób tworzyć doraźne wykresy dla kilku pozycji.

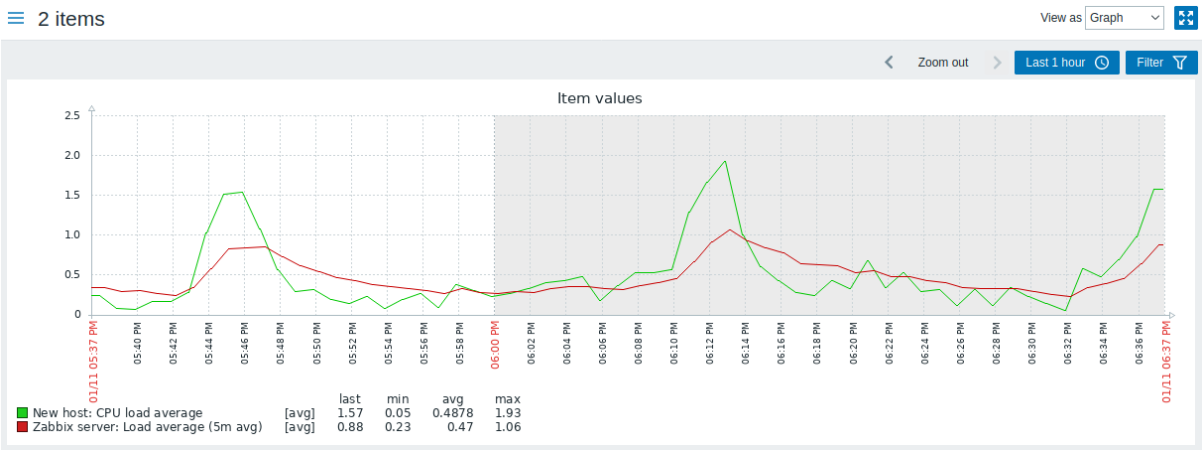
Konfiguracja

Aby utworzyć wykres ad hoc, wykonaj następujące czynności:

- Przejdź do *Monitoring* → *Latest data*
- Użyj filtra, aby wyświetlić pozycje, które chcesz uwzględnić
- Zaznacz pola wyboru przy pozycjach, które chcesz przedstawić na wykresie
- Kliknij przycisk *Display stacked graph* lub *Display graph*

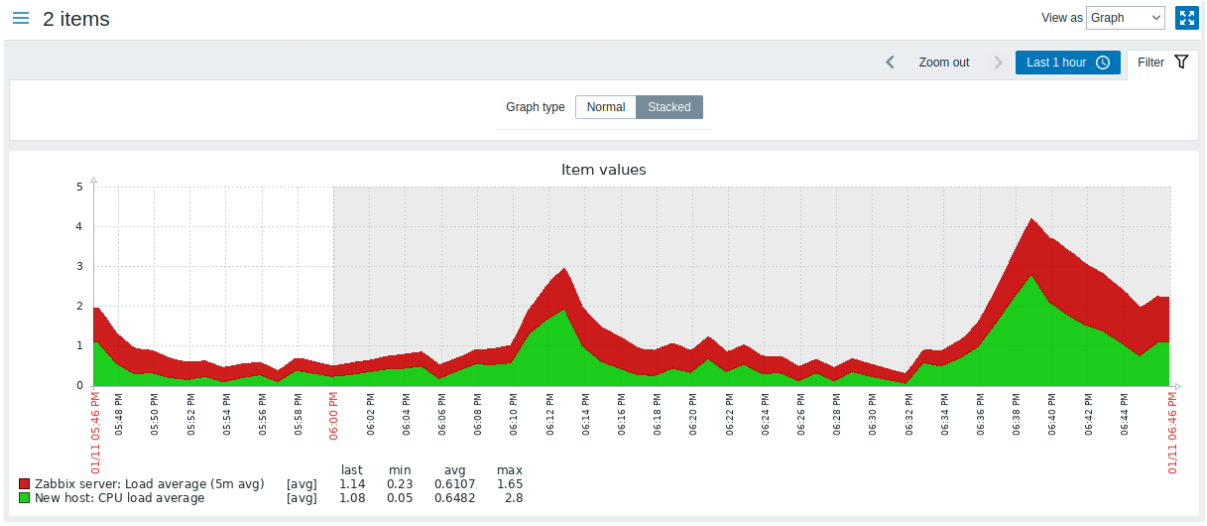


Wykres zostanie utworzony natychmiast:



Należy pamiętać, że aby uniknąć wyświetlania zbyt wielu linii na wykresie, dla każdej pozycji wyświetlana jest tylko wartość średnia (linie wartości minimalnej/maksymalnej nie są wyświetlane). Wyzwalacze i informacje o wyzwalaczach nie są wyświetlane na wykresie.

W oknie utworzonego wykresu dostępny jest selektor przedziału czasu oraz możliwość przełączania z „normalnego" wykresu liniowego na skumulowany (i z powrotem).



4 Agregacja na wykresach

Przegląd

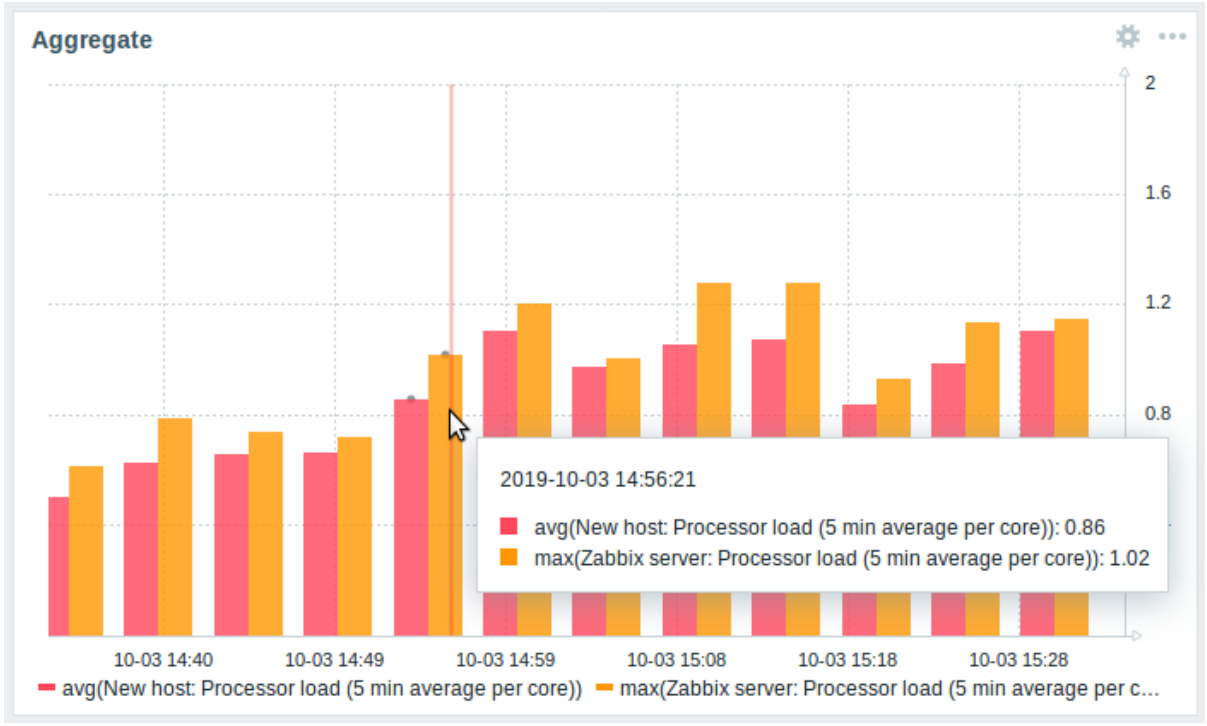
Funkcje agregacji, dostępne w widgetach wykresu i wykresu kołowego na pulpicie, umożliwiają wyświetlanie zagregowanej wartości dla wybranego przedziału (5 minut, godzina, dzień) zamiast wszystkich wartości.

Ta sekcja zawiera więcej szczegółów na temat opcji agregacji w widżecie wykresu.

Dostępne są następujące opcje agregacji:

- min
- max
- avg
- count
- sum
- first (pierwsza wyświetlana wartość)
- last (ostatnia wyświetlana wartość)

Najbardziej interesującym zastosowaniem agregacji danych jest możliwość tworzenia czytelnych porównań danych dla określonego okresu, wyświetlanych obok siebie:

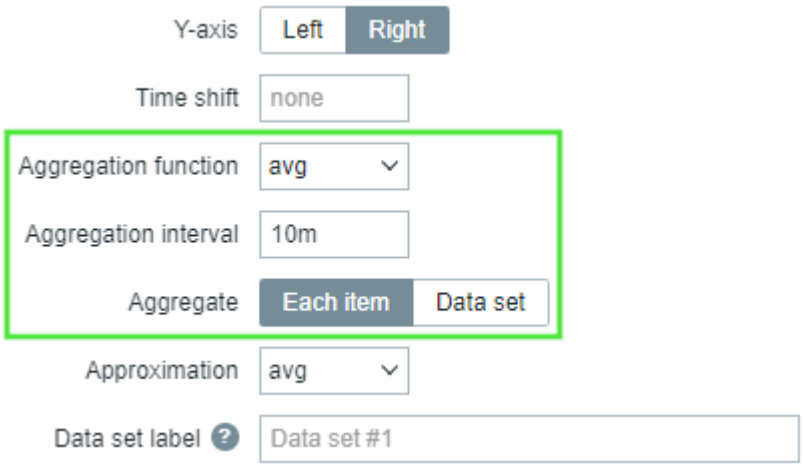


Po najechaniu kursorem na punkt w czasie na wykresie, oprócz pozycji i ich zagregowanych wartości wyświetlane są także data i godzina. Pozycje są wyświetlane w nawiasach, z prefiksem funkcji agregacji, która została użyta. Jeśli w widżecie wykresu

skonfigurowano *Data set label*, etykieta jest wyświetlana w nawiasach, z prefiksem użytej funkcji agregacji. Należy pamiętać, że jest to data i godzina punktu na wykresie, a nie rzeczywistych wartości.

Konfiguracja

Opcje agregacji są dostępne w ustawieniach zestawu danych podczas konfigurowania widżetu wykresu.



Możesz wybrać funkcję agregacji i przedział czasu. Ponieważ zestaw danych może obejmować kilka pozycji, dostępna jest również dodatkowa opcja umożliwiająca wyświetlanie zagregowanych danych dla każdej pozycji osobno lub dla wszystkich pozycji zestawu danych jako jednej zagregowanej wartości.

Przypadki użycia

Średnia liczba żądań do serwera Nginx

Wyświetl średnią liczbę żądań na sekundę dziennie dla serwera Nginx:

- dodaj pozycję liczby żądań na sekundę do zestawu danych
- wybierz funkcję agregującą `avg` i określ przedział `1d`
- zostanie wyświetlony wykres słupkowy, gdzie każdy słupek reprezentuje średnią liczbę żądań na sekundę w danym dniu

Minimalna tygodniowa ilość wolnego miejsca na dysku wśród klastrów

Wyświetl najniższą ilość wolnego miejsca na dysku wśród klastrów w ciągu tygodnia.

- dodaj do zestawu danych: hosty `cluster*`, klucz "Wolne miejsce na dysku na /data"
- wybierz funkcję agregującą `min` i określ przedział `1w`
- zostanie wyświetlony wykres słupkowy, na którym każdy słupek przedstawia minimalną ilość wolnego miejsca na dysku w tygodniu dla każdego woluminu /data w klastrze

2 Mapy sieciowe

Przegląd

Jeśli zarządzasz siecią, możesz chcieć mieć gdzieś ogólny widok swojej infrastruktury. W tym celu możesz tworzyć mapy w Zabbix — sieci oraz czegokolwiek zechcesz.

Wszyscy użytkownicy mogą tworzyć mapy sieci. Mapy mogą być publiczne (dostępne dla wszystkich użytkowników) lub prywatne (dostępne dla wybranych użytkowników).

Przejdź do konfigurowania mapy sieci.

1 Konfigurowanie mapy sieciowej

Przegląd

Konfigurowanie mapy w Zabbix wymaga najpierw utworzenia mapy przez zdefiniowanie jej ogólnych parametrów, a następnie rozpoczęcia wypełniania właściwej mapy elementami i ich połączeniami.

Mapę można wypełnić elementami, takimi jak host, grupa hostów, wyzwalacz, obraz lub inna mapa.

Ikony są używane do reprezentowania elementów mapy. Można zdefiniować informacje, które będą wyświetlane wraz z ikonami, a także ustawić specjalny sposób wyświetlania ostatnich problemów. Można łączyć ikony i definiować informacje wyświetlane na połączeniach.

Do ikon można dodać niestandardowe adresy URL dostępne po kliknięciu. Dzięki temu można powiązać ikonę hosta z właściwościami hosta lub ikonę mapy z inną mapą.

Liczba problemów na mapach jest wyświetlana tylko dla problemów przyczynowych.

Mapami zarządza się w *Monitoring* > *Maps*, gdzie można je konfigurować, zarządzać nimi i je przeglądać. W widoku monitorowania można klikać ikony i korzystać z odnośników do niektórych skryptów i adresów URL.

Mapy sieciowe są oparte na grafice wektorowej (SVG).

Mapy publiczne i prywatne

Wszyscy użytkownicy Zabbix (w tym użytkownicy niebędący administratorami) mogą tworzyć mapy sieci. Mapy mają właściciela — użytkownika, który je utworzył. Mapy mogą być publiczne lub prywatne.

- Mapy *publiczne* są widoczne dla wszystkich użytkowników, jednak aby je zobaczyć, użytkownik musi mieć uprawnienia do odczytu co najmniej jednego elementu mapy. Mapy publiczne mogą być edytowane, jeśli użytkownik/grupa użytkowników ma uprawnienia do odczytu i zapisu do tej mapy oraz co najmniej uprawnienia do odczytu do wszystkich elementów odpowiedniej mapy, w tym wyzwalaczy w połączeniach.
- Mapy *prywatne* są widoczne tylko dla ich właściciela oraz użytkowników/grup użytkowników, którym mapa została udostępniona przez właściciela. Zwykli użytkownicy (niebędący Super adminami) mogą udostępniać mapy tylko grupom, do których należą, oraz użytkownikom należącym do tych grup. Użytkownicy na poziomie Admin mogą widzieć mapy prywatne niezależnie od tego, czy są ich właścicielami, czy należą do listy użytkowników, którym mapa została udostępniona. Mapy prywatne mogą być edytowane przez właściciela mapy oraz wtedy, gdy użytkownik/grupa użytkowników ma uprawnienia do odczytu i zapisu do tej mapy oraz co najmniej uprawnienia do odczytu do wszystkich elementów odpowiedniej mapy, w tym wyzwalaczy w połączeniach.

Elementy mapy, do których użytkownik nie ma uprawnień odczytu, są wyświetlane z wyszarzoną ikoną, a wszystkie informacje tekstowe o elemencie są ukryte. Jednak etykieta wyzwalacza jest widoczna, nawet jeśli użytkownik nie ma uprawnień do wyzwalacza.

Aby dodać element do mapy, użytkownik musi również mieć co najmniej uprawnienia do odczytu tego elementu.

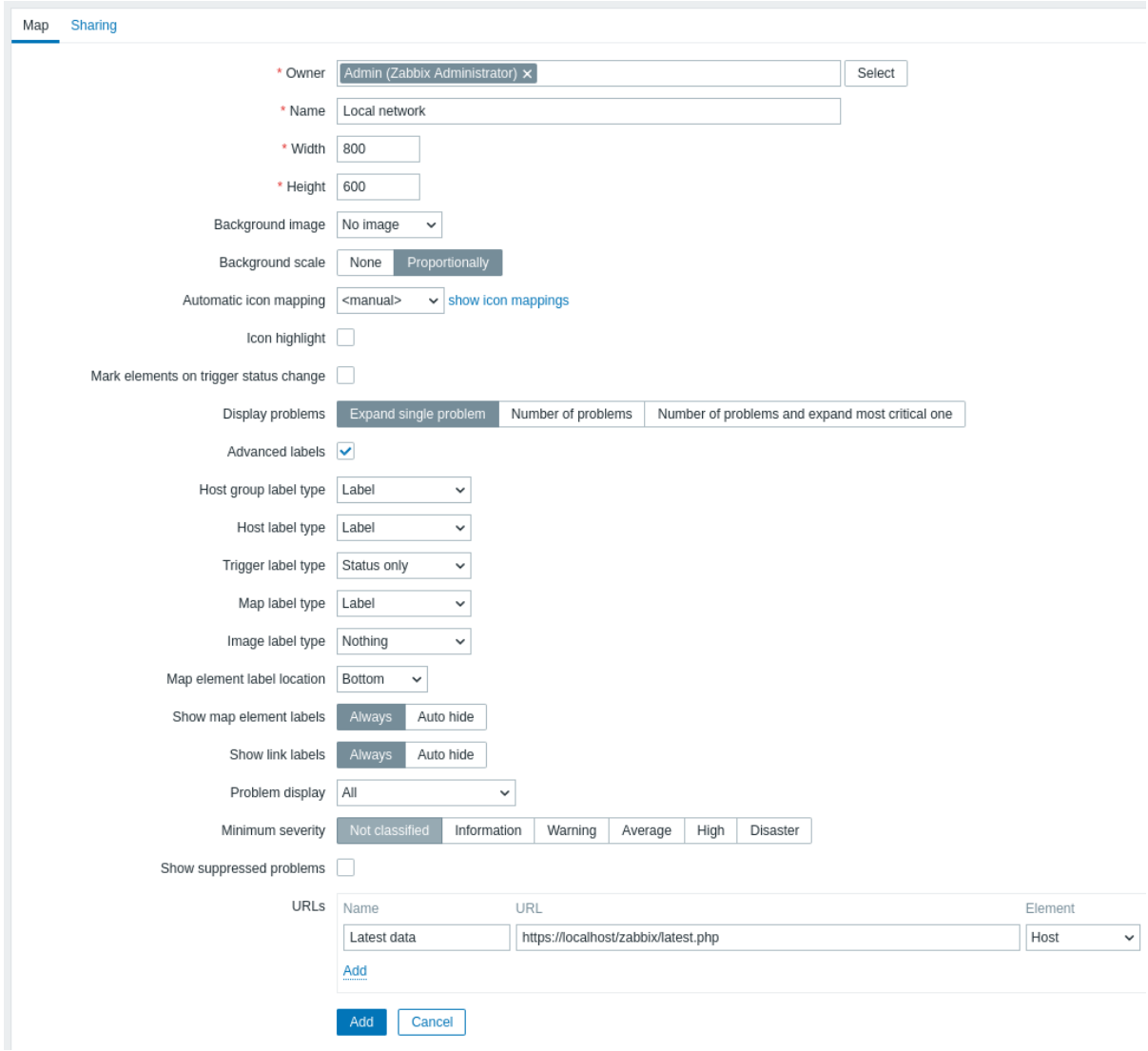
Tworzenie mapy

Aby utworzyć mapę, wykonaj następujące czynności:

1. Przejdź do *Monitoring* > *Maps*.
2. Przejdź do widoku ze wszystkimi mapami.
3. Kliknij *Create map*.

Możesz także użyć przycisku *Clone* w formularzu konfiguracji istniejącej mapy, aby utworzyć nową mapę. Ta mapa będzie miała wszystkie właściwości istniejącej mapy, w tym ogólne atrybuty układu, a także elementy istniejącej mapy.

Karta **Map** zawiera ogólne atrybuty mapy:



Wszystkie wymagane pola wejściowe są oznaczone czerwoną gwiazdką.

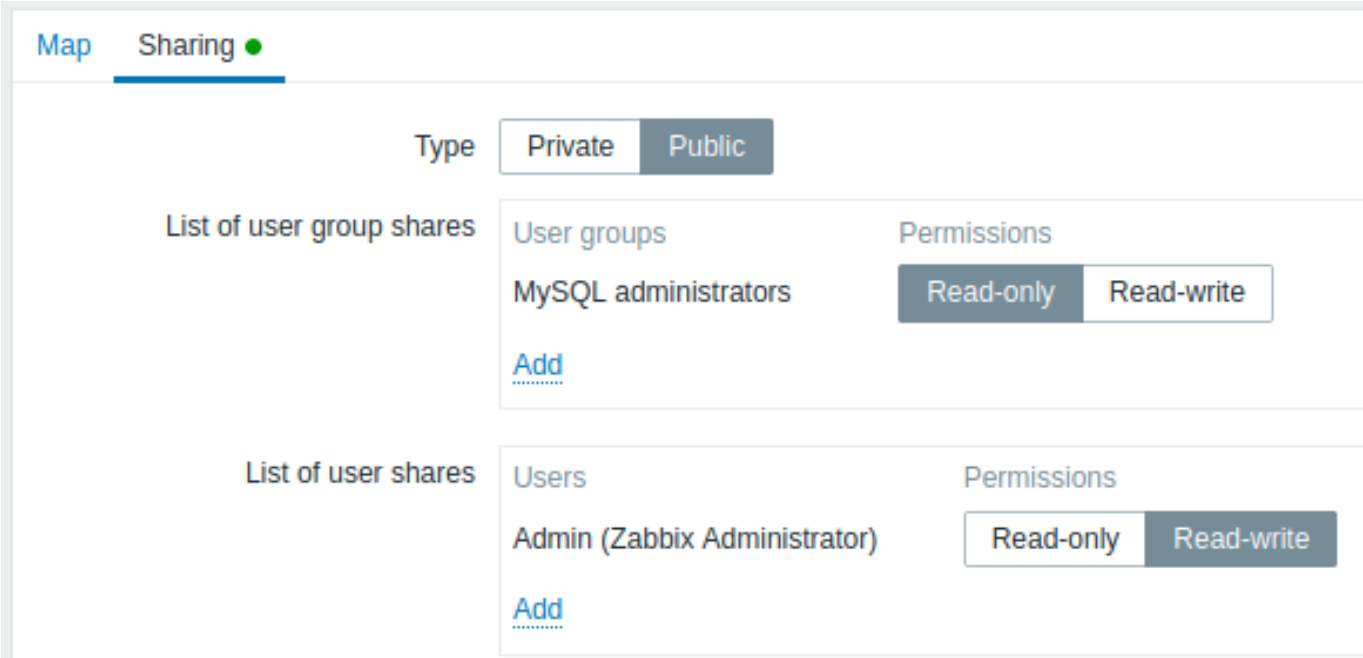
Ogólne atrybuty mapy:

Parameter	Description
Owner	Nazwa właściciela mapy.
Name	Unikalna nazwa mapy.
Width	Szerokość mapy w pikselach.
Height	Wysokość mapy w pikselach.
Background image	Użyj obrazu tła: **No image** - brak obrazu tła (białe tło) **Image** - wybrany obraz używany jako obraz tła. Możesz użyć mapy geograficznej lub dowolnego innego obrazu, aby ulepszyć swoją mapę.
Background scale	Użyj skalowania tła: **None** - bez skalowania; **Proportionally** - wypełnij całe tło mapy, ale zachowaj proporcje obrazu (domyślnie).
Automatic icon mapping	Możesz ustawić użycie automatycznego mapowania ikon, skonfigurowanego w *Administration > General > Icon mapping*. Mapowanie ikon umożliwia przypisanie określonych ikon do określonych pól inwentarza hosta.
Icon highlight	Jeśli zaznaczysz to pole wyboru, elementy mapy będą podświetlane. Elementy z aktywnym wyzwalaczem otrzymają okrągłe tło w tym samym kolorze co wyzwalacz o najwyższym poziomie ważności. Ponadto wokół okręgu zostanie wyświetlona gruba zielona linia, jeśli wszystkie problemy zostały potwierdzone. Elementy ze stanem „disabled” lub „in maintenance” otrzymają odpowiednio kwadratowe tło w kolorze szarym i pomarańczowym. Zobacz także: Viewing maps

Parameter	Description
Mark elements on trigger status change	Niedawna zmiana stanu wyzwalacza (niedawny problem lub rozwiązanie) będzie wyróżniona znacznikami (czerwone trójkąty skierowane do wewnątrz) po trzech stronach ikony elementu, które są wolne od etykiety. Znaczniki są wyświetlane przez 30 minut.
Display problems	Wybierz sposób wyświetlania problemów przy elemencie mapy: **Expand single problem** - jeśli istnieje tylko jeden problem, wyświetlana jest nazwa problemu. W przeciwnym razie wyświetlana jest łączna liczba problemów. **Number of problems** - wyświetlana jest łączna liczba problemów **Number of problems and expand most critical one** - wyświetlana jest nazwa problemu o najwyższym poziomie krytyczności oraz łączna liczba problemów. „Najbardziej krytyczny" jest określany na podstawie ważności problemu, a w przypadku równości na podstawie ID zdarzenia problemu (wyższe ID lub późniejszy problem jest wyświetlany jako pierwszy). Dla *trigger map element* jest to określane na podstawie ważności problemu, a w przypadku równości na podstawie pozycji wyzwalacza na liście wyzwalaczy. W przypadku wielu problemów tego samego wyzwalacza zostanie wyświetlony najnowszy.
Advanced labels	Jeśli zaznaczysz to pole wyboru, będziesz mógł zdefiniować oddzielne typy etykiet dla oddzielnych typów elementów.
Host group label type	Typ etykiety używany dla elementu mapy: **Label** - etykieta elementu mapy **IP address** - adres IP **Element name** - nazwa elementu (na przykład nazwa hosta) **Status only** - tylko stan (OK lub PROBLEM) **Nothing** - etykiety nie są wyświetlane
Host label type *Trigger label type* *Map label type* *Image label type*	
Map element label location	Położenie etykiety względem elementu mapy: **Bottom** - pod elementem mapy **Left** - po lewej stronie **Right** - po prawej stronie **Top** - nad elementem mapy
Show map element labels	Wybierz sposób wyświetlania etykiet elementów mapy: **Always** - zawsze wyświetlane (domyślnie); **Auto hide** - ukryj etykietę, jeśli nie jest wskazana kursorem ani zaznaczona.
Show link labels	Wybierz sposób wyświetlania etykiet łączy: **Always** - zawsze wyświetlane (domyślnie); **Auto hide** - ukryj etykietę, jeśli nie jest wskazana kursorem ani zaznaczona.
Problem display	Wyświetlaj liczbę problemów jako: **All** - zostanie wyświetlona pełna liczba problemów **Separated** - liczba niepotwierdzonych problemów będzie wyświetlana oddzielnie jako część całkowitej liczby problemów **Unacknowledged only** - wyświetlana będzie tylko liczba niepotwierdzonych problemów
Minimum severity	Problemy poniżej wybranego minimalnego poziomu ważności nie będą wyświetlane na mapie. Na przykład przy wybranym poziomie *Warning* zmiany z wyzwalaczami o poziomie *Information* i *Not classified* nie będą odzwierciedlane na mapie.
Show suppressed problems	Zaznacz pole wyboru, aby wyświetlać problemy, które w przeciwnym razie byłyby tłumione (niepokazywane) z powodu konserwacji hosta.
URLs	Tutaj można zdefiniować adresy URL dla każdego typu elementu, gdzie: **Name** - etykieta dla adresu URL; **URL** - adres URL (do 2048 znaków); **Element** - typ elementu (np. *Host*, *Host group* itp.). Będą one wyświetlane jako linki, gdy użytkownik kliknie element w trybie podglądu mapy. W nazwach i wartościach URL mapy można używać makr. Pełną listę znajdziesz w supported macros i wyszukaj „map URL names and values".

Udostępnianie

Zakładka **Udostępnianie** zawiera typ mapy oraz opcje udostępniania (grupy użytkowników, użytkownicy) dla map prywatnych:



Parameter	Description
Type	Wybierz typ mapy: **Prywatna** - mapa jest widoczna tylko dla wybranych grup użytkowników i użytkowników **Publiczna** - mapa jest widoczna dla wszystkich
List of user group shares	Wybierz grupy użytkowników, którym mapa ma być udostępniona. Możesz zezwolić na dostęp tylko do odczytu lub do odczytu i zapisu.
List of user shares	Wybierz użytkowników, którym mapa ma być udostępniona. Możesz zezwolić na dostęp tylko do odczytu lub do odczytu i zapisu.

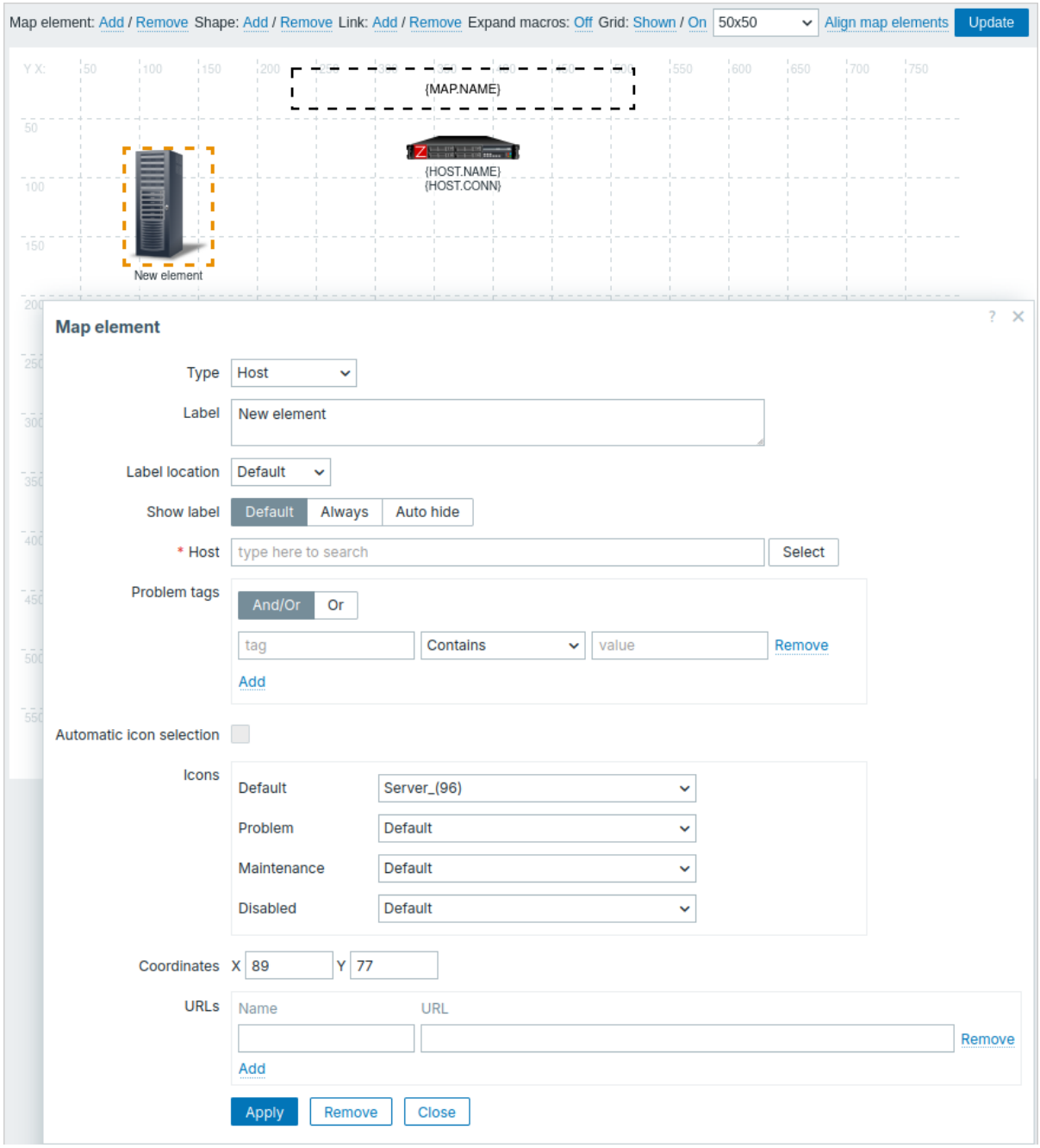
Po kliknięciu *Dodaj*, aby zapisać tę mapę, utworzysz pustą mapę z nazwą, wymiarami i określonymi preferencjami. Teraz musisz dodać kilka elementów. W tym celu kliknij *Edytuj* na liście map, aby otworzyć obszar edycji.

Dodawanie elementów

Aby dodać element, kliknij *Dodaj* obok `Element mapy`. Nowy element pojawi się w lewym górnym rogu mapy. Przeciągnij go i upuść w dowolnym miejscu.

Pamiętaj, że przy włączonej opcji siatki „On” elementy będą zawsze wyrównywane do siatki (możesz wybrać różne rozmiary siatki z listy rozwijanej, a także ukryć/pokazać siatkę). Jeśli chcesz umieszczać elementy w dowolnym miejscu bez wyrównania, ustaw tę opcję na „Off”. (Możesz też później wyrównać losowo rozmieszczone elementy do siatki, klikając *Wyrównaj elementy mapy*).

Gdy masz już kilka elementów na mapie, możesz chcieć zacząć je rozróżniać, nadając im nazwy itp. Po kliknięciu elementu wyświetlany jest formularz, w którym można ustawić typ elementu, nadać nazwę, wybrać inną ikonę itd.



Atrybuty elementu mapy:

Parameter	Description
Type	Typ elementu: **Host** - ikona przedstawiająca stan wszystkich wyzwalaczy wybranego hosta **Map** - ikona przedstawiająca stan wszystkich elementów mapy **Trigger** - ikona przedstawiająca stan jednego lub większej liczby wyzwalaczy **Host group** - ikona przedstawiająca stan wszystkich wyzwalaczy wszystkich hostów należących do wybranej grupy **Image** - ikona niepowiązana z żadnym zasobem
Label	Etykieta ikony, dowolny ciąg znaków. Można używać makr i ciągów wielowierszowych. Makra wyrażeń macros są obsługiwane w tym polu, ale tylko z funkcjami `avg`, `last`, `min` i `max`, z czasem jako parametrem (na przykład `{?avg(/host/key,1h)}`). Pełną listę obsługiwanych makr można znaleźć w sekcji supported macros, wyszukując „map element labels”.

Parameter	Description
Label location	Położenie etykiety względem ikony: **Default** - domyślne położenie etykiety mapy; **Bottom** - pod ikoną; **Left** - po lewej stronie; **Right** - po prawej stronie; **Top** - nad ikoną.
Show label	Wybierz sposób wyświetlania etykiety elementu: **Default** - użyj ustawień *Show map element labels* z konfiguracji mapy (domyślnie); **Always** - zawsze wyświetlana (domyślnie); **Auto hide** - ukryj etykietę, jeśli nie jest wskazana kursorem ani zaznaczona.
Host	Wybierz hosta; alternatywnie wpisz nazwę hosta. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy hosta zostanie wyświetlona lista rozwijana z pasującymi hostami. Przewiń w dół, aby wybrać jeden. Kliknij ikonę usuwania (x), aby usunąć wybór. To pole jest dostępne tylko dla elementów typu *Host*.
Map	Wybierz mapę; alternatywnie wpisz nazwę mapy. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy mapy zostanie wyświetlona lista rozwijana z pasującymi mapami. Przewiń w dół, aby wybrać jedną. Kliknij ikonę usuwania (x), aby usunąć wybór. To pole jest dostępne tylko dla elementów typu *Map*.
Triggers	Wybierz jeden lub więcej wyzwalaczy w polu *New triggers* poniżej i kliknij *Add*. Alternatywnie zacznij wpisywać nazwę wyzwalacza i wybierz go z listy rozwijanej pasujących wyzwalaczy. Kliknij ikonę usuwania (x), aby usunąć wybór. To pole jest dostępne tylko dla elementów typu *Trigger*. Kolejność wybranych wyzwalaczy można zmieniać, ale tylko w obrębie tego samego poziomu ważności wyzwalaczy. Wybór wielu wyzwalaczy wpływa również na rozwiązywanie makr {HOST.*} zarówno w trybie edycji, jak i widoku. W trybie edycji pierwsze wyświetlane makra {HOST.*} będą rozwiązywane zależnie od pierwszego wyzwalacza na liście (na podstawie ważności wyzwalacza). Tryb widoku zależy od parametru Display problems w ogólnych atrybutach mapy: - Jeśli wybrano tryb *Expand single problem*, pierwsze wyświetlane makra {HOST.*} będą rozwiązywane zależnie od ostatniego wykrytego problemowego wyzwalacza (niezależnie od ważności) lub od pierwszego wyzwalacza na liście (jeśli nie wykryto problemu). - Jeśli wybrano tryb *Number of problems and expand most critical one*, pierwsze wyświetlane makra {HOST.*} będą rozwiązywane zależnie od ważności wyzwalacza.
Host group	Wybierz grupę hostów; alternatywnie wpisz grupę hostów. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy grupy hostów zostanie wyświetlona lista rozwijana z pasującymi grupami hostów. Przewiń w dół, aby wybrać jedną. Kliknij ikonę usuwania (x), aby usunąć wybór. To pole jest dostępne tylko dla elementów typu *Host group*.
Problem tags	Określ tagi, aby ograniczyć liczbę problemów wyświetlanych w widżecie. Można zarówno uwzględniać, jak i wykluczać określone tagi oraz wartości tagów. Można ustawić kilka warunków. Dopasowanie nazw tagów zawsze uwzględnia wielkość liter. Dla każdego warunku dostępnych jest kilka operatorów: **Exists** - uwzględnij określone nazwy tagów **Equals** - uwzględnij określone nazwy tagów i wartości (z uwzględnieniem wielkości liter) **Contains** - uwzględnij określone nazwy tagów, których wartości zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter) **Does not exist** - wyklucz określone nazwy tagów **Does not equal** - wyklucz określone nazwy tagów i wartości (z uwzględnieniem wielkości liter) **Does not contain** - wyklucz określone nazwy tagów, których wartości zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter) Dostępne są dwa typy obliczania warunków: **And/Or** - wszystkie warunki muszą być spełnione, a warunki mające tę samą nazwę tagu będą grupowane operatorem Or **Or** - wystarczy spełnienie jednego warunku To pole jest dostępne tylko dla elementów typu *Host* i *Host group*.
Automatic icon selection	Po zaznaczeniu pola wyboru mapowanie ikon zostanie użyte do określenia, która ikona ma być wyświetlana.
Icons	Możesz wybrać wyświetlanie różnych ikon dla elementu w następujących przypadkach: *Default*, *Problem*, *Maintenance* i *Disabled*. To pole jest dostępne tylko dla elementów typu *Host*.

Parameter	Description
Coordinates	Współrzędne **X** i **Y** elementu mapy.
URLs	Tutaj można ustawić adresy URL specyficzne dla elementu, gdzie: **Name** - etykieta dla adresu URL; **URL** - adres URL (do 2048 znaków). Będą one wyświetlane jako linki, gdy użytkownik kliknie element w trybie przeglądania mapy. Jeśli element ma własne adresy URL i zdefiniowano adresy URL na poziomie mapy dla jego typu, zostaną one połączone w tym samym menu. W nazwach i wartościach elementów mapy można używać makr. Pełną listę można znaleźć w sekcji supported macros, wyszukując „map URL names and values”.

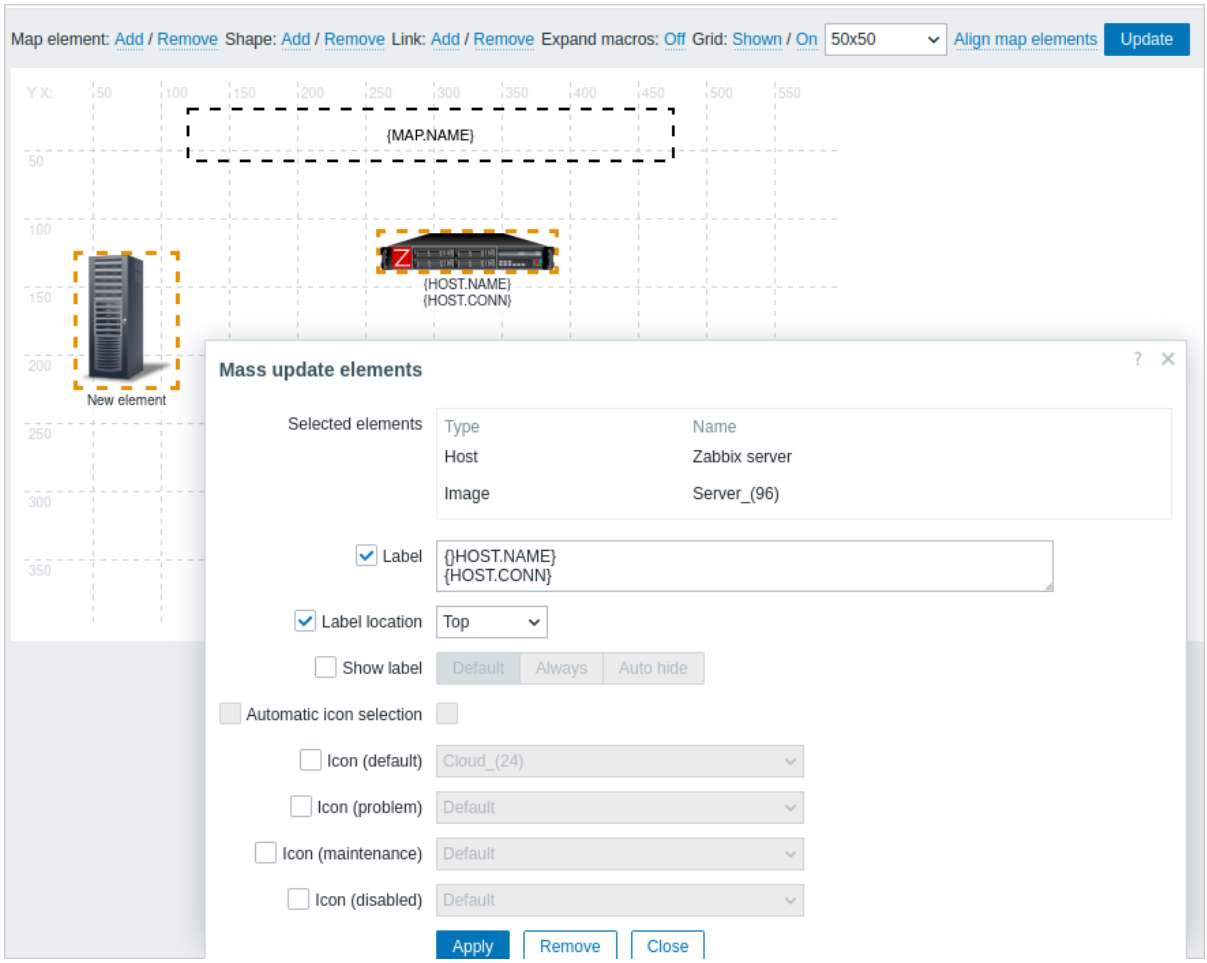
Attention:
Dodane elementy nie są zapisywane automatycznie. Jeśli opuścisz tę stronę, wszystkie zmiany mogą zostać utracone. Dlatego warto kliknąć przycisk **Update** w prawym górnym rogu. Po kliknięciu zmiany zostaną zapisane niezależnie od tego, co wybierzesz w następnym oknie podręcznym.
Wybrane opcje siatki są również zapisywane z każdą mapą.

Wybieranie elementów

Aby wybrać elementy, wybierz jeden z nich, a następnie przytrzymaj *Ctrl*, aby wybrać pozostałe.

Możesz również wybrać wiele elementów, przeciągając prostokąt w edytowalnym obszarze i zaznaczając wszystkie elementy, które się w nim znajdują.

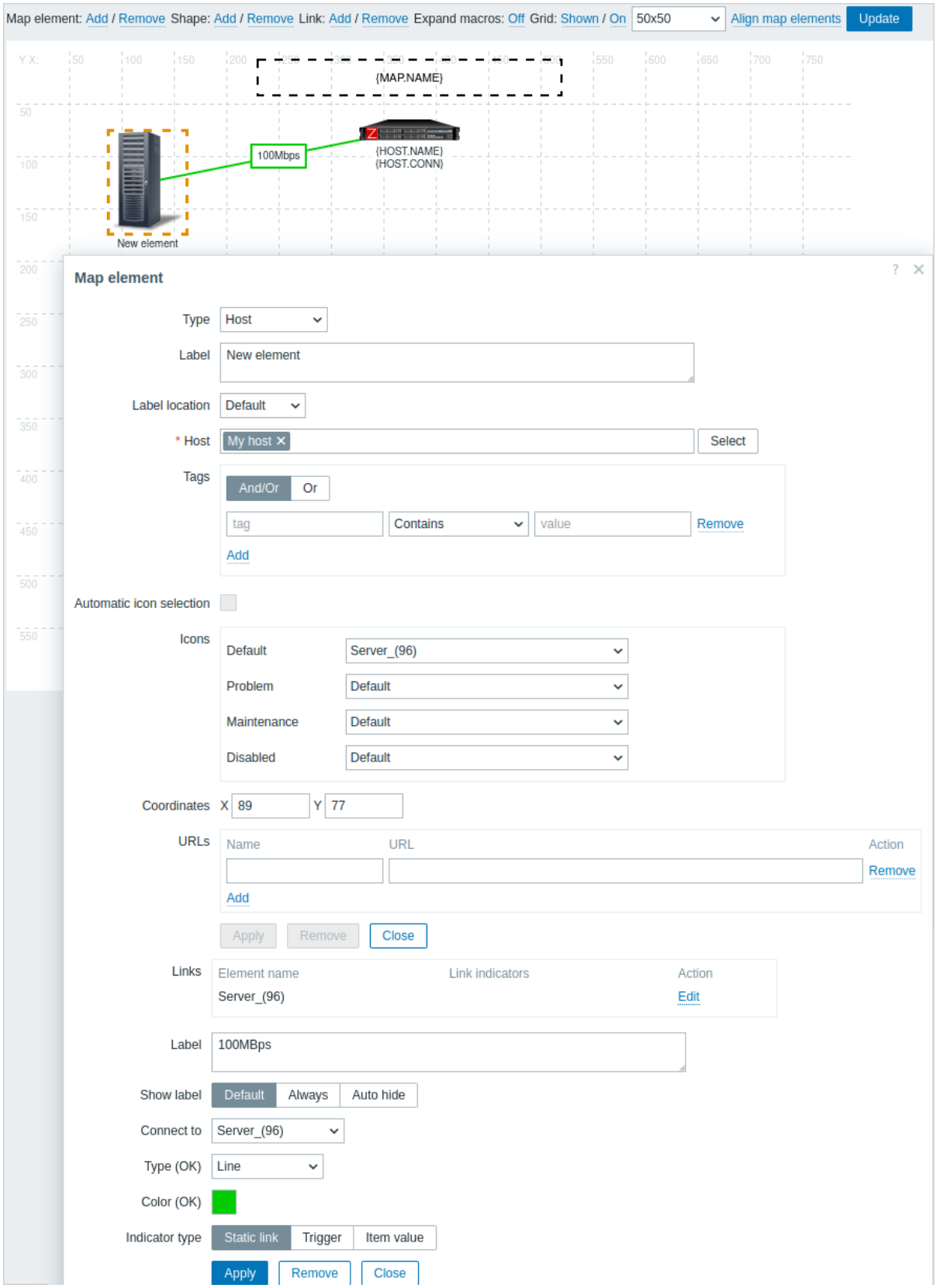
Po wybraniu więcej niż jednego elementu formularz właściwości elementu przełącza się w tryb masowej aktualizacji, dzięki czemu możesz jednocześnie zmienić atrybuty wybranych elementów. Aby to zrobić, zaznacz atrybut za pomocą pola wyboru i wprowadź dla niego nową wartość. Możesz tutaj używać makr (na przykład {HOST.NAME} jako etykiety elementu).



Łączenie elementów

Po umieszczeniu kilku elementów na mapie można rozpocząć ich łączenie. Aby połączyć dwa elementy, należy najpierw je zaznaczyć. Gdy elementy są zaznaczone, kliknij *Dodaj* obok pola Link.

Po utworzeniu połączenia formularz pojedynczego elementu zawiera teraz dodatkową sekcję *Links*. Kliknij *Edytuj*, aby edytować atrybuty połączenia.



Atrybuty połączenia:

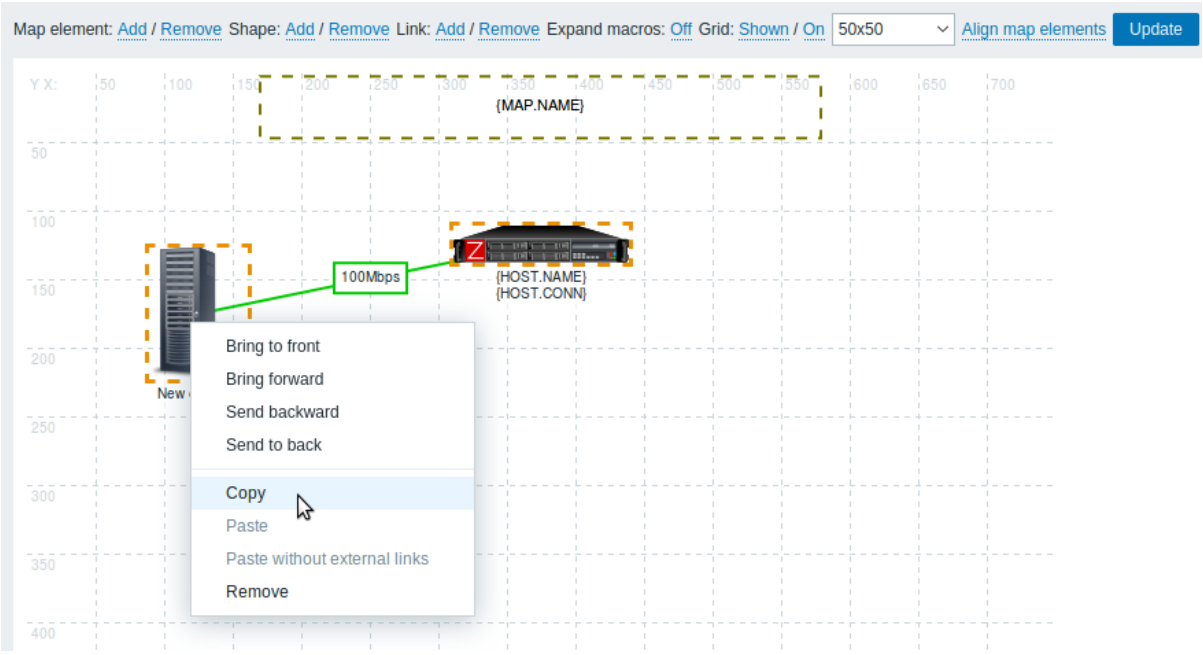
Parametr	Opis
Etykieta	Etykieta, która będzie wyświetlana nad połączeniem. W tym polu obsługiwane są wyrażenia makr, ale tylko z funkcjami `avg`, `last`, `min` i `max`, z czasem jako parametrem (na przykład `{?avg(/host/key,1h)}`).

Parametr	Opis
Pokaż etykietę	Wybierz sposób wyświetlania etykiety połączenia: **Domyślnie** - użyj ustawień *Show map element labels* z konfiguracji mapy (domyślnie); **Zawsze** - zawsze wyświetlana (domyślnie); **Ukryj automatycznie** - ukryj etykietę, jeśli nie jest wskazana kursorem ani zaznaczona.
Połącz z	Element, z którym połączenie jest zestawiane.
Typ (OK)	Domyślny styl połączenia. Wybierz styl: *Linia*, *Pogrubiona linia*, *Kropkowana* lub *Linia przerywana*.
Kolor (OK)	Domyślny kolor połączenia. Kliknij próbkę koloru, aby wybrać inny kolor.
Typ wskaźnika	Wybierz typ wskaźnika połączenia: **Połączenie statyczne** - bez wskaźników; **Wyzwalacz** - zezwala na wskaźniki połączenia oparte na wyzwalaczach; **Wartość pozycji** - zezwala na wskaźniki połączenia oparte na wartościach pozycji.
Pozycja	Wybierz pozycję. Wartość tej pozycji będzie wpływać na styl połączenia. To pole jest dostępne, gdy dla *Typ wskaźnika* wybrano *Wartość pozycji*.
Wskaźniki	Lista wskaźników połączenia. To pole jest dostępne, gdy *Typ wskaźnika* jest ustawiony na *Wyzwalacz* lub *Wartość pozycji*. Jeśli ustawiono *Wyzwalacz*, wyzwalacze mogą zostać przypisane jako wskaźniki połączenia. Gdy wyzwalacz jest w stanie *Problem*, jego styl (wybrany kolor i typ linii) zostanie zastosowany do połączenia. Jeśli ustawiono *Wartość pozycji* i w polu *Pozycja* wybrano pozycję, wartości pozycji mogą zostać przypisane jako wskaźniki połączenia. Gdy wartość pozycji osiągnie określony próg (dla pozycji numerycznej) lub będzie zgodna ze wzorcem (dla pozycji tekstowej), jej styl (wybrany kolor i typ linii) zostanie zastosowany do połączenia.

Przenoszenie i kopiowanie-wklejanie elementów

Kilka wybranych elementów można **przenieść** w inne miejsce na mapie, klikając jeden z zaznaczonych elementów, przytrzymując przycisk myszy i przesuwając kursor do żądanej lokalizacji.

Jeden lub więcej elementów można **skopiować**, zaznaczając elementy, następnie klikając zaznaczony element prawym przyciskiem myszy i wybierając z menu opcję *Kopiuj*.

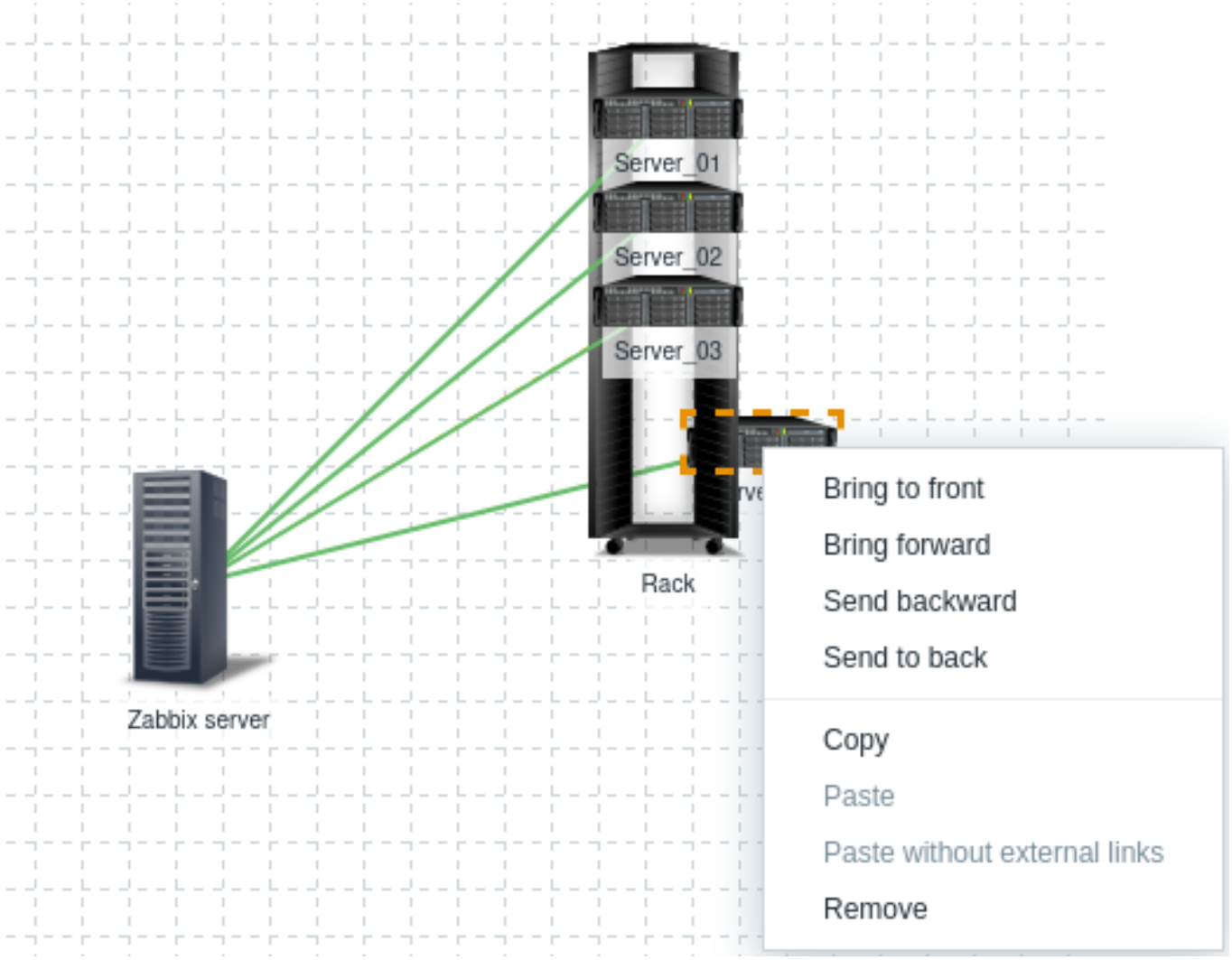


Aby wkleić elementy, kliknij obszar mapy prawym przyciskiem myszy i wybierz z menu opcję *Wklej*. Opcja *Wklej bez zewnętrznych połączeń* wklei elementy, zachowując tylko połączenia między zaznaczonymi elementami.

Kopiowanie i wklejanie działa w obrębie tego samego okna przeglądarki. Skróty klawiaturowe nie są obsługiwane.

Porządkowanie elementów

Aby przenieść jeden element przed drugi (lub odwrotnie), kliknij element prawym przyciskiem myszy i wybierz *Przesuń do przodu/Przenieś na wierzch* lub *Przesuń do tyłu/Przenieś na spód*.

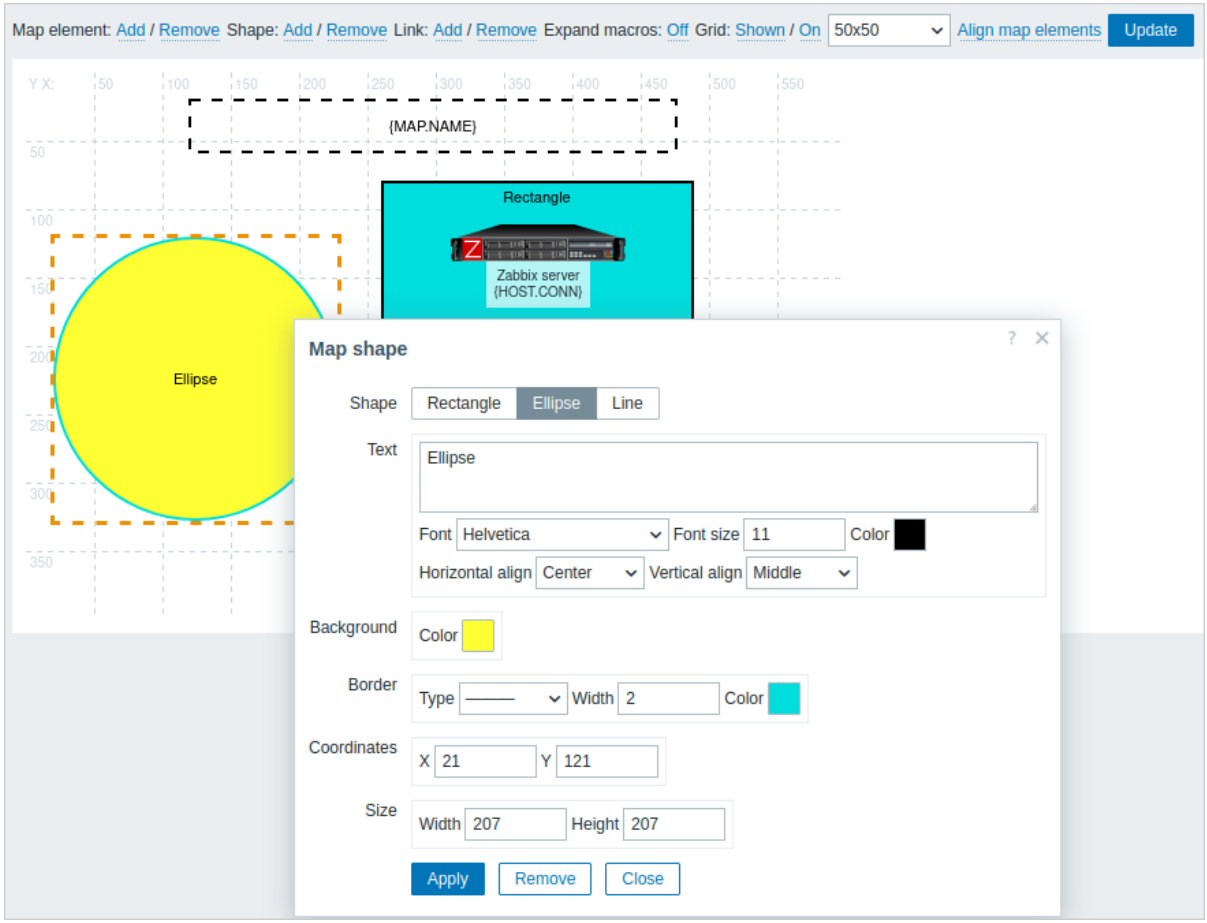


Dodawanie kształtów

Oprócz elementów mapy można również dodawać kształty. Kształty nie są elementami mapy; stanowią jedynie reprezentację wizualną. Na przykład kształt prostokąta może być użyty jako tło do grupowania kilku hostów. Można dodawać kształty prostokąta i elipsy.

Aby dodać kształt, kliknij *Dodaj* obok pola Kształt. Nowy kształt pojawi się w lewym górnym rogu mapy. Przeciągnij go i upuść w dowolnym miejscu.

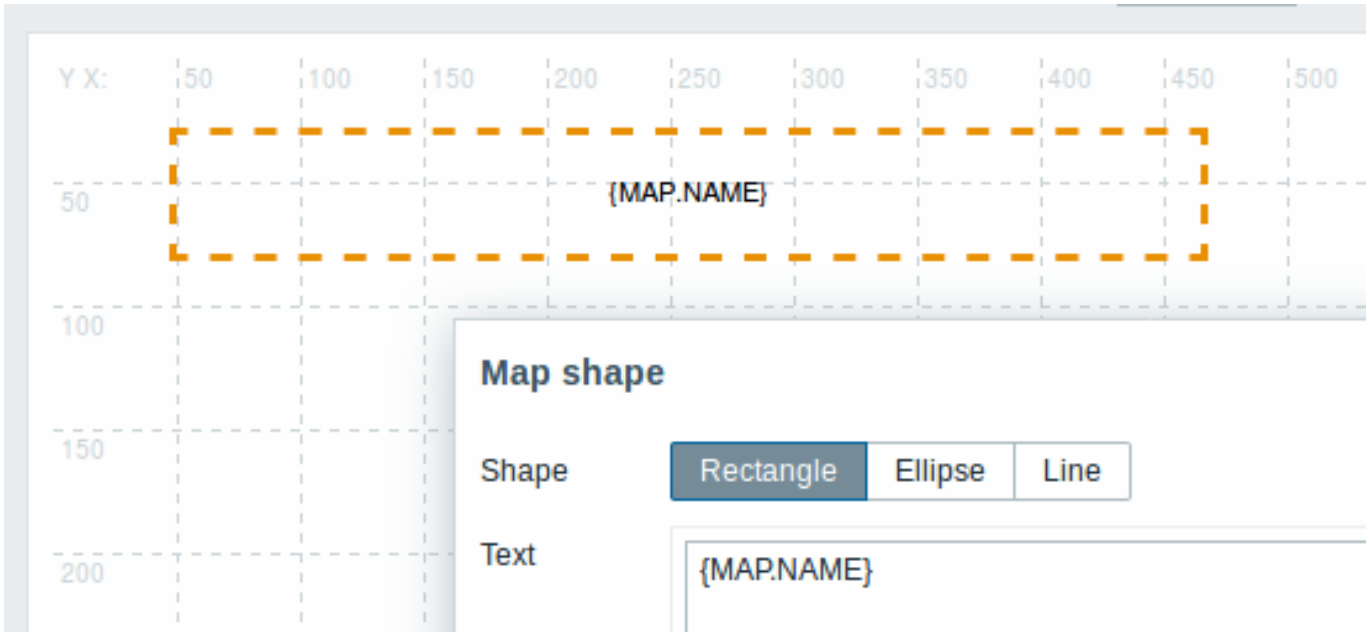
Nowy kształt jest dodawany z domyślnymi kolorami. Po kliknięciu kształtu zostanie wyświetlony formularz, w którym można dostosować wygląd kształtu, dodać tekst itd.



Aby zaznaczyć kształty, wybierz jeden z nich, a następnie przytrzymaj *Ctrl*, aby zaznaczyć pozostałe. Gdy zaznaczonych jest kilka kształtów, wspólne właściwości można zbiorczo zaktualizować, podobnie jak w przypadku elementów.

Do kształtów można dodawać tekst. Wyrażenia makr są obsługiwane w tekście, ale tylko z funkcjami `avg`, `last`, `min` i `max`, z czasem jako parametrem (na przykład `{?avg(/host/key,1h)}`).

Aby wyświetlać tylko tekst, można uczynić kształt niewidocznym przez usunięcie obramowania kształtu (wybierz „Brak” w polu *Obramowanie*). Na przykład zwróć uwagę, że makro {MAP.NAME}, widoczne na powyższym zrzucie ekranu, jest w rzeczywistości kształtem prostokąta z tekstem, co można zobaczyć po kliknięciu makra:



{MAP.NAME} jest rozwijane do skonfigurowanej nazwy mapy podczas wyświetlania mapy.

Jeśli w tekście używane są hiperłącza, stają się klikalne podczas wyświetlania mapy.

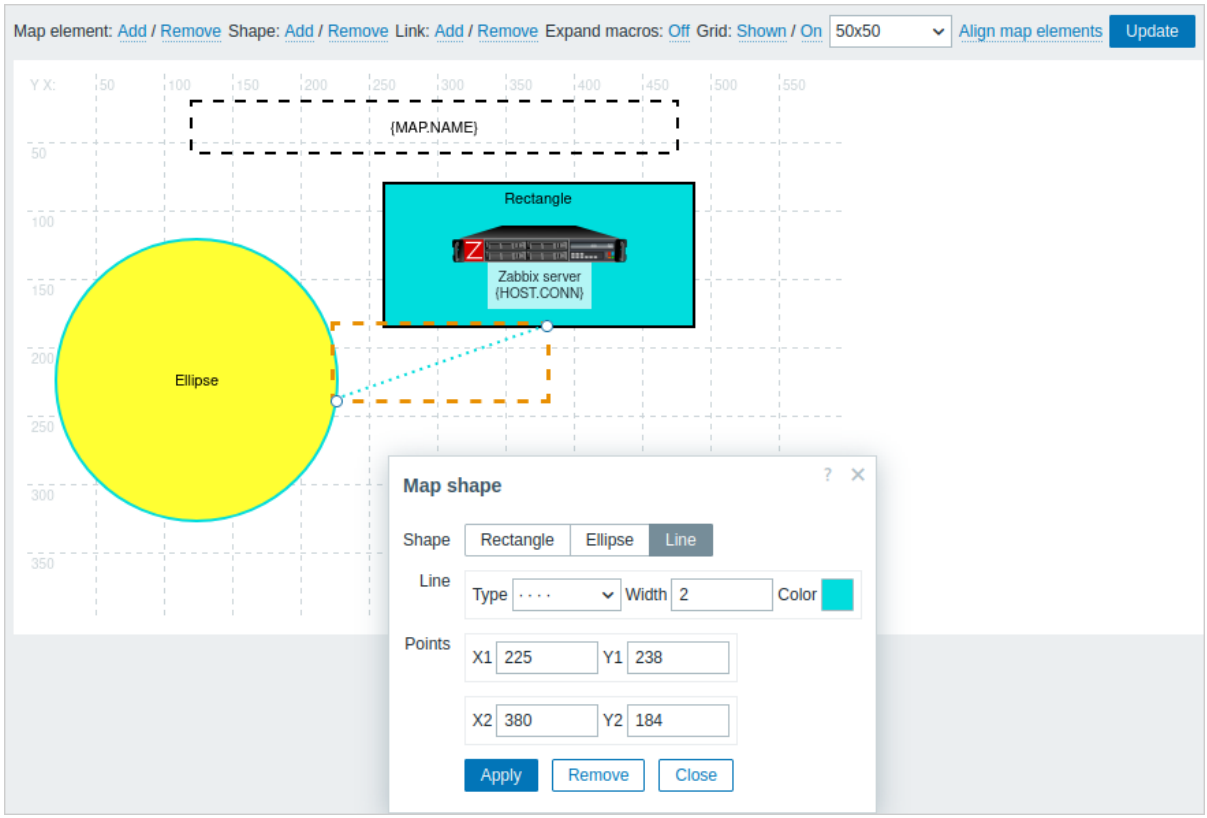
Zawijanie wierszy dla tekstu wewnątrz kształtów jest zawsze włączone. Jednak w obrębie elipsy wiersze są zawijane tak, jakby elipsa była prostokątem. Zawijanie wyrazów nie jest zaimplementowane, więc długie wyrazy (wyrazy, które nie mieszczą się w

kształcie) nie są zawijane, lecz maskowane (na stronie edycji mapy) albo przycinane (na innych stronach z mapami).

Dodawanie linii

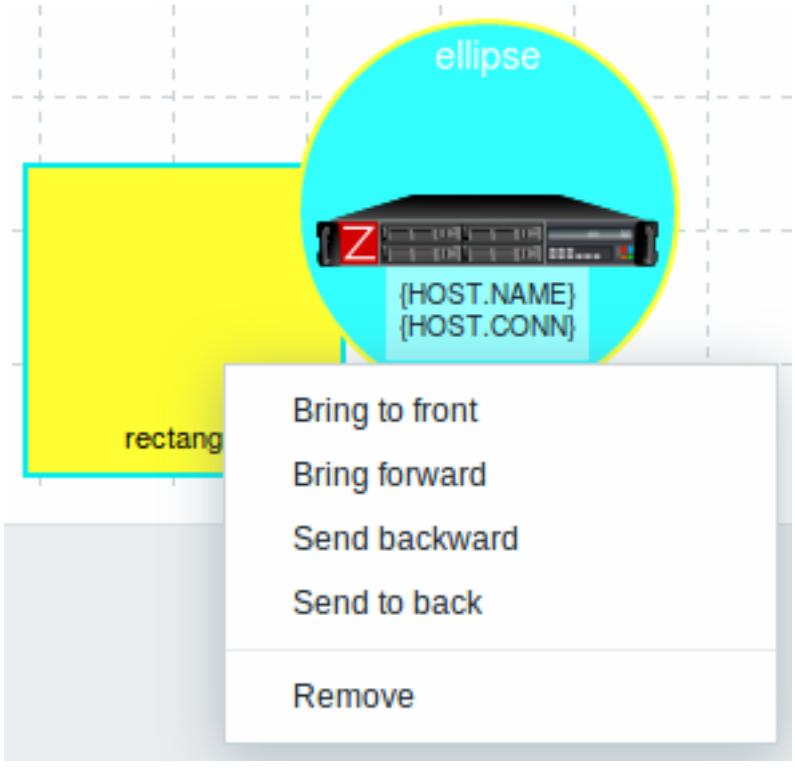
Oprócz kształtów można również dodawać linie. Linie mogą być używane do łączenia elementów lub kształtów na mapie.

Aby dodać linię, kliknij *Dodaj* obok opcji Kształt. Nowy kształt pojawi się w lewym górnym rogu mapy. Zaznacz go i kliknij *Linia* w formularzu edycji, aby zmienić kształt na linię. Następnie dostosuj właściwości linii, takie jak typ linii, szerokość, kolor itp.



Ustalanie kolejności kształtów i linii

Aby przenieść jeden kształt przed drugi (lub odwrotnie), kliknij kształt prawym przyciskiem myszy, aby wyświetlić menu kształtu mapy.

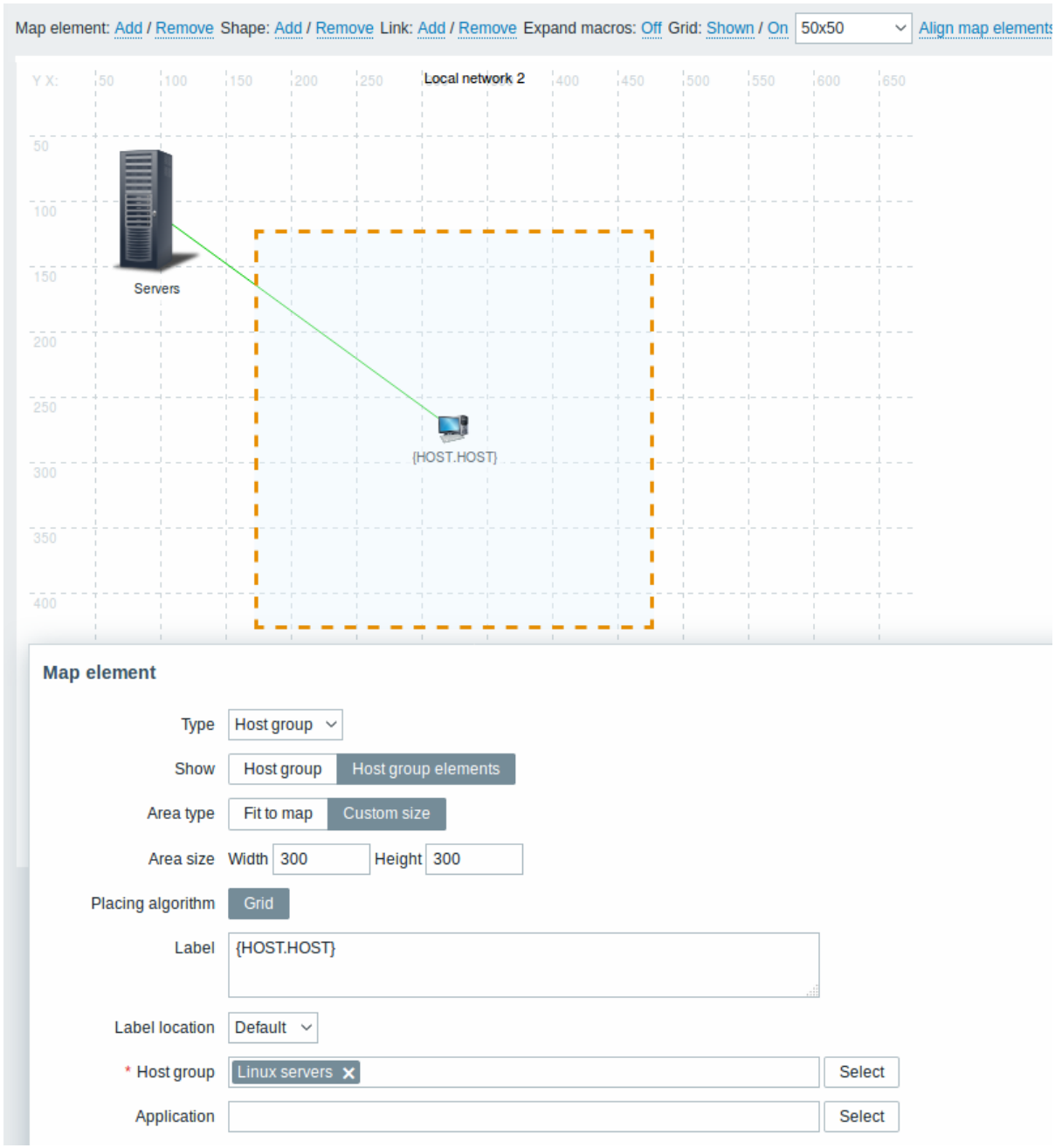


2 Elementy grup hostów

Przegląd

Ta sekcja wyjaśnia, jak dodać element typu *Grupa hostów* podczas konfigurowania mapy sieci.

Konfiguracja



Wszystkie wymagane pola wejściowe są oznaczone czerwoną gwiazdką.

Ta tabela zawiera parametry typowe dla typu elementu *Host group*:

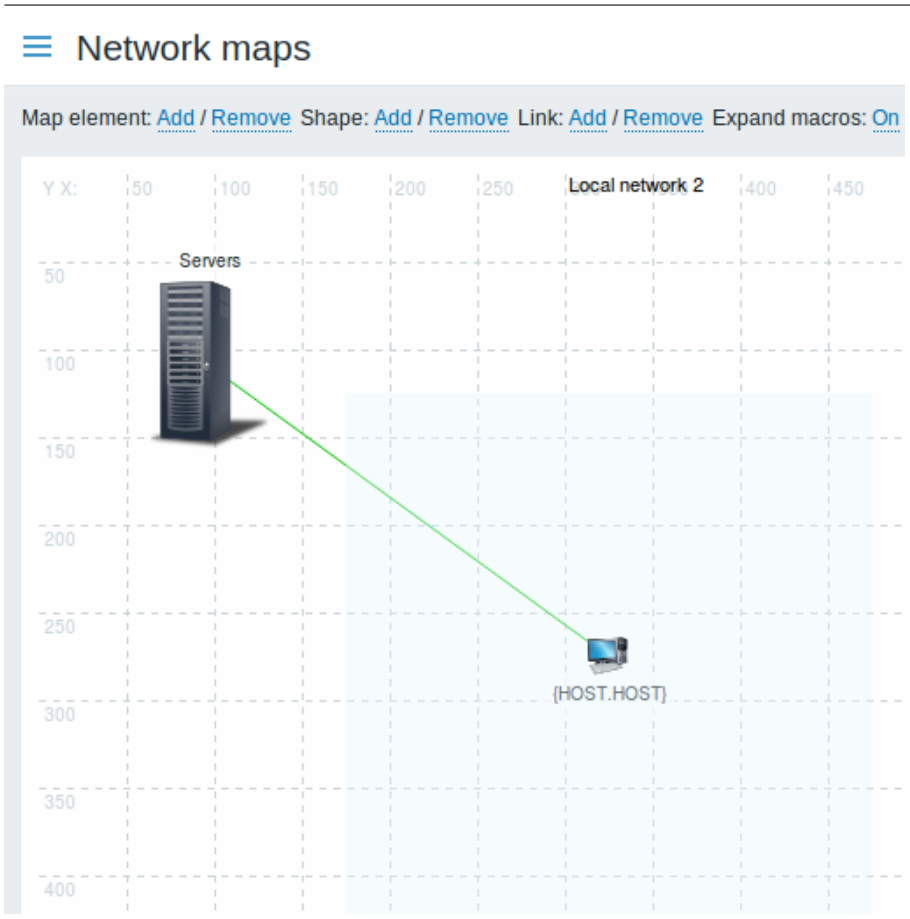
Parametr	Opis
Type	Wybierz typ elementu: **Host group** - Ikona reprezentująca stan wszystkich wyzwalaczy wszystkich hostów należących do wybranej grupy.
Show	Opcje wyświetlania: **Host group** - Wybranie tej opcji spowoduje wyświetlenie jednej ikony prezentującej odpowiednie informacje o określonej grupie hostów. **Host group elements** - Wybranie tej opcji spowoduje wyświetlenie wielu ikon prezentujących odpowiednie informacje o każdym pojedynczym elemencie (hoście) określonej grupy hostów.

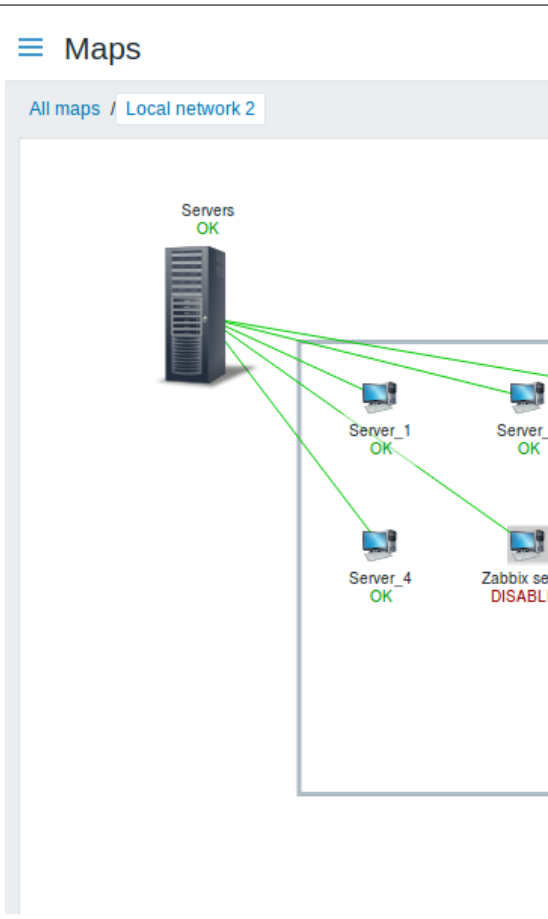
Parametr	Opis
Area type	To ustawienie jest dostępne, jeśli *Show* jest ustawione na *Host group elements*: **Fit to map** - Wszystkie elementy grupy hostów są rozmieszczane równomiernie na mapie. **Custom size** - Ręczne ustawienie obszaru mapy, w którym mają być wyświetlane wszystkie elementy grupy hostów.
Area size	To ustawienie jest dostępne, jeśli *Area type* jest ustawione na *Custom size*: **Width** - Wartość w pikselach określająca szerokość obszaru mapy. **Height** - Wartość w pikselach określająca wysokość obszaru mapy.
Placing algorithm	**Grid** - Jedyna dostępna opcja wyświetlania wszystkich elementów grupy hostów.
Label	Etykieta ikony, dowolny ciąg znaków. W etykietach można używać makr oraz ciągów wielowierszowych. Jeśli typ elementu mapy to *Host group*, określenie niektórych makr wpływa na widok mapy, wyświetlając odpowiednie informacje o każdym pojedynczym hoście. Na przykład, jeśli użyte jest makro {HOST.IP}, widok edycji mapy będzie wyświetlał tylko samo makro {HOST.IP}, natomiast widok mapy będzie zawierał i wyświetlał unikalny adres IP każdego hosta.

Wyświetlanie elementów grupy hostów

Ta opcja jest dostępna, jeśli wybrano opcję wyświetlania *Elementy grupy hostów*. Po wybraniu *Elementy grupy hostów* jako opcji *pokaż* początkowo zobaczysz tylko jedną ikonę dla grupy hostów. Jednak po zapisaniu mapy i przejściu do widoku mapy zobaczysz, że mapa zawiera wszystkie elementy (hosty) określonej grupy hostów:

Widok edycji mapy	Widok mapy





Zwróć uwagę, jak używane jest makro {HOST.HOST}. Podczas edycji mapy nazwa makra nie jest rozwinięta, natomiast w widoku mapy wyświetlane są wszystkie unikalne nazwy hostów.

3 Wskaźniki łączy

Przegląd

Możesz przypisać wskaźniki do łącza między elementami na mapie sieciowej.

Wskaźniki mogą być oparte na wyzwalaczach lub wartościach pozycji. Możliwe jest wyświetlanie różnych stylów i kolorów łączy:

- gdy wyzwalacze przechodzą w stan problemu;
- gdy wartość pozycji:
  - osiąga próg (dla pozycji numerycznych);
  - pasuje do wyrażenia regularnego (dla pozycji tekstowych).

Podczas konfigurowania łącza ustawiasz domyślny typ i kolor łącza. Przypisanie wskaźników do łącza pozwala uzależnić styl i kolor łącza od stanu wyzwalacza lub wartości pozycji.

Na przykład, jeśli którykolwiek z przypisanych wyzwalaczy przejdzie w stan problemu, styl i kolor łącza zmienią się, aby to odzwierciedlić. Być może domyślnie łącze było zieloną linią. Teraz, gdy wyzwalacz jest w stanie problemu, łącze może stać się pogrubioną czerwoną linią (jeśli zostało to tak zdefiniowane).

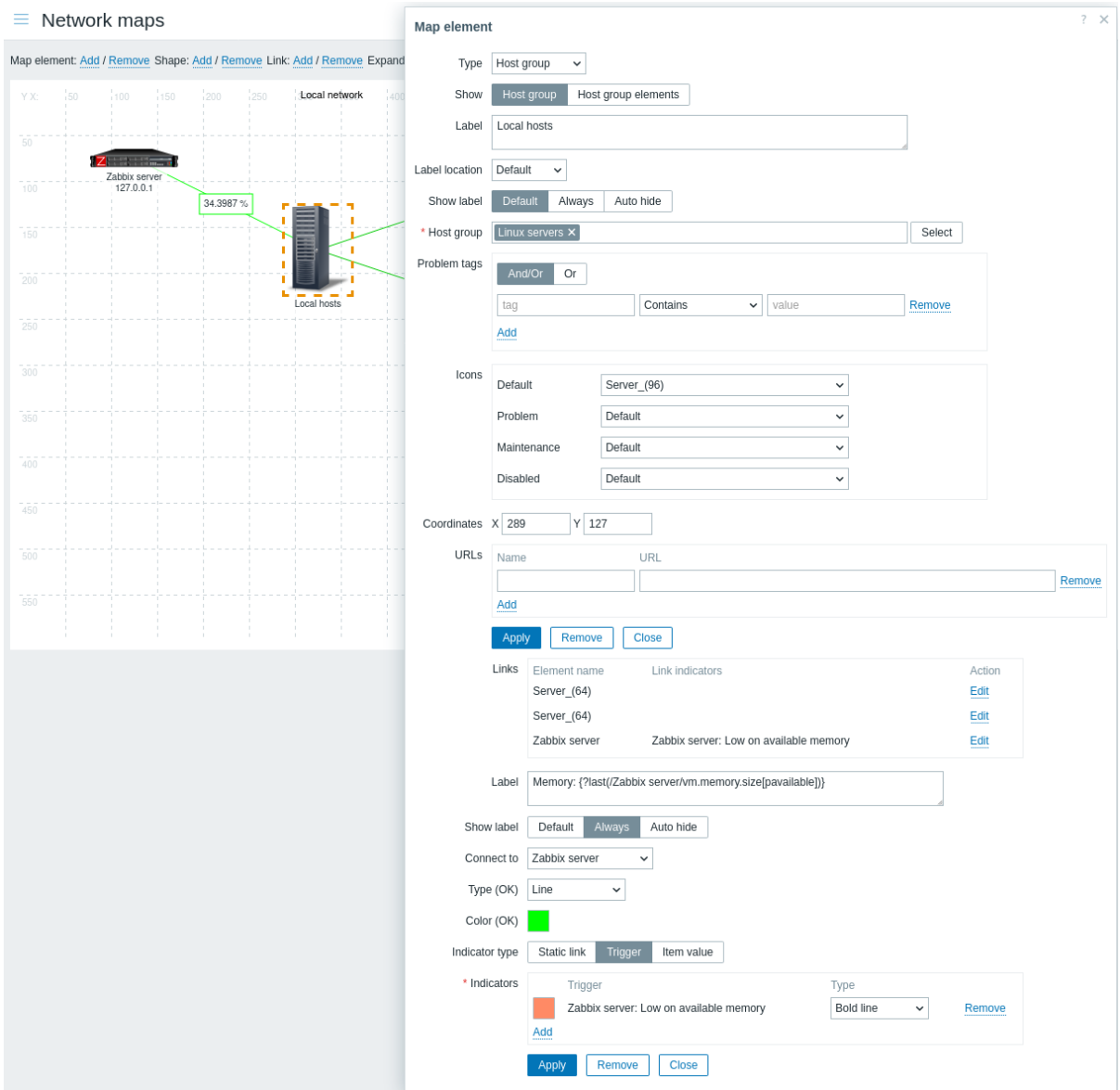
Podobnie, jeśli wartość pozycji osiągnie określony próg lub będzie pasować do określonego wyrażenia regularnego, styl łącza może to odzwierciedlać.

Konfiguracja

Wyzwalacze

Aby przypisać wyzwalacze jako wskaźniki łączy, wykonaj następujące czynności:

- wybierz element mapy
- kliknij *Edytuj* w sekcji *Łącza* dla odpowiedniego łącza
- wybierz *Wyzwalacz* jako typ wskaźnika
- kliknij *Dodaj* w bloku *Wskaźniki* i wybierz jeden lub więcej wyzwalaczy

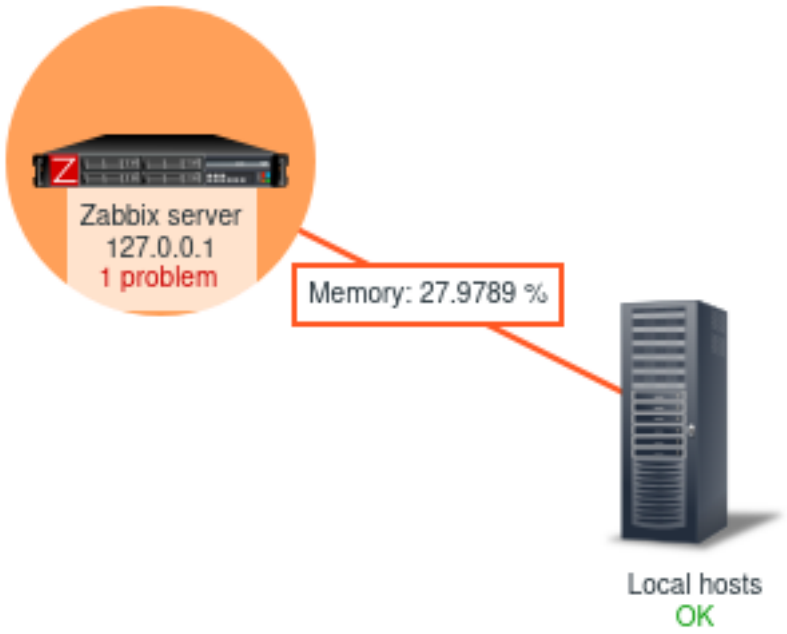


Wszystkie wymagane pola wejściowe są oznaczone czerwoną gwiazdką.

Dodane wyzwalacze są widoczne na liście *Wskaźniki*.

Typ łącza i kolor dla każdego wskaźnika można ustawić bezpośrednio z listy. Po zakończeniu kliknij *Zastosuj*, zamknij formularz i kliknij *Aktualizuj*, aby zapisać zmiany mapy.

W *Monitoring* → *Mapy* odpowiedni typ łącza i kolor będą wyświetlane, jeśli **wyzwalacz** przejdzie w stan problemu.



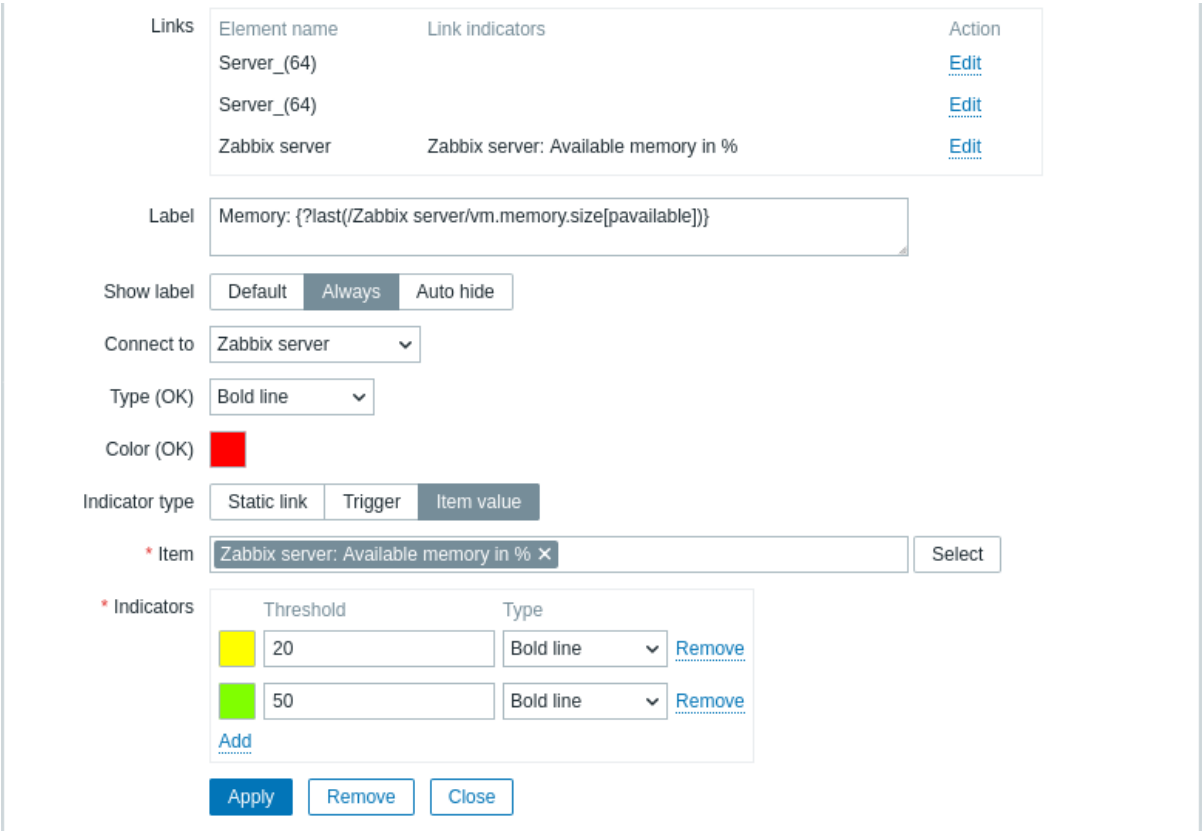
Note:
Jeśli wiele wyzwalaczy przejdzie w stan problemu, styl i kolor łącza zostaną określone przez problem o najwyższym poziomie ważności. Jeśli do tego samego łącza mapy przypisano wiele wyzwalaczy o tym samym poziomie ważności, pierwszeństwo ma ten o najniższym ID. Należy również pamiętać, że:

1. Ustawienia *Minimalny poziom ważności wyzwalacza* i *Pokaż ukryty problem* z konfiguracji mapy wpływają na to, które problemy są brane pod uwagę.
2. W przypadku wyzwalaczy z wieloma problemami (wielokrotne generowanie problemów) każdy problem może mieć poziom ważności różniący się od poziomu ważności wyzwalacza (zmieniony ręcznie), może mieć różne tagi (z powodu makr) i może być ukryty.

Wartości pozycji

Aby przypisać wartości pozycji jako wskaźniki łączy, wykonaj następujące czynności:

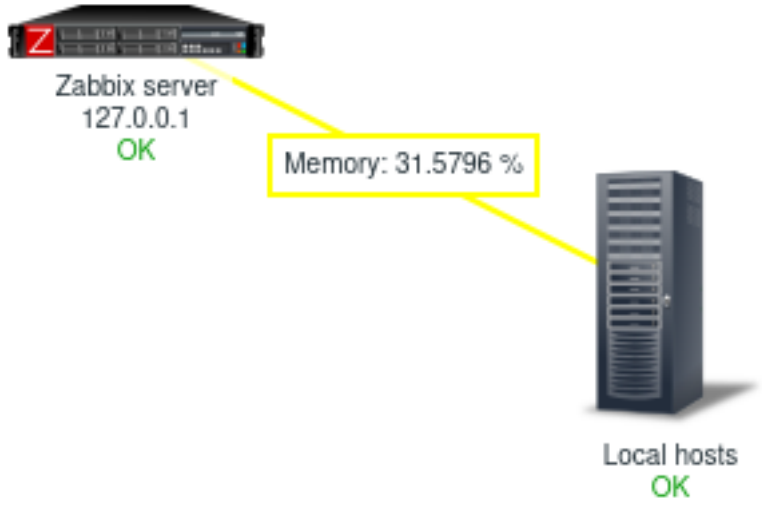
- wybierz element mapy
- kliknij *Edytuj* w sekcji *Łącza* dla odpowiedniego łącza
- wybierz *Wartość pozycji* jako typ wskaźnika
- wybierz pozycję
- dodaj jeden lub więcej progów wartości pozycji albo wzorców w bloku *Wskaźniki*



Dodane progi/wzorce pozycji są widoczne na liście *Wskaźniki*.

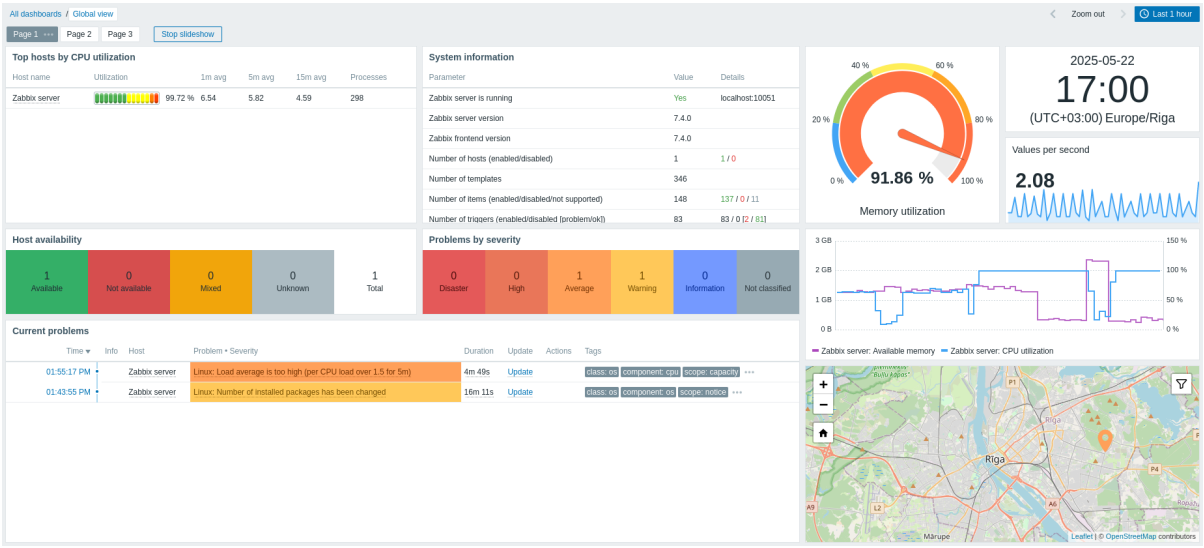
Typ łącza i kolor dla każdego wskaźnika można ustawić bezpośrednio z listy. Po zakończeniu kliknij *Zastosuj*, zamknij formularz i kliknij *Aktualizuj*, aby zapisać zmiany mapy.

W *Monitoring* → *Mapy* odpowiedni typ łącza i kolor będą wyświetlane, jeśli **wartość pozycji** osiągnie ustawiony próg (dla typów danych numerycznych) lub będzie zgodna ze wzorcem wyrażenia regularnego (dla tekstowych typów danych).



3 Pulpity

Pulpity — zarówno pulpity globalne, jak i pulpity hostów — zapewniają rozbudowaną platformę wizualizacji z takimi widgetami i narzędziami, jak nowoczesne wykresy, mapy, pokazy slajdów i inne.



8 Szablony i grupy szablonów

Przegląd

Użycie szablonów to doskonały sposób na zmniejszenie nakładu pracy i usprawnienie konfiguracji Zabbix. Szablon to zestaw encji, który można wygodnie zastosować do wielu hostów.

Encje te mogą obejmować:

- pozycje
- wyzwalacze
- wykresy
- pulpity
- reguły wykrywania niskiego poziomu
- scenariusze WWW

Ponieważ wiele hostów w rzeczywistości jest identycznych lub dość podobnych, naturalne jest, że zestaw encji (pozycji, wyzwalaczy, wykresów, ...) utworzony dla jednego hosta może być przydatny dla wielu innych. Oczywiście można skopiować je do każdego nowego hosta, ale wymagałoby to dużo ręcznej pracy. Zamiast tego, korzystając z szablonów, można skopiować je do jednego szablonu, a następnie zastosować ten szablon do dowolnej liczby hostów.

Gdy szablon jest podłączony do hosta, wszystkie encje (pozycje, wyzwalacze, wykresy, ...) ze szablonu są dodawane do hosta. Szablony są przypisywane bezpośrednio do każdego pojedynczego hosta (a nie do grupy hostów).

Szablony są często używane do grupowania encji dla określonych usług lub aplikacji (takich jak Apache, MySQL, PostgreSQL, Postfix...) i następnie stosowane do hostów, na których działają te usługi.

Kolejną korzyścią z używania szablonów jest możliwość wprowadzania zmian dla wszystkich hostów jednocześnie. Jednorazowa zmiana na poziomie szablonu zostanie propagowana do wszystkich powiązanych hostów.

Szablony są zorganizowane w grupy szablonów.

Przejdź do tworzenia i konfigurowania szablonu.

9 Szablony dostępne od razu

Przegląd

Zabbix udostępnia stale rosnący zestaw wstępnie skonfigurowanych szablonów, aby uprościć i przyspieszyć konfigurację monitorowanych obiektów.

Wszystkie gotowe szablony są dostępne w *Data collection* > *Templates*.

Podczas aktualizacji Zabbix istniejące szablony nie są aktualizowane automatycznie, aby uniknąć nadpisania niestandardowych modyfikacji. Aby zaktualizować istniejące szablony lub dodać nowe, zobacz Aktualizacja szablonów.

Skorzystaj z panelu bocznego, aby uzyskać informacje o określonych typach szablonów i wymaganiach operacyjnych.

Zobacz także:

- Podłączanie szablonu
- Znane problemy dotyczące szablonów

Aktualizacja szablonu

Aby zaktualizować pojedynczy szablon lub dodać nowy po aktualizacji Zabbix:

1. Przejdź do repozytorium Git Zabbix.
2. W selektorze gałęzi (pod etykietą *Source*) wybierz gałąź odpowiadającą używanej wersji Zabbix (np. *master* dla najnowszej wersji rozwojowej).
3. Otwórz szablon, który chcesz dodać lub zaktualizować (np. MySQL by Zabbix agent).
4. Skopiuj zawartość pliku szablonu (np. `template_db_mysql_agent.yaml`) i zapisz ją do pliku lokalnego.
5. W Zabbix frontend przejdź do *Data collection* > *Templates* i zaimportuj plik lokalny.

Możesz także zaktualizować wszystkie szablony i dodać nowe za jednym razem:

1. Pobierz pakiet szablonów odpowiedni dla swojego serwera WWW: `templates_1M_8.0.7z` (Nginx) lub `templates_2M_8.0.7z` (Apache).
2. Rozpakuj pakiet. Zawiera on pliki YAML (każdy z wieloma szablonami) oraz indeks (`index-1M_80.md`) zawierający listę szablonów uwzględnionych w każdym pliku YAML.
3. W Zabbix frontend przejdź do *Data collection* > *Templates* i zaimportuj pliki YAML jeden po drugim.

Alternatywnie możesz zaimportować wszystkie pliki YAML jednocześnie, używając skryptu `import_templates.sh`. Skrypt wymaga narzędzi `curl` i `jq` oraz używa metody API Zabbix `configuration.import`. Podczas uruchamiania skryptu podaj katalog zawierający pliki YAML oraz URL i token uwierzytelniający API Zabbix.

Warning:
Skrypt `import_templates.sh` nadpisuje wszystkie istniejące szablony, bez możliwości przeglądu lub cofnięcia zmian w szablonach.

Przykład:

```
./import_templates.sh /tmp/templates_2M_8.0 https://example.com/zabbix/api_jsonrpc.php d8d6b5c78ee2a8333db
```

Zgodność szablonu z Kreatorem hostów

Kreator hostów jest zgodny ze wszystkimi gotowymi szablonami.

Możesz również sprawić, aby własne szablony były zgodne z Kreatorem hostów:

1. W frontendzie Zabbix przejdź do *Data collection* > *Templates* i wyeksportuj własny szablon.
2. Edytuj wyeksportowany plik:
   - Dodaj element szablonu `wizard_ready`, aby wskazać zgodność z Kreatorem hostów.
   - Opcjonalnie dodaj element szablonu `readme` lub `config`, zależnie od potrzeb.
3. W frontendzie Zabbix przejdź do *Data collection* > *Templates* i zaimportuj zaktualizowany plik szablonu.

1 Działanie szablonów Zabbix agent

Kroki zapewniające prawidłowe działanie szablonów zbierających metryki za pomocą Zabbix agent:

1. Upewnij się, że Zabbix agent jest zainstalowany na hoście. W przypadku aktywnych kontroli upewnij się również, że adres serwera/proxy Zabbix został dodany do parametru 'ServerActive' w pliku konfiguracyjnym agenta.
2. Podłącz szablon do docelowego hosta (jeśli szablon nie jest dostępny w Twojej instalacji Zabbix, może być konieczne najpierw zaimportowanie szablonu).
3. W razie potrzeby dostosuj wartości makr szablonu.
4. Skonfiguruj monitorowaną instancję tak, aby umożliwiała udostępnianie danych do Zabbix.

Szczegółowy opis szablonu, w tym pełna lista makr, pozycji i wyzwalaczy, jest dostępny w pliku README szablonu (dostępnym po kliknięciu nazwy szablonu).

Dostępne są następujące szablony:

- Apache by Zabbix agent

- Apache by Zabbix agent active
- HAProxy by Zabbix agent
- IIS by Zabbix agent
- IIS by Zabbix agent active
- Microsoft Exchange Server 2016 by Zabbix agent
- Microsoft Exchange Server 2016 by Zabbix agent active
- MySQL by Zabbix agent
- MySQL by Zabbix agent active
- Nginx by Zabbix agent
- Nginx by Zabbix agent active
- PHP-FPM by Zabbix agent
- PHP-FPM by Zabbix agent active
- PostgreSQL by Zabbix agent
- PostgreSQL by Zabbix agent active
- RabbitMQ cluster by Zabbix agent

2 Działanie szablonów Zabbix agent 2

Kroki zapewniające prawidłowe działanie szablonów zbierających metryki za pomocą Zabbix agent 2:

1. Upewnij się, że agent 2 jest zainstalowany na hoście oraz że zainstalowana wersja zawiera wymagany plugin. W niektórych przypadkach może być konieczne najpierw uaktualnienie agent 2.

2. Podłącz szablon do docelowego hosta (jeśli szablon nie jest dostępny w Twojej instalacji Zabbix, może być konieczne najpierw zaimportowanie szablonu).

3. W razie potrzeby dostosuj wartości makr szablonu. Zwróć uwagę, że makra użytkownika mogą być używane do nadpisywania parametrów konfiguracyjnych.

4. Skonfiguruj monitorowaną instancję tak, aby umożliwić współdzielenie danych z Zabbix.

Attention:
Szablony Zabbix agent 2 działają w połączeniu z pluginami. Podstawową konfigurację można wykonać po prostu przez dostosowanie makr użytkownika, natomiast głębszą personalizację można osiągnąć przez skonfigurowanie samego pluginu. Na przykład, jeśli plugin obsługuje nazwane sesje, możliwe jest monitorowanie kilku obiektów tego samego typu (np. MySQL1 i MySQL2) przez określenie nazwanej sesji z własnym URI, nazwą użytkownika i hasłem dla każdego obiektu w pliku konfiguracyjnym.

Szczegółowy opis szablonu, w tym pełna lista makr, pozycji i wyzwalaczy, jest dostępny w pliku README szablonu (dostępnym po kliknięciu nazwy szablonu).

Dostępne są następujące szablony:

- Ceph by Zabbix agent 2
- Docker
- Memcached
- MongoDB cluster by Zabbix agent 2
- MongoDB node by Zabbix agent 2
- MySQL by Zabbix agent 2
- MySQL by Zabbix agent 2 active
- Oracle by Zabbix agent 2
- PostgreSQL by Zabbix agent 2
- PostgreSQL by Zabbix agent 2 active
- Redis
- SMART by Zabbix agent 2
- SMART by Zabbix agent 2 active
- Systemd by Zabbix agent 2
- Website certificate by Zabbix agent 2

3 Działanie szablonów HTTP

Kroki zapewniające prawidłowe działanie szablonów zbierających metryki za pomocą HTTP agent:

1. Utwórz w Zabbix host odpowiadający monitorowanemu celowi. Określ adres IP/nazwę DNS monitorowanego celu jako główny interfejs hosta. Jest to wymagane, aby makro {HOST.CONN} było prawidłowo rozwiązywane w pozycjach szablonu.

2. Podłącz szablon do hosta utworzonego w kroku 1 (jeśli szablon nie jest dostępny w Twojej instalacji Zabbix, może być konieczne najpierw zaimportowanie szablonu).

3. W razie potrzeby dostosuj wartości makr na poziomie szablonu.

4. Skonfiguruj monitorowaną instancję tak, aby umożliwiała współdzielenie danych z Zabbix.

Szczegółowy opis szablonu, w tym pełna lista makr, pozycji i wyzwalaczy, jest dostępny w pliku README szablonu (dostępnym po kliknięciu nazwy szablonu).

Dostępne są następujące szablony:

- Acronis Cyber Protect Cloud przez HTTP
- Apache przez HTTP
- Asterisk przez HTTP
- AWS przez HTTP
- AWS Cost Explorer przez HTTP
- AWS EC2 przez HTTP
- AWS ECS Cluster przez HTTP
- AWS ECS Serverless Cluster przez HTTP
- AWS ELB Application Load Balancer przez HTTP
- AWS ELB Network Load Balancer przez HTTP
- AWS Lambda przez HTTP
- Instancja AWS RDS przez HTTP
- Bucket AWS S3 przez HTTP
- Azure przez HTTP
- Organizacja Cisco Meraki przez HTTP
- Cisco SD-WAN przez HTTP
- Cisco Secure Firewall Threat Defense przez HTTP
- ClickHouse przez HTTP
- Cloudflare przez HTTP
- CockroachDB przez HTTP
- Control-M enterprise manager przez HTTP
- Control-M server przez HTTP
- Cradlepoint NCM v2 przez HTTP
- DELL PowerEdge R720 przez HTTP
- DELL PowerEdge R740 przez HTTP
- DELL PowerEdge R820 przez HTTP
- DELL PowerEdge R840 przez HTTP
- Domena RDAP przez HTTP
- Klaster Elasticsearch przez HTTP
- Envoy Proxy przez HTTP
- Etcd przez HTTP
- FortiGate przez HTTP
- Repozytorium GitHub przez HTTP
- GitLab przez HTTP
- Google Cloud Platform (GCP) przez HTTP
- Hadoop przez HTTP
- HAProxy przez HTTP
- Klaster HashiCorp Consul przez HTTP
- Węzeł HashiCorp Consul przez HTTP
- HashiCorp Nomad przez HTTP
- HashiCorp Vault przez HTTP
- Kamera Hikvision przez HTTP
- HPE iLO przez HTTP
- Macierz HPE MSA 2040 przez HTTP
- Macierz HPE MSA 2060 przez HTTP
- HPE Primera przez HTTP
- HPE Synergy przez HTTP
- InfluxDB przez HTTP
- Jenkins przez HTTP

- Serwer API Kubernetes przez HTTP
- Stan klastra Kubernetes przez HTTP

- Kubernetes Controller manager przez HTTP

- Kubernetes kubelet przez HTTP

- Węzły Kubernetes przez HTTP
- Kubernetes Scheduler przez HTTP
- MantisBT przez HTTP
- Raporty Microsoft 365 przez HTTP
- Microsoft SharePoint przez HTTP
- NetApp AFF A700 przez HTTP
- Nextcloud przez HTTP
- NGINX przez HTTP
- NGINX Plus przez HTTP
- Nutanix Prism Element przez HTTP
- OpenAI Platform przez HTTP
- OpenStack przez HTTP
- OpenWeatherMap przez HTTP
- Oracle Cloud przez HTTP
- Palo Alto PA-440 przez HTTP
- PHP-FPM przez HTTP
- Proxmox VE przez HTTP
- Pure Storage FlashArray v1 i v2 przez HTTP
- Klaster RabbitMQ przez HTTP
- Ribbon SBC Edge przez HTTP
- Ribbon SBC SWe CE przez HTTP
- Ribbon SBC SWe Core przez HTTP
- TiDB przez HTTP
- TiDB PD przez HTTP
- TiDB TiKV przez HTTP
- Travis CI przez HTTP
- Veeam Backup Enterprise Manager przez HTTP
- Veeam Backup and Replication przez HTTP
- VeloCloud SD-WAN przez HTTP
- VeloCloud SD-WAN Edge przez HTTP
- YugabyteDB przez HTTP
- ZooKeeper przez HTTP

4 Działanie szablonu IPMI

Szablony IPMI nie wymagają żadnej specjalnej konfiguracji. Aby rozpocząć monitorowanie, podłącz szablon do docelowego hosta (jeśli szablon nie jest dostępny w Twojej instalacji Zabbix, może być konieczne wcześniejsze zaimportowanie szablonu).

Szczegółowy opis szablonu, w tym pełna lista makr, pozycji i wyzwalaczy, jest dostępny w pliku README szablonu (dostępnym po kliknięciu nazwy szablonu).

Dostępny szablon:

- Chassis by IPMI

5 Działanie szablonów JMX

Kroki zapewniające prawidłowe działanie szablonów zbierających metryki przez JMX:

1. Upewnij się, że Java gateway Zabbix jest zainstalowany i poprawnie skonfigurowany.

2. Podłącz szablon do docelowego hosta. Host powinien mieć skonfigurowany interfejs JMX. Jeśli szablon nie jest dostępny w Twojej instalacji Zabbix, może być konieczne najpierw zaimportowanie szablonu.

3. W razie potrzeby dostosuj wartości makr szablonu.

4. Skonfiguruj monitorowaną instancję tak, aby umożliwiała udostępnianie danych do Zabbix.

Szczegółowy opis szablonu, w tym pełna lista makr, pozycji i wyzwalaczy, jest dostępny w pliku README szablonu (dostępnym po kliknięciu nazwy szablonu).

Dostępne są następujące szablony:

- Apache ActiveMQ by JMX
- Apache Cassandra by JMX
- Apache Kafka by JMX
- Apache Tomcat by JMX
- GridGain by JMX
- Ignite by JMX
- Jira Data Center by JMX
- WildFly Domain by JMX
- WildFly Server by JMX

6 Działanie szablonów ODBC

Kroki zapewniające prawidłowe działanie szablonów zbierających metryki za pomocą monitorowania ODBC:

1. Upewnij się, że wymagany sterownik ODBC jest zainstalowany na serwerze Zabbix lub proxy.
2. Podłącz szablon do docelowego hosta (jeśli szablon nie jest dostępny w Twojej instalacji Zabbix, może być konieczne jego wcześniejsze zaimportowanie).
3. W razie potrzeby dostosuj wartości makr szablonu.
4. Skonfiguruj monitorowaną instancję tak, aby umożliwiała udostępnianie danych do Zabbix.

Szczegółowy opis szablonu, w tym pełna lista makr, pozycji i wyzwalaczy, jest dostępny w pliku README szablonu (dostępnym po kliknięciu nazwy szablonu).

Dostępne są następujące szablony:

- MariaDB by ODBC
- MSSQL by ODBC
- MySQL by ODBC
- Oracle by ODBC
- Percona by ODBC
- PostgreSQL by ODBC

7 Standaryzowane szablony dla urządzeń sieciowych

Przegląd

Aby zapewnić monitorowanie urządzeń sieciowych, takich jak przełączniki i routery, utworzyliśmy dwa tak zwane modele: dla samego urządzenia sieciowego (zasadniczo jego obudowy) oraz dla interfejsu sieciowego.

Dostępne są szablony dla wielu rodzin urządzeń sieciowych. Wszystkie szablony obejmują (tam, gdzie możliwe jest pobranie tych pozycji z urządzenia):

- Monitorowanie usterek obudowy (zasilacze, wentylatory i temperatura, ogólny stan)
- Monitorowanie wydajności obudowy (pozycje CPU i pamięci)
- Zbieranie danych inwentaryzacyjnych obudowy (numery seryjne, nazwa modelu, wersja firmware)
- Monitorowanie interfejsów sieciowych za pomocą IF-MIB i EtherLike-MIB (stan interfejsu, obciążenie ruchem interfejsu, stan dupleksu dla Ethernet)

Jeśli szablon nie jest dostępny w Twojej instalacji Zabbix, może być konieczne najpierw jego zaimportowanie.

Jeśli importujesz nowe gotowe szablony, możesz również chcieć zaktualizować globalne wyrażenie regularne `@Network interfaces for discovery` do postaci:

```
Result is FALSE: ^Software Loopback Interface
Result is FALSE: ^(In)?[lL]oop[bB]ack[0-9._]*$
Result is FALSE: ^NULL[0-9.]*$
Result is FALSE: ^[lL]o[0-9.]*$
Result is FALSE: ^[sS]ystem$
```

`Result is FALSE: ^Nu[0-9.]*$`

aby odfiltrować interfejsy loopback i null w większości systemów.

Urządzenia

Lista rodzin urządzeń, dla których dostępne są szablony:

Nazwa szablonu	Dostawca	Rodzina urządzeń	Znane modele	System operacyjny	Używane MIB-y	**Tagi**
Alcatel Timetra TiMOS SNMP	Alcatel	Alcatel Timetra	ALCATEL SR 7750	TiMOS	TIMETRA-SYSTEM-MIB,TIMETRA-CHASSIS-MIB	Certyfikowany
Aruba CX 8300s by SNMP	HPE Aruba Networking	Seria przełączników Aruba CX	Aruba JL636A 8325, Aruba JL717A 8360	Aruba AOS-CX	ARUBAWIRED-FAN-MIB, ARUBAWIRED-POWERSUPPLY-MIB, ARUBAWIRED-SYSTEMINFO-MIB, ARUBAWIRED-TEMPSENSOR-MIB, OSPF-MIB	Certyfikowany
Brocade FC SNMP	Brocade	Przełączniki FC Brocade	Brocade 300 SAN Switch-	-	SW-MIB,ENTITY-MIB	Wydajność Awarie
Brocade_Foundry Stackable SNMP	Brocade	Brocade ICX	Brocade ICX6610, Brocade ICX7250-48, Brocade ICX7450-48F		FOUNDRY-SN-AGENT-MIB, FOUNDRY-SN-STACKING-MIB	Certyfikowany
Brocade_Foundry Nonstackable SNMP	Brocade, Foundry	Brocade MLX, Foundry	Brocade MLXe, Foundry FLS648, Foundry FWSX424		FOUNDRY-SN-AGENT-MIB	Wydajność Awarie
Check Point Next Generation Firewall by SNMP	Check Point	Zapora nowej generacji	-	Gaia	HOST-RESOURCES-MIB, CHECKPOINT-MIB, UCD-SNMP-MIB, SNMPv2-MIB, IF-MIB	Certyfikowany
Ciena 3906 by SNMP	Ciena	Ciena CPE	Ciena 3906	SAOS	WWP-LEOS-BLADE-MIB, WWP-LEOS-CHASSIS-MIB, WWP-LEOS-SYSTEM-CONFIG-MIB	Certyfikowany
Cisco Catalyst 3750<device model> SNMP	Cisco	Cisco Catalyst 3750	Cisco Catalyst 3750V2-24FS, Cisco Catalyst 3750V2-24PS, Cisco Catalyst 3750V2-24TS, Cisco Catalyst SNMP, Cisco Catalyst SNMP		CISCO-MEMORY-POOL-MIB, IF-MIB, EtherLike-MIB, SNMPv2-MIB, CISCO-PROCESS-MIB, CISCO-ENVMON-MIB, ENTITY-MIB	Certyfikowany
Cisco IOS SNMP	Cisco	Cisco IOS wer. > 12.2 3.5	Cisco C2950	IOS	CISCO-PROCESS-MIB,CISCO-MEMORY-POOL-MIB,CISCO-ENVMON-MIB	Certyfikowany

Nazwa szablonu	Dostawca	Rodzina urządzeń	Znane modele	System operacyjny	Używane MIB-y	**Tagi**
Cisco IOS versions 12.0_3_T-12.2_3.5 SNMP	Cisco	Cisco IOS > 12.0 3 T i 12.2 3.5	-	IOS	CISCO-PROCESS-MIB,CISCO-MEMORY-POOL-MIB,CISCO-ENVMON-MIB	Certyfikowany
Cisco IOS prior to 12.0_3_T SNMP	Cisco	Cisco IOS 12.0 3 T	-	IOS	OLD-CISCO-CPU-MIB,CISCO-MEMORY-POOL-MIB	Certyfikowany
D-Link DES_DGS Switch SNMP	D-Link	Przełączniki DES/DGX	D-Link DES-xxxx/DGS-xxxx,DLINK DGS-3420-26SC	-	DLINK-AGENT-MIB,EQUIPMENT-MIB,ENTITY-MIB	Certyfikowany
D-Link DES 7200 SNMP	D-Link	DES-7xxx	D-Link DES 7206	-	ENTITY-MIB,MY-SYSTEM-MIB,MY-PROCESS-MIB,MY-MEMORY-MIB	Wydajność Awarie Interfejsy
Dell Force S-Series SNMP	Dell	Dell Force S-Series	S4810		F10-S-SERIES-CHASSIS-MIB	Certyfikowany
Extreme Exos SNMP	Extreme	Extreme EXOS	X670V-48x	EXOS	EXTREME-SYSTEM-MIB,EXTREME-SOFTWARE-MONITOR-MIB	Certyfikowany
FortiGate by SNMP	Fortinet	FortiGate (NGFW)	-	FortiOS	HOST-RESOURCES-MIB FORTINET-FORTIGATE-MIB FORTINET-CORE-MIB SNMPv2-MIB IF-MIB ENTITY-MIB	Wydajność Inwentarz
HP Comware HH3C SNMP	HP	HP (H3C) Comware	HP A5500-24G-4SFP HI Switch		HH3C-ENTITY-EXT-MIB,ENTITY-MIB	Certyfikowany
HP Enterprise Switch SNMP	HP	HP Enterprise Switch	HP ProCurve J4900B Switch 2626, HP J9728A 2920-48G Switch		STATISTICS-MIB,NETSWITCH-MIB,HP-ICF-CHASSIS,ENTITY-MIB,SEMI-MIB	Certyfikowany
Huawei OceanStor 5300 V5 by SNMP	Huawei	Huawei OceanStor Dorado	Huawei OceanStor Dorado with V5 software		HUAWEI-STORAGE-HARDWARE-MIB, HUAWEI-STORAGE-SPACE-MIB, ISM-PERFORMANCE-MIB, HOST-RESOURCES-MIB, SNMPv2-MIB	Certyfikowany

Nazwa szablonu	Dostawca	Rodzina urządzeń	Znane modele	System operacyjny	Używane MIB-y	**Tagi**
Huawei OceanStor Dorado by SNMP	Huawei	Huawei OceanStor, Huawei OceanStor Dorado	Huawei OceanStor Dorado 3000/5000/6000/8000/18000/5300V5/5500/5600/6800/18500/18800 with V6/V700 software		HUAWEI-STORAGE-HARDWARE-MIB, HUAWEI-STORAGE-SPACE-MIB, ISM-PERFORMANCE-MIB, HOST-RESOURCES-MIB, SNMPv2-MIB	Certyfikowany
Huawei VRP by SNMP	Huawei	Huawei VRP	S2352P-EI		ENTITY-MIB,HUAWEI-ENTITY-EXTENT-MIB	Certyfikowany
Intel_Qlogic Infiniband SNMP	Intel/QLogic	Urządzenia Intel/QLogic Infiniband	Infiniband 12300		ICS-CHASSIS-MIB	Awarie Inwentarz
Juniper SNMP	Juniper	Modele MX,SRX,EX	Juniper MX240, Juniper EX4200-24F	JunOS	JUNIPER-MIB	Certyfikowany
Juniper MX NETCONF	Juniper	Modele MX	Juniper MX204 Edge Router	JunOS 24.2R1-S1.10	*Nie dotyczy (używa NETCONF przez SSH)*	Certyfikowany
Juniper MX SNMP	Juniper	Modele MX	Juniper MX204 Edge Router	JunOS 24.2R1-S1.10	OSPF-MIB, JUNIPER-DOM-MIB, JUNIPER-MIB, BGP4-V2-MIB-JUNIPER, OSPFV3-MIB-JUNIPER	Certyfikowany
Mellanox SNMP	Mellanox	Urządzenia Mellanox Infiniband	SX1036	MLNX-OS	HOST-RESOURCES-MIB,ENTITY-MIB,ENTITY-SENSOR-MIB,MELLANOX-MIB	Certyfikowany

Nazwa szablonu	Dostawca	Rodzina urządzeń	Znane modele	System opera-cyjny	Używane MIB-y	**Tagi**
MikroTik CCR<device model> SNMP	MikroTik	Routery MikroTik Cloud Core (seria CCR)	Dostępne są oddzielne dedykowane szablony dla: MikroTik CCR1009-7G-1C-1S+, MikroTik CCR1009-7G-1C-1S+PC, MikroTik CCR1009-7G-1C-PC, MikroTik CCR1016-12G, MikroTik CCR1016-12S-1S+, MikroTik CCR1036-12G-4S-EM, MikroTik CCR1036-12G-4S, MikroTik CCR1036-8G-2S+, MikroTik CCR1036-8G-2S+EM, MikroTik CCR1072-1G-8S+, MikroTik CCR2004-16G-2S+, MikroTik CCR2004-1G-12S+2XS	RouterOS	MIKROTIK-MIB,HOST-RESOURCES-MIB	Certyfikowany

Nazwa szablonu	Dostawca	Rodzina urządzeń	Znane modele	System opera-cyjny	Używane MIB-y	**Tagi**
MikroTik CRS<device model> SNMP	MikroTik	Przełączniki MikroTik Cloud Router (seria CRS)	Dostępne są oddzielne dedykowane szablony dla: MikroTik CRS106-1C-5S, MikroTik CRS109-8G-1S-2HnD-IN, MikroTik CRS112-8G-4S-IN, MikroTik CRS112-8P-4S-IN, MikroTik CRS125-24G-1S-2HnD-IN, MikroTik CRS212-1G-10S-1S+IN, MikroTik CRS305-1G-4S+IN, MikroTik CRS309-1G-8S+IN, MikroTik CRS312-4C+8XG-RM, MikroTik CRS317-1G-16S+RM, MikroTik CRS326-24G-2S+IN, MikroTik CRS326-24G-2S+RM, MikroTik CRS326-24S+2Q+RM, MikroTik CRS328-24P-4S+RM, MikroTik CRS328-4C-20S-4S+RM, MikroTik CRS354-48G-4S+2Q+RM, MikroTik CRS354-48P-4S+2Q+RM	RouterOS/SwitchOS	MIKROTIK-MIB,HOST-RESOURCES-MIB	Certyfikowany
MikroTik CSS<device model> SNMP	MikroTik	Przełączniki MikroTik Cloud Smart (seria CSS)	Dostępne są oddzielne dedykowane szablony dla: MikroTik CSS326-24G-2S+RM, MikroTik CSS610-8G-2S+IN	RouterOS	MIKROTIK-MIB,HOST-RESOURCES-MIB	Certyfikowany
MikroTik FiberBox SNMP	MikroTik	MikroTik FiberBox	MikroTik FiberBox	RouterOS	MIKROTIK-MIB,HOST-RESOURCES-MIB	Certyfikowany
MikroTik hEX <device model> SNMP	MikroTik	MikroTik hEX	Dostępne są oddzielne dedykowane szablony dla: MikroTik hEX, MikroTik hEX lite, MikroTik hEX PoE, MikroTik hEX PoE lite, MikroTik hEX S	RouterOS	MIKROTIK-MIB,HOST-RESOURCES-MIB	Certyfikowany

Nazwa szablonu	Dostawca	Rodzina urządzeń	Znane modele	System opera-cyjny	Używane MIB-y	**Tagi**
MikroTik netPower <device model> SNMP	MikroTik	MikroTik net-Power	Dostępne są oddzielne dedykowane szablony dla: MikroTik netPower 15FR, MikroTik netPower 16P SNMP, MikroTik netPower Lite 7R	RouterOS/SwitchOS, SwitchOS Lite	MIKROTIK-MIB,HOST-RESOURCES-MIB	Certyfikowany
MikroTik PowerBox <device model> SNMP	MikroTik	MikroTik Power-Box	Dostępne są oddzielne dedykowane szablony dla: MikroTik PowerBox, MikroTik PowerBox Pro	RouterOS	MIKROTIK-MIB,HOST-RESOURCES-MIB	Certyfikowany
MikroTik RB<device model> SNMP	MikroTik	Routery MikroTik serii RB	Dostępne są oddzielne dedykowane szablony dla: MikroTik RB1100AHx4, MikroTik RB1100AHx4 Dude Edition, MikroTik RB2011iL-IN, MikroTik RB2011iL-RM, MikroTik RB2011iLS-IN, MikroTik RB2011UiAS-IN, MikroTik RB2011UiAS-RM, MikroTik RB260GS, MikroTik RB3011UiAS-RM, MikroTik RB4011iGS+RM, MikroTik RB5009UG+S+IN	RouterOS	MIKROTIK-MIB,HOST-RESOURCES-MIB	Certyfikowany
MikroTik SNMP	MikroTik	Urządzenia MikroTik RouterOS	MikroTik CCR1016-12G, MikroTik RB2011UAS-2HnD, MikroTik 912UAG-5HPnD, MikroTik 941-2nD, MikroTik 951G-2HnD, MikroTik 1100AHx2	RouterOS	MIKROTIK-MIB,HOST-RESOURCES-MIB	Certyfikowany

Nazwa szablonu	Dostawca	Rodzina urządzeń	Znane modele	System operacyjny	Używane MIB-y	**Tagi**
Netgear Fastpath SNMP	Netgear	Netgear Fastpath	M5300-28G		FASTPATH-SWITCHING-MIB,FASTPATH-BOXSERVICES-PRIVATE-MIB	Awarie Inwentarz
QTech QSW SNMP	QTech	Urządzenia Qtech	Qtech QSW-2800-28T	-	QTECH-MIB,ENTITY-MIB	Wydajność Inwentarz
Stormshield SNS by SNMP	Stormshield	Zapory Stormshield Network Security (SNS)	SN3100	Stormshield SNS	HOST-RESOURCES-MIB, UCD-SNMP-MIB, STORMSHIELD-ASQ-STATS-MIB, STORMSHIELD-AUTOUPDATE-MIB, STORMSHIELD-HA-MIB, STORMSHIELD-PROPERTY-MIB, STORMSHIELD-HEALTH-MONITOR-MIB, STORMSHIELD-IF-MIB, STORMSHIELD-SYSTEM-MONITOR-MIB, STORMSHIELD-IPSEC-STATS-MIB	Certyfikowany
TP-LINK SNMP	TP-LINK	TP-LINK	T2600G-28TS v2.0		TPLINK-SYSMONITOR-MIB,TPLINK-SYSINFO-MIB	Wydajność Inwentarz
Ubiquiti AirOS SNMP	Ubiquiti	Bezprzewodowe urządzenia Ubiquiti AirOS	NanoBridge,NanoStation,Unifi	AirOS	FROGFOOT-RESOURCES-MIB,IEEE802dot11-MIB	Wydajność
Vyatta Virtual Router by SNMP	Ciena	Vyatta	Vyatta Virtual Router 1908e	Vyatta 1908e	SNMPv2-MIB, HOST-RESOURCES-MIB, UCD-SNMP-MIB, IF-MIB, DISMAN-EVENT-MIB	Wydajność Inwentarz

Projekt szablonów

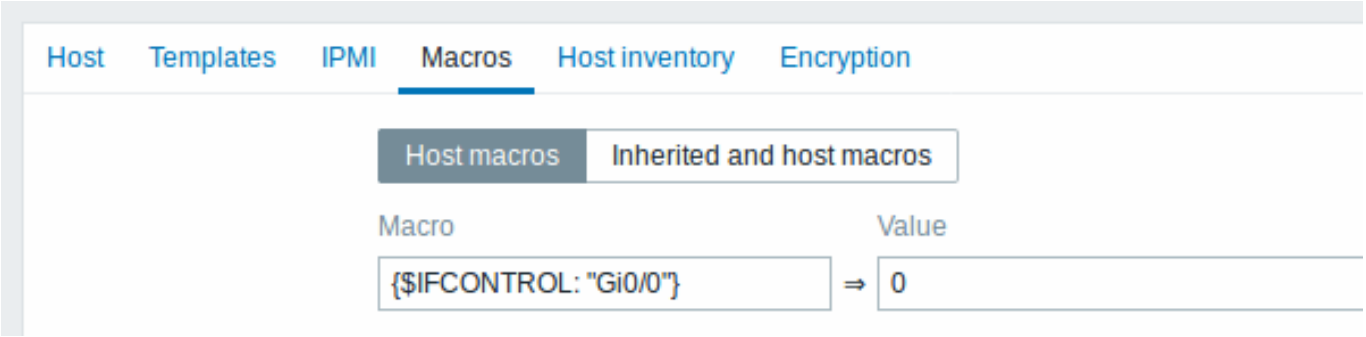
Szablony zostały zaprojektowane z uwzględnieniem następujących założeń:

- Makra użytkownika są używane w możliwie największym zakresie, aby wyzwalacze mogły być dostrajane przez użytkownika;
- Mechanizm wykrywania niskiego poziomu jest używany w możliwie największym zakresie, aby zminimalizować liczbę nieobsługiwanych pozycji;
- Wszystkie szablony zależą od Template ICMP Ping, dzięki czemu wszystkie urządzenia są również sprawdzane przez ICMP;
- Pozycje nie używają żadnych MIB-ów — w pozycjach i regułach wykrywania niskiego poziomu używane są OID-y SNMP. Dzięki temu nie ma potrzeby ładowania żadnych MIB-ów do Zabbix, aby szablony działały;
- Interfejsy sieciowe loopback są filtrowane podczas wykrywania, podobnie jak interfejsy z ifAdminStatus = down(2)
- Tam, gdzie to możliwe, używane są liczniki 64-bitowe z IF-MIB::ifXTable. Jeśli nie są obsługiwane, zamiast nich używane są domyślne liczniki 32-bitowe.

Wszystkie wykryte interfejsy sieciowe mają wyzwalacz monitorujący ich stan operacyjny (link), na przykład:

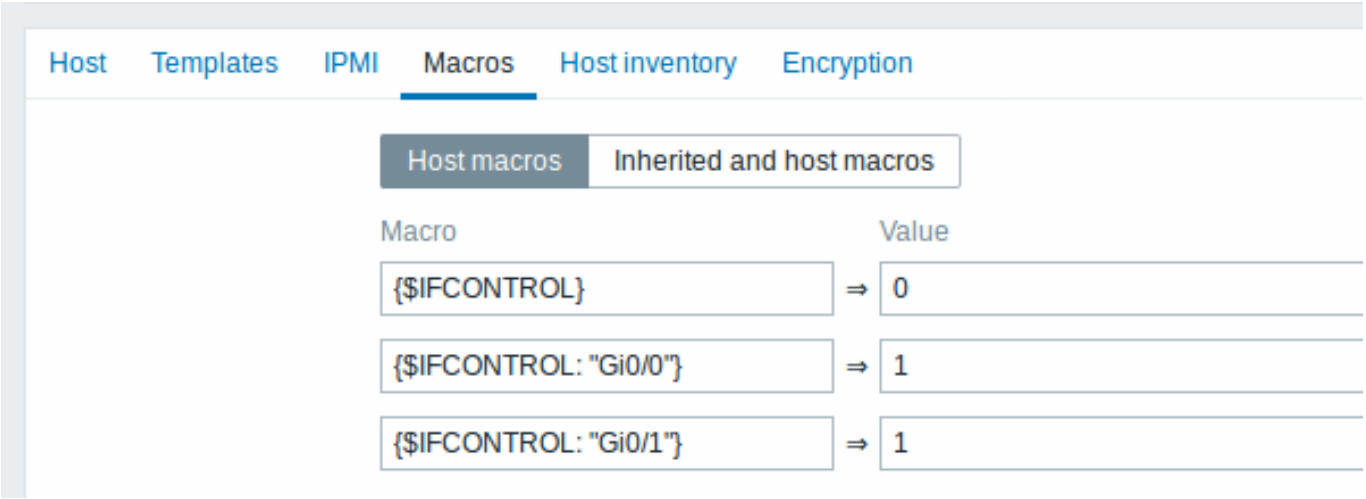
```
{$IFCONTROL:"{#IFNAME}"}=1 and last(/Alcatel Timetra TiMOS SNMP/net.if.status[ifOperStatus.{#SNMPINDEX}])
```

- Jeśli nie chcesz monitorować tego warunku dla określonego interfejsu, utwórz makro użytkownika z kontekstem o wartości 0. Na przykład:



gdzie Gi0/0 to {#IFNAME}. W ten sposób wyzwalacz nie będzie już używany dla tego konkretnego interfejsu.

- Możesz również zmienić domyślne zachowanie wszystkich wyzwalaczy tak, aby się nie uruchamiały, i aktywować ten wyzwalacz tylko dla ograniczonej liczby interfejsów, takich jak uplinki:



Tagi

- Wydajność – MIB-y rodziny urządzeń zapewniają sposób monitorowania pozycji CPU i pamięci;
- Błędy - MIB-y rodziny urządzeń zapewniają sposób monitorowania co najmniej jednego czujnika temperatury;
- Inwentaryzacja – MIB-y rodziny urządzeń zapewniają sposób zbierania co najmniej numeru seryjnego urządzenia i nazwy modelu;
- Certyfikowane – wszystkie trzy główne kategorie powyżej są objęte.

8 Działanie szablonu VMware

Przegląd

Zabbix zawiera szereg gotowych do użycia szablonów do monitorowania maszyn wirtualnych, przeznaczonych dla hiperwizorów VMware vCenter i ESXi. Dostępne szablony są zawarte w dwóch oddzielnych zestawach szablonów:

- VMware - używa danych UUID dla odpowiednich makr
- VMware FQDN - używa danych FQDN dla odpowiednich makr

Szablony przeznaczone do monitorowania hiperwizorów VMware vCenter lub ESXi zawierają wstępnie skonfigurowane reguły wykrywania niskiego poziomu wraz z różnymi wbudowanymi kontrolami do monitorowania instalacji wirtualnych.

Note:
Aby szablon *VMware FQDN* działał poprawnie, każda monitorowana maszyna wirtualna powinna mieć unikalną nazwę systemu operacyjnego zgodną z zasadami FQDN. Dodatkowo na każdej maszynie muszą być zainstalowane VMware Tools/Open Virtual Machine Tools. Jeśli te wymagania wstępne są spełnione, zalecane jest użycie szablonu *VMware FQDN*. Szablon *VMware FQDN* jest dostępny od Zabbix 5.2 wraz z wprowadzeniem możliwości tworzenia hostów z niestandardowymi interfejsami.

 Dostępny jest również klasyczny szablon *VMware*, którego można użyć, jeśli wymagania FQDN nie są spełnione. Jednak szablon *VMware* ma znany problem. Hosty dla wykrytych maszyn wirtualnych są tworzone z nazwami zapisanymi w vCenter (na przykład „VM1”, „VM2” itd.). Jeśli na tych hostach zainstalowany jest agent Zabbix i włączona jest aktywna autorejestracja agent Zabbix, proces autorejestracji odczyta nazwy hostów tak, jak zostały zarejestrowane podczas uruchomienia (na przykład „vm1.example.com”, „vm2.example.com” itd.). Może to prowadzić do tworzenia nowych hostów dla istniejących maszyn wirtualnych (ponieważ nie znaleziono zgodnych nazw), co skutkuje zduplikowanymi hostami o różnych nazwach.

Należy pamiętać:

- Szablon *VMware Hypervisor* może być ręcznie podłączony do hosta, a także używany w wykrywaniu;
- Szablon *VMware Guest* nie powinien być ręcznie podłączany do hosta i może być używany wyłącznie w wykrywaniu.

Konfiguracja makr hosta

Aby używać prostych kontroli VMware, host musi mieć zdefiniowane następujące makra użytkownika:

- {$VMWARE.URL} - adres URL SDK usługi VMware (vCenter lub hiperwizora ESXi) (https://servername/sdk)
- {$VMWARE.USERNAME} - nazwa użytkownika usługi VMware
- {$VMWARE.PASSWORD} - hasło użytkownika {$VMWARE.USERNAME} usługi VMware

10 Powiadomienia o zdarzeniach

Przegląd

Zakładając, że skonfigurowaliśmy już pewne pozycje i wyzwalacze, a teraz otrzymujemy zdarzenia występujące w wyniku zmiany stanu wyzwalaczy, nadszedł czas, aby rozważyć działania.

Na początek nie chcielibyśmy cały czas wpatrywać się w listę wyzwalaczy lub zdarzeń. Znacznie lepiej byłoby otrzymywać powiadomienie, jeśli wydarzyło się coś istotnego (na przykład problem). Ponadto, gdy wystąpią problemy, chcielibyśmy mieć pewność, że wszystkie zainteresowane osoby zostały poinformowane.

Dlatego wysyłanie powiadomień jest jednym z podstawowych działań oferowanych przez Zabbix. Można określić, kto i kiedy powinien zostać powiadomiony o określonym zdarzeniu.

Aby móc wysyłać i odbierać powiadomienia z Zabbix, należy:

- zdefiniować media
- skonfigurować działanie, które wysyła wiadomość do jednego ze zdefiniowanych mediów

Działania składają się z *warunków* i *operacji*. Zasadniczo, gdy warunki są spełnione, wykonywane są operacje. Dwie główne operacje to wysłanie wiadomości (powiadomienia) oraz wykonanie zdalnego polecenia.

W przypadku zdarzeń utworzonych przez wykrywanie i autorejestrację dostępne są dodatkowe operacje. Obejmują one dodawanie lub usuwanie hosta, podłączanie szablonu itp.

1 Typy mediów

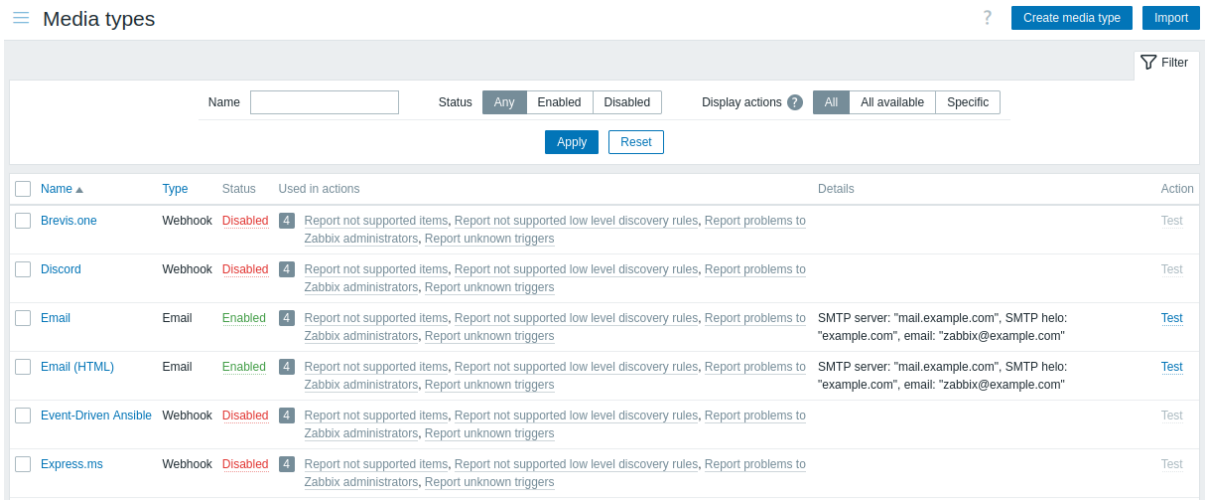
Przegląd

Typy mediów to kanały dostarczania używane do wysyłania powiadomień i alertów z Zabbix.

Typy mediów obsługują następujące metody dostarczania:

- E-mail
- SMS
- Skrypt niestandardowy
- Webhook

Typy mediów są utrzymywane w *Alerty* > *Typy mediów*. Niektóre typy mediów są wstępnie zdefiniowane w domyślnym zestawie danych. Wystarczy dostroić ich parametry, aby zaczęły działać.



Aby zobaczyć, jak typy mediów wpisują się w proces alertowania, przyjrzyjmy się trzem wymaganiom niezbędnym do dostarczania powiadomień z Zabbix do użytkowników końcowych:

1. Musi być zdefiniowana operacja akcji, która wysyła powiadomienia
2. Musi być zdefiniowany działający typ mediów (na przykład *E-mail*, który wysyła alerty przy użyciu SMTP)
3. Szczegóły dostarczania na poziomie użytkownika (takie jak adresy e-mail, numery telefonów itp.) muszą być zdefiniowane w mediach użytkownika

Testowanie typów mediów

Aby sprawdzić, czy skonfigurowany typ mediów działa, kliknij *Test* na liście typów mediów.

Żądanie testowe zostanie wysłane do serwera Zabbix. Serwer Zabbix spróbuje wysłać alert przy użyciu określonego typu mediów i zwróci wynik do frontend. Frontend będzie oczekiwać na zwrócenie wyników przez serwer. Testowanie typów mediów ma domyślnie limit czasu 65 sekund (można go skonfigurować w *Administracja* > *Ogólne* > *Timeouts*).

Zobacz także szczegóły testowania dla:

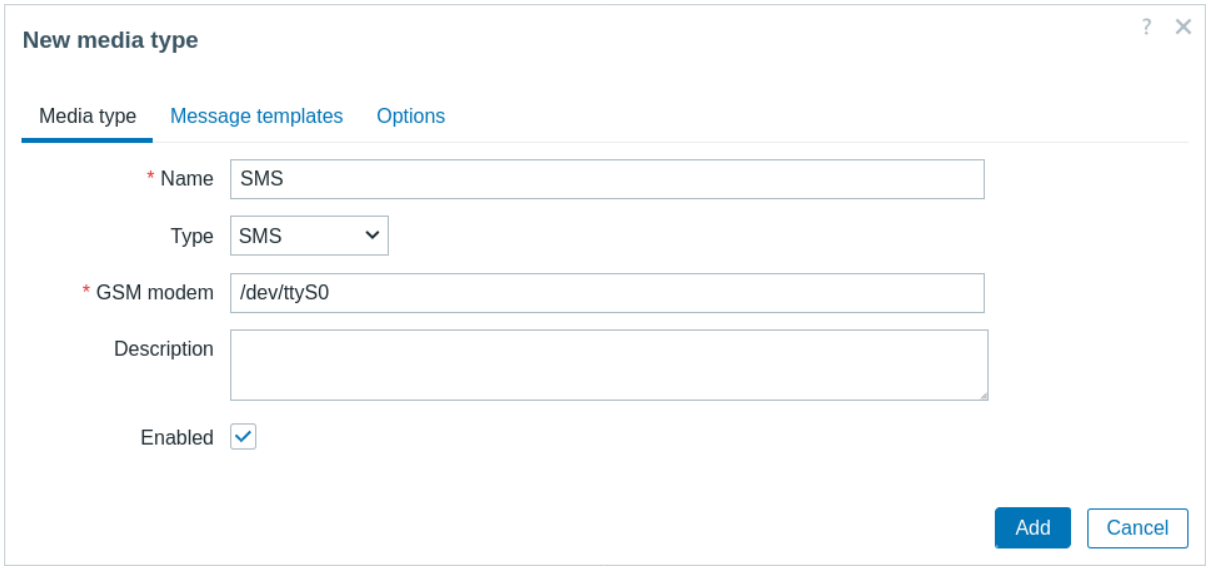
- Email
- Webhook
- Script

Konfiguracja

Aby utworzyć typ nośnika w frontend Zabbix:

- Przejdź do: *Alerty* > *Typy nośników*
- Kliknij *Utwórz typ nośnika*
- Wprowadź parametry typu nośnika w formularzu

Niektóre parametry są **wspólne** dla wszystkich metod dostarczania.

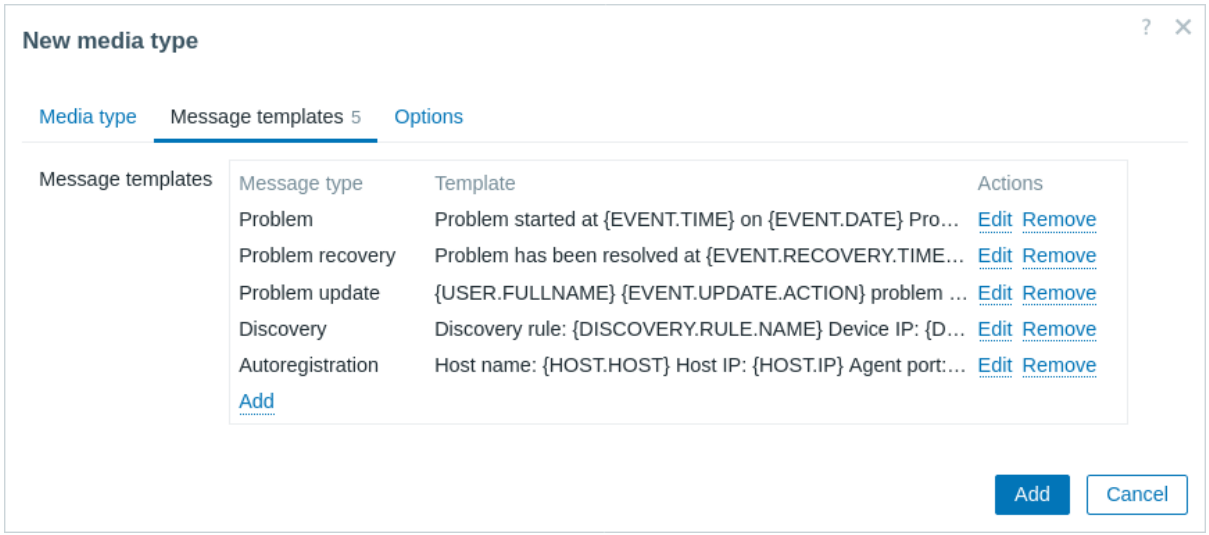


Parametr	Opis
Nazwa	Nazwa typu nośnika.
Typ	Wybierz metodę dostarczania dla typu nośnika.
Opis	Wprowadź opis typu nośnika.
Włączone	Zaznacz pole wyboru, aby włączyć typ nośnika.

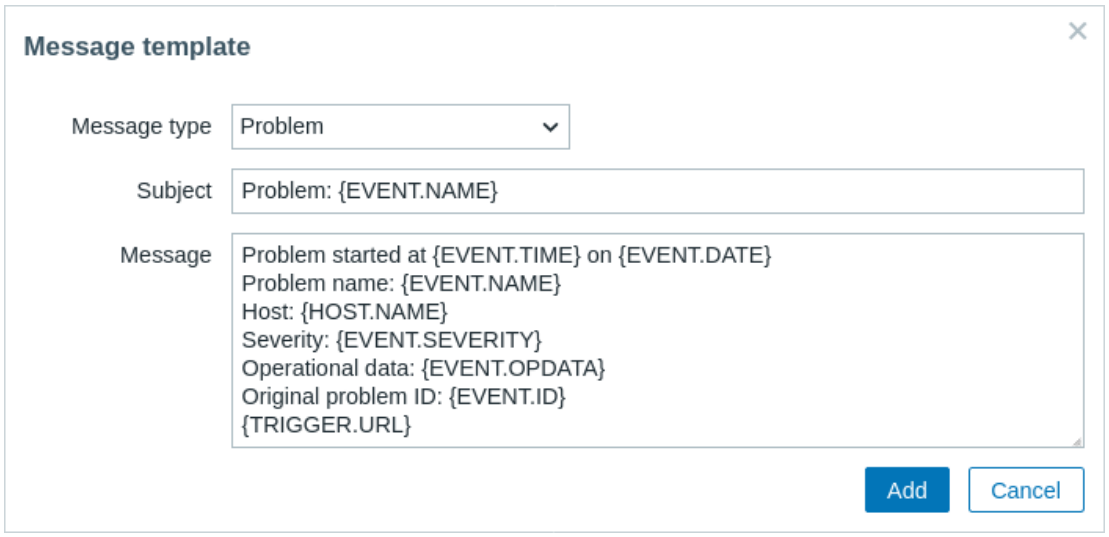
Parametry specyficzne dla danej metody opisano na stronach email, SMS, niestandardowy alertscript lub webhook.

Szablony wiadomości

Zakładka **Szablony wiadomości** zawiera domyślne wiadomości dla każdego typu zdarzenia (problem, odzyskanie po problemie, wykrycie itp.).



Kliknij **Dodaj**, aby zdefiniować domyślną wiadomość (lub **Edytuj**, aby zaktualizować istniejącą wiadomość):



Parametr	Opis
Typ wiadomości	Typ zdarzenia, dla którego ma być używana domyślna wiadomość. Dla każdego typu zdarzenia można zdefiniować tylko jedną domyślną wiadomość.
Temat	Temat domyślnej wiadomości. Temat może zawierać makra. Jest ograniczony do 255 znaków. Temat nie jest dostępny dla typu mediów SMS.
Wiadomość	Domyślna wiadomość. Jej długość jest ograniczona do określonej liczby znaków w zależności od typu bazy danych (więcej informacji znajduje się w Wysyłanie wiadomości). Wiadomość może zawierać obsługiwane makra. W wiadomościach o problemie i aktualizacji problemu obsługiwane są makra wyrażeń (na przykład `{?avg(/host/key,1h)}`).

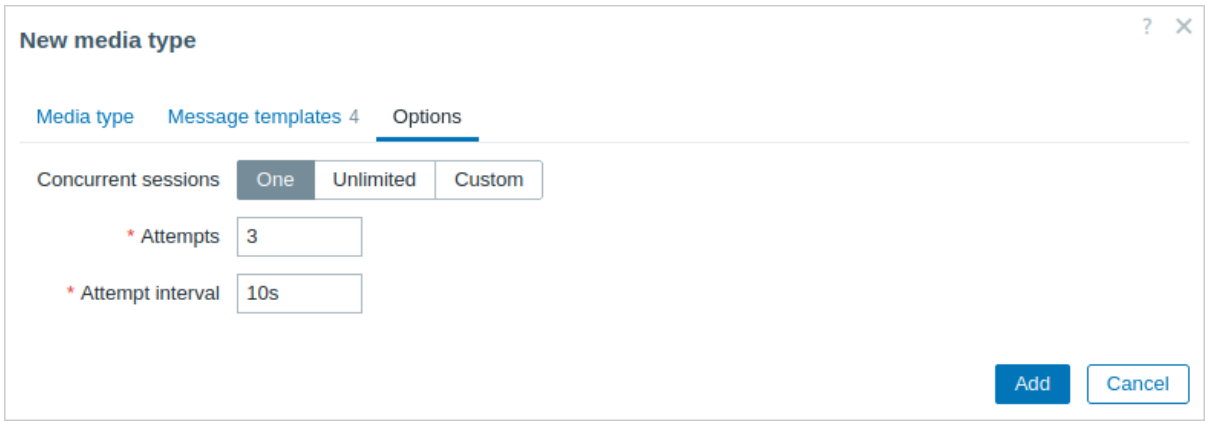
Należy pamiętać, że domyślne wiadomości są zastępowane przez wiadomości niestandardowe, jeśli zostały zdefiniowane w operacjach akcji.

Warning:
Definiowanie szablonów wiadomości jest obowiązkowe dla wszystkich metod dostarczania, w tym webhooków lub niestandardowych skryptów alertów, które nie używają domyślnych wiadomości do powiadomień. Na przykład akcja „Wyślij wiadomość do webhooka Pushover" nie wyśle powiadomień o problemach, jeśli wiadomość o problemie dla webhooka Pushover nie jest zdefiniowana.

Opcje

Zakładka **Opcje** zawiera ustawienia przetwarzania alertów. Ten sam zestaw opcji można skonfigurować dla każdego typu mediów.

Wszystkie typy mediów są przetwarzane równolegle. Maksymalna liczba równoczesnych sesji jest konfigurowalna dla każdego typu mediów, jednak łączna liczba procesów alertera na serwerze może być ograniczona wyłącznie przez parametr StartAlerters. Alerty wygenerowane przez jeden wyzwalacz są przetwarzane sekwencyjnie. Dlatego wiele powiadomień może być przetwarzanych jednocześnie tylko wtedy, gdy zostały wygenerowane przez wiele wyzwalaczy.



Parametr	Opis
Równoczesne sesje	Wybierz liczbę równoległych sesji alertera dla typu mediów: **Jedna** - jedna sesja **Nieograniczona** - nieograniczona liczba sesji **Niestandardowa** - wybierz niestandardową liczbę sesji Nieograniczone/wysokie wartości oznaczają więcej równoległych sesji i zwiększoną wydajność wysyłania powiadomień. Nieograniczone/wysokie wartości powinny być używane w dużych środowiskach, w których może być konieczne jednoczesne wysyłanie wielu powiadomień. Jeśli do wysłania będzie więcej powiadomień niż dostępnych równoczesnych sesji, pozostałe powiadomienia zostaną umieszczone w kolejce; nie zostaną utracone.
Próby	Liczba prób wysłania powiadomienia. Można określić maksymalnie 100 prób; wartość domyślna to „3". Jeśli określono „1", Zabbix wyśle powiadomienie tylko raz i nie będzie ponawiał próby, jeśli wysyłanie się nie powiedzie.
Interwał prób	Częstotliwość ponawiania próby wysłania powiadomienia w przypadku niepowodzenia wysyłania, w sekundach (0-3600). Jeśli określono „0", Zabbix ponowi próbę natychmiast. Obsługiwane są sufiksy czasu, np. 5s, 3m, 1h.

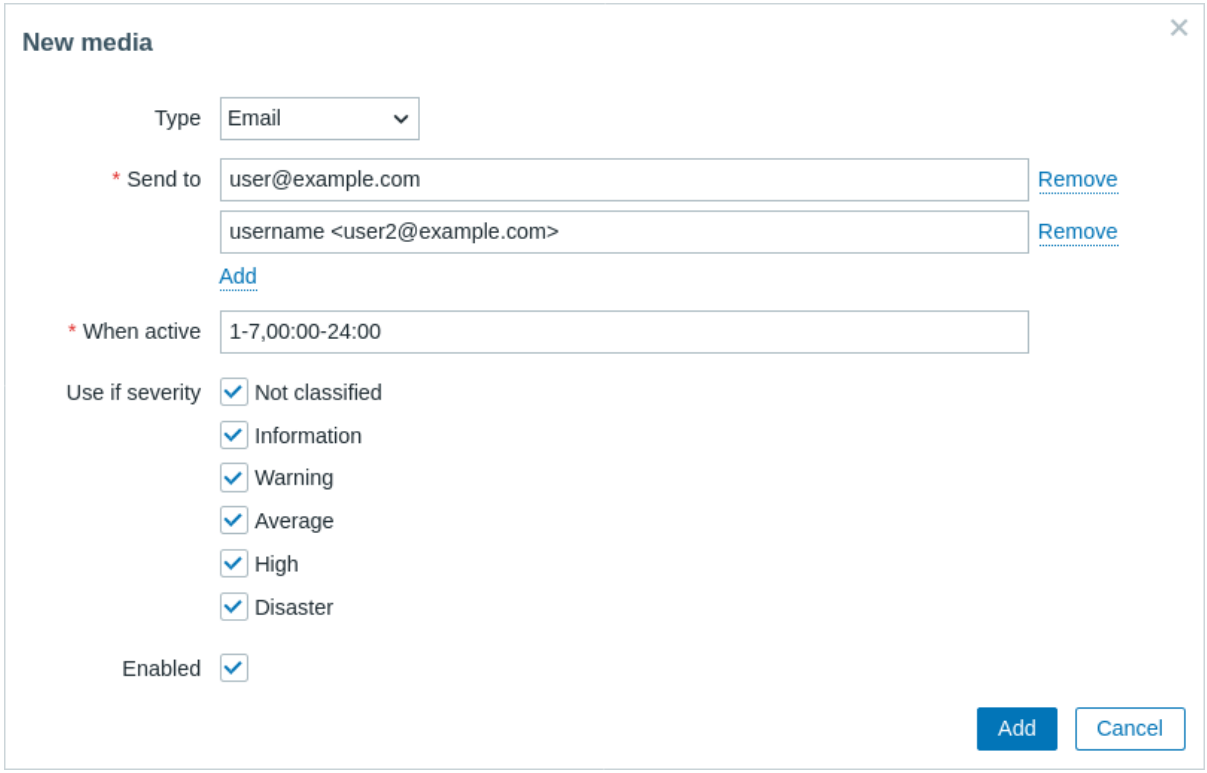
Media użytkownika

Podczas gdy typy mediów określają, **jak** powiadomienie zostanie wysłane, media użytkownika określają, **dokąd** powiadomienie ma zostać wysłane.

Media użytkownika (np. adres e-mail, identyfikator użytkownika webhooka itp.) muszą być zdefiniowane w profilu użytkownika niezależnie od metody dostarczania. Akcja wysyłająca wiadomości do użytkownika *Admin* przy użyciu webhooka *X* nie dostarczy ich, jeśli szczegóły dostarczania webhooka *X* nie są zdefiniowane w profilu użytkownika Admin.

Aby zdefiniować media użytkownika:

- Przejdź do *Users* > *Users* i otwórz formularz właściwości użytkownika (lub przejdź do *User settings* > *Notifications* we własnym profilu użytkownika)
- Kliknij *Add* na karcie Media



Parameter	Description
Type	Lista rozwijana zawiera nazwy włączonych typów mediów. Zwróć uwagę, że podczas edycji medium wyłączonego typu mediów jego typ będzie wyświetlany na czerwono.
Send to	Wprowadź dane kontaktowe, na które mają być wysyłane wiadomości. W przypadku typu mediów e-mail można dodać wiele adresów, klikając przycisk Add poniżej pola adresu. W takim przypadku powiadomienia będą wysyłane na wszystkie wymienione adresy. Przykłady adresów można znaleźć w opisie parametru *Email* dla typu mediów email.
When active	Możesz ograniczyć czas wysyłania wiadomości, na przykład ustawić tylko dni robocze (1-5,09:00-18:00). Zwróć uwagę, że to ograniczenie opiera się na strefie czasowej użytkownika. Jeśli strefa czasowa użytkownika zostanie zmieniona i będzie różna od strefy czasowej systemu, może być konieczne odpowiednie dostosowanie tego ograniczenia, aby nie przeoczyć ważnych wiadomości. Opis formatu znajduje się na stronie Time period specification. Makra użytkownika są obsługiwane.
Use if severity	Zaznacz pola wyboru dla ważności wyzwalaczy, dla których chcesz otrzymywać powiadomienia. *Uwaga*: domyślna ważność ('Not classified') **musi być** zaznaczona, jeśli chcesz otrzymywać powiadomienia o zdarzeniach niezwiązanych z wyzwalaczami. Po zapisaniu wybrane ważności wyzwalaczy będą wyświetlane w odpowiadających im kolorach ważności, a niewybrane zostaną wyszarzone.
Status	Status mediów użytkownika. **Enabled** - używane. **Disabled** - nieużywane.

1 E-mail

Przegląd

Aby skonfigurować e-mail jako kanał dostarczania wiadomości, należy skonfigurować e-mail jako typ mediów i przypisać użytkownikom określone adresy.

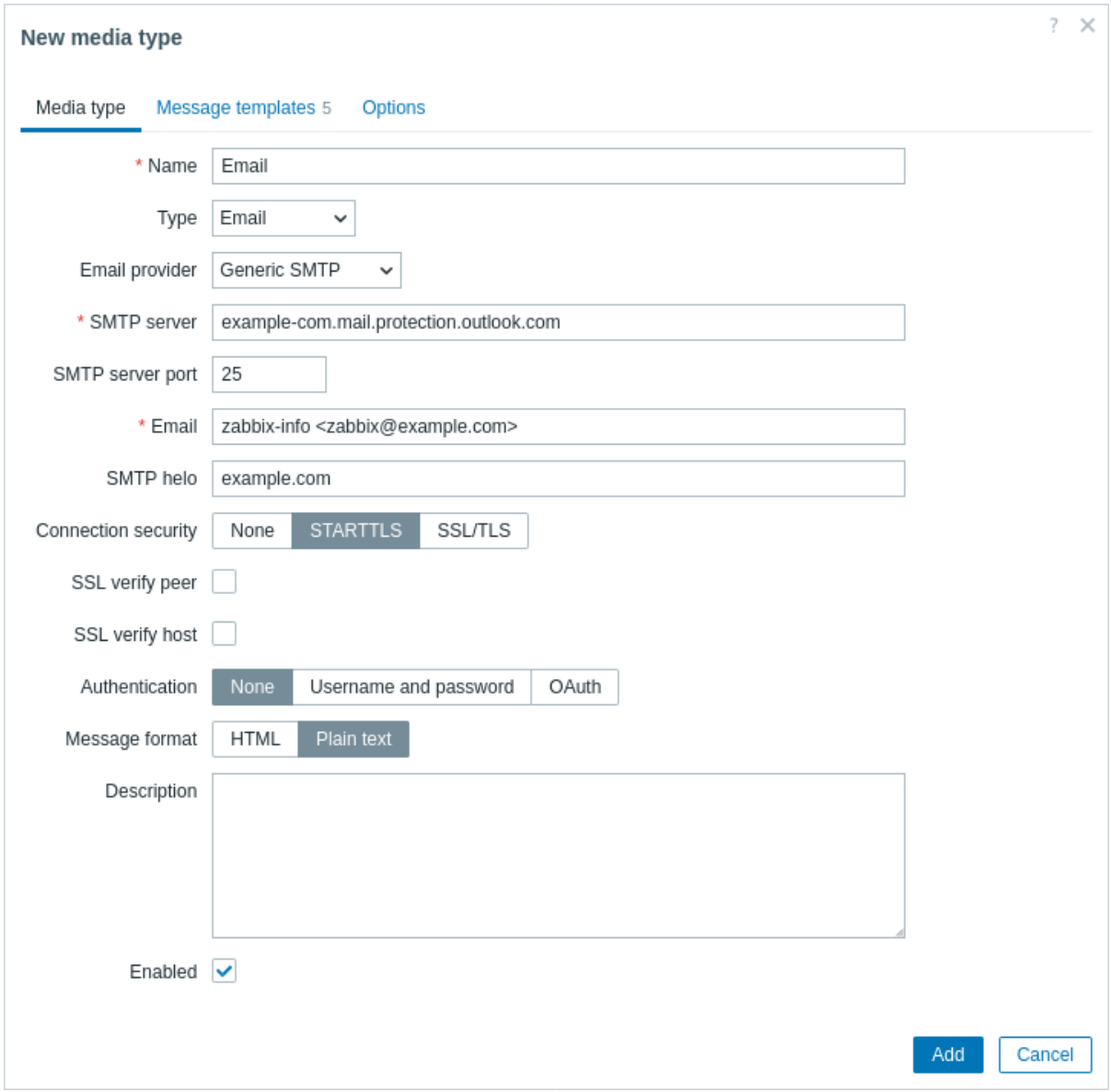
> **Note:**
> Wiele powiadomień dla pojedynczego zdarzenia zostanie zgrupowanych w tym samym wątku e-mail.

Konfiguracja

Aby skonfigurować e-mail jako typ nośnika:

1. Przejdź do *Alerty* > *Typy nośników*.
2. Kliknij *Utwórz typ nośnika* (lub kliknij *Email* na liście predefiniowanych typów nośników).

Zakładka **Typ nośnika** zawiera ogólne atrybuty typu nośnika:



Wszystkie wymagane pola wejściowe są oznaczone czerwoną gwiazdką.

Warning:
Hasło jest eksportowane w postaci jawnego tekstu podczas eksportu konfiguracji typu nośnika e-mail.

Następujące parametry są specyficzne dla typu nośnika e-mail:

Parameter	Description
Email provider	Wybierz dostawcę poczty e-mail: *Generic SMTP*, *Gmail*, *Gmail relay*, *Office365* lub *Office365 relay*. Jeśli wybierzesz opcje związane z Gmail/Office365, wystarczy podać adres e-mail nadawcy i hasło; takie opcje jak *SMTP server*, *SMTP server port*, *SMTP helo* i *Connection security* zostaną automatycznie uzupełnione przez Zabbix. Zobacz także: Automated Gmail/Office365 media types.
SMTP server	Ustaw serwer SMTP do obsługi wiadomości wychodzących. To pole jest dostępne, jeśli jako dostawcę poczty e-mail wybrano *Generic SMTP*.
SMTP server port	Ustaw port serwera SMTP do obsługi wiadomości wychodzących. To pole jest dostępne, jeśli jako dostawcę poczty e-mail wybrano *Generic SMTP*.

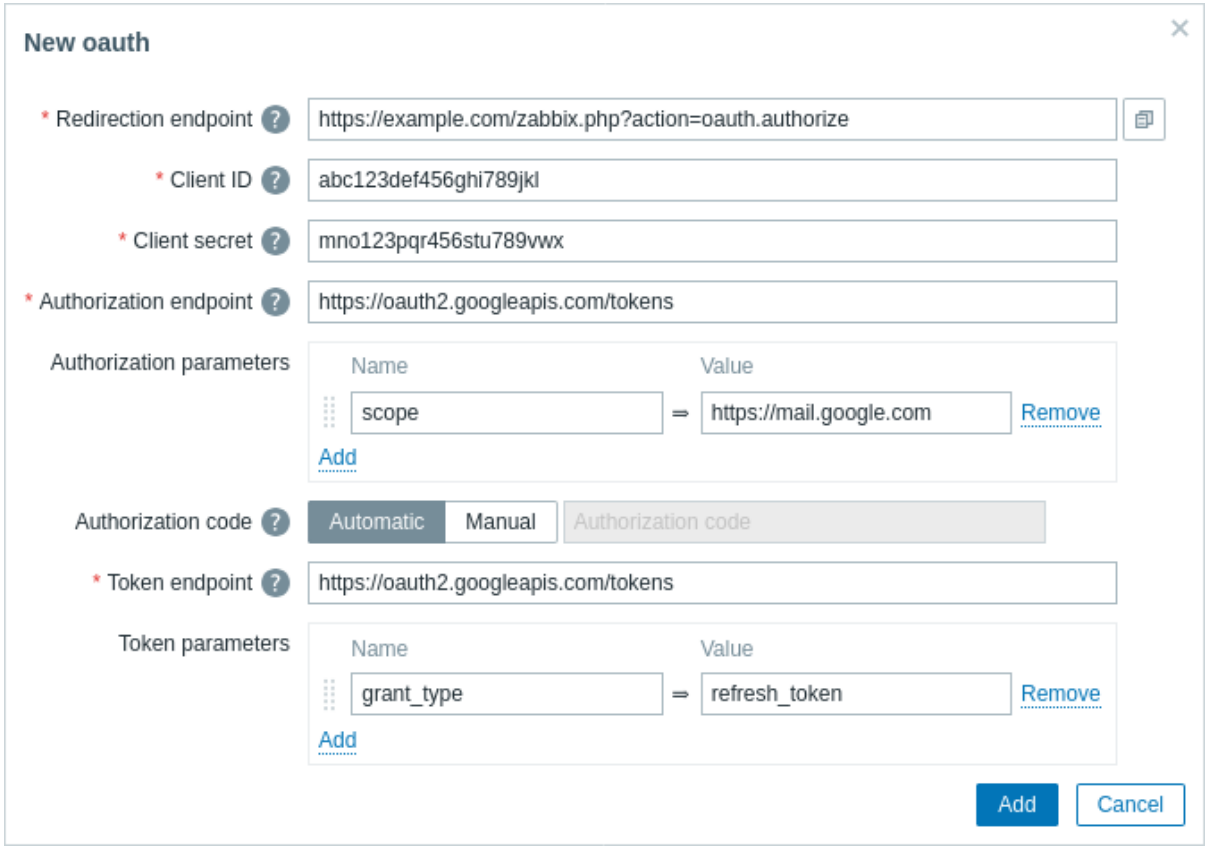
Parameter	Description
Email	Wprowadzony tutaj adres będzie używany jako adres **From** dla wysyłanych wiadomości. Obsługiwane jest dodanie wyświetlanej nazwy nadawcy (takiej jak ”Zabbix_info” w *Zabbix_info <zabbix@company.com>* na powyższym zrzucie ekranu) wraz z rzeczywistym adresem e-mail. W Zabbix obowiązują pewne ograniczenia dotyczące wyświetlanych nazw w wiadomościach e-mail w porównaniu z tym, na co zezwala RFC 5322, co ilustrują poniższe przykłady: Poprawne przykłady: *zabbix@company.com* (tylko adres e-mail, bez potrzeby używania nawiasów ostrych) *Zabbix_info <zabbix@company.com>* (wyświetlana nazwa i adres e-mail w nawiasach ostrych) *∑Ω-monitoring <zabbix@company.com>* (znaki UTF-8 w wyświetlanej nazwie) Niepoprawne przykłady: *Zabbix HQ zabbix@company.com* (obecna wyświetlana nazwa, ale brak nawiasów ostrych wokół adresu e-mail) *”Zabbix\@\<H(comment)Q\>” <zabbix@company.com>* (chociaż jest to poprawne według RFC 5322, pary cytowane i komentarze nie są obsługiwane w wiadomościach e-mail Zabbix)
SMTP helo	Ustaw poprawną wartość SMTP helo, zwykle nazwę domeny. Jeśli pole jest puste, zostanie wysłana nazwa domeny z adresu e-mail (tj. część po @ w polu *Email*). Jeśli nie będzie możliwe pobranie nazwy domeny, zostanie zapisane ostrzeżenie na poziomie debug, a jako domena dla polecenia HELO zostanie wysłana nazwa hosta serwera. To pole jest dostępne, jeśli jako dostawcę poczty e-mail wybrano *Generic SMTP*.
Connection security	Wybierz poziom bezpieczeństwa połączenia: **None** - nie używaj opcji CURLOPT_USE_SSL **STARTTLS** - użyj opcji CURLOPT_USE_SSL z wartością CURLUSESSL_ALL **SSL/TLS** - użycie CURLOPT_USE_SSL jest opcjonalne
SSL verify peer	Zaznacz pole wyboru, aby weryfikować certyfikat SSL serwera SMTP. Wartość dyrektywy konfiguracji serwera ”SSLCALocation” powinna zostać przekazana do CURLOPT_CAPATH w celu walidacji certyfikatu. Ustawia to opcję cURL CURLOPT_SSL_VERIFYPEER.
SSL verify host	Zaznacz pole wyboru, aby zweryfikować, czy pole *Common Name* lub *Subject Alternate Name* certyfikatu serwera SMTP jest zgodne. Ustawia to opcję cURL CURLOPT_SSL_VERIFYHOST.
Authentication	Wybierz poziom uwierzytelniania: **None** - nie są ustawiane żadne opcje cURL **Username and password** - implikuje ”AUTH=*”, pozostawiając wybór mechanizmu uwierzytelniania bibliotece cURL **OAuth** - uwierzytelnianie OAuth Uwierzytelnianie OAuth nie jest obsługiwane dla dostawcy poczty e-mail *Office365 relay*.
Username	Nazwa użytkownika używana do uwierzytelniania. Ustawia wartość CURLOPT_USERNAME. Obsługiwane są makra użytkownika.
Password	Hasło używane do uwierzytelniania. Ustawia wartość CURLOPT_PASSWORD. Obsługiwane są makra użytkownika. Wprowadzona tutaj wartość jest eksportowana w niezmienionej postaci podczas eksportu konfiguracji typu nośnika. Aby uniknąć ujawnienia poufnych danych uwierzytelniających w eksportowanych plikach, użyj makra użytkownika (na przykład `{$EMAIL_SMTP_PASSWORD}`) zamiast jawnego hasła — odwołanie do makra zostanie wyeksportowane, natomiast tajna wartość powinna zostać skonfigurowana (ponownie) w systemie docelowym.
OAuth tokens	Kliknij *Configure*, aby skonfigurować parametry pobierania OAuth tokens w nowym oknie. To pole jest dostępne tylko wtedy, gdy w polu *Authentication* wybrano ”OAuth”.
Message format	Wybierz format wiadomości: **HTML** - wyślij jako HTML **Plain text** - wyślij jako zwykły tekst

Attention:
Aby włączyć uwierzytelnianie SMTP, serwer Zabbix musi zostać skompilowany z opcją compilation `--with-libcurl`, która wymaga biblioteki libcurl (szczegóły dotyczące wersji znajdują się w wymaganiach dla server).

Zobacz także common media type parameters, aby uzyskać szczegółowe informacje o konfigurowaniu domyślnych wiadomości i opcji przetwarzania alertów.

Tokeny OAuth

Do pobrania tokenów OAuth wymagane są następujące parametry:



Parametr	Opis
Punkt końcowy przekierowania	Wprowadź adres URL frontend Zabbix, do którego usługa OAuth przekieruje z powrotem autoryzację OAuth (w formacie `https://<zabbix-frontend-url>/zabbix.php?action=oauth.authorize`). Dla nowego typu nośnika e-mail jest on ustawiany automatycznie, gdy zdefiniowano adres URL frontend.
ID klienta	Wprowadź unikalny identyfikator aplikacji klienckiej zarejestrowanej na serwerze autoryzacji OAuth.
Tajny klucz klienta	Wprowadź prywatny tajny klucz aplikacji klienckiej zarejestrowanej na serwerze autoryzacji OAuth.
Punkt końcowy autoryzacji	Wprowadź adres URL serwera autoryzacji OAuth służący do żądania autoryzacji użytkownika.
Parametry autoryzacji	Wprowadź parametry punktu końcowego autoryzacji.
Kod autoryzacji	Wprowadź kod autoryzacji: **Automatycznie** - kod zostanie pobrany automatycznie za pośrednictwem strony przekierowania **Ręcznie** - wprowadź kod ręcznie, jeśli automatyczne pobranie się nie powiedzie
Punkt końcowy tokenu	Wprowadź adres URL serwera autoryzacji OAuth służący do wymiany kodu autoryzacji na tokeny dostępu i odświeżania.
Parametry tokenu	Wprowadź parametry tokenu dostępu.

Note:
Pobieranie tokenów OAuth ma zautomatyzowane funkcje dla dostawców poczty e-mail **Gmail**, **Gmail relay** i **Office365**. Wymagane jest jedynie podanie wartości parametrów *Punkt końcowy przekierowania*, *ID klienta* i *Tajny klucz klienta*. Zabbix automatycznie uzupełni pozostałe wymagane wartości (zobacz Domyślne adresy URL OAuth według dostawcy).

Pobieranie tokenów dostępu i odświeżania OAuth

Po przesłaniu parametrów OAuth:

1. Otwierane jest wyskakujące okno przeglądarki, które kieruje użytkownika do *punktu końcowego autoryzacji*.
2. Użytkownik autoryzuje Zabbix w usłudze OAuth.

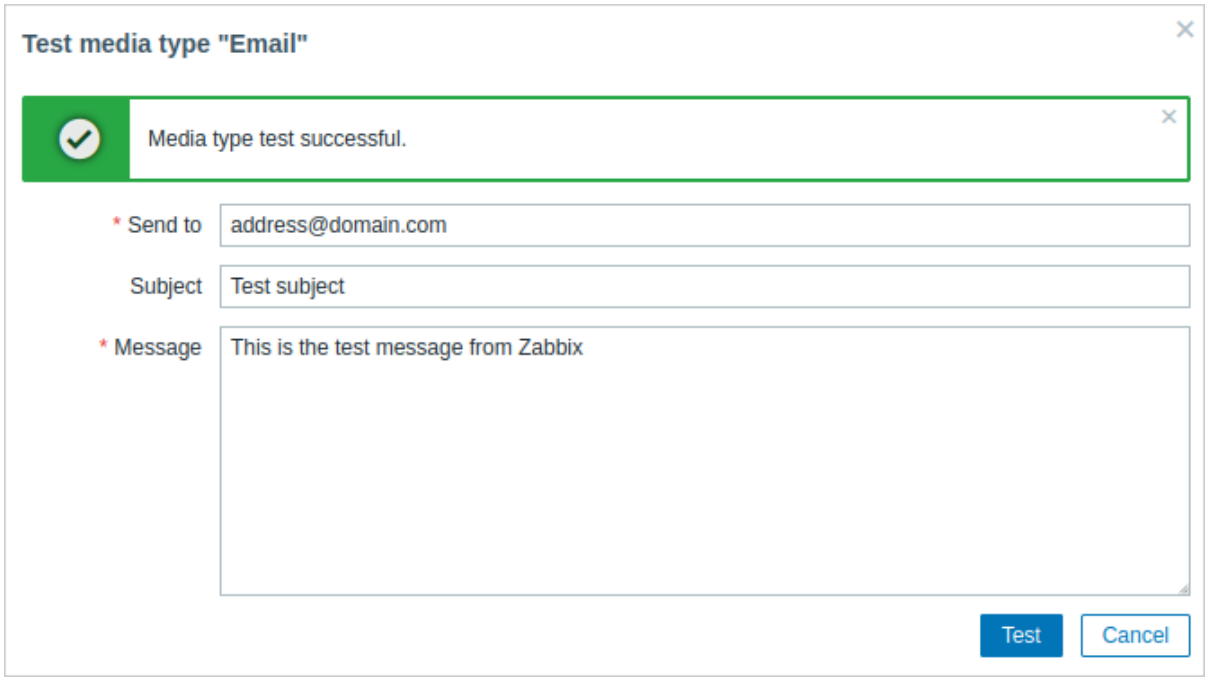
3. Usługa OAuth przekierowuje użytkownika do akcji frontendu Zabbix `oauth.authorize` z kodem autoryzacyjnym i wartością zakresu.
4. W odpowiedzi Zabbix wyśle żądanie do *punktu końcowego tokenu*, aby wymienić kod autoryzacyjny na token dostępu i token odświeżania.

Testowanie

Aby sprawdzić, czy skonfigurowany typ nośnika e-mail działa poprawnie:

1. Znajdź odpowiednią wiadomość e-mail na liście typów nośników.
2. Kliknij *Test* w ostatniej kolumnie listy (otworzy się okno testowania).
3. Wprowadź adres odbiorcy w polu *Send to*, treść wiadomości oraz opcjonalnie temat.
4. Kliknij *Test*, aby wysłać wiadomość testową.

Komunikat o powodzeniu lub niepowodzeniu testu zostanie wyświetlony w tym samym oknie:



Media użytkownika

Po skonfigurowaniu typu mediów e-mail przejdź do sekcji *Użytkownicy* > *Użytkownicy* i edytuj profil użytkownika, aby przypisać użytkownikowi media e-mail. Kroki konfiguracji mediów użytkownika, wspólne dla wszystkich typów mediów, opisano na stronie Typy mediów.

1 Zautomatyzowane typy mediów Gmail/Office365

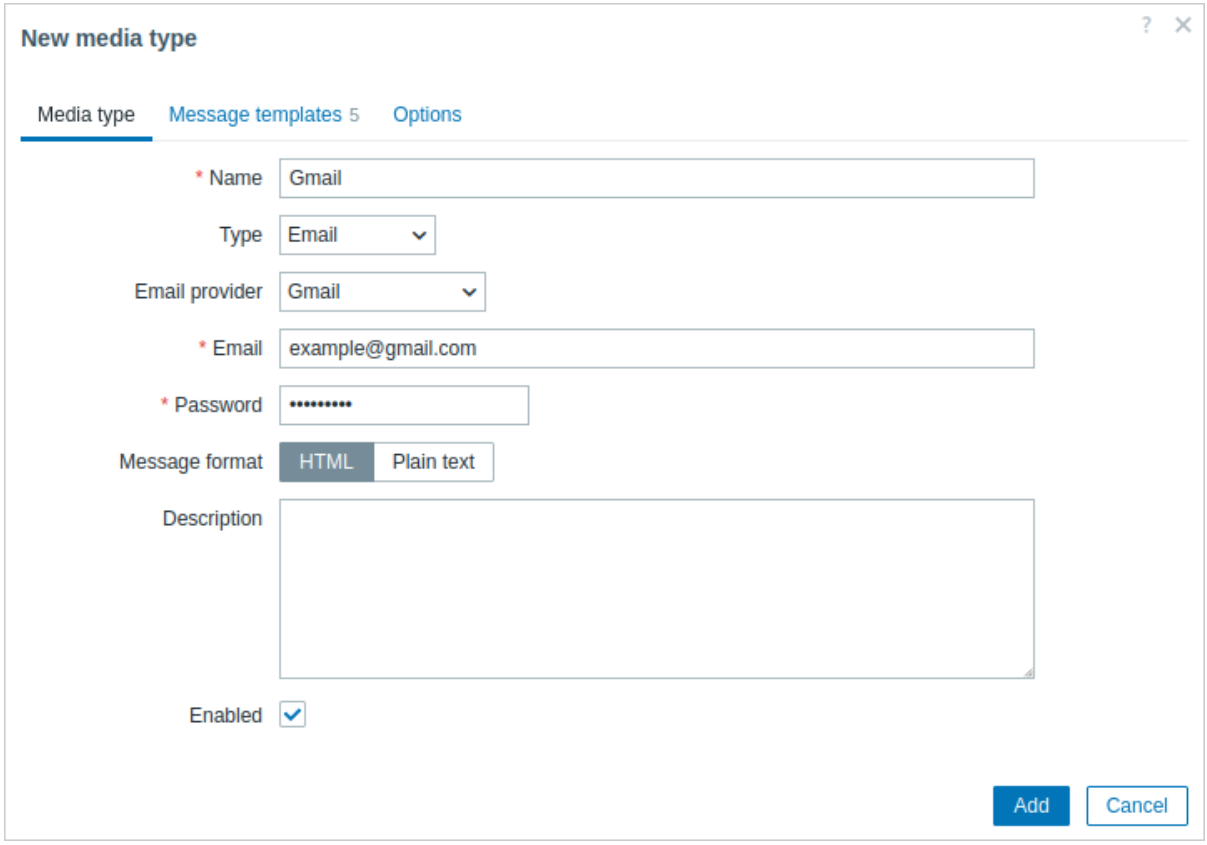
Przegląd

Użytkownicy Gmaila lub Office365 mogą skorzystać z automatycznych funkcji w konfiguracji typu mediów.

Konfiguracja

Pole *Dostawca poczty e-mail* w konfiguracji typu nośnika e-mail umożliwia wybór wstępnie skonfigurowanych opcji dla Gmail i Office 365.

Po wybraniu opcji związanych z Gmail/Office365, aby utworzyć działający typ nośnika, wystarczy podać adres e-mail nadawcy oraz hasło.



Po podaniu adresu e-mail/hasła Zabbix będzie mógł automatycznie uzupełnić wszystkie wymagane ustawienia dla typów nośników Gmail/Office365 rzeczywistymi/zalecanymi wartościami, tj. *Serwer SMTP*, *Port serwera SMTP*, *SMTP helo* oraz *Bezpieczeństwo połączenia*. Ze względu na tę automatyzację pola te nie są nawet wyświetlane, jednak możliwe jest sprawdzenie serwera SMTP i szczegółów wiadomości e-mail na liście typów nośników (zobacz kolumnę *Szczegóły*).

Należy również pamiętać, że:

- Hasło nie jest wymagane dla opcji relay.
- W przypadku relay Office365 nazwa domeny podanego adresu e-mail zostanie użyta do dynamicznego uzupełnienia serwera SMTP (tj. zastąpienia „example.com" w `example-com.mail.protection.outlook.com` rzeczywistą wartością).

Tokeny OAuth

Pobieranie tokenów OAuth ma zautomatyzowane funkcje dla dostawców poczty e-mail *Gmail*, *Gmail relay* i *Office365*.



Konieczne jest podanie jedynie ograniczonego zestawu parametrów do uzyskania dostępu OAuth oraz pobrania tokenu odświeżania — *Redirection endpoint*, *Client ID* i *Client secret*. Zabbix automatycznie uzupełni pozostałe wymagane wartości (zobacz Domyślne adresy URL OAuth według dostawcy).

Należy pamiętać, że możliwe jest również użycie formularza Generic SMTP do skonfigurowania autoryzacji OAuth dla tych dostawców.

Note:
SmtpClientAuthentication musi być włączone albo dla użytkownika/współdzielonej skrzynki pocztowej, albo dla całej dzierżawy w Office365 (domyślnie nie jest włączone).

Domyślne adresy URL OAuth według dostawcy

Poniższa tabela zawiera domyślne wartości adresów URL OAuth i parametrów dla poszczególnych dostawców używane przez Zabbix.

Parametr	Gmail	Office365	Generic SMTP
Punkt końcowy autoryzacji	`https://accounts.google.com/o/oauth2/auth`	`https://login.microsoftonline.com/common/oauth2/v2.0/authori`	Brak wartości domyślnej
scope	`https://mail.google.com`	`https://outlook.office.com/SMTP.Send offline_access`	Brak wartości domyślnej
access_type	`offline`	Nieużywane	Brak wartości domyślnej
prompt	`consent`	Nieużywane	Brak wartości domyślnej
redirect_uri	Wartość pola *Redirection endpoint* jest dodawana automatycznie przez kod. Nie jest wymieniona w parametrach *Authorization endpoint*.		
state	Unikalny hash identyfikujący nośnik aktualizowany tokenem OAuth jest dodawany automatycznie przez kod. Nie jest wymieniony w parametrach *Authorization endpoint*.		
Punkt końcowy tokenu	`https://oauth2.googleapis.com/token`	`https://login.microsoftonline.com/common/oauth2/v2.0/token`	Brak wartości domyślnej
grant_type	`authorization_code`	`authorization_code`	Brak wartości domyślnej
redirect_uri	Wartość pola *Redirection endpoint* jest dodawana automatycznie przez kod. Nie jest wymieniona w parametrach *Token endpoint*.		
state	Unikalny hash identyfikujący nośnik aktualizowany tokenem OAuth jest dodawany automatycznie przez kod. Nie jest wymieniony w parametrach *Token endpoint*.		

Obejście dla kont osobistych Office365

Konta osobiste Office365 nie obsługują ciągów zapytań w adresie URL przekierowania.

Aby obejść ten problem, administrator serwera WWW Apache może dodać następującą regułę przepisywania do pliku `.htaccess`:

```
RewriteEngine On
RewriteRule ^/oauth\.authorize$ /zabbix.php?action=oauth.authorize [QSA,L,PT]
```

Umożliwia to użycie uproszczonego adresu URL przekierowania, takiego jak:

```
http://server-name/zabbix/oauth.authorize
```

zamiast adresu URL z parametrami zapytania, co zapewnia zgodność z kontami osobistymi Office365.

2 SMS

Przegląd

Zabbix obsługuje wysyłanie wiadomości SMS przy użyciu szeregowego modemu GSM podłączonego do portu szeregowego serwera Zabbix.

Upewnij się, że:

- Prędkość urządzenia szeregowego (zwykle /dev/ttyS0 w systemie Linux) odpowiada prędkości modemu GSM. Zabbix nie ustawia prędkości połączenia szeregowego. Używa ustawień domyślnych.
- Użytkownik 'zabbix' ma uprawnienia odczytu/zapisu do urządzenia szeregowego. Uruchom polecenie ls –l /dev/ttyS0, aby sprawdzić bieżące uprawnienia urządzenia szeregowego.
- W modemie GSM wprowadzono kod PIN i jest on zachowywany po ponownym włączeniu zasilania. Alternatywnie możesz wyłączyć kod PIN na karcie SIM. Kod PIN można wprowadzić, wydając polecenie AT+CPIN="NNNN" (NNNN to Twój numer PIN, cudzysłowy muszą być obecne) w programie terminalowym, takim jak Unix minicom lub Windows HyperTerminal.

Zabbix został przetestowany z następującymi modemami GSM:

- Siemens MC35
- Teltonika ModemCOM/G10

Aby skonfigurować SMS jako kanał dostarczania wiadomości, należy również skonfigurować SMS jako typ mediów i wprowadzić odpowiednie numery telefonów dla użytkowników.

Konfiguracja

Aby skonfigurować SMS jako typ nośnika:

- Przejdź do *Alerty* → *Typy nośników*
- Kliknij *Utwórz typ nośnika* (lub kliknij *SMS* na liście predefiniowanych typów nośników).

Następujące parametry są specyficzne dla typu nośnika SMS:

Parameter	Description
Modem GSM	Ustaw nazwę urządzenia szeregowego modemu GSM. Ścieżka wprowadzona tutaj zostanie zweryfikowana względem parametru serwera SMSDevices (jeśli został określony).

Szczegółowe informacje o konfiguracji domyślnych wiadomości i opcji przetwarzania alertów można znaleźć w sekcji wspólne parametry typu nośnika. Należy pamiętać, że równoległe przetwarzanie wysyłania powiadomień SMS nie jest możliwe.

Media użytkownika

Po skonfigurowaniu typu mediów SMS przejdź do sekcji *Użytkownicy* → *Użytkownicy* i edytuj profil użytkownika, aby przypisać użytkownikowi media SMS. Kroki konfiguracji mediów użytkownika, wspólne dla wszystkich typów mediów, są opisane na stronie Typy mediów.

3 Niestandardowe skrypty alertów

Przegląd

Jeśli istniejące typy mediów do wysyłania alertów nie spełniają Twoich oczekiwań, istnieje alternatywny sposób realizacji tego zadania. Możesz utworzyć skrypt, który będzie obsługiwał powiadomienia w wybrany przez Ciebie sposób.

Niestandardowe skrypty alertów są wykonywane na serwerze Zabbix. Skrypty te muszą znajdować się w katalogu określonym przez parametr AlertScriptsPath w pliku konfiguracyjnym serwera.

Oto przykład niestandardowego skryptu alertu:

```
#####!/bin/bash

to=$1
subject=$2
body=$3
host=$4
value=$5

cat <<EOF | mail -s "$subject" "$to"
$body

Host: $host
```

```
Value: $value
EOF
```

Attention:
Zabbix sprawdza kod zakończenia wykonywanych poleceń i skryptów. Każdy kod zakończenia różny od **0** jest traktowany jako błąd wykonania polecenia. W takich przypadkach Zabbix podejmie próbę ponowienia nieudanego wykonania.

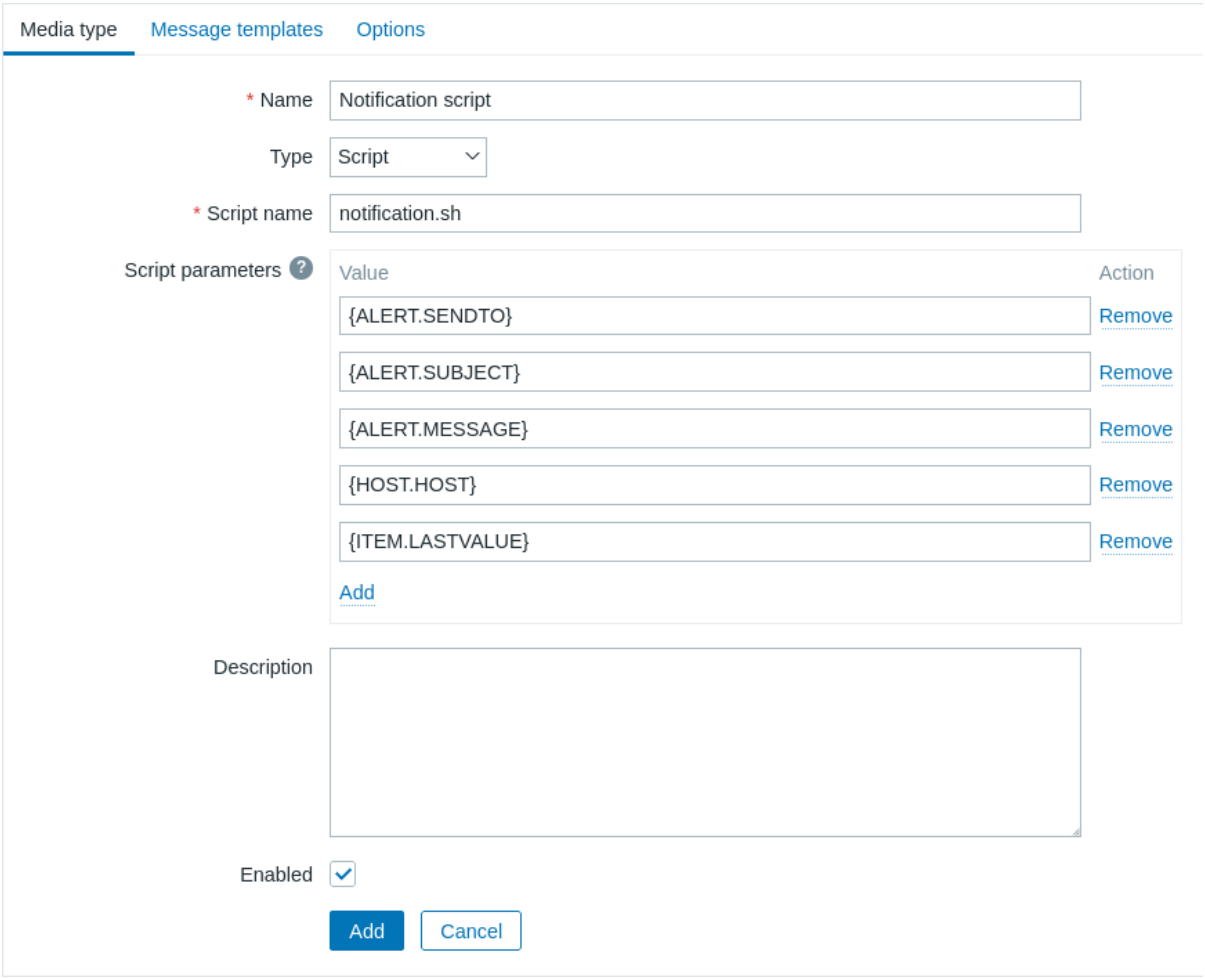
Zmienne środowiskowe nie są zachowywane ani tworzone dla skryptu, dlatego należy obsłużyć je jawnie.

Konfiguracja

Aby skonfigurować niestandardowe skrypty alertów jako typ nośnika:

1. Przejdź do *Alerty → Typy nośników*.
2. Kliknij *Utwórz typ nośnika*.

Zakładka **Typ nośnika** zawiera ogólne atrybuty typu nośnika:



Wszystkie wymagane pola wejściowe są oznaczone czerwoną gwiazdką.

Następujące parametry są specyficzne dla typu nośnika skryptowego:

Parameter	Description
Nazwa skryptu	Wprowadź nazwę pliku skryptu (np. notification.sh), który znajduje się w katalogu określonym w parametrze konfiguracji serwera AlertScriptsPath.
Parametry skryptu	Dodaj opcjonalne parametry skryptu, które zostaną przekazane do skryptu jako argumenty wiersza poleceń w kolejności, w jakiej zostały zdefiniowane. Parametry skryptu obsługują makra {ALERT.SENDTO}, {ALERT.SUBJECT}, {ALERT.MESSAGE} oraz wszystkie makra obsługiwane w powiadomieniach, a także makra użytkownika.

Szczegółowe informacje o konfiguracji domyślnych wiadomości i opcji przetwarzania alertów można znaleźć w sekcji wspólne parametry typu nośnika.

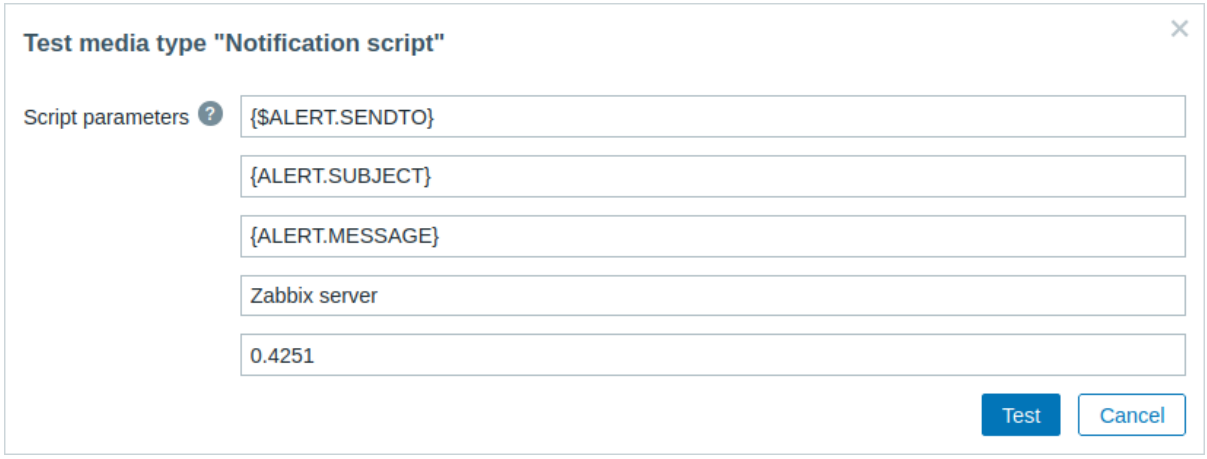
Warning:
Nawet jeśli skrypt alertu nie używa domyślnych wiadomości, szablony wiadomości dla typów operacji używanych przez ten typ nośnika nadal muszą być zdefiniowane. W przeciwnym razie powiadomienie nie zostanie wysłane.

Attention:
Jeśli skonfigurowano więcej niż jeden typ nośnika skryptowego, skrypty te mogą być przetwarzane równolegle przez procesy alertera. Łączna liczba procesów alertera jest ograniczona przez parametr pliku konfiguracyjnego serwera `StartAlerters`.

Testowanie

Aby przetestować skonfigurowany skryptowy typ nośnika:

1. Odszukaj odpowiedni skrypt na liście typów nośników.
2. Kliknij *Test* w ostatniej kolumnie listy; formularz testowy otworzy się w wyskakującym oknie. Formularz testowy będzie zawierał taką samą liczbę parametrów, jaka jest skonfigurowana dla skryptowego typu nośnika.
3. W razie potrzeby edytuj wartości parametrów skryptu. Edycja wpływa tylko na procedurę testową; rzeczywiste wartości nie zostaną zmienione.
4. Kliknij *Test*.



Note:
Podczas testowania skonfigurowanego skryptowego typu nośnika makra {ALERT.SENDTO}, {ALERT.SUBJECT}, {ALERT.MESSAGE} oraz makra użytkownika zostaną rozwinięte do swoich wartości, ale makra powiązane ze zdarzeniami (np. {HOST.HOST}, {ITEM.LASTVALUE} itd.) nie zostaną rozwinięte, ponieważ podczas testu nie ma powiązanego zdarzenia, z którego można pobrać szczegóły. Zwróć uwagę, że makra wewnątrz makr {ALERT.SUBJECT} i {ALERT.MESSAGE} również nie zostaną rozwinięte. Na przykład, jeśli wartość {ALERT.SUBJECT} ma postać "Problem: {EVENT.NAME}", to makro {EVENT.NAME} nie zostanie rozwinięte.

Media użytkownika

Po skonfigurowaniu typu mediów przejdź do sekcji *Użytkownicy* → *Użytkownicy* i edytuj profil użytkownika, przypisując temu użytkownikowi ten typ mediów. Kroki konfiguracji mediów użytkownika, wspólne dla wszystkich typów mediów, opisano na stronie Typy mediów.

Należy pamiętać, że podczas definiowania mediów użytkownika pole *Wyślij do* nie może być puste. Jeśli to pole nie jest używane w skrypcie alertu, wprowadź dowolną kombinację obsługiwanych znaków, aby obejść wymagania walidacji.

4 Webhook

Przegląd

Typ nośnika webhook jest przydatny do wykonywania wywołań HTTP przy użyciu niestandardowego kodu JavaScript w celu łatwej integracji z zewnętrznym oprogramowaniem, takim jak systemy helpdesk, czaty lub komunikatory. Możesz wybrać import integracji dostarczonej przez Zabbix lub utworzyć własną integrację od podstaw.

Integracje

Dostępne są następujące integracje, umożliwiające użycie predefiniowanych typów mediów webhook do wysyłania powiadomień Zabbix do:

- brevis.one
- Discord
- Event-Driven Ansible
- Express.ms messenger
- GitHub
- GLPi
- IBM Maximo Service Request
- iLert
- iTop
- Jira
- Jira Service Management
- ManageEngine ServiceDesk
- Mantis Bug Tracker
- Mattermost
- MS Teams
- MS Teams Workflows
- LINE
- Opsgenie
- OTRS CE
- Pagerduty
- Pushover
- Redmine
- Rocket.Chat
- ServiceNow
- SIGNL4
- Slack
- SolarWinds
- SysAid
- Telegram
- TOPdesk
- VictorOps
- Zammad
- Zendesk

Note:
Oprócz usług wymienionych tutaj, Zabbix można zintegrować również z **Spiceworks** (webhook nie jest wymagany). Aby przekształcać powiadomienia Zabbix w zgłoszenia Spiceworks, utwórz typ mediów e-mail i wprowadź adres e-mail helpdesku Spiceworks (np. help@zabbix.on.spiceworks.com) w ustawieniach profilu wyznaczonego użytkownika Zabbix.

Konfiguracja

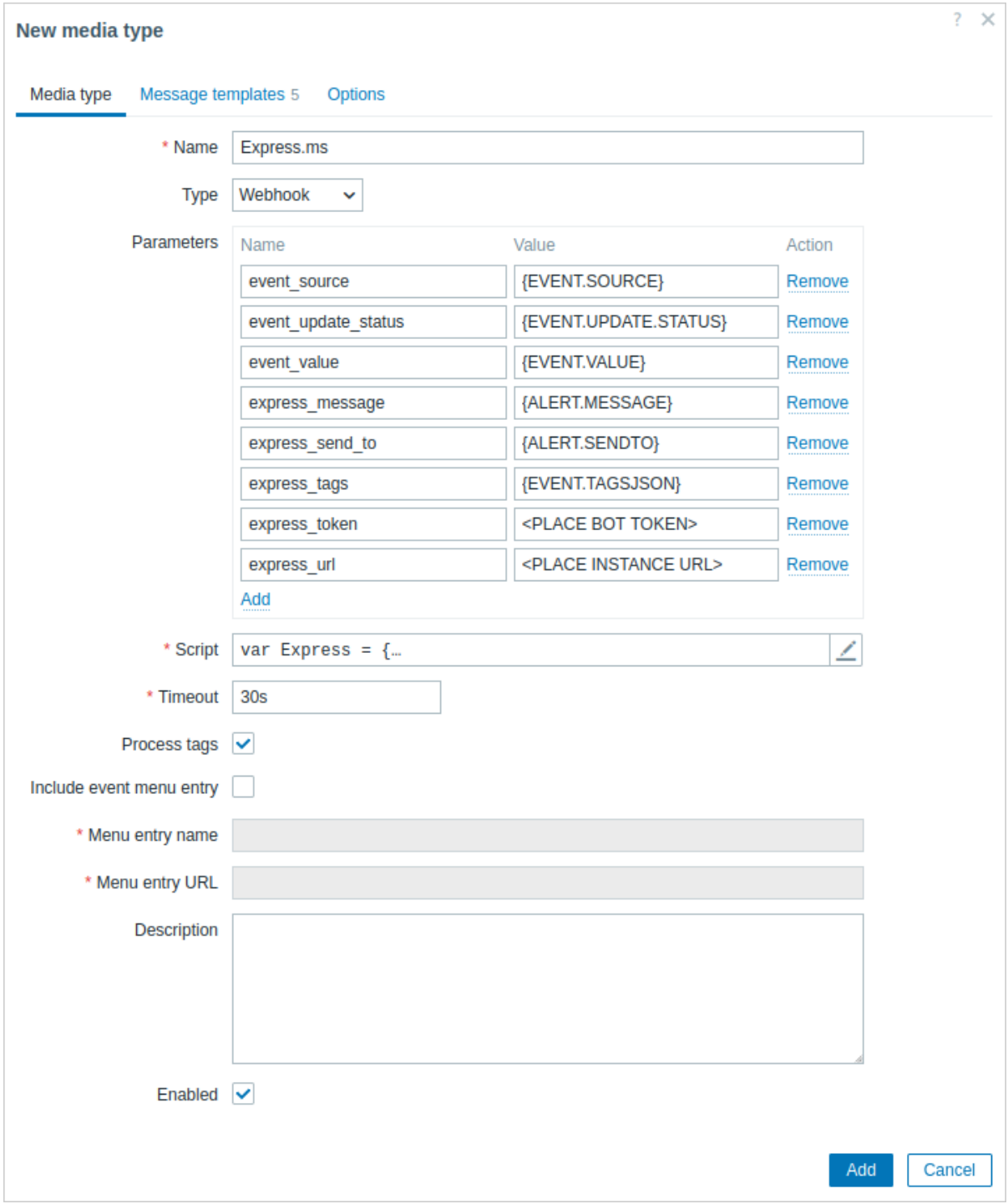
Aby rozpocząć korzystanie z integracji webhook:

1. Odszukaj wymagany plik .yaml w katalogu `templates/media` pobranej wersji Zabbix lub pobierz go z repozytorium git Zabbix.
2. Zaimportuj plik do swojej instalacji Zabbix. Webhook pojawi się na liście typów mediów.
3. Skonfiguruj webhook zgodnie z instrukcjami w pliku *Readme.md* (możesz kliknąć nazwę webhooka powyżej, aby szybko przejść do pliku *Readme.md*).

Aby utworzyć własny webhook od podstaw:

1. Przejdź do *Alerty* > *Typy mediów*.
2. Kliknij *Utwórz typ mediów*.

Zakładka **Typ mediów** zawiera różne atrybuty specyficzne dla tego typu mediów:



Wszystkie obowiązkowe pola wejściowe są oznaczone czerwoną gwiazdką.

Następujące parametry są specyficzne dla typu mediów webhook:

Parametr	Opis
Parametry	Określ zmienne webhooka jako pary atrybut-wartość. W przypadku wstępnie skonfigurowanych webhooków lista parametrów różni się w zależności od usługi. Opis parametrów znajdziesz w pliku *Readme.md* webhooka. W przypadku nowych webhooków domyślnie uwzględnionych jest kilka wspólnych zmiennych (URL:<empty>, HTTPProxy:<empty>, To:{ALERT.SENDTO}, Subject:{ALERT.SUBJECT}, Message:{ALERT.MESSAGE}); możesz je zachować lub usunąć. Parametry webhooka obsługują makra użytkownika, wszystkie makra obsługiwane w powiadomieniach o problemach oraz dodatkowo makra {ALERT.SENDTO}, {ALERT.SUBJECT} i {ALERT.MESSAGE}. Jeśli określisz proxy HTTP, pole obsługuje tę samą funkcjonalność co pole HTTP proxy w konfiguracji pozycji. Ciąg proxy może być poprzedzony prefiksem `[scheme]://`, aby określić, jaki rodzaj proxy jest używany (np. https, socks4, socks5; zobacz documentation).
Script	Wprowadź kod JavaScript w modalnym edytorze, który otwiera się po kliknięciu w pole parametru lub ikonę ołówka obok niego. Ten kod wykona operację webhooka. Skrypt jest kodem funkcji, który przyjmuje pary parametr-wartość. Wartości należy przekonwertować na obiekty JSON za pomocą metody JSON.parse(), na przykład: `var params = JSON.parse(value);`. Kod ma dostęp do wszystkich parametrów, może wykonywać żądania HTTP GET, POST, PUT i DELETE, obsługuje dodatkowe metody, takie jak CONNECT, PATCH, HEAD, OPTIONS i TRACE, oraz zapewnia kontrolę nad nagłówkami HTTP i treścią żądania. Skrypt musi zawierać operator return, w przeciwnym razie nie będzie prawidłowy. Może zwracać status OK wraz z opcjonalną listą tagów i wartości tagów (zobacz opcję *Przetwarzaj tagi*) albo ciąg błędu. Zdarzenia odzyskania (niezależnie od tego, czy zostały wygenerowane automatycznie, czy w wyniku ręcznego zamknięcia) są tworzone przez serwer i zawierają rozwiązane tagi zdarzenia (w tym tagi dziedziczone z szablonów, hostów i wyzwalaczy). Skrypty webhook są wykonywane po utworzeniu alertu; dlatego tagi zwrócone przez skrypt webhooka są dodawane dopiero po początkowym utworzeniu alertu i nie będą obecne w makrach {EVENT.TAGS} oraz {EVENT.RECOVERY.TAGS} początkowej wiadomości o problemie ani wiadomości o natychmiastowym odzyskaniu. *Uwaga*: Zaleca się używanie zmiennych lokalnych (np. `var local = 1`) zamiast globalnych (np. `global = 1`), aby zapewnić, że każdy skrypt operuje na własnych danych, i uniknąć kolizji między równoczesnymi wywołaniami (zobacz known issues). Zobacz także: Webhook development guidelines, Przykłady skryptów webhook, Dodatkowe obiekty JavaScript.
Timeout	Limit czasu wykonania JavaScript (1-60s, domyślnie 30s). Obsługiwane są sufiksy czasu, np. 30s, 1m.
Process tags	Zaznacz pole wyboru, aby przetwarzać zwrócone wartości właściwości JSON jako tagi. Tagi te są dodawane do wszystkich istniejących tagów problemu. Zwróć uwagę, że przy użyciu tagów webhook webhook musi zwrócić obiekt JSON zawierający co najmniej pusty obiekt tags: `var result = {tags: {}};` Przykłady tagów, które mogą zostać zwrócone: *jira-id:prod-1234*, *responsible:John Smith*, *processed:<no value>*
Include event menu entry	Zaznacz pole wyboru, aby dodać wpis w menu zdarzenia prowadzący do utworzonego zewnętrznego zgłoszenia. Wpis zostanie dodany dla każdego webhooka, który jest włączony i ma zaznaczone to pole wyboru. Zwróć uwagę, że jeśli parametry *Menu entry name* i *Menu entry URL* zawierają jakiekolwiek makra {EVENT.TAGS.<tag name>}, wpis zostanie dodany tylko wtedy, gdy te makra będzie można rozwiązać (to znaczy, gdy zdarzenie ma zdefiniowane te tagi). Jeśli opcja jest zaznaczona, webhook nie powinien być używany do wysyłania powiadomień do różnych użytkowników (rozważ zamiast tego utworzenie dedykowanego użytkownika) i nie powinien być używany w wielu akcjach alertów dla pojedynczego zdarzenia problemu.
Menu entry name	Określ nazwę wpisu menu. Obsługiwane jest makro {EVENT.TAGS.<tag name>}. To pole jest obowiązkowe tylko wtedy, gdy zaznaczono *Include event menu entry*.

Parametr	Opis
Menu entry URL	Określ bazowy adres URL wpisu menu. Obsługiwane jest makro {EVENT.TAGS.<tag name>}. To pole jest obowiązkowe tylko wtedy, gdy zaznaczono *Include event menu entry*.

Zobacz wspólne parametry typu mediów, aby uzyskać szczegółowe informacje o konfigurowaniu domyślnych wiadomości i opcji przetwarzania alertów.

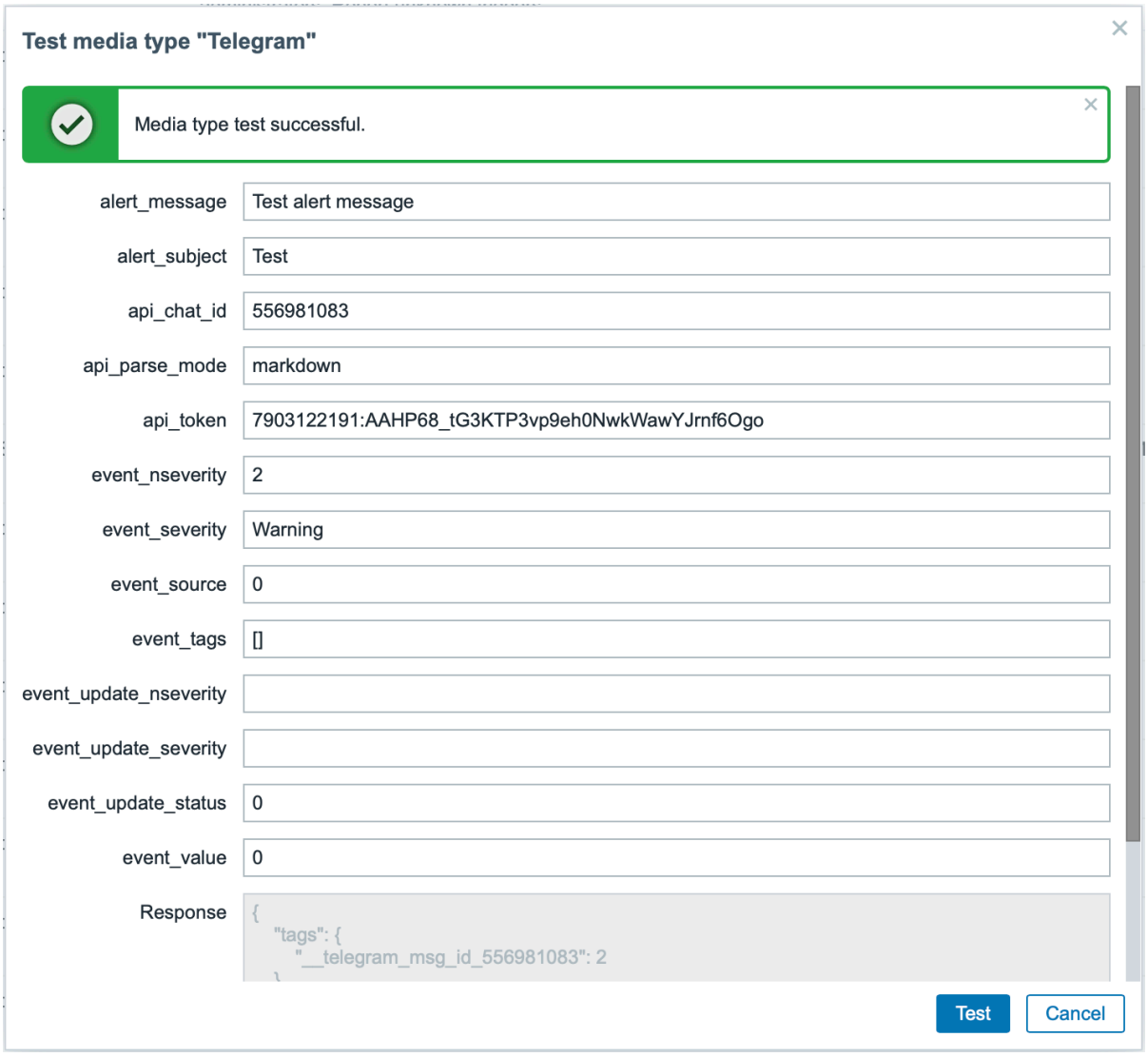
Warning:
Nawet jeśli webhook nie używa domyślnych wiadomości, szablony wiadomości dla typów operacji używanych przez ten webhook nadal muszą być zdefiniowane.

Testowanie

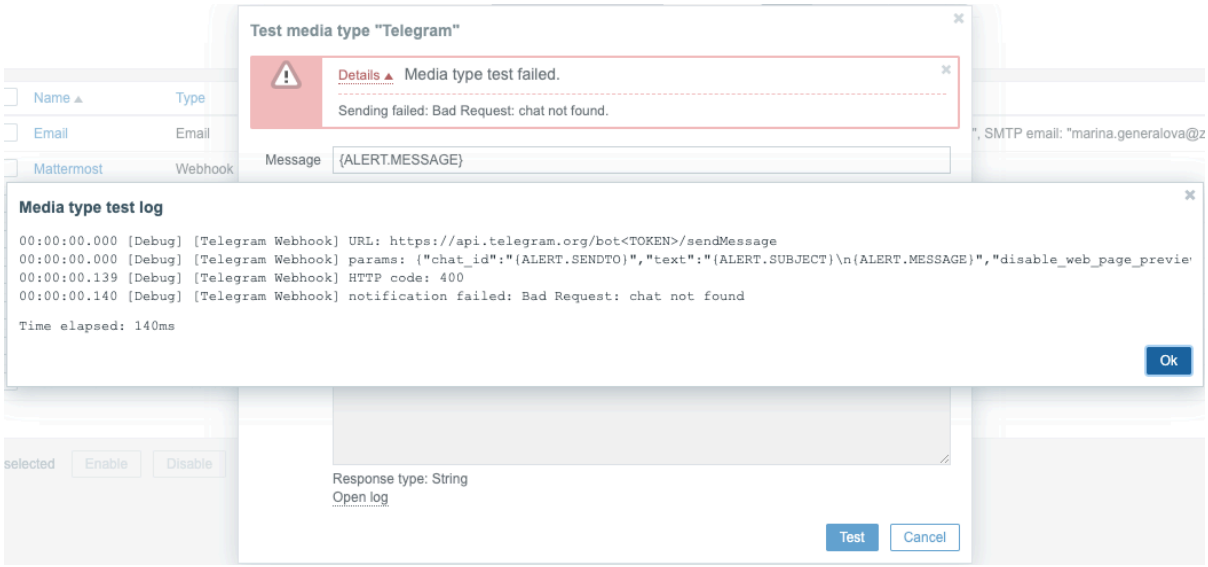
Aby przetestować skonfigurowany typ nośnika webhook:

1. Znajdź odpowiedni webhook na liście typów nośników.
2. Kliknij *Test* w ostatniej kolumnie listy (otworzy się okno testowania).
3. W razie potrzeby edytuj wartości parametrów webhooka. Zastąp makra przykładowymi wartościami; w przeciwnym razie makra nie zostaną rozwinięte, a test zakończy się niepowodzeniem.
4. Kliknij *Test*.

Zastąpienie lub usunięcie wartości w oknie testowania wpływa tylko na procedurę testową; rzeczywiste wartości atrybutów webhooka pozostaną bez zmian.



Aby wyświetlić wpisy dziennika testu typu nośnika bez opuszczania okna testowego, kliknij *Open log* (otworzy się nowe wyskakujące okno).



Jeśli test webhooka zakończy się powodzeniem:

- Wyświetlany jest komunikat *„Media type test successful.”*.
- Odpowiedź serwera pojawia się w szarym polu *Response*.
- Typ odpowiedzi (JSON lub String) jest określony poniżej pola *Response*.

Jeśli test webhooka zakończy się niepowodzeniem:

- Wyświetlany jest komunikat *„Test typu nośnika nie powiódł się.”*, po którym podawane są dodatkowe szczegóły dotyczące błędu.

Media użytkownika

Po skonfigurowaniu typu mediów przejdź do sekcji *Użytkownicy* > *Użytkownicy* i przypisz media webhook do istniejącego użytkownika lub utwórz nowego użytkownika reprezentującego webhook. Kroki konfiguracji mediów użytkownika dla istniejącego użytkownika, wspólne dla wszystkich typów mediów, opisano na stronie Typy mediów.

Jeśli webhook używa tagów do przechowywania identyfikatora zgłoszenia\wiadomości, unikaj przypisywania tego samego webhooka jako mediów różnym użytkownikom, ponieważ może to powodować błędy webhooka (dotyczy to większości webhooków korzystających z opcji *Dołącz wpis menu zdarzenia*). W takim przypadku zalecaną praktyką jest utworzenie dedykowanego użytkownika reprezentującego webhook:

1. Po skonfigurowaniu typu mediów webhook przejdź do sekcji *Użytkownicy* > *Użytkownicy* i utwórz dedykowanego użytkownika Zabbix reprezentującego webhook — na przykład z nazwą użytkownika *Slack* dla webhooka Slack. Wszystkie ustawienia, z wyjątkiem mediów, można pozostawić domyślne, ponieważ ten użytkownik nie będzie logował się do Zabbix.
2. W profilu użytkownika przejdź do zakładki *Media* i dodaj webhook, podając wymagane informacje kontaktowe. Jeśli webhook nie używa pola *Wyślij do*, wprowadź dowolną kombinację obsługiwanych znaków, aby obejść wymagania walidacji.
3. Przyznaj temu użytkownikowi co najmniej uprawnienia do odczytu do wszystkich hostów, dla których ma wysyłać alerty, zgodnie z uprawnieniami.

Podczas konfigurowania akcji alertu dodaj tego użytkownika w polu *Wyślij do użytkowników* w szczegółach operacji — poinformuje to Zabbix, aby używał webhooka do powiadomień z tej akcji.

Konfigurowanie akcji alertów

Akcje określają, które powiadomienia mają być wysyłane za pośrednictwem webhooka. Kroki konfigurowania akcji z użyciem webhooków są takie same jak dla wszystkich innych typów mediów, z następującymi wyjątkami:

- Jeśli webhook używa tagów webhooka do przechowywania ID zgłoszenia\wiadomości oraz obsługi operacji aktualizacji\rozwiązania, należy unikać używania tego samego webhooka w wielu akcjach alertów dla pojedynczego zdarzenia problemu. Jeśli {EVENT.TAGS.<tag name>} istnieje i zostanie zaktualizowane w webhooku, jego wynikowa wartość będzie niezdefiniowana. Aby tego uniknąć, użyj w webhooku nowej nazwy tagu do przechowywania zaktualizowanych wartości. Dotyczy to webhooków Jira, Jira Service Desk, Mattermost, Opsgenie, OTRS, Redmine, ServiceNow, Slack, Zammad i Zendesk dostarczanych przez Zabbix oraz większości webhooków wykorzystujących opcję *Include event menu entry*. Należy jednak pamiętać, że pojedynczy webhook może być używany w wielu operacjach lub krokach eskalacji tej samej akcji, a także w różnych akcjach, które nie zostaną wyzwolone przez to samo zdarzenie problemu z powodu różnych warunków.
- W przypadku używania webhooka w akcjach dla zdarzeń wewnętrznych należy zaznaczyć pole wyboru *Custom message* i zdefiniować własną wiadomość w konfiguracji operacji akcji. W przeciwnym razie powiadomienie nie zostanie wysłane.

1 Przykłady skryptów webhooka

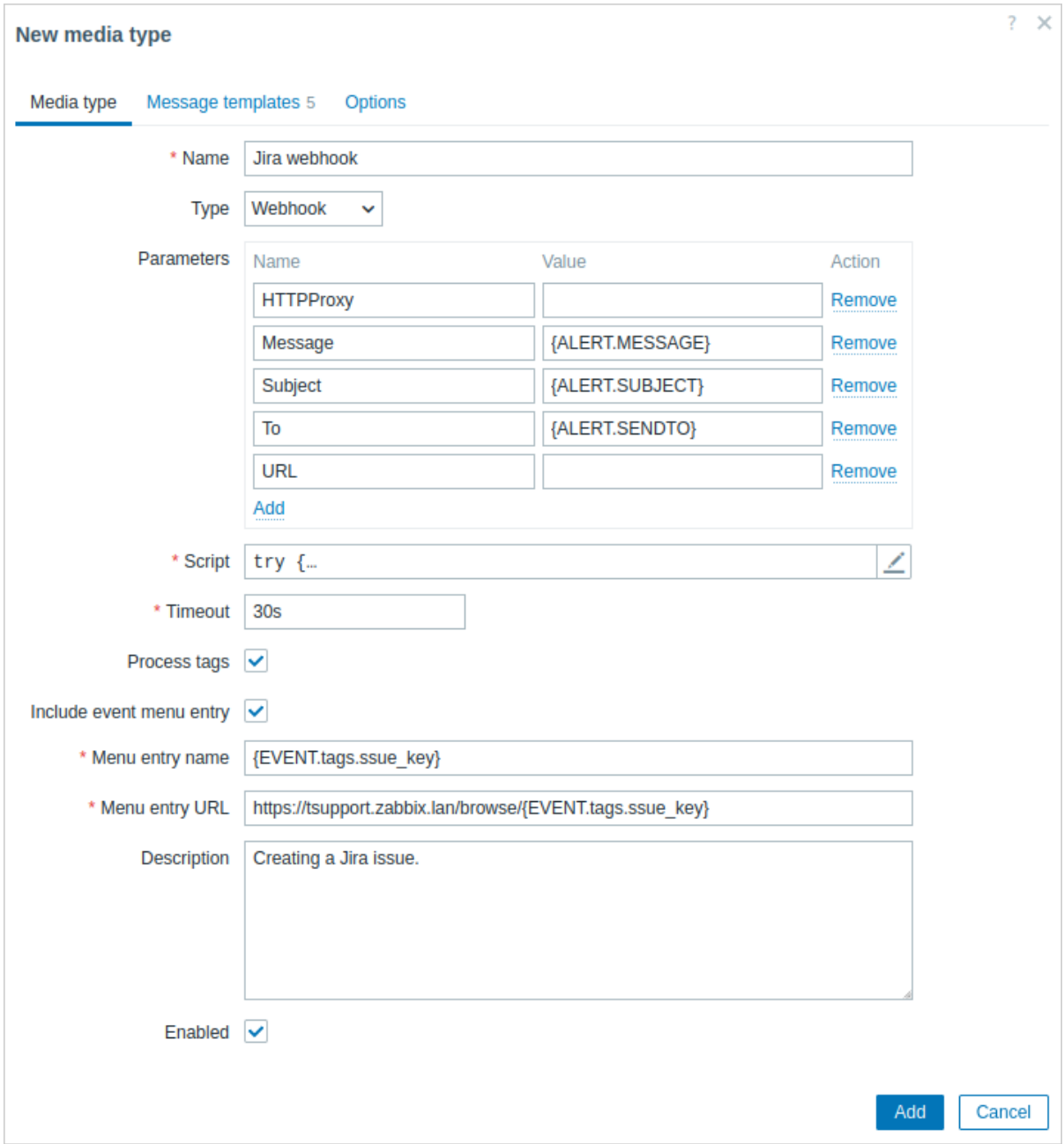
Przegląd

Chociaż Zabbix oferuje dużą liczbę integracji webhook dostępnych od razu po instalacji, możesz chcieć zamiast tego utworzyć własne webhooki. Ta sekcja zawiera przykłady niestandardowych skryptów webhook (używanych w parametrze *Script*). Opis innych parametrów webhook znajduje się w sekcji webhook.

Attention:
Nie używaj niezadeklarowanych przypisań w JavaScript przetwarzania wstępnego. Używaj `var` do deklarowania zmiennych lokalnych.

Zdarzenia odzyskania (niezależnie od tego, czy zostały wygenerowane automatycznie, czy po ręcznym zamknięciu) zawierają tagi rozwiązanych zdarzeń (w tym tagi dziedziczone z szablonów, hostów i wyzwalaczy). Skrypty webhook są wykonywane po utworzeniu alertu; tagi zwrócone przez skrypt webhook są zatem stosowane po początkowym utworzeniu alertu i mogą nie być obecne w alercie, który wywołał webhook. Jeśli integracja wymaga, aby tagi utworzone przez webhook były obecne w początkowym powiadomieniu, pobierz tagi zdarzenia z serwera (na przykład za pomocą API Event) albo przechowuj tagi utworzone przez webhook w zewnętrznym trwałym magazynie i tam je koreluj.

Jira webhook (niestandardowy)



Ten skrypt utworzy zgłoszenie JIRA i zwróci pewne informacje o utworzonym zgłoszeniu.

```
try {
    Zabbix.log(4, '[ Jira webhook ] Started with params: ' + value);

    var result = {
            'tags': {
                'endpoint': 'jira'
            }
        },
        params = JSON.parse(value),
        req = new HttpRequest(),
        fields = {},
        resp;

    if (params.HTTPProxy) {
        req.setProxy(params.HTTPProxy);
    }

    req.addHeader('Content-Type: application/json');
    req.addHeader('Authorization: Basic ' + params.authentication);

    fields.summary = params.summary;
    fields.description = params.description;
    fields.project = {key: params.project_key};
    fields.issuetype = {id: params.issue_id};

    resp = req.post('https://jira.example.com/rest/api/2/issue/',
        JSON.stringify({"fields": fields})
    );

    if (req.getStatus() != 201) {
        throw 'Response code: ' + req.getStatus();
    }

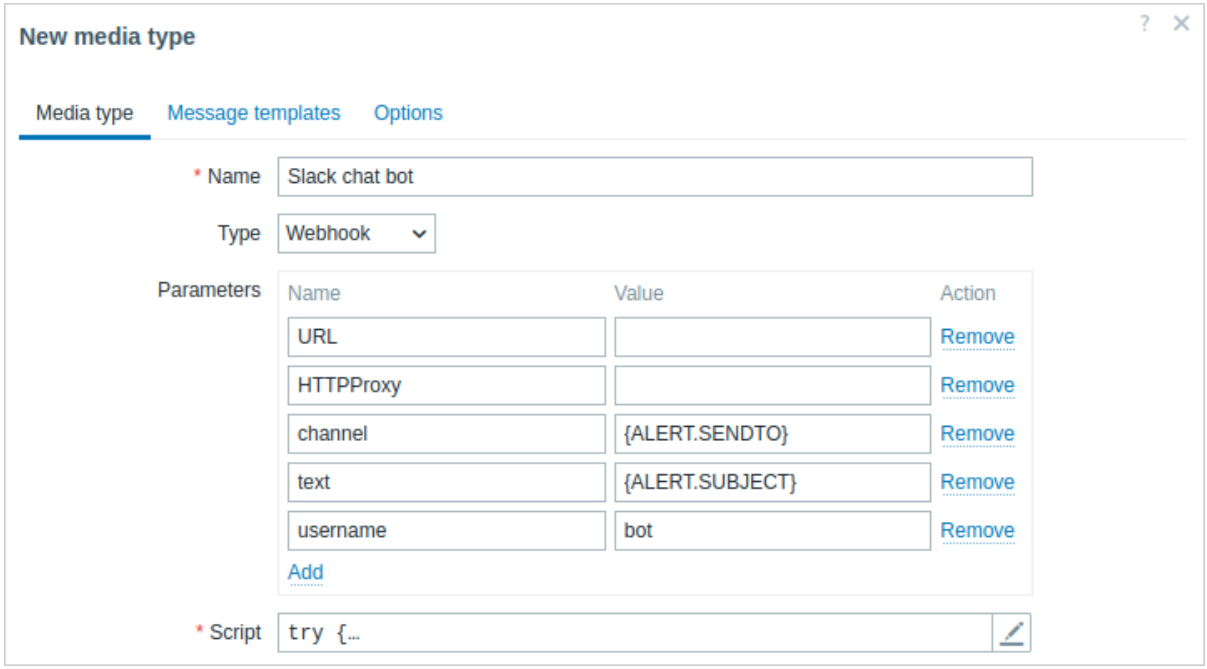
    resp = JSON.parse(resp);
    result.tags.issue_id = resp.id;
    result.tags.issue_key = resp.key;

    return JSON.stringify(result);
}
catch (error) {
    Zabbix.log(4, '[ Jira webhook ] Issue creation failed json : ' + JSON.stringify({"fields": fields}));
    Zabbix.log(3, '[ Jira webhook ] issue creation failed : ' + error);

    throw 'Failed with error: ' + error;
}
```

Slack webhook (niestandardowy)

Ten webhook będzie przekazywać powiadomienia z Zabbix do kanału Slack.




```
try {
    var params = JSON.parse(value),
        req = new HttpRequest(),
        response;

    if (params.HTTPProxy) {
        req.setProxy(params.HTTPProxy);
    }

    req.addHeader('Content-Type: application/x-www-form-urlencoded');

    Zabbix.log(4, '[ Slack webhook ] Webhook request with value=' + value);

    response = req.post(params.hook_url, 'payload=' + encodeURIComponent(value));
    Zabbix.log(4, '[ Slack webhook ] Responded with code: ' + req.getStatus() + '. Response: ' + response)

    try {
        response = JSON.parse(response);
    }
    catch (error) {
        if (req.getStatus() < 200 || req.getStatus() >= 300) {
            throw 'Request failed with status code ' + req.getStatus();
        }
        else {
            throw 'Request success, but response parsing failed.';
        }
    }

    if (req.getStatus() !== 200 || !response.ok || response.ok === 'false') {
        throw response.error;
    }

    return 'OK';
}
catch (error) {
    Zabbix.log(3, '[ Slack webhook ] Sending failed. Error: ' + error);

    throw 'Failed with error: ' + error;
}
```

2 Akcje

Przegląd

Jeśli chcesz, aby w wyniku zdarzeń były wykonywane określone operacje (na przykład wysyłane powiadomienia), musisz skonfigurować akcje.

Akcje mogą być definiowane w odpowiedzi na zdarzenia wszystkich obsługiwanych typów:

- Akcje wyzwalaczy - dla zdarzeń, gdy stan wyzwalacza zmienia się między `OK` a `Problem`
- Akcje usług - dla zdarzeń, gdy stan usługi zmienia się między `OK` a `Problem`
- Akcje wykrywania - dla zdarzeń, gdy odbywa się wykrywanie sieci
- Akcje autorejestracji - dla zdarzeń, gdy nowe aktywne agenty rejestrują się automatycznie (lub gdy metadane hosta zmieniają się dla już zarejestrowanych)
- Akcje wewnętrzne - dla zdarzeń, gdy pozycje stają się nieobsługiwane lub wyzwalacze przechodzą w stan nieznany

Kluczowe różnice dotyczące akcji usług to:

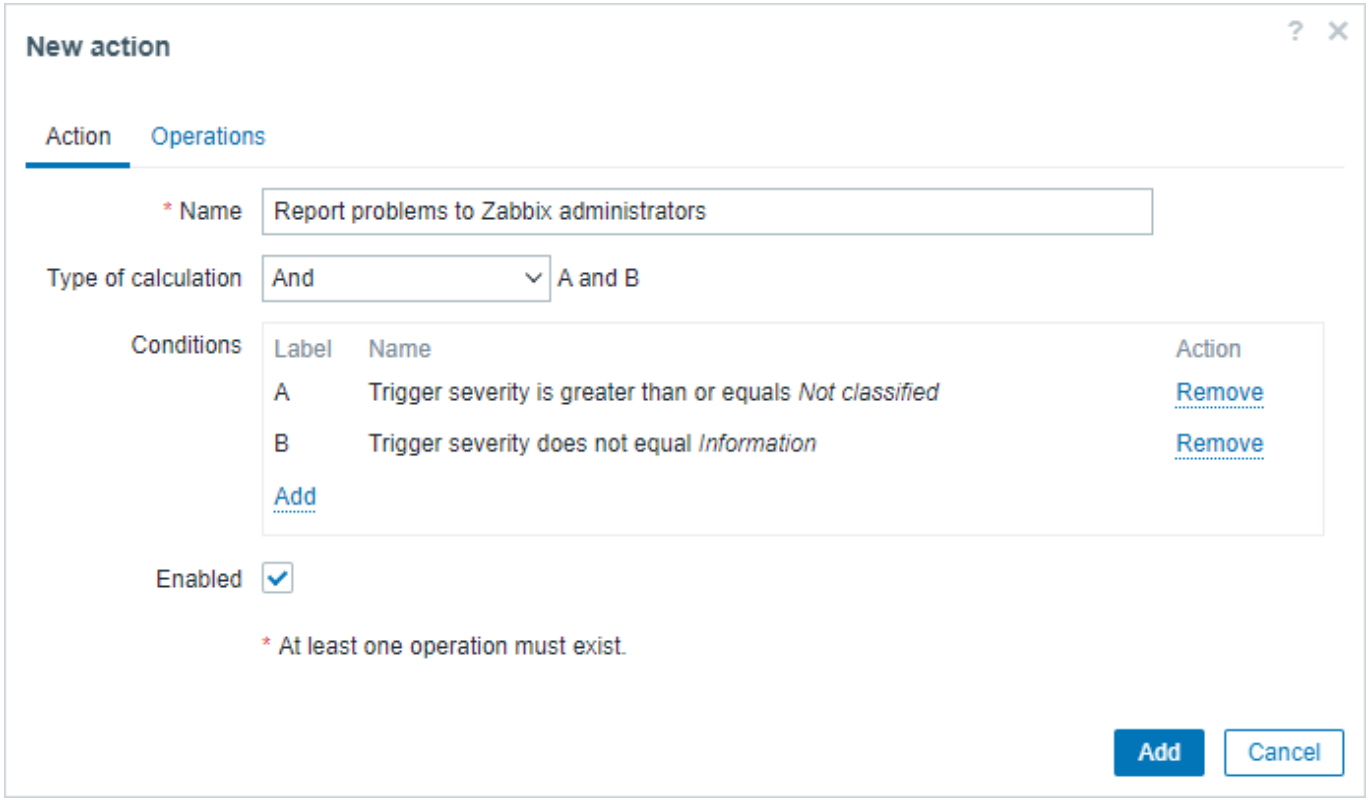
- Dostęp użytkownika do akcji usług zależy od uprawnień dostępu do usług przyznanych przez rolę
- Akcje usług obsługują inny zestaw warunków

Konfigurowanie akcji

Aby skonfigurować akcję, wykonaj następujące czynności:

- Przejdź do *Alerty* > *Akcje* i wybierz wymagany typ akcji z podmenu (możesz później przełączyć się na inny typ, używając rozwijanej listy w tytule).
- Kliknij *Utwórz akcję*.
- Nadaj akcji nazwę.
- Wybierz warunki, przy których wykonywane są operacje.
- Wybierz operacje, które mają zostać wykonane.

Ogólne atrybuty akcji:



Wszystkie wymagane pola wejściowe są oznaczone czerwoną gwiazdką.

Parametr	Opis
Nazwa	Unikalna nazwa akcji.

Parametr	Opis
Typ obliczania	Wybierz opcję oceny warunków akcji (gdy jest więcej niż jeden warunek): **I** - wszystkie warunki muszą być spełnione. **Lub** - wystarczy, że jeden warunek jest spełniony. **I/Lub** - połączenie obu: AND dla różnych typów warunków oraz OR dla tego samego typu warunku. **Wyrażenie niestandardowe** - zdefiniowana przez użytkownika formuła obliczeniowa do oceny warunków akcji.
Warunki	Lista warunków akcji. Kliknij *Dodaj*, aby dodać nowy warunek. Jeśli nie skonfigurowano żadnych warunków, akcja zostanie uruchomiona dla każdego zdarzenia odpowiadającego konfigurowanemu typowi akcji.
Włączone	Zaznacz pole wyboru, aby włączyć akcję. W przeciwnym razie będzie ona wyłączona.

1 Warunki

Przegląd

Można określić, że akcja zostanie wykonana tylko wtedy, gdy zdarzenie pasuje do zdefiniowanego zestawu warunków. Warunki ustawia się podczas konfigurowania akcji.

Dopasowanie warunków uwzględnia wielkość liter.

Akcje wyzwalaczy

W akcjach opartych na wyzwalaczach można używać następujących warunków:

Typ warunku	Obsługiwane operatory	Opis
Grupa hostów	równa się nie równa się	Określ grupy hostów lub grupy hostów do wykluczenia. **równa się** - zdarzenie należy do tej grupy hostów. **nie równa się** - zdarzenie nie należy do tej grupy hostów. Określenie nadrzędnej grupy hostów niejawnie wybiera wszystkie zagnieżdżone grupy hostów. Aby wskazać tylko grupę nadrzędną, wszystkie zagnieżdżone grupy muszą zostać dodatkowo ustawione z operatorem **nie równa się**.
Szablon	równa się nie równa się	Określ szablony lub szablony do wykluczenia. **równa się** - zdarzenie należy do wyzwalacza dziedziczonego z tego szablonu. **nie równa się** - zdarzenie nie należy do wyzwalacza dziedziczonego z tego szablonu.
Host	równa się nie równa się	Określ hosty lub hosty do wykluczenia. **równa się** - zdarzenie należy do tego hosta. **nie równa się** - zdarzenie nie należy do tego hosta.
Nazwa tagu	równa się nie równa się zawiera nie zawiera	Określ tag zdarzenia lub tag zdarzenia do wykluczenia. **równa się** - zdarzenie ma ten tag. **nie równa się** - zdarzenie nie ma tego tagu. **zawiera** - zdarzenie ma tag zawierający ten ciąg znaków. **nie zawiera** - zdarzenie nie ma tagu zawierającego ten ciąg znaków.
Wartość tagu	równa się nie równa się zawiera nie zawiera	Określ kombinację tagu zdarzenia i wartości lub kombinację tagu i wartości do wykluczenia. **równa się** - zdarzenie ma ten tag i wartość. **nie równa się** - zdarzenie nie ma tego tagu i wartości. **zawiera** - zdarzenie ma tag i wartość zawierające te ciągi znaków. **nie zawiera** - zdarzenie nie ma tagu i wartości zawierających te ciągi znaków.
Wyzwalacz	równa się nie równa się	Określ wyzwalacze lub wyzwalacze do wykluczenia. **równa się** - zdarzenie jest generowane przez ten wyzwalacz. **nie równa się** - zdarzenie jest generowane przez dowolny inny wyzwalacz, z wyjątkiem tego.

Typ warunku	Obsługiwane operatory	Opis
Nazwa zdarzenia	zawiera nie zawiera	Określ ciąg znaków w nazwie zdarzenia wygenerowanego przez wyzwalacz lub ciąg znaków do wykluczenia. Domyślnie nazwa zdarzenia odpowiada nazwie wyzwalacza, chyba że w konfiguracji wyzwalacza określono niestandardową nazwę zdarzenia. **zawiera** - nazwa zdarzenia zawiera ten ciąg znaków. **nie zawiera** - ten ciąg znaków jest wykluczony z nazwy zdarzenia. Uwaga: Wprowadzona wartość będzie porównywana z nazwą zdarzenia po rozwinięciu wszystkich makr.
Poziom ważności wyzwalacza	równa się nie równa się jest większy lub równy jest mniejszy lub równy	Określ poziom ważności wyzwalacza. **równa się** - równy poziomowi ważności wyzwalacza. **nie równa się** - nie równy poziomowi ważności wyzwalacza. **jest większy lub równy** - większy lub równy poziomowi ważności wyzwalacza. **jest mniejszy lub równy** - mniejszy lub równy poziomowi ważności wyzwalacza.
Okres czasu	w nie w	Określ okres czasu lub okres czasu do wykluczenia. **w** - czas zdarzenia mieści się w okresie czasu. **nie w** - czas zdarzenia nie mieści się w okresie czasu. Opis formatu znajduje się na stronie specyfikacji okresu czasu. Obsługiwane są makra użytkownika.
Problem jest wyciszony	nie tak	Określ, czy problem jest wyciszony (niewyświetlany) z powodu konserwacji hosta. **nie** - problem nie jest wyciszony. **tak** - problem jest wyciszony.

Akcje usług

W akcjach usług można używać następujących warunków:

Typ warunku	Obsługiwane operatory	Opis
Usługa	równa się nie równa się	Określ usługę lub usługę do wykluczenia. **równa się** - zdarzenie należy do tej usługi. **nie równa się** - zdarzenie nie należy do tej usługi. Określenie usługi nadrzędnej niejawnie wybiera wszystkie usługi podrzędne. Aby wskazać tylko usługę nadrzędną, wszystkie zagnieżdżone usługi muszą zostać dodatkowo ustawione z operatorem **nie równa się**.
Nazwa usługi	zawiera nie zawiera	Określ ciąg znaków w nazwie usługi lub ciąg znaków do wykluczenia. **zawiera** - zdarzenie jest generowane przez usługę, której nazwa zawiera ten ciąg znaków. **nie zawiera** - tego ciągu znaków nie można znaleźć w nazwie usługi.
Nazwa tagu usługi	równa się nie równa się zawiera nie zawiera	Określ tag zdarzenia lub tag zdarzenia do wykluczenia. Tagi zdarzeń usługi można zdefiniować w sekcji konfiguracji usługi *Tagi*. **równa się** - zdarzenie ma ten tag. **nie równa się** - zdarzenie nie ma tego tagu. **zawiera** - zdarzenie ma tag zawierający ten ciąg znaków. **nie zawiera** - zdarzenie nie ma tagu zawierającego ten ciąg znaków.
Wartość tagu usługi	równa się nie równa się zawiera nie zawiera	Określ kombinację tagu zdarzenia i wartości lub kombinację tagu i wartości do wykluczenia. Tagi zdarzeń usługi można zdefiniować w sekcji konfiguracji usługi *Tagi*. **równa się** - zdarzenie ma ten tag i wartość. **nie równa się** - zdarzenie nie ma tego tagu i wartości. **zawiera** - zdarzenie ma tag i wartość zawierające te ciągi znaków. **nie zawiera** - zdarzenie nie ma tagu i wartości zawierających te ciągi znaków.

Attention:
Upewnij się, że w menu *Alerty* → *Typy mediów* zdefiniowano szablony wiadomości dla akcji usług. W przeciwnym razie powiadomienia nie będą wysyłane.

Akcje wykrywania

W zdarzeniach opartych na wykrywaniu można używać następujących warunków:

Typ warunku	Obsługiwane operatory	Opis
IP hosta	równa się nie równa się	Określ zakres adresów IP lub zakres do wykluczenia dla wykrytego hosta. **równa się** - IP hosta znajduje się w zakresie. **nie równa się** - IP hosta nie znajduje się w zakresie. Może mieć następujące formaty: Pojedynczy adres IP: 192.168.1.33 Zakres adresów IP: 192.168.1-10.1-254 Maska IP: 192.168.4.0/24 Lista: 192.168.1.1-254, 192.168.2.1-100, 192.168.2.200, 192.168.4.0/24 Spacje w formacie listy są obsługiwane.
Typ usługi	równa się nie równa się	Określ typ usługi wykrytej usługi lub typ usługi do wykluczenia. **równa się** - pasuje do wykrytej usługi. **nie równa się** - nie pasuje do wykrytej usługi. Dostępne typy usług: SSH, LDAP, SMTP, FTP, HTTP, HTTPS, POP, NNTP, IMAP, TCP, Zabbix agent, SNMPv1 agent, SNMPv2 agent, SNMPv3 agent, ICMP ping, telnet.
Port usługi	równa się nie równa się	Określ zakres portów TCP wykrytej usługi lub zakres do wykluczenia. **równa się** - port usługi znajduje się w zakresie. **nie równa się** - port usługi nie znajduje się w zakresie.
Reguła wykrywania	równa się nie równa się	Określ regułę wykrywania lub regułę wykrywania do wykluczenia. **równa się** - używa tej reguły wykrywania. **nie równa się** - używa dowolnej innej reguły wykrywania, z wyjątkiem tej.
Sprawdzenie wykrywania	równa się nie równa się	Określ sprawdzenie wykrywania lub sprawdzenie wykrywania do wykluczenia. **równa się** - używa tego sprawdzenia wykrywania. **nie równa się** - używa dowolnego innego sprawdzenia wykrywania, z wyjątkiem tego.
Obiekt wykrywania	równa się	Określ wykryty obiekt. **równa się** - równe wykrytemu obiektowi (urządzenie lub usługa).
Status wykrywania	równa się	**Up** - pasuje do zdarzeń „Host Up” i „Service Up”. **Down** - pasuje do zdarzeń „Host Down” i „Service Down”. **Discovered** - pasuje do zdarzeń „Host Discovered” i „Service Discovered”. **Lost** - pasuje do zdarzeń „Host Lost” i „Service Lost”.
Czas działania/przestoju	jest większy lub równy jest mniejszy lub równy	Czas działania dla zdarzeń „Host Up” i „Service Up”. Czas przestoju dla zdarzeń „Host Down” i „Service Down”. **jest większy lub równy** - jest większy lub równy. Parametr jest podawany w sekundach. **jest mniejszy lub równy** - jest mniejszy lub równy. Parametr jest podawany w sekundach.

Typ warunku	Obsługiwane operatory	Opis
Otrzymana wartość	równa się nie równa się jest większy lub równy jest mniejszy lub równy zawiera nie zawiera	Określ wartość otrzymaną ze sprawdzenia agent (Zabbix, SNMP) w regule wykrywania. Porównanie ciągów znaków. Jeśli dla reguły skonfigurowano kilka sprawdzeń Zabbix agent lub SNMP, sprawdzane są otrzymane wartości dla każdego z nich (każde sprawdzenie generuje nowe zdarzenie, które jest dopasowywane do wszystkich warunków). **równa się** - równe wartości. **nie równa się** - nie równe wartości. **jest większy lub równy** - większe lub równe wartości. **jest mniejszy lub równy** - mniejsze lub równe wartości. **zawiera** - zawiera podciąg. Parametr jest podawany jako ciąg znaków. **nie zawiera** - nie zawiera podciągu. Parametr jest podawany jako ciąg znaków.
Proxy	równa się nie równa się	Określ proxy lub proxy do wykluczenia. **równa się** - używa tego proxy. **nie równa się** - używa dowolnego innego proxy z wyjątkiem tego.

Note:
Sprawdzenia usług w regule wykrywania, które skutkują zdarzeniami wykrywania, nie są wykonywane jednocześnie. Dlatego jeśli w akcji skonfigurowano **wiele** wartości dla warunków `Service type`, `Service port` lub `Received value`, będą one porównywane z jednym zdarzeniem wykrywania naraz, ale **nie** z kilkoma zdarzeniami jednocześnie. W rezultacie akcje z wieloma wartościami dla tych samych typów sprawdzeń mogą nie być wykonywane poprawnie.

Akcje autorejestracji

W akcjach opartych na aktywnej autorejestracji agent można używać następujących warunków:

Typ warunku	Obsługiwane operatory	Opis
Metadane hosta	zawiera nie zawiera pasuje nie pasuje	Określ metadane hosta lub metadane hosta do wykluczenia. **zawiera** - metadane hosta zawierają ciąg znaków. **nie zawiera** - metadane hosta nie zawierają ciągu znaków. Metadane hosta można określić w pliku konfiguracyjnym agent. **pasuje** - metadane hosta pasują do wyrażenia regularnego. **nie pasuje** - metadane hosta nie pasują do wyrażenia regularnego.
Nazwa hosta	zawiera nie zawiera pasuje nie pasuje	Określ nazwę hosta lub nazwę hosta do wykluczenia. **zawiera** - nazwa hosta zawiera ciąg znaków. **nie zawiera** - nazwa hosta nie zawiera ciągu znaków. **pasuje** - nazwa hosta pasuje do wyrażenia regularnego. **nie pasuje** - nazwa hosta nie pasuje do wyrażenia regularnego.
Proxy	równa się nie równa się	Określ proxy lub proxy do wykluczenia. **równa się** - używane jest to proxy. **nie równa się** - używane jest dowolne inne proxy poza tym.

Akcje zdarzeń wewnętrznych

Dla akcji opartych na zdarzeniach wewnętrznych można ustawić następujące warunki:

Typ warunku	Obsługiwane operatory	Opis
Typ zdarzenia	equals	**Pozycja w stanie „nieobsługiwane”** - pasuje do zdarzeń, w których pozycja przechodzi ze stanu „normalny” do stanu „nieobsługiwane”. **Reguła wykrywania niskiego poziomu w stanie „nieobsługiwane”** - pasuje do zdarzeń, w których reguła wykrywania niskiego poziomu przechodzi ze stanu „normalny” do stanu „nieobsługiwane”. **Wyzwalacz w stanie „nieznany”** - pasuje do zdarzeń, w których wyzwalacz przechodzi ze stanu „normalny” do stanu „nieznany”.
Grupa hostów	equals does not equal	Określ grupy hostów lub grupy hostów do wykluczenia. **equals** - zdarzenie należy do tej grupy hostów. **does not equal** - zdarzenie nie należy do tej grupy hostów.

Typ warunku	Obsługiwane operatory	Opis
Nazwa tagu	equals does not equal contains does not contain	Określ tag zdarzenia lub tag zdarzenia do wykluczenia. **equals** - zdarzenie ma ten tag. **does not equal** - zdarzenie nie ma tego tagu. **contains** - zdarzenie ma tag zawierający ten ciąg znaków. **does not contain** - zdarzenie nie ma tagu zawierającego tego ciągu znaków.
Wartość tagu	equals does not equal contains does not contain	Określ kombinację tagu zdarzenia i wartości lub kombinację tagu i wartości do wykluczenia. **equals** - zdarzenie ma ten tag i wartość. **does not equal** - zdarzenie nie ma tego tagu i wartości. **contains** - zdarzenie ma tag i wartość zawierające te ciągi znaków. **does not contain** - zdarzenie nie ma tagu i wartości zawierających tych ciągów znaków.
Szablon	equals does not equal	Określ szablony lub szablony do wykluczenia. **equals** - zdarzenie należy do pozycji/wyzwalacza/reguły wykrywania niskiego poziomu dziedziczonych z tego szablonu. **does not equal** - zdarzenie nie należy do pozycji/wyzwalacza/reguły wykrywania niskiego poziomu dziedziczonych z tego szablonu.
Host	equals does not equal	Określ hosty lub hosty do wykluczenia. **equals** - zdarzenie należy do tego hosta. **does not equal** - zdarzenie nie należy do tego hosta.

Typ obliczania

Dostępne są następujące opcje obliczania warunków:

- **And** - wszystkie warunki muszą być spełnione

Należy pamiętać, że użycie obliczania „And” jest niedozwolone między kilkoma wyzwalaczami, gdy są one wybrane jako warunek `Trigger=`. Akcje mogą być wykonywane tylko na podstawie zdarzenia jednego wyzwalacza.

- **Or** - wystarczy, że jeden warunek jest spełniony
- **And/Or** - połączenie obu: AND dla różnych typów warunków oraz OR dla tego samego typu warunku, na przykład:

Grupa hostów równa się Oracle servers
Grupa hostów równa się MySQL servers
Nazwa zdarzenia zawiera ’Database is down’
Nazwa zdarzenia zawiera ’Database is unavailable’

jest oceniane jako

(Grupa hostów równa się Oracle servers **or** Grupa hostów równa się MySQL servers**) and (**Nazwa zdarzenia zawiera ’Database is down’ **or** Nazwa zdarzenia zawiera ’Database is unavailable’**)**

- **Custom expression** - formuła obliczeniowa zdefiniowana przez użytkownika do oceny warunków akcji. Musi zawierać wszystkie warunki (reprezentowane jako wielkie litery A, B, C, ...) i może zawierać spacje, tabulatory, nawiasy ( ), **and** (z rozróżnianiem wielkości liter), **or** (z rozróżnianiem wielkości liter), **not** (z rozróżnianiem wielkości liter).

Podczas gdy poprzedni przykład z `And/Or` byłby przedstawiony jako (A or B) and (C or D), w wyrażeniu niestandardowym można mieć również wiele innych sposobów obliczania:

(A and B) and (C or D)
(A and B) or (C and D)
((A or B) and C) or D
(not (A or B) and C) or not D
itd.

Usuwanie obiektów używanych w akcjach

Podczas próby usunięcia obiektów, które są używane w warunku/operacji akcji, użytkownik otrzyma odpowiedni komunikat o błędzie.

Akcje nie są wyłączane, jeśli warunki lub operacje akcji:

- mają usunięte obiekty;
- mają obiekty, które nie są już wykrywane przez wykrywanie niskopoziomowe i zostały usunięte (po upływie okresu *Delete lost resources*).

Warunki/operacje akcji nie są usuwane, jeśli mają brakujące obiekty. Zamiast tego usunięte obiekty są wyświetlane jako *Deleted host group*, *Deleted host*, *Deleted trigger* itd. Ikona ostrzeżenia z komunikatem „This action has conditions or operations referencing deleted object(s).” jest wyświetlana w kolumnie „Info” na liście akcji.

2 Operacje

Przegląd

Dla wszystkich zdarzeń można zdefiniować następujące operacje:

- Wyślij wiadomość
- Wykonaj zdalne polecenie

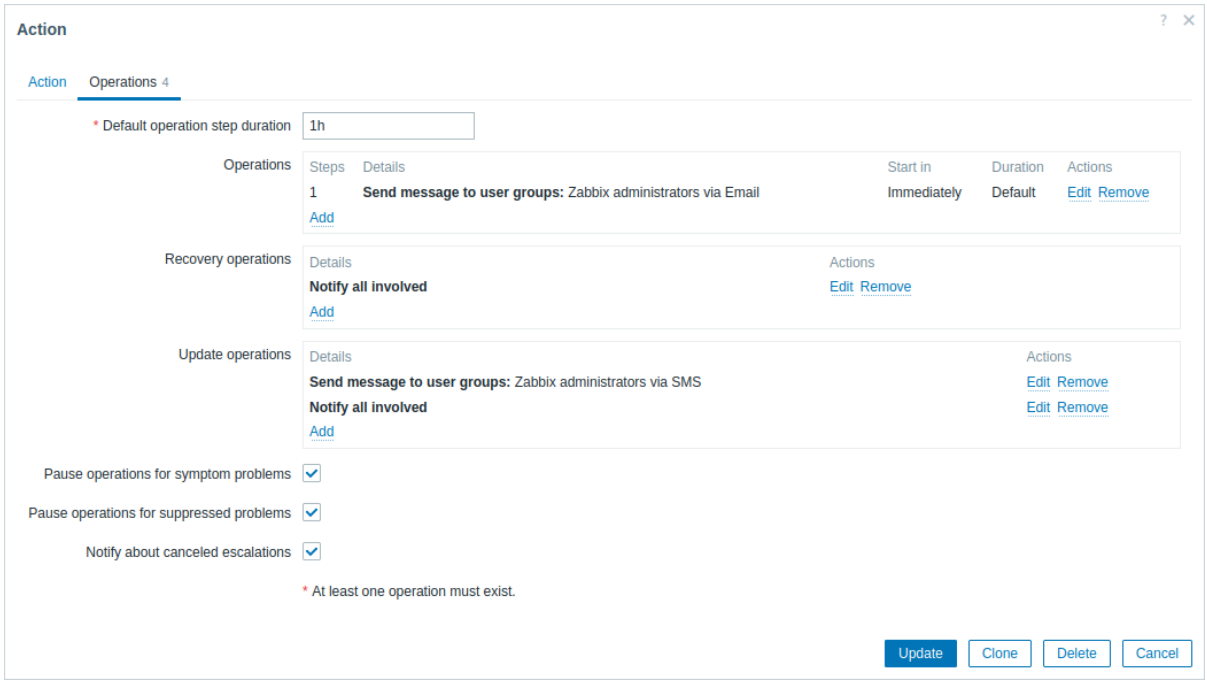
Attention:
Serwer Zabbix nie tworzy alertów, jeśli dostęp do hosta jest jawnie „denied” dla użytkownika zdefiniowanego jako odbiorca operacji akcji lub jeśli użytkownik w ogóle nie ma zdefiniowanych żadnych uprawnień do hosta.

Dla zdarzeń wykrywania i autorejestracji dostępne są dodatkowe operacje:

- Dodaj host
- Usuń host
- Włącz host
- Wyłącz host
- Dodaj do grupy hostów
- Usuń z grupy hostów
- Dodaj tagi hosta
- Usuń tagi hosta
- Podłącz szablon
- Odłącz szablon
- Ustaw tryb inwentaryzacji hosta

Konfigurowanie operacji

Aby skonfigurować operację, przejdź do zakładki *Operacje* w konfiguracji action.



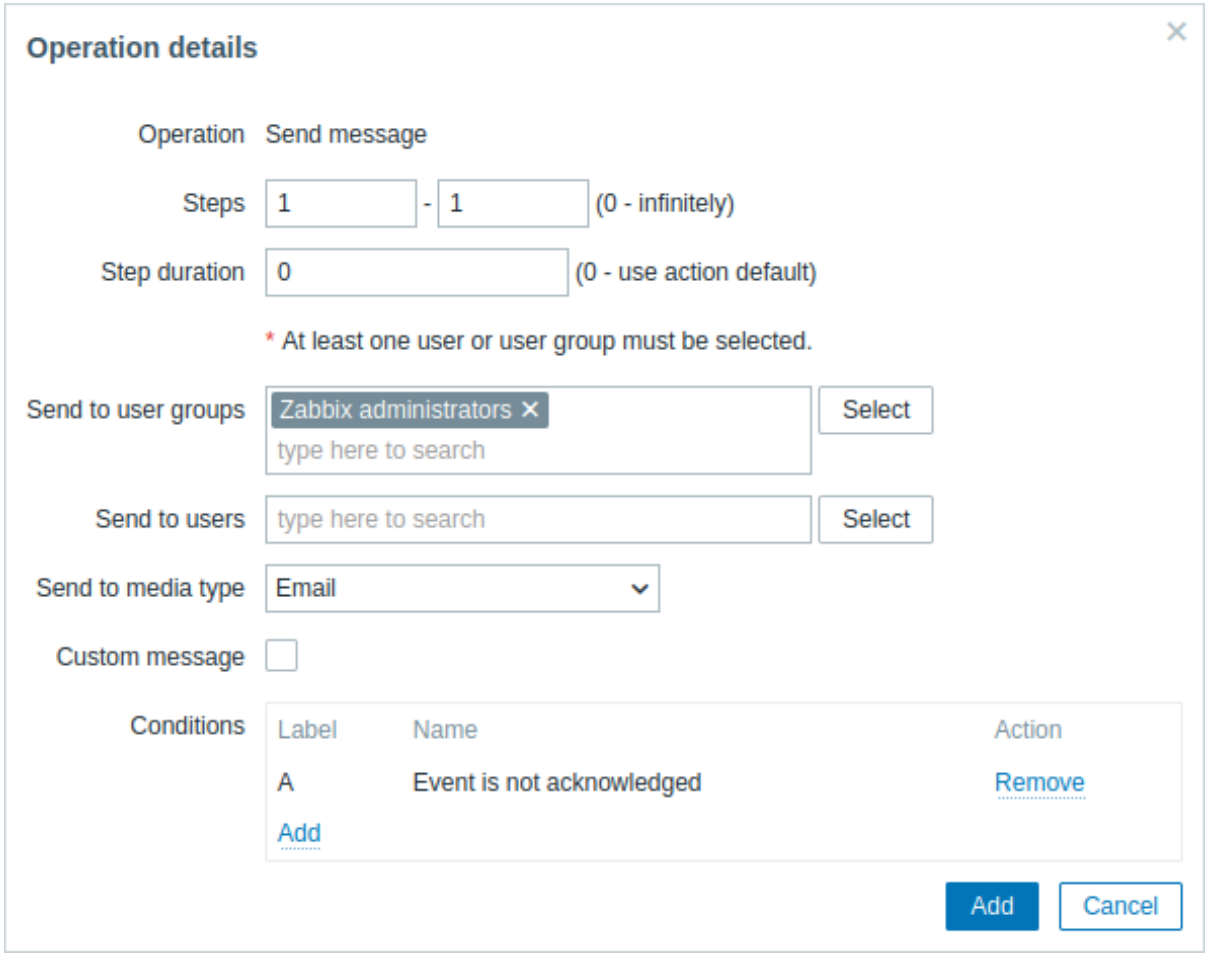
Ogólne atrybuty operacji:

Parametr	Opis
Domyślny czas trwania kroku operacji	Domyślny czas trwania jednego kroku operacji (od 60 sekund do 1 tygodnia). Na przykład godzinny czas trwania kroku oznacza, że jeśli operacja zostanie wykonana, przed następnym krokiem upłynie godzina. Obsługiwane są sufiksy czasu, np. 60s, 1m, 2h, 1d. Obsługiwane są makra użytkownika.
Operacje	Wyświetlane są operacje akcji (jeśli istnieją) wraz z następującymi szczegółami: **Kroki** — krok(i) eskalacji, do których przypisana jest operacja. **Szczegóły** — typ operacji oraz jej odbiorca/cel. Na liście operacji wyświetlany jest również używany typ nośnika (e-mail, SMS lub skrypt), a także imię i nazwisko (w nawiasie po nazwie użytkownika) odbiorcy powiadomienia. **Rozpocznij za** — po jakim czasie od zdarzenia operacja zostanie wykonana. **Czas trwania (sek.)** — wyświetlany jest czas trwania kroku. Jeśli krok używa czasu domyślnego, wyświetlane jest *Domyślny*, a jeśli używany jest czas niestandardowy, wyświetlany jest czas. **Działania** — wyświetlane są odnośniki do edycji i usunięcia operacji.
Operacje odzyskiwania	Wyświetlane są operacje akcji (jeśli istnieją) wraz z następującymi szczegółami: **Szczegóły** — typ operacji oraz jej odbiorca/cel. Na liście operacji wyświetlany jest również używany typ nośnika (e-mail, SMS lub skrypt), a także imię i nazwisko (w nawiasie po nazwie użytkownika) odbiorcy powiadomienia. **Działania** — wyświetlane są odnośniki do edycji i usunięcia operacji.
Operacje aktualizacji	Wyświetlane są operacje akcji (jeśli istnieją) wraz z następującymi szczegółami: **Szczegóły** — typ operacji oraz jej odbiorca/cel. Na liście operacji wyświetlany jest również używany typ nośnika (e-mail, SMS lub skrypt), a także imię i nazwisko (w nawiasie po nazwie użytkownika) odbiorcy powiadomienia. **Działania** — wyświetlane są odnośniki do edycji i usunięcia operacji.
Wstrzymaj operacje dla problemów symptomów	Zaznacz to pole wyboru, aby wstrzymać operacje (po pierwszej operacji) dla problemów symptomów. Pamiętaj, że to ustawienie wpływa tylko na eskalacje problemów; operacje odzyskiwania i aktualizacji nie będą nim objęte. Ta opcja jest dostępna tylko dla *Akcji wyzwalaczy*.
Wstrzymaj operacje dla wyciszonych problemów	Zaznacz to pole wyboru, aby opóźnić rozpoczęcie operacji na czas trwania okresu konserwacji. Po uruchomieniu operacji, po zakończeniu konserwacji, zostaną wykonane wszystkie operacje, w tym także te dotyczące zdarzeń z okresu konserwacji. Pamiętaj, że to ustawienie wpływa tylko na eskalacje problemów; operacje odzyskiwania i aktualizacji nie będą nim objęte. Jeśli odznaczysz to pole wyboru, operacje będą wykonywane bez opóźnienia nawet w trakcie okresu konserwacji. Ta opcja nie jest dostępna dla *Akcji usług*.
Powiadamiaj o anulowanych eskalacjach	Odznacz to pole wyboru, aby wyłączyć powiadomienia o anulowanych eskalacjach (gdy host, pozycja, wyzwalacz lub akcja są wyłączone).

Wszystkie wymagane pola wejściowe są oznaczone czerwoną gwiazdką.

Aby skonfigurować szczegóły nowej operacji, kliknij Add w bloku *Operacje*. Aby edytować istniejącą operację, kliknij Edit obok operacji. Otworzy się wyskakujące okno, w którym można edytować szczegóły kroków operacji.

Szczegóły operacji



Parametr	Opis
Operacja	Wybierz operację: **Wyślij wiadomość** - wyślij wiadomość do użytkownika. **<nazwa zdalnego polecenia>** - wykonaj zdalne polecenie. Polecenia są dostępne do wykonania, jeśli zostały wcześniej zdefiniowane w skryptach globalnych z wybranym zakresem *Operacja akcji*. Więcej operacji jest dostępnych dla zdarzeń opartych na wykrywaniu i autorejestracji (patrz wyżej).
Kroki	Wybierz krok(i), do których ma zostać przypisana operacja w harmonogramie eskalacji: **Od** - wykonuj od tego kroku. **Do** - wykonuj do tego kroku (0=nieskończoność, wykonanie nie będzie ograniczone).
Czas tr-wa-nia kroku	Niestandardowy czas trwania dla tych kroków (0=użyj domyślnego czasu trwania kroku). Obsługiwane są sufiksy czasu, np. 60s, 1m, 2h, 1d. Obsługiwane są makra użytkownika. Do tego samego kroku można przypisać kilka operacji. Jeśli dla tych operacji zdefiniowano różny czas trwania kroku, brany jest pod uwagę najkrótszy i stosowany do kroku.
Typ op-er-acji: wyślij wiado-mość	
Wyślij do grup użytkown-ików	Wybierz grupy użytkowników, do których ma zostać wysłana wiadomość. Aby otrzymać powiadomienie, grupa użytkowników musi mieć co najmniej uprawnienia „odczyt” do hosta.

Parametr	Opis
Wyślij do użytkowników	Wybierz użytkowników, do których ma zostać wysłana wiadomość. Aby otrzymać powiadomienie, użytkownik musi mieć co najmniej uprawnienia „odczyt” do hosta.
Wyślij do typu mediów	Wyślij wiadomość do wszystkich dostępnych (skonfigurowanych i włączonych) typów mediów lub tylko do jednego określonego.
Własna wiadomość	Jeśli opcja jest zaznaczona, można skonfigurować własną wiadomość. W przypadku powiadomień o zdarzeniach wewnętrznych przez webhooki, własna wiadomość jest obowiązkowa.
Temat	Temat własnej wiadomości. Temat może zawierać makra. Jest ograniczony do 255 znaków.
Wiadomość	Własna wiadomość. Wiadomość może zawierać makra. Jej długość jest ograniczona do określonej liczby znaków w zależności od typu bazy danych (więcej informacji znajduje się w sekcji Wysyłanie wiadomości).
Typ operacji: zdalne polecenie	
Lista celów	Wybierz cele, na których ma zostać wykonane polecenie: **Bieżący host** - polecenie jest wykonywane na hoście wyzwalacza, który spowodował zdarzenie problemu. Ta opcja nie zadziała, jeśli w wyzwalaczu występuje wiele hostów. **Host** - wybierz host(y), na których ma zostać wykonane polecenie. **Grupa hostów** - wybierz grupę(y) hostów, na których ma zostać wykonane polecenie. Określenie nadrzędnej grupy hostów niejawnie wybiera wszystkie zagnieżdżone grupy hostów. W ten sposób zdalne polecenie zostanie również wykonane na hostach z grup zagnieżdżonych. Polecenie na hoście jest wykonywane tylko raz, nawet jeśli host pasuje więcej niż jeden raz (np. z kilku grup hostów; indywidualnie i z grupy hostów). Lista celów nie ma znaczenia, jeśli na serwerze Zabbix wykonywany jest skrypt niestandardowy. Wybranie większej liczby celów w takim przypadku powoduje jedynie wielokrotne wykonanie skryptu na serwerze. Zwróć uwagę, że w przypadku skryptów globalnych wybór celu zależy również od ustawienia *Grupa hostów* w konfiguracji skryptu globalnego. Opcja *Lista celów* nie jest dostępna dla *Akcji usługi*, ponieważ w tym przypadku zdalne polecenia są zawsze wykonywane na serwerze Zabbix.
Warunki	Warunek wykonania operacji: **Zdarzenie nie jest potwierdzone** - tylko gdy zdarzenie nie jest potwierdzone. **Zdarzenie jest potwierdzone** - tylko gdy zdarzenie jest potwierdzone. Opcja *Warunki* jest dostępna tylko dla *Akcji wyzwalacza*.

Po zakończeniu kliknij *Dodaj*, aby dodać operację do listy *Operacje*.

1 Wysyłanie wiadomości

Przegląd

Wysłanie wiadomości jest jednym z najlepszych sposobów powiadamiania ludzi o problemie. Dlatego jest to jedna z podstawowych akcji oferowanych przez Zabbix.

Konfiguracja

Aby móc wysyłać i odbierać powiadomienia z Zabbix, musisz:

- zdefiniować media, na które mają być wysyłane wiadomości

Jeśli operacja ma miejsce poza okresem When active, zdefiniowanym dla wybranego medium w konfiguracji użytkownika, wiadomość nie zostanie wysłana.

Domyślny poziom ważności wyzwalacza („Not classified”) **musi być** zaznaczony w konfiguracji mediów użytkownika, jeśli chcesz otrzymywać powiadomienia o zdarzeniach niezwiązanych z wyzwalaczami, takich jak wykrywanie, aktywna autorejestracja agent lub zdarzenia wewnętrzne.

- skonfigurować operację akcji, która wysyła wiadomość na jedno ze zdefiniowanych mediów

Attention:
Zabbix wysyła powiadomienia tylko do tych użytkowników, którzy mają co najmniej uprawnienia „odczyt” do host, który wygenerował zdarzenie. Co najmniej jeden host z wyrażenia wyzwalacza musi być dostępny.

Możesz skonfigurować niestandardowe scenariusze wysyłania wiadomości za pomocą eskalacji.

Aby poprawnie odbierać i odczytywać wiadomości e-mail z Zabbix, serwery/klienci poczty muszą obsługiwać standardowy format „SMTP/MIME email”, ponieważ Zabbix wysyła dane UTF-8 (jeśli temat zawiera wyłącznie znaki ASCII, nie jest kodowany w UTF-8). Temat i treść wiadomości są kodowane base64 zgodnie ze standardem formatu „SMTP/MIME email”.

Limit wiadomości po rozwinięciu wszystkich makr jest taki sam jak limit wiadomości dla zdalnych poleceń.

Śledzenie wiadomości

Możesz wyświetlić status wiadomości wysłanych w *Monitoring* → *Problemy*.

W kolumnie *Akcje* możesz zobaczyć podsumowane informacje o wykonanych działaniach. Zielone liczby oznaczają tam wysłane wiadomości, czerwone — wiadomości, których nie udało się wysłać. *W toku* wskazuje, że działanie zostało zainicjowane. *Niepowodzenie* informuje, że żadne działanie nie zostało wykonane pomyślnie.

Jeśli klikniesz czas zdarzenia, aby wyświetlić szczegóły zdarzenia, będziesz mógł zobaczyć szczegóły wiadomości wysłanych (lub niewysłanych) z powodu tego zdarzenia w bloku *Akcje*.

W *Raporty* → *Dziennik akcji* zobaczysz szczegóły wszystkich wykonanych działań dla tych zdarzeń, dla których skonfigurowano akcję.

2 Zdalne polecenia

Przegląd

Za pomocą zdalnych poleceń można zdefiniować, że określone, wcześniej zdefiniowane polecenie zostanie automatycznie wykonane na monitorowanym hoście po spełnieniu określonego warunku.

Dzięki temu zdalne polecenia są potężnym mechanizmem inteligentnego, proaktywnego monitorowania.

W najbardziej oczywistych zastosowaniach tej funkcji można spróbować:

- Automatycznie restartować aplikację (serwer WWW, middleware, CRM), jeśli nie odpowiada
- Użyć polecenia IPMI „reboot”, aby ponownie uruchomić zdalny serwer, jeśli nie odpowiada na żądania
- Automatycznie zwalniać miejsce na dysku (usuwanie starszych plików, czyszczenie /tmp), jeśli kończy się wolne miejsce na dysku
- Migrować maszynę wirtualną z jednego fizycznego serwera na inny w zależności od obciążenia CPU
- Dodawać nowe węzły do środowiska chmurowego przy niewystarczających zasobach CPU (dysku, pamięci lub innych)

Konfigurowanie akcji dla zdalnych poleceń jest podobne do konfigurowania akcji wysyłania wiadomości; jedyna różnica polega na tym, że Zabbix wykona polecenie zamiast wysyłać wiadomość.

Zdalne polecenia mogą być wykonywane przez serwer Zabbix, proxy lub agent. Zdalne polecenia na Zabbix agent mogą być wykonywane bezpośrednio przez serwer Zabbix lub za pośrednictwem Zabbix proxy. Zarówno na Zabbix agent, jak i Zabbix proxy zdalne polecenia są domyślnie wyłączone. Można je włączyć przez:

- dodanie parametru `AllowKey=system.run[*]` w konfiguracji agenta;
- ustawienie parametru EnableRemoteCommands na „1” w konfiguracji proxy.

Zdalne polecenia wykonywane przez serwer Zabbix są uruchamiane zgodnie z opisem w Command execution, łącznie ze sprawdzaniem kodu wyjścia.

Zdalne polecenia są wykonywane nawet wtedy, gdy docelowy host jest w trybie konserwacji.

Limit zdalnych poleceń

Limit zdalnego polecenia po rozwinięciu wszystkich makr zależy od typu bazy danych i zestawu znaków (znaki spoza ASCII wymagają do zapisania więcej niż jednego bajtu):

Database	Limit in characters	Limit in bytes
MySQL	65535	65535
PostgreSQL	65535	bez limitu
SQLite (tylko Zabbix proxy)	65535	bez limitu

Dane wyjściowe wykonania zdalnego polecenia (wartość zwracana) są ograniczone do 16 MB (włącznie z końcowymi białymi znakami, które są obcinane). Limit zdalnego polecenia IPMI zależy od zainstalowanej biblioteki IPMI. Należy pamiętać, że limity bazy danych mają zastosowanie do wszystkich zdalnych poleceń.

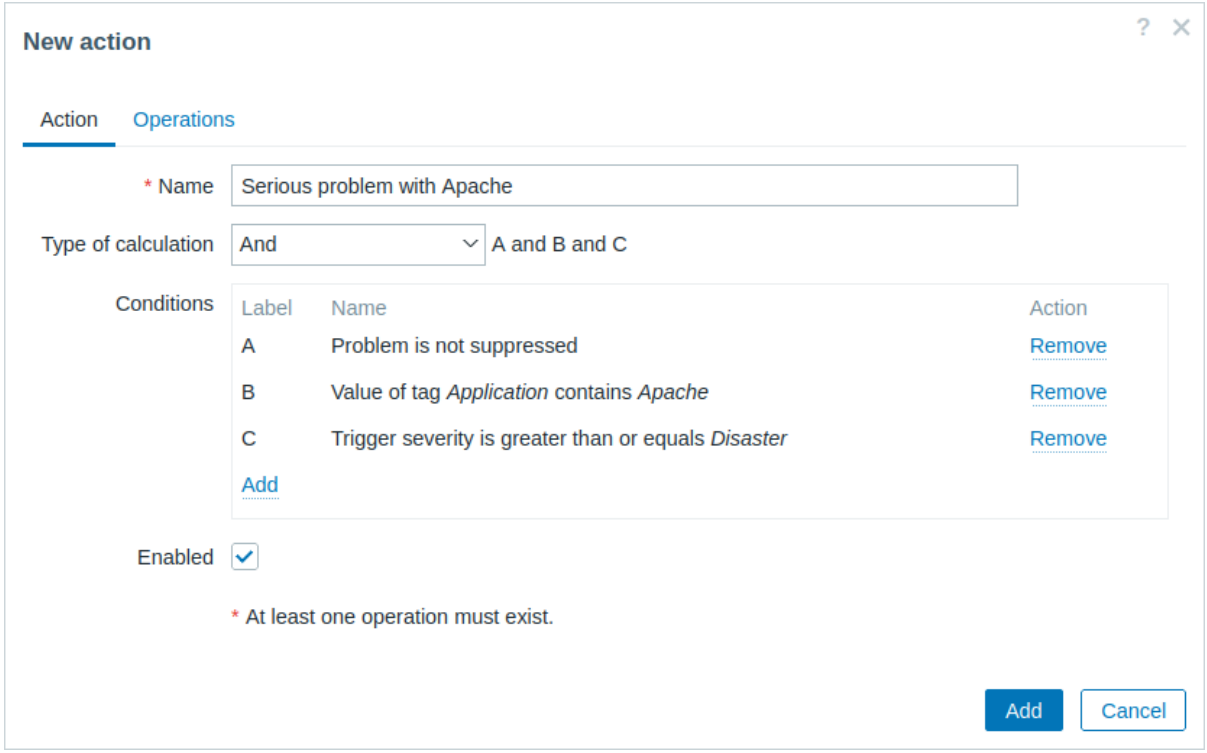
Konfiguracja

Te zdalne polecenia, które są wykonywane na Zabbix agent (niestandardowe skrypty), muszą być najpierw włączone w konfiguracji agenta.

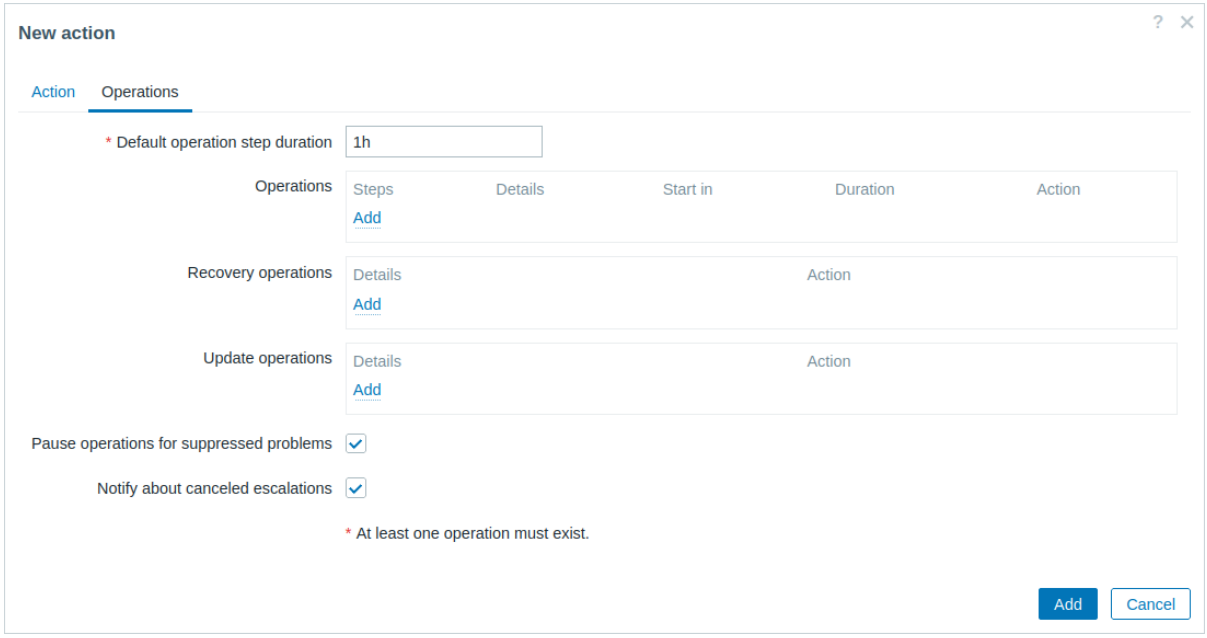
Upewnij się, że parametr AllowKey=system.run[<command>,*] jest dodany dla każdego dozwolonego polecenia w konfiguracji agenta, aby zezwolić na określone polecenie w trybie nowait. Jeśli zmieniasz ten parametr, uruchom ponownie demon agenta.

Następnie, podczas konfigurowania nowej akcji w *Alerty* → *Akcje* → *Akcje wyzwalaczy*:

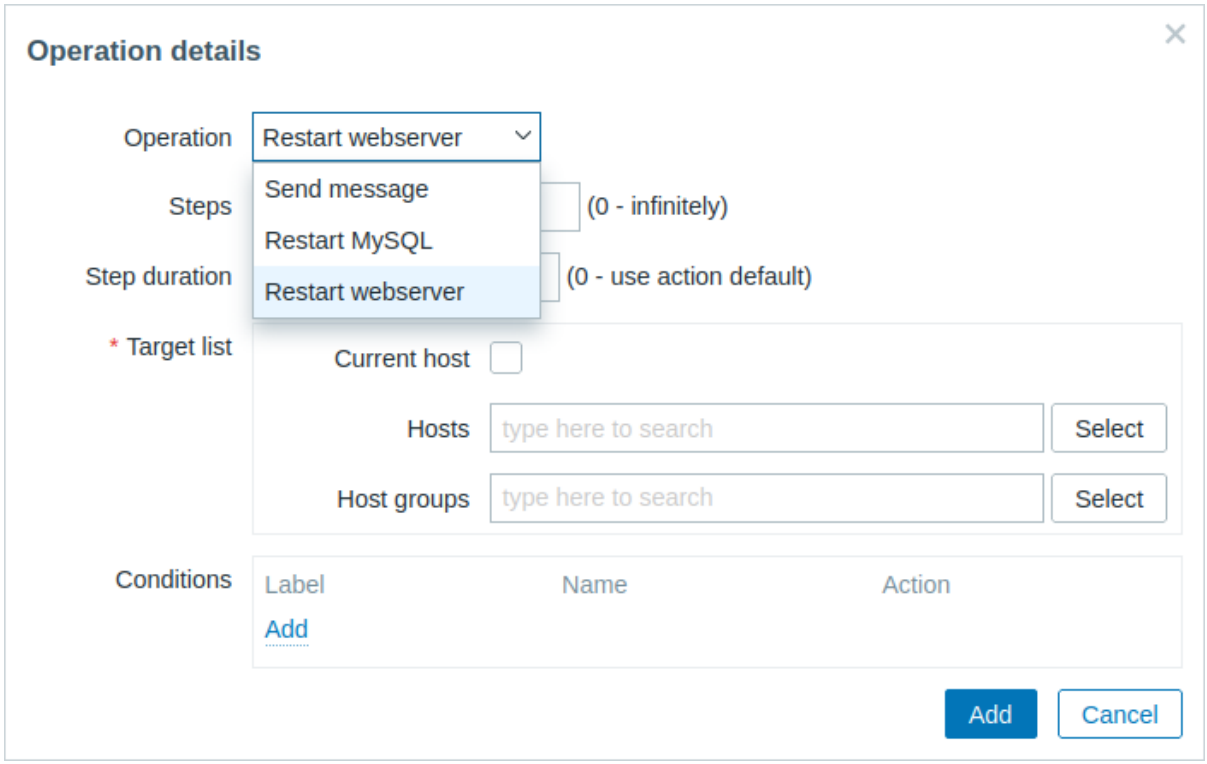
1. Zdefiniuj odpowiednie warunki, na przykład ustaw, aby akcja była aktywowana przy dowolnych problemach o poziomie katastrofa dla jednej z aplikacji Apache.



2. Na karcie *Operacje* kliknij *Dodaj* w bloku *Operacje*, *Operacje odzyskiwania* lub *Operacje aktualizacji*.



3. Wybierz jeden ze wstępnie zdefiniowanych skryptów z listy rozwijanej *Operacja* i ustaw *Listę docelową* dla skryptu.



Predefiniowane skrypty

Skrypty dostępne dla operacji akcji (webhook, skrypt, SSH, Telnet, IPMI) są definiowane w skryptach globalnych.

Na przykład:

```
sudo /etc/init.d/apache restart
```

W tym przypadku Zabbix spróbuje zrestartować proces Apache. W przypadku tego polecenia należy upewnić się, że polecenie jest wykonywane na Zabbix agent (kliknij przycisk *Zabbix agent* przy opcji *Execute on*).

Attention:
Zwróć uwagę na użycie **sudo** — użytkownik Zabbix domyślnie nie ma uprawnień do restartowania usług systemowych. Poniżej znajdują się wskazówki dotyczące konfiguracji **sudo**.

Note:
Począwszy od Zabbix agent 7.0, polecenia zdalne mogą być również wykonywane na agencie działającym w trybie aktywnym. Zabbix agent — zarówno aktywny, jak i pasywny — powinien działać na zdalnym hoście i wykonuje polecenia w tle.

Polecenia zdalne na Zabbix agent są wykonywane bez limitu czasu przez klucz system.run[,nowait] i nie są sprawdzane pod kątem wyników wykonania. Na Zabbix serwer i Zabbix proxy polecenia zdalne są wykonywane z limitem czasu ustawionym w parametrze TrapperTimeout pliku zabbix_server.conf lub zabbix_proxy.conf, a ich wyniki wykonania są sprawdzane. Dodatkowe informacje można znaleźć w sekcji *Limit czasu skryptu*.

Uprawnienia dostępu

Upewnij się, że użytkownik 'zabbix' ma uprawnienia do wykonywania skonfigurowanych poleceń. Można rozważyć użycie **sudo**, aby przyznać dostęp do uprzywilejowanych poleceń. Aby skonfigurować dostęp, wykonaj jako root:

```
visudo
```

Przykładowe linie, które można umieścić w pliku *sudoers*:

```
# pozwala użytkownikowi 'zabbix' uruchamiać wszystkie polecenia bez hasła.
zabbix ALL=NOPASSWD: ALL

# pozwala użytkownikowi 'zabbix' restartować apache bez hasła.
zabbix ALL=NOPASSWD: /etc/init.d/apache restart
```

Note:
W niektórych systemach plik *sudoers* uniemożliwia użytkownikom nielokalnym wykonywanie poleceń. Aby to zmienić, zakomentuj opcję **requiretty** w */etc/sudoers*.

Zdalne polecenia przy wielu interfejsach

Jeśli system docelowy ma wiele interfejsów wybranego typu (agent Zabbix lub IPMI), zdalne polecenia będą wykonywane na domyślnym interfejsie.

Możliwe jest wykonywanie zdalnych poleceń przez SSH i Telnet przy użyciu interfejsu innego niż interfejs agenta Zabbix. Dostępny interfejs do użycia jest wybierany w następującej kolejności:

- Domyślny interfejs agenta Zabbix
- Domyślny interfejs SNMP
- Domyślny interfejs JMX
- Domyślny interfejs IPMI

Zdalne polecenia IPMI

Dla zdalnych poleceń IPMI należy używać następującej składni:

```
<command> [<value>]
```

gdzie

- <command> - jedno z poleceń IPMI bez spacji
- <value> - 'on', 'off' lub dowolna nieujemna liczba całkowita. <value> jest parametrem opcjonalnym.

Przykłady

Przykłady globalnych skryptów, które mogą być używane jako zdalne polecenia w operacjach akcji.

Przykład 1

Restart systemu Windows przy określonym warunku.

Aby automatycznie zrestartować system Windows po wykryciu problemu przez Zabbix, zdefiniuj następujący skrypt:

Parametr skryptu	Wartość
Zakres	'Operacja akcji'
Typ	'Skrypt'
Polecenie	c:\windows\system32\shutdown.exe -r -f

Przykład 2

Uruchom ponownie host przy użyciu sterowania IPMI.

Parametr skryptu	Wartość
Zakres	'Operacja akcji'
Typ	'IPMI'
Polecenie	reset

Przykład 3

Wyłącz zasilanie hosta za pomocą sterowania IPMI.

Parametr skryptu	Wartość
Zakres	'Operacja akcji'
Typ	'IPMI'
Polecenie	power off

3 Dodatkowe operacje

Przegląd

W tej sekcji możesz znaleźć szczegóły dodatkowych operacji dla zdarzeń wykrywania/autorejestracji.

Dodawanie hosta

Hosty są dodawane podczas procesu wykrywania, natychmiast po wykryciu hosta, a nie dopiero na końcu procesu wykrywania.

Note:
Ponieważ wykrywanie sieci może zająć trochę czasu z powodu wielu niedostępnych hostów/usług, zaleca się cierpliwość i używanie rozsądnych zakresów IP.

Podczas dodawania hosta jego nazwa jest ustalana przez standardową funkcję **gethostbyname**. Jeśli host może zostać rozwiązany, używana jest rozwiązana nazwa. Jeśli nie, używany jest adres IP. Ponadto, jeśli jako nazwa hosta musi zostać użyty adres IPv6, wszystkie ":" (dwukropki) są zastępowane przez "_" (podkreślenia), ponieważ dwukropki nie są dozwolone w nazwach hostów.

Attention:
Jeśli wykrywanie jest wykonywane przez proxy, obecnie wyszukiwanie nazwy hosta nadal odbywa się na serwerze Zabbix.

Attention:
Jeśli host o tej samej nazwie co nowo wykryty już istnieje w konfiguracji Zabbix, Zabbix doda **_N** do nazwy hosta, gdzie **N** jest rosnącą liczbą, zaczynając od 2.

4 Używanie makr w wiadomościach

Przegląd

W tematach wiadomości i treści wiadomości można używać makr w celu bardziej efektywnego raportowania problemów.

Oprócz wielu wbudowanych makr obsługiwane są również makra użytkownika oraz makra wyrażeń. Dostępna jest pełna lista makr obsługiwanych przez Zabbix.

Przykłady

Przykłady tutaj ilustrują, jak można używać makr w wiadomościach.

Przykład 1

Temat wiadomości:

```
Problem: {TRIGGER.NAME}
```

Po otrzymaniu wiadomości temat wiadomości zostanie zastąpiony czymś takim jak:

```
Problem: Obciążenie procesora jest zbyt wysokie na serwerze Zabbix
```

Przykład 2

Wiadomość:

```
Obciążenie procesora wynosi: {?last(/zabbix.zabbix.com/system.cpu.load[,avg1])}
```

Po otrzymaniu wiadomości treść wiadomości zostanie zastąpiona czymś takim jak:

```
Obciążenie procesora wynosi: 1.45
```

Przykład 3

Wiadomość:

```
Ostatnia wartość: {?last(/{HOST.HOST}/{ITEM.KEY})}
MAX z 15 minut: {?max(/{HOST.HOST}/{ITEM.KEY},15m)}
MIN z 15 minut: {?min(/{HOST.HOST}/{ITEM.KEY},15m)}
```

Po otrzymaniu wiadomości jej treść zostanie zastąpiona czymś takim jak:

```
Ostatnia wartość: 1.45
MAX z 15 minut: 2.33
MIN z 15 minut: 1.01
```

Przykład 4

Wiadomość:

```
http://<server_ip_or_name>/zabbix/tr_events.php?triggerid={TRIGGER.ID}&eventid={EVENT.ID}
```

Po otrzymaniu wiadomości będzie ona zawierać link do strony *Szczegóły zdarzenia*, która zawiera informacje o zdarzeniu, jego wyzwalaczu oraz listę najnowszych zdarzeń wygenerowanych przez ten sam wyzwalacz.

Przykład 5

Informowanie o wartościach z kilku hostów w wyrażeniu wyzwalacza.

Wiadomość:

```
Nazwa problemu: {TRIGGER.NAME}
Wyrażenie wyzwalacza: {TRIGGER.EXPRESSION}

1. Wartość pozycji na hoście {HOST.NAME1}: {ITEM.VALUE1} ({ITEM.NAME1})
2. Wartość pozycji na hoście {HOST.NAME2}: {ITEM.VALUE2} ({ITEM.NAME2})
```

Po otrzymaniu wiadomości zostanie ona zastąpiona czymś takim:

```
Nazwa problemu: Obciążenie procesora jest zbyt wysokie na lokalnym hoście
Wyrażenie wyzwalacza: last(/Myhost/system.cpu.load[percpu,avg1])>5 or last(/Myotherhost/system.cpu.load[pe

1. Wartość pozycji na hoście Myhost: 0.83 (Obciążenie procesora (średnia 1-minutowa na rdzeń))
2. Wartość pozycji na hoście Myotherhost: 5.125 (Obciążenie procesora (średnia 1-minutowa na rdzeń))
```

Przykład 6

Otrzymywanie szczegółów zarówno zdarzenia problemu, jak i zdarzenia odzyskania w wiadomości odzyskania:

Wiadomość:

```
Problem:

ID zdarzenia: {EVENT.ID}
Wartość zdarzenia: {EVENT.VALUE}
Status zdarzenia: {EVENT.STATUS}
Czas zdarzenia: {EVENT.TIME}
Data zdarzenia: {EVENT.DATE}
Wiek zdarzenia: {EVENT.AGE}
Potwierdzenie zdarzenia: {EVENT.ACK.STATUS}
Historia aktualizacji zdarzenia: {EVENT.UPDATE.HISTORY}

Odzyskanie:
```

```
ID zdarzenia: {EVENT.RECOVERY.ID}
Wartość zdarzenia: {EVENT.RECOVERY.VALUE}
Status zdarzenia: {EVENT.RECOVERY.STATUS}
Czas zdarzenia: {EVENT.RECOVERY.TIME}
Data zdarzenia: {EVENT.RECOVERY.DATE}
Dane operacyjne: {EVENT.OPDATA}
```

Po otrzymaniu wiadomości makra zostaną zastąpione czymś takim:

```
Problem:

ID zdarzenia: 21874
Wartość zdarzenia: 1
Status zdarzenia: PROBLEM
Czas zdarzenia: 13:04:30
Data zdarzenia: 2018.01.02
Wiek zdarzenia: 5m 0s
Potwierdzenie zdarzenia: Tak
Historia aktualizacji zdarzenia: 2018.01.02 13:05:51 "John Smith (Admin)"
Działania: potwierdzono.

Odzyskanie:

ID zdarzenia: 21896
Wartość zdarzenia: 0
Status zdarzenia: OK
Czas zdarzenia: 13:10:07
Data zdarzenia: 2018.01.02
Dane operacyjne: Bieżąca wartość to 0.83
```

3 Operacje odzyskiwania

Przegląd

Operacje odzyskiwania umożliwiają otrzymywanie powiadomień, gdy problemy zostaną rozwiązane.

Zarówno wiadomości, jak i zdalne polecenia są obsługiwane w operacjach odzyskiwania. Chociaż można dodać kilka operacji, eskalacja nie jest obsługiwana — wszystkie operacje są przypisane do jednego kroku i dlatego zostaną wykonane jednocześnie.

Przypadki użycia

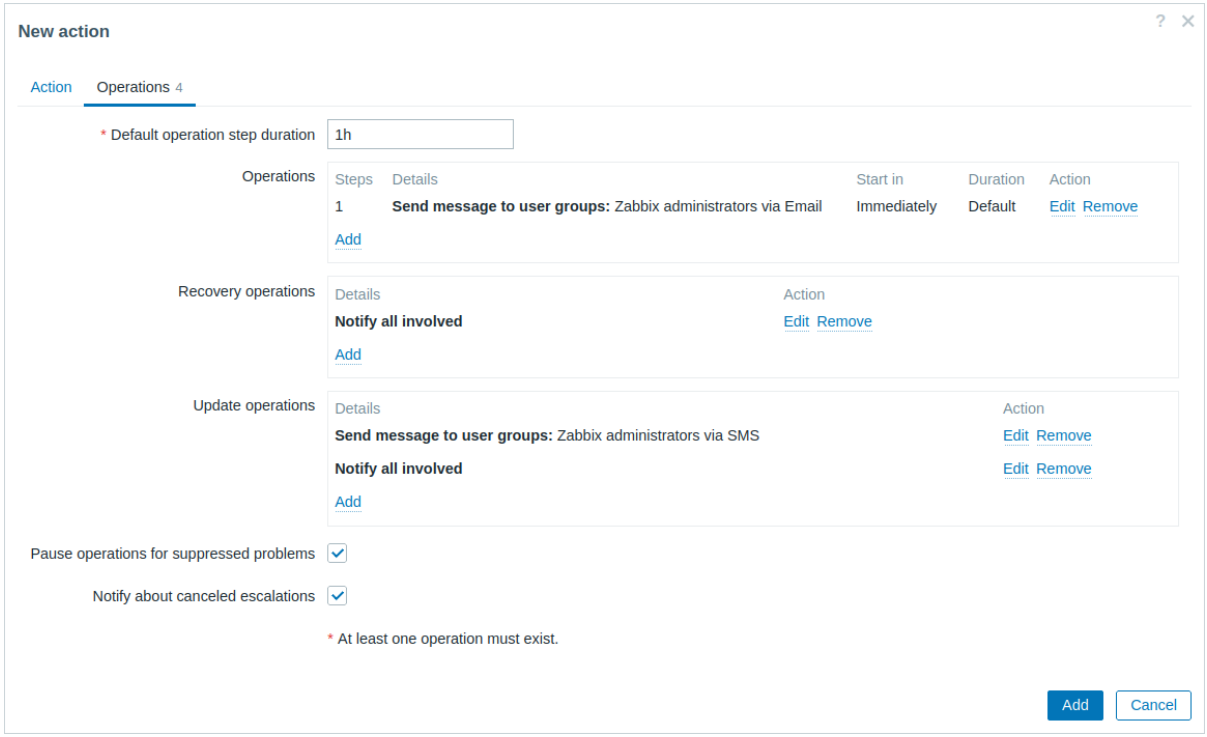
Niektóre przypadki użycia operacji odzyskiwania są następujące:

1. Powiadom przy odzyskaniu wszystkich użytkowników, którzy zostali powiadomieni o problemie:
   - Wybierz *Powiadom wszystkich zaangażowanych* jako typ operacji.
2. Miej wiele operacji przy odzyskaniu: wyślij powiadomienie i wykonaj zdalne polecenie:
   - Dodaj typy operacji do wysyłania wiadomości i wykonywania polecenia.
3. Otwórz zgłoszenie w zewnętrznym systemie helpdesk/ticketing i zamknij je po rozwiązaniu problemu:
   - Utwórz zewnętrzny skrypt, który komunikuje się z systemem helpdesk.
   - Utwórz akcję z operacją, która wykonuje ten skrypt i w ten sposób otwiera zgłoszenie.
   - Skonfiguruj operację odzyskiwania, która wykonuje ten skrypt z innymi parametrami i zamyka zgłoszenie.
   - Użyj makra {EVENT.ID}, aby odwołać się do pierwotnego problemu.

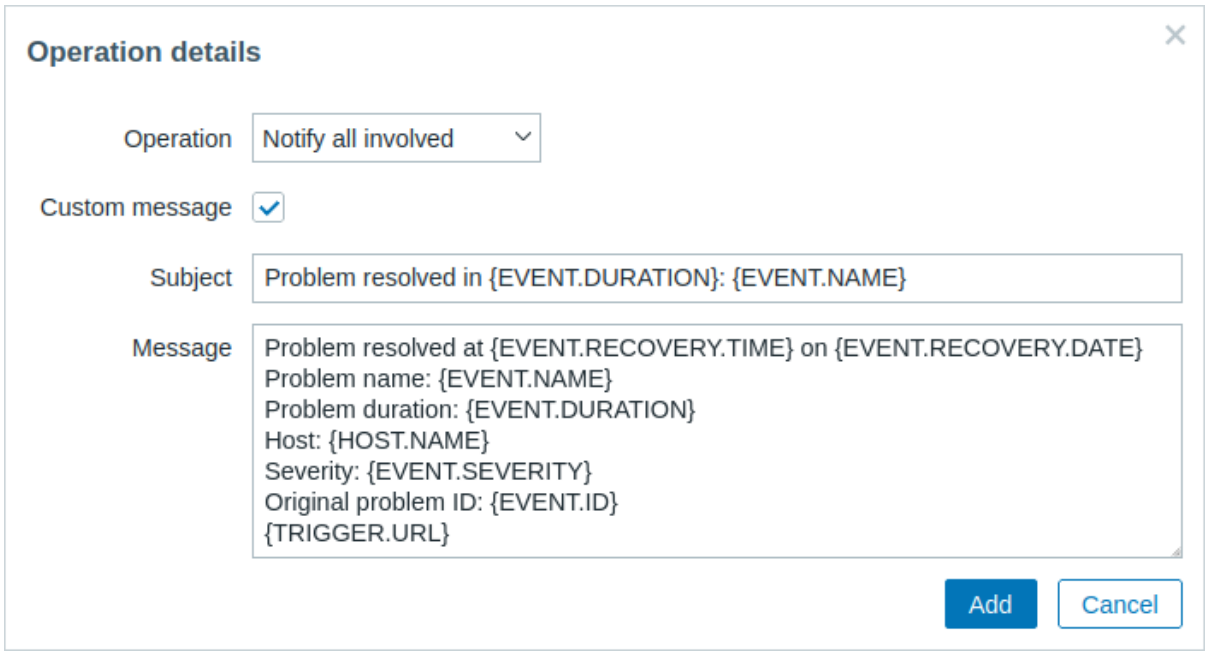
Konfigurowanie operacji odzyskiwania

Aby skonfigurować operację odzyskiwania, wykonaj następujące kroki:

1. Przejdź do zakładki *Operations* w formularzu konfiguracji akcji.
2. Aby skonfigurować nową operację odzyskiwania, kliknij *Add* w sekcji *Recovery operations*. Aby edytować istniejącą operację, kliknij *Edit* obok operacji.
3. Skonfiguruj szczegóły operacji.



Szczegóły operacji odzyskiwania



Dla zdarzeń odzyskiwania dostępne są trzy typy operacji:

- **Wyślij wiadomość** — wyślij wiadomość odzyskiwania do określonego użytkownika;
- **Powiadom wszystkich zaangażowanych** — wyślij wiadomość odzyskiwania do wszystkich użytkowników, którzy zostali powiadomieni o zdarzeniu problemowym;
- **<nazwa zdalnego polecenia>** — wykonaj zdalne polecenie. Polecenia są dostępne do wykonania, jeśli zostały wcześniej zdefiniowane w skryptach globalnych z wybranym zakresem *Action operation*.

Parametry dla każdego typu operacji opisano poniżej. Wszystkie wymagane pola wejściowe są oznaczone czerwoną gwiazdką. Po zakończeniu kliknij *Dodaj*, aby dodać operację do listy *Operacje odzyskiwania*.

Note:
Zwróć uwagę, że jeśli ten sam odbiorca jest zdefiniowany w kilku typach operacji bez określonej opcji *Własna wiadomość*, zduplikowane powiadomienia nie są wysyłane.

Typ operacji: wyślij wiadomość

Parametr		Opis
Wyślij do grup użytkowników		Wybierz grupy użytkowników, do których ma zostać wysłana wiadomość o odzyskaniu. Aby otrzymać powiadomienie, grupa użytkowników musi mieć co najmniej uprawnienia „odczyt” do hosta permissions.
Wyślij do użytkowników		Wybierz użytkowników, do których ma zostać wysłana wiadomość o odzyskaniu. Aby otrzymać powiadomienie, użytkownik musi mieć co najmniej uprawnienia „odczyt” do hosta permissions.
Wyślij do typu nośnika		Wyślij domyślną wiadomość o odzyskaniu do wszystkich dostępnych (skonfigurowanych i włączonych) typów nośników lub tylko do jednego określonego typu.
Własna wiadomość		Jeśli ta opcja jest zaznaczona, można zdefiniować własną wiadomość.
	Temat	Temat własnej wiadomości. Temat może zawierać makra.
	Wiadomość	Własna wiadomość. Wiadomość może zawierać makra.

Typ operacji: zdalne polecenie

Parametr	Opis
Lista celów	Wybierz cele, na których ma zostać wykonane polecenie: **Bieżący host** - polecenie jest wykonywane na hoście wyzwalacza, który spowodował zdarzenie problemu. Ta opcja nie będzie działać, jeśli w wyzwalaczu występuje wiele hostów. **Host** - wybierz host(y), na których ma zostać wykonane polecenie. **Grupa hostów** - wybierz grupę(y) hostów, na których ma zostać wykonane polecenie. Określenie nadrzędnej grupy hostów powoduje domyślnie wybranie wszystkich zagnieżdżonych grup hostów. W związku z tym zdalne polecenie zostanie również wykonane na hostach z grup zagnieżdżonych. Polecenie na hoście jest wykonywane tylko raz, nawet jeśli host pasuje więcej niż jeden raz (np. z kilku grup hostów; indywidualnie i z grupy hostów). Lista celów nie ma znaczenia, jeśli polecenie jest wykonywane na serwerze Zabbix. Wybranie większej liczby celów w takim przypadku powoduje jedynie, że polecenie zostanie wykonane na serwerze więcej razy. Zwróć uwagę, że w przypadku skryptów globalnych wybór celu zależy również od ustawienia *Grupa hostów* w konfiguracji skryptu globalnego.

Typ operacji: powiadom wszystkich zaangażowanych

Parametr		Opis
Własna wiadomość		Jeśli zaznaczone, można zdefiniować własną wiadomość.
	Temat	Temat własnej wiadomości. Temat może zawierać makra.
	Wiadomość	Własna wiadomość. Wiadomość może zawierać makra.

4 Operacje aktualizacji

Przegląd

Operacje aktualizacji są dostępne w akcjach z następującymi źródłami zdarzeń:

- *Wyzwalacze* — gdy problemy są aktualizowane przez innych użytkowników, tj. dodano do nich komentarz, zostały potwierdzone, zmieniono ich ważność, zamknięto je (ręcznie);
- *Usługi* — gdy ważność usługi uległa zmianie, ale usługa nadal nie została przywrócona.

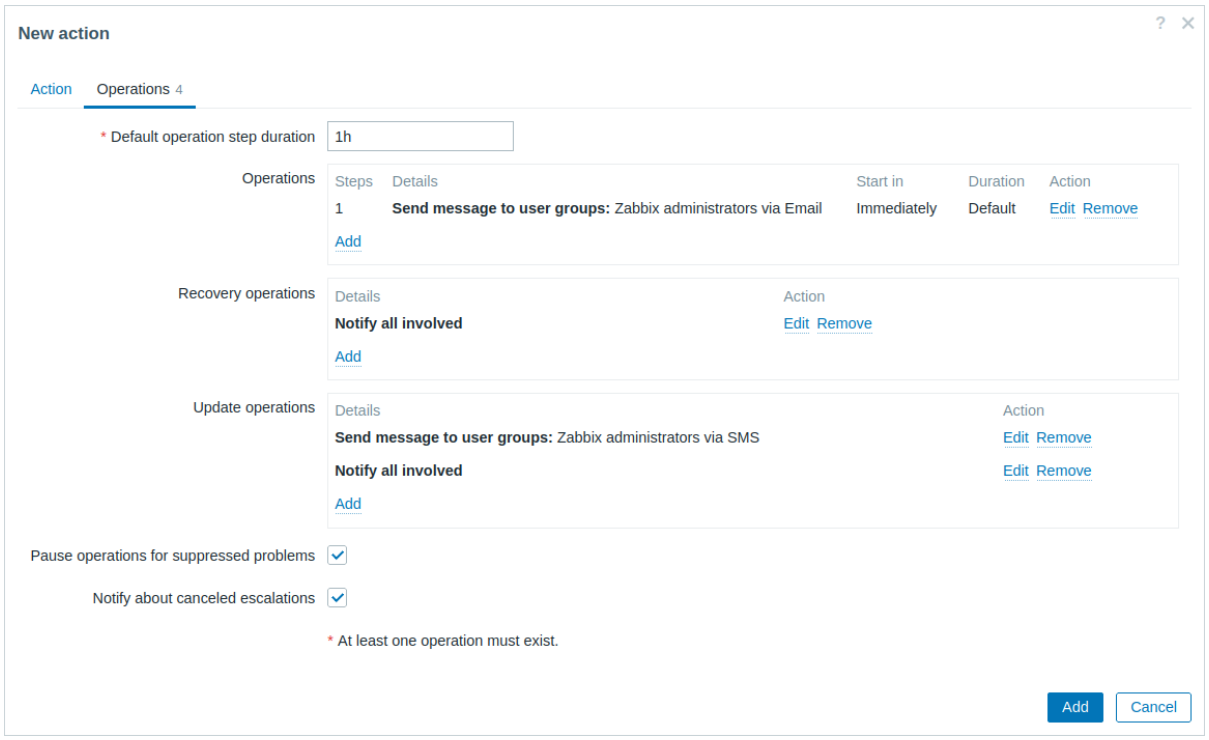
Należy pamiętać, że użytkownicy nie otrzymują powiadomień o własnych aktualizacjach.

W operacjach aktualizacji obsługiwane są zarówno wiadomości, jak i zdalne polecenia. Chociaż można dodać kilka operacji, eskalacja nie jest obsługiwana — wszystkie operacje są przypisywane do jednego kroku i dlatego będą wykonywane jednocześnie.

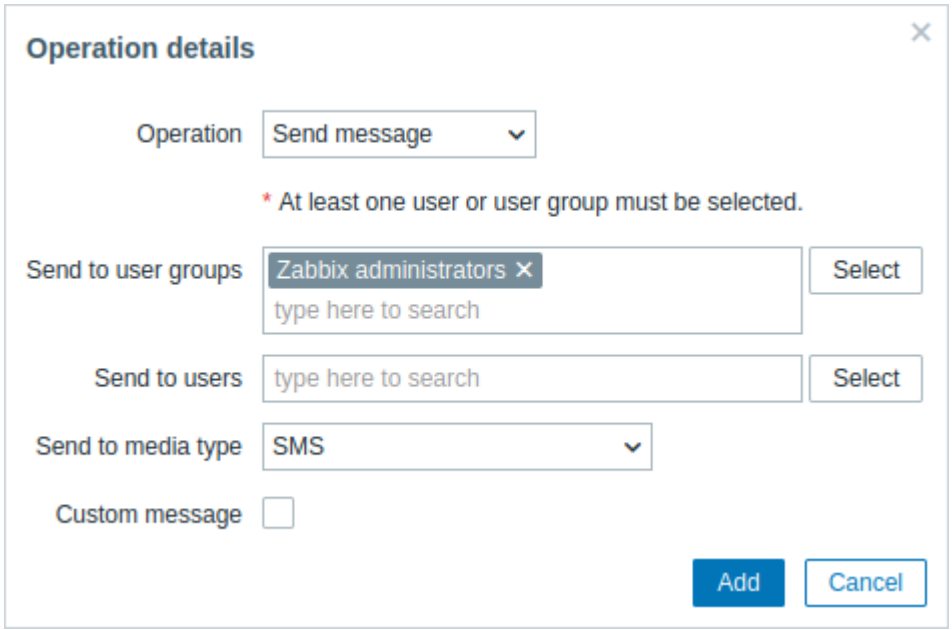
Konfigurowanie operacji aktualizacji

Aby skonfigurować operację aktualizacji, wykonaj następujące kroki:

1. Przejdź do zakładki *Operacje* w formularzu konfiguracji akcji.
2. Aby skonfigurować nową operację aktualizacji, kliknij *Dodaj* w sekcji *Operacje aktualizacji*. Aby edytować istniejącą operację, kliknij *Edytuj* obok operacji.
3. Skonfiguruj szczegóły operacji.



Szczegóły operacji aktualizacji



Operacje aktualizacji oferują ten sam zestaw parametrów co Operacje odzyskiwania.

5 Eskalacje

Overview

With escalations you can create custom scenarios for sending notifications or executing remote commands.

In practical terms it means that:

- Users can be informed about new problems immediately
- Notifications can be repeated until the problem is resolved
- Sending a notification can be delayed
- Notifications can be escalated to another ”higher” user group
- Remote commands can be executed immediately or when a problem is not resolved for a lengthy period

Actions are escalated based on the **escalation step**. Each step has a duration in time.

You can define both the default duration and a custom duration of an individual step. The minimum duration of one escalation step is 60 seconds.

You can start actions, such as sending notifications or executing commands, from any step. Step one is for immediate actions. If you want to delay an action, you can assign it to a later step. For each step, several actions can be defined.

The number of escalation steps is not limited.

Escalations are defined when configuring an operation. Escalations are supported for problem operations only, not recovery.

Różne aspekty zachowania eskalacji

Rozważmy, co dzieje się w różnych okolicznościach, jeśli akcja zawiera kilka kroków eskalacji.

Sytuacja	Zachowanie
Dany host przechodzi w tryb maintenance po wysłaniu początkowego powiadomienia o problemie	W zależności od ustawienia *Pause operations for suppressed problems* w konfiguracji akcji, wszystkie pozostałe kroki eskalacji są wykonywane albo z opóźnieniem spowodowanym okresem maintenance, albo bez opóźnienia. Okres maintenance nie anuluje operacji.
*Okres czasu zdefiniowany w warunku akcji **Time period** kończy się po wysłaniu początkowego powiadomienia*	Wszystkie pozostałe kroki eskalacji są wykonywane. Warunek *Time period* nie może zatrzymać operacji; wpływa on na to, kiedy akcje są uruchamiane lub nie są uruchamiane, a nie na operacje.
Problem rozpoczyna się podczas maintenance i trwa dalej (nie zostaje rozwiązany) po zakończeniu maintenance	W zależności od ustawienia *Pause operations for suppressed problems* w konfiguracji akcji, wszystkie kroki eskalacji są wykonywane albo od momentu zakończenia maintenance, albo natychmiast.
Problem rozpoczyna się podczas maintenance typu no-data i trwa dalej (nie zostaje rozwiązany) po zakończeniu maintenance	Należy poczekać, aż wyzwalacz zostanie uruchomiony, zanim zostaną wykonane wszystkie kroki eskalacji.
Różne eskalacje następują po sobie w krótkich odstępach czasu i nakładają się	Wykonanie każdej nowej eskalacji zastępuje poprzednią eskalację, ale co najmniej jeden krok eskalacji z poprzedniej eskalacji jest zawsze wykonywany. To zachowanie ma znaczenie w akcjach dla zdarzeń tworzonych przy KAŻDEJ ocenie problemu przez wyzwalacz.
W trakcie trwającej eskalacji (na przykład podczas wysyłania wiadomości), na podstawie dowolnego typu zdarzenia: - akcja zostaje wyłączona Na podstawie zdarzenia wyzwalacza: - wyzwalacz zostaje wyłączony - host lub pozycja zostaje wyłączony/wyłączona Na podstawie zdarzenia wewnętrznego dotyczącego wyzwalaczy: - wyzwalacz zostaje wyłączony Na podstawie zdarzenia wewnętrznego dotyczącego pozycji/reguł low-level discovery: - pozycja zostaje wyłączona - host zostaje wyłączony	Wiadomość będąca w trakcie wysyłania zostaje wysłana, a następnie wysyłana jest jeszcze jedna wiadomość w ramach eskalacji. Wiadomość uzupełniająca będzie miała na początku treści komunikat anulowania (*NOTE: Escalation canceled*) z podaniem przyczyny (na przykład *NOTE: Escalation canceled: action ’<Nazwa akcji>’ disabled*). W ten sposób odbiorca zostaje poinformowany, że eskalacja została anulowana i żadne dalsze kroki nie zostaną wykonane. Ta wiadomość jest wysyłana do wszystkich, którzy wcześniej otrzymali powiadomienia. Przyczyna anulowania jest również zapisywana w pliku dziennika serwera (od Debug Level 3=Warning). Zwróć uwagę, że wiadomość *Escalation canceled* jest również wysyłana, jeśli operacje zostały zakończone, ale operacje odzyskiwania są skonfigurowane i nie zostały jeszcze wykonane.

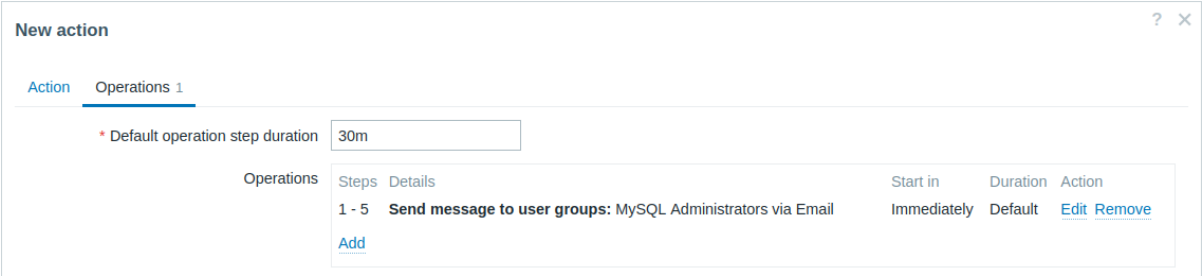
Sytuacja	Zachowanie
W trakcie trwającej eskalacji (na przykład podczas wysyłania wiadomości) akcja zostaje usunięta	Żadne dalsze wiadomości nie są wysyłane. Informacja ta jest zapisywana w pliku dziennika serwera (od Debug Level 3=Warning), na przykład: `escalation canceled: action id:334 deleted`

Przykłady eskalacji

Przykład 1

Wysyłanie powtarzanego powiadomienia co 30 minut (łącznie 5 razy) do grupy „MySQL Administrators". Aby to skonfigurować:

- Na karcie *Operations* ustaw *Default operation step duration* na „30m" (30 minut).
- Ustaw *Steps* eskalacji od „1" do „5".
- Wybierz grupę „MySQL Administrators" jako odbiorców wiadomości.



Powiadomienia będą wysyłane po 0:00, 0:30, 1:00, 1:30 i 2:00 godziny od wystąpienia problemu (chyba że problem zostanie oczywiście rozwiązany wcześniej).

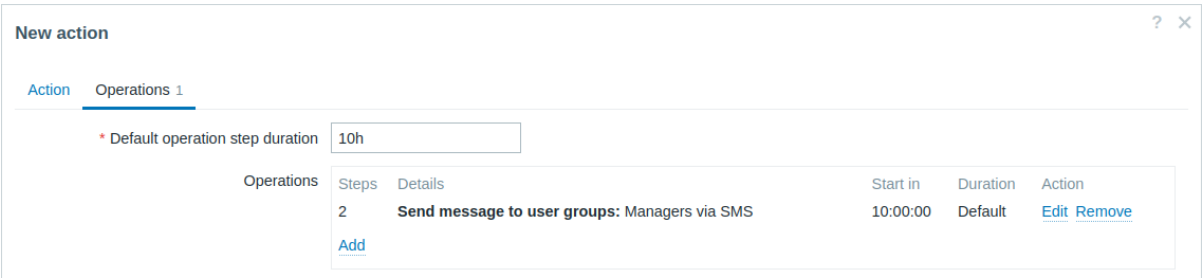
Jeśli problem zostanie rozwiązany i skonfigurowano wiadomość o odzyskaniu, zostanie ona wysłana do tych, którzy otrzymali co najmniej jedną wiadomość o problemie w ramach tego scenariusza eskalacji.

Note:
Jeśli wyzwalacz, który wygenerował aktywną eskalację, zostanie wyłączony, Zabbix wyśle wszystkim osobom, które otrzymały już powiadomienia, wiadomość informacyjną na ten temat.

Przykład 2

Wysyłanie opóźnionego powiadomienia o długotrwałym problemie. Aby to skonfigurować:

- Na karcie *Operations* ustaw *Default operation step duration* na „10h" (10 godzin).
- Ustaw *Steps* eskalacji od „2" do „2".



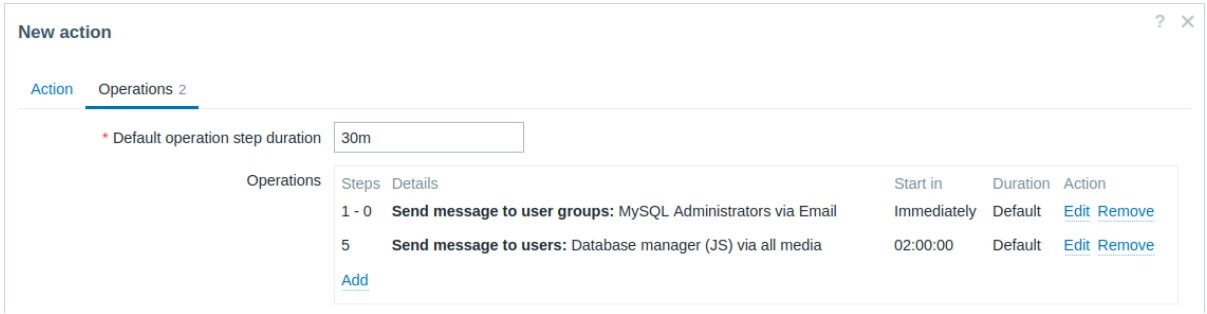
Powiadomienie zostanie wysłane dopiero w kroku 2 scenariusza eskalacji, czyli 10 godzin po wystąpieniu problemu.

Możesz dostosować treść wiadomości do czegoś w rodzaju „Problem trwa dłużej niż 10 godzin".

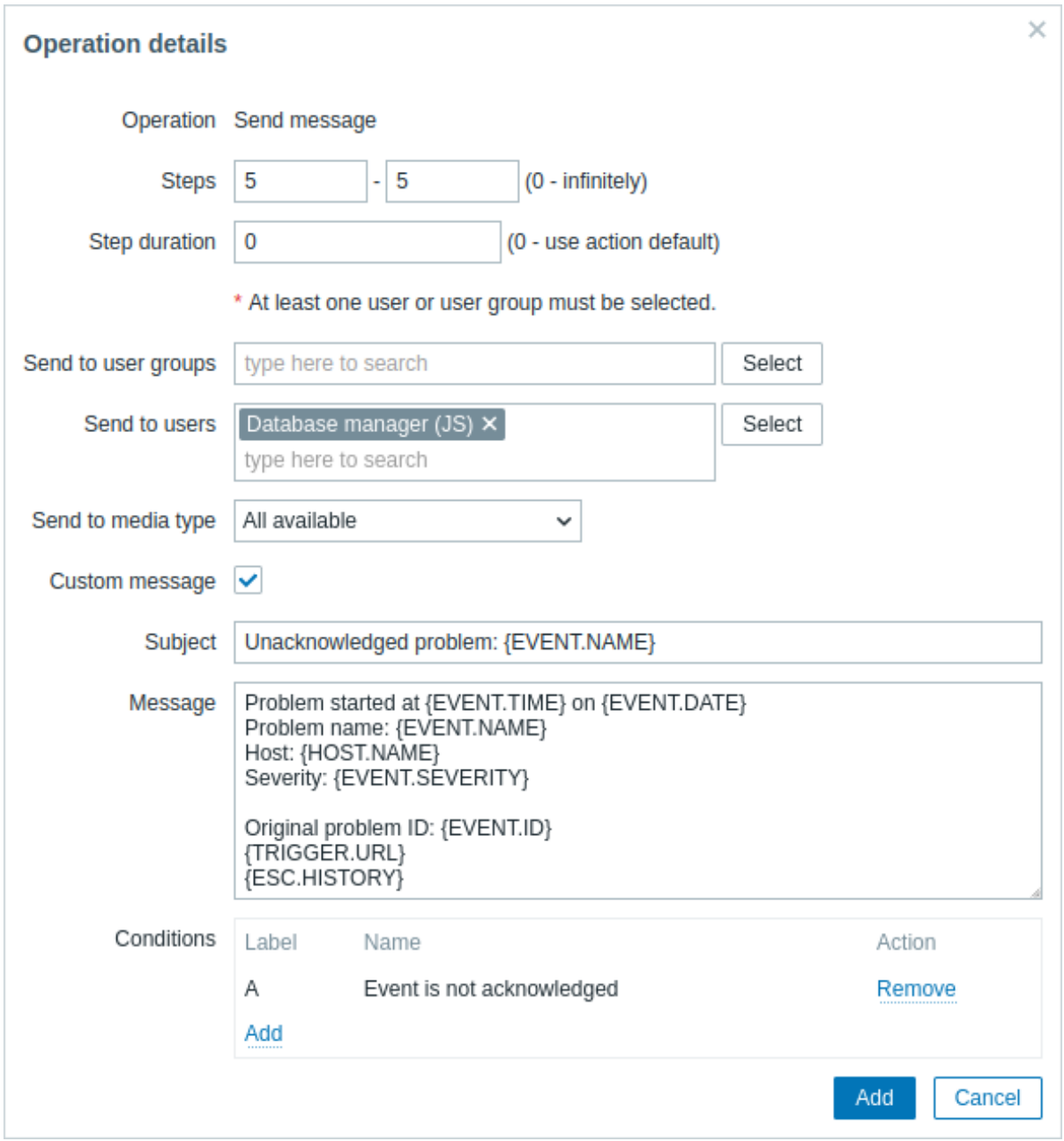
Przykład 3

Eskalacja problemu do Szefa.

W pierwszym przykładzie powyżej skonfigurowaliśmy okresowe wysyłanie wiadomości do administratorów MySQL. W tym przypadku administratorzy otrzymają cztery wiadomości, zanim problem zostanie eskalowany do menedżera bazy danych. Należy pamiętać, że menedżer otrzyma wiadomość tylko wtedy, gdy problem nie został jeszcze potwierdzony, co oznacza, że prawdopodobnie nikt jeszcze nad nim nie pracuje.



Szczegóły operacji 2:



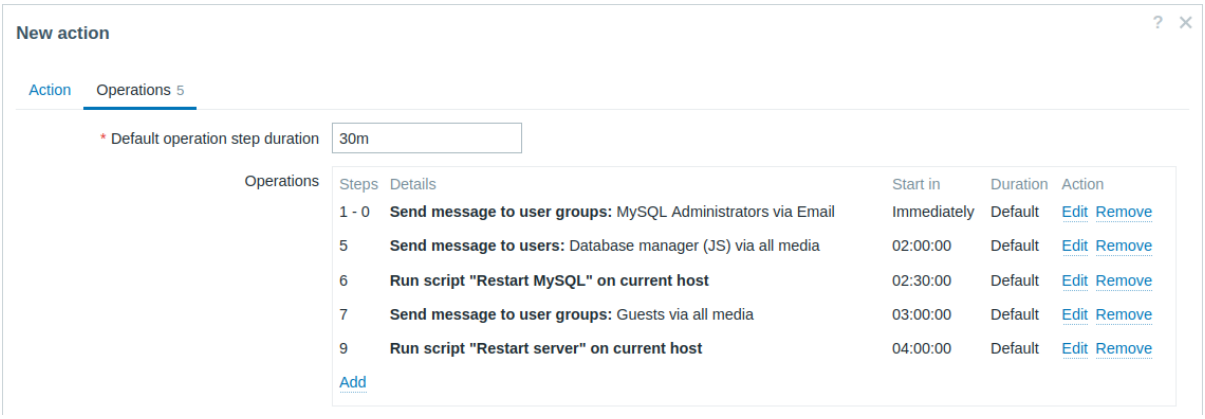
Zwróć uwagę na użycie makra {ESC.HISTORY} w dostosowanej wiadomości. Makro to będzie zawierać informacje o wszystkich wcześniej wykonanych krokach tej eskalacji, takich jak wysłane powiadomienia i wykonane polecenia.

Przykład 4

Bardziej złożony scenariusz. Po wysłaniu wielu wiadomości do administratorów MySQL i eskalacji do menedżera, Zabbix spróbuje ponownie uruchomić bazę danych MySQL. Stanie się to, jeśli problem będzie występował przez 2:30 godziny i nie zostanie potwierdzony.

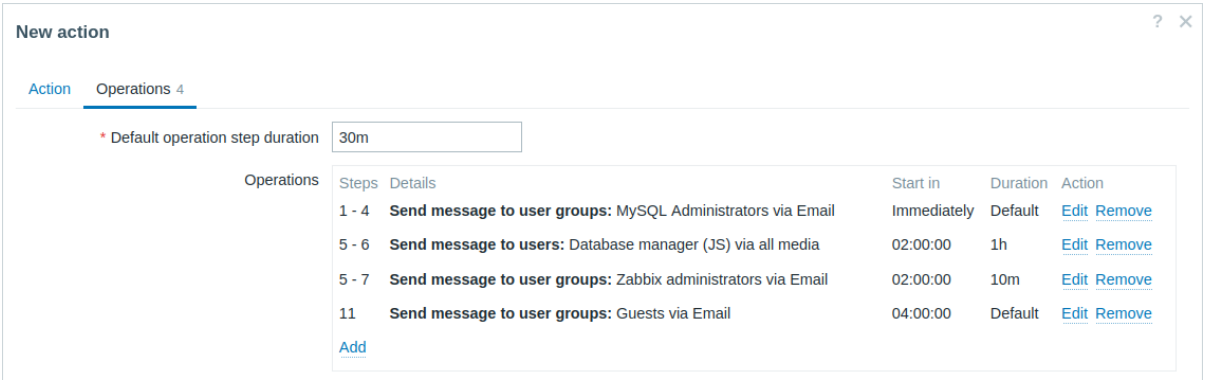
Jeśli problem nadal będzie występował, po kolejnych 30 minutach Zabbix wyśle wiadomość do wszystkich użytkowników gościnnych.

Jeśli to nie pomoże, po kolejnej godzinie Zabbix zrestartuje serwer z bazą danych MySQL (drugie zdalne polecenie) przy użyciu poleceń IPMI.



Przykład 5

Eskalacja z kilkoma operacjami, które mają nakładające się zakresy kroków i niestandardowe interwały. Domyślny czas trwania kroku operacji wynosi 30 minut.



Powiadomienia będą wysyłane w następujący sposób:

- Do administratorów MySQL o 0:00, 0:30, 1:00 i 1:30 od momentu wystąpienia problemu.
- Do menedżera bazy danych o 2:00 i 2:10 (krótszy niestandardowy czas trwania kroku wynoszący 10 minut, zdefiniowany w kolejnej operacji, zastępuje dłuższy czas trwania kroku wynoszący 1 godzinę skonfigurowany tutaj, zgodnie z opisem w Szczegóły operacji dla *Czas trwania kroku*, gdy kroki nakładają się).
- Do administratorów Zabbix o 2:00, 2:10 i 2:20 od momentu wystąpienia problemu (zastosowany jest niestandardowy czas trwania kroku wynoszący 10 minut).
- Do użytkowników guest o 4:00 od momentu wystąpienia problemu (domyślny czas trwania kroku wynoszący 30 minut obowiązuje między krokami 8 i 11).

3 Otrzymywanie powiadomień o nieobsługiwanych pozycjach

Przegląd

Możliwe jest otrzymywanie powiadomień o nieobsługiwanych pozycjach w Zabbix.

Jest to część koncepcji zdarzeń wewnętrznych w Zabbix, umożliwiającej użytkownikom otrzymywanie powiadomień w takich sytuacjach. Zdarzenia wewnętrzne odzwierciedlają zmianę stanu:

- gdy pozycje przechodzą ze stanu „normalny” do „nieobsługiwany” (i z powrotem);
- gdy wyzwalacze przechodzą ze stanu „normalny” do „nieznany” (i z powrotem);
- gdy reguły wykrywania niskiego poziomu przechodzą ze stanu „normalny” do „nieobsługiwany” (i z powrotem).

Ta sekcja przedstawia instrukcję, jak **otrzymywać powiadomienia**, gdy pozycja stanie się nieobsługiwana.

Konfiguracja

Ogólnie proces konfigurowania powiadomienia powinien być znajomy dla osób, które wcześniej konfigurowały alerty w Zabbix.

Krok 1

Skonfiguruj wybrane medium, takie jak e-mail, SMS lub skrypt, które będzie używane do powiadomień. Aby wykonać to zadanie, zapoznaj się z odpowiednimi sekcjami podręcznika.

Attention:
Do powiadamiania o zdarzeniach wewnętrznych używany jest domyślny poziom ważności („Niesklasyfikowane”), więc pozostaw go zaznaczonego podczas konfigurowania mediów użytkownika, jeśli chcesz otrzymywać powiadomienia o zdarzeniach wewnętrznych.

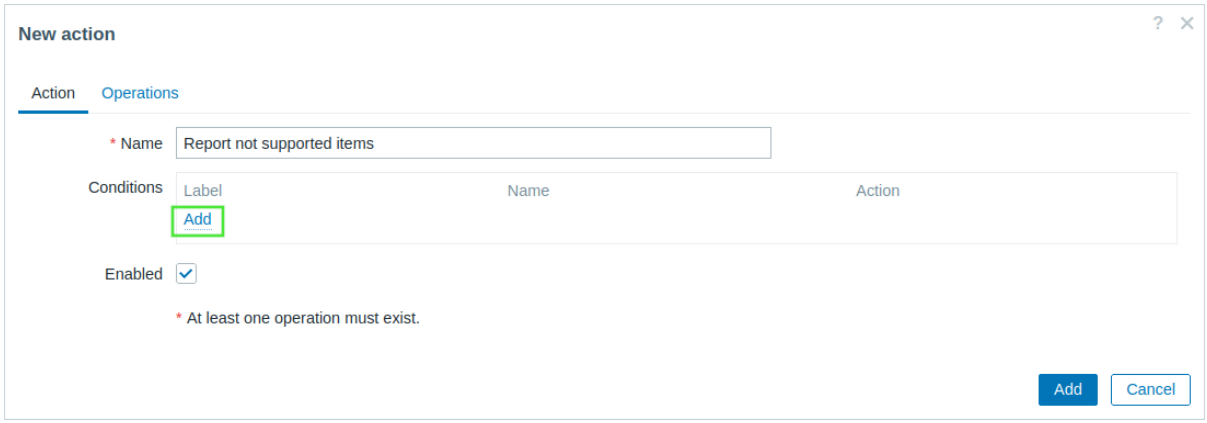
Krok 2

Przejdź do *Alerty* → *Akcje* → *Akcje wewnętrzne*.

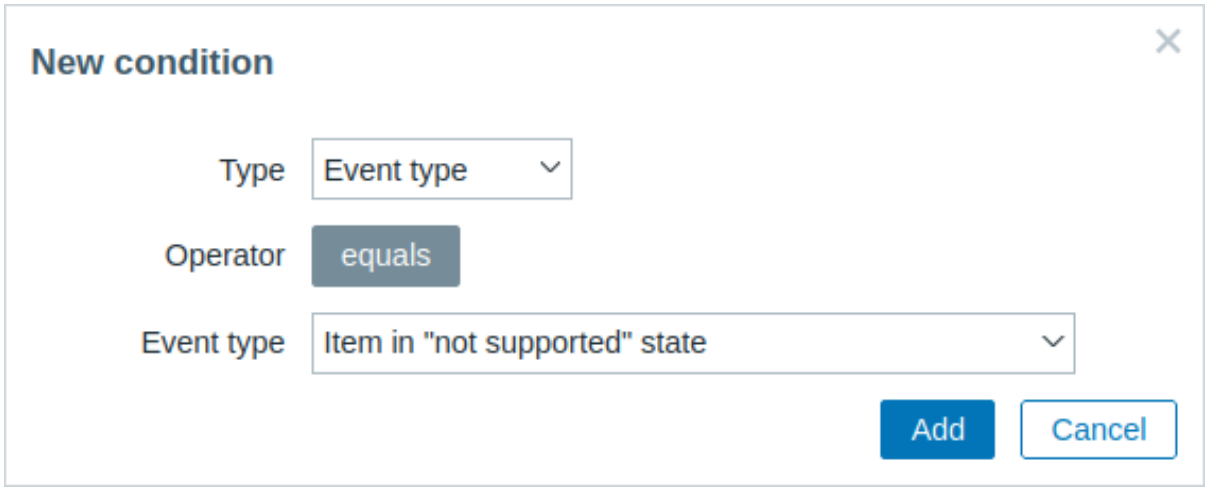
Kliknij *Utwórz akcję* w prawym górnym rogu strony, aby otworzyć formularz konfiguracji akcji.

Krok 3

Na karcie *Action* wprowadź nazwę akcji. Następnie kliknij *Add* w bloku *Conditions*, aby dodać nowy warunek.



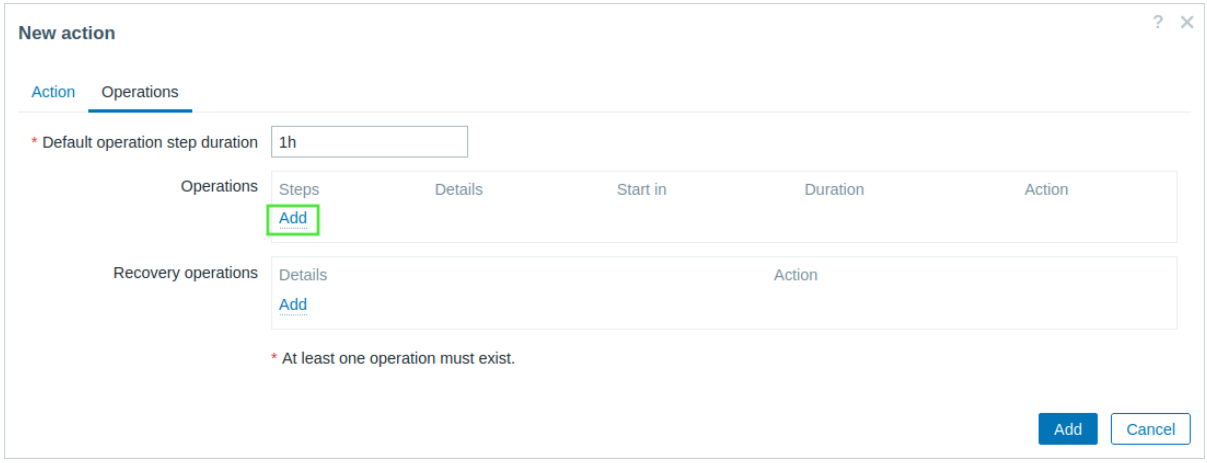
W wyskakującym oknie *New condition* wybierz „Event type” jako typ warunku, a następnie wybierz „Item in ’not supported’ state” jako typ zdarzenia.



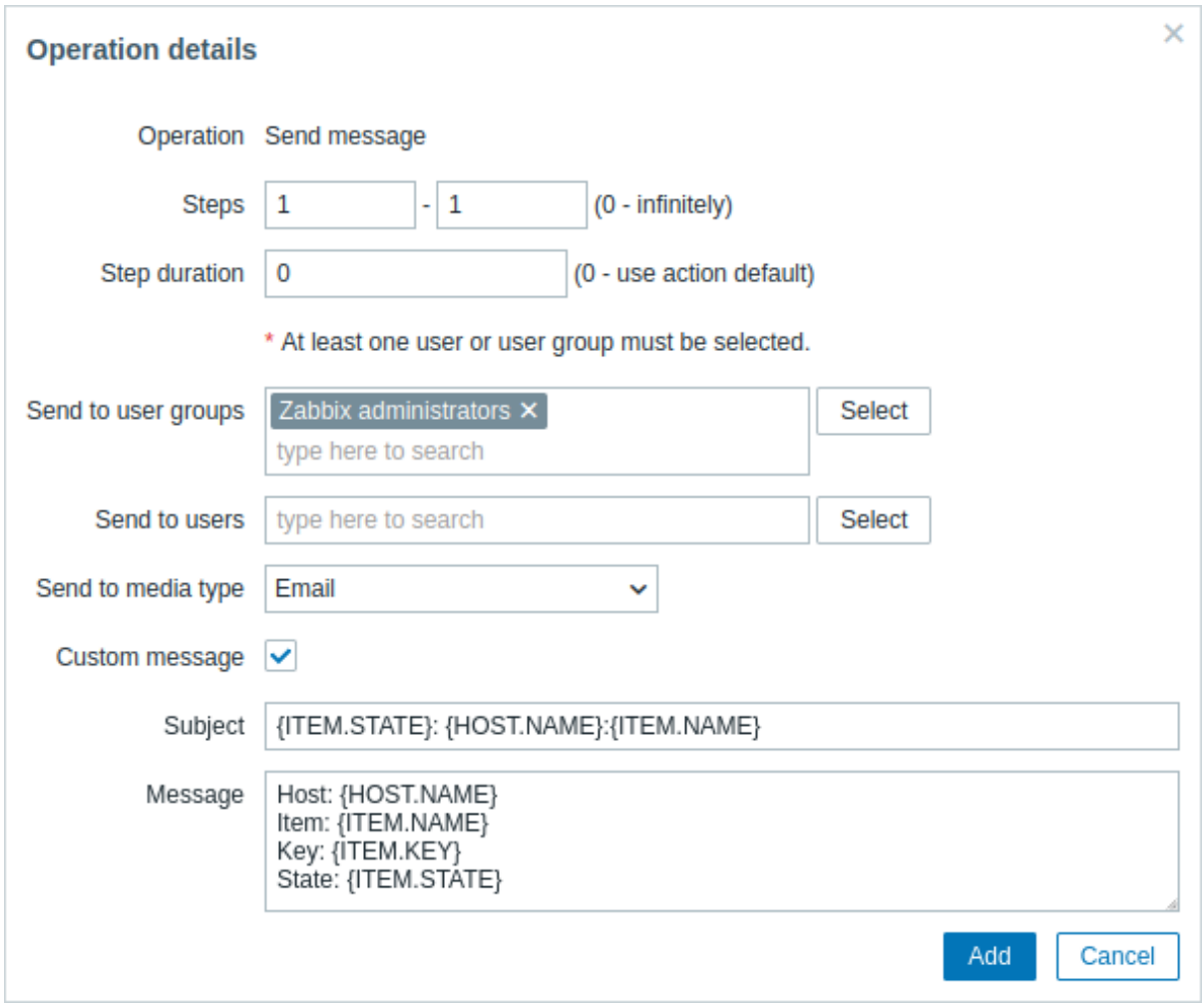
Nie zapomnij kliknąć *Add*, aby warunek został faktycznie dodany do listy w bloku *Conditions*.

Krok 4

W zakładce *Operacje* kliknij *Dodaj* w bloku *Operacje*, aby dodać nową operację.



Wybierz odbiorców wiadomości (grupy użytkowników/użytkowników) oraz typ mediów (lub „Wszystkie”), który ma zostać użyty do dostarczenia wiadomości. Zaznacz pole wyboru *Własna wiadomość*, jeśli chcesz wprowadzić własny temat/treść wiadomości o problemie.

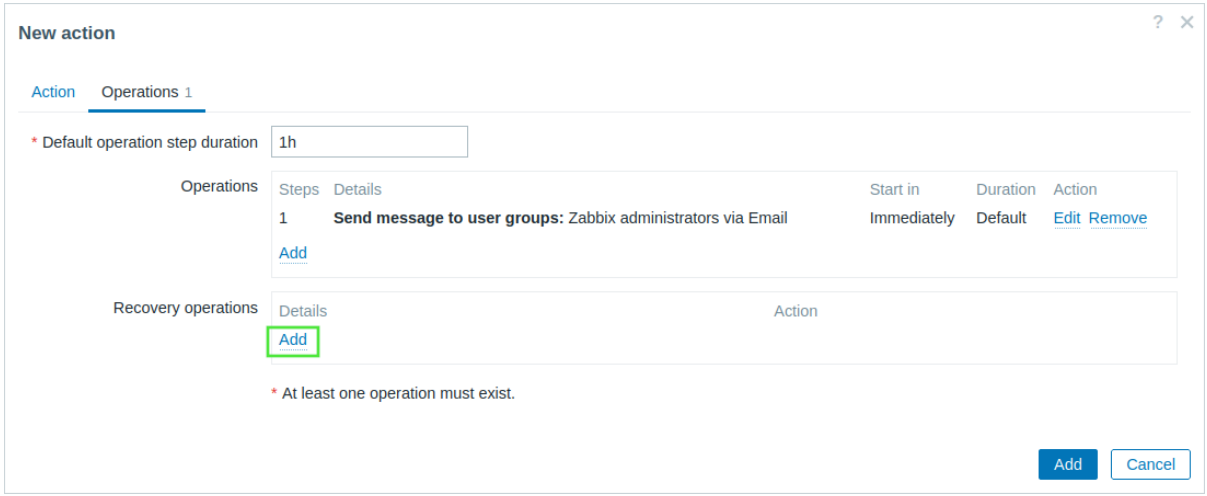


Kliknij *Dodaj*, aby faktycznie wyświetlić operację w bloku *Operacje*.

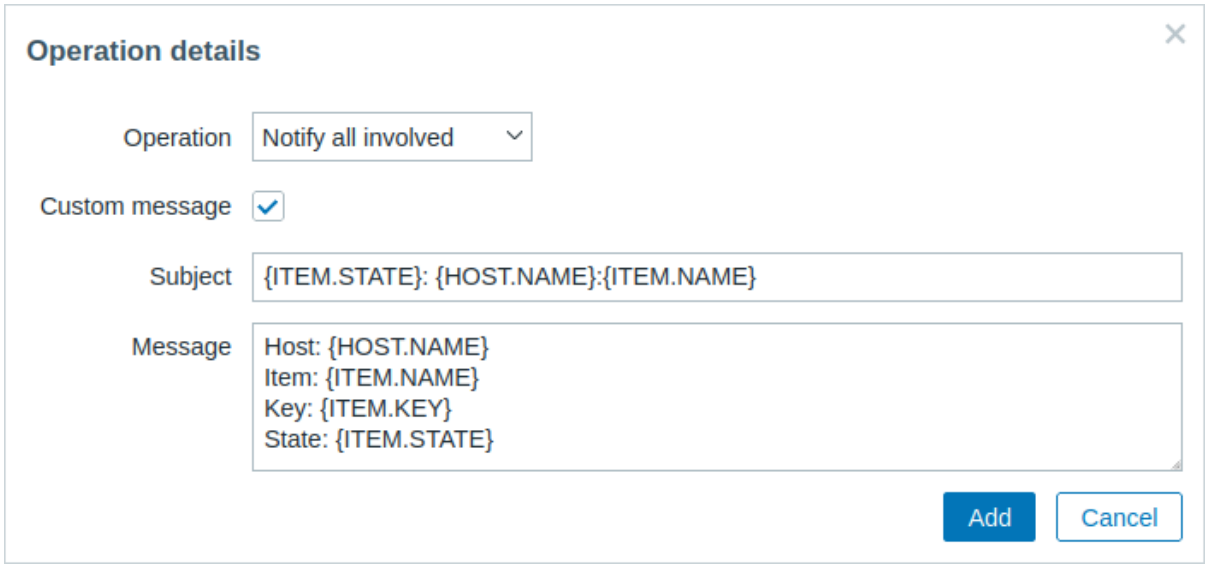
Jeśli chcesz otrzymać więcej niż jedno powiadomienie, ustaw czas trwania kroku operacji (odstęp między wysyłanymi wiadomościami) i dodaj kolejny krok.

Krok 5

Blok *Operacje odzyskiwania* umożliwia skonfigurowanie powiadomienia o odzyskaniu, gdy pozycja wróci do normalnego stanu. Kliknij *Dodaj* w bloku *Operacje odzyskiwania*, aby dodać nową operację odzyskiwania.



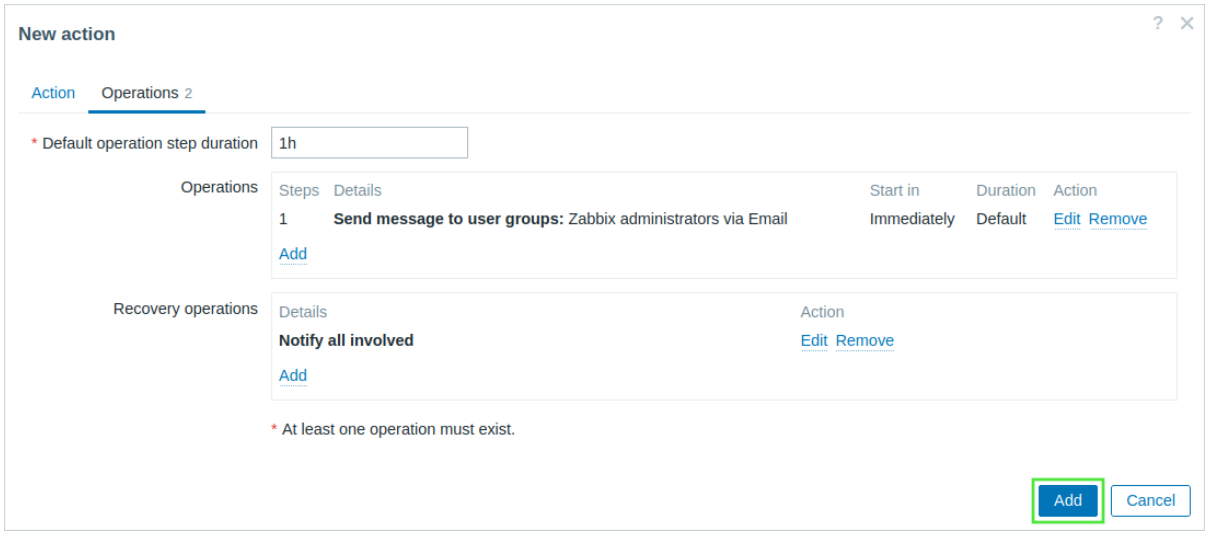
Wybierz typ operacji „Powiadom wszystkich zaangażowanych". Zaznacz pole wyboru *Własna wiadomość*, jeśli chcesz wprowadzić niestandardowy temat/treść wiadomości odzyskiwania.



Kliknij *Dodaj* w wyskakującym oknie *Szczegóły operacji*, aby faktycznie dodać operację do listy w bloku *Operacje odzyskiwania*.

Krok 6

Po zakończeniu kliknij przycisk *Dodaj* u dołu formularza.



I to wszystko, gotowe! Teraz możesz oczekiwać pierwszego powiadomienia z Zabbix, jeśli jakaś pozycja stanie się nieobsługiwana.

11 Makra

Przegląd

Zabbix obsługuje szereg wbudowanych makr, które mogą być używane w różnych sytuacjach. Makra te są zmiennymi identyfikowanymi przez określoną składnię:

`{MACRO}`

Makra są rozwijane do określonej wartości w zależności od kontekstu.

Efektywne użycie makr pozwala zaoszczędzić czas i uczynić konfigurację Zabbix bardziej przejrzystą.

W jednym z typowych zastosowań makro może być użyte w szablonie. W ten sposób wyzwalacz w szablonie może mieć nazwę „Obciążenie procesora jest zbyt wysokie na {HOST.NAME}". Gdy szablon zostanie zastosowany do hosta, na przykład Zabbix server, nazwa zostanie rozwinięta do „Obciążenie procesora jest zbyt wysokie na Zabbix server", gdy wyzwalacz będzie wyświetlany w sekcji Monitorowanie.

Makra mogą być używane w parametrach klucza pozycji. Makro może być użyte tylko dla części parametru, na przykład `item.key[server_{HOST.HOST}_local]`. Ujęcie parametru w podwójny cudzysłów nie jest konieczne, ponieważ Zabbix zadba o wszelkie niejednoznaczne znaki specjalne, jeśli wystąpią w rozwiniętym makrze.

W Zabbix istnieją także inne typy makr.

Zabbix obsługuje następujące makra:

- `{MACRO}` - wbudowane makro (zobacz pełną listę)
- `{<macro>.<func>(<params>)}` - funkcje makr
- `{$MACRO}` - makro zdefiniowane przez użytkownika, opcjonalnie z kontekstem
- `{#MACRO}` - makro dla odkrywania niskiego poziomu
- `{?EXPRESSION}` - makro wyrażenia

1 Funkcje makr

Przegląd

Funkcje makr umożliwiają dostosowanie wartości makr (na przykład skrócenie ich lub wyodrębnienie określonych podciągów), dzięki czemu łatwiej się z nimi pracuje.

Składnia funkcji makra jest następująca:

```
{macro.func(params)}
```

gdzie

- **macro** - makro do dostosowania;
- **func** - funkcja do zastosowania (zobacz obsługiwane funkcje);
- **params** - lista parametrów funkcji rozdzielonych przecinkami, które muszą być ujęte w **podwójne cudzysłowy**, jeśli:
  - zaczynają się od spacji lub podwójnego cudzysłowu;
  - zawierają zamykający nawias lub przecinek.

Na przykład:

```
{{TIME}.fmttime(format,time_shift)}
{{ITEM.VALUE}.regsub(pattern, output)}
{{$USERMACRO}.regsub(pattern, output)}
{{#LLDMACRO}.regsub(pattern, output)}
```

Funkcje makr są obsługiwane dla

- Makr wbudowanych
- Makr użytkownika
- Makr wykrywania niskiego poziomu
- Makr wyrażeń

Funkcje makr mogą być używane we wszystkich miejscach obsługujących wymienione makra. Dotyczy to wszystkich przypadków, chyba że wyraźnie zaznaczono, że oczekiwane jest tylko makro (na przykład podczas konfigurowania makr hosta lub filtrów reguły wykrywania niskiego poziomu).

Obsługiwana jest pojedyncza funkcja na makro; wiele funkcji makr połączonych w łańcuch nie jest obsługiwanych.

Note:
Zobacz przykłady znaków ucieczki dla przypadków, gdy funkcje makr są używane w innych kontekstach (funkcja, klucz pozycji, inne makro itd.).

Obsługiwane funkcje

Funkcje są wymienione bez dodatkowych informacji. Kliknij funkcję, aby zobaczyć pełne szczegóły.

Function	Description
btoa	Kodowanie wartości makra do formatu Base64.
fmtnum	Formatowanie liczby w celu kontrolowania liczby cyfr wyświetlanych po przecinku.
fmttime	Formatowanie czasu.
htmldecode	Dekodowanie wartości makra z kodowania HTML.
htmlencode	Kodowanie wartości makra do kodowania HTML.
iregsub	Wyodrębnianie podciągu na podstawie dopasowania wyrażenia regularnego (bez rozróżniania wielkości liter).
lowercase	Przekształcanie znaków wartości makra na małe litery.
regrepl	Zastępowanie znaku/podciągu w wartości makra.
regsub	Wyodrębnianie podciągu na podstawie dopasowania wyrażenia regularnego (z rozróżnianiem wielkości liter).
tr	Transliteracja znaków wartości makra.
uppercase	Przekształcanie znaków wartości makra na wielkie litery.
urldecode	Dekodowanie wartości makra z kodowania URL.
urlencode	Kodowanie wartości makra do kodowania URL.

Szczegóły funkcji

Opcjonalne parametry funkcji są oznaczone przez < >.

btoa

Kodowanie wartości makra do kodowania Base64. Kodowanie Base64 to metoda przedstawiania danych binarnych jako tekstu, przydatna do przechowywania i bezpiecznego przesyłania zawartości binarnej za pośrednictwem protokołów tekstowych.

Przykład:

```
{{ITEM.VALUE}.btoa()} - zakoduje wartość taką jak "zabbix" do postaci Base64 "emFiYml4"
```

fmtnum(digits)

Formatowanie liczb umożliwiające kontrolę liczby cyfr wyświetlanych po przecinku.

Parametry:

- **digits** — liczba cyfr po przecinku. Prawidłowy zakres: 0-20. Końcowe zera nie będą dodawane.

Przykłady:

```
{{ITEM.VALUE}.fmtnum(2)} - zwróci "24.35" dla otrzymanej wartości "24.3483523"
{{ITEM.VALUE}.fmtnum(0)} - zwróci "24" dla otrzymanej wartości "24.3483523"
```

fmttime(format,<time_shift>)

Formatowanie czasu.
Należy pamiętać, że tej funkcji można używać z makrami, które są rozwijane do wartości w jednym z następujących formatów czasu:

- `hh:mm:ss`
- `yyyy-mm-ddThh:mm:ss[tz]` (standard ISO8601)
- znacznik czasu UNIX

Parametry:

- **format** - obowiązkowy ciąg formatu, zgodny z formatowaniem funkcji `strftime`;
- **time_shift** (opcjonalnie) - przesunięcie czasu stosowane do czasu przed formatowaniem; powinno zaczynać się od `-<N><time_unit>` lub `+<N><time_unit>`, gdzie:
  - `N` - liczba jednostek czasu do dodania lub odjęcia;
  - `time_unit` - h (godzina), d (dzień), w (tydzień), M (miesiąc) lub y (rok).

Uwagi:

- Parametr `time_shift` obsługuje wieloetapowe operacje na czasie i może zawierać `/<time_unit>` do przesunięcia na początek jednostki czasu (`/d` - północ, `/w` - 1. dzień tygodnia (poniedziałek), `/M` - 1. dzień miesiąca itd.). Przykłady: `-1w` - dokładnie 7 dni wstecz; `-1w/w` - poniedziałek poprzedniego tygodnia; `-1w/w+1d` - wtorek poprzedniego tygodnia.
- Operacje na czasie są obliczane od lewej do prawej bez priorytetów. Na przykład `-1M/d+1h/w` zostanie zinterpretowane jako `((-1M/d)+1h)/w`.

Przykłady:

```
{{TIME}.fmttime(%B)} - zwróci "October" dla otrzymanej wartości "1633098961"
{{TIME}.fmttime(%d %B,-1M/M)} - zwróci "1 September" dla otrzymanej wartości "1633098961"
```

htmldecode

Dekodowanie wartości makra z kodowania HTML.

Obsługiwane są następujące znaki:

Wartość	Zdekodowana wartość
&	&
<	<
>	>
"	"
'	'
'	'

Przykład:

```
{{ITEM.VALUE}.htmldecode()} - zdekoduje HTML wartość taką jak "&lt;" do "<"
```

htmlencode

Kodowanie wartości makra do kodowania HTML.

Obsługiwane są następujące znaki:

Wartość	Zakodowana wartość
&	&
<	<
>	>
"	"
'	'

Przykład:

```
{{ITEM.VALUE}.htmlencode()} - zakoduje znak HTML, taki jak "<", do postaci "&lt;"
```

iregsub(pattern,output)

Wyodrębnianie podciągu na podstawie dopasowania wyrażenia regularnego (bez rozróżniania wielkości liter).

Parametry:

- **pattern** - wyrażenie regularne do dopasowania;
- **output** - opcje wyjściowe. Symbole zastępcze **\1 - \9** są obsługiwane dla grup przechwytywania. **\0** zwraca dopasowany tekst.

Uwagi:

- Jeśli nie ma dopasowania dla wyrażenia regularnego, funkcja zwraca pusty ciąg.
- Jeśli wzorzec funkcji jest niepoprawnym wyrażeniem regularnym, makro jest obliczane jako 'UNKNOWN' (z wyjątkiem makr wykrywania niskiego poziomu, w których przypadku funkcja zostanie zignorowana, a makro pozostanie nierozwiązane).
- Odwołania do nieistniejących grup przechwytywania w ciągu zastępczym są zastępowane pustym ciągiem.

Przykład:

```
{{ITEM.VALUE}.iregsub("fail|error|fault|problem","ERROR")} - zostanie rozwinięte do "ERROR", jeśli zostaną
```

małe litery

Przekształcenie wszystkich znaków wartości makra na małe litery.
Działa z jednobajtowymi zestawami znaków (takimi jak ASCII) i nie obsługuje UTF-8.

Przykład:

```
{{ITEM.VALUE}.lowercase()} - przekształci wartość taką jak "Zabbix SERVER" na "zabbix server" (małe litery
```

regrepl(pattern,replacement,<pattern2>,<replacement2>,...)

Zastępowanie znaku/podciągu w wartości makra.

Parametry:

- **pattern** - wyrażenie regularne do dopasowania;
- **replacement** - ciąg zastępujący. Symbole zastępcze **\1 - \9** są obsługiwane w ciągach zastępujących dla grup przechwytywania.

Uwagi:

- Wzorce i ciągi zastępujące są przetwarzane sekwencyjnie, przy czym każda kolejna para jest stosowana zgodnie z wynikiem poprzedniego zastąpienia;
- Odwołania do nieistniejących grup przechwytywania w ciągu zastępującym są zastępowane pustym ciągiem.

Przykłady:

```
{{ITEM.VALUE}.regrepl("oldParam", "newParam")} - zastąpi "oldParam" przez "newParam"
{{ITEM.VALUE}.regrepl("([^a-z])","\\\1")} - wszystkie znaki niebędące literami zostaną poprzedzone ukośnik
{$THRESHOLD:"{{#FSNAME}.regrepl(\"\\$\",\"\")}"} - usunie końcowy ukośnik odwrotny (na przykład, aby zastą
{{ITEM.VALUE}.regrepl("_v1\.0", "_v2.0", "\(final\)", "")} - zastąpi wiele fragmentów w wartości pozycji
```

regsub(pattern,output)

Wyodrębnianie podciągu na podstawie dopasowania wyrażenia regularnego (z uwzględnieniem wielkości liter).

Parametry:

- **pattern** - wyrażenie regularne do dopasowania;
- **output** - opcje danych wyjściowych. Symbole zastępcze **\1 - \9** są obsługiwane dla grup przechwytywania. **\0** zwraca dopasowany tekst.

Uwagi:

- Jeśli nie ma dopasowania do wyrażenia regularnego, funkcja zwraca pusty ciąg.
- Jeśli wzorzec funkcji jest niepoprawnym wyrażeniem regularnym, makro przyjmuje wartość 'UNKNOWN' (z wyjątkiem makr wykrywania niskiego poziomu, w których przypadku funkcja zostanie zignorowana, a makro pozostanie nierozwiązane).
- Odwołania do nieistniejących grup przechwytywania w ciągu zastępczym są zastępowane pustym ciągiem.

Przykłady:

```
{{ITEM.VALUE}.regsub("^([0-9]+)", Problem ID: \1)} - zostanie rozwinięte do "Problem ID: 123", jeśli zosta
{{ITEM.VALUE}.regsub("fail|error|fault|problem","ERROR")} - zostanie rozwinięte do "ERROR", jeśli zostaną
```

Zobacz więcej przykładów.

tr(characters,replacement)

Transliteracja znaków wartości makra.

- **characters** - zestaw znaków do zastąpienia;
- **replacement** - zestaw odpowiadających im pozycyjnie znaków zastępczych.

Przykłady:

```
{{ITEM.VALUE}.tr(abc, xyz)} - zastąpi wszystkie wystąpienia "a" przez "x", "b" przez "y", "c" przez "z"
{{ITEM.VALUE}.tr(abc, xyzq)} - zastąpi wszystkie wystąpienia "a" przez "x", "b" przez "y", "c" przez "z" (
{{ITEM.VALUE}.tr(abcde, xyz)} - zastąpi wszystkie wystąpienia "a" przez "x", "b" przez "y", "c" przez "z",
{{ITEM.VALUE}.tr("\\\'", "\/\"")} - zastąpi wszystkie wystąpienia ukośnika odwrotnego ukośnikiem prostym,
{{ITEM.VALUE}.tr(A-Z,a-z)} - przekonwertuje wszystkie litery na małe
{{ITEM.VALUE}.tr(0-9a-z,*)} - zastąpi wszystkie cyfry i małe litery znakiem "*"
{{ITEM.VALUE}.tr(0-9,ab)} - zastąpi wszystkie wystąpienia 0 przez "a", a wszystkie wystąpienia 1, 2, 3, 4,
{{ITEM.VALUE}.tr(0-9abcA-L,*)} - zastąpi wszystkie cyfry, znaki "abc" oraz zakres A-L znakiem "*"
{{ITEM.VALUE}.tr("\n","*")} - zastąpi wystąpienia końca linii znakiem *
{{ITEM.VALUE}.tr("e", "\n")} - zastąpi wszystkie "e" znakiem końca linii
```

Aby uwzględnić znaki literałowe:

```
ukośnik odwrotny - musi być zapisany jako \\
pojedynczy cudzysłów - musi być zapisany jako \'
podwójny cudzysłów - musi być zapisany jako \"
```

Obsługiwane sekwencje ucieczki z ukośnikiem odwrotnym:

```
\\\\ => \\ - podwójny ukośnik odwrotny na pojedynczy ukośnik odwrotny
\\a  => \a - alert
\\b  => \b - backspace
\\f  => \f - wysunięcie strony
\\n  => \n - nowa linia
\\r  => \r - powrót karetki
\\t  => \t - tabulator poziomy
\\v  => \v - tabulator pionowy
```

wielkie litery

Przekształcenie wszystkich znaków wartości makra na wielkie litery. Działa z jednobajtowymi zestawami znaków (takimi jak ASCII) i nie obsługuje UTF-8.

Przykład:

```
{{ITEM.VALUE}.uppercase()} - przekształci wartość taką jak "Zabbix Server" na "ZABBIX SERVER" (wielkie lit
```

urldecode

Dekodowanie wartości makra z kodowania URL.

Przykład:

```
{{ITEM.VALUE}.urldecode()} - zdekoduje URL wartość taką jak "%2F" do "/"
```

urlencode

Kodowanie wartości makra do formatu URL encoding.

Przykład:

```
{{ITEM.VALUE}.urlencode()} - zakoduje znak taki jak "/" do postaci "%2F"
```

Dodatkowe przykłady

Poniższa tabela pokazuje więcej przykładów użycia funkcji makr.

{#IFALIAS} jest makrem LLD i jest zdefiniowane tylko w kontekstach low-level discovery (reguły wykrywania, prototypy oraz pozycje/wyzwalacze utworzone na ich podstawie). Użycie go poza LLD spowoduje pozostawienie tokenu bez rozwinięcia.

Funkcja makra	Otrzymana wartość	Wynik
{{ITEM.VALUE}.regsub(^[0-9]+, Problem)}	123Log line	Problem
{{ITEM.VALUE}.regsub("^([0-9]+)", "Problem")}	123 Log line	Problem
{{ITEM.VALUE}.regsub(".*", "Problem ID: \1")}	Log line	Problem ID:
{{ITEM.VALUE}.regsub("^(\w+).*?([0-9]+)", " Problem ID: \1_\2 ")}	MySQL crashed errno 123	Problem ID: MySQL_123
{{ITEM.VALUE}.regsub("([1-9]+", "Problem ID: \1")}	123 Log line	*UNKNOWN* (nieprawidłowe wyrażenie regularne)
{{#IFALIAS}.regsub("(.*)_([0-9]+)", \1)}	customername_1	customername
{{#IFALIAS}.regsub("(.*)_([0-9]+)", \2)}	customername_11	
{{#IFALIAS}.regsub("(.*)_([0-9]+", \1)}	customername_1	{{#IFALIAS}.regsub("(.*)_([0-9]+", \1)} (nieprawidłowe wyrażenie regularne)
{$MACRO:"{{#IFALIAS}.regsub(\"(.*)_([0-9]+)\", \1)}"}	customername_1	{$MACRO:"customername"}

Funkcja makra	Otrzymana wartość	Wynik
{$MACRO:"{{#IFALIAS}.regsub(\"(.*)_([0-9]+)\", \2)}"}	customername_1	{$MACRO:"1"}
{$MACRO:"{{#IFALIAS}.regsub(\"(.*)_([0-9]+\", \1)}"}	customername_1	{$MACRO:"{{#IFALIAS}.regsub(\"(.*)_([0-9]+\", \1)}"} (nieprawidłowe wyrażenie regularne)
"{$MACRO:"\{{#IFALIAS}.regsub("(.*)_([0-9]+)", \1)}\"}"	customername_1	"{$MACRO:"\customername\"}"
"{$MACRO:"\{{#IFALIAS}.regsub("(.*)_([0-9]+)", \2)}\"}"	customername_1	"{$MACRO:"\1\"}"
"{$MACRO:\"{{#IFALIAS}.regsub(\\"(.*)_([0-9]+\\", \1)}\"}"	customername_1	"{$MACRO:\"{{#IFALIAS}.regsub(\\"(.*)_([0-9]+\\", \1)}\"}" (nieprawidłowe wyrażenie regularne)

Wyświetlanie pełnych wartości pozycji

Długie wartości rozwiniętych makr {ITEM.VALUE} i {ITEM.LASTVALUE} dla pozycji tekstowych/logów są w niektórych miejscach frontend skracane do 20 znaków. Aby zobaczyć pełne wartości tych makr, można użyć funkcji makr, np.:

```
{{ITEM.VALUE}.regsub("(.*)", \1)}
{{ITEM.LASTVALUE}.regsub("(.*)", \1)}
```

Zobacz także: szczegóły makr {ITEM.VALUE} i {ITEM.LASTVALUE}.

2 Makra użytkownika

Przegląd

Makra użytkownika są obsługiwane w Zabbix w celu zapewnienia większej elastyczności, oprócz makr obsługiwanych domyślnie.

Makra użytkownika można definiować na poziomie globalnym, szablonu i hosta. Makra te mają specjalną składnię:

{$MACRO}

Zabbix rozwiązuje makra zgodnie z następującym priorytetem:

1. makra na poziomie hosta (sprawdzane jako pierwsze)
2. makra zdefiniowane dla szablonów pierwszego poziomu hosta (tj. szablonów połączonych bezpośrednio z hostem), posortowane według ID szablonu
3. makra zdefiniowane dla szablonów drugiego poziomu hosta, posortowane według ID szablonu
4. makra zdefiniowane dla szablonów trzeciego poziomu hosta, posortowane według ID szablonu itd.
5. makra globalne (sprawdzane jako ostatnie)

Innymi słowy, jeśli makro nie istnieje dla hosta, Zabbix spróbuje znaleźć je w szablonach hosta o rosnącej głębokości. Jeśli nadal nie zostanie znalezione, zostanie użyte makro globalne, jeśli istnieje.

Warning:
Jeśli makro o **tej samej nazwie** istnieje w wielu podłączonych szablonach na tym samym poziomie, zostanie użyte makro z szablonu o najniższym ID. Oznacza to, że posiadanie makr o tej samej nazwie w wielu szablonach stanowi ryzyko konfiguracyjne.

Jeśli Zabbix nie będzie w stanie znaleźć makra, makro nie zostanie rozwiązane.

Attention:
Makra (w tym makra użytkownika) celowo pozostają nierozwiązane w sekcji Konfiguracja (na przykład na liście wyzwalaczy), aby zwiększyć przejrzystość złożonej konfiguracji.

Makra użytkownika mogą być używane w:

- nazwie pozycji
- parametrze klucza pozycji
- interwałach aktualizacji pozycji i interwałach elastycznych
- nazwie i opisie wyzwalacza
- parametrach wyrażenia wyzwalacza i stałych (zobacz przykłady)
- wielu innych miejscach — zobacz pełną listę

Typowe przypadki użycia makr globalnych i makr hosta

- użycie makra globalnego w kilku miejscach; następnie zmiana wartości makra i zastosowanie zmian konfiguracji we wszystkich miejscach jednym kliknięciem
- wykorzystanie szablonów z atrybutami specyficznymi dla hosta: hasła, numery portów, nazwy plików, wyrażenia regularne itp.

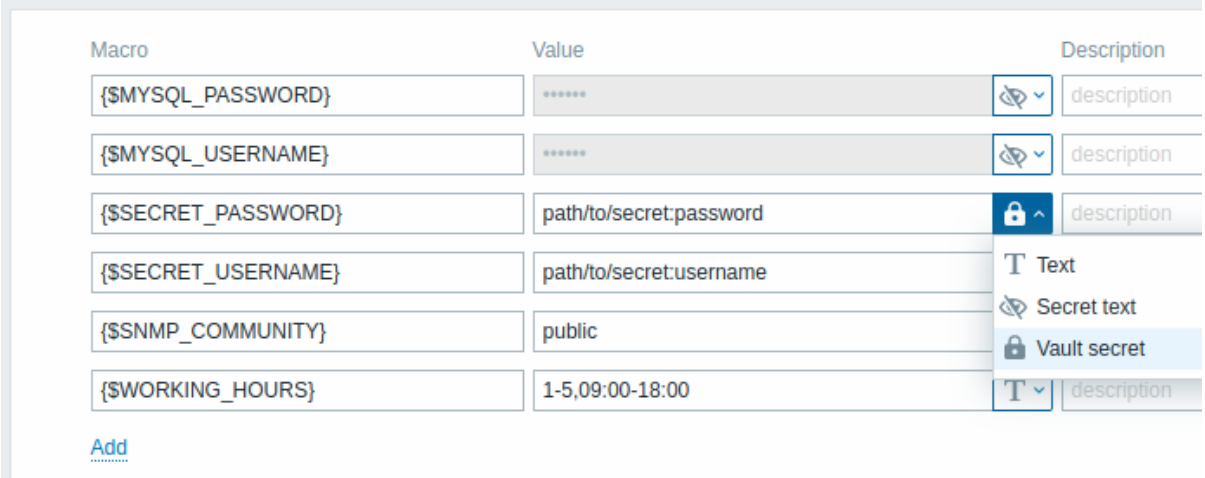
Note:
Zaleca się używanie makr hosta zamiast makr globalnych, ponieważ dodawanie, aktualizowanie lub usuwanie makr globalnych wymusza przyrostową aktualizację konfiguracji dla wszystkich hostów. Więcej informacji można znaleźć w sekcji Passive and active agent checks.

Konfiguracja

Aby zdefiniować makra użytkownika, przejdź do odpowiedniego miejsca we frontend:

- dla makr globalnych przejdź do *Administracja* → *Makra*
- dla makr na poziomie hosta i szablonu otwórz właściwości hosta lub szablonu i znajdź kartę *Makra*

Makro użytkownika ma następujące atrybuty:



Parametr	Opis
Macro	Nazwa makra. Nazwa musi być ujęta w nawiasy klamrowe i zaczynać się od znaku dolara. Przykład: {$FRONTEND_URL}. W nazwach makr dozwolone są następujące znaki: **A-Z** (tylko wielkie litery), **0-9**, _, **.**
Value	Wartość makra. Obsługiwane są trzy typy wartości: **Text** (domyślnie) — wartość w postaci zwykłego tekstu **Secret text** — wartość jest maskowana gwiazdkami **Vault secret** — wartość zawiera ścieżkę/zapytanie do vault secret. Aby zmienić typ wartości, kliknij przycisk na końcu pola wprowadzania wartości. Maksymalna długość wartości makra użytkownika wynosi 2048 znaków.
Description	Pole tekstowe używane do podania dodatkowych informacji o tym makrze.

Podczas konfigurowania makr użytkownika **zwróć uwagę** na następujące zachowania zależne od kontekstu:

- jeśli makra użytkownika są używane w pozycjach lub wyzwalaczach szablonu, rozważ dodanie tych makr również do szablonu (nawet jeśli są zdefiniowane globalnie); dzięki temu makra typu *Text* będą działać zgodnie z oczekiwaniami po wyeksportowaniu szablonu do XML i zaimportowaniu go do innego systemu (wartości tajnych makr nie są eksportowane)
- jeśli makra użytkownika są używane w wyrażeniach wyzwalaczy, te makra zostaną rozwinięte tylko wtedy, gdy odwołują się do parametru lub stałej; NIE zostaną rozwinięte, jeśli odwołują się do hosta, klucza pozycji, funkcji, operatora lub innego wyrażenia wyzwalacza (tajne makra nie mogą być używane w wyrażeniach wyzwalaczy)
- jeśli makra użytkownika są używane na hoście, który ma regułę wykrywania niskiego poziomu z prototypami hostów, wykryte hosty odziedziczą wszystkie makra użytkownika zdefiniowane na tym hoście

Przykłady

Przykład 1

Użycie makra na poziomie hosta w kluczu pozycji „Status demona SSH”:

```
net.tcp.service[ssh,,{$SSH_PORT}]
```

Ta pozycja może zostać przypisana do wielu hostów, pod warunkiem że wartość **{$SSH_PORT}** jest zdefiniowana na tych hostach.

Przykład 2

Użycie makra na poziomie hosta w wyzwalaczu „Obciążenie CPU jest zbyt wysokie”:

```
last(/ca_001/system.cpu.load[,avg1])>{$MAX_CPULOAD}
```

Taki wyzwalacz zostałby utworzony w szablonie, a nie edytowany na poszczególnych hostach.

Note:
Jeśli chcesz użyć liczby wartości jako parametru funkcji (na przykład **max(/host/key,#3)**), uwzględnij znak hash w definicji makra w ten sposób: SOME_PERIOD => #3

Przykład 3

Użycie dwóch makr w wyzwalaczu „Obciążenie CPU jest zbyt wysokie”:

```
min(/ca_001/system.cpu.load[,avg1],{$CPULOAD_PERIOD})>{$MAX_CPULOAD}
```

Zwróć uwagę, że makro może być użyte jako parametr funkcji wyzwalacza, w tym przykładzie funkcji **min()**.

Przykład 4

Zsynchronizuj warunek niedostępności agenta z interwałem aktualizacji pozycji:

- zdefiniuj makro {$INTERVAL} i użyj go w interwale aktualizacji pozycji;
- użyj {$INTERVAL} jako parametru wyzwalacza niedostępności agenta:

```
nodata(/ca_001/agent.ping,{$INTERVAL})=1
```

Przykład 5

Scentralizuj konfigurację godzin pracy:

- utwórz globalne makro {$WORKING_HOURS} o wartości 1-5,09:00-18:00;
- użyj go w polu *Working time* w *Administration → General → GUI*;
- użyj go w polu *When active* w *Users → Users*, karta *Media* użytkownika;
- użyj go do skonfigurowania częstszego odpytywania pozycji w godzinach pracy:

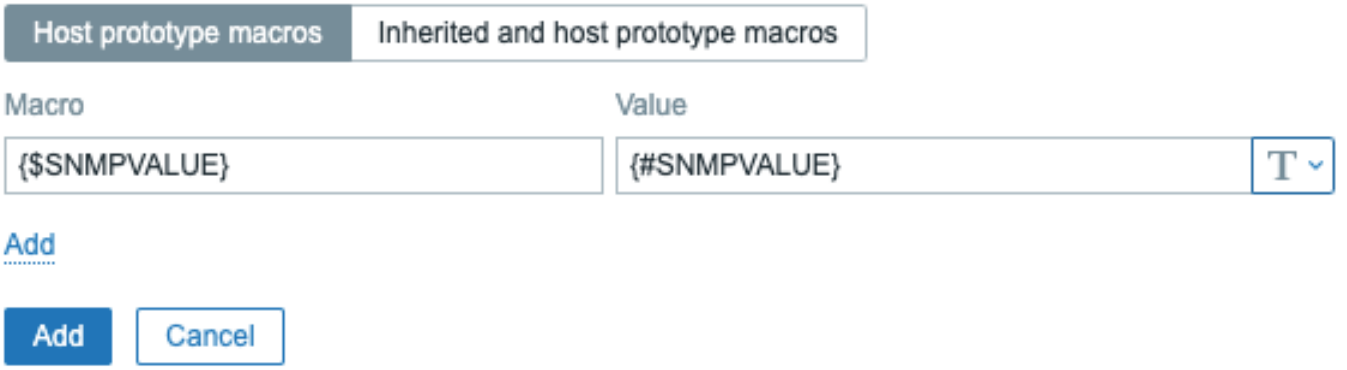


- użyj go w warunku akcji *Time period*;
- w razie potrzeby dostosuj godziny pracy w *Administration → Macros*.

Przykład 6

Użyj makra prototypu hosta do skonfigurowania pozycji dla wykrytych hostów:

- w prototypie hosta zdefiniuj makro użytkownika {$SNMPVALUE} z makrem low-level discovery {#SNMPVALUE} jako wartością:



- przypisz szablon *Generic SNMPv2* do prototypu hosta;
- użyj {$SNMPVALUE} w polu *SNMP OID* pozycji szablonu *Generic SNMPv2*.

Kontekst makra użytkownika

Zobacz makra użytkownika z kontekstem.

3 Makra użytkownika z kontekstem

Przegląd

Opcjonalny kontekst może być używany w makrach użytkownika, co pozwala zastąpić wartość domyślną wartością specyficzną dla danego kontekstu.

Kontekst jest dołączany do nazwy makra; składnia zależy od tego, czy kontekst jest statyczną wartością tekstową:

```
{$MACRO:"tekst statyczny"}
```

czy wyrażeniem regularnym:

```
{$MACRO:regex:"wyrażenie regularne"}
```

Należy pamiętać, że makro z kontekstem wyrażenia regularnego może być zdefiniowane wyłącznie w konfiguracji makr użytkownika. Jeśli prefiks `regex:` zostanie użyty w innym miejscu jako kontekst makra użytkownika, na przykład w wyrażeniu wyzwalacza, zostanie potraktowany jako kontekst statyczny.

Ujmowanie kontekstu w cudzysłów jest opcjonalne (zobacz także ważne uwagi).

Przykłady kontekstu makra:

Przykład	Opis
{$LOW_SPACE_LIMIT}	Makro użytkownika bez kontekstu.
{$LOW_SPACE_LIMIT:/tmp}	Makro użytkownika z kontekstem (ciąg statyczny).
{$LOW_SPACE_LIMIT:regex:"^/tmp$"}	Makro użytkownika z kontekstem (wyrażenie regularne). To samo co {$LOW_SPACE_LIMIT:/tmp}.
{$LOW_SPACE_LIMIT:regex:"^/var/log/.*$"}	Makro użytkownika z kontekstem (wyrażenie regularne). Dopasowuje wszystkie ciągi poprzedzone prefiksem /var/log/.

Przykłady użycia

Makra użytkownika z kontekstem można definiować w celu uzyskania bardziej elastycznych progów w wyrażeniach wyzwalaczy (na podstawie wartości pobranych przez wykrywanie niskiego poziomu). Na przykład można zdefiniować następujące makra:

- {$LOW_SPACE_LIMIT} = 10
- {$LOW_SPACE_LIMIT:/home} = 20
- {$LOW_SPACE_LIMIT:regex:”^/[a-z]+$”} = 30

Następnie makro wykrywania niskiego poziomu może zostać użyte jako kontekst makra w prototypie wyzwalacza dla wykrywania zamontowanych systemów plików:

```
last(/host/vfs.fs.size[{#FSNAME},pfree])<{$LOW_SPACE_LIMIT:"{#FSNAME}"}
```

Po wykryciu w wyzwalaczach będą stosowane różne progi niskiej ilości wolnego miejsca w zależności od wykrytych punktów montowania lub typów systemów plików. Zdarzenia problemów będą generowane, jeśli:

- katalog /home ma mniej niż 20% wolnego miejsca na dysku
- katalogi pasujące do wzorca regexp (takie jak /etc, /tmp lub /var) mają mniej niż 30% wolnego miejsca na dysku
- katalogi, które nie pasują do wzorca regexp i nie są /home, mają mniej niż 10% wolnego miejsca na dysku

Ważne uwagi

- Jeśli istnieje więcej niż jedna makrodefinicja użytkownika z kontekstem, Zabbix najpierw spróbuje dopasować makra z prostym kontekstem, a następnie makra kontekstowe z wyrażeniami regularnymi w niezdefiniowanej kolejności.

Warning:
Nie twórz różnych makr kontekstowych pasujących do tego samego ciągu, aby uniknąć niezdefiniowanego zachowania.

- Jeśli makro wraz z jego kontekstem nie zostanie znalezione na hoście, w podłączonych szablonach ani globalnie, wyszukiwane jest makro bez kontekstu.

- W kontekście obsługiwane są tylko makra wykrywania niskiego poziomu. Wszelkie inne makra są ignorowane i traktowane jako zwykły tekst.

Technicznie rzecz biorąc, kontekst makra jest określany przy użyciu reguł podobnych do parametrów klucza pozycji, z wyjątkiem tego, że kontekst makra nie jest analizowany jako kilka parametrów, jeśli zawiera znak ,:

- Kontekst makra musi być ujęty w " , jeśli kontekst zawiera znak } lub zaczyna się od znaku ". Cudzysłowy wewnątrz ujętego w cudzysłów kontekstu muszą być poprzedzone znakiem ucieczki \.
- Sam znak \ nie jest znakowany znakiem ucieczki, co oznacza, że niemożliwe jest użycie ujętego w cudzysłów kontekstu kończącego się znakiem \ — makro {$MACRO:"a:\b\c\"} jest nieprawidłowe.
- Początkowe spacje w kontekście są ignorowane, końcowe nie:
  - Na przykład {$MACRO:A} jest takie samo jak {$MACRO: A}, ale nie jak {$MACRO:A }.
- Wszystkie spacje przed początkowym cudzysłowem i po końcowym cudzysłowie są ignorowane, ale wszystkie spacje wewnątrz cudzysłowów nie:
  - Makra {$MACRO:"A"}, {$MACRO: "A"}, {$MACRO:"A" } oraz {$MACRO: "A" } są takie same, ale makra {$MACRO:"A"} i {$MACRO:" A "} nie są.

Wszystkie poniższe makra są równoważne, ponieważ mają ten sam kontekst: {$MACRO:A}, {$MACRO: A} oraz {$MACRO:"A"}. Stanowi to kontrast wobec kluczy pozycji, gdzie 'key[a]', 'key[a]' oraz 'key["a"]' są semantycznie takie same, ale różnią się pod względem unikalności.

4 Tajne makra użytkownika

Przegląd

Zabbix udostępnia dwie opcje ochrony poufnych informacji w wartościach makr użytkownika:

- Tajny tekst
- Sekret z vault

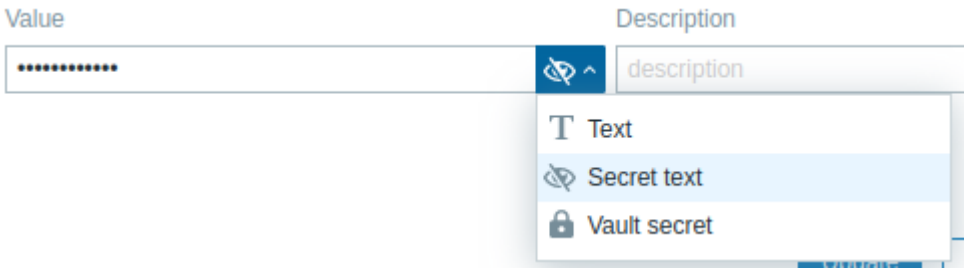
Note:
Chociaż wartość tajnego makra jest ukryta, może zostać ujawniona poprzez użycie w pozycjach. Na przykład w skrypcie zewnętrznym instrukcja echo odwołująca się do tajnego makra może zostać użyta do ujawnienia wartości makra we front-tend, ponieważ serwer Zabbix ma dostęp do rzeczywistej wartości makra. Zobacz lokalizacje, w których wartości tajnych makr są odsłaniane.

Tajnych makr nie można używać w wyrażeniach wyzwalaczy.

Tajny tekst

W przypadku makr typu Tajny tekst wartość makra jest maskowana gwiazdkami.

Aby ustawić wartość makra jako tajną, kliknij przycisk na końcu pola *Value* i wybierz opcję *Secret text*:



Po zapisaniu konfiguracji wyświetlenie wartości nie będzie już możliwe.

Aby zmienić wartość makra, najedź kursorem na pole *Value* i kliknij przycisk *Set new value* (pojawia się po najechaniu kursorem):



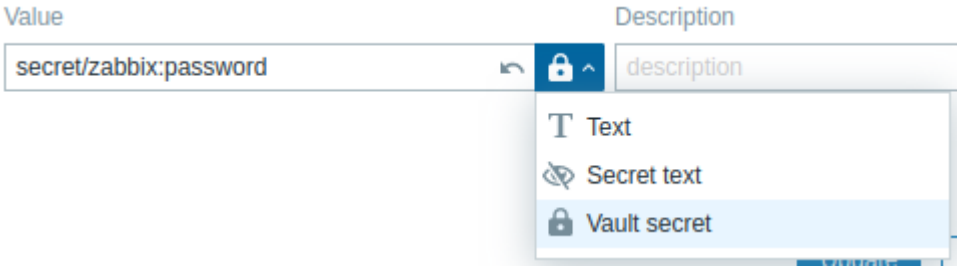
Po kliknięciu przycisku *Set new value* (lub zmianie typu wartości makra) bieżąca wartość zostanie usunięta. Możesz przywrócić oryginalną wartość, klikając strzałkę na końcu pola *Value* (dostępne tylko przed zapisaniem nowej konfiguracji). Pamiętaj, że przywrócenie oryginalnej wartości nie spowoduje jej ujawnienia.

Note:
Adresy URL zawierające tajne makro nie będą działać, ponieważ makro w nich zostanie rozwinięte jako "******".

Sekret Vault

W przypadku makr sekretów Vault wartość makra jest przechowywana w zewnętrznym oprogramowaniu do zarządzania sekretami (vault).

Aby skonfigurować makro sekretu Vault, kliknij przycisk na końcu pola *Value* i wybierz opcję *Vault secret*:



Wartość makra musi wskazywać na sekret w vault. Format wejściowy zależy od dostawcy vault. Przykłady konfiguracji dla poszczególnych dostawców znajdują się tutaj:

- HashiCorp
- CyberArk

Wartości makr sekretów Vault są pobierane z vault przez serwer Zabbix (oraz proxy Zabbix, jeśli *Resolve secret vault macros by* jest ustawione na *Zabbix server and proxy*) przy każdym odświeżeniu danych konfiguracyjnych, a następnie przechowywane w pamięci podręcznej konfiguracji. Serwer Zabbix i proxy Zabbix mogą używać różnych vaultów.

Jeśli *Resolve secret vault macros by* jest ustawione na *Zabbix server*, wówczas sekrety vault są pobierane tylko przez serwer, a proxy Zabbix otrzymuje wartości makr sekretów Vault z serwera Zabbix przy każdej synchronizacji konfiguracji i przechowuje je we własnej pamięci podręcznej konfiguracji. Oznacza to, że proxy Zabbix nie może rozpocząć zbierania danych po restarcie, dopóki nie otrzyma aktualizacji konfiguracji z serwera Zabbix.

Aby ręcznie odświeżyć wartości sekretów z vault, użyj opcji kontroli w czasie działania `secrets_reload` (tylko serwer).

Szyfrowanie musi być włączone między serwerem Zabbix a proxy; w przeciwnym razie rejestrowany jest komunikat ostrzegawczy serwera.

Warning:
Jeśli wartości makra nie można pomyślnie pobrać, odpowiednia pozycja korzystająca z tej wartości stanie się nieobsługiwana.

Niemaskowane lokalizacje

Ta lista przedstawia lokalizacje parametrów, w których wartości tajnych makr są niemaskowane.

Note:
Wartości tajnych makr pozostaną zamaskowane w poniższych lokalizacjach, jeśli są przywoływane pośrednio. Na przykład wbudowane makra {ITEM.KEY}, {ITEM.KEY<1-9>}, {LLDRULE.KEY} built-in macros używane w typach mediów (parametry Skryptu lub webhooka) zostaną rozwinięte do kluczy pozycji zawierających zamaskowane tajne makra, takich jak `net.tcp.port[******,******]` zamiast `net.tcp.port[192.0.2.0,80]`.

Kontekst		Parametr
Pozycje, prototypy pozycji, reguły LLD		
	Pozycja	*Parametry klucza pozycji*
	Prototyp pozycji	*Parametry klucza prototypu pozycji*
	Reguła wykrywania niskiego poziomu	*Parametry klucza pozycji wykrywania*
	agent SNMP	*Społeczność SNMP*
		Nazwa kontekstu (SNMPv3)
		Nazwa bezpieczeństwa (SNMPv3)
		Hasło uwierzytelniania (SNMPv3)
		Hasło prywatności (SNMPv3)
	agent HTTP	*URL*
		Pola zapytania
		Treść żądania
		Nagłówki
		Nazwa użytkownika
		Hasło

Kontekst		Parametr
		Hasło klucza SSL
	Skrypt	*Parametry*
		Skrypt
	Przeglądarka	*Parametry*
		Skrypt
	Monitor bazy danych	*Zapytanie SQL*
	agent TELNET	*Skrypt*
		Nazwa użytkownika
		Hasło
	agent SSH	*Skrypt*
		Nazwa użytkownika
		Hasło
	Proste sprawdzenie	*Nazwa użytkownika*
		Hasło
	agent JMX	*Nazwa użytkownika*
		Hasło
Wstępne przetwarzanie wartości pozycji		
	Krok wstępnego przetwarzania JavaScript	*Skrypt*
Scenariusze WWW		
	Scenariusz WWW	*Wartość zmiennej*
		Wartość nagłówka
		URL
		Wartość pola zapytania
		Wartość pola POST
		Surowe dane POST
	Uwierzytelnianie scenariusza WWW	*Użytkownik*
		Hasło
		Hasło klucza SSL
Konektory		
	Konektor	*URL*
		Nazwa użytkownika
		Hasło
		Token
		Proxy HTTP
		Plik certyfikatu SSL
		Plik klucza SSL
		Hasło klucza SSL
Wykrywanie sieci		
	SNMP	*Społeczność SNMP*
		Nazwa kontekstu (SNMPv3)
		Nazwa bezpieczeństwa (SNMPv3)
		Hasło uwierzytelniania (SNMPv3)
		Hasło prywatności (SNMPv3)
Skrypty globalne		
	Webhook	*Skrypt JavaScript*
		Wartość parametru skryptu JavaScript
	Telnet	*Nazwa użytkownika*
		Hasło
	SSH	*Nazwa użytkownika*
		Hasło
	Skrypt	*Skrypt*
Typy mediów		
	Skrypt	*Parametry skryptu*
	Webhook	*Parametry*
Zarządzanie IPMI		
	Host	*Nazwa użytkownika*
		Hasło

5 Makra wykrywania niskiego poziomu

Przegląd

Istnieje typ makra używanego w funkcji low-level discovery (LLD):

```
{#MACRO}
```

Jest to makro używane w regule LLD, które zwraca rzeczywiste wartości nazwy systemu plików, interfejsu sieciowego, SNMP OID itp.

Te makra mogą być używane do tworzenia prototypów encji (pozycja, wyzwalacz, wykres, reguła LLD, prototyp hosta i grupy hostów). Podczas wykrywania rzeczywistych systemów plików, interfejsów sieciowych, maszyn wirtualnych itp. makra te są zastępowane rzeczywistymi wartościami i stanowią podstawę do tworzenia rzeczywistych encji.

Niektóre makra low-level discovery są dostarczane „w pakiecie" z funkcją LLD w Zabbix — {#FSNAME}, {#FSTYPE}, {#IFNAME}, {#SNMPINDEX}, {#SNMPVALUE}. Jednak podczas tworzenia niestandardowej reguły low-level discovery nie ma obowiązku stosowania tych nazw. Możesz wtedy użyć dowolnej innej nazwy makra LLD i odwoływać się do tej nazwy.

Obsługiwane typy danych

Podczas definiowania niestandardowych reguł wykrywania wartości właściwości zwracane w obiektach JSON dla makr LLD muszą być jednym z następujących typów prostych:

- string
- number
- boolean

Tablice, obiekty i wartości null nie są obsługiwane. Każde makro LLD odwołujące się do takiej wartości pozostanie nierozwinięte i będzie wyświetlane dosłownie (np. `'{#MY_MACRO}'`) podczas wstępnego przetwarzania i tworzenia pozycji.

Obsługiwane lokalizacje

Makra LLD mogą być używane:

- w filtrze reguły wykrywania niskiego poziomu
- w zagnieżdżonych regułach wykrywania niskiego poziomu, w
  - parametrach przetwarzania wstępnego JSONPath
  - polu JSONPath dla niestandardowych makr LLD
- dla prototypów pozycji i prototypów wykrywania w
  - nazwie
  - parametrach klucza
  - jednostce
  - interwale aktualizacji[1]
  - limicie czasu[1]
  - okresie przechowywania historii[1]
  - okresie przechowywania trendów[1]
  - krokach przetwarzania wstępnego wartości pozycji
  - OID SNMP
  - polu sensora IPMI
  - wyrażeniu pozycji obliczanej/agregowanej, w:
    - stałych wyrażenia i parametrach funkcji
    - parametrach klucza pozycji
  - warunkach filtra pozycji agregowanej (nazwa grupy hostów i nazwa tagu)
  - skrypcie SSH i skrypcie Telnet
  - zapytaniu SQL monitorowania bazy danych
  - polu endpointu pozycji JMX
  - opisie
  - polu URL agenta HTTP
  - polu pól zapytania HTTP agenta HTTP
  - polu treści żądania agenta HTTP
  - polu wymaganych kodów statusu agenta HTTP
  - kluczu i wartości pola nagłówków agenta HTTP
  - polu nazwy użytkownika uwierzytelniania HTTP agenta HTTP
  - polu hasła uwierzytelniania HTTP agenta HTTP
  - polu proxy HTTP agenta HTTP
  - polu pliku certyfikatu SSL HTTP agenta HTTP
  - polu pliku klucza SSL HTTP agenta HTTP
  - polu hasła klucza SSL HTTP agenta HTTP
  - tagach
- dla prototypów wyzwalaczy w

    - nazwie
    - danych operacyjnych
    - wyrażeniu (tylko w stałych i parametrach funkcji)
    - URL
    - opisie
    - tagach
- dla prototypów wykresów w
    - nazwie
- dla prototypów hostów w
    - nazwie
    - widocznej nazwie
    - niestandardowych polach interfejsu: IP, DNS, port, społeczność SNMP v1/v2, nazwa kontekstu SNMP v3, nazwa zabezpieczeń SNMP v3, hasło uwierzytelniania SNMP v3, hasło prywatności SNMP v3
    - nazwie prototypu grupy hostów
    - wartości tagu hosta
    - wartości makra hosta
    - (zobacz pełną listę)

We wszystkich tych miejscach, z wyjątkiem filtra reguły wykrywania niskiego poziomu, makra LLD mogą być używane wewnątrz statycznego kontekstu makra użytkownika.

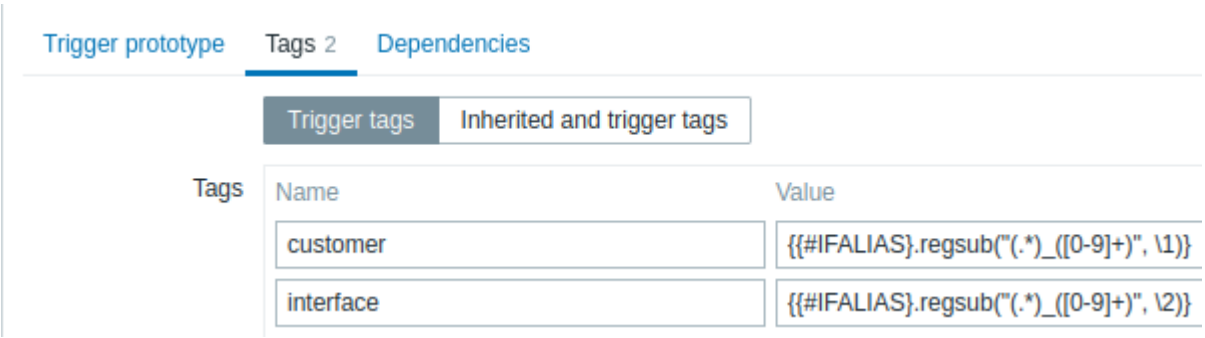
Używanie funkcji makr

Funkcje makr są obsługiwane w makrach low-level discovery (z wyjątkiem filtra reguły low-level discovery), umożliwiając wyodrębnienie określonej części wartości makra przy użyciu wyrażenia regularnego.

Na przykład możesz chcieć wyodrębnić nazwę klienta i numer interfejsu z następującego makra LLD na potrzeby tagowania zdarzeń:

```
{#IFALIAS}=customername_1
```

Aby to zrobić, można użyć funkcji makra `regsub` z makrem w polu wartości tagu zdarzenia prototypu wyzwalacza:



Należy pamiętać, że przecinki nie są dozwolone w nieujętych w cudzysłów parametrach klucza pozycji, dlatego parametr zawierający funkcję makra musi być ujęty w cudzysłów. Znaku ukośnika odwrotnego (\) należy używać do poprzedzania podwójnych cudzysłowów wewnątrz parametru. Przykład:

```
net.if.in["{{#IFALIAS}.regsub(\"(.*)_([0-9]+)\", \1)}",bytes]
```

Więcej informacji o składni funkcji makr znajduje się tutaj: Funkcje makr

Funkcje makr są obsługiwane w makrach low-level discovery od wersji Zabbix 4.0.

Prototypy pozycji bez parametrów klucza

Gdy parametry klucza pozycji nie są używane, umieść makro LLD wewnątrz nawiasów parametrów klucza pozycji `[...]`, aby było traktowane jako parametr i zastępowane podczas wykrywania:

```
v_[{#MACRO}]
```

Przypisy

[1] W polach oznaczonych [1] pojedyncze makro musi wypełniać całe pole. Wiele makr w polu lub makra zmieszane z tekstem nie są obsługiwane.

6 Makra wyrażeń

Przegląd

Makra wyrażeń umożliwiają wykonywanie obliczeń w polach.

Ich wartość jest obliczana poprzez najpierw rozwinięcie wszystkich zagnieżdżonych makr, a następnie obliczenie wynikowego wyrażenia.

Składnia:

```
{?EXPRESSION}
```

EXPRESSION używa tej samej składni i obsługuje te same funkcje, co wyrażenia wyzwalaczy.

Przykład:

```
{?trendavg(/host/item1,1M:now/M)/trendavg(/host/item1,1M:now/M-1y)*100}
```

Aby sprawdzić miejsca obsługujące makra wyrażeń, wyszukaj „{?EXPRESSION}" w tabeli obsługiwanych makr.

Uwagi dotyczące użycia:

- Używaj makr {FUNCTION.*}, aby odwoływać się do wartości funkcji wyrażeń wyzwalaczy/wyrażeń odzyskiwania.
- Używaj makr {HOST.HOST<1-9>} i {ITEM.KEY<1-9>}, aby odwoływać się do hostów i pozycji.
- W szablonach używaj makr {HOST.HOST<1-9>} lub całkowicie pomijaj host dla pierwszego hosta — na przykład {?avg(//item1,1h)} — zamiast nazw szablonów, ponieważ nazwy szablonów nie są zastępowane nazwami hostów podczas podłączania szablonów.

```
{?{FUNCTION.VALUE2} - {FUNCTION.VALUE3}}
{?max(/{HOST.HOST}/{ITEM.KEY},3h)}
```

Zobacz także Przykłady wyrażeń wyzwalaczy, aby zapoznać się z przykładem użycia makra wyrażenia w nazwie zdarzenia.

12 Użytkownicy i grupy użytkowników

Przegląd

Wszyscy użytkownicy w Zabbix uzyskują dostęp do aplikacji Zabbix za pośrednictwem internetowego frontend. Każdemu użytkownikowi przypisywana jest unikalna nazwa logowania i hasło.

Wszystkie hasła użytkowników są szyfrowane i przechowywane w bazie danych Zabbix. Użytkownicy nie mogą używać swojego identyfikatora użytkownika i hasła do bezpośredniego logowania się do serwera UNIX, chyba że zostali również odpowiednio skonfigurowani w systemie UNIX. Komunikacja między serwerem WWW a przeglądarką użytkownika może być chroniona przy użyciu SSL.

Dzięki elastycznemu schematowi uprawnień użytkowników można ograniczać i rozróżniać uprawnienia do:

- dostępu do administracyjnych funkcji frontend Zabbix
- wykonywania określonych działań we frontend
- dostępu do monitorowanych hostów w grupach hostów
- korzystania z określonych metod API

1 Konfigurowanie użytkownika

Przegląd

Początkowa instalacja Zabbix zawiera dwóch predefiniowanych użytkowników:

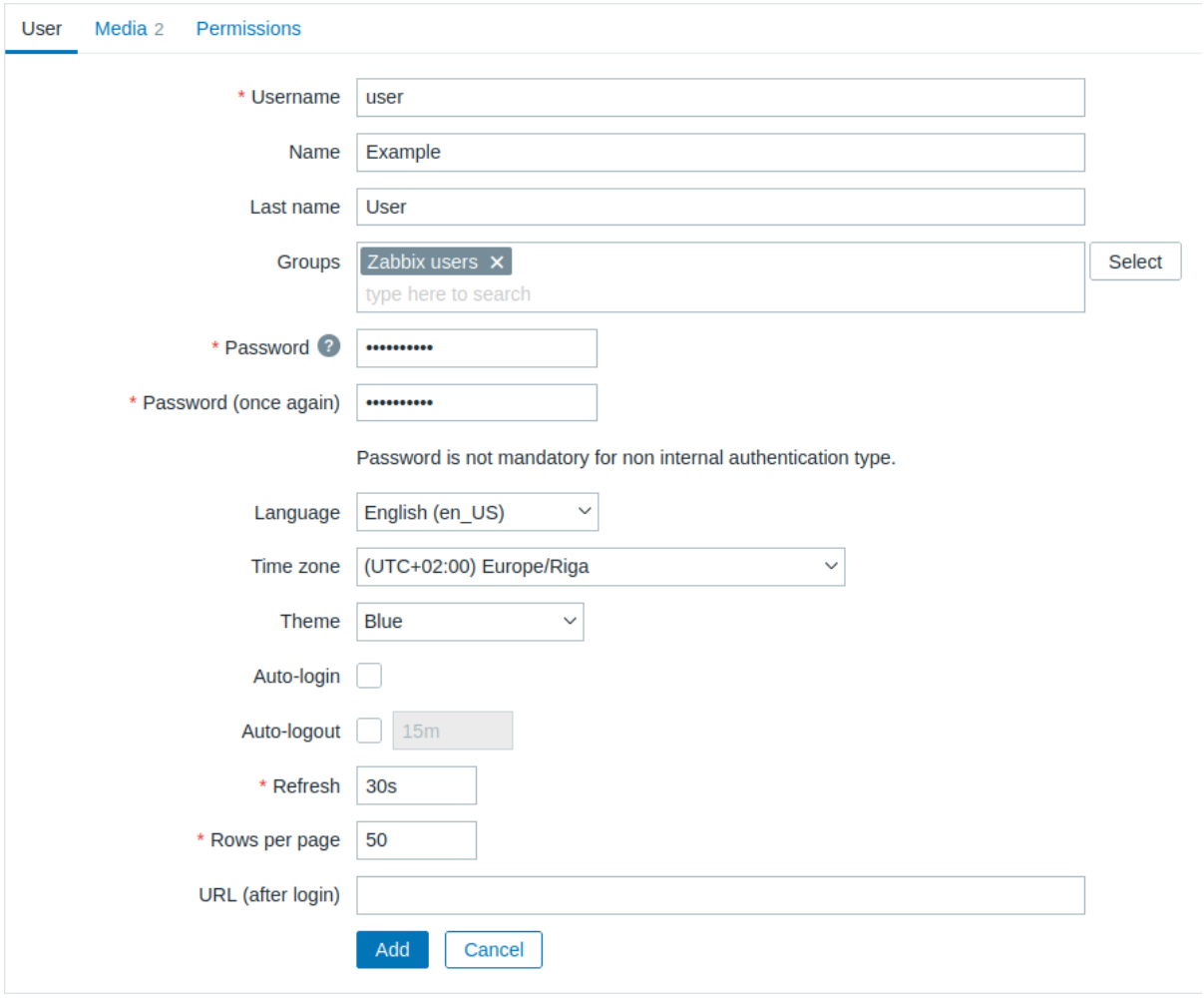
- *Admin* — superużytkownik Zabbix z pełnymi uprawnieniami.
- *guest* — specjalny użytkownik Zabbix. Użytkownik „guest" jest domyślnie wyłączony. Jeśli dodasz go do grupy użytkowników Guests, możesz zalogować się na to konto i uzyskać dostęp do stron monitorowania w Zabbix. Pamiętaj, że domyślnie użytkownik „guest" nie ma żadnych uprawnień do obiektów Zabbix.

Aby skonfigurować użytkownika:

- Przejdź do *Users* → *Users*.
- Kliknij *Create user* (lub nazwę użytkownika, aby edytować istniejącego użytkownika).
- Edytuj atrybuty użytkownika w formularzu.

Atrybuty ogólne

Zakładka *Użytkownik* zawiera ogólne atrybuty użytkownika:



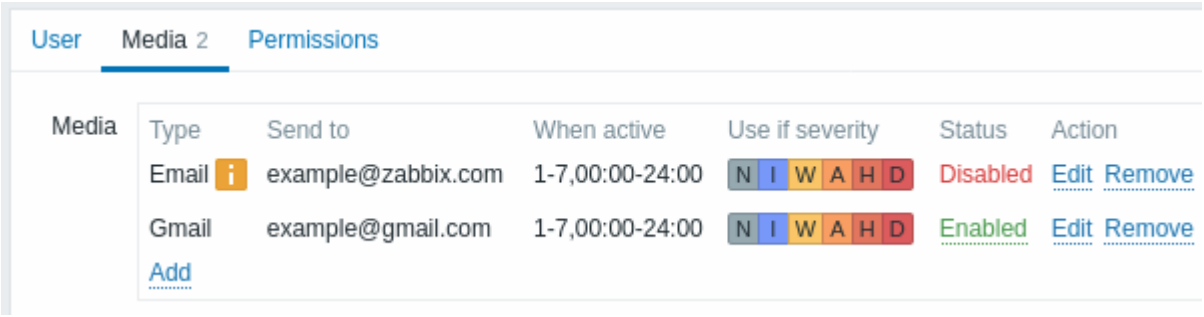
Wszystkie wymagane pola wejściowe są oznaczone czerwoną gwiazdką.

Parametr	Opis
Username	Unikalna nazwa użytkownika, używana jako nazwa logowania.
Name	Imię użytkownika (opcjonalnie). Jeśli pole nie jest puste, jest widoczne w informacjach o potwierdzeniu i informacjach o odbiorcy powiadomienia.
Last name	Nazwisko użytkownika (opcjonalnie). Jeśli pole nie jest puste, jest widoczne w informacjach o potwierdzeniu i informacjach o odbiorcy powiadomienia.
Groups	Wybierz grupy użytkowników, do których należy użytkownik. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy grupy użytkowników zostanie wyświetlona rozwijana lista pasujących grup. Przewiń w dół, aby wybrać. Alternatywnie kliknij *Select*, aby dodać grupy. Kliknij „x", aby usunąć wybrane. Przynależność do grup użytkowników określa, do których grup hostów i hostów użytkownik będzie miał dostęp.
Password	Dwa pola do wprowadzenia hasła użytkownika lub przycisk *Change password*, jeśli użytkownik już istnieje. Kliknięcie przycisku *Change password* otwiera dwa pola do wprowadzenia nowego hasła. Dla użytkownika z rolą *Super admin role*, który zmienia własne hasło, kliknięcie przycisku *Change password* otwiera dodatkowe pole do wprowadzenia bieżącego (starego) hasła. Po pomyślnej zmianie hasła użytkownik, którego hasło zostało zmienione, zostanie wylogowany ze wszystkich aktywnych sesji. Należy pamiętać, że hasło można zmienić tylko dla użytkowników korzystających z uwierzytelniania wewnętrznego Zabbix.
Language	Język frontendu Zabbix. Do działania tłumaczeń wymagane jest rozszerzenie php gettext.
Time zone	Wybierz strefę czasową, aby zastąpić globalną strefę czasową na poziomie użytkownika, lub wybierz **System default**, aby użyć globalnych ustawień strefy czasowej.

Parametr	Opis
Theme	Określa wygląd frontendu: **System default** - użyj domyślnych ustawień systemowych **Blue** - standardowy niebieski motyw **Dark** - alternatywny ciemny motyw **High-contrast light** - jasny motyw o wysokim kontraście **High-contrast dark** - ciemny motyw o wysokim kontraście
Auto-login	Zaznacz to pole wyboru, aby Zabbix zapamiętał użytkownika i logował go automatycznie przez 30 dni. Podczas logowania z opcją *Remember for 30 days*: - Automatyczne wylogowanie jest resetowane (sesja utrzymuje się przez 30 dni). - Auto-login jest włączane w celu płynnego ponownego uwierzytelniania. Podczas logowania bez opcji *Remember for 30 days*: - Auto-login jest włączane w celu płynnego ponownego uwierzytelniania. - Auto-logout pozostaje zależne od standardowego ustawienia limitu czasu. W tym celu używane są pliki cookie przeglądarki.
Auto-logout	Po zaznaczeniu tego pola wyboru użytkownik zostanie wylogowany automatycznie po upływie ustawionej liczby sekund (minimum 90 sekund, maksimum 1 dzień). Należy pamiętać, że to ustawienie jest nadpisywane, jeśli włączona jest opcja *Remember for 30 days*, ponieważ sesja jest przedłużana na cały ten okres. Obsługiwane są sufiksy czasu, np. 90s, 5m, 2h, 1d. Należy pamiętać, że ta opcja nie będzie działać: * Jeśli globalna opcja konfiguracji „Show warning if Zabbix server is down” jest włączona i frontend Zabbix pozostaje otwarty. * Gdy strony menu Monitoring wykonują odświeżanie informacji w tle. * Jeśli logowanie odbywa się z zaznaczoną opcją *Remember me for 30 days*.
Refresh	Ustaw częstotliwość odświeżania używaną dla wykresów, danych w postaci zwykłego tekstu itp. Można ustawić 0, aby wyłączyć. Obsługiwane są sufiksy czasu, np. 90s, 5m, 1h.
Rows per page	Możesz określić, ile wierszy na stronę będzie wyświetlanych na listach.
URL (after login)	Możesz sprawić, aby Zabbix po pomyślnym zalogowaniu przekierował użytkownika pod określony adres URL, na przykład na stronę *Problems*.

Media użytkownika

Zakładka *Media* zawiera listę wszystkich mediów zdefiniowanych dla użytkownika. Media są używane do wysyłania powiadomień.



Kliknij *Add*, aby przypisać media do użytkownika.

Jeśli typ mediów został wyłączony:

- Po nazwie wyświetlana jest żółta ikona informacyjna.
- W kolumnie Status wyświetlane jest *Disabled*.

Note:
Uprawnienia użytkownika do zmiany szczegółów własnych mediów mogą być przyznawane/odbierane na podstawie jego roli użytkownika (zobacz opcję *Create and edit own media*). Uprawnienia użytkownika Super admin do zmiany szczegółów mediów innych użytkowników również mogą być przyznawane/odbierane na podstawie jego roli użytkownika (zobacz opcję *Create and edit user media*)

Szczegółowe informacje o konfigurowaniu mediów użytkownika można znaleźć w sekcji Typy mediów.

Uprawnienia

Zakładka *Uprawnienia* zawiera informacje o następujących elementach:

- Rola użytkownika (wymagana dla każdego nowo utworzonego użytkownika), którą może zmienić wyłącznie użytkownik typu *Super admin*.

Attention:
Nie można tworzyć użytkowników bez roli użytkownika (z wyjątkiem użycia User API Zabbix). Użytkownicy utworzeni wcześniej, którzy nie mają przypisanej roli, nadal mogą być edytowani bez przypisywania im roli. Jednak po przypisaniu roli można ją już tylko zmienić, a nie usunąć.

 Należy pamiętać, że użytkownicy bez roli mogą logować się do Zabbix wyłącznie przy użyciu uwierzytelniania LDAP lub SAML, pod warunkiem że ich informacje LDAP/SAML odpowiadają mapowaniom grup użytkowników skonfigurowanym w Zabbix.

- Typ użytkownika (*User*, *Admin*, *Super admin*), który jest definiowany w konfiguracji roli użytkownika.
- Grupy hostów i grupy szablonów, do których użytkownik ma dostęp.
  - Użytkownicy typu *User* i *Admin* domyślnie nie mają dostępu do żadnych grup, szablonów ani hostów. Aby przyznać taki dostęp, użytkownicy muszą zostać dodani do grup użytkowników skonfigurowanych z uprawnieniami do odpowiednich obiektów.
- Prawa dostępu do sekcji i elementów Zabbix frontend, modułów oraz metod API.
  - Elementy z dozwolonym dostępem są wyświetlane na zielono, natomiast te z zabronionym dostępem — jasnoszarym kolorem.
- Uprawnienia do wykonywania określonych działań.
  - Działania, które użytkownik może wykonywać, są wyświetlane na zielono, natomiast te zabronione — jasnoszarym kolorem.

Szczegóły znajdują się na stronie Uprawnienia.

2 Uprawnienia

Przegląd

Uprawnienia w Zabbix zależą od typu użytkownika, dostosowanych ról użytkowników oraz dostępu do hostów, który jest określany na podstawie grupy użytkowników.

Typy użytkowników

Uprawnienia w Zabbix zależą przede wszystkim od typu użytkownika:

- *User* — ma ograniczone prawa dostępu do sekcji menu (zob. poniżej) i domyślnie nie ma dostępu do żadnych zasobów. Wszelkie uprawnienia do grup hostów lub grup szablonów muszą zostać jawnie przypisane;
- *Admin* — ma niepełne prawa dostępu do sekcji menu (zob. poniżej). Użytkownik domyślnie nie ma dostępu do żadnych grup hostów. Wszelkie uprawnienia do grup hostów lub grup szablonów muszą zostać jawnie nadane;
- *Super admin* — ma dostęp do wszystkich sekcji menu. Użytkownik ma dostęp do odczytu i zapisu do wszystkich grup hostów i grup szablonów. Uprawnień nie można cofnąć przez odmowę dostępu do określonych grup.

Dostęp do menu

Note:
Ograniczony dostęp do niektórych elementów interfejsu użytkownika zapobiega jedynie otwarciu tej strony — nie usuwa możliwości dostępu do bazowych danych w innych częściach interfejsu.

Poniższa tabela przedstawia dostęp do sekcji menu Zabbix według typu użytkownika:

Sekcja menu		User	Admin	Super admin
Panele		+	+	+
Monitorowanie		+	+	+
	Problemy	+	+	+
	Hosty	+	+	+
	Najnowsze dane	+	+	+
	Mapy	+	+	+
	Wykrywanie		+	+
Usługi		+	+	+
	Usługi	+	+	+
	SLA		+	+
	Raport SLA	+	+	+
Inwentaryzacja		+	+	+

Sekcja menu		User	Admin	Super admin
	Przegląd	+	+	+
	Hosty	+	+	+
Raporty		+	+	+
	Informacje o systemie			+
	Raporty cykliczne		+	+
	Raport dostępności	+	+	+
	Top 100 wyzwalaczy	+	+	+
	Dziennik audytu			+
	Dziennik działań			+
	Powiadomienia		+	+
Zbieranie danych			+	+
	Grupy szablonów		+	+
	Grupy hostów		+	+
	Szablony		+	+
	Hosty		+	+
	Konserwacja		+	+
	Korelacja zdarzeń			+
	Wykrywanie		+	+
Alerty			+	+
	Akcje wyzwalaczy		+	+
	Akcje usług		+	+
	Akcje wykrywania		+	+
	Akcje autorejestracji		+	+
	Akcje wewnętrzne		+	+
	Typy mediów			+
	Skrypty			+
Użytkownicy				+
	Grupy użytkowników			+
	Role użytkowników			+
	Użytkownicy			+
	Tokeny API			+
	Uwierzytelnianie			+
Administracja				+
	Ogólne			+
	Dziennik audytu			+
	Housekeeping			+
	Grupy proxy			+
	Proxy			+
	Makra			+
	Kolejka			+

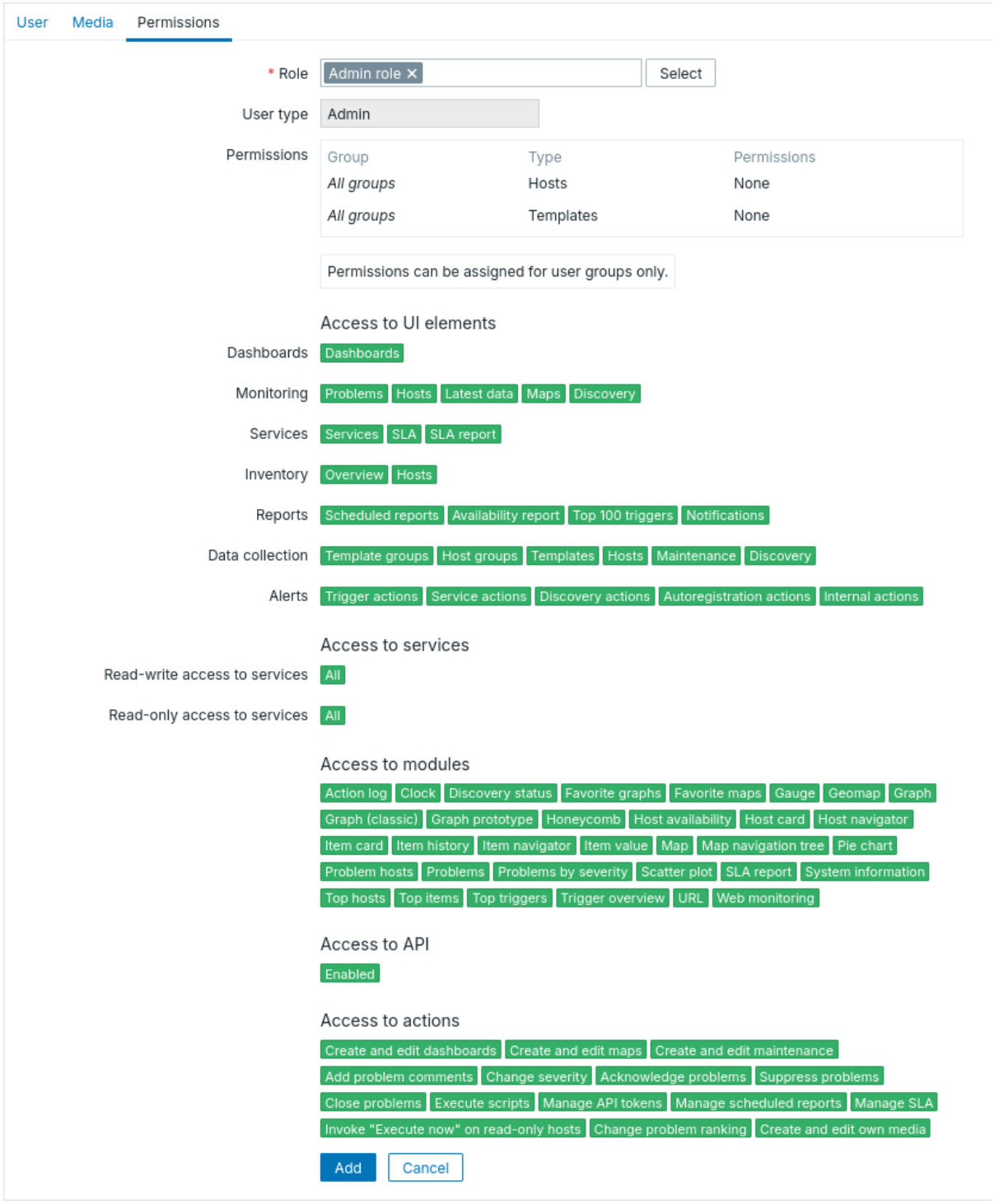
Role użytkowników

Role użytkowników umożliwiają wprowadzanie niestandardowych zmian w uprawnieniach zdefiniowanych przez typ użytkownika. Chociaż nie można dodawać żadnych uprawnień (ponieważ wykraczałoby to poza uprawnienia typu użytkownika), niektóre uprawnienia można odebrać.

Ponadto rola użytkownika określa dostęp nie tylko do sekcji menu, ale także do usług, modułów, metod API oraz różnych działań we frontend.

Role użytkowników są konfigurowane w sekcji *Użytkownicy* → *Role użytkowników* przez użytkowników typu Super admin.

Role użytkowników są przypisywane użytkownikom w formularzu konfiguracji użytkownika, na karcie *Uprawnienia*, przez użytkowników typu Super admin.



Dostęp do hostów

Dostęp do danych dowolnego hosta i szablonu w Zabbix jest przyznawany grupom użytkowników wyłącznie na poziomie grupy hostów/szablonów.

Oznacza to, że pojedynczemu użytkownikowi nie można bezpośrednio przyznać dostępu do hosta (ani grupy hostów). Dostęp do hosta może on uzyskać wyłącznie poprzez przynależność do grupy użytkowników, której przyznano dostęp do grupy hostów zawierającej tego hosta.

Podobnie, użytkownik może uzyskać dostęp do szablonu wyłącznie poprzez przynależność do grupy użytkowników, której przyznano dostęp do grupy szablonów zawierającej ten szablon.

3 Grupy użytkowników

Przegląd

Grupy użytkowników umożliwiają grupowanie użytkowników zarówno do celów organizacyjnych, jak i do przypisywania uprawnień do danych. Uprawnienia do przeglądania i konfigurowania danych grup hostów i grup szablonów są przypisywane do grup użytkown-

ików, a nie do poszczególnych użytkowników.

Często sensowne jest rozdzielenie, jakie informacje są dostępne dla jednej grupy użytkowników, a jakie dla innej. Można to osiągnąć przez grupowanie użytkowników, a następnie przypisywanie zróżnicowanych uprawnień do grup hostów i grup szablonów.

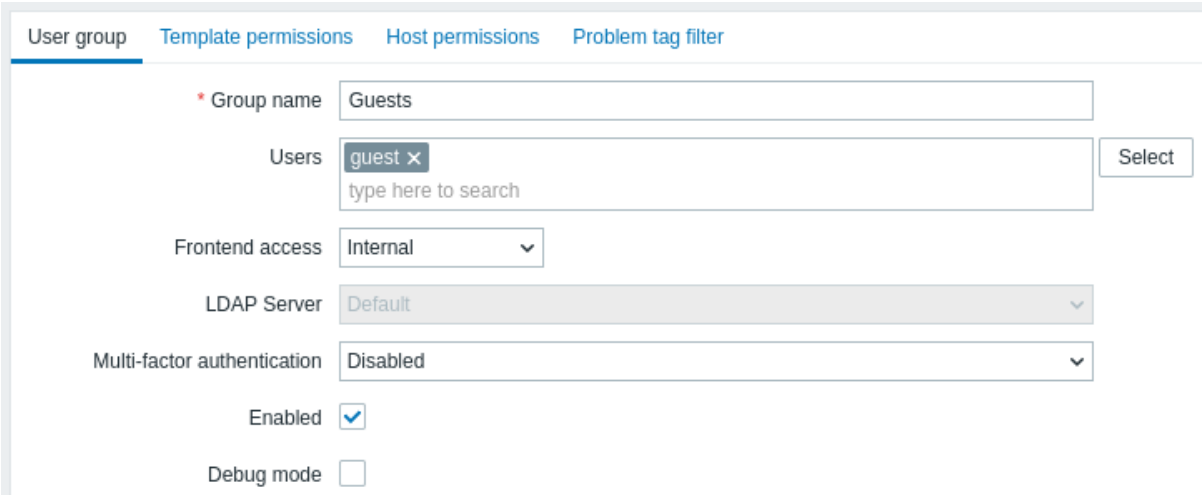
Użytkownik może należeć do dowolnej liczby grup.

Konfiguracja

Aby skonfigurować grupę użytkowników:

- Przejdź do *Użytkownicy* > *Grupy użytkowników*
- Kliknij *Utwórz grupę użytkowników* (lub nazwę grupy, aby edytować istniejącą grupę)
- Edytuj atrybuty grupy w formularzu

Zakładka **Grupa użytkowników** zawiera ogólne atrybuty grupy:

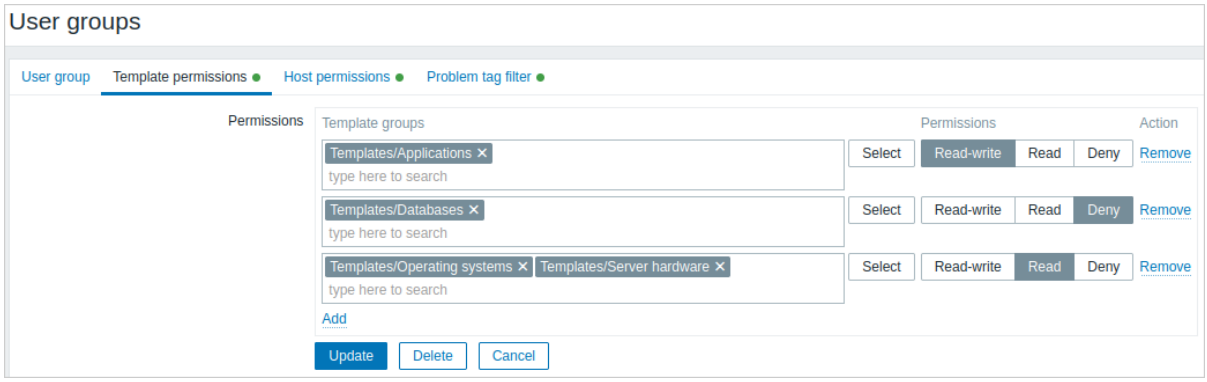


Wszystkie wymagane pola wejściowe są oznaczone czerwoną gwiazdką.

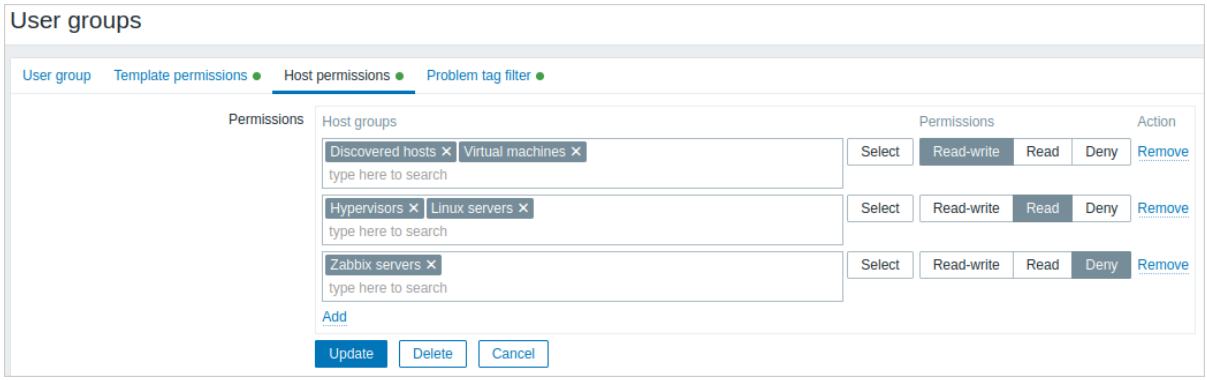
Parameter	Description
Nazwa grupy	Unikalna nazwa grupy.
Użytkownicy	Aby dodać użytkowników do grupy, zacznij wpisywać nazwę istniejącego użytkownika. Gdy pojawi się lista rozwijana z pasującymi nazwami użytkowników, przewiń ją w dół, aby wybrać użytkownika. Alternatywnie możesz kliknąć przycisk *Wybierz*, aby wybrać użytkowników w wyskakującym oknie.
Dostęp do frontend	Sposób uwierzytelniania użytkowników z tej grupy. **Domyślny systemowy** - użyj domyślnej metody uwierzytelniania (ustawionej globalnie) **Wewnętrzny** - użyj wewnętrznego uwierzytelniania Zabbix (nawet jeśli globalnie używane jest uwierzytelnianie LDAP). Ignorowane, jeśli globalnym ustawieniem domyślnym jest uwierzytelnianie HTTP. **LDAP** - użyj uwierzytelniania LDAP (nawet jeśli globalnie używane jest uwierzytelnianie wewnętrzne). Ignorowane, jeśli globalnym ustawieniem domyślnym jest uwierzytelnianie HTTP. **Wyłączony** - dostęp do frontend Zabbix jest zabroniony dla tej grupy
Serwer LDAP	Wybierz, którego serwera LDAP użyć do uwierzytelniania użytkownika. To pole jest dostępne tylko wtedy, gdy *Dostęp do frontend* jest ustawiony na LDAP lub Domyślny systemowy.
Uwierzytelnianie wieloskładnikowe	Wybierz, której metody uwierzytelniania wieloskładnikowego użyć do uwierzytelniania użytkownika: **Domyślna** - użyj metody ustawionej jako domyślna w konfiguracji MFA; ta opcja jest domyślnie wybierana dla nowych grup użytkowników, jeśli MFA jest włączone; **<Nazwa metody>** - użyj wybranej metody (na przykład „Zabbix TOTP”); **Wyłączone** - MFA jest wyłączone dla tej grupy; ta opcja jest domyślnie wybierana dla nowych grup użytkowników, jeśli MFA jest wyłączone. Zwróć uwagę, że jeśli użytkownik należy do wielu grup użytkowników z włączonym MFA (lub przynajmniej jedna grupa ma włączone MFA), obowiązują następujące zasady uwierzytelniania: jeśli jakakolwiek grupa używa domyślnej metody MFA „Domyślna”, zostanie ona użyta do uwierzytelnienia użytkownika; w przeciwnym razie do uwierzytelnienia zostanie użyta pierwsza metoda w kolejności alfabetycznej.

Parameter	Description
Włączona	Status grupy użytkowników i członków grupy. *Zaznaczone* - grupa użytkowników i użytkownicy są włączeni *Niezaznaczone* - grupa użytkowników i użytkownicy są wyłączeni
Tryb debugowania	Zaznacz to pole wyboru, aby włączyć tryb debugowania dla użytkowników.

Zakładka **Uprawnienia do szablonów** umożliwia określenie dostępu grupy użytkowników do danych grup szablonów (a tym samym szablonów):



Zakładka **Uprawnienia do hostów** umożliwia określenie dostępu grupy użytkowników do danych grup hostów (a tym samym hostów):



Kliknij Add, aby wybrać grupy szablonów/hostów (zarówno nadrzędne, jak i zagnieżdżone) i przypisać im uprawnienia. Zacznij wpisywać nazwę grupy (pojawi się lista rozwijana z pasującymi grupami) lub kliknij *Wybierz*, aby otworzyć wyskakujące okno z listą wszystkich grup.

Następnie użyj przycisków opcji, aby przypisać uprawnienia do wybranych grup. Dostępne są następujące uprawnienia:

- **Odczyt-zapis** - dostęp do grupy z prawem odczytu i zapisu
- **Odczyt** - dostęp do grupy tylko do odczytu
- **Odmów** - dostęp do grupy zabroniony

Jeśli ta sama grupa szablonów/hostów zostanie dodana w kilku wierszach z różnymi ustawionymi uprawnieniami, zastosowane zostanie najbardziej restrykcyjne uprawnienie.

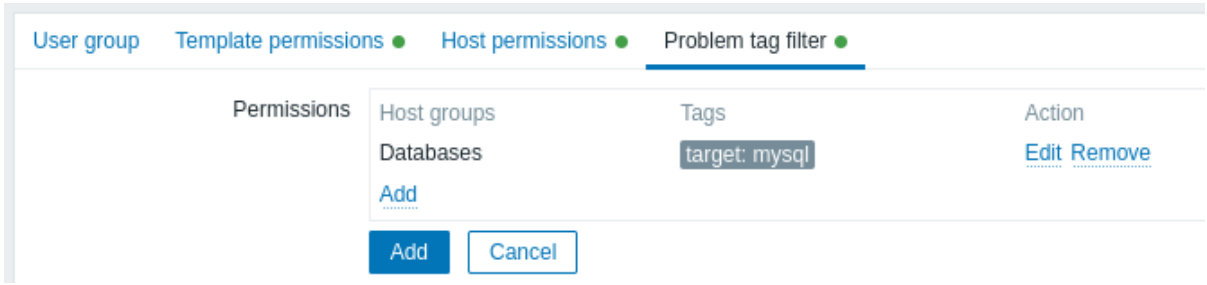
Zwróć uwagę, że użytkownik *Super admin* może wymusić, aby grupy zagnieżdżone miały ten sam poziom uprawnień co grupa nadrzędna; można to zrobić w formularzu konfiguracji grup hostów/szablonów.

Zakładki **Uprawnienia do szablonów** i **Uprawnienia do hostów** obsługują ten sam zestaw parametrów.

Bieżące uprawnienia do grup są wyświetlane w bloku *Uprawnienia* i mogą być tam modyfikowane lub usuwane.

Note:
Jeśli grupa użytkowników ma uprawnienia **Odczyt-zapis** do hosta oraz uprawnienia **Odmów** lub brak uprawnień do szablonu podłączonego do tego hosta, użytkownicy tej grupy nie będą mogli edytować pozycji pochodzących z szablonu na hoście, a nazwa szablonu będzie wyświetlana jako *Niedostępny szablon*.

Zakładka **Filtr tagów problemów** umożliwia ustawienie opartych na tagach uprawnień dla grup użytkowników do wyświetlania problemów filtrowanych według nazwy i wartości tagu:

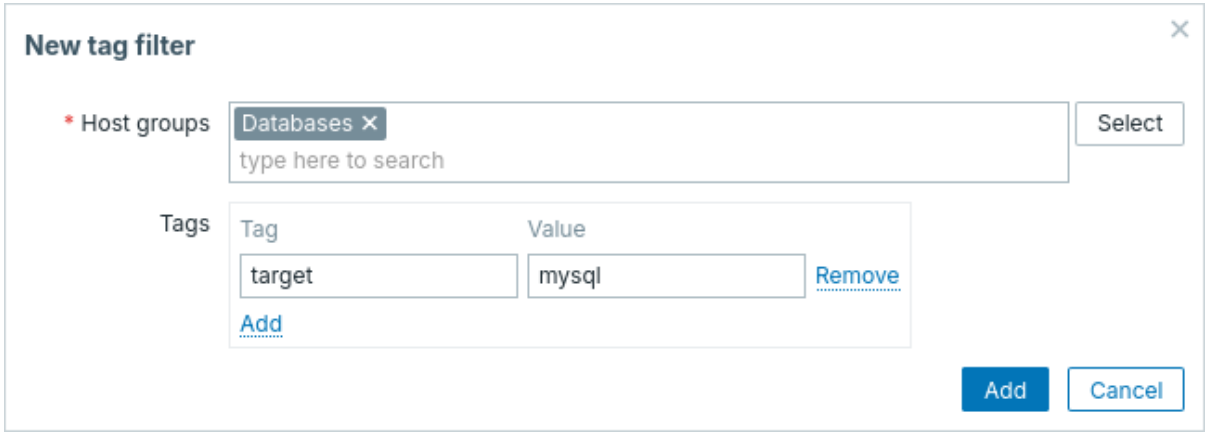


Kliknij Add, aby wybrać grupy hostów. Aby wybrać grupę hostów, dla której ma zostać zastosowany filtr tagów, kliknij *Wybierz*, aby uzyskać pełną listę istniejących grup hostów, lub zacznij wpisywać nazwę grupy hostów, aby wyświetlić listę rozwijaną z pasującymi grupami. Wyświetlane będą tylko grupy hostów, ponieważ filtr tagów problemów nie może być stosowany do grup szablonów.

Można dodawać nazwy tagów bez wartości, ale nie można dodawać wartości bez nazw. W bloku *Uprawnienia* wyświetlane są tylko pierwsze trzy tagi (wraz z wartościami, jeśli istnieją); jeśli jest ich więcej, można je zobaczyć po kliknięciu lub najechaniu kursorem na ikonę •••.

Filtr tagów pozwala oddzielić dostęp do grupy hostów od możliwości wyświetlania problemów.

Na przykład, jeśli administrator bazy danych ma widzieć tylko problemy bazy danych „MySQL", należy najpierw utworzyć grupę użytkowników dla administratorów baz danych, a następnie określić nazwę tagu „target" i wartość „mysql".



Jeśli określono nazwę tagu „target", a pole wartości pozostawiono puste, grupa użytkowników będzie widzieć wszystkie problemy z nazwą tagu „target" dla wybranej grupy hostów.

Upewnij się, że nazwa tagu i wartość tagu są określone poprawnie, w przeciwnym razie grupa użytkowników nie będzie widzieć żadnych problemów.

Przeanalizujmy przykład, w którym użytkownik jest członkiem kilku wybranych grup użytkowników. W takim przypadku filtrowanie będzie używać warunku OR dla tagów.

Grupa użytkowników A			**Grupa użytkowników B**			**Wynik widoczny dla użytkownika (członka) obu grup**
Filtr tagów						
Grupa hostów	*Nazwa tagu*	*Wartość tagu*	*Grupa hostów*	*Nazwa tagu*	*Wartość tagu*	
Bazy danych	target	mysql	Bazy danych	target	oracle	widoczne problemy target:mysql lub target:oracle
Nieskonfigurowane w **Filtr tagów problemów**			Bazy danych	target	oracle	widoczne problemy target:oracle

Dostęp z kilku grup użytkowników

Użytkownik może należeć do dowolnej liczby grup użytkowników. Grupy te mogą mieć różne uprawnienia dostępu do hostów lub szablonów.

Dlatego ważne jest, aby wiedzieć, do jakich encji nieuprzywilejowany użytkownik będzie miał w rezultacie dostęp. W poniższym przykładzie rozważmy, jak dostęp do hosta **X** (w grupie hostów 1) będzie zależał od różnych sytuacji dla użytkownika należącego do grup użytkowników A i B.

- Jeśli grupa A ma tylko dostęp *Odczyt* do grupy hostów 1, a grupa B ma dostęp *Odczyt-zapis* do grupy hostów 1, użytkownik otrzyma dostęp **Odczyt-zapis** do „X".

Attention:
Uprawnienia „Odczyt-zapis" mają pierwszeństwo przed uprawnieniami „Odczyt".

- W tym samym scenariuszu co powyżej, jeśli „X" jednocześnie należy także do grupy hostów 2, do której dostęp jest **zabroniony** dla grupy A lub B, dostęp do „X" będzie **niedostępny**, pomimo dostępu *Odczyt-zapis* do grupy hostów 1.
- Jeśli grupa A nie ma zdefiniowanych żadnych uprawnień, a grupa B ma dostęp *Odczyt-zapis* do grupy hostów 1, użytkownik otrzyma dostęp **Odczyt-zapis** do „X".
- Jeśli grupa A ma dostęp *Odmowa* do grupy hostów 1, a grupa B ma dostęp *Odczyt-zapis* do grupy hostów 1, dostęp użytkownika do „X" będzie **zabroniony**.

Inne szczegóły

- Użytkownik na poziomie Admin z uprawnieniami *Read-write* do hosta nie będzie mógł podłączać/odłączać szablonów, jeśli nie ma dostępu do grupy szablonów, do której one należą. Przy uprawnieniach *Read* do grupy szablonów będzie mógł podłączać/odłączać szablony do hosta, jednak nie będzie widział żadnych szablonów na liście szablonów i nie będzie mógł wykonywać operacji na szablonach w innych miejscach.
- Użytkownik na poziomie Admin z uprawnieniami *Read* do hosta nie zobaczy hosta na liście hostów w sekcji konfiguracji; jednak wyzwalacze hosta będą dostępne w konfiguracji usług IT.
- Każdy użytkownik niebędący Super Adminem (w tym „guest") może widzieć mapy sieci, o ile mapa jest pusta lub zawiera tylko obrazy. Gdy do mapy zostaną dodane hosty, grupy hostów lub wyzwalacze, uprawnienia będą respektowane.
- Serwer Zabbix nie będzie wysyłał powiadomień do użytkowników zdefiniowanych jako odbiorcy operacji akcji, jeśli dostęp do danego hosta jest jawnie „denied".

13 Przechowywanie sekretów

Przegląd

Zabbix można skonfigurować tak, aby pobierał poufne informacje z bezpiecznego sejfu. Obsługiwane są następujące usługi zarządzania sekretami: HashiCorp Vault KV Secrets Engine - Version 2, CyberArk Vault CV12.

Sekrety mogą być używane do pobierania:

- wartości makr użytkownika
- poświadczeń dostępu do bazy danych

Zabbix zapewnia dostęp tylko do odczytu do sekretów w sejfie, przy założeniu, że sekretami zarządza ktoś inny.

Aby uzyskać informacje o konfiguracji konkretnego dostawcy sejfu, zobacz:

- Konfiguracja HashiCorp
- Konfiguracja CyberArk

Buforowanie wartości sekretów

Domyślnie wartości makr sekretów z vault są pobierane przez serwer Zabbix przy każdym odświeżeniu danych konfiguracyjnych, a następnie przechowywane w pamięci podręcznej konfiguracji. Zabbix proxy otrzymuje wartości makr sekretów z vault od serwera Zabbix przy każdej synchronizacji konfiguracji i przechowuje je we własnej pamięci podręcznej konfiguracji.

Attention:
Szyfrowanie musi być włączone między serwerem Zabbix a proxy; w przeciwnym razie rejestrowany jest komunikat ostrzegawczy serwera.

Można również skonfigurować, aby wartości makr były pobierane niezależnie przez serwer Zabbix i Zabbix proxy.

Aby ręcznie wywołać odświeżenie buforowanych wartości sekretów z vault, użyj opcji wiersza poleceń 'secrets_reload' option.

W przypadku poświadczeń bazy danych Zabbix frontend buforowanie jest domyślnie wyłączone, ale można je włączyć, ustawiając opcję `$DB['VAULT_CACHE'] = true` w pliku zabbix.conf.php. Poświadczenia będą przechowywane w lokalnej pamięci

podręcznej z użyciem tymczasowego katalogu systemu plików. Serwer WWW musi zezwalać na zapis w prywatnym folderze tymczasowym (na przykład dla Apache musi być ustawiona opcja konfiguracyjna `PrivateTmp=True`). Aby kontrolować, jak często pamięć podręczna danych jest odświeżana/unieważniana, użyj stałej ZBX_DATA_CACHE_TTL constant .

Konfiguracja TLS

Aby skonfigurować TLS do komunikacji między komponentami Zabbix a skarbcem, dodaj certyfikat podpisany przez urząd certyfikacji (CA) do domyślnego magazynu CA dla całego systemu. Aby użyć innej lokalizacji, określ katalog w parametrze konfiguracyjnym SSLCALocation Zabbix serwer/proxy, umieść plik certyfikatu w tym katalogu, a następnie uruchom polecenie CLI:

```
c_rehash .
```

1 Konfiguracja CyberArk

W tej sekcji wyjaśniono, jak skonfigurować Zabbix do pobierania sekretów z CyberArk Vault CV12.

Vault powinien być zainstalowany i skonfigurowany zgodnie z opisem w oficjalnej dokumentacji CyberArk.

Aby dowiedzieć się więcej o konfiguracji TLS w Zabbix, zobacz *Przechowywanie sekretów*.

Dane uwierzytelniające bazy danych

Dostęp do sekretu zawierającego dane uwierzytelniające bazy danych jest konfigurowany oddzielnie dla każdego komponentu Zabbix.

Serwer i proxy

Aby pobrać dane uwierzytelniające bazy danych z sejfu dla Zabbix serwer lub proxy, należy określić następujące parametry konfiguracyjne w pliku konfiguracyjnym:

- `Vault` - który dostawca sejfu ma być używany;
- `VaultURL` - adres URL HTTP[S] serwera sejfu;
- `VaultDBPath` - zapytanie do sekretu sejfu zawierającego dane uwierzytelniające bazy danych, które zostaną pobrane przy użyciu kluczy ”Content” i ”UserName” (tej opcji można użyć tylko wtedy, gdy nie określono DBUser i DBPassword);
- `VaultTLSCertFile`, `VaultTLSKeyFile` - nazwy plików certyfikatu SSL i klucza; skonfigurowanie tych opcji nie jest obowiązkowe, ale jest zdecydowanie zalecane;
- `VaultPrefix` - niestandardowy prefiks ścieżki lub zapytania sejfu, w zależności od sejfu; jeśli nie zostanie określony, użyta zostanie najbardziej odpowiednia wartość domyślna.

Attention:
Parametry konfiguracyjne `Vault`, `VaultURL`, `VaultTLSCertFile`, `VaultTLSKeyFile` oraz `VaultPrefix` są również używane do uwierzytelniania w sejfie podczas przetwarzania makr sekretów sejfu przez Zabbix serwer (oraz Zabbix proxy, jeśli jest skonfigurowany). Zabbix serwer i proxy nie będą otwierać makr sekretów sejfu zawierających dane uwierzytelniające bazy danych z VaultDBPath.

Zabbix serwer i Zabbix proxy odczytują parametry konfiguracyjne związane z sejfem z plików *zabbix_server.conf* i *zabbix_proxy.conf* podczas uruchamiania.

Przykład

1. W *zabbix_server.conf* określ następujące parametry:

```
Vault=CyberArk
VaultURL=https://127.0.0.1:1858
VaultDBPath=AppID=zabbix_server&Query=Safe=passwordSafe;Object=zabbix_server_database
VaultTLSCertFile=cert.pem
VaultTLSKeyFile=key.pem
VaultPrefix=/AIMWebService/api/Accounts?
```

2. Zabbix wyśle do sejfu następujące żądanie API:

```
curl \
--header "Content-Type: application/json" \
--cert cert.pem \
--key key.pem \
https://127.0.0.1:1858/AIMWebService/api/Accounts?AppID=zabbix_server&Query=Safe=passwordSafe;Object=zabbi
```

3. Odpowiedź sejfu będzie zawierać klucze „Content” i „UserName”:

```
{
    "Content": <password>,
    "UserName": <username>,
    "Address": <address>,
    "Database": <Database>,
    "PasswordChangeInProcess":<PasswordChangeInProcess>
}
```

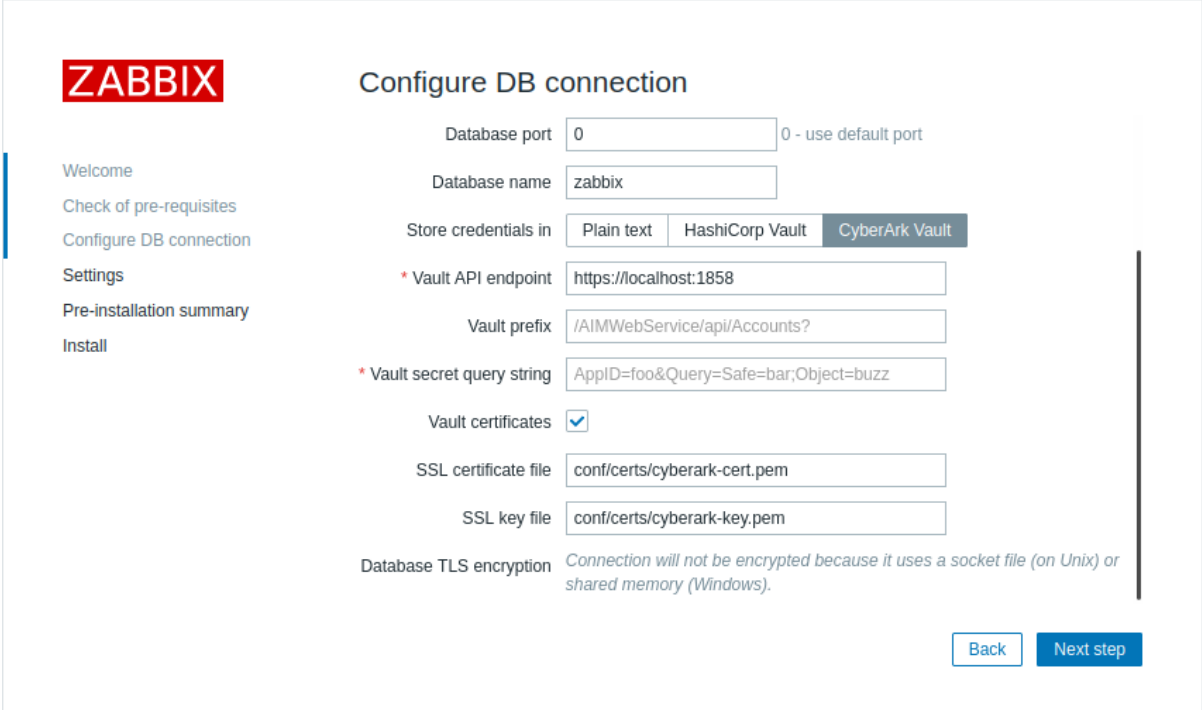
4. W rezultacie Zabbix użyje następujących poświadczeń do uwierzytelniania w bazie danych:

- Nazwa użytkownika: <username>
- Hasło: <password>

Frontend

Aby uzyskać poświadczenia bazy danych z sejfu dla frontend Zabbix, podczas instalacji frontend należy określić następujące parametry.

1. W kroku *Configure DB Connection* ustaw parametr *Store credentials in* na „CyberArk Vault”.



2. Następnie uzupełnij dodatkowe parametry:

Parametr	Wymagany	Wartość domyślna	Opis
Vault API endpoint	tak	https://localhost:1858	Określ adres URL połączenia z sejfem w formacie `scheme://host:port`
Vault prefix	nie	/AIMWebService/api/Accounts?	Podaj niestandardowy prefiks dla ścieżki lub zapytania sejfu. Jeśli nie zostanie podany, użyta zostanie wartość domyślna.
Vault secret query string	tak		Zapytanie określające, skąd mają zostać pobrane poświadczenia bazy danych. Przykład: `AppID=foo&Query=Safe=bar;Object=buzz`
Vault certificates	nie		Po zaznaczeniu tego pola wyboru pojawią się dodatkowe parametry umożliwiające skonfigurowanie uwierzytelniania klienta. Chociaż ten parametr jest opcjonalny, zdecydowanie zaleca się jego włączenie do komunikacji z CyberArk Vault.
SSL certificate file	nie	conf/certs/cyberark-cert.pem	Ścieżka do pliku certyfikatu SSL. Plik musi być w formacie PEM. Jeśli plik certyfikatu zawiera również klucz prywatny, pozostaw parametr SSL key file pusty.

Parametr	Wymagany	Wartość domyślna	Opis
SSL key file	nie	conf/certs/cyberark-key.pem	Nazwa pliku prywatnego klucza SSL używanego do uwierzytelniania klienta. Plik musi być w formacie PEM.

Wartości makr użytkownika

Aby używać CyberArk Vault do przechowywania wartości makr użytkownika typu *Vault secret*, upewnij się, że:

- serwer Zabbix jest skonfigurowany do pracy z CyberArk Vault;
- parametr *Vault provider* w *Administracja → Ogólne → Inne* jest ustawiony na „CyberArk Vault”.



Note:
Serwer Zabbix (oraz proxy Zabbix, jeśli jest skonfigurowany) wymaga dostępu do wartości makr typu *Vault secret* z sejfu. Frontend Zabbix nie potrzebuje takiego dostępu.

Wartość makra powinna zawierać zapytanie (w postaci `query:key`).

Szczegółowe informacje o przetwarzaniu wartości makr przez Zabbix można znaleźć w sekcji *Makra typu Vault secret*.

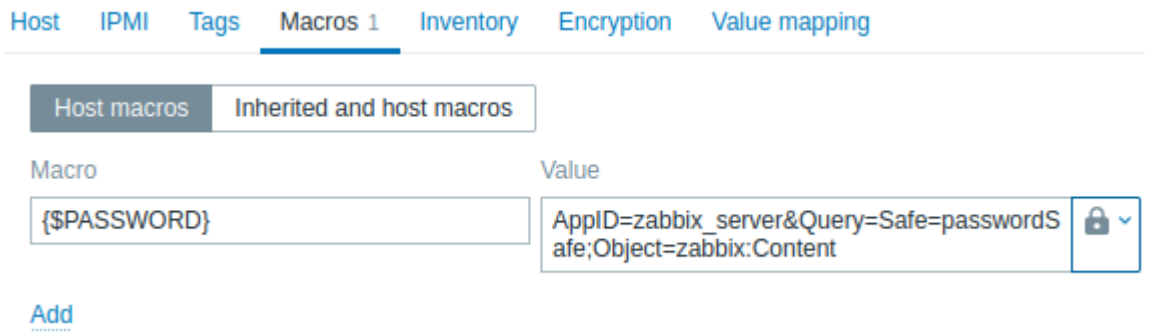
Składnia zapytania

Dwukropek (”:”) jest zarezerwowany do oddzielania zapytania od klucza.

Jeśli samo zapytanie zawiera ukośnik lub dwukropek, symbole te powinny być zakodowane w formacie URL (”/” jest kodowany jako ”%2F”, ”:” jest kodowany jako ”%3A”).

Przykład

1. W Zabbix dodaj makro użytkownika {$PASSWORD} typu *Vault secret* o wartości `AppID=zabbix_server&Query=Safe=passwordSaf`



2. Zabbix wyśle do sejfu następujące żądanie API:

```
curl \
--header "Content-Type: application/json" \
--cert cert.pem \
--key key.pem \
https://127.0.0.1:1858/AIMWebService/api/Accounts?AppID=zabbix_server&Query=Safe=passwordSafe;Object=zabbi
```

3. Odpowiedź sejfu będzie zawierać klucz ”Content”:

```
{
    "Content": <password>,
    "UserName": <username>,
    "Address": <address>,
    "Database" :<Database>,
    "PasswordChangeInProcess":<PasswordChangeInProcess>
}
```

4. W rezultacie Zabbix rozwiąże makro {$PASSWORD} do wartości - <password>

Aktualizacja istniejącej konfiguracji

Aby zaktualizować istniejącą konfigurację pobierania sekretów z CyberArk Vault:

1. Zaktualizuj parametry pliku konfiguracyjnego serwera Zabbix lub proxy zgodnie z opisem w sekcji *Dane logowania do bazy danych*.
2. Zaktualizuj ustawienia połączenia z bazą danych, rekonfigurując frontend Zabbix i podając wymagane parametry zgodnie z opisem w sekcji *Frontend*. Aby ponownie skonfigurować frontend Zabbix, otwórz w przeglądarce URL konfiguracji frontendu:

- dla Apache: http://<server_ip_or_name>/zabbix/setup.php
- dla Nginx: http://<server_ip_or_name>/setup.php

Alternatywnie parametry te można ustawić w pliku konfiguracyjnym frontendu (*zabbix.conf.php*):

```
$DB['VAULT']                    = 'CyberArk';
$DB['VAULT_URL']                = 'https://127.0.0.1:1858';
$DB['VAULT_DB_PATH']            = 'AppID=foo&Query=Safe=bar;Object=buzz';
$DB['VAULT_TOKEN']              = '';
$DB['VAULT_CERT_FILE']          = 'conf/certs/cyberark-cert.pem';
$DB['VAULT_KEY_FILE']           = 'conf/certs/cyberark-key.pem';
$DB['VAULT_PREFIX']             = '';
```

3. W razie potrzeby skonfiguruj makra użytkownika zgodnie z opisem w sekcji *Wartości makr użytkownika*.

Aby zaktualizować istniejącą konfigurację pobierania sekretów z HashiCorp Vault, zobacz *Konfiguracja HashiCorp*.

2 Konfiguracja HashiCorp

Przegląd

Ta sekcja wyjaśnia, jak skonfigurować Zabbix do pobierania sekretów z HashiCorp Vault KV Secrets Engine - wersja 2.

Vault powinien zostać wdrożony i skonfigurowany zgodnie z opisem w oficjalnej dokumentacji HashiCorp.

Aby dowiedzieć się więcej o konfigurowaniu TLS w Zabbix, zobacz *Przechowywanie sekretów*.

Pobieranie poświadczeń bazy danych

Aby pomyślnie pobrać sekret zawierający poświadczenia bazy danych, należy skonfigurować oba następujące elementy:

- serwer/proxy Zabbix
- frontend Zabbix

Serwer/proxy

Aby skonfigurować serwer lub proxy Zabbix, należy określić następujące parametry konfiguracyjne w pliku konfiguracyjnym:

- `Vault` — który dostawca vault ma być używany;
- `VaultToken` — token uwierzytelniania vault (szczegóły znajdują się w pliku konfiguracyjnym serwera/proxy Zabbix);
- `VaultURL` — adres URL HTTP[S] serwera vault;
- `VaultDBPath` — ścieżka do sekretu vault zawierającego poświadczenia bazy danych (tej opcji można użyć tylko wtedy, gdy nie określono DBUser i DBPassword); serwer lub proxy Zabbix pobierze poświadczenia przy użyciu kluczy „password” i „username”;
- `VaultPrefix` — niestandardowy prefiks ścieżki lub zapytania vault, zależnie od vault; jeśli nie zostanie określony, użyta zostanie najbardziej odpowiednia wartość domyślna.

Attention:
Parametry konfiguracyjne `Vault`, `VaultToken`, `VaultURL` i `VaultPrefix` są również używane do uwierzytelniania w vault podczas przetwarzania makr sekretów vault przez serwer Zabbix (oraz proxy Zabbix, jeśli jest skonfigurowany). Serwer Zabbix i proxy Zabbix nie będą otwierać makr sekretów vault zawierających poświadczenia DB z VaultDB-Path.

Zdecydowanie zaleca się używanie różnych tokenów dla różnych proxy.

Serwer Zabbix i proxy Zabbix odczytują parametry konfiguracyjne związane z vault z plików *zabbix_server.conf* i *zabbix_proxy.conf* podczas uruchamiania. Dodatkowo serwer Zabbix i proxy Zabbix odczytają zmienną środowiskową `VAULT_TOKEN` jednokrotnie podczas uruchamiania, a następnie ją usuną, aby nie była dostępna dla skryptów potomnych; wystąpi błąd, jeśli zarówno parametr `VaultToken`, jak i `VAULT_TOKEN` zawierają wartość.

Przykład

1. W pliku *zabbix_server.conf* określ następujące parametry:

```
Vault=HashiCorp
VaultToken=hvs.CAESIIG_PILmULFYOsEyWHxkZ2mF2a8VPKNLE8eHqd4autYGGh4KHGh2cy5aeTYONFNSaUp3ZnpWbDF1RUNjUkNTZEg
VaultURL=https://127.0.0.1:8200
VaultDBPath=database
VaultPrefix=/v1/secret/data/zabbix/
```

2. Uruchom następujące polecenia CLI, aby utworzyć wymagany sekret w vault:

```
#### Włącz punkt montowania "secret/", jeśli nie jest jeszcze włączony; zwróć uwagę, że musi być użyte "ku
vault secrets enable -path=secret/ kv-v2

#### Dodaj nowe sekrety z kluczami username i password w punkcie montowania "secret/" oraz pod ścieżką "za
vault kv put -mount=secret zabbix/database username=zabbix password=<password>

#### Sprawdź, czy sekret został pomyślnie dodany.
vault kv get secret/zabbix/database

#### Na koniec przetestuj za pomocą Curl; zwróć uwagę, że "data" należy dodać ręcznie po punkcie montowani
curl --header "X-Vault-Token: <VaultToken>" https://127.0.0.1:8200/v1/secret/data/zabbix/database
```

3. W rezultacie serwer Zabbix pobierze następujące dane uwierzytelniające do uwierzytelniania bazy danych:

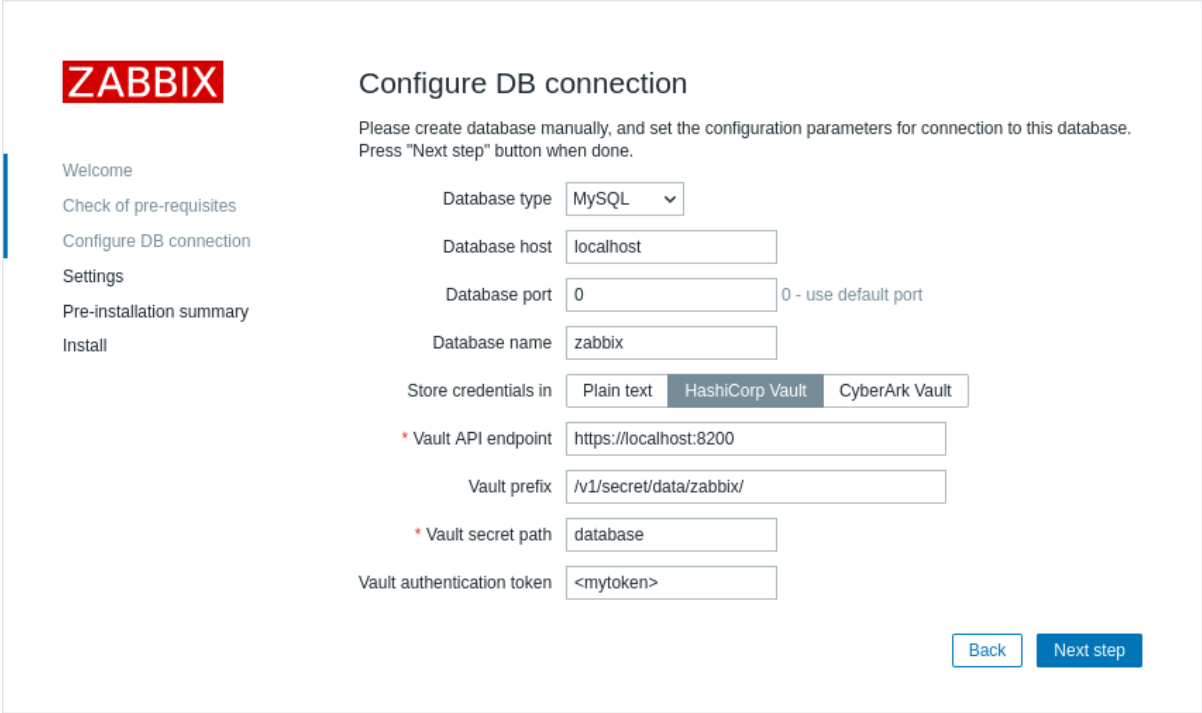
- Nazwa użytkownika: zabbix
- Hasło: <password>

Frontend

Frontend Zabbix może być skonfigurowany do pobierania poświadczeń bazy danych z vault zarówno podczas instalacji frontend, jak i przez aktualizację pliku konfiguracyjnego frontend (`zabbix.conf.php`).

Attention:
Jeśli poświadczenia vault zostały zmienione od czasu poprzedniej instalacji frontend, uruchom ponownie instalację frontend lub zaktualizuj `zabbix.conf.php`. Zobacz także: Aktualizacja istniejącej konfiguracji.

Podczas **instalacji frontend** parametry konfiguracyjne muszą zostać określone w kroku *Configure DB Connection*:



- Ustaw parametr *Store credentials in* na „HashiCorp Vault”.
- Określ parametry połączenia:

Parametr	Obowiązkowy	Wartość domyślna	Opis
Vault API endpoint	tak	https://localhost:8200	Podaj adres URL połączenia z vault w formacie `scheme://host:port`
Vault prefix	nie	/v1/secret/data/	Podaj niestandardowy prefiks dla ścieżki lub zapytania vault. Jeśli nie zostanie podany, użyty zostanie prefiks domyślny. Przykład: `/v1/secret/data/zabbix/`
Vault secret path	nie		Ścieżka do sekretu, z którego poświadczenia bazy danych będą pobierane przy użyciu kluczy „password” i „username”. Przykład: `database`
Vault authentication token	nie		Podaj token uwierzytelniający zapewniający dostęp tylko do odczytu ścieżki sekretu. Informacje o tworzeniu tokenów i polityk vault można znaleźć w dokumentacji HashiCorp.

Pobieranie wartości makr użytkownika

Aby używać HashiCorp Vault do przechowywania wartości makr użytkownika typu *Vault secret*, upewnij się, że:

- serwer/proxy Zabbix jest skonfigurowany do pracy z HashiCorp Vault;
- parametr *Vault provider* w *Administracja → Ogólne → Inne* jest ustawiony na „HashiCorp Vault” (domyślnie);



Note:
Serwer Zabbix (oraz proxy Zabbix, jeśli jest skonfigurowany) wymaga dostępu do wartości makr typu *Vault secret* z sejfu. Frontend Zabbix nie wymaga takiego dostępu.

Wartość makra powinna zawierać ścieżkę referencyjną (w postaci `path:key`, na przykład `macros:password`). Token uwierzytelniający określony podczas konfiguracji serwera/proxy Zabbix (parametrem `VaultToken`) musi zapewniać dostęp tylko do odczytu do tej ścieżki.

Szczegółowe informacje o przetwarzaniu wartości makr przez Zabbix można znaleźć w sekcji *Makra typu Vault secret*.

Składnia ścieżki

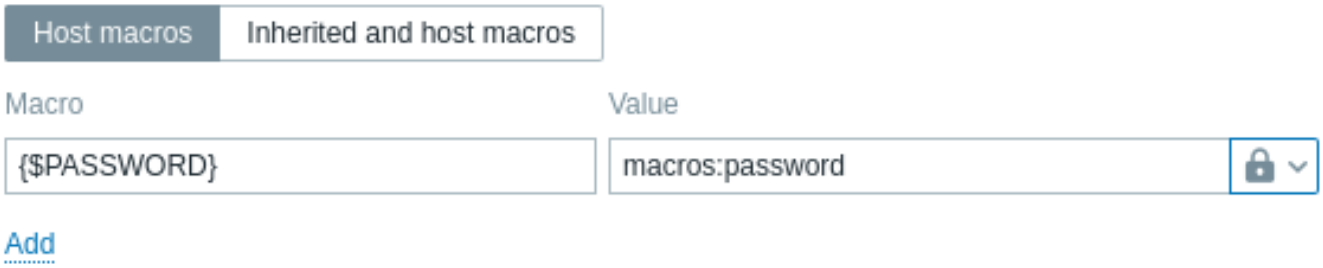
Symbole ukośnika (”/”) i dwukropka (”:”) są zastrzeżone.

Ukośnik może być używany wyłącznie do oddzielania punktu montowania od ścieżki (np. *secret/zabbix*, gdzie punkt montowania to ”secret”, a ścieżka to ”zabbix”). W przypadku makr Vault dwukropek może być używany wyłącznie do oddzielania ścieżki/zapytania od klucza.

Możliwe jest zakodowanie symboli ukośnika i dwukropka w formacie URL, jeśli istnieje potrzeba utworzenia punktu montowania o nazwie rozdzielonej ukośnikiem (np. *foo/bar/zabbix*, gdzie punkt montowania to ”foo/bar”, a ścieżka to ”zabbix”, można zakodować jako ”foo%2Fbar/zabbix”), a także jeśli nazwa punktu montowania lub ścieżka muszą zawierać dwukropek.

Przykład

1. W Zabbix dodaj makro użytkownika {$PASSWORD} typu ”Vault secret” o wartości `macros:password`



2. Uruchom następujące polecenia CLI, aby utworzyć wymagany sekret w vault:

```
#### Włącz punkt montowania "secret/", jeśli nie jest jeszcze włączony; zwróć uwagę, że musi zostać użyte
vault secrets enable -path=secret/ kv-v2

#### Umieść nowy sekret z kluczem "password" w punkcie montowania "secret/" i pod ścieżką "zabbix/macros".
vault kv put -mount=secret zabbix/macros password=<password>

#### Sprawdź, czy sekret został pomyślnie dodany.
vault kv get secret/zabbix/macros

#### Na koniec przetestuj za pomocą Curl; zwróć uwagę, że "data" należy dodać ręcznie po punkcie montowani
curl --header "X-Vault-Token: <VaultToken>" https://127.0.0.1:8200/v1/secret/data/zabbix/macros
```

3. W rezultacie Zabbix rozwiąże makro {$PASSWORD} do wartości: <password>

Aktualizacja istniejącej konfiguracji

Aby zaktualizować istniejącą konfigurację pobierania sekretów z HashiCorp Vault:

1. Zaktualizuj parametry pliku konfiguracyjnego serwera Zabbix lub proxy zgodnie z opisem w sekcji *Dane uwierzytelniające bazy danych*.
2. Zaktualizuj ustawienia połączenia z DB, rekonfigurując frontend Zabbix i podając wymagane parametry zgodnie z opisem w sekcji *Frontend*. Aby ponownie skonfigurować frontend Zabbix, otwórz w przeglądarce URL konfiguracji frontend:

- dla Apache: http://<server_ip_or_name>/zabbix/setup.php
- dla Nginx: http://<server_ip_or_name>/setup.php

Alternatywnie parametry te można ustawić w pliku konfiguracyjnym frontend (*zabbix.conf.php*):

```
$DB['VAULT']                    = 'HashiCorp';
$DB['VAULT_URL']                = 'https://localhost:8200';
$DB['VAULT_DB_PATH']            = 'database';
$DB['VAULT_TOKEN']              = '<mytoken>';
$DB['VAULT_CERT_FILE']          = '';
$DB['VAULT_KEY_FILE']           = '';
$DB['VAULT_PREFIX']             = '/v1/secret/data/zabbix/';
```

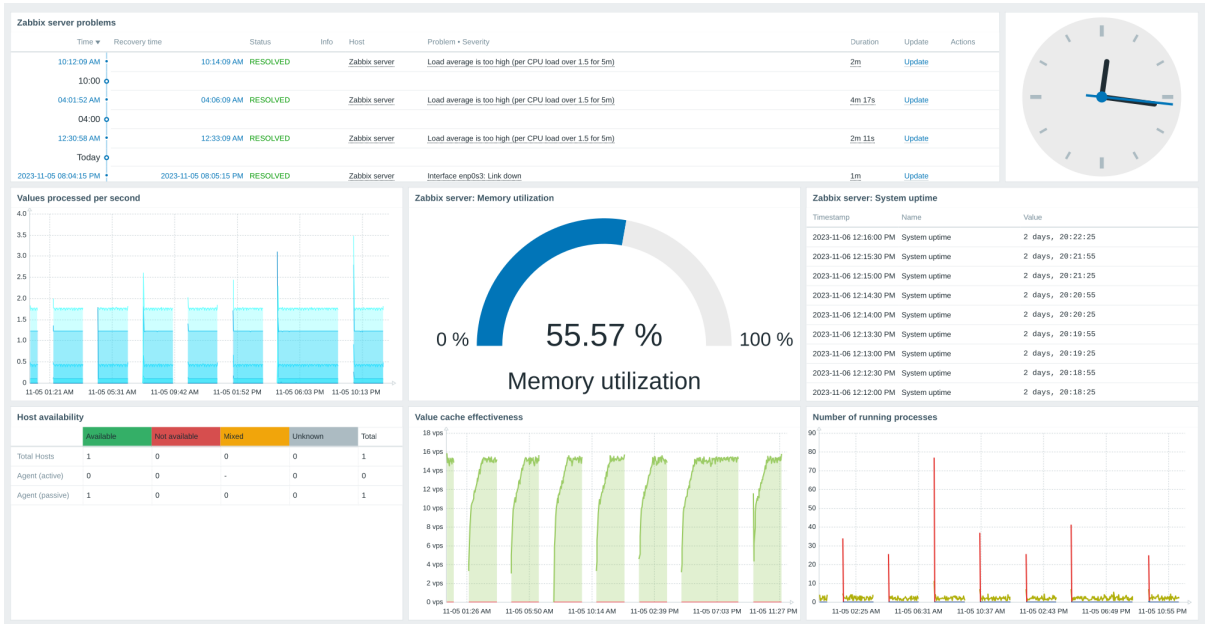
3. W razie potrzeby skonfiguruj makra użytkownika zgodnie z opisem w sekcji *Wartości makr użytkownika*.

Aby zaktualizować istniejącą konfigurację pobierania sekretów z CyberArk Vault, zobacz *Konfiguracja CyberArk*.

14 Zaplanowane raporty

Przegląd

Funkcja *Raporty cykliczne* umożliwia skonfigurowanie wysyłania wersji PDF wybranego dashboardu do określonych odbiorców w regularnych odstępach czasu.



Wymagania wstępne:

- Usługa internetowa Zabbix musi być zainstalowana i poprawnie skonfigurowana, aby umożliwić generowanie raportów cyklicznych — instrukcje znajdują się w Konfigurowanie raportów cyklicznych.
- Użytkownik musi mieć rolę użytkownika typu *Admin* lub *Super admin* z następującymi uprawnieniami:
  - *Raporty cykliczne* w sekcji *Dostęp do elementów interfejsu użytkownika* (aby wyświetlać ustawienia raportów)
  - *Zarządzanie raportami cyklicznymi* w sekcji *Dostęp do działań* (aby tworzyć/edytować raporty)

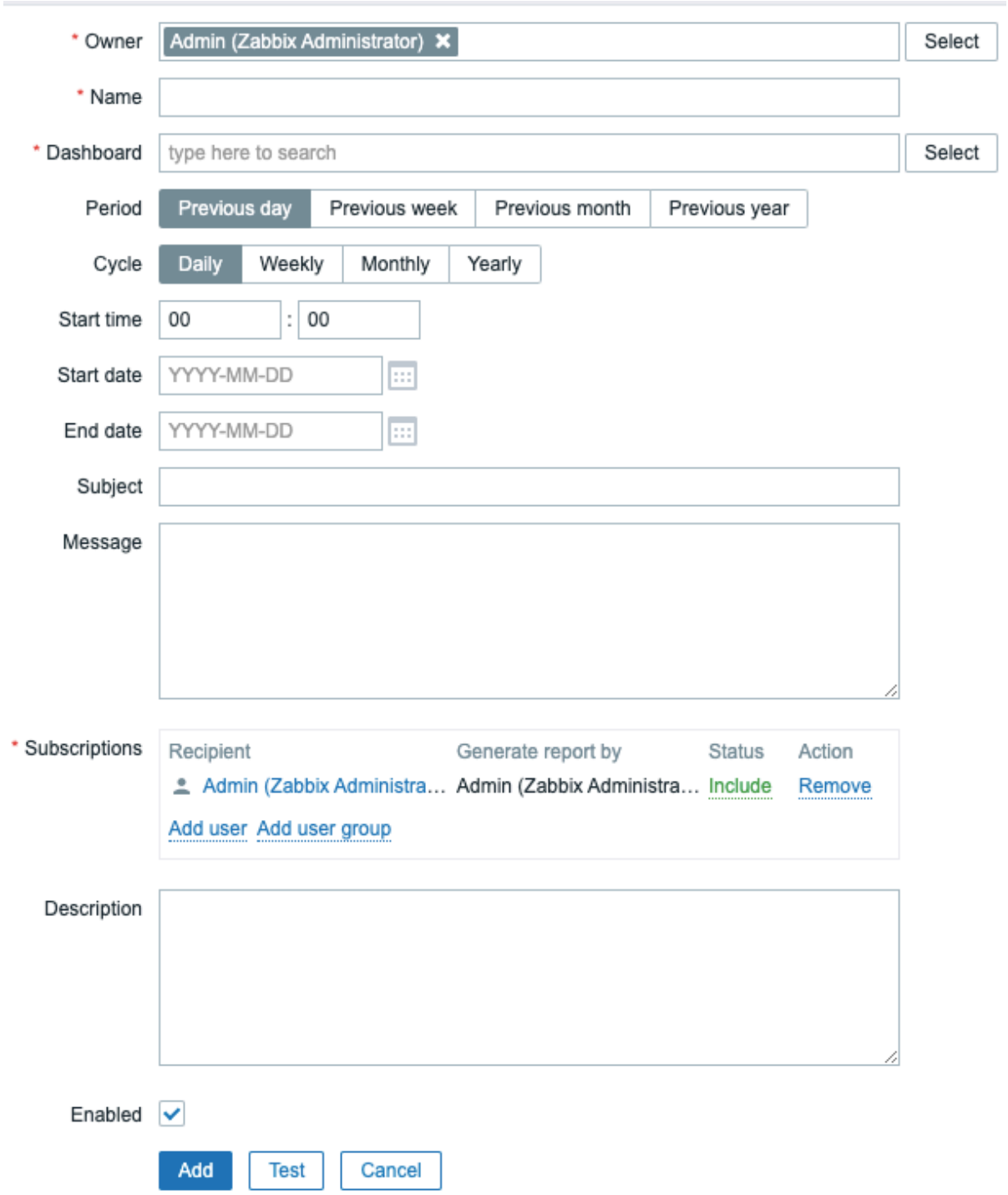
Aby utworzyć raport cykliczny w frontendzie Zabbix, wykonaj następujące czynności:

- Przejdź do: *Raporty* > *Raporty cykliczne*.
- Kliknij *Utwórz raport* w prawym górnym rogu ekranu.
- Wprowadź parametry raportu w formularzu.

Raport można również utworzyć, otwierając istniejący raport, klikając przycisk *Klonuj*, a następnie zapisując go pod inną nazwą.

Konfiguracja

Zakładka *Scheduled reports* zawiera ogólne atrybuty raportu.



Wszystkie wymagane pola wejściowe są oznaczone czerwoną gwiazdką.

Parametr	Opis
Owner	Użytkownik tworzący raport. Użytkownicy z poziomem *Super admin* mogą zmieniać właściciela. Dla użytkowników z poziomem *Admin* to pole jest tylko do odczytu.
Name	Nazwa raportu; musi być unikalna.
Dashboard	Pulpit, na podstawie którego tworzony jest raport; jednocześnie można wybrać tylko jeden pulpit. Aby wybrać pulpit, zacznij wpisywać nazwę — pojawi się lista pasujących pulpitów; przewiń w dół, aby wybrać. Alternatywnie możesz kliknąć *Select* obok pola i wybrać pulpit z wyświetlonej listy.
Period	Okres, dla którego raport zostanie przygotowany. Wybierz poprzedni dzień, tydzień, miesiąc lub rok.
Cycle	Częstotliwość generowania raportu. Raporty mogą być wysyłane codziennie, co tydzień, co miesiąc lub co rok. Tryb „Weekly” umożliwia wybór dni tygodnia, w których raport będzie wysyłany.
Start time	Pora dnia w formacie hh:mm, o której raport zostanie przygotowany. Zwróć uwagę, że zostanie użyta strefa czasowa serwera Zabbix.

Parametr	Opis
Repeat on	Dni tygodnia, w których raport będzie wysyłany. To pole jest dostępne tylko wtedy, gdy *Cycle* jest ustawione na „Weekly”.
Start date	Data rozpoczęcia regularnego generowania raportu.
End date	Data zakończenia regularnego generowania raportu.
Subject	Temat wiadomości e-mail z raportem. Obsługiwane makra: {TIME}, {TIMESTAMP}.
Message	Treść wiadomości e-mail z raportem. Obsługiwane makra: {TIME}, {TIMESTAMP}.
Subscriptions	Lista odbiorców raportu. Domyślnie zawiera tylko właściciela raportu. Jako odbiorcę raportu można wskazać dowolnego użytkownika Zabbix ze skonfigurowanym medium e-mail. Kliknij *Add user* lub *Add user group*, aby dodać kolejnych odbiorców. Kliknij nazwę użytkownika, aby edytować ustawienia: *Generate report by* — określa, czy dane raportu mają być generowane na podstawie uprawnień do pulpitu bieżącego użytkownika czy odbiorcy. *Status* — wybierz „Include”, aby wysłać raport do użytkownika, lub „Exclude”, aby zapobiec wysłaniu raportu do tego użytkownika. Co najmniej jeden użytkownik musi mieć status „Include”. Status „Exclude” może być użyty do wykluczenia określonych użytkowników z uwzględnionej grupy użytkowników. Zwróć uwagę, że użytkownicy z niewystarczającymi uprawnieniami (to znaczy użytkownicy z rolą opartą na typie użytkownika *Admin*, którzy nie są członkami tej samej grupy użytkowników co odbiorca lub właściciel raportu) zobaczą „Inaccessible user” lub „Inaccessible user group” zamiast rzeczywistych nazw w polach *Recipient* i *Generate report by*; pola *Status* i *Action* będą wyświetlane jako tylko do odczytu.
Enabled	Status raportu. Odznaczenie tego pola wyboru wyłączy raport.
Description	Opcjonalny opis raportu. Ten opis jest przeznaczony do użytku wewnętrznego i nie będzie wysyłany do odbiorców raportu.

Przyciski formularza

Przyciski na dole formularza umożliwiają wykonanie kilku operacji.

Add	Dodaj raport. Ten przycisk jest dostępny tylko dla nowych raportów.
Update	Zaktualizuj właściwości raportu.
Clone	Utwórz kolejny raport na podstawie właściwości bieżącego raportu.
Test	Sprawdź, czy konfiguracja raportu jest poprawna, wysyłając raport do bieżącego użytkownika.
Delete	Usuń raport.
Cancel	Anuluj edycję właściwości raportu.

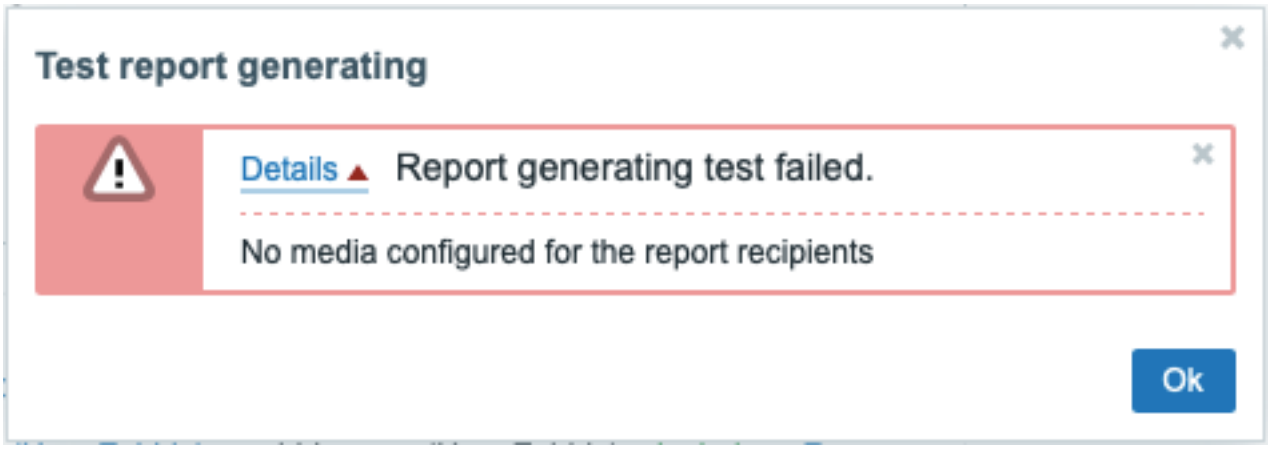
Testowanie

Aby przetestować raport, kliknij przycisk *Test* na dole formularza konfiguracji raportu.

Note:
Przycisk *Test* nie jest dostępny, jeśli formularz konfiguracji raportu został otwarty z menu działań pulpitu.

Jeśli konfiguracja jest poprawna, raport testowy jest natychmiast wysyłany do bieżącego użytkownika. W przypadku raportów testowych subskrybenci oraz ustawienia użytkownika *Generate report by* są ignorowane.

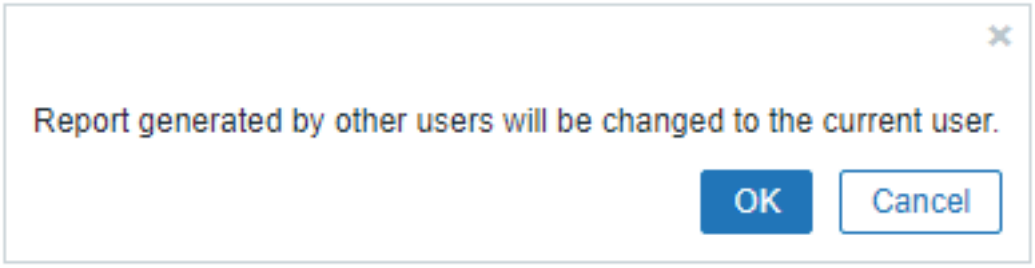
Jeśli konfiguracja jest niepoprawna, wyświetlany jest komunikat o błędzie opisujący możliwą przyczynę.



Aktualizacja raportu

Aby zaktualizować istniejący raport, kliknij nazwę raportu, wprowadź wymagane zmiany konfiguracyjne, a następnie kliknij przycisk *Update*.

Jeśli istniejący raport zostanie zaktualizowany przez innego użytkownika i ten użytkownik zmieni Dashboard, po kliknięciu przycisku *Update* zostanie wyświetlony komunikat ostrzegawczy „Raport generowany przez innych użytkowników zostanie zmieniony na bieżącego użytkownika".



Kliknięcie *OK* na tym etapie spowoduje następujące zmiany:

- Ustawienia *Generate report by* zostaną zaktualizowane tak, aby wyświetlać użytkownika, który edytował raport jako ostatni (chyba że *Generate report by* jest ustawione na odbiorcę).
- Użytkownicy wyświetlani jako „Inaccessible user" lub „Inaccessible user group" zostaną usunięci z listy subskrybentów raportu.

Kliknięcie *Cancel* spowoduje zamknięcie formularza konfiguracji i anulowanie aktualizacji raportu.

Klonowanie raportu

Aby szybko sklonować istniejący raport, kliknij przycisk *Clone* u dołu formularza konfiguracji istniejącego raportu. W przypadku klonowania raportu utworzonego przez innego użytkownika bieżący użytkownik staje się właścicielem nowego raportu.

Ustawienia raportu zostaną skopiowane do nowego formularza konfiguracji raportu z uwzględnieniem uprawnień użytkownika:

- Jeśli użytkownik klonujący raport nie ma uprawnień do pulpitu, pole *Dashboard* zostanie wyczyszczone.
- Jeśli użytkownik klonujący raport nie ma uprawnień do niektórych użytkowników lub grup użytkowników na liście *Subscriptions*, niedostępni odbiorcy nie zostaną sklonowani.
- Ustawienia *Generate report by* zostaną zaktualizowane tak, aby wyświetlać bieżącego użytkownika (chyba że w polu *Generate report by* ustawiono odbiorcę).

Zmień wymagane ustawienia i nazwę raportu, a następnie kliknij *Add*.

15 Eksport danych

Przegląd

Zabbix obsługuje eksport danych w czasie rzeczywistym na dwa sposoby:

- eksport do plików
- przesyłanie strumieniowe do systemów zewnętrznych

Można eksportować następujące encje:

- zdarzenia wyzwalaczy
- wartości pozycji
- trendy (eksport tylko do plików)

1 Eksport do plików

Przegląd

Możliwe jest skonfigurowanie eksportu w czasie rzeczywistym zdarzeń wyzwalaczy, wartości pozycji oraz trendów w formacie JSON rozdzielanym znakami nowej linii.

Eksport jest wykonywany do plików, gdzie każda linia pliku eksportu jest obiektem JSON. Mapowania wartości nie są stosowane.

W przypadku błędów (gdy danych nie można zapisać do pliku eksportu albo nie można zmienić nazwy pliku eksportu lub utworzyć nowego po zmianie jego nazwy), element danych jest odrzucany i nigdy nie jest zapisywany do pliku eksportu. Jest on zapisywany wyłącznie w bazie danych Zabbix. Zapisywanie danych do pliku eksportu jest wznawiane po rozwiązaniu problemu z zapisem.

Plik eksportu jest tworzony z uprawnieniami odczytu i zapisu tylko dla właściciela pliku. Dodatkowo plik jest dostępny do odczytu dla grupy właściciela. Wszystkie pozostałe uprawnienia są zabronione.

Aby uzyskać dokładne informacje o tym, jakie dane są eksportowane, zobacz stronę protokołu eksportu.

Należy pamiętać, że host/pozycja mogą nie mieć metadanych (grupy hostów, nazwa hosta, nazwa pozycji), jeśli host/pozycja zostały usunięte po odebraniu danych, ale przed ich wyeksportowaniem przez serwer.

Konfiguracja

Eksport w czasie rzeczywistym zdarzeń wyzwalaczy, wartości pozycji i trendów jest konfigurowany przez określenie katalogu dla plików eksportu — zobacz parametr ExportDir w konfiguracji serwera.

Dostępne są jeszcze dwa inne parametry:

- `ExportFileSize` może być użyty do ustawienia maksymalnego dopuszczalnego rozmiaru pojedynczego pliku eksportu. Gdy proces musi zapisać dane do pliku, najpierw sprawdza jego rozmiar. Jeśli przekracza on skonfigurowany limit rozmiaru, plik jest zmieniany przez dodanie do jego nazwy rozszerzenia .old, a następnie tworzony jest nowy plik z oryginalną nazwą.

> **Attention:**
> Dla każdego procesu zapisującego dane zostanie utworzony osobny plik (tj. około 4–30 plików). Ponieważ domyślny rozmiar pojedynczego pliku eksportu wynosi 1G, przechowywanie dużych plików eksportu może szybko doprowadzić do wyczerpania miejsca na dysku.

- `ExportType` pozwala określić, które typy encji (zdarzenia, historia, trendy) będą eksportowane.

2 Strumieniowanie do systemów zewnętrznych

Przegląd

Możliwe jest strumieniowanie wartości pozycji i zdarzeń z Zabbix do zewnętrznych systemów przez HTTP (zobacz szczegóły protokołu).

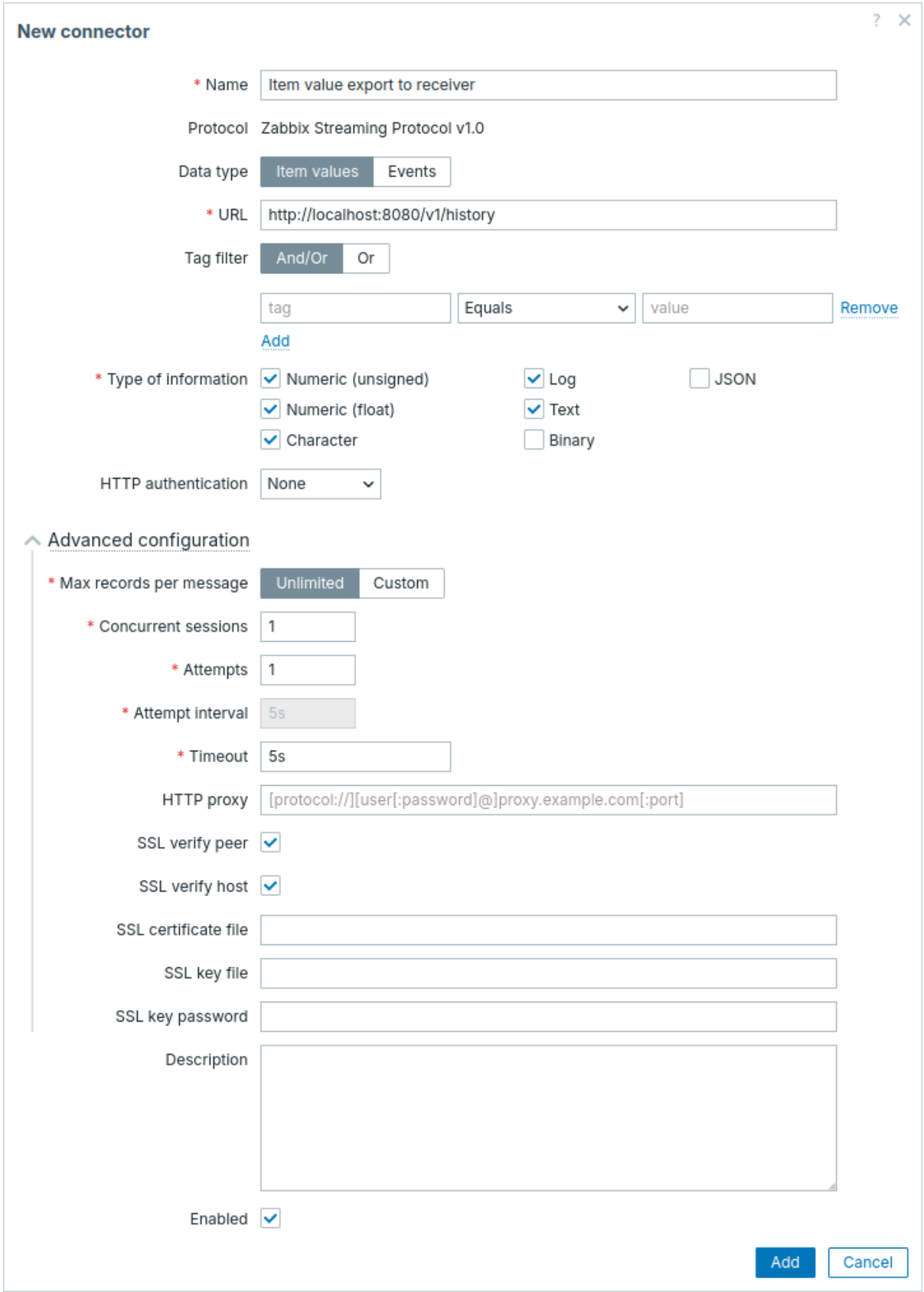
Filtr tagów może być używany do strumieniowania podzbiorów wartości pozycji lub zdarzeń.

Za strumieniowanie danych odpowiadają dwa procesy serwera Zabbix: `connector manager` i `connector worker`. Wewnętrzna pozycja Zabbix `zabbix[connector_queue]` umożliwia monitorowanie liczby wartości umieszczonych w kolejce connector.

Konfiguracja

Aby skonfigurować strumieniowanie danych do systemu zewnętrznego, wymagane są następujące kroki:

1. Należy przygotować zdalny system do odbierania danych z Zabbix. W tym celu dostępne są następujące narzędzia:
   - Przykład prostego odbiornika, który zapisuje odebrane informacje w plikach `events.ndjson` i `history.ndjson`.
   - Kafka connector for Zabbix server — lekki serwer napisany w Go, przeznaczony do przekazywania wartości pozycji i zdarzeń z serwera Zabbix do brokera Kafka.
2. Ustaw wymaganą liczbę procesów roboczych connectora w Zabbix, dostosowując parametr `StartConnectors` w pliku `zabbix_server.conf`. Liczba procesów roboczych connectora powinna odpowiadać (lub być większa, jeśli liczba współbieżnych sesji jest większa niż 1) skonfigurowanej liczbie connectorów w Zabbix frontend. Następnie uruchom ponownie serwer Zabbix.
3. Skonfiguruj nowy connector w Zabbix frontend (*Administration* > *General* > *Connectors*) i przeładuj pamięć podręczną serwera poleceniem `zabbix_server -R config_cache_reload`.



Pola obowiązkowe są oznaczone gwiazdką.

Parameter	Description
Name	Wprowadź nazwę connectora.
Data type	Wybierz typ danych do strumieniowania: **Item values** — strumieniowanie wartości pozycji z Zabbix do systemów zewnętrznych; **Events** — strumieniowanie zdarzeń z Zabbix do systemów zewnętrznych.
URL	Wprowadź URL odbiornika. Makra użytkownika są obsługiwane.

Parameter	Description
Tag filter	Eksportuj tylko wartości pozycji lub zdarzenia pasujące do filtra tagów. Jeśli nie ustawiono, eksportowane będzie wszystko. Można zarówno uwzględniać, jak i wykluczać określone tagi oraz wartości tagów. Można ustawić kilka warunków. Dopasowanie nazw tagów zawsze uwzględnia wielkość liter. Dla każdego warunku dostępnych jest kilka operatorów: **Exists** — uwzględnij określone nazwy tagów; **Equals** — uwzględnij określone nazwy i wartości tagów (z uwzględnieniem wielkości liter); **Contains** — uwzględnij określone nazwy tagów, których wartości zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter); **Does not exist** — wyklucz określone nazwy tagów; **Does not equal** — wyklucz określone nazwy i wartości tagów (z uwzględnieniem wielkości liter); **Does not contain** — wyklucz określone nazwy tagów, których wartości zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter). Dla warunków dostępne są dwa typy obliczeń: **And/Or** — wszystkie warunki muszą być spełnione, a warunki mające tę samą nazwę tagu będą grupowane operatorem Or; **Or** — wystarczy spełnienie jednego warunku.
Type of information	Wybierz typ informacji (numeric (unsigned), numeric (float), character itp.), według którego mają być filtrowane wartości pozycji strumieniowane przez connector. To pole jest dostępne, jeśli *Data type* jest ustawione na „Item values”.
HTTP authentication	Wybierz opcję uwierzytelniania: **None** — bez uwierzytelniania; **Basic** — używane jest uwierzytelnianie podstawowe; **NTLM** — używane jest uwierzytelnianie NTLM (Windows NT LAN Manager); **Kerberos** — używane jest uwierzytelnianie Kerberos (zobacz także: Configuring Kerberos with Zabbix); **Digest** — używane jest uwierzytelnianie Digest; **Bearer** — używane jest uwierzytelnianie Bearer.
Username	Wprowadź nazwę użytkownika (do 255 znaków). Makra użytkownika są obsługiwane. To pole jest dostępne, jeśli *HTTP authentication* jest ustawione na „Basic”, „NTLM”, „Kerberos” lub „Digest”.
Password	Wprowadź hasło użytkownika (do 255 znaków). Makra użytkownika są obsługiwane. To pole jest dostępne, jeśli *HTTP authentication* jest ustawione na „Basic”, „NTLM”, „Kerberos” lub „Digest”.
Bearer token	Wprowadź token Bearer. Makra użytkownika są obsługiwane. To pole jest dostępne i wymagane, jeśli *HTTP authentication* jest ustawione na „Bearer”.
Advanced configuration	Kliknij etykietę *Advanced configuration*, aby wyświetlić zaawansowane opcje konfiguracji (patrz poniżej).
Max records per message	Określ maksymalną liczbę wartości lub zdarzeń, które mogą być strumieniowane w jednej wiadomości.
Concurrent sessions	Wybierz liczbę procesów nadawczych uruchamianych dla tego connectora. Można określić do 100 sesji; wartość domyślna to „1”.
Attempts	Liczba prób strumieniowania danych. Można określić do 5 prób; wartość domyślna to „1”.
Attempt interval	Określ, jak długo connector powinien czekać po nieudanej próbie strumieniowania danych. Można określić do 10s; wartość domyślna to „5s”. To pole jest dostępne, jeśli *Attempts* jest ustawione na „2” lub więcej. Nieudane próby to takie, w których nie udało się nawiązać połączenia lub kod odpowiedzi HTTP nie wynosi 200, 201, 202, 203, 204. Ponowne próby są **wyzwalane** w przypadku błędów komunikacji lub gdy kod odpowiedzi HTTP nie wynosi 200, 201, 202, 203, 204, 400, 401, 403, 404, 405, 415, 422. Przekierowania są śledzone, więc 302 -> 200 jest odpowiedzią pozytywną; natomiast 302 -> 503 spowoduje ponowną próbę.
Timeout	Określ limit czasu wiadomości (1–60 sekund, domyślnie 5 sekund). Obsługiwane są sufiksy czasu, np. 30s, 1m. Makra użytkownika są obsługiwane.

Parameter	Description
HTTP proxy	Możesz określić HTTP proxy do użycia w następującym formacie: `[protocol://][username[:password]@]proxy.example.com[:port]` Makra użytkownika są obsługiwane. Opcjonalny prefiks `protocol://` może być użyty do określenia alternatywnych protokołów proxy (obsługa prefiksu protokołu została dodana w cURL 7.21.7). Jeśli nie określono protokołu, proxy będzie traktowane jako HTTP proxy. Domyślnie użyty zostanie port 1080. Jeśli określono *HTTP proxy*, proxy nadpisze zmienne środowiskowe związane z proxy, takie jak `http_proxy`, `HTTPS_PROXY`. Jeśli nie określono, proxy nie nadpisze zmiennych środowiskowych związanych z proxy. Wprowadzona wartość jest przekazywana bez zmian, bez sprawdzania poprawności. Możesz także wprowadzić adres proxy SOCKS. Jeśli określisz niewłaściwy protokół, połączenie nie powiedzie się, a pozycja stanie się nieobsługiwana. Należy pamiętać, że w przypadku HTTP proxy obsługiwane jest tylko proste uwierzytelnianie.
SSL verify peer	Zaznacz pole wyboru, aby weryfikować certyfikat SSL serwera WWW. Certyfikat serwera zostanie automatycznie pobrany z systemowej lokalizacji urzędu certyfikacji (CA). Możesz nadpisać lokalizację plików CA za pomocą parametru konfiguracyjnego serwera Zabbix lub proxy `SSLCALocation`.
SSL verify host	Zaznacz pole wyboru, aby zweryfikować, czy pole *Common Name* lub pole *Subject Alternate Name* certyfikatu serwera WWW jest zgodne. Ustawia to opcję cURL `CURLOPT_SSL_VERIFYHOST`.
SSL certificate file	Nazwa pliku certyfikatu SSL używanego do uwierzytelniania klienta. Plik certyfikatu musi być w formacie PEM[1]. Makra użytkownika są obsługiwane. Jeśli plik certyfikatu zawiera również klucz prywatny, pozostaw pole *SSL key file* puste. Jeśli klucz jest zaszyfrowany, podaj hasło w polu *SSL key password*. Katalog zawierający ten plik jest określany przez parametr konfiguracyjny serwera Zabbix lub proxy `SSLCertLocation`.
SSL key file	Nazwa pliku klucza prywatnego SSL używanego do uwierzytelniania klienta. Plik klucza prywatnego musi być w formacie PEM[1]. Makra użytkownika są obsługiwane. Katalog zawierający ten plik jest określany przez parametr konfiguracyjny serwera Zabbix lub proxy `SSLKeyLocation`.
SSL key password	Hasło do pliku klucza prywatnego SSL. Makra użytkownika są obsługiwane.
Description	Wprowadź opis connectora.
Enabled	Zaznacz pole wyboru, aby włączyć connector.

Gdy connector Kafka jest skonfigurowany z rozdzieloną przecinkami listą adresów brokerów bootstrap (na przykład `Kafka.URL=kafka1.exam`
klient Kafka łączy się z brokerem (brokerami), który odpowie jako pierwszy, i używa jego metadanych klastra. Jeśli lista zawiera adresy z różnych klastrów Kafka, użyty zostanie tylko klaster odpowiadający najszybciej, a pozostałe adresy zostaną zapisane w logu jako niedostępne; w rezultacie podczas uruchamiania mogą pojawić się ostrzeżenia takie jak poniższe, mimo że connector jest połączony:

```
kafka cluster connected, but broker(s) "kafka1.example.com:9093, kafka2.example.com:9093" unavailable; wil
```

W niektórych środowiskach (sieci prywatne, sieci kontenerowe lub niestandardowe konfiguracje DNS/hosts) nazwy hostów lub adresy IP mogą być rozwiązywane do adresów pętli zwrotnej (na przykład `127.0.0.1/localhost`) albo normalizowane przez klienta, co może sprawiać, że takie ostrzeżenia będą mylące. Aby ograniczyć nieporozumienia, upewnij się, że wszystkie adresy `Kafka.URL` należą do tego samego klastra Kafka, zweryfikuj rozwiązywanie DNS z hosta connectora oraz ustawienie `advertised.listeners` brokerów, a także preferuj adresy, które są rozwiązywane do adresu rozgłaszanego przez brokera.

Protokół

Komunikacja między serwerem a odbiorcą odbywa się przez HTTP z użyciem REST API, NDJSON, „Content-Type: application/x-ndjson".

Więcej informacji można znaleźć w protokole eksportu JSON rozdzielanego znakami nowej linii.

Żądanie serwera

Przykład strumieniowania wartości pozycji:

```
POST /v1/history HTTP/1.1
Host: localhost:8080
Accept: */*
```

```
Accept-Encoding: deflate, gzip, br, zstd
Content-Length: 628
Content-Type: application/x-ndjson

{"host":{"host":"Zabbix server","name":"Zabbix server"},"groups":["Zabbix servers"],"item_tags":[{"tag":"f
{"host":{"host":"Zabbix server","name":"Zabbix server"},"groups":["Zabbix servers"],"item_tags":[{"tag":"f
{"host":{"host":"Zabbix server","name":"Zabbix server"},"groups":["Zabbix servers"],"item_tags":[{"tag":"b
```

Przykład strumieniowania zdarzeń:

```
POST /v1/events HTTP/1.1
Host: localhost:8080
Accept: */*
Accept-Encoding: deflate, gzip, br, zstd
Content-Length: 333
Content-Type: application/x-ndjson

{"clock":1673454303,"ns":800155804,"value":1,"eventid":5,"name":"trigger for foo being 0","severity":0,"ho
{"clock":1673454303,"ns":832290669,"value":0,"eventid":6,"p_eventid":5}
```

Odpowiedź odbiorcy

Odpowiedź składa się z kodu statusu odpowiedzi HTTP oraz ładunku JSON. Kod statusu odpowiedzi HTTP musi mieć wartość „200”, „201”, „202”, „203” lub „204” dla żądań, które zostały obsłużone pomyślnie; inne wartości oznaczają nieudane żądania.

Przykład powodzenia:

```
localhost:8080/v1/history": HTTP/1.1 200 OK
Date: Wed, 11 Jan 2023 16:40:30 GMT
Content-Length: 0
```

Przykład z błędami:

```
localhost:8080/v1/history": HTTP/1.1 422 Unprocessable Entity
Content-Type: application/json
Date: Wed, 11 Jan 2023 17:07:36 GMT
Content-Length: 55

{"error":"invalid character '{' after top-level value"}
```

3 Brama SNMP

Przegląd

Zabbix SNMP gateway to rozszerzenie AgentX dla snmpd, obsługujące zarówno odpytywanie SNMP, jak i pułapki SNMP.

Za pomocą Zabbix SNMP gateway można używać protokołu SNMP do pobierania:

- danych wyzwalacza;
- danych wyzwalacza problemu;
- statusu grupy hostów (liczby wyzwalaczy według stanu wyzwalacza w każdej grupie)

Dane są pobierane za pomocą OID, który jest kombinacją wspólnej bazy i określonego sufiksu. Wspólna **baza** jest ustawiana w pliku konfiguracyjnym SNMP gateway, na przykład:

- `BaseOID=1.3.6.1.4.1.3043.7.55` - dla dowolnych danych wyzwalacza;
- `ProblemBaseOID=1.3.6.1.4.1.3047.7.55` - dla danych wyzwalacza problemu;
- `BaseOID=1.3.6.1.4.1.3046.7.55` - dla statusu grupy hostów.

Sufiks OID jest ustawiany w konfiguracji wyzwalaczy hosta jako **tag** (na przykład `OIDSuffix:3`) we frontend.

W takim przypadku wszystkie informacje o wyzwalaczu będą dostępne pod `OID=1.3.6.1.4.1.3043.7.55.X.3`. „X” oznacza tutaj numer pola danych wyzwalacza (tj. 1 - sufiks, 2 - ID, 3 - wyrażenie, 4 - opis itd.).

Bardziej szczegółowy opis oraz przykład pliku konfiguracyjnego można znaleźć w pliku readme SNMP gateway.

Instalacja i konfiguracja

Instrukcje dotyczące:

- instalacji i konfiguracji snmpd;
- włączania obsługi AgentX;
- konfiguracji bramy SNMP Zabbix;
- konfiguracji pułapek SNMP dla zmian stanu wyzwalacza

znajdują się w pliku readme bramy SNMP.

Pobieranie danych

Po poprawnym skonfigurowaniu wszystkiego możesz użyć poleceń `snmpwalk` i `snmpget`, aby pobrać dane:

```
[user@localhost ~]# snmpget -v2c -c public 127.0.0.1 1.3.6.1.4.1.3043.7.55.2.3
SNMPv2-SMI::enterprises.3043.7.55.2.3 = INTEGER: 15247
```

```
[user@localhost ~]# snmpwalk -v2c -c public 127.0.0.1 1.3.6.1.4.1.3043.7.55
SNMPv2-SMI::enterprises.3043.7.55.1.1 = INTEGER: 1
SNMPv2-SMI::enterprises.3043.7.55.1.3 = INTEGER: 3
SNMPv2-SMI::enterprises.3043.7.55.1.4 = INTEGER: 4
SNMPv2-SMI::enterprises.3043.7.55.1.5 = INTEGER: 5
SNMPv2-SMI::enterprises.3043.7.55.1.6 = INTEGER: 6
SNMPv2-SMI::enterprises.3043.7.55.1.10 = INTEGER: 10
SNMPv2-SMI::enterprises.3043.7.55.2.1 = INTEGER: 15367
SNMPv2-SMI::enterprises.3043.7.55.2.3 = INTEGER: 15247
SNMPv2-SMI::enterprises.3043.7.55.2.4 = INTEGER: 15365
SNMPv2-SMI::enterprises.3043.7.55.2.5 = INTEGER: 15366
SNMPv2-SMI::enterprises.3043.7.55.2.6 = INTEGER: 13493
SNMPv2-SMI::enterprises.3043.7.55.2.10 = INTEGER: 13503
...
```

Opcje filtrowania

Możesz ograniczyć informacje o problemach wyzwalaczy w konfiguracji bramy SNMP:

- według ważności (domyślnie `ProblemMinSeverity=-1`)
- przez ukrywanie potwierdzonych problemów (domyślnie `ProblemHideAck=false`)

Możesz ograniczyć liczbę problemów na grupę hostów w konfiguracji bramy SNMP:

- według wyzwalaczy w stanie nieznanym (domyślnie `CountUnknown=false`)
- według wyzwalaczy z potwierdzonymi/niepotwierdzonymi/wszystkimi problemami (domyślnie `CountAcknowledgeStatus=all`)

6 Monitorowanie usług

Przegląd Monitorowanie usług to monitorowanie na poziomie biznesowym, które może być używane do uzyskania przeglądu całego drzewa usług infrastruktury IT, identyfikowania słabych punktów infrastruktury, obliczania SLA różnych usług IT oraz sprawdzania innych informacji na wyższym poziomie. Monitorowanie usług koncentruje się na ogólnej dostępności usługi zamiast na szczegółach niskiego poziomu, takich jak brak miejsca na dysku, wysokie obciążenie procesora itp. Monitorowanie usług zapewnia również funkcjonalność umożliwiającą znalezienie głównej przyczyny problemu, jeśli usługa nie działa zgodnie z oczekiwaniami.

Monitorowanie usług umożliwia utworzenie hierarchicznej reprezentacji monitorowanych danych.

Bardzo prosta struktura usług może wyglądać następująco:

```
Usługa
|
|-Stacje robocze
| |
| |-StacjaRobocza1
| |
| |-StacjaRobocza2
|
|-Serwery
```

Każdy węzeł struktury ma atrybut status. Status jest obliczany i propagowany na wyższe poziomy zgodnie z wybranym algorytmem. Na status poszczególnych węzłów wpływa status powiązanych problemów. Mapowanie problemów jest realizowane za pomocą tagowania.

Zabbix może wysyłać powiadomienia lub automatycznie wykonywać skrypt na serwerze Zabbix w przypadku wykrycia zmiany stanu usługi. Możliwe jest zdefiniowanie elastycznych reguł określających, czy nadrzędna usługa powinna przejść do „stanu problemu" na podstawie statusów usług podrzędnych. Dane o problemach usług mogą być następnie używane do obliczania SLA i wysyłania raportów SLA na podstawie elastycznego zestawu warunków.

Monitorowanie usług jest konfigurowane w menu Usługi, które składa się z następujących sekcji:

- Usługi

Sekcja Usługi umożliwia zbudowanie hierarchii monitorowanej infrastruktury przez dodawanie usług nadrzędnych, a następnie usług podrzędnych do usług nadrzędnych.

Oprócz konfiguracji drzewa usług sekcja ta zapewnia przegląd całej infrastruktury i umożliwia szybkie zidentyfikowanie problemów, które doprowadziły do zmiany stanu usługi.

- SLA

W tej sekcji można definiować umowy SLA i ustawiać cele poziomu usług dla określonych usług.

- Raport SLA

W tej sekcji można przeglądać raporty SLA.

Akcje usług

Można również skonfigurować akcje usług.

Akcje usług są opcjonalne i umożliwiają:

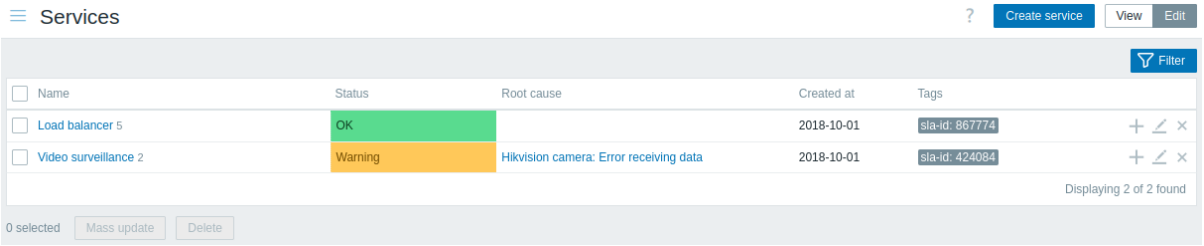
- wysłanie powiadomienia, że usługa jest niedostępna
- wykonanie zdalnego polecenia na serwerze Zabbix po zmianie stanu usługi
- wysłanie powiadomienia o odzyskaniu, gdy usługa znów jest dostępna.

Zobacz także:

- Przykład konfiguracji monitorowania SLA
- Uwagi dotyczące aktualizacji usług z wersji Zabbix wcześniejszych niż 6.0

1 Drzewo usług

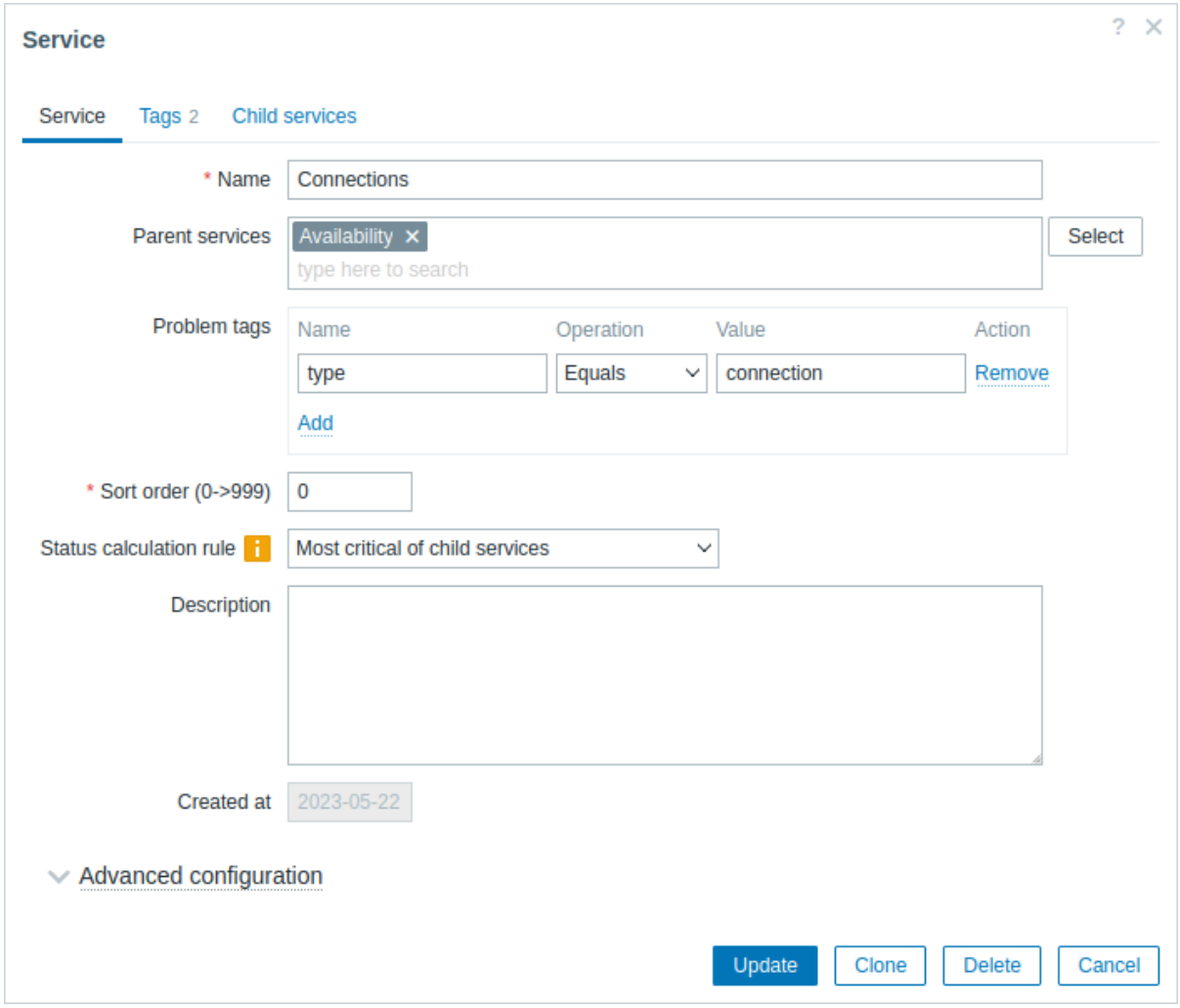
Drzewo usług konfiguruje się w sekcji menu *Usługi -> Usługi*. W prawym górnym rogu przełącz z widoku do trybu edycji.



Aby skonfigurować nową usługę, kliknij przycisk *Utwórz usługę* w prawym górnym rogu.

Aby szybko dodać usługę podrzędną, możesz alternatywnie nacisnąć ikonę plusa obok usługi nadrzędnej. Spowoduje to otwarcie tego samego formularza konfiguracji usługi, ale parametr *Usługi nadrzędne* będzie już wstępnie wypełniony.

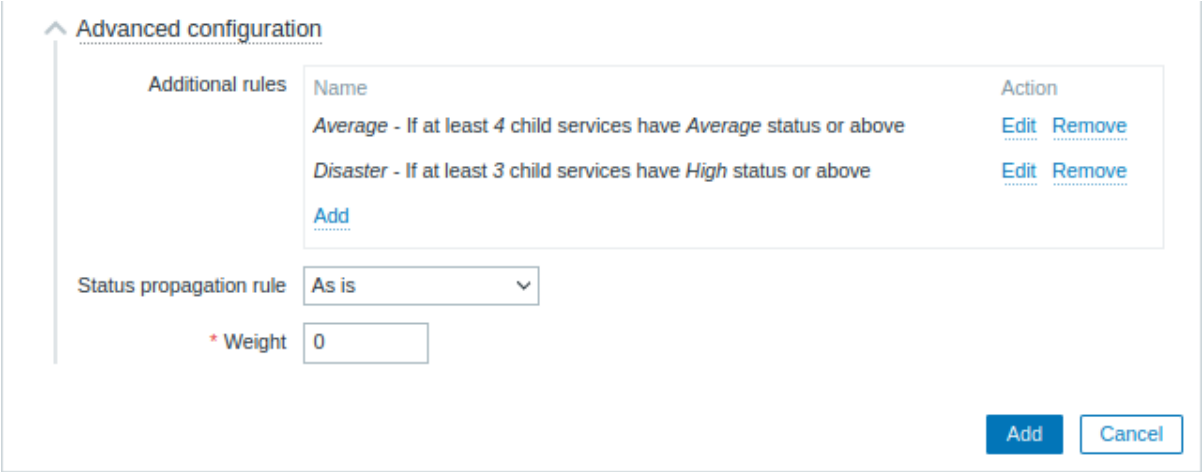
Konfiguracja usługi W zakładce **Usługa** należy określić wymagane parametry usługi:



Wszystkie obowiązkowe pola wejściowe są oznaczone czerwoną gwiazdką.

Parametr	Opis
Nazwa	Nazwa usługi.
Usługi nadrzędne	Usługi nadrzędne, do których należy usługa. Pozostaw to pole puste, jeśli dodajesz usługę najwyższego poziomu. Jedna usługa może mieć wiele usług nadrzędnych. W takim przypadku będzie ona wyświetlana w drzewie usług pod każdą z usług nadrzędnych.
Tagi problemów	Określ tagi, aby mapować dane problemów do usługi. Można ustawić kilka warunków. Dopasowanie nazw tagów zawsze uwzględnia wielkość liter. Dla każdego warunku dostępne są dwa operatory: **Equals** - uwzględnij określone nazwy i wartości tagów (z uwzględnieniem wielkości liter) **Contains** - uwzględnij określone nazwy tagów, w których wartości tagów zawierają wprowadzony ciąg znaków (dopasowanie podciągu, z uwzględnieniem wielkości liter)
Kolejność sortowania	Kolejność sortowania do wyświetlania, od najmniejszej do największej.
Reguła obliczania statusu	Reguła obliczania statusu usługi: **Most critical if all children have problems** - najbardziej krytyczny problem w usługach podrzędnych jest używany do określenia koloru statusu usługi, jeśli wszystkie usługi podrzędne mają problemy **Most critical of child services** - najbardziej krytyczny problem w usługach podrzędnych jest używany do określenia koloru statusu usługi **Set status to OK** - nie obliczaj statusu usługi Dodatkowe reguły obliczania statusu można skonfigurować w opcjach konfiguracji zaawansowanej.
Opis	Opis usługi.
Utworzono	Czas utworzenia usługi; wyświetlany podczas edycji istniejącej usługi.
Konfiguracja zaawansowana	Kliknij etykietę *Konfiguracja zaawansowana*, aby wyświetlić opcje konfiguracji zaawansowanej.

Konfiguracja zaawansowana



Parametr	Opis
Dodatkowe reguły	Kliknij *Dodaj*, aby skonfigurować dodatkowe reguły obliczania statusu.
Ustaw status na	Ustaw status usługi na *OK* (domyślnie), *Niesklasyfikowany*, *Informacja*, *Ostrzeżenie*, *Przeciętny*, *Wysoki* lub *Katastrofa* w przypadku spełnienia warunku.
Warunek	Wybierz warunek dla bezpośrednich usług podrzędnych: **jeśli co najmniej (N) usług podrzędnych ma status (Status) lub wyższy** **jeśli co najmniej (N%) usług podrzędnych ma status (Status) lub wyższy** **jeśli mniej niż (N) usług podrzędnych ma status (Status) lub niższy** **jeśli mniej niż (N%) usług podrzędnych ma status (Status) lub niższy** **jeśli waga usług podrzędnych ze statusem (Status) lub wyższym wynosi co najmniej (W)** **jeśli waga usług podrzędnych ze statusem (Status) lub wyższym wynosi co najmniej (N%)** **jeśli waga usług podrzędnych ze statusem (Status) lub niższym jest mniejsza niż (W)** **jeśli waga usług podrzędnych ze statusem (Status) lub niższym jest mniejsza niż (N%)** Jeśli określono kilka warunków i sytuacja spełnia więcej niż jeden warunek, zostanie ustawiony najwyższy poziom ważności.
N (W)	Ustaw wartość N lub W (1-100000) albo N% (1-100) w warunku.
Status	Wybierz wartość *Status* w warunku: *OK* (domyślnie), *Niesklasyfikowany*, *Informacja*, *Ostrzeżenie*, *Przeciętny*, *Wysoki* lub *Katastrofa*.
Reguła propagacji statusu	Reguła propagowania statusu usługi do usługi nadrzędnej: **Bez zmian** - status jest propagowany bez zmian **Zwiększ o** - możesz zwiększyć propagowany status o 1 do 5 poziomów ważności **Zmniejsz o** - możesz zmniejszyć propagowany status o 1 do 5 poziomów ważności **Ignoruj tę usługę** - status nie jest w ogóle propagowany do usługi nadrzędnej **Stały status** - status jest propagowany statycznie, tj. zawsze jako taki sam
Waga	Waga usługi (liczba całkowita z zakresu od 0 (domyślnie) do 1000000).

Note:
Dodatkowe reguły obliczania statusu mogą być używane wyłącznie do zwiększania poziomu ważności ponad poziom obliczony zgodnie z głównym parametrem *Reguła obliczania statusu*. Jeśli zgodnie z dodatkowymi regułami status powinien być *Ostrzeżenie*, ale zgodnie z *Reguła obliczania statusu* status to *Katastrofa* — usługa będzie miała status *Katastrofa*.

Zakładka **Tagi** zawiera tagi na poziomie usługi. Tagi na poziomie usługi są używane do identyfikacji usługi. Tagi tego typu nie są używane do mapowania problemów do usługi (w tym celu użyj *Tagi problemów* z pierwszej zakładki).

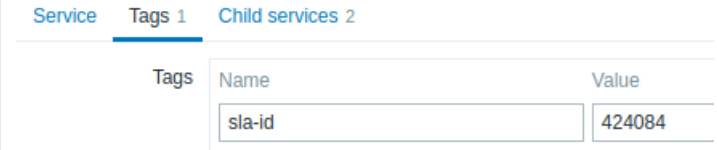
Zakładka **Usługi podrzędne** umożliwia określenie usług zależnych. Kliknij *Dodaj*, aby dodać usługę z listy istniejących usług. Jeśli chcesz dodać nową usługę podrzędną, najpierw zapisz tę usługę, a następnie kliknij ikonę plusa obok usługi, którą właśnie utworzyłeś.

Tagi W usługach istnieją dwa różne typy tagów:

- Tagi usługi
- Tagi problemu

Tagi usługi

Tagi usługi są używane do dopasowywania usług do akcji usług i SLA. Tagi te są określane na karcie konfiguracji usługi *Tagi*. Do mapowania SLA używana jest logika *OR*: usługa zostanie przypisana do SLA, jeśli ma co najmniej jeden pasujący tag. W akcjach usług reguły mapowania można konfigurować i mogą one używać logiki *AND*, *OR* lub *AND/OR*.

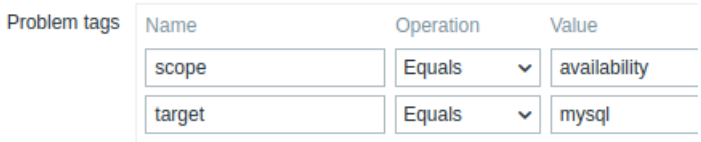


Tagi problemów

Tagi problemów są używane do dopasowywania problemów i usług. Tagi te są określane na karcie konfiguracji usługi podstawowej.

Tylko usługi podrzędne na najniższym poziomie hierarchii mogą mieć zdefiniowane tagi problemów i być bezpośrednio skorelowane z problemami. Jeśli tagi problemów są zgodne, status usługi zmieni się na taki sam status, jaki ma problem. W przypadku kilku problemów usługa będzie miała status problemu o najwyższym poziomie ważności. Status usługi nadrzędnej jest następnie obliczany na podstawie statusów usług podrzędnych zgodnie z regułami obliczania statusu.

Jeśli określono kilka tagów, stosowana jest logika *AND*: problem musi mieć wszystkie tagi określone w konfiguracji usługi, aby został przypisany do usługi.



Note:
Problem w Zabbix dziedziczy tagi z całego łańcucha szablonów, hostów, pozycji, scenariuszy WWW i wyzwalaczy. Każdy z tych tagów może zostać użyty do dopasowywania problemów do usług.

Przykład:

Problem *Kamera internetowa 3 jest niedostępna* ma tagi `type:video-surveillance`, `floor:1` i `name:webcam-3` oraz status *Ostrzeżenie*

Usługa **Kamera internetowa 3** ma określony tylko jeden tag problemu: `name:webcam-3`



Status usługi zmieni się z *OK* na *Ostrzeżenie*, gdy ten problem zostanie wykryty.

Gdyby usługa **Kamera internetowa 3** miała tagi problemu `name:webcam-3` i `floor:2`, jej status nie zostałby zmieniony po wykryciu problemu, ponieważ warunki są spełnione tylko częściowo.

Modyfikowanie istniejących usług

Note:
Przyciski opisane poniżej są widoczne tylko wtedy, gdy sekcja *Usługi* jest w trybie edycji.

Aby edytować istniejącą usługę, naciśnij ikonę ołówka obok usługi.

Aby sklonować istniejącą usługę, naciśnij ikonę ołówka, aby otworzyć jej konfigurację, a następnie naciśnij przycisk Clone. Po sklonowaniu usługi jej powiązania nadrzędne zostaną zachowane, natomiast powiązania podrzędne nie.

Aby usunąć usługę, naciśnij ikonę x obok niej. Po usunięciu usługi nadrzędnej jej usługi podrzędne nie zostaną usunięte i zostaną przeniesione o jeden poziom wyżej w drzewie usług (dzieci 1. poziomu otrzymają ten sam poziom co usunięta usługa nadrzędna).

Dwa przyciski poniżej listy usług oferują opcje edycji zbiorczej:

- *Mass update* - zbiorcza aktualizacja właściwości usług
- *Delete* - usunięcie usług

Aby skorzystać z tych opcji, zaznacz pola wyboru przy odpowiednich usługach, a następnie kliknij wymagany przycisk.

2 SLA

Przegląd Po utworzeniu usług można rozpocząć monitorowanie, czy ich wydajność jest zgodna z umową o gwarantowanym poziomie usług (SLA).

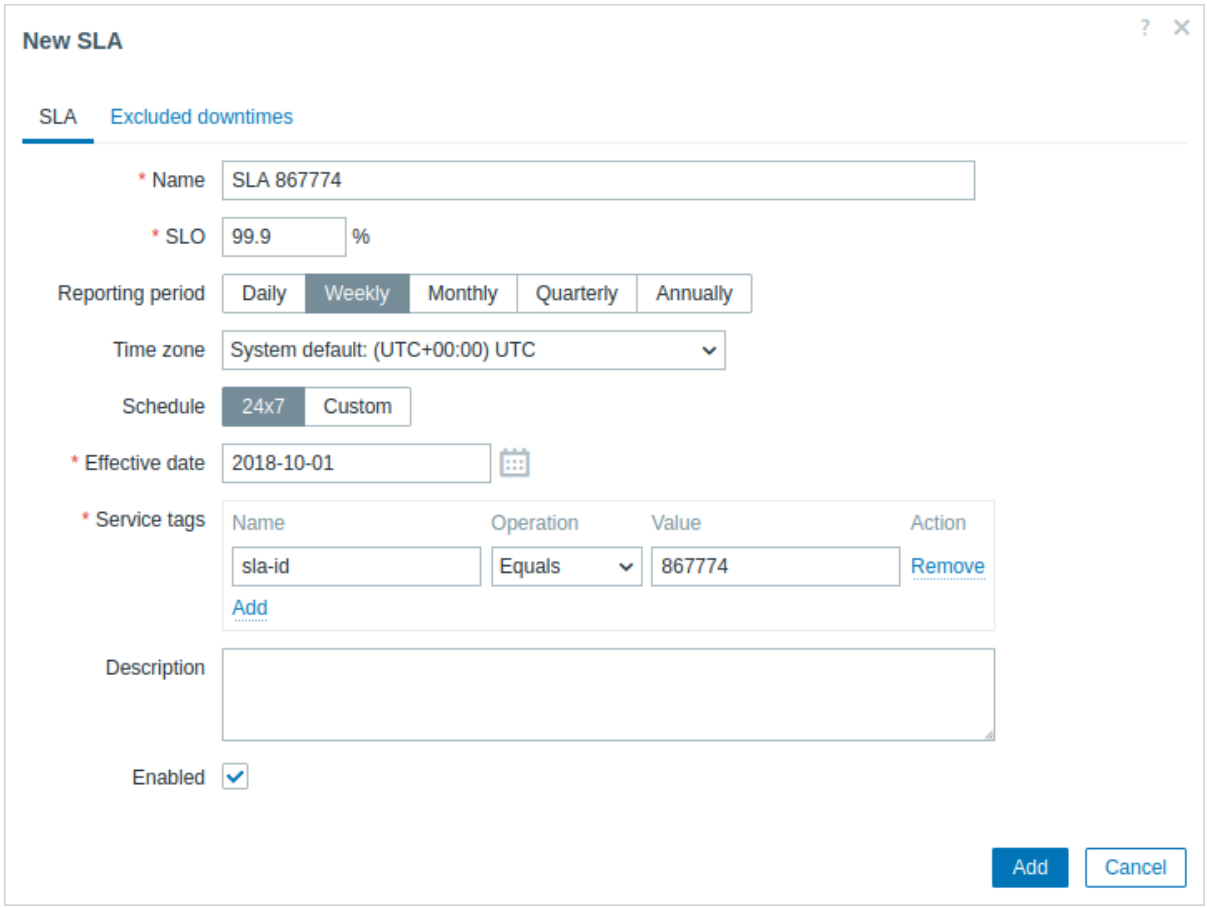
Sekcja menu *Usługi->SLA* umożliwia konfigurowanie umów SLA dla różnych usług. Umowa SLA w Zabbix definiuje cel poziomu usług (SLO), oczekiwany harmonogram dostępności oraz planowane przestoje.

Umowy SLA i usługi są dopasowywane za pomocą tagów usług. Ta sama umowa SLA może być zastosowana do wielu usług — wydajność będzie mierzona oddzielnie dla każdej pasującej usługi. Do jednej usługi może być przypisanych wiele umów SLA — dane dla każdej z nich będą wyświetlane osobno.

W raportach SLA Zabbix udostępnia dane wskaźnika poziomu usług (SLI), który mierzy rzeczywistą dostępność usługi. To, czy usługa spełnia cele SLA, jest określane przez porównanie SLO (oczekiwana dostępność w %) ze SLI (rzeczywista dostępność w %).

Konfiguracja Aby utworzyć nowe SLA, kliknij przycisk *Create SLA*.

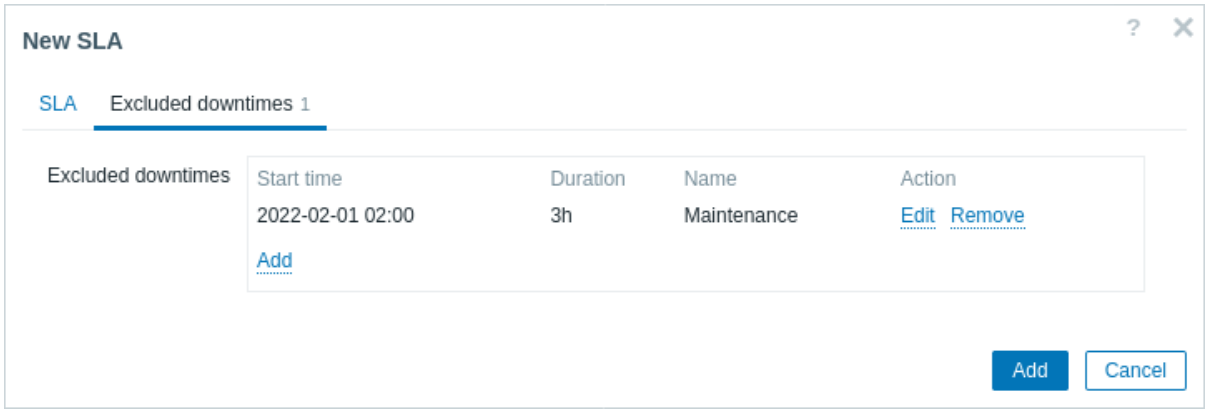
Zakładka **SLA** umożliwia określenie ogólnych parametrów SLA.



Parametr	Opis
Name	Wprowadź nazwę SLA.
SLO	Wprowadź docelowy poziom usługi (SLO) jako wartość procentową.
Reporting period	Wybierz okres raportowania SLI używany do obliczania danych SLI w raporcie SLA: **Daily** - każdy dzień, od 00:00:00 do 23:59:59. **Weekly** - każdy tydzień, od niedzieli 00:00:00 do soboty 23:59:59. **Monthly** - każdy miesiąc, od pierwszego dnia 00:00:00 do ostatniego dnia 23:59:59. **Quarterly** - każdy kwartał kalendarzowy: Q1 (sty–mar), Q2 (kwi–cze), Q3 (lip–wrz), Q4 (paź–gru). **Annually** - każdy rok kalendarzowy, od 1 stycznia 00:00:00 do 31 grudnia 23:59:59.
Time zone	Wybierz strefę czasową SLA.
Schedule	Wybierz harmonogram SLA - 24x7 lub niestandardowy.
Effective date	Wybierz datę rozpoczęcia obliczania SLA.

Parametr	Opis
Service tags	Dodaj tagi usługi, aby zidentyfikować usługi, do których to SLA ma być stosowane. **Name** - nazwa tagu usługi; musi być dokładnie zgodna, z rozróżnieniem wielkości liter. **Operation** - wybierz *Equals*, jeśli wartość tagu musi być dokładnie zgodna (z rozróżnieniem wielkości liter), lub *Contains*, jeśli ma pasować część wartości tagu (bez rozróżniania wielkości liter). **Value** - wartość tagu usługi do wyszukania zgodnie z wybraną operacją. SLA jest stosowane do usługi, jeśli pasuje co najmniej jeden tag usługi.
Description	Dodaj opis SLA.
Enabled	Zaznacz pole wyboru, aby włączyć obliczanie SLA.

Zakładka **Excluded downtimes** umożliwia określenie przestojów, które są wyłączone z obliczania SLA.



Kliknij *Add*, aby skonfigurować wykluczone przestoje, a następnie wprowadź nazwę okresu, datę rozpoczęcia i czas trwania.

Raporty SLA To, jak usługa działa w porównaniu do SLA, jest widoczne w raporcie SLA. Raporty SLA można wyświetlać:

- z sekcji *SLA*, klikając hiperłącze raportu SLA;
- z sekcji *Usługi*, klikając nazwę SLA na karcie informacji;
- w widżecie pulpitu *Raport SLA*.

Po skonfigurowaniu SLA karta *Informacje* w sekcji usług będzie również wyświetlać pewne informacje o wydajności usługi.

3 Przykład konfiguracji

Przegląd Ta sekcja opisuje prostą konfigurację monitorowania klastra wysokiej dostępności Zabbix jako usługi.

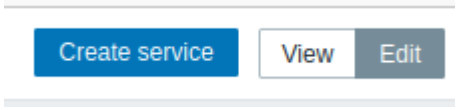
Wymagania wstępne Przed skonfigurowaniem monitorowania usług należy mieć skonfigurowane hosty:

- *Węzeł HA 1* z co najmniej jednym wyzwalaczem i tagiem (najlepiej ustawionym na poziomie wyzwalacza) `component:ha-node-1`
- *Węzeł HA 2* z co najmniej jednym wyzwalaczem i tagiem (najlepiej ustawionym na poziomie wyzwalacza) `component:ha-node-2`

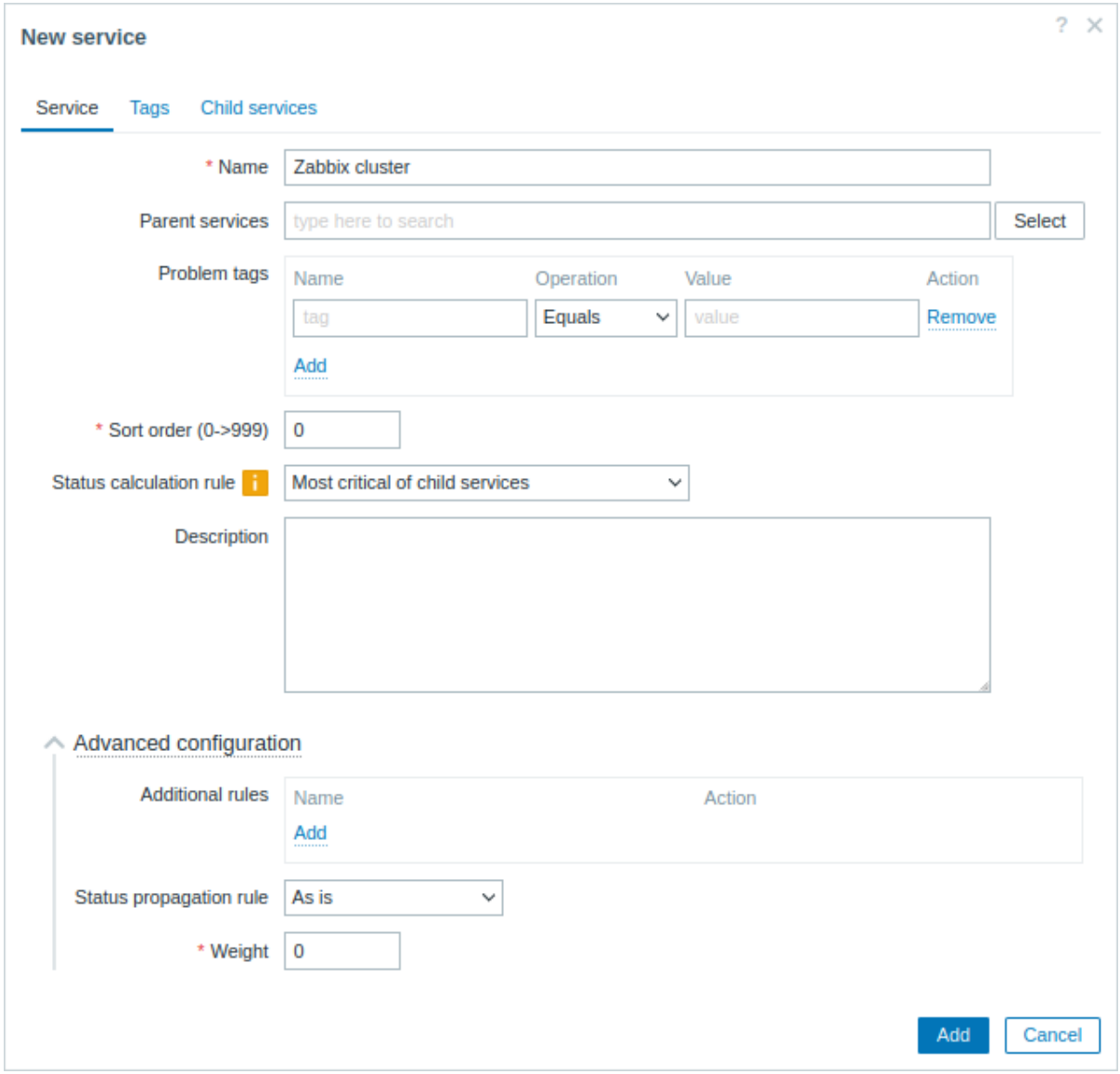
Drzewo usług Następnym krokiem jest zbudowanie drzewa usług. W tym przykładzie infrastruktura jest bardzo podstawowa i składa się z trzech usług: *Zabbix cluster* (nadrzędna) oraz dwóch usług podrzędnych *Zabbix server node 1* i *Zabbix server node 2*.

```
Zabbix cluster
|
|- Zabbix server node 1
|- Zabbix server node 2
```

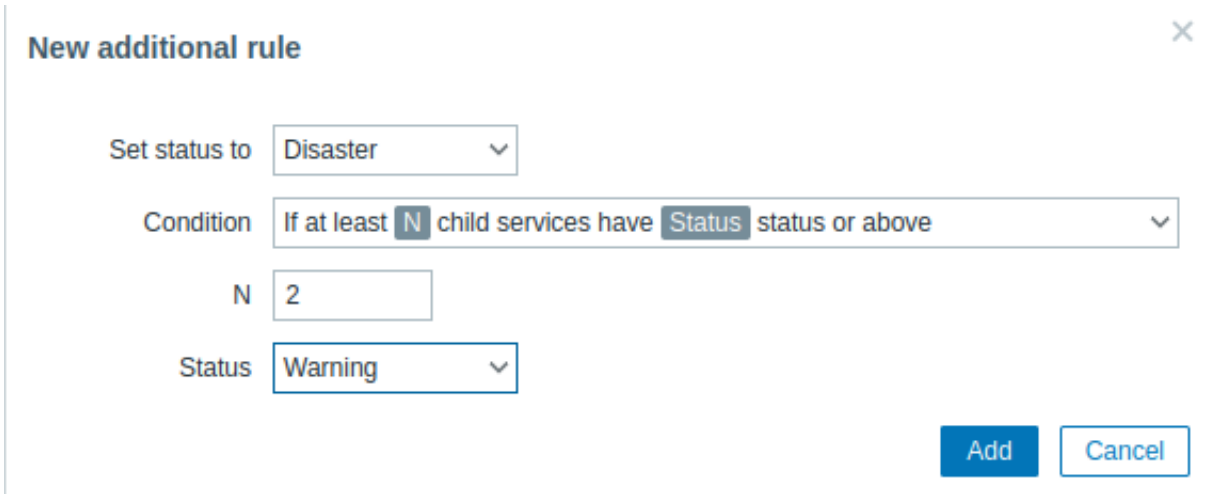
Na stronie Usługi włącz tryb *Edit* i naciśnij Create service:



W oknie konfiguracji usługi wprowadź nazwę *Zabbix cluster* i kliknij etykietę *Advanced configuration*, aby wyświetlić zaawansowane opcje konfiguracji.



Skonfiguruj dodatkową regułę:

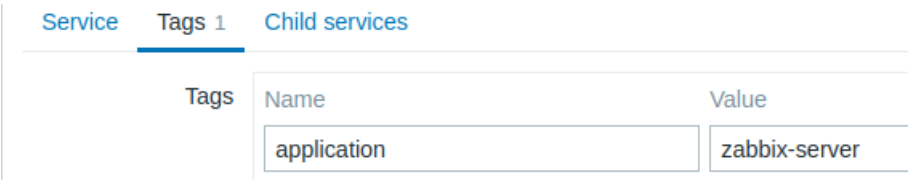


Zabbix cluster będzie mieć dwie usługi podrzędne — po jednej dla każdego z węzłów HA. Jeśli oba węzły HA mają problemy o statusie co najmniej *Warning*, status usługi nadrzędnej powinien zostać ustawiony na *Disaster*. Aby to osiągnąć, dodatkową regułę należy skonfigurować następująco:

- Set status to: Disaster
- Condition: If at least `N` child services have `Status` status or above
- N: 2
- Status: Warning

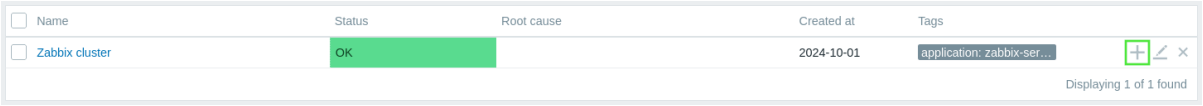
Przejdź do zakładki *Tags* i dodaj tag `application:zabbix-server`. Ten tag zostanie później użyty w akcjach usług i raportach

SLA.



Zapisz nową usługę.

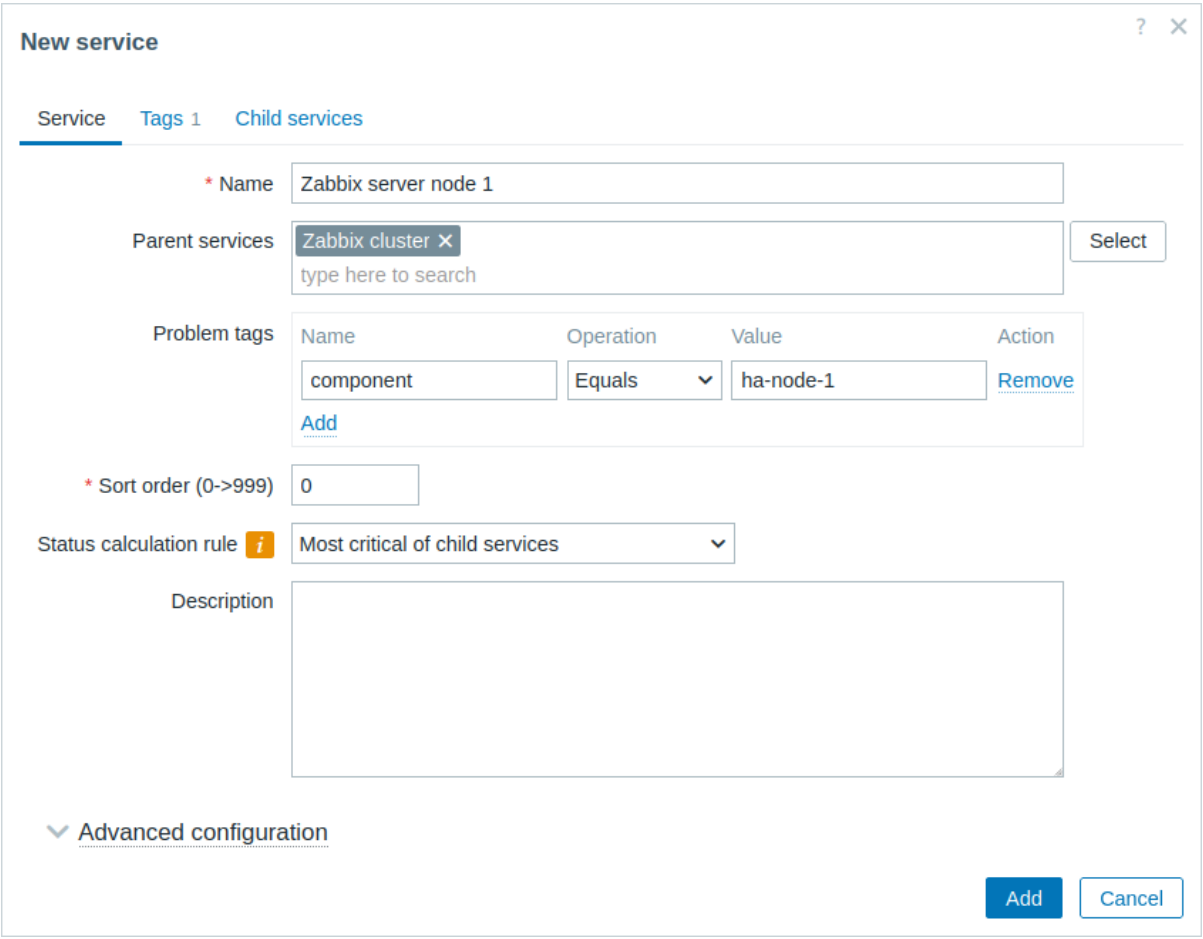
Aby dodać usługę podrzędną, naciśnij ikonę plusa obok usługi Zabbix cluster (ikona jest widoczna tylko w trybie *Edit*).



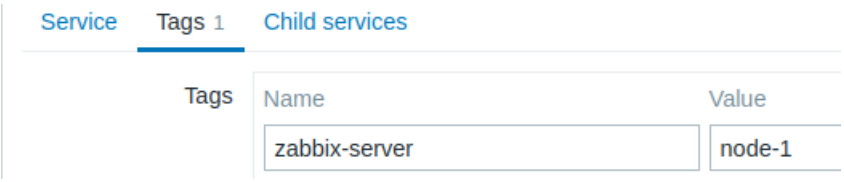
W oknie konfiguracji usługi wprowadź nazwę *Zabbix server node 1*. Zwróć uwagę, że parametr Parent services jest już wstępnie wypełniony wartością *Zabbix cluster*.

Dostępność tej usługi zależy od problemów na hoście *HA node 1*, oznaczonych tagiem problemu `component:ha-node-1`. W parametrze Problem tags wprowadź:

- Nazwa: component
- Operacja: Equals
- Wartość: ha-node-1



Przejdź do zakładki *Tags* i dodaj tag usługi: `zabbix-server:node-1`. Ten tag zostanie później użyty w akcjach usług i raportach SLA.



Zapisz nową usługę.

Utwórz kolejną usługę podrzędną klastra Zabbix o nazwie „Zabbix server node 2”.

Ustaw tagi problemów w następujący sposób:

- Nazwa: component
- Operacja: Równa się
- Wartość: ha-node-2

Przejdź do zakładki *Tagi* i dodaj tag usługi: `zabbix-server:node-2`.

Zapisz nową usługę.

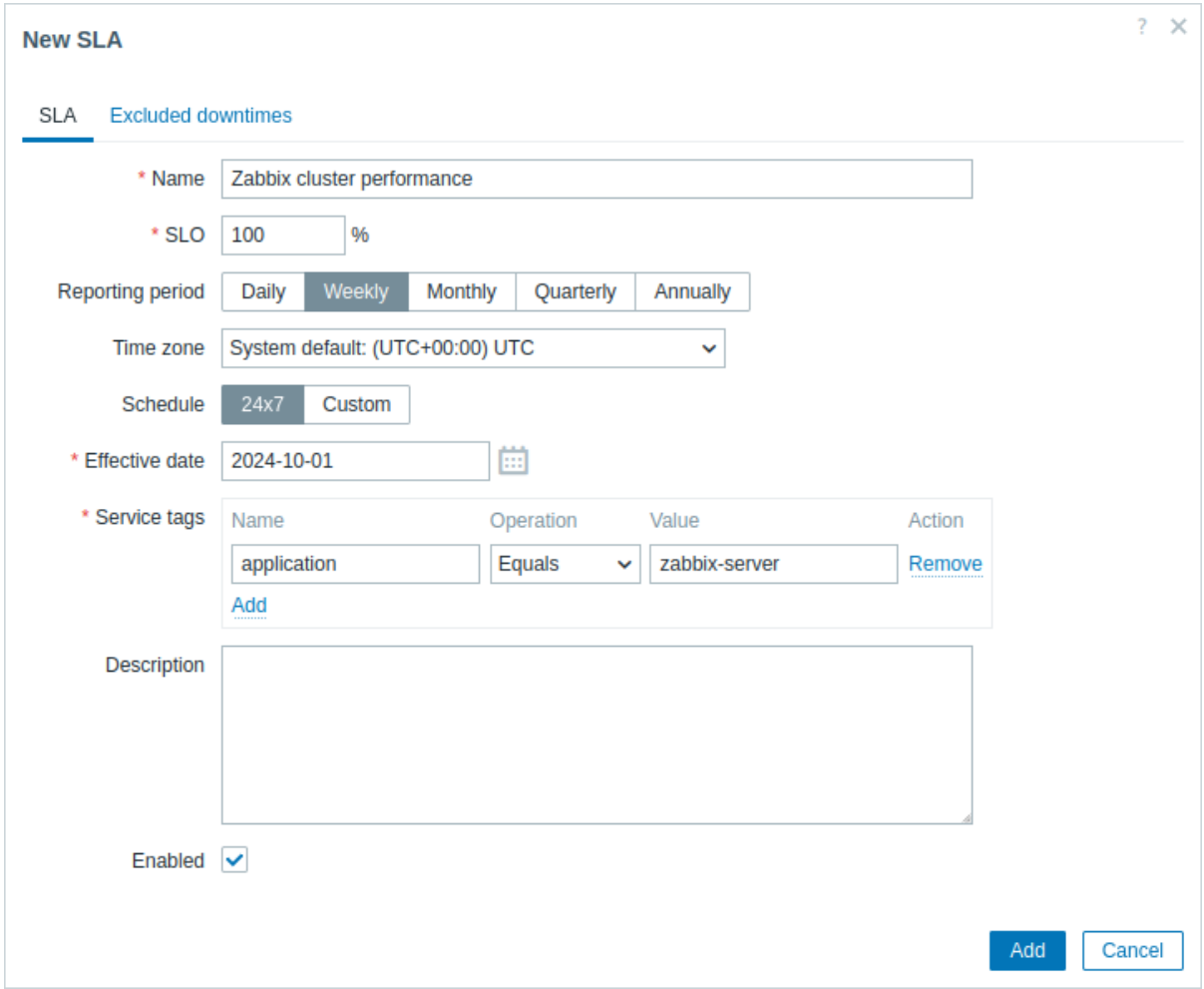
SLA W tym przykładzie oczekiwana wydajność klastra Zabbix wynosi 100%, z wyłączeniem półrocznego, jednogodzinnego okresu konserwacji.

Najpierw należy dodać nową umowę SLA.

Przejdź do sekcji menu *Services->SLA* i naciśnij Create SLA. Wprowadź nazwę *Zabbix cluster performance* i ustaw SLO na 100%.

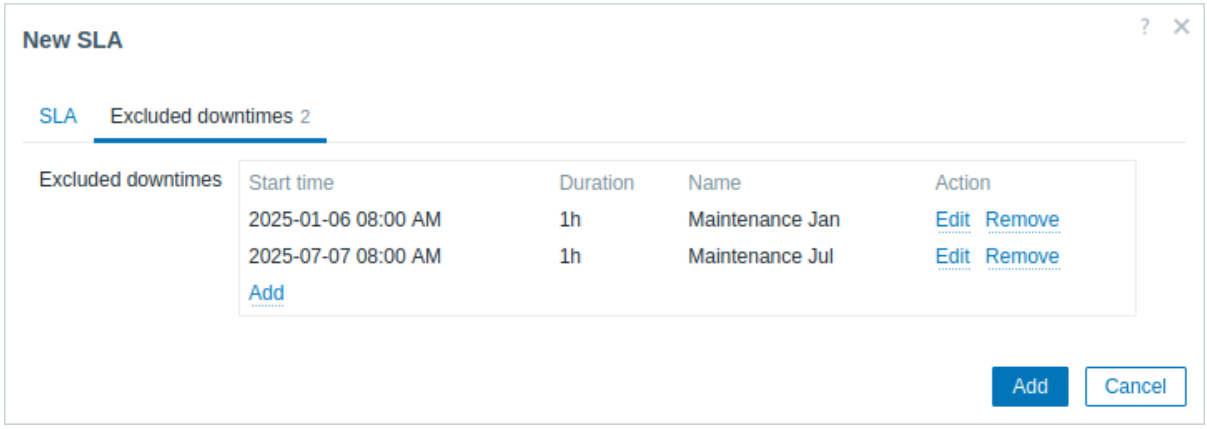
Usługa Zabbix cluster ma tag usługi `application:zabbix-server`. Aby użyć tej umowy SLA do mierzenia wydajności klastra Zabbix, w parametrze *Service tags* podaj:

- Nazwa: application
- Operacja: Equals
- Wartość: zabbix-server



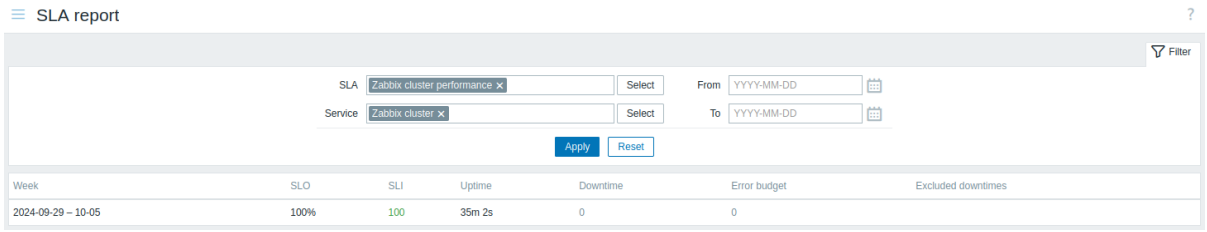
W rzeczywistej konfiguracji można również zaktualizować żądany okres raportowania, strefę czasową i datę rozpoczęcia lub zmienić harmonogram z 24/7 na niestandardowy. W tym przykładzie ustawienia domyślne są wystarczające.

Przejdź do karty *Excluded downtimes* i dodaj przestoje dla zaplanowanych okresów konserwacji, aby wykluczyć te okresy z obliczania SLA. W sekcji Excluded downtimes naciśnij odnośnik Add, wprowadź nazwę przestoju, planowany czas rozpoczęcia i czas trwania.

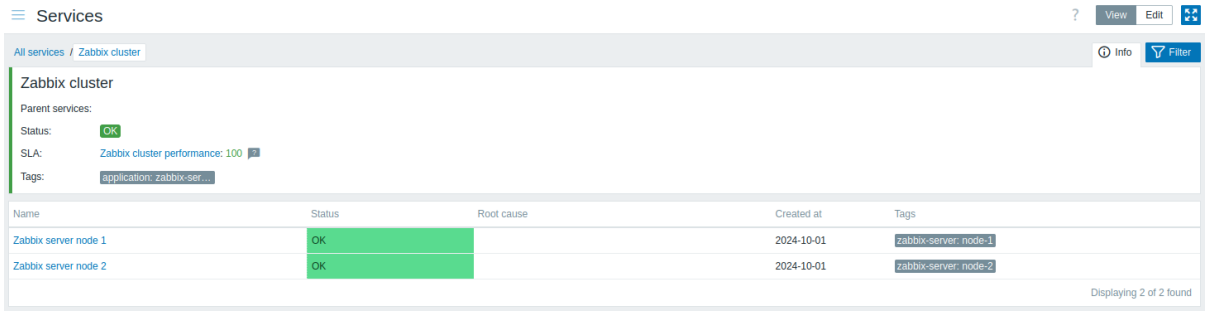


Naciśnij Add, aby zapisać nową umowę SLA.

Przejdź do sekcji raportów SLA, aby wyświetlić raport SLA dla Zabbix cluster.



Informacje o SLA można również sprawdzić w sekcji *Services*.



7 Monitorowanie WWW

Przegląd Za pomocą Zabbix można sprawdzać kilka aspektów dostępności stron internetowych.

Attention:
Aby wykonywać monitoring WWW, serwer Zabbix musi być wcześniej skonfigurowany z obsługą cURL (libcurl).

Aby włączyć monitoring WWW, należy zdefiniować scenariusze WWW. Scenariusz WWW składa się z jednego lub kilku żądań HTTP, czyli „kroków”. Kroki są okresowo wykonywane przez serwer Zabbix we wcześniej zdefiniowanej kolejności. Jeśli host jest monitorowany przez proxy, kroki są wykonywane przez proxy.

Scenariusze WWW są przypisywane do hostów/szablonów w taki sam sposób jak pozycje, wyzwalacze itd. Oznacza to, że scenariusze WWW można również tworzyć na poziomie szablonu, a następnie zastosować do wielu hostów jednocześnie.

W każdym scenariuszu WWW zbierane są następujące informacje:

- średnia prędkość pobierania na sekundę dla wszystkich kroków całego scenariusza
- numer kroku, który zakończył się niepowodzeniem
- ostatni komunikat o błędzie

W każdym kroku scenariusza WWW zbierane są następujące informacje:

- prędkość pobierania na sekundę
- czas odpowiedzi

- kod odpowiedzi

Więcej informacji można znaleźć w sekcji pozycje monitoringu WWW.

Dane zebrane podczas wykonywania scenariuszy WWW są przechowywane w bazie danych. Dane te są automatycznie wykorzystywane do tworzenia wykresów, wyzwalaczy i powiadomień.

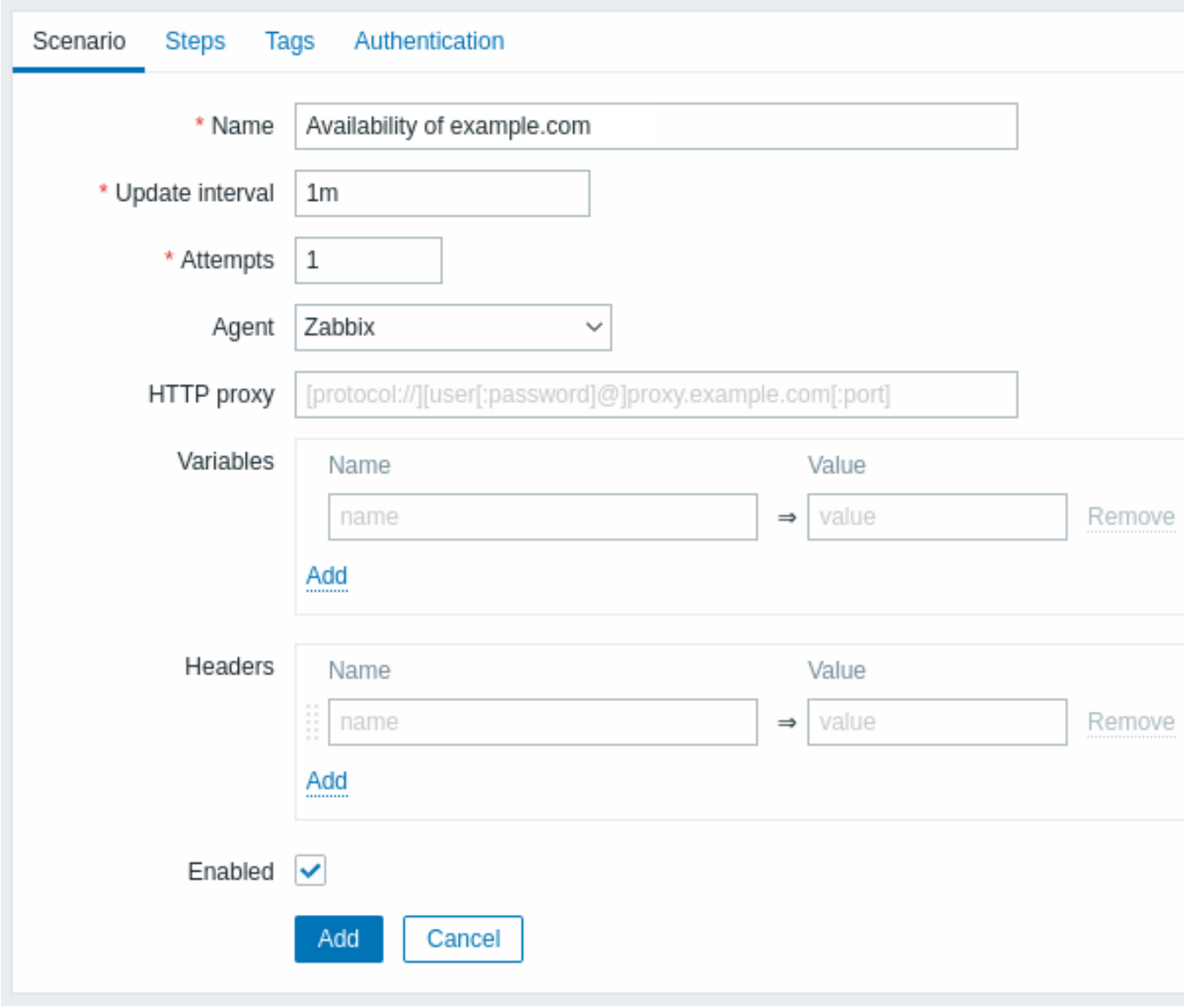
Zabbix może również sprawdzać, czy pobrana strona HTML zawiera wcześniej zdefiniowany ciąg znaków. Może wykonywać symulowane logowanie i podążać ścieżką symulowanych kliknięć myszą na stronie.

Monitoring WWW w Zabbix obsługuje zarówno HTTP, jak i HTTPS. Podczas uruchamiania scenariusza WWW Zabbix może opcjonalnie podążać za przekierowaniami (zobacz opcję *Follow redirects* poniżej). Maksymalna liczba przekierowań jest na stałe ustawiona na 10 (przy użyciu opcji cURL CURLOPT_MAXREDIRS). Wszystkie pliki cookie są zachowywane podczas wykonywania pojedynczego scenariusza.

Konfigurowanie scenariusza WWW Aby skonfigurować scenariusz WWW:

- Przejdź do: *Data collection* → *Hosts* (lub *Templates*)
- Kliknij *Web* w wierszu hosta/szablonu
- Kliknij *Create web scenario* po prawej stronie (lub nazwę scenariusza, aby edytować istniejący scenariusz)
- Wprowadź parametry scenariusza w formularzu

Zakładka **Scenario** umożliwia skonfigurowanie ogólnych parametrów scenariusza WWW.



Wszystkie wymagane pola wejściowe są oznaczone czerwoną gwiazdką.

Parametry scenariusza:

Parameter	Description
Name	Unikalna nazwa scenariusza. Obsługiwane są makra użytkownika. *Uwaga*: jeśli używane są makra użytkownika, makra te pozostaną nierozwinięte w nazwach pozycji monitorowania WWW.
Update interval	Jak często scenariusz będzie wykonywany. Obsługiwane są sufiksy czasu, np. 30s, 1m, 2h, 1d. Obsługiwane są makra użytkownika. *Uwaga*: jeśli używane jest makro użytkownika i jego wartość zostanie zmieniona (np. 5m → 30s), następne sprawdzenie zostanie wykonane zgodnie z poprzednią wartością (w przykładzie wartości — później). Nowe scenariusze WWW zostaną sprawdzone w ciągu 60 sekund od ich utworzenia.
Attempts	Liczba prób wykonania kroków scenariusza WWW. W przypadku problemów sieciowych (timeout, brak łączności itp.) Zabbix może powtórzyć wykonanie kroku kilka razy. Ustawiona wartość będzie miała jednakowy wpływ na każdy krok scenariusza. Można określić maksymalnie 10 prób, wartość domyślna to 1. *Uwaga*: Zabbix nie powtórzy kroku z powodu nieprawidłowego kodu odpowiedzi lub niedopasowania wymaganego ciągu znaków.
Agent	Wybierz agent klienta. Zabbix będzie udawał wybraną przeglądarkę. Jest to przydatne, gdy witryna zwraca różną zawartość dla różnych przeglądarek. W tym polu można używać makr użytkownika.
HTTP proxy	Możesz określić używany HTTP proxy, stosując format `[protocol://][username[:password]@]proxy.example.com[:port]`. Ustawia to opcję cURL CURLOPT_PROXY. Opcjonalny prefiks `protocol://` może być użyty do określenia alternatywnych protokołów proxy (obsługa prefiksu protokołu została dodana w cURL 7.21.7). Jeśli nie określono protokołu, proxy będzie traktowany jako HTTP proxy. Domyślnie zostanie użyty port 1080. Jeśli określono, proxy nadpisze zmienne środowiskowe związane z proxy, takie jak http_proxy, HTTPS_PROXY. Jeśli nie określono, proxy nie nadpisze zmiennych środowiskowych związanych z proxy. Wprowadzona wartość jest przekazywana „as is”, bez sprawdzania poprawności. Możesz również podać adres SOCKS proxy. Jeśli określisz nieprawidłowy protokół, połączenie nie powiedzie się, a pozycja stanie się nieobsługiwana. *Uwaga*: w przypadku HTTP proxy obsługiwane jest tylko proste uwierzytelnianie. W tym polu można używać makr użytkownika.
Variables	Zmienne, które mogą być używane w krokach scenariusza (URL, zmienne post). Mają one następujący format: **{macro1}**=value1 **{macro2}**=value2 **{macro3}**=regex:<regular expression> **{macro4}**=jsonpath:<jsonpath> **{macro5}**=xmlxpath:<xmlxpath> **{macro6}**={{macro}.function()} (zobacz funkcje makr) Na przykład: {username}=Alexei {password}=kj3h5kJ34bd {hostid}=regex:hostid is ([0-9]+) {url}=jsonpath:$.host_url {status}=xmlxpath://host/response/status {newvar}={{myvar}.btoa()} Do makr można następnie odwoływać się w krokach jako {username}, {password}, {hostid} itd. Zabbix automatycznie zastąpi je rzeczywistymi wartościami. Należy pamiętać, że zmienne z `regex:` wymagają jednego kroku do pobrania wartości wyrażenia regularnego, więc wyodrębniona wartość może zostać zastosowana dopiero w następnym kroku. Jeśli część wartości zaczyna się od `regex:`, część po niej jest traktowana jako wyrażenie regularne przeszukujące stronę WWW i, jeśli zostanie znalezione, zapisujące dopasowanie w zmiennej. Musi być obecna co najmniej jedna podgrupa, aby można było wyodrębnić dopasowaną wartość. Obsługiwane są makra użytkownika oraz makra {HOST.*}. Zmienne są automatycznie kodowane URL przy użyciu w polach zapytania lub danych formularza dla zmiennych post, ale muszą być kodowane URL ręcznie, gdy są używane w surowym post lub bezpośrednio w URL.

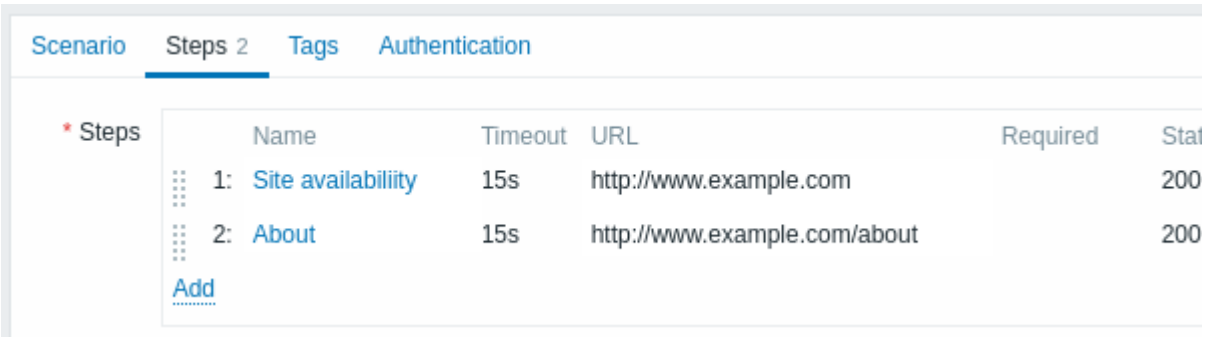
Parameter	Description
Headers	Nagłówki HTTP są używane podczas wykonywania żądania. Można używać nagłówków domyślnych i niestandardowych. Nagłówki będą przypisywane przy użyciu ustawień domyślnych zależnych od typu Agent wybranego z listy rozwijanej na poziomie scenariusza i będą stosowane do wszystkich kroków, chyba że zostaną niestandardowo zdefiniowane na poziomie kroku. **Należy pamiętać, że zdefiniowanie nagłówka na poziomie kroku automatycznie odrzuca wszystkie wcześniej zdefiniowane nagłówki, z wyjątkiem domyślnego nagłówka przypisanego przez wybranie 'User-Agent' z listy rozwijanej na poziomie scenariusza.** Jednak nawet domyślny nagłówek 'User-Agent' może zostać nadpisany przez określenie go na poziomie kroku. Aby usunąć nagłówek na poziomie scenariusza, należy podać nazwę nagłówka i przypisać mu pustą wartość na poziomie kroku. Nagłówki powinny być podawane przy użyciu tej samej składni, w jakiej występują w protokole HTTP, opcjonalnie z użyciem dodatkowych funkcji obsługiwanych przez opcję cURL CURLOPT_HTTPHEADER. Na przykład: Accept-Charset=utf-8 Accept-Language=en-US Content-Type=application/xml; charset=utf-8 Obsługiwane są makra użytkownika oraz makra {HOST.*}.
Enabled	Scenariusz jest aktywny, jeśli to pole jest zaznaczone, w przeciwnym razie — wyłączony.

Należy pamiętać, że podczas edycji istniejącego scenariusza w formularzu dostępne są dwa dodatkowe przyciski:

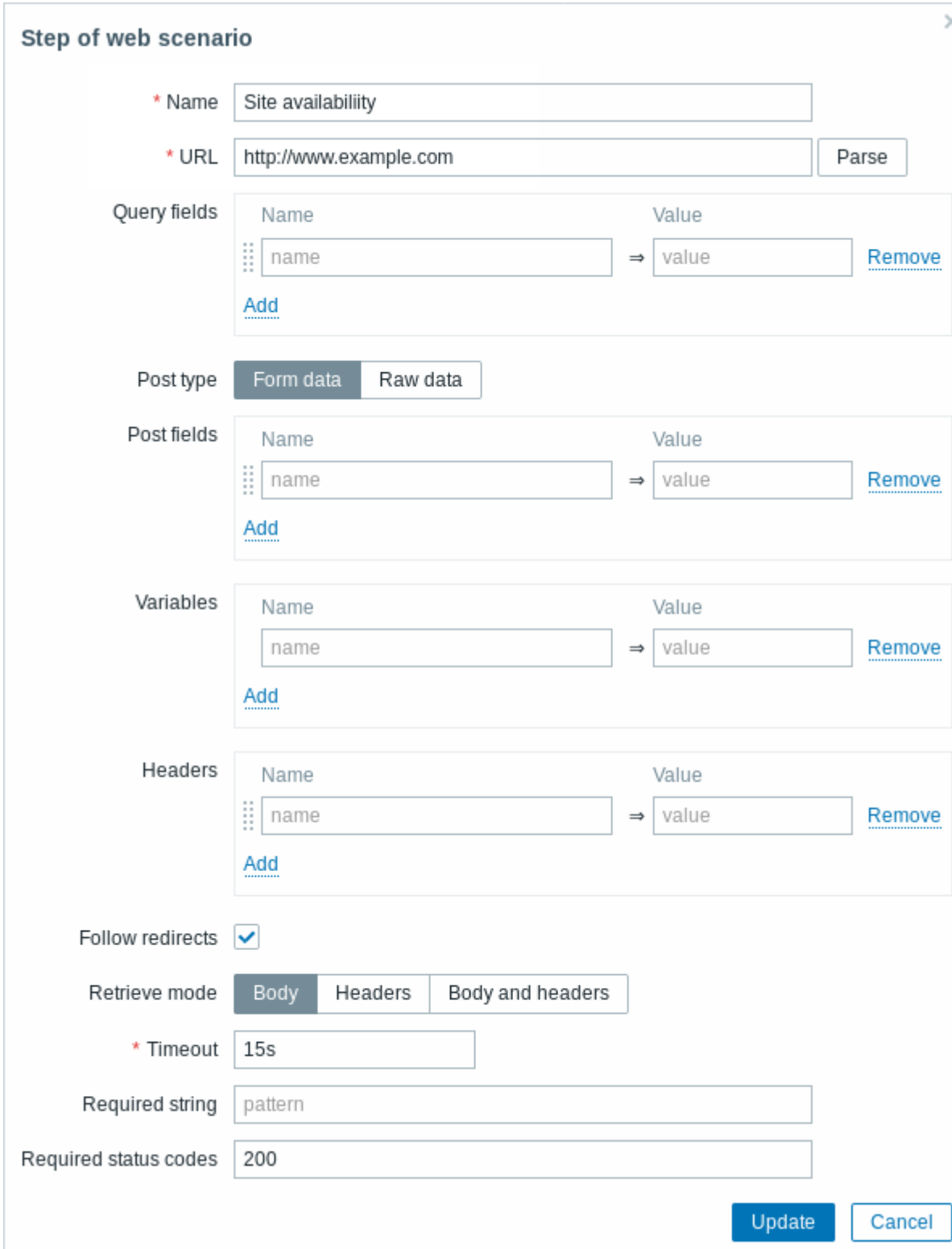
Clone	Utwórz kolejny scenariusz na podstawie właściwości istniejącego.
Clear history and trends	Usuń dane historyczne i trendy dla scenariusza. Spowoduje to, że serwer wykona scenariusz natychmiast po usunięciu danych.

Note:
Jeśli pole *HTTP proxy* pozostanie puste, innym sposobem użycia HTTP proxy jest ustawienie zmiennych środowiskowych związanych z proxy.
Dla sprawdzeń HTTP — ustaw zmienną środowiskową **http_proxy** dla użytkownika serwera Zabbix. Na przykład, `http_proxy=http://proxy_ip:proxy_port`.
Dla sprawdzeń HTTPS — ustaw zmienną środowiskową **HTTPS_PROXY**. Na przykład `HTTPS_PROXY=http://proxy_ip:proxy_port`. Więcej szczegółów jest dostępnych po uruchomieniu polecenia powłoki: *# man curl*.

Zakładka **Steps** umożliwia skonfigurowanie kroków scenariusza WWW. Aby dodać krok scenariusza WWW, kliknij *Add* w bloku *Steps*.



Note:
Tajne makra użytkownika nie mogą być używane w adresach URL, ponieważ zostaną rozwinięte do "******".



Konfigurowanie kroków

Parametry kroku:

Parametr	Opis
Nazwa	Unikalna nazwa kroku. Obsługiwane są makra użytkownika. *Uwaga*: jeśli używane są makra użytkownika, makra te pozostaną nierozwinięte w nazwach pozycji monitorowania WWW.

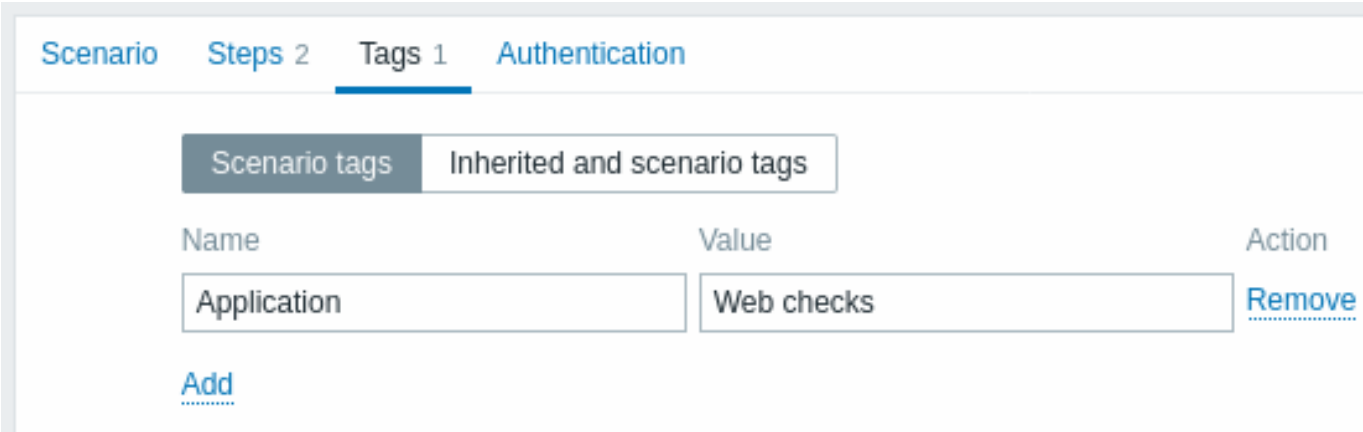
Parametr	Opis
URL	URL, z którym ma zostać nawiązane połączenie i z którego mają zostać pobrane dane. Na przykład: https://www.example.com http://www.example.com/download Nazwy domen mogą być podawane przy użyciu znaków Unicode. Podczas wykonywania kroku scenariusza WWW są one automatycznie konwertowane z punycode do ASCII. Przycisk *Parse* może zostać użyty do oddzielenia opcjonalnych pól zapytania (takich jak ?name=Admin&password=mypassword) od URL, przenosząc atrybuty i wartości do *Pól zapytania* w celu automatycznego kodowania URL. W URL można używać zmiennych, stosując składnię {macro}. Zmienne mogą być kodowane URL ręcznie przy użyciu składni {{macro}.urlencode()}. Obsługiwane są makra użytkownika oraz makra {HOST.*}. Ograniczone do 2048 znaków.
Pola zapytania	Zmienne HTTP GET dla URL. Określane jako pary atrybut-wartość. Wartości są automatycznie kodowane URL. Wartości ze zmiennych scenariusza, makr użytkownika lub makr {HOST.*} są rozwijane, a następnie automatycznie kodowane URL. Użycie składni {{macro}.urlencode()} spowoduje ich podwójne zakodowanie URL. Obsługiwane są makra użytkownika oraz makra {HOST.*}.
Post	Zmienne HTTP POST. W trybie **Form data** są określane jako pary atrybut-wartość. Wartości są automatycznie kodowane URL. Wartości ze zmiennych scenariusza, makr użytkownika lub makr {HOST.*} są rozwijane, a następnie automatycznie kodowane URL. W trybie **Raw data** atrybuty/wartości są wyświetlane w jednym wierszu i łączone symbolem **&**. Surowe wartości mogą być kodowane/dekodowane URL ręcznie przy użyciu składni {{macro}.urlencode()} lub {{macro}.urldecode()}. Na przykład: id=2345&userid={user} Jeśli {user} jest zdefiniowane jako zmienna scenariusza WWW, zostanie zastąpione swoją wartością podczas wykonywania kroku. Jeśli chcesz zakodować URL tej zmiennej, zastąp {user} przez {{user}.urlencode()}. Obsługiwane są makra użytkownika oraz makra {HOST.*}.
Zmienne	Zmienne na poziomie kroku, które mogą być używane przez funkcje GET i POST. Określane jako pary atrybut-wartość. Zmienne na poziomie kroku zastępują zmienne na poziomie scenariusza lub zmienne z poprzedniego kroku. Jednak wartość zmiennej na poziomie kroku wpływa tylko na następny krok (a nie na bieżący krok). Mają one następujący format: **{macro}**=value **{macro}**=regex:<regular expression> Więcej informacji można znaleźć w opisie zmiennych na poziomie scenariusza. Zmienne są automatycznie kodowane URL, gdy są używane w polach zapytania lub danych formularza dla zmiennych post, ale muszą być kodowane URL ręcznie, gdy są używane w surowych danych post lub bezpośrednio w URL.
Nagłówki	Niestandardowe nagłówki HTTP, które zostaną wysłane podczas wykonywania żądania. Określane jako pary atrybut-wartość. Nagłówek zdefiniowany na poziomie kroku będzie używany dla tego konkretnego kroku. **Należy pamiętać, że zdefiniowanie nagłówka na poziomie kroku automatycznie odrzuca wszystkie wcześniej zdefiniowane nagłówki, z wyjątkiem nagłówka domyślnego przypisanego przez wybranie „User-Agent” z listy rozwijanej na poziomie scenariusza.** Jednak nawet domyślny nagłówek „User-Agent” może zostać nadpisany przez określenie go na poziomie kroku. Na przykład przypisanie nazwy nagłówkowi bez ustawienia wartości spowoduje usunięcie domyślnego nagłówka na poziomie scenariusza. Obsługiwane są makra użytkownika oraz makra {HOST.*}. Ustawia to opcję cURL CURLOPT_HTTPHEADER.
Podążaj za przekierowaniami	Zaznacz pole wyboru, aby podążać za przekierowaniami HTTP. Ustawia to opcję cURL CURLOPT_FOLLOWLOCATION.
Tryb pobierania	Wybierz tryb pobierania: **Body** - pobierz tylko treść z odpowiedzi HTTP **Headers** - pobierz tylko nagłówki z odpowiedzi HTTP **Body and headers** - pobierz treść i nagłówki z odpowiedzi HTTP

Parametr	Opis
Limit czasu	Zabbix nie poświęci na przetwarzanie URL więcej czasu niż ustawiona wartość (od jednej sekundy do maksymalnie 1 godziny). W rzeczywistości parametr ten definiuje maksymalny czas na nawiązanie połączenia z URL oraz maksymalny czas wykonania żądania HTTP. Dlatego Zabbix nie poświęci na krok więcej niż **2 x Limit czasu** sekund. Obsługiwane są sufiksy czasu, np. 30s, 1m, 1h. Obsługiwane są makra użytkownika.
Wymagany ciąg	Wymagany wzorzec wyrażenia regularnego. Jeśli pobrana zawartość (HTML) nie pasuje do wymaganego wzorca, krok zakończy się niepowodzeniem. Jeśli pole jest puste, sprawdzanie wymaganego ciągu nie jest wykonywane. Na przykład: Homepage of Zabbix Welcome.*admin *Uwaga*: Odwoływanie się w tym polu do wyrażeń regularnych utworzonych w Zabbix frontend nie jest obsługiwane. Obsługiwane są makra użytkownika oraz makra {HOST.*}.
Wymagane kody statusu	Lista oczekiwanych kodów statusu HTTP. Jeśli Zabbix otrzyma kod, którego nie ma na liście, krok zakończy się niepowodzeniem. Jeśli pole jest puste, sprawdzanie kodów statusu nie jest wykonywane. Na przykład: 200,201,210-299 Obsługiwane są makra użytkownika.

Note:
Wszelkie zmiany w krokach scenariusza WWW zostaną zapisane dopiero po zapisaniu całego scenariusza.

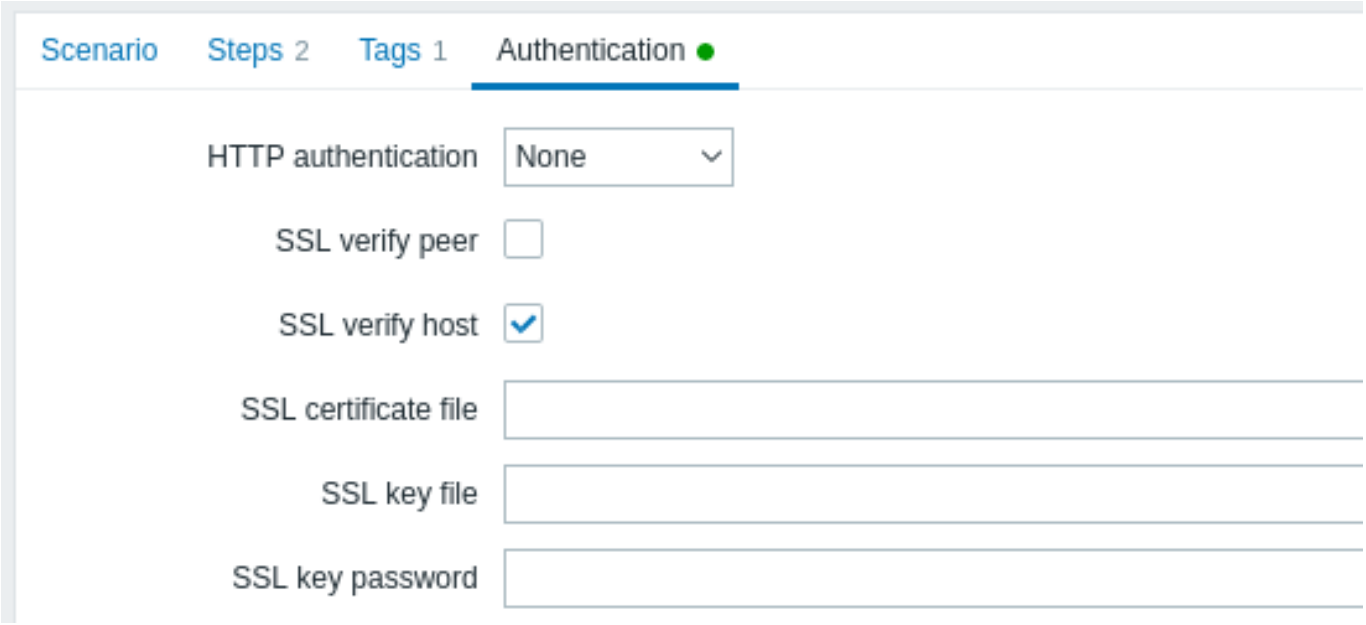
Zobacz także praktyczny przykład tego, jak można skonfigurować kroki monitorowania WWW.

Konfigurowanie tagów Zakładka **Tagi** umożliwia definiowanie tagów na poziomie scenariusza.



Tagowanie umożliwia filtrowanie scenariuszy WWW oraz pozycji monitorowania WWW.

Konfigurowanie uwierzytelniania Zakładka **Authentication** umożliwia skonfigurowanie opcji uwierzytelniania scenariusza. Zielona kropka obok nazwy zakładki wskazuje, że włączony jest jakiś typ uwierzytelniania HTTP.



Parametry uwierzytelniania:

Parameter	Description
HTTP authentication	Wybierz opcję uwierzytelniania: **None** — bez uwierzytelniania; **Basic** — używane jest uwierzytelnianie podstawowe; **NTLM** — używane jest uwierzytelnianie NTLM (Windows NT LAN Manager); **Kerberos** — używane jest uwierzytelnianie Kerberos (zobacz także: Konfigurowanie Kerberos w Zabbix); **Digest** — używane jest uwierzytelnianie Digest.
User	Wprowadź nazwę użytkownika (do 255 znaków). To pole jest dostępne, jeśli *HTTP authentication* jest ustawione na Basic, NTLM, Kerberos lub Digest. Obsługiwane są makra użytkownika.
Password	Wprowadź hasło użytkownika (do 255 znaków). To pole jest dostępne, jeśli *HTTP authentication* jest ustawione na Basic, NTLM, Kerberos lub Digest. Obsługiwane są makra użytkownika.
SSL verify peer	Zaznacz pole wyboru, aby weryfikować certyfikat SSL serwera WWW. Certyfikat serwera zostanie automatycznie pobrany z systemowej lokalizacji urzędu certyfikacji (CA). Lokalizację plików CA można nadpisać za pomocą parametru konfiguracyjnego serwera lub proxy Zabbix SSLCALocation. Ustawia to opcję cURL CURLOPT_SSL_VERIFYPEER.
SSL verify host	Zaznacz pole wyboru, aby zweryfikować, czy pole *Common Name* lub pole *Subject Alternate Name* certyfikatu serwera WWW jest zgodne. Ustawia to opcję cURL CURLOPT_SSL_VERIFYHOST.
SSL certificate file	Nazwa pliku certyfikatu SSL używanego do uwierzytelniania klienta. Plik certyfikatu musi być w formacie PEM[1]. Jeśli plik certyfikatu zawiera również klucz prywatny, pozostaw pole *SSL key file* puste. Jeśli klucz jest zaszyfrowany, podaj hasło w polu *SSL key password*. Katalog zawierający ten plik jest określony przez parametr konfiguracyjny serwera lub proxy Zabbix SSLCertLocation. W tym polu można używać makr `HOST.*` i makr użytkownika. Ustawia to opcję cURL CURLOPT_SSLCERT.
SSL key file	Nazwa pliku klucza prywatnego SSL używanego do uwierzytelniania klienta. Plik klucza prywatnego musi być w formacie PEM[1]. Katalog zawierający ten plik jest określony przez parametr konfiguracyjny serwera lub proxy Zabbix SSLKeyLocation. W tym polu można używać makr `HOST.*` i makr użytkownika. Ustawia to opcję cURL CURLOPT_SSLKEY.
SSL key password	Hasło do pliku klucza prywatnego SSL. W tym polu można używać makr użytkownika. Ustawia to opcję cURL CURLOPT_KEYPASSWD.

Attention:
[1] Zabbix obsługuje wyłącznie pliki certyfikatów i kluczy prywatnych w formacie PEM. Jeśli dane certyfikatu i klucza prywatnego są zapisane w pliku w formacie PKCS #12 (zwykle z rozszerzeniem *.p12 lub *.pfx), można wygenerować z niego plik PEM za pomocą następujących poleceń:

```
openssl pkcs12 -in ssl-cert.p12 -clcerts -nokeys -out ssl-cert.pem
openssl pkcs12 -in ssl-cert.p12 -nocerts -nodes  -out ssl-cert.key
```

Note:
Serwer Zabbix wykrywa zmiany w certyfikatach bez konieczności ponownego uruchamiania.

Note:
Jeśli certyfikat klienta i klucz prywatny znajdują się w jednym pliku, po prostu podaj go w polu ”SSL certificate file” i pozostaw pole ”SSL key file” puste. Certyfikat i klucz nadal muszą być w formacie PEM. Połączenie certyfikatu i klucza jest proste:

```
cat client.crt client.key > client.pem
```

Wyświetlanie Aby wyświetlić scenariusze WWW skonfigurowane dla hosta, przejdź do *Monitoring* → *Hosts*, odszukaj host na liście i kliknij hiperłącze *Web* w ostatniej kolumnie. Kliknij nazwę scenariusza, aby uzyskać szczegółowe informacje.



Przegląd scenariuszy WWW można również wyświetlić w *Dashboards* za pomocą widżetu monitorowania WWW.

Ostatnie wyniki wykonania scenariusza WWW są dostępne w sekcji *Monitoring* → *Latest data*.

Rozszerzone monitorowanie Czasami konieczne jest rejestrowanie otrzymanej zawartości strony HTML. Jest to szczególnie przydatne, jeśli jakiś krok scenariusza WWW zakończy się niepowodzeniem. Do tego celu służy poziom debugowania 5 (trace). Ten poziom można ustawić w plikach konfiguracyjnych serwer i proxy lub za pomocą opcji runtime control (`-R log_level_increase="http poller,N"`, gdzie N to numer procesu). Poniższe przykłady pokazują, jak można uruchomić rozszerzone monitorowanie, zakładając, że poziom debugowania 4 jest już ustawiony:

```
# Zwiększ poziom logowania wszystkich procesów http poller:
zabbix_server -R log_level_increase="http poller"

# Zwiększ poziom logowania drugiego procesu http poller:
zabbix_server -R log_level_increase="http poller,2"
```

Jeśli rozszerzone monitorowanie WWW nie jest wymagane, można je zatrzymać za pomocą opcji `-R log_level_decrease`.

1 Pozycje monitorowania WWW

Przegląd

Niektóre nowe pozycje są automatycznie dodawane do monitorowania podczas tworzenia scenariuszy WWW.

Wszystkie pozycje dziedziczą tagi ze scenariusza WWW.

Pozycje scenariusza

Gdy tylko scenariusz zostanie utworzony, Zabbix automatycznie dodaje następujące pozycje do monitorowania.

Pozycja	Opis
Prędkość pobierania dla scenariusza <Scenario>	Ta pozycja będzie zbierać informacje o prędkości pobierania (bajty na sekundę) dla całego scenariusza, tj. średnią dla wszystkich kroków. Klucz pozycji: web.test.in[Scenario„bps] Typ: *Numeric(float)*
Nieudany krok scenariusza <Scenario>	Ta pozycja będzie wyświetlać numer kroku, który zakończył się niepowodzeniem w scenariuszu. Jeśli wszystkie kroki zostaną wykonane pomyślnie, zwracane jest 0. Klucz pozycji: web.test.fail[Scenario] Typ: *Numeric(unsigned)*
Treść ostatniego komunikatu o błędzie scenariusza <Scenario>	Ta pozycja zwraca treść ostatniego komunikatu o błędzie scenariusza. Nowa wartość jest zapisywana tylko wtedy, gdy scenariusz ma nieudany krok. Jeśli wszystkie kroki są poprawne, żadna nowa wartość nie jest zbierana. Klucz pozycji: web.test.error[Scenario] Typ: *Character*

Zamiast „Scenario” zostanie użyta rzeczywista nazwa scenariusza.

Note:
Jeśli nazwa scenariusza zawiera makra użytkownika, makra te pozostaną nierozwinięte w nazwach pozycji monitorowania WWW.

 Jeśli nazwa scenariusza zaczyna się od cudzysłowu lub zawiera przecinek albo nawias kwadratowy, zostanie poprawnie ujęta w cudzysłowy w kluczach pozycji. W pozostałych przypadkach nie zostanie zastosowane dodatkowe ujmowanie w cudzysłowy.

Note:
Pozycje monitorowania WWW są dodawane z 30-dniowym okresem przechowywania historii i 90-dniowym okresem przechowywania trendów.

Te pozycje mogą być używane do tworzenia wyzwalaczy i definiowania warunków powiadomień.

Przykład 1

Aby utworzyć wyzwalacz „Web scenario failed”, możesz zdefiniować wyrażenie wyzwalacza:

`last(/host/web.test.fail[Scenario])<>0`

Pamiętaj, aby zastąpić „Scenario” rzeczywistą nazwą swojego scenariusza.

Przykład 2

Aby utworzyć wyzwalacz „Web scenario failed” z użytecznym opisem problemu w nazwie wyzwalacza, możesz zdefiniować wyzwalacz o nazwie:

`Web scenario "Scenario" failed: {ITEM.VALUE}`

oraz wyrażeniu wyzwalacza:

`length(last(/host/web.test.error[Scenario]))>0 and last(/host/web.test.fail[Scenario])>0`

Pamiętaj, aby zastąpić „Scenario” rzeczywistą nazwą scenariusza.

Przykład 3

Aby utworzyć wyzwalacz „Aplikacja web jest wolna”, możesz zdefiniować wyrażenie wyzwalacza:

`last(/host/web.test.in[Scenario,,bps])<10000`

Pamiętaj, aby zastąpić „Scenario” rzeczywistą nazwą swojego scenariusza.

Pozycje kroków scenariusza

Gdy tylko krok zostanie utworzony, Zabbix automatycznie dodaje następujące pozycje do monitorowania.

Pozycja	Opis
Prędkość pobierania dla kroku <Step> scenariusza <Scenario>	Ta pozycja będzie zbierać informacje o prędkości pobierania (bajty na sekundę) dla kroku. Klucz pozycji: web.test.in[Scenario,Step,bps] Typ: *Numeric(float)*
Czas odpowiedzi dla kroku <Step> scenariusza <Scenario>	Ta pozycja będzie zbierać informacje o czasie odpowiedzi kroku w sekundach. Czas odpowiedzi jest liczony od początku żądania do momentu przesłania wszystkich informacji. Klucz pozycji: web.test.time[Scenario,Step,resp] Typ: *Numeric(float)*
Kod odpowiedzi dla kroku <Step> scenariusza <Scenario>	Ta pozycja będzie zbierać kody odpowiedzi kroku. Klucz pozycji: web.test.rspcode[Scenario,Step] Typ: *Numeric(unsigned)*

Zamiast ”Scenario” i ”Step” zostaną użyte odpowiednio rzeczywiste nazwy scenariusza i kroku.

Note:
Pozycje monitorowania WWW są dodawane z 30-dniowym okresem przechowywania historii i 90-dniowym okresem przechowywania trendów.

Note:
Jeśli nazwa scenariusza zaczyna się od cudzysłowu lub zawiera przecinek albo nawias kwadratowy, zostanie poprawnie ujęta w cudzysłowy w kluczach pozycji. W innych przypadkach nie zostanie zastosowane dodatkowe ujmowanie w cudzysłowy.

Te pozycje mogą być używane do tworzenia wyzwalaczy i definiowania warunków powiadomień. Na przykład, aby utworzyć wyzwalacz ”Logowanie do GUI Zabbix jest zbyt wolne”, można zdefiniować wyrażenie wyzwalacza:

`last(/zabbix/web.test.time[ZABBIX GUI,Login,resp])>3`

2 Scenariusz z życia wzięty

Przegląd

Ta sekcja przedstawia krok po kroku rzeczywisty przykład użycia monitorowania WWW.

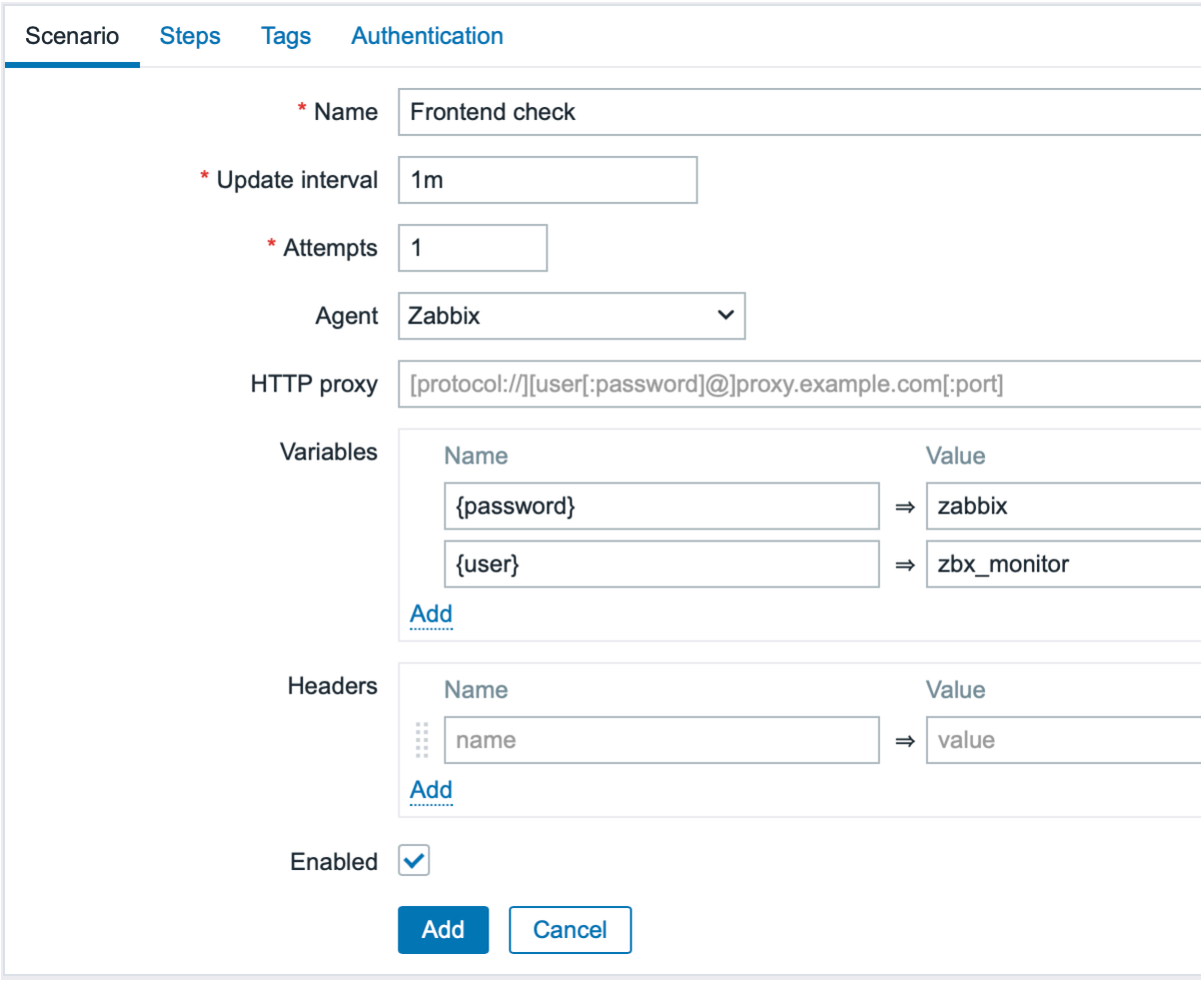
Monitorowanie WWW w Zabbix zostanie użyte do monitorowania frontend Zabbix. Celem jest określenie, czy jest on dostępny, dostarcza właściwą treść oraz jak szybko działa. Aby to osiągnąć, wymaganych jest kilka kroków, w tym sprawdzenie dostępności

pierwszej strony, zalogowanie się przy użyciu nazwy użytkownika i hasła, zweryfikowanie poprawności logowania, wylogowanie się oraz potwierdzenie wylogowania.

Scenariusz

Dodawanie nowego scenariusza WWW

Przejdź do *Zbieranie danych* → *Hosty*, wybierz host i kliknij *WWW* w wierszu tego hosta.
Następnie kliknij *Utwórz scenariusz WWW*.



W formularzu nowego scenariusza uzupełnij następujące pola:

- **Nazwa** - Frontend check
- **Interwał aktualizacji** - 1m
- **Próby** - 1
- **Agent** - Zabbix

W sekcji *Zmienne* dodaj dwie zmienne: *{password}* oraz *{user}*.
Jako wartości wprowadź dane logowania istniejącego użytkownika Zabbix.

Ze względów bezpieczeństwa zaleca się utworzenie osobnego użytkownika z minimalnymi uprawnieniami, który będzie używany do celów monitorowania.

Opcjonalnie przejdź do zakładki *Tagi* i dodaj tagi scenariusza WWW.

Note:
Po pełnej konfiguracji ten scenariusz WWW automatycznie doda do hosta pozycja typu Zabbix trapper.
Możesz używać tagów scenariusza WWW do szybkiej identyfikacji powiązanych pozycji i wyzwalaczy lub do przeszukiwania zebranych danych.
Na przykład odpowiednimi tagami dla tego samouczka są `component: web-scenario` i/lub `target: frontend`.

Konfiguracja kroków scenariusza web

Przejdź do zakładki *Steps* i zdefiniuj kroki dla scenariusza. Kliknij przycisk *Add*, aby dodać pojedynczy krok.

Wspólne pola

Dla każdego kroku opisanego poniżej wypełnij następujące pola oprócz pól specyficznych dla danego kroku:

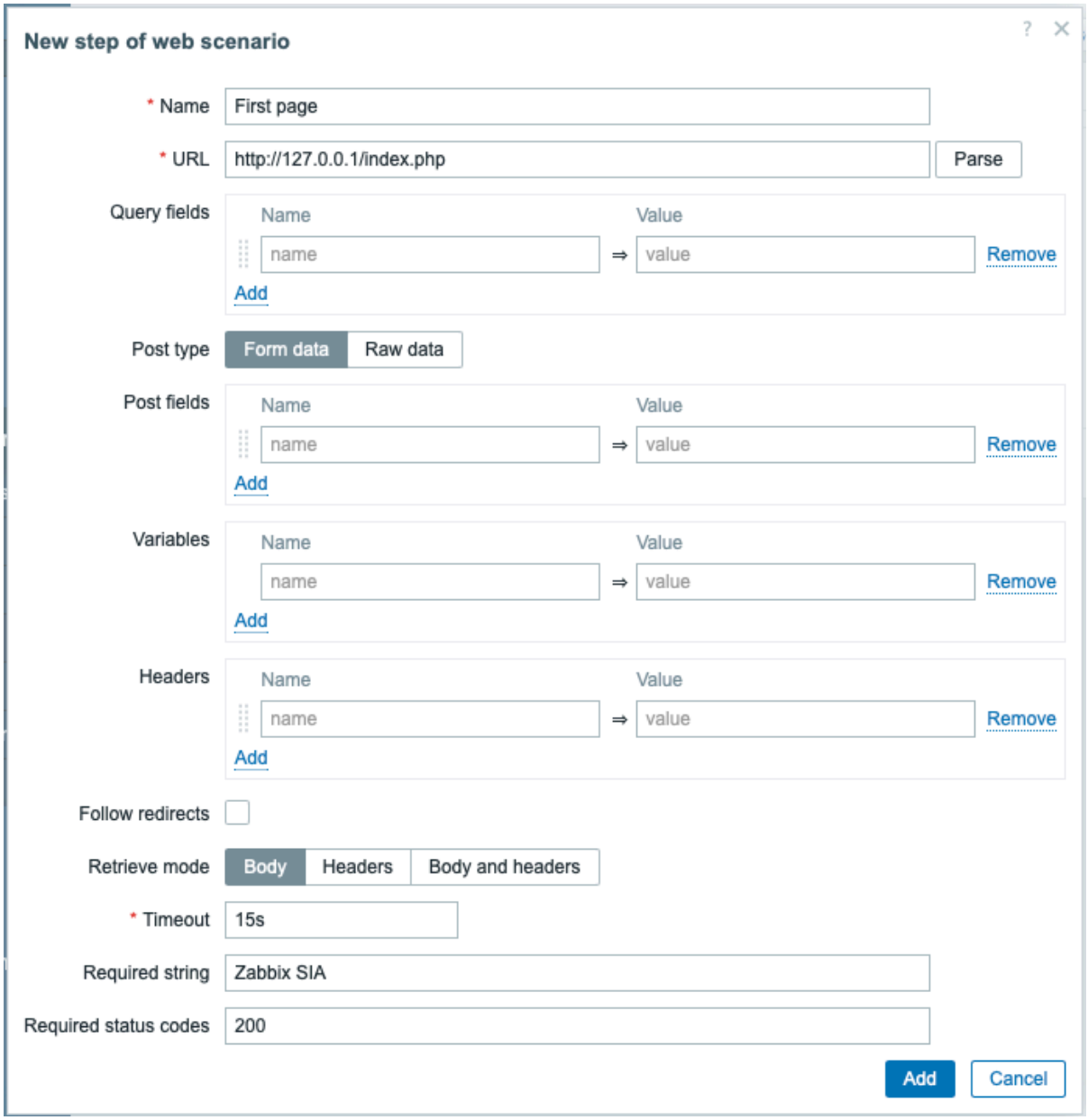
- **URL** - adres URL frontend Zabbix
- **Timeout** - 15s
- **Required status codes** - 200

Krok 1 scenariusza WWW

Sprawdź, czy pierwsza strona odpowiada poprawnie, zwraca kod odpowiedzi HTTP 200 i zawiera tekst „Zabbix SIA”.

- W polu **Nazwa** wpisz *Pierwsza strona*.
- W polu **Wymagany ciąg** wpisz *Zabbix SIA*.
- Wypełnij wspólne pola.

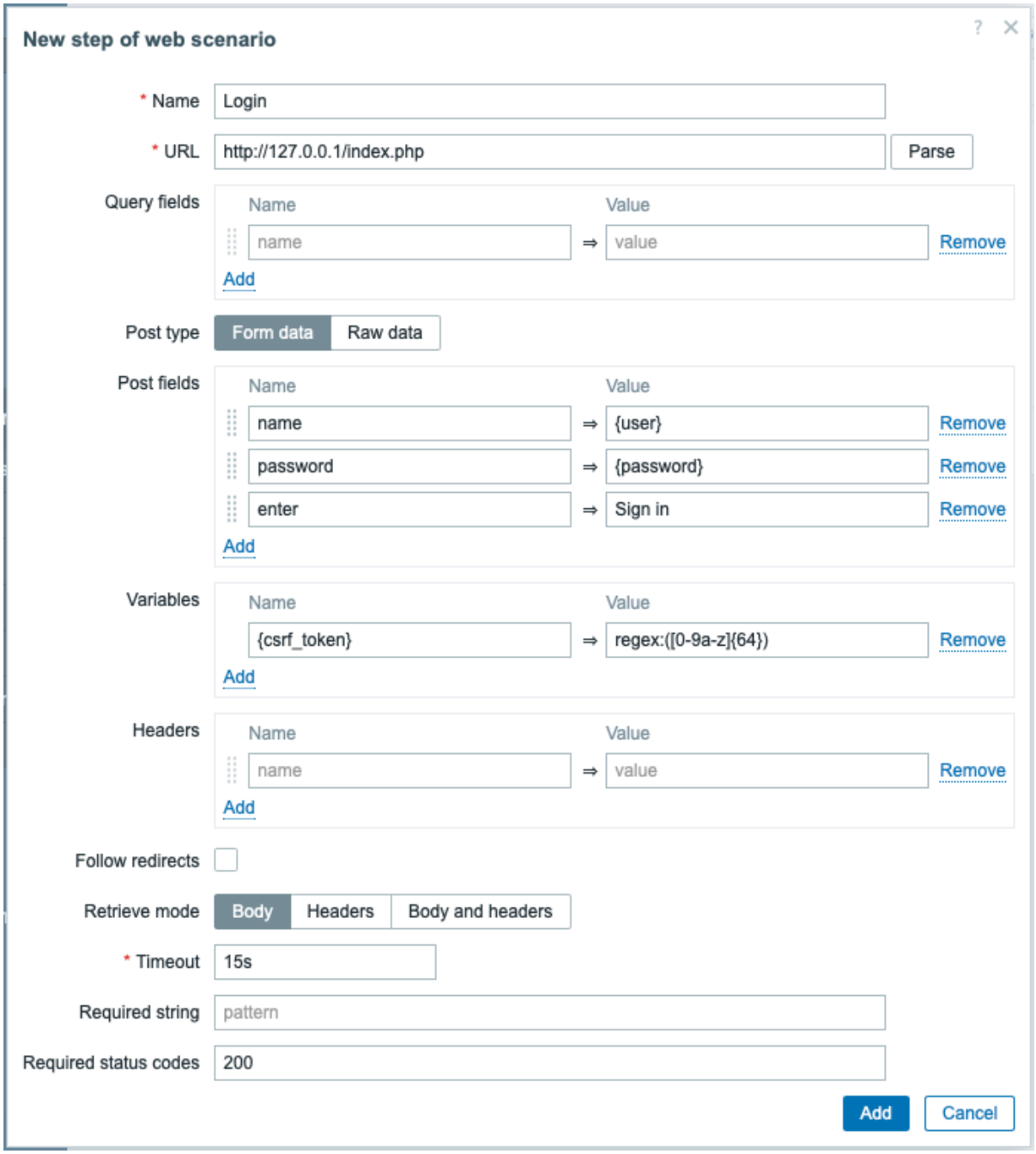
Po zakończeniu konfiguracji kroku naciśnij przycisk *Dodaj*.



Krok 2 scenariusza WWW

Zaloguj się do frontend Zabbix, używając makr (zmiennych) zdefiniowanych na poziomie scenariusza - *{user}* i *{password}*.

- W polu **Name** wpisz *Login*.
- W sekcji **Post fields** dodaj trzy pola post:
  - *name* z wartością *{user}*
  - *password* z wartością *{password}*
  - *enter* z wartością *Sign in*
- W sekcji **Variables** dodaj nową zmienną *{csrf_token}* z wartością *regex:([0-9a-z]{64})*. Ta zmienna przechwyci wartość przypisanego tokena CSRF, aby użyć jej ponownie w kroku 4.
- Uzupełnij wspólne pola.

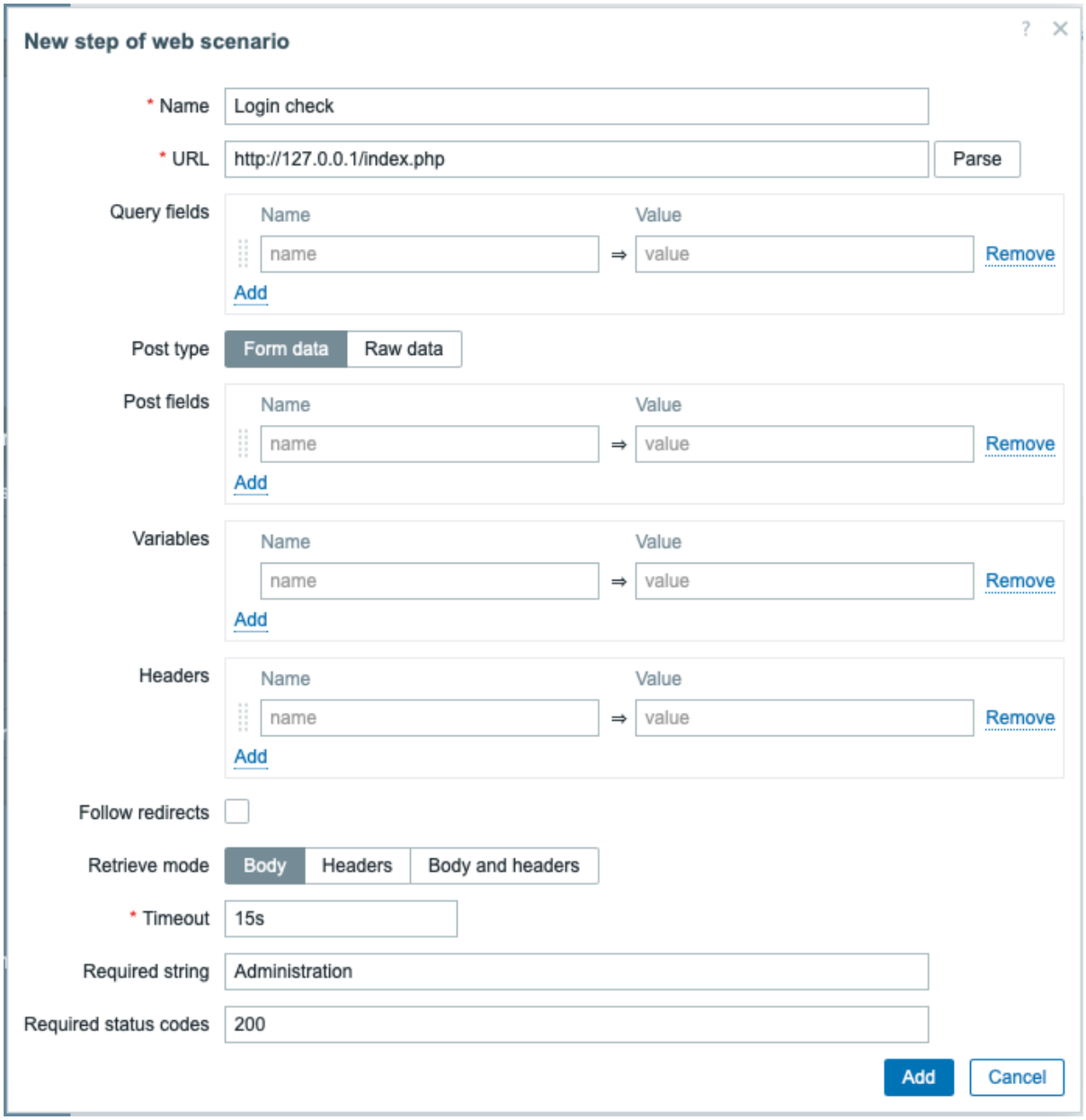


Attention:
Zwróć uwagę, że frontend Zabbix używa przekierowania JavaScript podczas logowania, dlatego logowanie musi nastąpić najpierw, a funkcje dostępne po zalogowaniu można sprawdzać dopiero w kolejnych krokach. Dodatkowo krok logowania musi używać pełnego adresu URL do pliku **index.php**.

Krok 3 scenariusza WWW

Po zalogowaniu zweryfikuj powodzenie, sprawdzając obecność ciągu znaków widocznego tylko po zalogowaniu — na przykład *Administration*.

- W polu **Nazwa** wprowadź *Login check*.
- W polu **Wymagany ciąg znaków** wprowadź *Administration*.
- Wypełnij wspólne pola.

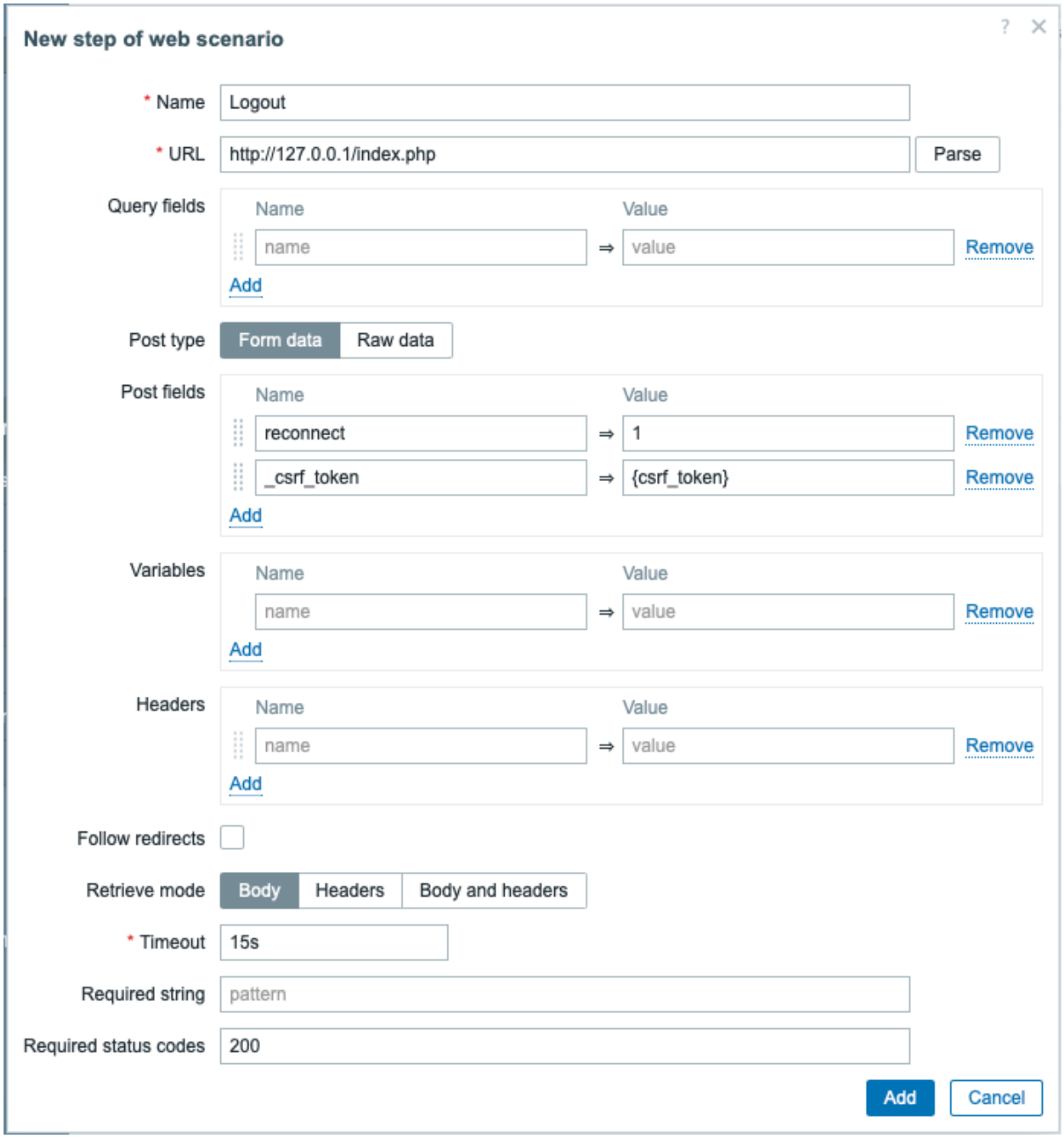


Krok 4 scenariusza WWW

Po zweryfikowaniu dostępności frontend oraz logowania dodaj krok wylogowania — w przeciwnym razie baza danych Zabbix będzie zaśmiecona wieloma rekordami otwartych sesji.

- W polu **Name** wpisz *Logout*.
- W sekcji **Post fields** dodaj dwa pola post:
  - *reconnect* o wartości *1*
  - *_csrf_token* o wartości *{csrf_token}*.
- Wypełnij wspólne pola.

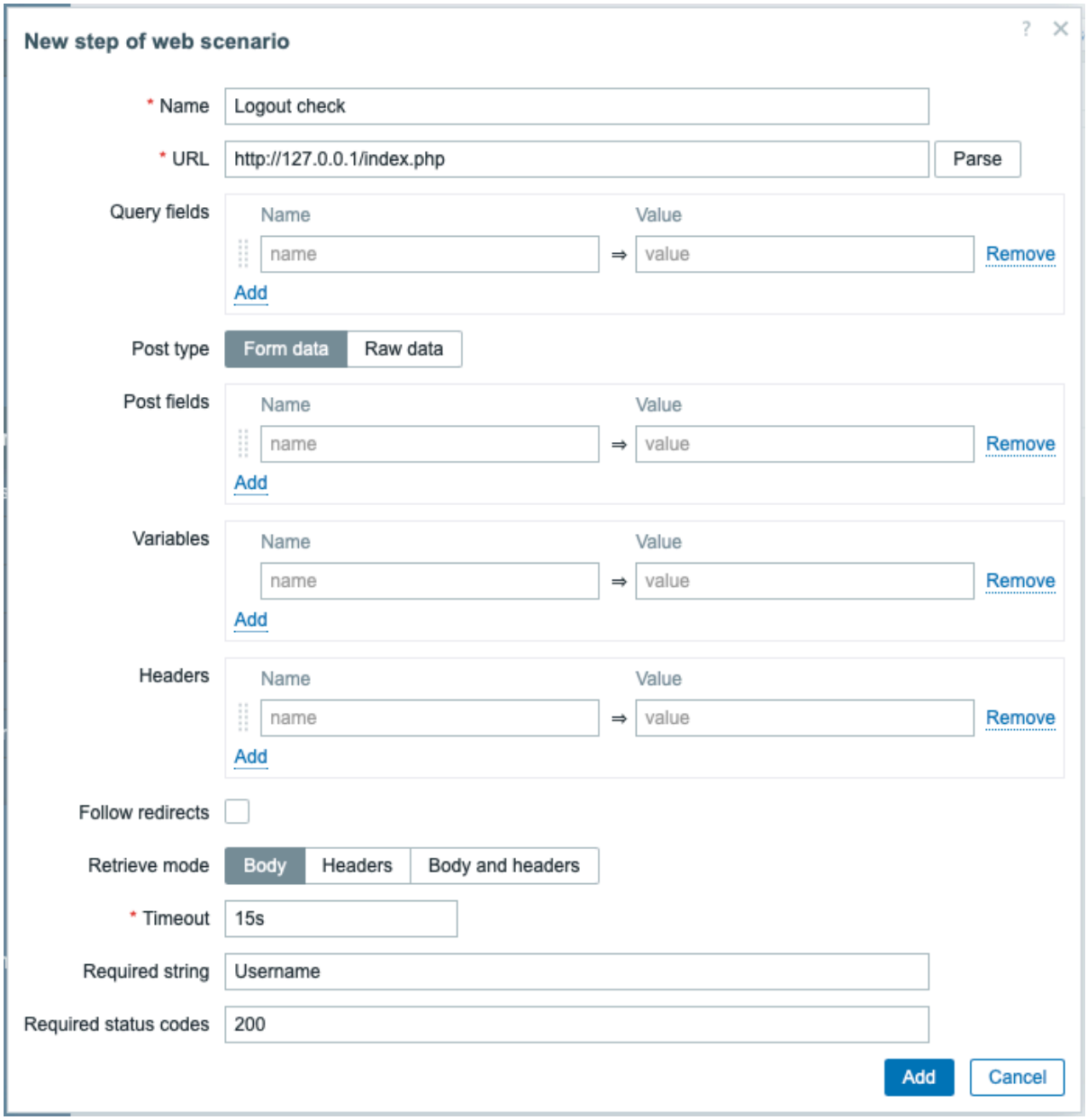
Ten krok używa zmiennej {csrf_token} uzyskanej w kroku 2



Krok 5 scenariusza WWW

Aby potwierdzić wylogowanie, sprawdź ciąg **Username**.

- W polu **Nazwa** wprowadź *Logout check*.
- W polu **Wymagany ciąg** wprowadź *Username*.
- Uzupełnij wspólne pola.



Pełna konfiguracja kroków

Pełna konfiguracja kroków scenariusza WWW powinna wyglądać następująco:

	Name	Timeout	URL	Required	Status codes	Action
1:	First page	15s	http://127.0.0.1/index.php	Zabbix SIA	200	Remove
2:	Log in	15s	http://127.0.0.1/index.php		200	Remove
3:	Log in Check	15s	http://127.0.0.1/index.php	Administrati…	200	Remove
4:	Log out	15s	http://127.0.0.1/index.php		200	Remove
5:	Log out check	15s	http://127.0.0.1/index.php	Username	200	Remove

Add

Sprawdź wyniki

Zapisz ukończony scenariusz monitorowania WWW.

Scenariusz zostanie dodany do hosta. Aby wyświetlić informacje o scenariuszu WWW, przejdź do *Monitoring* → *Hosts*, znajdź host na liście i kliknij hiperłącze Web w ostatniej kolumnie.



Kliknij nazwę scenariusza, aby zobaczyć bardziej szczegółowe statystyki:



8 Monitorowanie maszyn wirtualnych

Przegląd Zabbix może używać reguł odkrywania niskiego poziomu do automatycznego wykrywania hiperwizorów VMware i maszyn wirtualnych oraz tworzenia hostów do ich monitorowania na podstawie wstępnie zdefiniowanych prototypów hostów.

Zabbix zawiera również gotowe do użycia szablony do monitorowania VMware vCenter lub hiperwizorów ESXi.

Minimalna wymagana wersja VMware vCenter lub vSphere to 5.1.

Zbieranie danych Monitorowanie maszyn wirtualnych składa się z dwóch etapów:

1. Procesy Zabbix *vmware collector* przetwarzają dane maszyn wirtualnych — procesy te pobierają niezbędne informacje z usług sieciowych VMware za pośrednictwem protokołu SOAP, wstępnie je przetwarzają i zapisują we współdzielonej pamięci serwera Zabbix.
2. Procesy Zabbix *poller* pobierają dane przy użyciu prostego sprawdzenia Zabbix klucze pozycji monitorowania VMware.

Zabbix dzieli zebrane dane na dane konfiguracyjne VMware oraz dane liczników wydajności VMware. Oba typy danych są zbierane niezależnie przez procesy *vmware collector*.

Na podstawie informacji z liczników wydajności VMware dostępne są następujące statystyki:

- Magazyn danych
- Urządzenie dyskowe
- CPU
- Zasilanie
- Interfejs sieciowy
- Niestandardowe pozycje liczników wydajności

Pełną listę pozycji pobierających dane z liczników wydajności VMware można znaleźć w *kluczach pozycji monitorowania VMware*.

Należy pamiętać, że częstotliwość pobierania zdarzeń VMware zależy od interwału odpytywania vmware.eventlog, ale nie może być mniejsza niż 5 sekund.

Konfiguracja Jeśli serwer Zabbix jest skompilowany ze źródeł, musi zostać skompilowany z opcjami konfiguracji `--with-libcurl --with-libxml2`, aby włączyć monitorowanie maszyn wirtualnych. Pakiety Zabbix są już skompilowane z włączonymi tymi opcjami.

Następujące parametry pliku konfiguracyjnego serwera Zabbix można zmodyfikować na potrzeby monitorowania maszyn wirtualnych:

- `StartVMwareCollectors`

Note:
Zaleca się włączenie większej liczby kolektorów niż liczba monitorowanych usług VMware; w przeciwnym razie pobieranie statystyk liczników wydajności VMware może być opóźnione przez pobieranie danych konfiguracyjnych VMware (co zajmuje trochę czasu w przypadku dużych instalacji).

 Ogólnie rzecz biorąc, wartość `StartVMwareCollectors` nie powinna być mniejsza niż 2 i nie powinna przekraczać dwukrotności liczby monitorowanych usług VMware: Liczba usług < `StartVMwareCollectors` < (Liczba usług * 2). Na przykład podczas monitorowania jednej usługi VMware ustaw `StartVMwareCollectors` na 2; podczas monitorowania trzech usług ustaw `StartVMwareCollectors` na 5.

 Należy pamiętać, że wymagana liczba kolektorów zależy również od zakresu środowiska VMware oraz parametrów konfiguracyjnych `VMwareFrequency` i `VMwarePerfFrequency`.

- `VMwareCacheSize`
- `VMwareFrequency`
- `VMwarePerfFrequency`
- `VMwareTimeout`

Attention:
Aby obsługiwać metryki pojemności magazynu danych, upewnij się, że wartość klucza VMware `vpxd.stats.maxQueryMetrics` jest ustawiona co najmniej na 64. Więcej informacji można znaleźć w artykule *VMware Knowledge Base*.

Wykrywanie

Zabbix może używać reguł wykrywania niskiego poziomu (na przykład *vmware.hv.discovery[{$VMWARE.URL}]*) do automatycznego wykrywania hiperwizorów VMware i maszyn wirtualnych. Ponadto Zabbix może używać prototypów hostów do automatycznego generowania rzeczywistych hostów dla wykrytych obiektów. Aby uzyskać więcej informacji, zobacz *Prototypy hostów*.

Configuration examples

For a basic example of how to set up Zabbix for monitoring VMware using the *VMware FQDN* template, see *Monitor VMware with Zabbix*.

For a more detailed example of how to create a host, a low-level discovery rule, and a host prototype for monitoring VMware, see *Setup example*.

Rozszerzone logowanie Dane zbierane przez procesy *vmware collector* mogą być zapisywane w logach na potrzeby szczegółowego debugowania przy użyciu poziomu debugowania 5. Poziom debugowania można skonfigurować w plikach konfiguracyjnych serwer i proxy lub za pomocą opcji kontroli w czasie działania `-R log_level_increase="vmware collector,N"`, gdzie „N” oznacza numer procesu.

Na przykład, aby zwiększyć poziom debugowania z 4 do 5 dla wszystkich procesów *vmware collector*, uruchom następujące polecenie:

```
zabbix_server -R log_level_increase="vmware collector"
```

Aby zwiększyć poziom debugowania z 4 do 5 dla drugiego procesu *vmware collector*, uruchom następujące polecenie:

```
zabbix_server -R log_level_increase="vmware collector,2"
```

Gdy rozszerzone logowanie danych kolektora VMware nie jest już wymagane, zaleca się zmniejszenie poziomu debugowania do wartości domyślnej (3) przez uruchomienie polecenia `-R log_level_decrease`.

Rozwiązywanie problemów

- W przypadku niedostępnych metryk upewnij się, że nie są one domyślnie niedostępne lub wyłączone w nowszych wersjach VMware vSphere oraz że nie nałożono żadnych limitów na zapytania do bazy danych metryk wydajności. Więcej informacji można znaleźć w ZBX-12094.
- Jeśli występuje błąd `config.vpxd.stats.maxQueryMetrics` is invalid or exceeds the maximum number of characters permitted, dodaj parametr `config.vpxd.stats.maxQueryMetrics` do ustawień vCenter Server. Wartość tego parametru powinna być taka sama jak wartość `maxQuerysize` w pliku *web.xml* VMware. Więcej informacji można znaleźć w artykule *VMware Knowledge Base*.
- Jeśli podejrzewasz, że twoja instalacja Zabbix używa zbyt dużo pamięci, zobacz Profiling excessive memory usage with tcmalloc.

1 Klucze pozycji monitorowania VMware

Przegląd Ta strona zawiera szczegółowe informacje o prostych kontrolach, które mogą być używane do monitorowania środowisk VMware. Metryki są pogrupowane według celu monitorowania.

Obsługiwane klucze pozycji Klucze pozycji są wymienione bez parametrów i dodatkowych informacji. Kliknij klucz pozycji, aby zobaczyć pełne szczegóły.

Item key	Description	Item group
vmware.eventlog	Dziennik zdarzeń VMware.	Ogólna usługa
vmware.fullname	Pełna nazwa usługi VMware.	
vmware.version	Wersja usługi VMware.	
vmware.cl.perfcounter	Metryki licznika wydajności klastra VMware.	Klaster
vmware.cluster.alarms.get	Dane alarmów klastra VMware.	
vmware.cluster.discovery	Wykrywanie klastrów VMware.	
vmware.cluster.property	Właściwość klastra VMware.	
vmware.cluster.status	Stan klastra VMware.	
vmware.cluster.tags.get	Tablica tagów klastra VMware.	
vmware.datastore.alarms.get	Dane alarmów magazynu danych VMware.	Magazyn danych
vmware.datastore.discovery	Wykrywanie magazynów danych VMware.	
vmware.datastore.hv.list	Lista hypervisorów magazynu danych.	
vmware.datastore.perfcounter	Wartość licznika wydajności magazynu danych VMware.	
vmware.datastore.property	Właściwość magazynu danych VMware.	
vmware.datastore.read	Czas trwania operacji odczytu z magazynu danych.	
vmware.datastore.size	Przestrzeń magazynu danych VMware w bajtach lub jako procent całości.	
vmware.datastore.tags.get	Tablica tagów magazynu danych VMware.	
vmware.datastore.write	Czas trwania operacji zapisu do magazynu danych.	
vmware.dc.alarms.get	Dane alarmów centrum danych VMware.	Centrum danych
vmware.dc.discovery	Wykrywanie centrów danych VMware.	
vmware.dc.tags.get	Tablica tagów centrum danych VMware.	

Item key	Description	Item group
vmware.dvswitch.discovery	Wykrywanie przełączników VMware vSphere Distributed Switch.	vSphere Distributed Switch
vmware.dvswitch.fetchportsget	Dane portów VMware vSphere Distributed Switch.	
vmware.hv.alarms.get	Dane alarmów hypervisora VMware.	Hypervisor
vmware.hv.cluster.name	Nazwa klastra hypervisora VMware.	
vmware.hv.connectionstate	Stan połączenia hypervisora VMware.	
vmware.hv.cpu.usage	Użycie procesora hypervisora VMware (Hz).	
vmware.hv.cpu.usage.perf	Użycie procesora hypervisora VMware jako wartość procentowa w danym przedziale czasu.	
vmware.hv.cpu.utilization	Użycie procesora hypervisora VMware jako wartość procentowa w danym przedziale czasu, zależne od zarządzania energią lub HT.	
vmware.hv.datacenter.name	Nazwa centrum danych hypervisora VMware.	
vmware.hv.datastore.discovery	Wykrywanie magazynów danych hypervisora VMware.	
vmware.hv.datastore.list	Lista magazynów danych hypervisora VMware.	
vmware.hv.datastore.multipath	Liczba dostępnych ścieżek magazynu danych.	
vmware.hv.datastore.read	Średni czas trwania operacji odczytu z magazynu danych.	
vmware.hv.datastore.size	Przestrzeń magazynu danych VMware w bajtach lub jako procent całości.	
vmware.hv.datastore.write	Średni czas trwania operacji zapisu do magazynu danych.	
vmware.hv.discovery	Wykrywanie hypervisorów VMware.	
vmware.hv.diskinfo.get	Dane dysków hypervisora VMware.	
vmware.hv.fullname	Pełna nazwa produktu, łącznie z informacją o wersji.	
vmware.hv.hw.cpu.freq	Częstotliwość procesora hypervisora VMware.	
vmware.hv.hw.cpu.model	Model procesora hypervisora VMware.	
vmware.hv.hw.cpu.num	Liczba rdzeni procesora w hypervisorze VMware.	
vmware.hv.hw.cpu.threads	Liczba wątków procesora w hypervisorze VMware.	
vmware.hv.hw.memory	Całkowity rozmiar pamięci hypervisora VMware.	
vmware.hv.hw.model	Model hypervisora VMware.	
vmware.hv.hw.sensors.get	Wartość czujników sprzętowych hypervisora VMware.	
vmware.hv.hw.serialnumber	Numer seryjny hypervisora VMware.	
vmware.hv.hw.uuid	UUID BIOS hypervisora VMware.	
vmware.hv.hw.vendor	Nazwa dostawcy hypervisora VMware.	
vmware.hv.maintenance	Stan konserwacji hypervisora VMware.	
vmware.hv.memory.size.ballooned	Rozmiar pamięci ballooned hypervisora VMware.	
vmware.hv.memory.used	Rozmiar używanej pamięci hypervisora VMware.	
vmware.hv.net.if.discovery	Wykrywanie interfejsów sieciowych hypervisora VMware.	
vmware.hv.network.in	Statystyki ruchu przychodzącego sieci hypervisora VMware.	
vmware.hv.network.linkspeed	Prędkość interfejsu sieciowego hypervisora VMware.	
vmware.hv.network.out	Statystyki ruchu wychodzącego sieci hypervisora VMware.	
vmware.hv.perfcounter	Wartość licznika wydajności hypervisora VMware.	
vmware.hv.property	Właściwość hypervisora VMware.	
vmware.hv.power	Zużycie energii hypervisora VMware.	
vmware.hv.sensor.health.state	Zbiorczy czujnik stanu kondycji hypervisora VMware.	
vmware.hv.sensors.get	Czujniki stanu dostawcy sprzętu hypervisora VMware.	
vmware.hv.status	Stan hypervisora VMware.	
vmware.hv.tags.get	Tablica tagów hypervisora VMware.	
vmware.hv.uptime	Czas pracy hypervisora VMware.	
vmware.hv.version	Wersja hypervisora VMware.	
vmware.hv.vm.num	Liczba maszyn wirtualnych w hypervisorze VMware.	
vmware.rp.cpu.usage	Użycie CPU w hercach w danym przedziale czasu w puli zasobów VMware.	Pula zasobów
vmware.rp.memory	Metryki pamięci puli zasobów VMware.	
vmware.alarms.get	Dane alarmów wirtualnego centrum VMware.	Wirtualne centrum
vmware.vm.alarms.get	Dane alarmów maszyny wirtualnej VMware.	Maszyna wirtualna
vmware.vm.attribute	Wartość niestandardowego atrybutu maszyny wirtualnej VMware.	
vmware.vm.cluster.name	Nazwa maszyny wirtualnej VMware.	
vmware.vm.consolidationneeded	Dysk maszyny wirtualnej VMware wymaga konsolidacji.	
vmware.vm.cpu.latency	Procent czasu, w którym maszyna wirtualna nie może działać, ponieważ konkuruje o dostęp do fizycznych procesorów CPU.	

Item key	Description	Item group
vmware.vm.cpu.num	Liczba procesorów w maszynie wirtualnej VMware.	
vmware.vm.cpu.readiness	Procent czasu, w którym maszyna wirtualna była gotowa do działania, ale nie mogła zostać zaplanowana do uruchomienia na fizycznym CPU.	
vmware.vm.cpu.ready	Czas, w którym maszyna wirtualna była gotowa do działania, ale nie mogła zostać zaplanowana do uruchomienia na fizycznym CPU.	
vmware.vm.cpu.swapwait	Procent czasu CPU spędzonego na oczekiwaniu na swap-in.	
vmware.vm.cpu.usage	Użycie procesora maszyny wirtualnej VMware (Hz).	
vmware.vm.cpu.usage.perf	Użycie procesora maszyny wirtualnej VMware jako wartość procentowa w danym przedziale czasu.	
vmware.vm.datacenter.name	Nazwa centrum danych maszyny wirtualnej VMware.	
vmware.vm.discovery	Wykrywanie maszyn wirtualnych VMware.	
vmware.vm.guest.memory.swapped	Ilość fizycznej pamięci gościa przeniesionej do przestrzeni wymiany.	
vmware.vm.guest.osuptime	Całkowity czas, jaki upłynął od ostatniego uruchomienia systemu operacyjnego.	
vmware.vm.hv.maintenance	Stan konserwacji hypervisora maszyny wirtualnej VMware.	
vmware.vm.hv.name	Nazwa hypervisora maszyny wirtualnej VMware.	
vmware.vm.memory.size	Całkowity rozmiar pamięci maszyny wirtualnej VMware.	
vmware.vm.memory.size.ballooned	Rozmiar pamięci ballooned maszyny wirtualnej VMware.	
vmware.vm.memory.size.compressed	Rozmiar skompresowanej pamięci maszyny wirtualnej VMware.	
vmware.vm.memory.size.consumed	Ilość fizycznej pamięci hosta zużytej na podtrzymanie stron fizycznej pamięci gościa.	
vmware.vm.memory.size.private	Rozmiar pamięci prywatnej maszyny wirtualnej VMware.	
vmware.vm.memory.size.shared	Rozmiar pamięci współdzielonej maszyny wirtualnej VMware.	
vmware.vm.memory.size.swapped	Rozmiar pamięci wymiany maszyny wirtualnej VMware.	
vmware.vm.memory.size.usage.guest	Użycie pamięci gościa maszyny wirtualnej VMware.	
vmware.vm.memory.size.usage.host	Użycie pamięci hosta maszyny wirtualnej VMware.	
vmware.vm.memory.usage	Procent fizycznej pamięci hosta, który został zużyty.	
vmware.vm.net.if.discovery	Wykrywanie interfejsów sieciowych maszyny wirtualnej VMware.	
vmware.vm.net.if.in	Statystyki ruchu przychodzącego interfejsu sieciowego maszyny wirtualnej VMware.	
vmware.vm.net.if.out	Statystyki ruchu wychodzącego interfejsu sieciowego maszyny wirtualnej VMware.	
vmware.vm.net.if.usage	Wykorzystanie sieci maszyny wirtualnej VMware w danym przedziale czasu.	
vmware.vm.perfcounter	Wartość licznika wydajności maszyny wirtualnej VMware.	
vmware.vm.powerstate	Stan zasilania maszyny wirtualnej VMware.	
vmware.vm.property	Właściwość maszyny wirtualnej VMware.	
vmware.vm.snapshot.get	Stan migawki maszyny wirtualnej VMware.	
vmware.vm.state	Stan maszyny wirtualnej VMware.	
vmware.vm.storage.committed	Przydzielona przestrzeń dyskowa maszyny wirtualnej VMware.	
vmware.vm.storage.readoio	Średnia liczba oczekujących żądań odczytu do dysku wirtualnego w czasie przedziału zbierania danych.	
vmware.vm.storage.totalreadlatency	Średni czas trwania odczytu z dysku wirtualnego.	
vmware.vm.storage.totalwritelatency	Średni czas trwania zapisu do dysku wirtualnego.	
vmware.vm.storage.uncommitted	Nieprzydzielona przestrzeń dyskowa maszyny wirtualnej VMware.	
vmware.vm.storage.unshared	Niewspółdzielona przestrzeń dyskowa maszyny wirtualnej VMware.	
vmware.vm.storage.writeoio	Średnia liczba oczekujących żądań zapisu do dysku wirtualnego w czasie przedziału zbierania danych.	
vmware.vm.tags.get	Tablica tagów maszyny wirtualnej VMware.	
vmware.vm.tools	Stan lub wersja narzędzi gościa maszyny wirtualnej VMware.	
vmware.vm.uptime	Czas pracy maszyny wirtualnej VMware.	
vmware.vm.vfs.dev.discovery	Wykrywanie urządzeń dyskowych maszyny wirtualnej VMware.	
vmware.vm.vfs.dev.read	Statystyki odczytu urządzenia dyskowego maszyny wirtualnej VMware.	
vmware.vm.vfs.dev.write	Statystyki zapisu urządzenia dyskowego maszyny wirtualnej VMware.	
vmware.vm.vfs.fs.discovery	Wykrywanie systemów plików maszyny wirtualnej VMware.	
vmware.vm.vfs.fs.size	Statystyki systemu plików maszyny wirtualnej VMware.	

Szczegóły klucza pozycji Parametry bez nawiasów ostrych są obowiązkowe. Parametry oznaczone nawiasami ostrymi **< >** są opcjonalne.

vmware.eventlog[url,<mode>,<severity>]

 Dziennik zdarzeń VMware.
 Zwracana wartość: *Log*.

Parametry:

- **url** - URL usługi VMware;
- **mode** - *all* (domyślnie) lub *skip* - pomiń przetwarzanie starszych danych;
- **severity** - filtruj według poziomu ważności: *error*, *warning*, *info* lub *user*. Ten parametr musi być ujęty w cudzysłów, jeśli określono więcej niż jeden poziom ważności na liście rozdzielanej przecinkami (np. `"error,warning,info,user"`). Domyślnie wyłączone.

Uwagi:

- Dla każdego URL może istnieć tylko jeden klucz pozycji `vmware.eventlog`;
- Zobacz także przykład filtrowania rekordów dziennika zdarzeń VMware.

vmware.fullnameurl

 Pełna nazwa usługi VMware.
 Zwracana wartość: *String*.

Parametry:

- **url** — adres URL usługi VMware.

vmware.versionurl

 Wersja usługi VMware.
 Zwracana wartość: *String*.

Parametry:

- **url** - URL usługi VMware.

vmware.cl.perfcounter[url,id,path,<instance>]

 Metryki licznika wydajności klastra VMware.
 Zwracana wartość: *Integer*.

Parametry:

- **url** - URL usługi VMware;
- **id** - ID klastra VMware. `id` można uzyskać z `vmware.cluster.discovery[]` jako {#CLUSTER.ID}.
- **path** - ścieżka licznika wydajności[1];
- **instance** - instancja licznika wydajności.

vmware.cluster.alarms.get[url,id]

 Dane alarmów klastra VMware.
 Zwracana wartość: obiekt JSON.

Parametry:

- **url** - adres URL usługi VMware;
- **id** - identyfikator klastra VMware.

vmware.cluster.discoveryurl

 Wykrywanie klastrów VMware.
 Zwracana wartość: obiekt JSON.

Parametry:

- **url** - adres URL usługi VMware.

vmware.cluster.property[url,id,prop]

 Właściwość klastra VMware.
 Zwracana wartość: *String*.

Parametry:

- **url** — adres URL usługi VMware;
- **id** — identyfikator klastra VMware;
- **prop** — ścieżka właściwości, będąca nazwą właściwości obiektu VM zgodnie z definicją w VMware SDK.

Przykłady:

```
vmware.vm.property[{$VMWARE.URL},{$VMWARE.VM.UUID},overallStatus]
vmware.vm.property[{$VMWARE.URL},{$VMWARE.VM.UUID},runtime.powerState]
```

vmware.cluster.status[url,name]

 Status klastra VMware.
 Zwracana wartość: *0* - szary; *1* - zielony; *2* - żółty; *3* - czerwony.

Parametry:

- **url** - adres URL usługi VMware;
- **name** - nazwa klastra VMware.

vmware.cluster.tags.get[url,id]

 Tablica tagów klastra VMware.
 Zwracana wartość: obiekt JSON.

Parametry:

- **url** - URL usługi VMware;
- **id** - ID klastra VMware.

Ta pozycja działa z vSphere 6.5 i nowszymi wersjami.

vmware.datastore.alarms.get[url,uuid]

 Dane alarmów magazynu danych VMware.
 Zwracana wartość: obiekt JSON.

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator magazynu danych VMware.

vmware.datastore.discovery[url,<filter_uuid>]

 Odkrywanie magazynów danych VMware.
 Wartość zwracana: obiekt JSON.

Parametry:

- **url** — adres URL usługi VMware;
- **filter_uuid** — pojedynczy unikalny identyfikator HV lub VM (domyślnie: pusty). Jeśli zostanie określony, zostaną odkryte tylko powiązane magazyny danych.

vmware.datastore.hv.list[url,datastore]

 Lista hypervisorów datastore.
 Zwracana wartość: *String*.

Parametry:

- **url** - adres URL usługi VMware;
- **datastore** - UUID lub nazwa datastore.

Przykład danych wyjściowych:

```
esx7-01-host.zabbix.sandbox
esx7-02-host.zabbix.sandbox
```

vmware.datastore.perfcounter[url,uuid,path,<instance>]

 Wartość licznika wydajności magazynu danych VMware.
 Zwracana wartość: *Integer* [2].

Parametry:

- **url** — URL usługi VMware;
- **uuid** — globalnie unikalny identyfikator magazynu danych VMware;
- **path** — ścieżka licznika wydajności[1];
- **instance** — instancja licznika wydajności. Dla wartości zagregowanych (domyślnie) użyj pustej instancji. Wartość `instance` można otrzymać z `vmware.datastore.discovery[]` jako część tablicy {#DATASTORE.EXTENT}.

vmware.datastore.property[url,uuid,prop]

 Właściwość magazynu danych VMware.
 Zwracana wartość: *String*.

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator magazynu danych VMware;
- **prop** — ścieżka właściwości.

vmware.datastore.read[url,datastore,<mode>]

 Czas trwania operacji odczytu z datastore (w milisekundach).
 Zwracana wartość: *Integer* [2].

Parametry:

- **url** — adres URL usługi VMware;
- **datastore** — UUID lub nazwa datastore;
- **mode** — *latency* (wartość średnia, domyślnie) lub *maxlatency* (wartość maksymalna).

vmware.datastore.size[url,datastore,<mode>]

 Przestrzeń VMware datastore w bajtach lub jako wartość procentowa całkowitej przestrzeni.
 Zwracana wartość: *Integer* - dla bajtów; *Float* - dla wartości procentowej.

Parametry:

- **url** - adres URL usługi VMware;
- **datastore** - UUID lub nazwa datastore;
- **mode** - możliwe wartości: *total* (domyślnie), *free*, *pfree* (procent wolnej przestrzeni), *uncommitted*.

vmware.datastore.tags.get[url,uuid]

 Tablica tagów magazynu danych VMware.
 Zwracana wartość: obiekt JSON.

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator magazynu danych VMware.

Ta pozycja działa z vSphere 6.5 i nowszymi wersjami.

vmware.datastore.write[url,datastore,<mode>]

 Czas trwania operacji zapisu do datastore (w milisekundach).
 Zwracana wartość: *Integer* [2].

Parametry:

- **url** - URL usługi VMware;
- **datastore** - UUID lub nazwa datastore;
- **mode** - *latency* (wartość średnia, domyślnie) lub *maxlatency* (wartość maksymalna).

vmware.dc.alarms.get[url,id]

 Dane alarmów centrum danych VMware.
 Wartość zwracana: obiekt JSON.

Parametry:

- **url** — adres URL usługi VMware;
- **id** — identyfikator centrum danych VMware.

vmware.dc.discoveryurl

 Wykrywanie centrów danych VMware.
 Zwracana wartość: obiekt JSON.

Parametry:

- **url** — adres URL usługi VMware.

vmware.dc.tags.get[url,id]

 Tablica tagów centrum danych VMware.
 Zwracana wartość: obiekt JSON.

Parametry:

- **url** — URL usługi VMware;
- **id** — identyfikator centrum danych VMware.

Ta pozycja działa z vSphere 6.5 i nowszymi wersjami.

vmware.dvswitch.discoveryurl

 Wykrywanie przełączników rozproszonych VMware vSphere.
 Zwracana wartość: obiekt JSON.

Parametry:

- **url** - adres URL usługi VMware.

vmware.dvswitch.fetchports.get[url,uuid,<filter>,<mode>]

 Dane portów VMware vSphere Distributed Switch.
 Zwracana wartość: obiekt JSON.

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator VMware DVSwitch.
- **filter** - pojedynczy ciąg znaków z kryteriami rozdzielonymi przecinkami do wyboru portów;
- **mode** - *state* (cały XML bez węzłów XML „config”, domyślnie) lub *full*.

Parametr **filter** obsługuje kryteria dostępne w obiekcie danych VMware DistributedVirtualSwitchPortCriteria.

Przykład:

```
vmware.dvswitch.fetchports.get[{$VMWARE.URL},{$VMWARE.DVS.UUID},"connected:true,active:true,uplinkPort:fal
```

vmware.hv.alarms.get[url,uuid]

 Dane alarmów hipernadzorcy VMware.
 Zwracana wartość: obiekt JSON.

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator hipernadzorcy VMware.

vmware.hv.cluster.name[url,uuid]

 Nazwa klastra hipernadzorcy VMware.
 Zwracana wartość: *String*.

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator hipernadzorcy VMware.

vmware.hv.connectionstate[url,uuid]

 Stan połączenia z hiperwizorem VMware.
 Zwracana wartość: *String*: *connected*, *disconnected* lub *notResponding*.

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator hiperwizora VMware.

vmware.hv.cpu.usage[url,uuid]

 Użycie procesora hypervisora VMware (Hz).
 Zwracana wartość: *Integer*.

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator hypervisora VMware.

vmware.hv.cpu.usage.perf[url,uuid]

 Użycie procesora hypervisora VMware jako wartość procentowa w danym przedziale czasu.
 Zwracana wartość: *Float*.

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator hypervisora VMware.

vmware.hv.cpu.utilization[url,uuid]

 Użycie procesora hipernadzorcy VMware jako wartość procentowa w danym przedziale czasu; zależy od zarządzania energią lub HT.
 Zwracana wartość: *Float*.

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator hipernadzorcy VMware.

vmware.hv.datacenter.name[url,uuid]

 Nazwa centrum danych hipernadzorcy VMware.
 Zwracana wartość: *String*.

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator hipernadzorcy VMware.

vmware.hv.datastore.discovery[url,uuid]

 Wykrywanie magazynów danych hipernadzorcy VMware.
 Zwracana wartość: obiekt JSON.

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator hipernadzorcy VMware.

vmware.hv.datastore.list[url,uuid]

 Lista magazynów danych hipernadzorcy VMware.
 Zwracana wartość: *String*.

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator hipernadzorcy VMware.

Przykład danych wyjściowych:

```
SSD-RAID1-VAULT1
SSD-RAID1-VAULT2
SSD-RAID10
```

vmware.hv.datastore.multipath[url,uuid,<datastore>,<partitionid>]

 Liczba dostępnych ścieżek datastore.
 Zwracana wartość: *Integer*.

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator hiperwizora VMware;
- **datastore** - UUID lub nazwa datastore;
- **partitionid** - wewnętrzny identyfikator urządzenia fizycznego z `vmware.hv.datastore.discovery`.

vmware.hv.datastore.read[url,uuid,datastore,<mode>]

 Średni czas trwania operacji odczytu z datastore (w milisekundach).
 Zwracana wartość: *Integer* [2].

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator hipernadzorcy VMware;
- **datastore** — UUID lub nazwa datastore;
- **mode** — *latency* (domyślnie).

vmware.hv.datastore.size[url,uuid,datastore,<mode>]

 Miejsce w VMware datastore w bajtach lub jako wartość procentowa całkowitej pojemności.
 Zwracana wartość: *Integer* - dla bajtów; *Float* - dla wartości procentowej.

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator hipernadzorcy VMware;
- **datastore** - UUID lub nazwa datastore;
- **mode** - możliwe wartości: *total* (domyślnie), *free*, *pfree* (procent wolnego miejsca), *uncommitted*.

vmware.hv.datastore.write[url,uuid,datastore,<mode>]

 Średni czas trwania operacji zapisu do datastore (w milisekundach).
 Zwracana wartość: *Integer* [2].

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator hipernadzorcy VMware;
- **datastore** — UUID lub nazwa datastore;
- **mode** — *latency* (domyślnie).

vmware.hv.discoveryurl

 Wykrywanie hiperwizorów VMware.
 Zwracana wartość: obiekt JSON.

Parametry:

- **url** — adres URL usługi VMware.

vmware.hv.diskinfo.get[url,uuid]

 Dane dysków hipernadzorcy VMware.
 Zwracana wartość: obiekt JSON.

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator hipernadzorcy VMware.

vmware.hv.fullname[url,uuid]

 Pełna nazwa produktu, włącznie z informacją o wersji.
 Zwracana wartość: *String*.

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator hipernadzorcy VMware.

vmware.hv.hw.cpu.freq[url,uuid]

 Częstotliwość procesora hiperwizora VMware (Hz).
 Zwracana wartość: *Integer*.

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator hiperwizora VMware.

vmware.hv.hw.cpu.model[url,uuid]

 Model procesora hiperwizora VMware.
 Zwracana wartość: *String*.

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator hiperwizora VMware.

vmware.hv.hw.cpu.num[url,uuid]

 Liczba rdzeni procesora w hiperwizorze VMware.
 Zwracana wartość: *Integer*.

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator hiperwizora VMware.

vmware.hv.hw.cpu.threads[url,uuid]

 Liczba wątków procesora w hiperwizorze VMware.
 Zwracana wartość: *Integer*.

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator hiperwizora VMware.

vmware.hv.hw.memory[url,uuid]

 Całkowity rozmiar pamięci hipernadzorcy VMware (w bajtach).
 Zwracana wartość: *Integer*.

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator hipernadzorcy VMware.

vmware.hv.hw.model[url,uuid]

 Model hypervisora VMware.
 Zwracana wartość: *String*.

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator hypervisora VMware.

vmware.hv.hw.sensors.get[url,uuid]

 Wartość czujników sprzętowych hiperwizora VMware.
 Zwracana wartość: obiekt JSON.

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator hiperwizora VMware.

vmware.hv.hw.serialnumber[url,uuid]

 Numer seryjny hipernadzorcy VMware.
 Zwracana wartość: *String*.

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator hipernadzorcy VMware.

Ta pozycja działa z API vSphere 6.7 i nowszym.

vmware.hv.hw.uuid[url,uuid]

 UUID BIOS hiperwizora VMware.
 Zwracana wartość: *String*.

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator hiperwizora VMware.

Ta pozycja działa z API vSphere 6.7 i nowszym.

vmware.hv.hw.vendor[url,uuid]

 Nazwa dostawcy hypervisora VMware.
 Zwracana wartość: *String*.

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator hypervisora VMware.

Ta pozycja działa z API vSphere 6.7 i nowszym.

vmware.hv.maintenance[url,uuid]

 Status trybu konserwacji hipernadzorcy VMware.
 Zwracana wartość: *0* - nie jest w trybie konserwacji; *1* - jest w trybie konserwacji.

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator hipernadzorcy VMware.

vmware.hv.memory.size.ballooned[url,uuid]

 Rozmiar pamięci ballooned hipernadzorcy VMware (w bajtach).
 Zwracana wartość: *Integer*.

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator hipernadzorcy VMware.

vmware.hv.memory.used[url,uuid]

 Rozmiar używanej pamięci hipernadzorcy VMware (w bajtach).
 Zwracana wartość: *Integer*.

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator hipernadzorcy VMware.

vmware.hv.net.if.discovery[url,uuid]

 Wykrywanie interfejsów sieciowych hypervisora VMware.
 Zwracana wartość: *obiekt JSON*.

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator hypervisora VMware.

vmware.hv.network.in[url,uuid,<mode>]

 Statystyki ruchu przychodzącego sieci hipernadzorcy VMware (bajty na sekundę).
 Zwracana wartość: *Integer* [2].

Parametry:

- **url** — URL usługi VMware;
- **uuid** — globalny unikalny identyfikator hipernadzorcy VMware;
- **mode** — *bps* (domyślnie), *packets*, *dropped*, *errors*, *broadcast*.

vmware.hv.network.linkspeed[url,uuid,ifname]

 Prędkość interfejsu sieciowego hipernadzorcy VMware.
 Wartość zwracana: *Integer*. Zwraca *0*, jeśli interfejs sieciowy jest wyłączony, w przeciwnym razie zwraca wartość prędkości interfejsu.

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator hipernadzorcy VMware;

- **ifname** — nazwa interfejsu.

vmware.hv.network.out[url,uuid,<mode>]

 Statystyki wyjścia sieciowego hypervisora VMware (bajty na sekundę).
 Zwracana wartość: *Integer* [2].

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator hypervisora VMware;
- **mode** - *bps* (domyślnie), *packets*, *dropped*, *errors*, *broadcast*.

vmware.hv.perfcounter[url,uuid,path,<instance>]

 Wartość licznika wydajności hipernadzorcy VMware.
 Zwracana wartość: *Integer* [2].

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator hipernadzorcy VMware;
- **path** - ścieżka licznika wydajności [1];
- **instance** - instancja licznika wydajności. Użyj pustej instancji dla wartości zagregowanych (domyślnie).

vmware.hv.property[url,uuid,prop]

 Właściwość hiperwizora VMware.
 Zwracana wartość: *String*.

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator hiperwizora VMware;
- **prop** — ścieżka właściwości.

vmware.hv.power[url,uuid,<max>]

 Zużycie energii hiperwizora VMware (W).
 Wartość zwracana: *Integer*.

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator hiperwizora VMware;
- **max** - maksymalne dozwolone zużycie energii.

vmware.hv.sensor.health.state[url,uuid]

 Sensor zbiorczego stanu kondycji hiperwizora VMware.
 Zwracana wartość: *Integer*: *0* - szary; *1* - zielony; *2* - żółty; *3* - czerwony.

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator hiperwizora VMware.

Należy pamiętać, że ta pozycja może nie działać w VMware vSphere 6.5 i nowszych wersjach, ponieważ VMware wycofał sensor *VMware Rollup Health State*.

vmware.hv.sensors.get[url,uuid]

 Czujniki stanu dostawcy sprzętu hiperwizora VMware.
 Wartość zwracana: obiekt JSON.

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator hiperwizora VMware.

vmware.hv.status[url,uuid]

 Status hipernadzorcy VMware.
 Zwracana wartość: *Integer*: *0* - szary; *1* - zielony; *2* - żółty; *3* - czerwony.

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator hipernadzorcy VMware.

Ta pozycja używa właściwości ogólnego stanu systemu hosta.

vmware.hv.tags.get[url,uuid]

 Tablica tagów hiperwizora VMware.
 Zwracana wartość: obiekt JSON.

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator hiperwizora VMware.

Ta pozycja działa z vSphere 6.5 i nowszymi wersjami.

vmware.hv.uptime[url,uuid]

 Czas działania hipernadzorcy VMware (w sekundach).
 Zwracana wartość: *Integer*.

Parametry:

- **url** — URL usługi VMware;
- **uuid** — globalny unikalny identyfikator hipernadzorcy VMware.

Ta pozycja używa właściwości ogólnego stanu systemu hosta.

vmware.hv.version[url,uuid]

 Wersja hiperwizora VMware.
 Zwracana wartość: *String*.

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator hiperwizora VMware.

vmware.hv.vm.num[url,uuid]

 Liczba maszyn wirtualnych na hiperwizorze VMware.
 Zwracana wartość: *Integer*.

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator hiperwizora VMware.

vmware.rp.cpu.usage[url,rpid]

 Użycie CPU w hercach w danym przedziale czasu dla puli zasobów VMware.
 Zwracana wartość: *Integer*.

Parametry:

- **url** — adres URL usługi VMware;
- **rpid** — identyfikator puli zasobów VMware.

vmware.rp.memory[url,rpid,<mode>]

 Metryki pamięci puli zasobów VMware.
 Zwracana wartość: *Integer*.

Parametry:

- **url** - adres URL usługi VMware;
- **rpid** - identyfikator puli zasobów VMware;
- **mode** - możliwe wartości:
consumed (domyślnie) - ilość fizycznej pamięci hosta zużywanej do obsługi stron fizycznej pamięci gościa
 ballooned - ilość fizycznej pamięci gościa odzyskanej z maszyny wirtualnej przez sterownik balloon w systemie gościa
overhead - fizyczna pamięć hosta zużywana przez struktury danych ESXi do uruchamiania maszyn wirtualnych

vmware.alarms.geturl

 Dane alarmów VMware VirtualCenter.
 Zwracana wartość: obiekt JSON.

Parametry:

- **url** - adres URL usługi VMware.

vmware.vm.alarms.get[url,uuid]

 Dane alarmów maszyny wirtualnej VMware.
 Zwracana wartość: obiekt JSON.

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator maszyny wirtualnej VMware.

vmware.vm.attribute[url,uuid,name]

 Wartość atrybutu niestandardowego maszyny wirtualnej VMware.
 Zwracana wartość: *String*.

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator maszyny wirtualnej VMware;
- **name** - nazwa atrybutu niestandardowego.

vmware.vm.cluster.name[url,uuid]

 Nazwa maszyny wirtualnej VMware.
 Zwracana wartość: *String*.

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator maszyny wirtualnej VMware.

vmware.vm.consolidationneeded[url,uuid]

 Dysk maszyny wirtualnej VMware wymaga konsolidacji.
 Zwracana wartość: *String*: *true* - konsolidacja jest wymagana; *false* - konsolidacja nie jest wymagana.

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator maszyny wirtualnej VMware.

vmware.vm.cpu.latency[url,uuid]

 Procent czasu, w którym maszyna wirtualna nie może działać, ponieważ konkuruje o dostęp do fizycznych procesorów CPU.
 Wartość zwracana: *Float*.

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator maszyny wirtualnej VMware.

vmware.vm.cpu.num[url,uuid]

 Liczba procesorów w maszynie wirtualnej VMware.
 Zwracana wartość: *Integer*.

Parametry:

- **url** — URL usługi VMware;
- **uuid** — globalny unikalny identyfikator maszyny wirtualnej VMware.

vmware.vm.cpu.readiness[url,uuid,<instance>]

 Procent czasu, w którym maszyna wirtualna była gotowa, ale nie mogła zostać zaplanowana do uruchomienia na fizycznym CPU.
 Zwracana wartość: *Float*.

Parametry:

- **url** - URL usługi VMware;
- **uuid** - globalny unikalny identyfikator maszyny wirtualnej VMware;
- **instance** - instancja CPU.

vmware.vm.cpu.ready[url,uuid]

 Czas (w milisekundach), przez który maszyna wirtualna była gotowa, ale nie mogła zostać zaplanowana do uruchomienia na fizycznym CPU. Czas gotowości CPU zależy od liczby maszyn wirtualnych na hoście i ich obciążeń CPU (%).
 Zwracana wartość: *Integer* [2].

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator maszyny wirtualnej VMware.

vmware.vm.cpu.swapwait[url,uuid,<instance>]

 Procent czasu CPU spędzonego na oczekiwaniu na swap-in.
 Zwracana wartość: *Float*.

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator maszyny wirtualnej VMware;
- **instance** - instancja CPU.

vmware.vm.cpu.usage[url,uuid]

 Użycie procesora maszyny wirtualnej VMware (Hz).
 Zwracana wartość: *Integer*.

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator maszyny wirtualnej VMware.

vmware.vm.cpu.usage.perf[url,uuid]

 Użycie procesora maszyny wirtualnej VMware jako wartość procentowa w danym przedziale czasu.
 Zwracana wartość: *Float*.

Parametry:

- **url** - URL usługi VMware;
- **uuid** - globalny unikalny identyfikator maszyny wirtualnej VMware.

vmware.vm.datacenter.name[url,uuid]

 Nazwa centrum danych maszyny wirtualnej VMware.
 Zwracana wartość: *String*.

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator maszyny wirtualnej VMware.

vmware.vm.discoveryurl

 Wykrywanie maszyn wirtualnych VMware.
 Zwracana wartość: obiekt JSON.

Parametry:

- **url** - adres URL usługi VMware.

vmware.vm.guest.memory.size.swapped[url,uuid]

 Ilość fizycznej pamięci gościa przeniesionej do przestrzeni wymiany (swap) (KB).
 Zwracana wartość: *Integer*.

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator maszyny wirtualnej VMware.

vmware.vm.guest.osuptime[url,uuid]

 Całkowity czas, jaki upłynął od ostatniego uruchomienia systemu operacyjnego (w sekundach).
 Zwracana wartość: *Integer*.

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator maszyny wirtualnej VMware.

vmware.vm.hv.maintenance[url,uuid]

 Status konserwacji hypervisora maszyny wirtualnej VMware.
 Zwracana wartość: *0* - nie jest w trybie konserwacji; *1* - jest w trybie konserwacji.

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator maszyny wirtualnej VMware.

vmware.vm.hv.name[url,uuid]

 Nazwa hypervisora maszyny wirtualnej VMware.
 Zwracana wartość: *String*.

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator maszyny wirtualnej VMware.

vmware.vm.memory.size[url,uuid]

 Całkowity rozmiar pamięci maszyny wirtualnej VMware (w bajtach).
 Zwracana wartość: *Integer*.

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator maszyny wirtualnej VMware.

vmware.vm.memory.size.ballooned[url,uuid]

 Rozmiar pamięci ballooned maszyny wirtualnej VMware (w bajtach).
 Zwracana wartość: *Integer*.

Parametry:

- **url** - URL usługi VMware;
- **uuid** - globalny unikalny identyfikator maszyny wirtualnej VMware.

vmware.vm.memory.size.compressed[url,uuid]

 Rozmiar skompresowanej pamięci maszyny wirtualnej VMware (w bajtach).
 Zwracana wartość: *Integer*.

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator maszyny wirtualnej VMware.

vmware.vm.memory.size.consumed[url,uuid]

 Ilość fizycznej pamięci hosta zużywanej do obsługi stron fizycznej pamięci gościa (KB).
 Zwracana wartość: *Integer*.

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator maszyny wirtualnej VMware.

vmware.vm.memory.size.private[url,uuid]

 Rozmiar pamięci prywatnej maszyny wirtualnej VMware (w bajtach).
 Zwracana wartość: *Integer*.

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator maszyny wirtualnej VMware.

vmware.vm.memory.size.shared[url,uuid]

 Rozmiar pamięci współdzielonej maszyny wirtualnej VMware (w bajtach).
 Zwracana wartość: *Liczba całkowita*.

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator maszyny wirtualnej VMware.

vmware.vm.memory.size.swapped[url,uuid]

 Rozmiar pamięci wymienionej do przestrzeni wymiany maszyny wirtualnej VMware (w bajtach).
 Zwracana wartość: *Integer*.

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator maszyny wirtualnej VMware.

vmware.vm.memory.size.usage.guest[url,uuid]

 Użycie pamięci gościa maszyny wirtualnej VMware (w bajtach).
 Zwracana wartość: *Integer*.

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator maszyny wirtualnej VMware.

vmware.vm.memory.size.usage.host[url,uuid]

 Użycie pamięci hosta maszyny wirtualnej VMware (w bajtach).
 Zwracana wartość: *Integer*.

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator maszyny wirtualnej VMware.

vmware.vm.memory.usage[url,uuid]

 Procent pamięci fizycznej hosta, która została zużyta.
 Zwracana wartość: *Float*.

Parametry:

- **url** - adres URL usługi VMware;

- **uuid** - globalny unikalny identyfikator maszyny wirtualnej VMware.

vmware.vm.net.if.discovery[url,uuid]

 Wykrywanie interfejsów sieciowych maszyn wirtualnych VMware.
 Zwracana wartość: obiekt JSON.

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator maszyny wirtualnej VMware.

vmware.vm.net.if.in[url,uuid,instance,<mode>]

 Statystyki wejściowe interfejsu sieciowego maszyny wirtualnej VMware (bajty/pakiety na sekundę).
 Zwracana wartość: *Integer* [2].

Parametry:

- **url** - URL usługi VMware;
- **uuid** - globalny unikalny identyfikator maszyny wirtualnej VMware;
- **instance** - instancja interfejsu sieciowego;
- **mode** - *bps* (domyślnie) lub *pps* - bajty lub pakiety na sekundę.

vmware.vm.net.if.out[url,uuid,instance,<mode>]

 Statystyki ruchu wychodzącego interfejsu sieciowego maszyny wirtualnej VMware (bajty/pakiety na sekundę).
 Zwracana wartość: *Integer* [2].

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator maszyny wirtualnej VMware;
- **instance** — instancja interfejsu sieciowego;
- **mode** — *bps* (domyślnie) lub *pps* — bajty lub pakiety na sekundę.

vmware.vm.net.if.usage[url,uuid,<instance>]

 Wykorzystanie sieci maszyny wirtualnej VMware (łączne szybkości wysyłania i odbierania) w danym przedziale czasu (KBps).
 Zwracana wartość: *Integer*.

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator maszyny wirtualnej VMware;
- **instance** — instancja interfejsu sieciowego.

vmware.vm.perfcounter[url,uuid,path,<instance>]

 Wartość licznika wydajności maszyny wirtualnej VMware.
 Zwracana wartość: *Integer* [2].

Parametry:

- **url** - URL usługi VMware;
- **uuid** - globalny unikalny identyfikator maszyny wirtualnej VMware;
- **path** - ścieżka licznika wydajności [1];
- **instance** - instancja licznika wydajności. Dla wartości zagregowanych (domyślnie) użyj pustej instancji.

vmware.vm.powerstate[url,uuid]

 Stan zasilania maszyny wirtualnej VMware.
 Zwracana wartość: *0* - poweredOff; *1* - poweredOn; *2* - suspended.

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator maszyny wirtualnej VMware.

vmware.vm.property[url,uuid,prop]

 Właściwość maszyny wirtualnej VMware.
 Zwracana wartość: *String*.

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator maszyny wirtualnej VMware;
- **prop** - ścieżka właściwości.

vmware.vm.snapshot.get[url,uuid]

 Stan migawki maszyny wirtualnej VMware.
 Zwracana wartość: obiekt JSON.

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator maszyny wirtualnej VMware.

vmware.vm.state[url,uuid]

 Stan maszyny wirtualnej VMware.
 Zwracana wartość: *String*: *notRunning*, *resetting*, *running*, *shuttingDown*, *standby* lub *unknown*.

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator maszyny wirtualnej VMware.

vmware.vm.storage.committed[url,uuid]

 Zajęta przestrzeń dyskowa maszyny wirtualnej VMware (w bajtach).
 Zwracana wartość: *Integer*.

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator maszyny wirtualnej VMware.

vmware.vm.storage.readoio[url,uuid,instance]

 Średnia liczba oczekujących żądań odczytu do dysku wirtualnego w czasie interwału zbierania danych.
 Zwracana wartość: *Integer*.

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator maszyny wirtualnej VMware;
- **instance** - instancja urządzenia dyskowego.

vmware.vm.storage.totalreadlatency[url,uuid,instance]

 Średni czas trwania odczytu z dysku wirtualnego (w milisekundach).
 Zwracana wartość: *Integer*.

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator maszyny wirtualnej VMware;
- **instance** — instancja urządzenia dyskowego.

vmware.vm.storage.totalwritelatency[url,uuid,instance]

 Średni czas trwania zapisu na dysk wirtualny (w milisekundach).
 Zwracana wartość: *Integer*.

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator maszyny wirtualnej VMware;
- **instance** — instancja urządzenia dyskowego.

vmware.vm.storage.uncommitted[url,uuid]

 Niezatwierdzona przestrzeń dyskowa maszyny wirtualnej VMware (w bajtach).
 Zwracana wartość: *Integer*.

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator maszyny wirtualnej VMware.

vmware.vm.storage.unshared[url,uuid]

 Niewspółdzielona przestrzeń dyskowa maszyny wirtualnej VMware (w bajtach).
 Zwracana wartość: *Integer*.

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator maszyny wirtualnej VMware.

vmware.vm.storage.writeoio[url,uuid,instance]

 Średnia liczba oczekujących żądań zapisu do dysku wirtualnego w czasie interwału zbierania danych.
 Zwracana wartość: *Integer*.

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator maszyny wirtualnej VMware;
- **instance** — instancja urządzenia dyskowego.

vmware.vm.tags.get[url,uuid]

 Tablica tagów maszyny wirtualnej VMware.
 Zwracana wartość: obiekt JSON.

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator maszyny wirtualnej VMware.

Ta pozycja działa z vSphere 6.5 i nowszymi wersjami.

vmware.vm.tools[url,uuid,<mode>]

 Stan narzędzi gościa maszyny wirtualnej VMware.
 Zwracana wartość: *String*.
 W trybie *status*: *guestToolsExecutingScripts* - VMware Tools uruchamia się; *guestToolsNotRunning* - VMware Tools nie jest uruchomione; *guestToolsRunning* - VMware Tools jest uruchomione.
 W trybie *version*: wersja.

Parametry:

- **url** - URL usługi VMware;
- **uuid** - globalny unikalny identyfikator maszyny wirtualnej VMware;
- **mode** - *version*, *status* (domyślnie).

vmware.vm.uptime[url,uuid]

 Czas działania maszyny wirtualnej VMware (w sekundach).
 Zwracana wartość: *Integer*.

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator maszyny wirtualnej VMware.

vmware.vm.vfs.dev.discovery[url,uuid]

 Wykrywanie urządzeń dyskowych maszyny wirtualnej VMware.
 Zwracana wartość: obiekt JSON.

Parametry:

- **url** — URL usługi VMware;
- **uuid** — globalny unikalny identyfikator maszyny wirtualnej VMware.

vmware.vm.vfs.dev.read[url,uuid,instance,<mode>]

 Statystyki odczytu urządzenia dyskowego maszyny wirtualnej VMware (bajty/operacje na sekundę).
 Zwracana wartość: *Integer* [2].

Parametry:

- **url** — URL usługi VMware;
- **uuid** — globalny unikalny identyfikator maszyny wirtualnej VMware;
- **instance** — instancja urządzenia dyskowego;
- **mode** — *bps* (domyślnie) lub *ops* — bajty lub operacje na sekundę.

vmware.vm.vfs.dev.write[url,uuid,instance,<mode>]

 Statystyki zapisu urządzenia dyskowego maszyny wirtualnej VMware (bajty/operacje na sekundę).
 Zwracana wartość: *Integer* [2].

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator maszyny wirtualnej VMware;
- **instance** — instancja urządzenia dyskowego;
- **mode** — *bps* (domyślnie) lub *ops* — bajty lub operacje na sekundę.

vmware.vm.vfs.fs.discovery[url,uuid]

 Wykrywanie systemów plików maszyny wirtualnej VMware.
 Wartość zwracana: obiekt JSON.

Parametry:

- **url** — adres URL usługi VMware;
- **uuid** — globalny unikalny identyfikator maszyny wirtualnej VMware.

Aby ta pozycja działała, w gościnnej maszynie wirtualnej muszą być zainstalowane VMware Tools.

vmware.vm.vfs.fs.size[url,uuid,fsname,<mode>]

 Statystyki systemu plików maszyny wirtualnej VMware (bajty/procenty).
 Zwracana wartość: *Integer* - dla bajtów; *Float* - dla wartości procentowych.

Parametry:

- **url** - adres URL usługi VMware;
- **uuid** - globalny unikalny identyfikator maszyny wirtualnej VMware;
- **fsname** - nazwa systemu plików;
- **mode** - *total*, *free*, *used*, *pfree* lub *pused*.

Aby ta pozycja działała, na gościnnej maszynie wirtualnej muszą być zainstalowane VMware Tools.

Przypisy

[1] Zobacz Tworzenie niestandardowych nazw liczników wydajności dla VMware.

[2] Wartość tych pozycji jest pobierana z liczników wydajności VMware, a parametr VMwarePerfFrequency parameter jest używany do odświeżania ich danych w pamięci podręcznej VMware Zabbix:

- vmware.cl.perfcounter
- vmware.hv.datastore.read
- vmware.hv.datastore.write
- vmware.hv.network.in
- vmware.hv.network.out
- vmware.hv.perfcounter
- vmware.vm.cpu.ready
- vmware.vm.net.if.in
- vmware.vm.net.if.out
- vmware.vm.perfcounter
- vmware.vm.vfs.dev.read
- vmware.vm.vfs.dev.write

Więcej informacji

Szczegółowe informacje o tym, jak skonfigurować Zabbix do monitorowania środowisk VMware, można znaleźć w sekcji Monitorowanie maszyn wirtualnych.

2 Kluczowe pola wykrywania maszyn wirtualnych

Poniższa tabela zawiera pola zwracane przez klucze wykrywania związane z maszynami wirtualnymi.

Klucz pozycji		
Opis	**Pole**	**Pobrana zawartość**
vmware.cluster.discovery		
Wykonuje wykrywanie klastrów.	{#CLUSTER.ID}	Identyfikator klastra.
	{#CLUSTER.NAME}	Nazwa klastra.

Klucz pozycji		

	”resource_pool”	Tablica zawierająca dane puli zasobów, w tym identyfikator grupy zasobów, tablicę tagów, ścieżkę puli zasobów, liczbę maszyn wirtualnych.
		
		Struktura tablicy:
		`[{`
		`"rpid":"resource group id",`
		`"tags":[{}],`
		`"rpath":"resource group path",`
		`"vm_count":0`
		`}]`
		
		Dla struktury tablicy "tags" zobacz pole ”tags”.

	”tags”	Tablica zawierająca tagi z nazwą tagu, opisem i kategorią.
		
		Struktura tablicy:
		`[{`
		`"tag":"tag name",`
		`"tag_description":"tag description",`
		`"category":"tag category"`
		`}]`

vmware.datastore.discovery		
Wykonuje wykrywanie magazynów danych.	{#DATASTORE}	Nazwa magazynu danych.

	{#DATASTORE.EXTENT}	Tablica zawierająca identyfikator partycji extent magazynu danych oraz nazwę instancji.
		
		Struktura tablicy:
		`[{`
		`"partitionid":1,`
		`"instance":"name"`
		`}]`

	{#DATASTORE.TYPE}	Typ magazynu danych. Przykładowe wartości: VMFS, NFS, vsan itp.
	{#DATASTORE.UUID}	Identyfikator magazynu danych.

	”tags”	Tablica zawierająca tagi z nazwą tagu, opisem i kategorią.
		
		Struktura tablicy:
		`[{`
		`"tag":"tag name",`
		`"tag_description":"tag description",`
		`"category":"tag category"`
		`}]`

vmware.dc.discovery		
Wykonuje wykrywanie centrów danych.	{#DATACENTER}	Nazwa centrum danych.
	{#DATACENTERID}	Identyfikator centrum danych.

	”tags”	Tablica zawierająca tagi z nazwą tagu, opisem i kategorią.
		
		Struktura tablicy:
		`[{`
		`"tag":"tag name",`
		`"tag_description":"tag description",`
		`"category":"tag category"`
		`}]`

vmware.dvswitch.discovery		
Wykonuje wykrywanie przełączników rozproszonych vSphere.	{#DVS.NAME}	Nazwa przełącznika.

Klucz pozycji		
	{#DVS.UUID}	Identyfikator przełącznika.
vmware.hv.discovery		
Wykonuje wykrywanie hypervisorów.	{#HV.UUID}	Unikalny identyfikator hypervisora.
	{#HV.ID}	Identyfikator hypervisora (nazwa obiektu zarządzanego HostSystem).
	{#HV.NAME}	Nazwa hypervisora.
	{#HV.NETNAME}	Nazwa sieciowa hosta hypervisora.
	{#HV.IP}	Adres IP hypervisora, może być pusty. W przypadku konfiguracji HA z wieloma interfejsami sieciowymi obowiązuje następujący priorytet wyboru interfejsu: - preferowany jest adres IP współdzielący podsieć IP z adresem IP vCenter; - preferowany jest adres IP z podsieci IP z bramą domyślną; - preferowany jest adres IP z interfejsu o najniższym ID.
	{#CLUSTER.NAME}	Nazwa klastra, może być pusta.
	{#DATACENTER.NAME}	Nazwa centrum danych.
	{#PARENT.NAME}	Nazwa kontenera przechowującego hypervisor.
	{#PARENT.TYPE}	Typ kontenera, w którym przechowywany jest hypervisor. Wartości mogą być następujące: `Datacenter`, `Folder`, `ClusterComputeResource`, `VMware`, gdzie ”VMware” oznacza nieznany typ kontenera.

	”resource_pool”	Tablica zawierająca dane puli zasobów, w tym identyfikator grupy zasobów, tablicę tagów, ścieżkę puli zasobów, liczbę maszyn wirtualnych.
		
		Struktura tablicy:
		`[{`
		`"rpid":"resource group id",`
		`"tags":[{}],`
		`"rpath":"resource group path",`
		`"vm_count":0`
		`}]`
		
		Dla struktury tablicy `"tags"` zobacz pole ”tags”.

	”tags”	Tablica zawierająca tagi z nazwą tagu, opisem i kategorią.
		
		Struktura tablicy:
		`[{`
		`"tag":"tag name",`
		`"tag_description":"tag description",`
		`"category":"tag category"`
		`}]`

vmware.hv.datastore.discovery		
Wykonuje wykrywanie magazynów danych hypervisora. Należy pamiętać, że wiele hypervisorów może używać tego samego magazynu danych.	{#DATASTORE}	Nazwa magazynu danych.
	{#DATASTORE.TYPE}	Typ magazynu danych. Przykładowe wartości: `VMFS`, `NFS`, `vsan` itp.
	{#DATASTORE.UUID}	Identyfikator magazynu danych.
	{#MULTIPATH.COUNT}	Zarejestrowana liczba ścieżek magazynu danych.
	{#MULTIPATH.PARTITION.COUNT}	Liczba dostępnych partycji dysku.

Klucz pozycji		

	”datastore_extent”	Tablica zawierająca nazwę instancji extent magazynu danych oraz identyfikator partycji.
		
		Struktura tablicy:
		`[{`
		`"partitionid":1,`
		`"instance":"name"`
		`}]`

	”tags”	Tablica zawierająca tagi z nazwą tagu, opisem i kategorią.
		
		Struktura tablicy:
		`[{`
		`"tag":"tag name",`
		`"tag_description":"tag description",`
		`"category":"tag category"`
		`}]`

vmware.hv.net.if.discovery		
Wykonuje wykrywanie interfejsów sieciowych hypervisora.	{#IFNAME}	Nazwa interfejsu.
	{#IFDRIVER}	Sterownik interfejsu.
	{#IFDUPLEX}	Ustawienia dupleksu interfejsu.
	{#IFSPEED}	Prędkość interfejsu.
	{#IFMAC}	Adres MAC interfejsu.
vmware.vm.discovery		
Wykonuje wykrywanie maszyn wirtualnych.	{#VM.UUID}	Unikalny identyfikator maszyny wirtualnej.
	{#VM.ID}	Identyfikator maszyny wirtualnej (nazwa obiektu zarządzanego VirtualMachine).
	{#VM.NAME}	Nazwa maszyny wirtualnej.
	{#HV.NAME}	Nazwa hypervisora.
	{#HV.UUID}	Unikalny identyfikator hypervisora.
	{#HV.ID}	Identyfikator hypervisora (nazwa obiektu zarządzanego HostSystem).
	{#CLUSTER.NAME}	Nazwa klastra, może być pusta.
	{#DATACENTER.NAME}	Nazwa centrum danych.
	{#DATASTORE.NAME}	Nazwa magazynu danych.
	{#DATASTORE.UUID}	Identyfikator magazynu danych.
	{#VM.IP}	Adres IP maszyny wirtualnej, może być pusty.
	{#VM.DNS}	Nazwa DNS maszyny wirtualnej, może być pusta.
	{#VM.GUESTFAMILY}	Rodzina systemu operacyjnego gościa maszyny wirtualnej, może być pusta.
	{#VM.GUESTFULLNAME}	Pełna nazwa systemu operacyjnego gościa maszyny wirtualnej, może być pusta.
	{#VM.FOLDER}	Łańcuch folderów nadrzędnych maszyny wirtualnej; może być używany jako wartość dla grup zagnieżdżonych; nazwy folderów są łączone znakiem ”/”. Może być pusty.
	{#VM.TOOLS.STATUS}	Stan narzędzi maszyny wirtualnej VMware.
	{#VM.POWERSTATE}	Stan zasilania maszyny wirtualnej VMware (`poweredOff`, `poweredOn` lub `suspended`).
	{#VM.RPOOL.ID}	Identyfikator puli zasobów.
	{#VM.RPOOL.PATH}	Pełna ścieżka puli zasobów z wyłączeniem nazwy głównej ”Resources”. Nazwy folderów są łączone znakiem ”/”.
	{#VM.SNAPSHOT.COUNT}	Liczba migawek VM.

	”tags”	Tablica zawierająca tagi z nazwą tagu, opisem i kategorią.
		
		Struktura tablicy:
		`[{`
		`"tag":"tag name",`
		`"tag_description":"tag description",`
		`"category":"tag category"`
		`}]`

Klucz pozycji		

	”vm_customattribute”	Tablica niestandardowych atrybutów maszyny wirtualnej (jeśli są zdefiniowane).
		
		Struktura tablicy:
		`[{`
		`"name":"custom field name",`
		`"value":"custom field value"`
		`}]`

	”net_if”	Tablica interfejsów sieciowych maszyny wirtualnej.
		
		Struktura tablicy:
		`[{`
		`"ifname": "interface name",`
		`"ifdesc": "interface description",`
		`"ifmac": "00:00:00:00:00:00",`
		`"ifconnected": true,`
		`"iftype": "interface type",`
		`"ifbackingdevice": "interface backing device",`
		`"ifdvswitch_uuid": "interface switch uuid",`
		`"ifdvswitch_portgroup": "interface switch port group",`
		`"ifdvswitch_port": "interface switch port",`
		`"ifip": ["interface ip addresses"]`
		`}]`
		
		Opis zwracanych danych znajduje się w kluczu pozycji ”vmware.vm.net.if.discovery”.

vmware.vm.net.if.discovery		
Wykonuje wykrywanie interfejsów sieciowych maszyny wirtualnej.	{#IFNAME}	Nazwa interfejsu sieciowego.
	{#IFDESC}	Opis interfejsu.
	{#IFMAC}	Adres MAC interfejsu.
	{#IFCONNECTED}	Stan połączenia interfejsu (`false` - rozłączony; `true` - połączony).
	{#IFTYPE}	Typ interfejsu.
	{#IFBACKINGDEVICE}	Nazwa urządzenia bazowego.
	{#IFDVSWITCH.UUID}	Unikalny identyfikator vSphere Distributed Switch.
	{#IFDVSWITCH.PORTGROUP}	Rozproszona grupa portów.
	{#IFDVSWITCH.PORT}	Port vSphere Distributed Switch.
	”ifip”	Tablica adresów interfejsu.
vmware.vm.vfs.dev.discovery		
Wykonuje wykrywanie urządzeń dyskowych maszyny wirtualnej.	{#DISKNAME}	Nazwa urządzenia dyskowego.
vmware.vm.vfs.fs.discovery		
Wykonuje wykrywanie systemów plików maszyny wirtualnej.	{#FSNAME}	Nazwa systemu plików.

3 przykłady JSON dla pozycji VMware

Przegląd Ta sekcja zawiera dodatkowe informacje o obiektach JSON zwracanych przez różne pozycje.

vmware.*.alarms.get Pozycje **vmware.alarms.get[]**, **vmware.cluster.alarms.get[]**, **vmware.datastore.alarms.get[]**, **vmware.dc.alarms.get[]**, **vmware.hv.alarms.get[]**, **vmware.vm.alarms.get[]** zwracają obiekty JSON o następującej strukturze (wartości podano jako przykład):

```
{
    "alarms": [
        {
            "name": "Host connection and power state",
            "system_name": "alarm.HostConnectionStateAlarm",
            "description": "Default alarm to monitor host connection and power state",
            "enabled": true,
            "key": "alarm-1.host-2013",
            "time": "2022-06-27T05:27:38.759976Z",
            "overall_status": "red",
            "acknowledged": false
        },
        {
            "name": "Host memory usage",
            "system_name": "alarm.HostMemoryUsageAlarm",
            "description": "Default alarm to monitor host memory usage",
            "enabled": true,
            "key": "alarm-4.host-1004",
            "time": "2022-05-16T13:32:42.47863Z",
            "overall_status": "yellow",
            "acknowledged": false
        },
        {
            // inne alarmy
        }
    ]
}
```

vmware.*.tags.get Pozycje **vmware.cluster.tags.get[]**, **vmware.datastore.tags.get[]**, **vmware.dc.tags.get[]**, **vmware.hv.tags.g**
vmware.vm.tags.get[] zwracają obiekty JSON o następującej strukturze (wartości podano jako przykład):

```
{
    "tags": [
        {
            "name": "Windows",
        "description": "tag dla kategorii typ systemu operacyjnego",
        "category": "typ systemu operacyjnego"
    },
    {
            "name": "SQL Server",
        "description": "tag dla kategorii nazwa aplikacji",
        "category": "nazwa aplikacji"
        },
    {
            // inne tagi
        }
    ]
}
```

vmware.hv.diskinfo.get Pozycja **vmware.hv.diskinfo.get[]** zwraca obiekty JSON o następującej strukturze (wartości podano jako przykład):

```
[
  {
    "instance": "mpx.vmhba32:C0:T0:L0",
    "hv_uuid": "8002299e-d7b9-8728-d224-76004bbb6100",
    "datastore_uuid": "",
    "operational_state": [
      "ok"
    ],
    "lun_type": "disk",
    "queue_depth": 1,
    "model": "USB DISK",
```

```
    "vendor": "SMI Corp",
    "revision": "1100",
    "serial_number": "CCYYMMDDHHmmSS9S62CK",
    "vsan": {}
  },
  {
    // other instances
  }
]
```

vmware.dvswitch.fetchports.get Pozycja **vmware.dvswitch.fetchports.get[]** zwraca obiekty JSON o następującej strukturze (wartości podano jako przykład):

```
{
    "FetchDVPortsResponse":
    {
        "returnval": [
            {
                "key": "0",
                "dvsUuid": "50 36 6a 24 25 c0 10 9e-05 4a f6 ea 4e 3d 09 88",
                "portgroupKey": "dvportgroup-2023",
                "proxyHost":
                {
                    "@type": "HostSystem",
                    "#text": "host-2021"
                },
                "connectee":
                {
                    "connectedEntity":
                    {
                        "@type": "HostSystem",
                        "#text": "host-2021"
                    },
                    "nicKey": "vmnic0",
                    "type": "pnic"
                },
                "conflict": "false",
                "state":
                {
                    "runtimeInfo":
                    {
                        "linkUp": "true",
                        "blocked": "false",
                        "vlanIds":
                        {
                            "start": "0",
                            "end": "4094"
                        },
                        "trunkingMode": "true",
                        "linkPeer": "vmnic0",
                        "macAddress": "00:00:00:00:00:00",
                        "statusDetail": null,
                        "vmDirectPathGen2Active": "false",
                        "vmDirectPathGen2InactiveReasonOther": "portNptIncompatibleConnectee"
                    },
                    "stats":
                    {
                        "packetsInMulticast": "2385470",
                        "packetsOutMulticast": "45",
                        "bytesInMulticast": "309250248",
                        "bytesOutMulticast": "5890",
                        "packetsInUnicast": "155601537",
                        "packetsOutUnicast": "113008658",
```

```
                        "bytesInUnicast": "121609489384",
                        "bytesOutUnicast": "47240279759",
                        "packetsInBroadcast": "1040420",
                        "packetsOutBroadcast": "7051",
                        "bytesInBroadcast": "77339771",
                        "bytesOutBroadcast": "430392",
                        "packetsInDropped": "0",
                        "packetsOutDropped": "0",
                        "packetsInException": "0",
                        "packetsOutException": "0"
                    }
                },
                "connectionCookie": "1702765133",
                "lastStatusChange": "2022-03-25T14:01:11Z",
                "hostLocalPort": "false"
            },
            {
                //inne klucze
            }
        ]
    }
}
```

vmware.hv.hw.sensors.get Pozycja **vmware.hv.hw.sensors.get[]** zwraca obiekty JSON o następującej strukturze (wartości podano jako przykład):

```
{
    "val":
        {
            "@type": "HostHardwareStatusInfo",
            "storageStatusInfo": [
                {
                    "name": "Intel Corporation HD Graphics 630 #2",
                "status":
                        {
                            "label": "Unknown",
                    "summary": "Cannot report on the current status of the physical element",
                    "key": "Unknown"
                }
            },
            {
                    "name": "Intel Corporation 200 Series/Z370 Chipset Family USB 3.0 xHCI Controller #20"
                "status":
                        {
                     "label": "Unknown",
                     "summary": "Cannot report on the current status of the physical element",
                     "key": "Unknown"
                 }
            },
            {
                    // inne czujniki sprzętowe hv
                }
        ]
        }
}
```

vmware.hv.sensors.get Pozycja **vmware.hv.sensors.get[]** zwraca obiekty JSON o następującej strukturze (wartości podano jako przykład):

```
{
    "val":
        {
            "@type": "ArrayOfHostNumericSensorInfo", "HostNumericSensorInfo": [
```

```
                {
                    "@type": "HostNumericSensorInfo",
                    "name": "System Board 1 PwrMeter Output --- Normal",
                    "healthState":
                        {
                            "label": "Green",
                            "summary": "Sensor is operating under normal conditions",
                    "key": "green"
                },
                    "currentReading": "10500",
                "unitModifier": "-2",
                "baseUnits": "Watts",
                "sensorType": "other"
            },
                {
                    "@type": "HostNumericSensorInfo",
                    "name": "Power Supply 1 PS 1 Output --- Normal",
                    "healthState":
                        {
                            "label": "Green",
                    "summary": "Sensor is operating under normal conditions",
                    "key": "green"
                },
                    "currentReading": "10000",
            "unitModifier": "-2",
            "baseUnits": "Watts",
            "sensorType": "power"
        },
                {
                        // inne sensory hv
                }
        ]
        }
}
```

vmware.vm.snapshot.get Jeśli istnieją jakiekolwiek snapshoty, pozycja **vmware.snapshot.get[]** zwraca obiekt JSON o następującej strukturze (wartości podano jako przykład):

```
{
  "snapshot": [
    {
      "name": "VM Snapshot 4%2f1%2f2022, 9:16:39 AM",
      "description": "Descr 1",
      "createtime": "2022-04-01T06:16:51.761Z",
      "size": 5755795171,
      "uniquesize": 5755795171
    },
    {
      "name": "VM Snapshot 4%2f1%2f2022, 9:18:21 AM",
      "description": "Descr 2",
      "createtime": "2022-04-01T06:18:29.164999Z",
      "size": 118650595,
      "uniquesize": 118650595
    },
    {
      "name": "VM Snapshot 4%2f1%2f2022, 9:37:29 AM",
      "description": "Descr 3",
      "createtime": "2022-04-01T06:37:53.534999Z",
      "size": 62935016,
      "uniquesize": 62935016
    }
  ],
  "count": 3,
```

```
  "latestdate": "2022-04-01T06:37:53.534999Z",
  "latestage": 22729203,
  "oldestdate": "2022-04-01T06:16:51.761Z",
  "oldestage": 22730465,
  "size": 5937380782,
  "uniquesize": 5937380782
}
```

Jeśli nie istnieje żaden snapshot, pozycja **vmware.snapshot.get[]** zwraca obiekt JSON z pustymi wartościami:

```
{
  "snapshot": [],
  "count": 0,
  "latestdate": null,
  "latestage": 0,
  "oldestdate": null,
  "oldestage": 0,
  "size": 0,
  "uniquesize": 0
}
```

4 Przykład konfiguracji monitorowania VMware

Przegląd

Poniższy przykład opisuje, jak skonfigurować Zabbix do monitorowania maszyn wirtualnych VMware. Obejmuje to:

- utworzenie hosta reprezentującego środowisko VMware;
- utworzenie reguły wykrywania niskiego poziomu, która wykrywa maszyny wirtualne w środowisku VMware;
- utworzenie prototypu hosta, na podstawie którego Zabbix wygeneruje rzeczywiste hosty dla maszyn wirtualnych wykrytych przez regułę wykrywania niskiego poziomu.

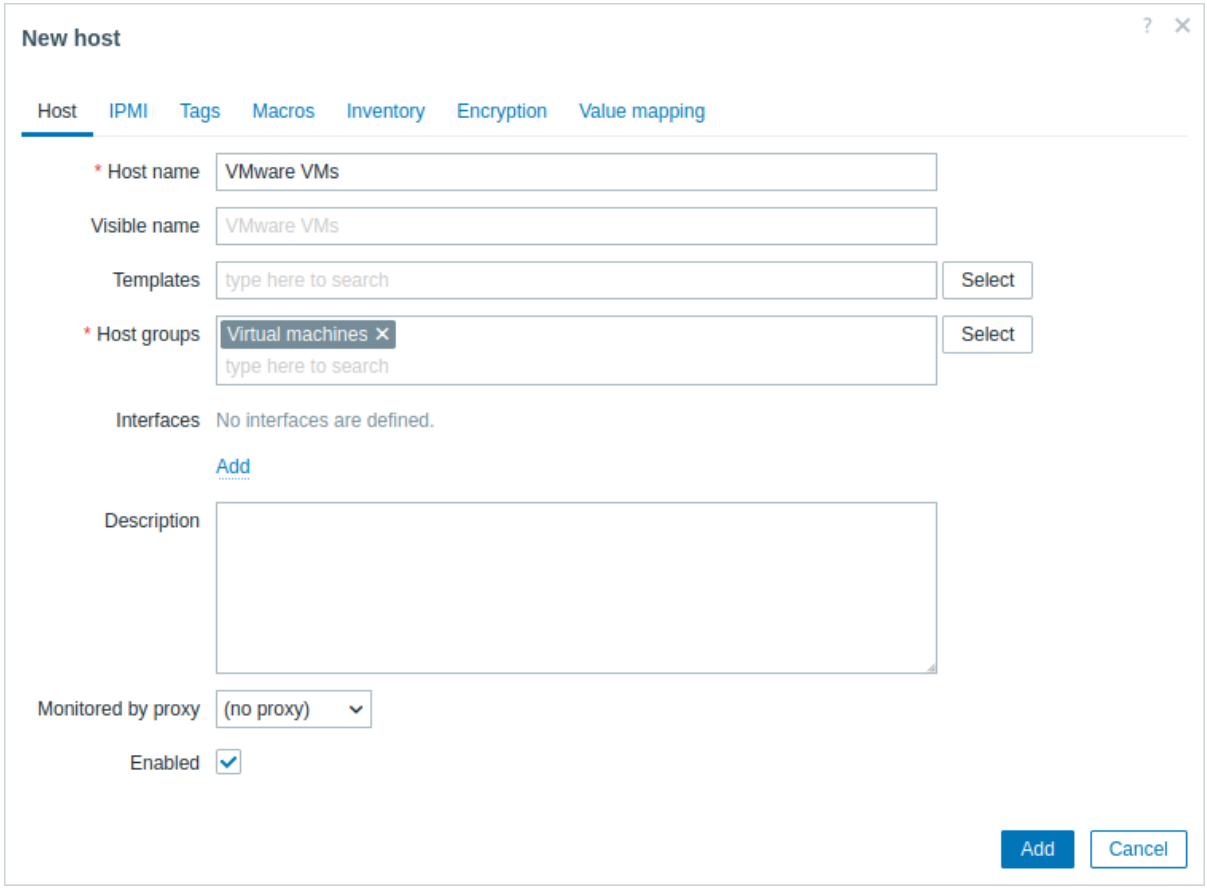
Wymagania wstępne

> **Note:**
> Ten przykład nie obejmuje konfiguracji VMware. Zakłada się, że VMware jest już skonfigurowane.

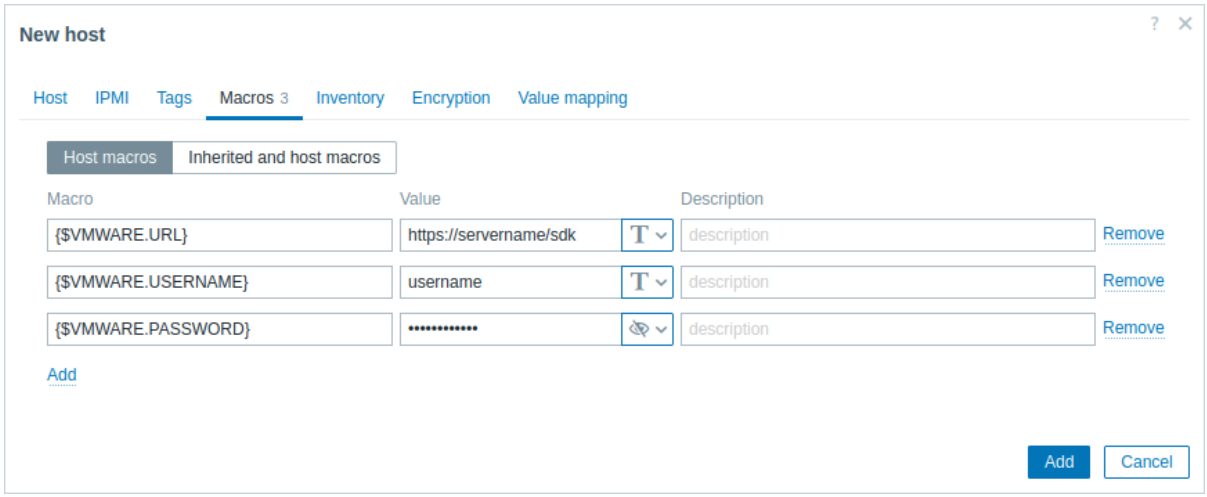
Przed kontynuowaniem ustaw parametr `StartVMwareCollectors` w pliku konfiguracyjnym serwera Zabbix na 2 lub więcej (wartość domyślna to 0).

Utwórz host

1. Przejdź do *Data collection* → *Hosts*.
2. Utwórz host:
   - W polu *Host name* wprowadź nazwę hosta (na przykład „VMware VMs”).
   - W polu *Host groups* wpisz lub wybierz grupę hostów (na przykład „Virtual machines”).



- Na karcie *Macros* ustaw następujące makra hosta:
  - {$VMWARE.URL} — adres URL SDK usługi VMware (hipernadzorcy ESXi) (https://servername/sdk)
  - {$VMWARE.USERNAME} — nazwa użytkownika usługi VMware
  - {$VMWARE.PASSWORD} — hasło użytkownika {$VMWARE.USERNAME} usługi VMware



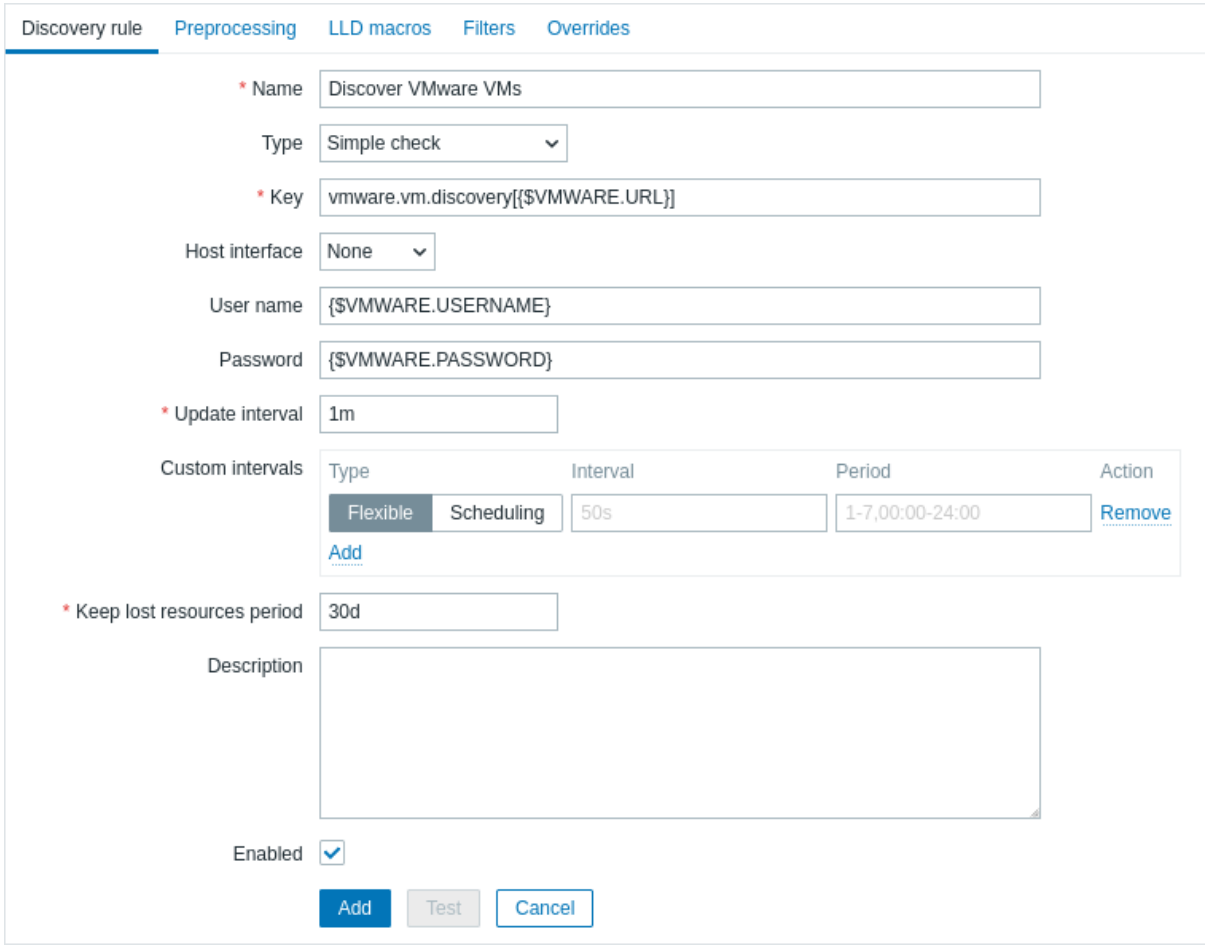
3. Kliknij przycisk *Add*, aby utworzyć host. Ten host będzie reprezentować Twoje środowisko VMware.

Utwórz regułę wykrywania niskiego poziomu

1. Kliknij *Discovery* dla utworzonego hosta, aby przejść do listy reguł wykrywania niskiego poziomu dla tego hosta.

2. Utwórz regułę wykrywania niskiego poziomu:

- W polu *Name* wprowadź nazwę reguły wykrywania niskiego poziomu (na przykład „Wykryj maszyny wirtualne VMware”).
- W polu *Type* wybierz „Simple check”.
- W polu *Key* wprowadź wbudowany klucz pozycji do wykrywania maszyn wirtualnych VMware: `vmware.vm.discovery[{$VMWARE.URL`
- W polach *User name* i *Password* wprowadź odpowiednie makra wcześniej skonfigurowane na hoście.



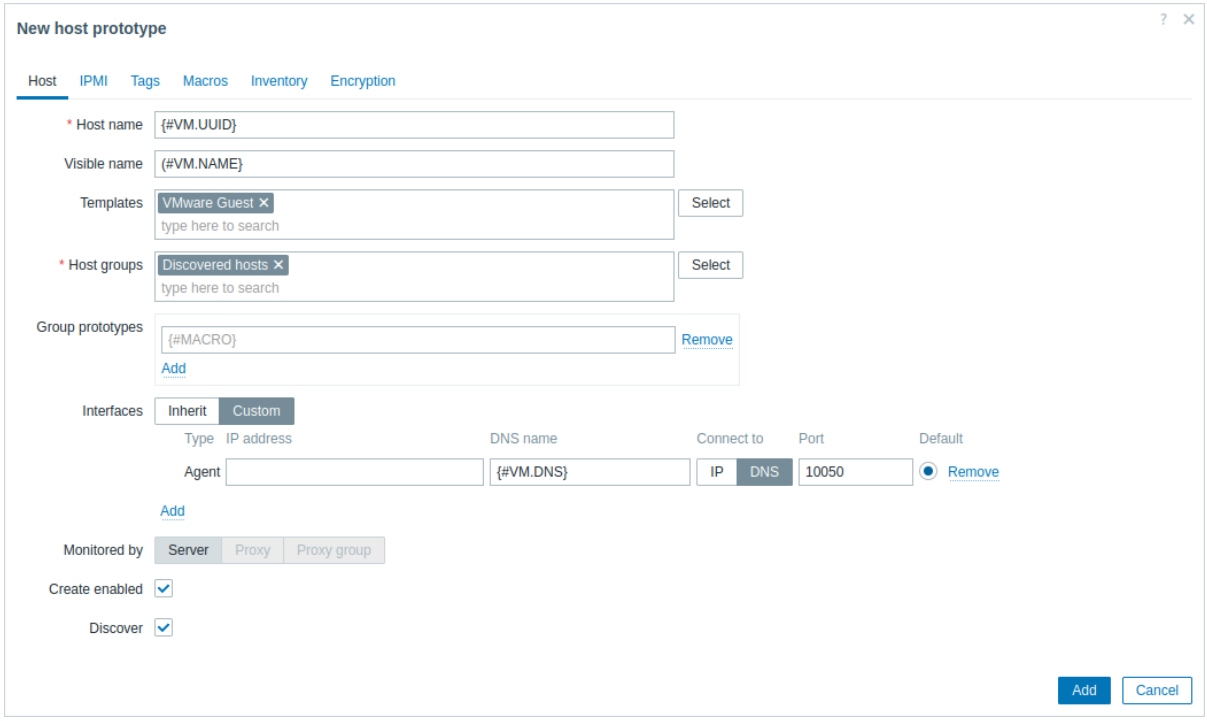
3. Kliknij przycisk *Add*, aby utworzyć regułę wykrywania niskiego poziomu. Ta reguła wykrywania wykryje maszyny wirtualne w Twoim środowisku VMware.

Utwórz prototyp hosta

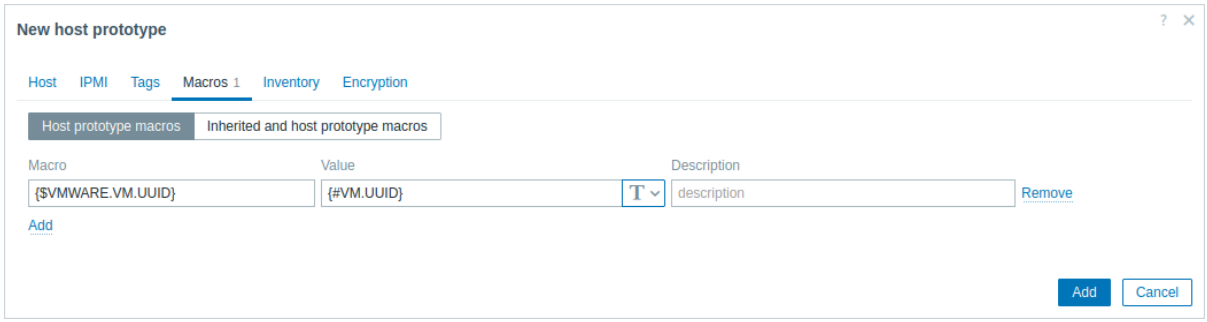
1. Na liście reguł wykrywania niskiego poziomu kliknij *Host prototypes* dla wcześniej utworzonej reguły wykrywania niskiego poziomu.

2. Utwórz prototyp hosta. Ponieważ prototypy hostów są wzorcami do tworzenia hostów za pomocą reguł wykrywania niskiego poziomu, większość pól będzie zawierać makra wykrywania niskiego poziomu. Zapewnia to tworzenie hostów z właściwościami opartymi na zawartości pobranej przez wcześniej utworzoną regułę wykrywania niskiego poziomu.

- W polu *Host name* wprowadź makro {#VM.UUID}.
- W polu *Visible name* wprowadź makro {#VM.NAME}.
- W polu *Templates* wprowadź lub wybierz szablon ”VMware Guest”. Ten szablon zawiera pozycje VMware oraz reguły wykrywania do monitorowania stanu zasilania maszyny wirtualnej, użycia CPU, użycia pamięci, urządzeń sieciowych itp.
- W polu *Host groups* wprowadź lub wybierz grupę hostów (na przykład ”Discovered hosts”).
- W polu *Interfaces* dodaj niestandardowy interfejs hosta. Następnie wprowadź makro {#VM.DNS} w polu *DNS name* lub wprowadź makro {#VM.IP} w polu *IP address*. Alternatywnie, jeśli maszyny wirtualne w Twoim środowisku VMware mają wiele interfejsów, przejdź do sekcji *Zaawansowana konfiguracja interfejsu hosta*. Skonfigurowanie niestandardowego interfejsu hosta jest konieczne do prawidłowego działania szablonu *VMware Guest*.



- Na karcie *Macros* ustaw makro {$VMWARE.VM.UUID} z wartością {#VM.UUID}. Jest to konieczne do prawidłowego działania szablonu *VMware Guest*, który używa tego makra jako makra użytkownika na poziomie hosta w parametrach pozycji (na przykład *vmware.vm.net.if.discovery[{$VMWARE.URL}, {$VMWARE.VM.UUID}]*).

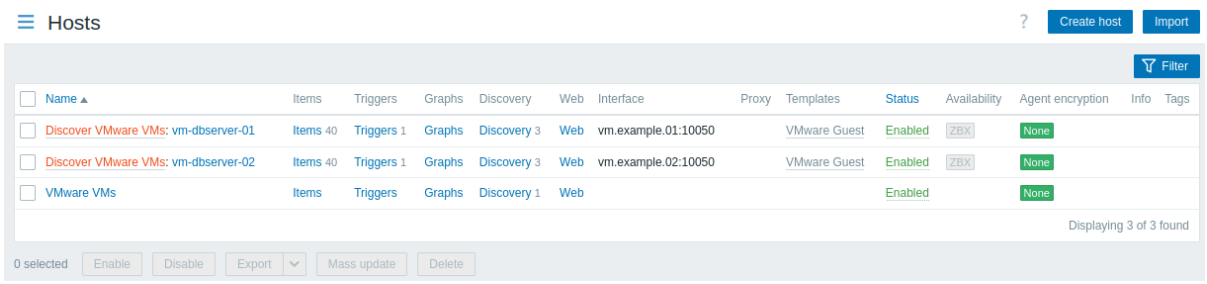


3. Kliknij przycisk *Add*, aby utworzyć prototyp hosta. Ten prototyp hosta będzie używany do tworzenia hostów dla maszyn wirtualnych wykrytych przez wcześniej utworzoną regułę wykrywania niskiego poziomu.

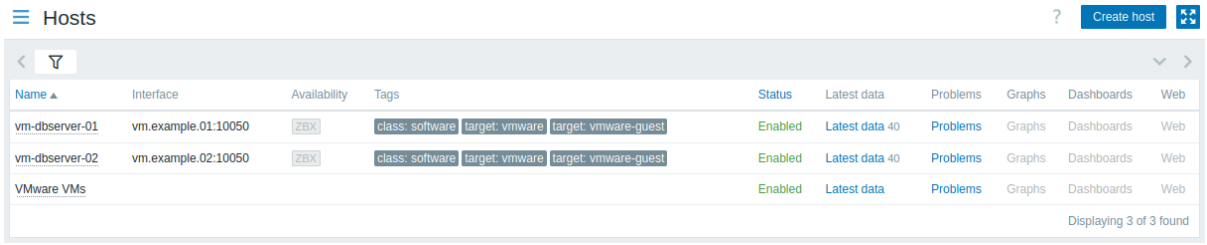
Wyświetlanie hostów i metryk

Po utworzeniu prototypu hosta reguła wykrywania niskiego poziomu utworzy hosty dla wykrytych maszyn wirtualnych VMware, a Zabbix rozpocznie ich monitorowanie. Należy pamiętać, że wykrywanie i tworzenie hostów można również wykonać ręcznie, jeśli to konieczne.

Aby wyświetlić utworzone hosty, przejdź do sekcji menu *Zbieranie danych → Hosty*.



Aby wyświetlić zebrane metryki, przejdź do sekcji menu *Monitorowanie → Hosty* i kliknij *Najnowsze dane* dla jednego z hostów.



Zaawansowana konfiguracja interfejsu hosta

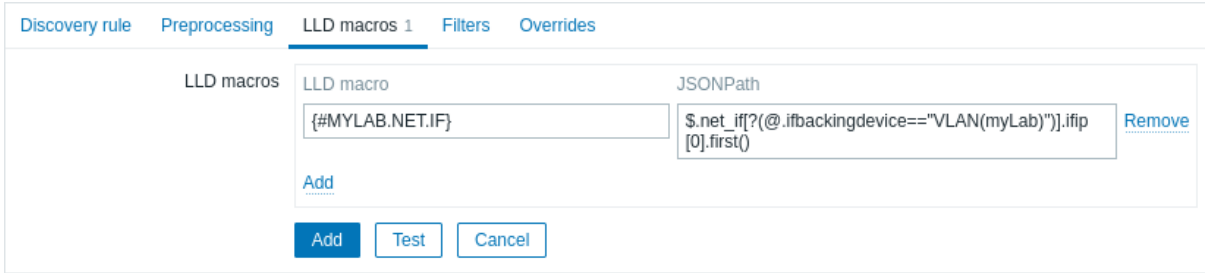
Klucz pozycji `vmware.vm.discovery[{$VMWARE.URL}]`, skonfigurowany w sekcji *Utwórz regułę wykrywania niskiego poziomu*, zwraca dane interfejsów sieciowych w polu "net_if":

```
"net_if": [
      {
        "ifname": "5000",
        "ifdesc": "Network adapter 1",
        "ifmac": "00:11:22:33:44:55",
        "ifconnected": true,
        "iftype": "VirtualVmxnet3",
        "ifbackingdevice": "VLAN(myLab)",
        "ifdvswitch_uuid": "",
        "ifdvswitch_portgroup": "",
        "ifdvswitch_port": "",
        "ifip": [
          "127.0.0.1",
          "::1"
        ]
      },
      {
        "ifname": "5001",
        "ifdesc": "Network adapter 2",
        "ifmac": "00:11:22:33:44:55",
        "ifconnected": false,
        "iftype": "VirtualVmxnet3",
        "ifbackingdevice": "VLAN(myLab2)",
        "ifdvswitch_uuid": "",
        "ifdvswitch_portgroup": "",
        "ifdvswitch_port": "",
        "ifip": []
      }
    ]
```

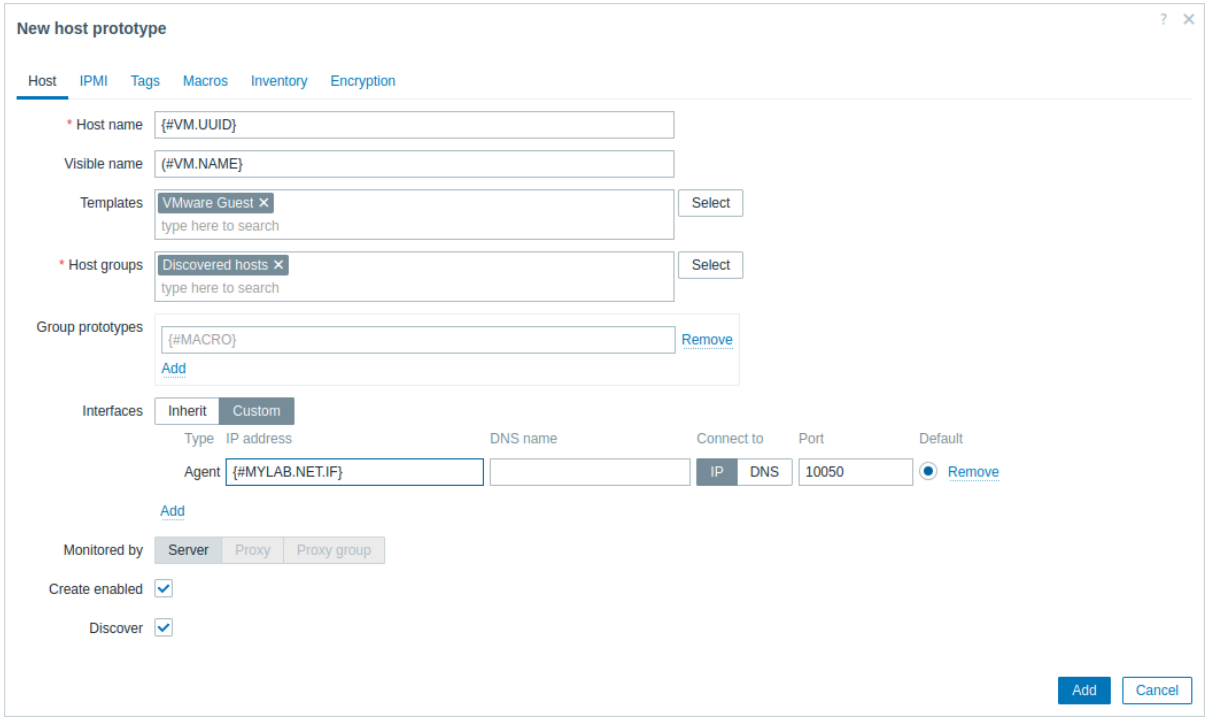
Dane te można wykorzystać do skonfigurowania niestandardowego interfejsu hosta.

1. Podczas tworzenia reguły wykrywania niskiego poziomu dodatkowo skonfiguruj makro wykrywania niskiego poziomu. Na karcie *Makra LLD* utwórz niestandardowe makro LLD z wartością JSONPath. Na przykład:

- `{#MYLAB.NET.IF}` - `$.net_if[?(@.ifbackingdevice=="VLAN(myLab)")].ifip[0].first()`



2. Podczas tworzenia prototypu hosta dodaj niestandardowy interfejs hosta i wprowadź makro LLD w polu *Nazwa DNS* lub *Adres IP*.



9 Konserwacja

Przegląd W Zabbix można definiować okresy konserwacji dla hostów i grup hostów.

Ponadto możliwe jest zdefiniowanie konserwacji tylko dla pojedynczego wyzwalacza (lub podzbioru wyzwalaczy) przez określenie tagów wyzwalacza. W takim przypadku konserwacja zostanie aktywowana tylko dla tych wyzwalaczy; wszystkie pozostałe wyzwalacze hosta lub grupy hostów nie będą objęte konserwacją.

Istnieją dwa typy konserwacji — z gromadzeniem danych oraz bez gromadzenia danych.

Podczas konserwacji „z gromadzeniem danych" wyzwalacze są przetwarzane jak zwykle, a zdarzenia są tworzone, gdy jest to wymagane. Jednak eskalacje problemów są wstrzymywane dla hostów/wyzwalaczy objętych konserwacją, jeśli w konfiguracji akcji zaznaczona jest opcja *Pause operations for suppressed problems*. W takim przypadku kroki eskalacji, które mogą obejmować wysyłanie powiadomień lub zdalnych poleceń, będą ignorowane tak długo, jak trwa okres konserwacji. Należy pamiętać, że operacje przywrócenia problemu i aktualizacji nie są wstrzymywane podczas konserwacji — wstrzymywane są tylko eskalacje.

Na przykład, jeśli kroki eskalacji są zaplanowane na 0, 30 i 60 minut po wystąpieniu problemu, a półgodzinna konserwacja trwa od 10 do 40 minuty po pojawieniu się rzeczywistego problemu, kroki drugi i trzeci zostaną wykonane pół godziny później, czyli po 60 i 90 minutach (o ile problem nadal istnieje). Podobnie, jeśli problem pojawi się podczas konserwacji, eskalacja rozpocznie się po zakończeniu konserwacji.

Aby otrzymywać powiadomienia o problemach podczas konserwacji normalnie (bez opóźnienia), należy odznaczyć opcję *Pause operations for suppressed problems* w konfiguracji akcji.

> **Note:**
> Jeśli co najmniej jeden host (użyty w wyrażeniu wyzwalacza) nie jest w trybie konserwacji, Zabbix wyśle powiadomienie o problemie.

serwer Zabbix musi działać podczas konserwacji. Konserwacje są przeliczane co minutę lub natychmiast po przeładowaniu pamięci podręcznej konfiguracji, jeśli wprowadzono zmiany w okresie konserwacji.

Procesy timera sprawdzają, czy status hosta powinien zostać zmieniony na/z trybu konserwacji o 0 sekundzie każdej minuty. Dodatkowo co sekundę proces timera sprawdza, czy jakiekolwiek konserwacje powinny zostać uruchomione/zatrzymane na podstawie zmian w [okresach konserwacji] po aktualizacji konfiguracji. Dlatego szybkość uruchamiania/zatrzymywania okresów konserwacji zależy od interwału aktualizacji konfiguracji (domyślnie 10 sekund). Należy pamiętać, że zmiany okresu konserwacji nie obejmują ustawień *Active since/Active till*. Ponadto, jeśli host/grupa hostów zostanie dodana do istniejącego aktywnego okresu konserwacji, zmiany zostaną aktywowane przez proces timera dopiero na początku następnej minuty.

Należy pamiętać, że gdy host przechodzi w tryb konserwacji, procesy timera serwera Zabbix odczytają wszystkie otwarte problemy, aby sprawdzić, czy wymagają one wyciszenia. Może to mieć wpływ na wydajność, jeśli istnieje wiele otwartych problemów. serwer

Zabbix odczyta również wszystkie otwarte problemy podczas uruchamiania, nawet jeśli w danym momencie nie skonfigurowano żadnych konserwacji.

Należy pamiętać, że serwer Zabbix (lub proxy) zawsze zbiera dane niezależnie od typu konserwacji (w tym konserwacji „bez danych"). Dane są później ignorowane przez serwer, jeśli ustawiono opcję „bez gromadzenia danych".

Po zakończeniu konserwacji „bez danych" wyzwalacze używające funkcji nodata() nie uruchomią się przed następnym sprawdzeniem w okresie, który sprawdzają.

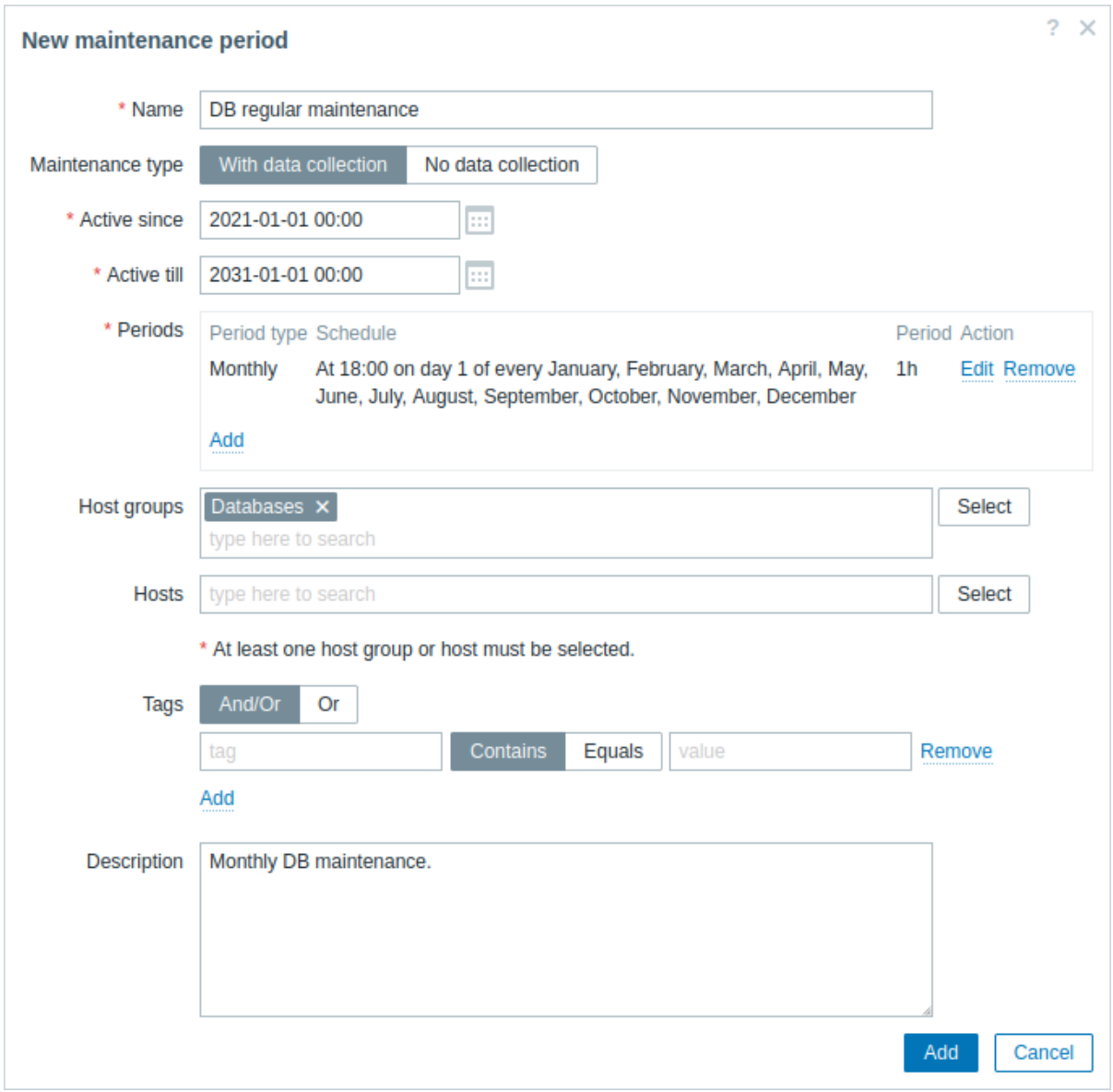
Jeśli pozycja logu zostanie dodana, gdy host jest w trakcie konserwacji, a konserwacja się zakończy, zostaną zebrane tylko nowe wpisy pliku dziennika od momentu zakończenia konserwacji.

Jeśli wartość ze znacznikiem czasu zostanie wysłana dla hosta, który znajduje się w konserwacji typu „bez danych" (np. przy użyciu Zabbix sender), wartość ta zostanie odrzucona, jednak możliwe jest wysłanie wartości ze znacznikiem czasu dla wygasłego okresu konserwacji i zostanie ona zaakceptowana.

Jeśli okres konserwacji, hosty, grupy lub tagi zostaną zmienione przez użytkownika, zmiany zaczną obowiązywać dopiero po synchronizacji pamięci podręcznej konfiguracji.

Konfiguracja Aby skonfigurować okres konserwacji:

1. Przejdź do: *Data collection* > *Maintenance*.
2. Kliknij *Create maintenance period* (lub nazwę istniejącego okresu konserwacji).
3. Wprowadź parametry konserwacji w formularzu.

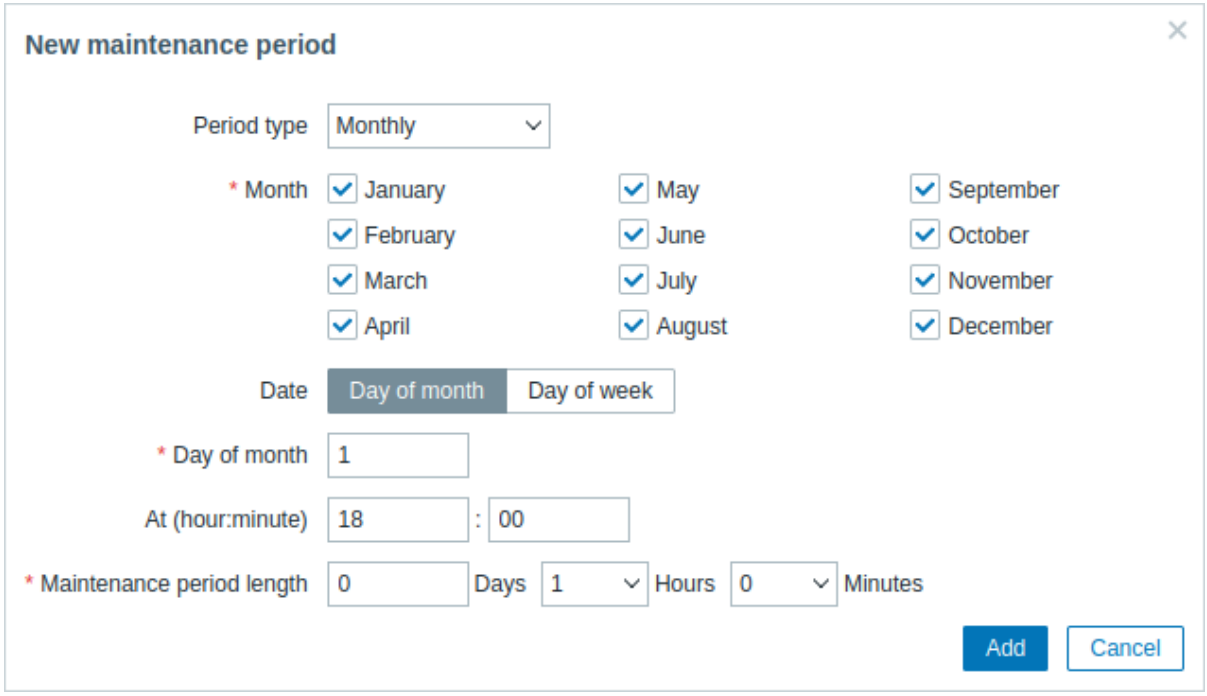


Wszystkie wymagane pola wejściowe są oznaczone czerwoną gwiazdką.

Parametr	Opis
Name	Nazwa okresu konserwacji.
Maintenance type	Można ustawić dwa typy konserwacji: **With data collection** - dane będą zbierane przez serwer podczas konserwacji, wyzwalacze będą przetwarzane; **No data collection** - dane nie będą zbierane przez serwer podczas konserwacji. Zobacz Wpływ okresów konserwacji, aby dowiedzieć się, jak każdy typ wpływa na raport dostępności.
Active since	Data i godzina, od których wykonywanie okresów konserwacji staje się aktywne. *Uwaga:* Ustawienie tylko tego czasu nie aktywuje okresu konserwacji; okresy konserwacji muszą być skonfigurowane w sekcji *Periods* (patrz poniżej).
Active till	Data i godzina, do których wykonywanie okresów konserwacji pozostaje aktywne.
Periods	Ten blok umożliwia zdefiniowanie dokładnych dni i godzin, w których odbywa się konserwacja. Kliknięcie Add otwiera wyskakujące okno z elastycznym formularzem *Maintenance period*, w którym można zdefiniować harmonogram konserwacji. Szczegółowy opis znajduje się w sekcji Okresy konserwacji.
Host groups	Wybierz grupy hostów, dla których konserwacja będzie aktywowana. Konserwacja zostanie aktywowana dla wszystkich hostów z określonych grup hostów. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania zostanie wyświetlona lista rozwijana wszystkich dostępnych grup hostów. Określenie nadrzędnej grupy hostów powoduje niejawne wybranie wszystkich zagnieżdżonych grup hostów. W rezultacie konserwacja zostanie również aktywowana dla hostów z grup zagnieżdżonych.
Hosts	Wybierz hosty, dla których konserwacja będzie aktywowana. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania zostanie wyświetlona lista rozwijana wszystkich dostępnych hostów.
Tags	Określ tagi, aby ukryć problemy z pasującymi tagami na hostach objętych konserwacją. Można ustawić kilka warunków. Dopasowanie nazw tagów zawsze uwzględnia wielkość liter. Dla każdego warunku dostępne są dwa operatory: **Contains** - uwzględnij określone nazwy tagów, których wartości tagów zawierają wprowadzony ciąg (dopasowanie podciągu, z uwzględnieniem wielkości liter); **Equals** - uwzględnij określone nazwy i wartości tagów (z uwzględnieniem wielkości liter). Dostępne są dwa typy obliczania warunków: **And/Or** - wszystkie warunki muszą być spełnione, warunki mające tę samą nazwę tagu będą grupowane operatorem Or; **Or** - wystarczy spełnienie jednego warunku. Tagi można określać tylko wtedy, gdy wybrany jest tryb *With data collection*.
Description	Opis okresu konserwacji.

Okresy konserwacji

Okno okresu konserwacji służy do planowania czasu dla cyklicznej lub jednorazowej konserwacji. Formularz jest dynamiczny, a dostępne pola zmieniają się w zależności od wybranego *Typu okresu*.



Typ okresu	Opis
Tylko jednorazowo	Skonfiguruj jednorazowy okres konserwacji: *Data* - data i godzina okresu konserwacji; *Długość okresu konserwacji* - jak długo konserwacja będzie aktywna.
Codziennie	Skonfiguruj codzienny okres konserwacji: *Co ile dni* - częstotliwość konserwacji (1 - *(domyślnie)* codziennie, 2 - co dwa dni itd.); *O (godzina:minuta)* - pora dnia, o której rozpoczyna się konserwacja; *Długość okresu konserwacji* - jak długo konserwacja będzie aktywna. Gdy parametr *Co ile dni* jest większy niż „1”, dniem początkowym jest dzień, na który przypada czas *Aktywne od*. Przykłady: - jeśli *Aktywne od* ustawiono na „2021-01-01 12:00”, *Co ile dni* ustawiono na „2”, a *O (godzina:minuta)* ustawiono na „23:00”, to pierwszy okres konserwacji rozpocznie się 1 stycznia o 23:00, a drugi okres konserwacji rozpocznie się 3 stycznia o 23:00; - jeśli *Aktywne od* ustawiono na „2021-01-01 12:00”, *Co ile dni* ustawiono na „2”, a *O (godzina:minuta)* ustawiono na „01:00”, to pierwszy okres konserwacji rozpocznie się 3 stycznia o 01:00, a drugi okres konserwacji rozpocznie się 5 stycznia o 01:00.
Co tydzień	Skonfiguruj tygodniowy okres konserwacji: *Co ile tygodni* - częstotliwość konserwacji (1 - *(domyślnie)* co tydzień, 2 - co dwa tygodnie itd.); *Dzień tygodnia* - dzień, w którym ma odbywać się konserwacja; *O (godzina:minuta)* - pora dnia, o której rozpoczyna się konserwacja; *Długość okresu konserwacji* - jak długo konserwacja będzie aktywna. Gdy parametr *Co ile tygodni* jest większy niż „1”, tygodniem początkowym jest tydzień, na który przypada czas *Aktywne od*. Przykłady można znaleźć w opisie parametru *Codziennie* powyżej.
Co miesiąc	Skonfiguruj miesięczny okres konserwacji: *Miesiąc* - wybierz wszystkie miesiące, w których wykonywana jest regularna konserwacja; *Data:* ***Dzień miesiąca*** - wybierz tę opcję, jeśli konserwacja ma odbywać się tego samego dnia każdego miesiąca (na przykład każdego 1. dnia miesiąca), a następnie wybierz wymagany dzień w polu *Dzień miesiąca*, które się pojawi; *Data:* ***Dzień tygodnia*** - wybierz tę opcję, jeśli konserwacja ma odbywać się tylko w określone dni (na przykład w każdy pierwszy poniedziałek miesiąca), a następnie wybierz (z listy rozwijanej) wymagany tydzień miesiąca (pierwszy, drugi, trzeci, czwarty lub ostatni), po czym zaznacz pola wyboru dla dnia/dni konserwacji; *O (godzina:minuta)* - pora dnia, o której rozpoczyna się konserwacja; *Długość okresu konserwacji* - jak długo konserwacja będzie aktywna.

Attention:
Podczas tworzenia okresu utrzymania używana jest strefa czasowa użytkownika, który go tworzy. Jednak gdy planowane są cykliczne okresy utrzymania (*Codziennie*, *Co tydzień*, *Co miesiąc*), używana jest strefa czasowa serwera Zabbix. Aby zapewnić przewidywalne działanie cyklicznych okresów utrzymania, należy używać wspólnej strefy czasowej we wszystkich częściach Zabbix.

Po zakończeniu naciśnij *Dodaj*, aby dodać okres konserwacji do bloku *Okresy*.

Należy pamiętać, że zmiany czasu letniego (DST) nie wpływają na długość trwania konserwacji. Na przykład załóżmy, że mamy skonfigurowaną dwugodzinną konserwację, która zwykle rozpoczyna się o 01:00 i kończy o 03:00:

- jeśli po jednej godzinie konserwacji (o 02:00) nastąpi zmiana czasu letniego i bieżący czas zmieni się z 02:00 na 03:00, konserwacja będzie kontynuowana jeszcze przez jedną godzinę (do 04:00);
- jeśli po dwóch godzinach konserwacji (o 03:00) nastąpi zmiana czasu letniego i bieżący czas zmieni się z 03:00 na 02:00, konserwacja zostanie zatrzymana, ponieważ minęły dwie godziny;
- jeśli okres konserwacji rozpoczyna się w godzinie pomijanej z powodu zmiany czasu letniego, konserwacja nie rozpocznie się.

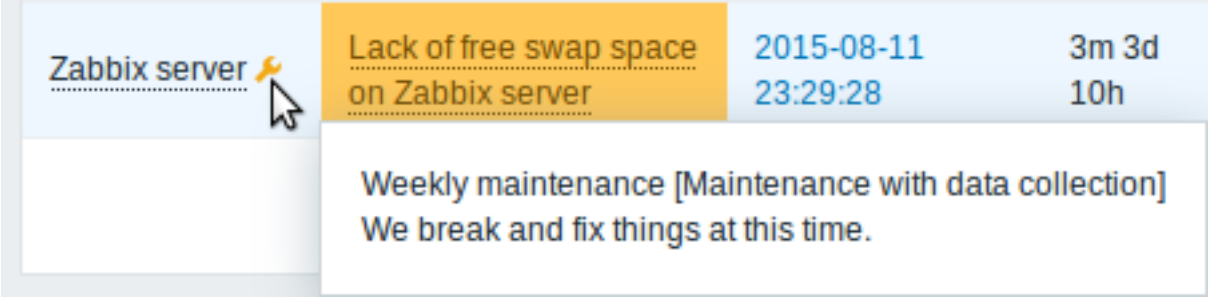
Jeśli okres konserwacji jest ustawiony na „1 dzień" (rzeczywisty okres konserwacji wynosi 24 godziny, ponieważ Zabbix oblicza dni w godzinach), rozpoczyna się o 00:00 i kończy o 00:00 następnego dnia:

- konserwacja zakończy się o 01:00 następnego dnia, jeśli bieżący czas zostanie przesunięty do przodu o jedną godzinę;
- konserwacja zakończy się o 23:00 tego dnia, jeśli bieżący czas zostanie cofnięty o jedną godzinę.

Wyświetlanie Wyświetlanie hostów w konserwacji

Pomarańczowa ikona klucza obok nazwy hosta wskazuje, że ten host jest w konserwacji w:

- *Dashboardach*
- *Monitoring* > *Problemy*
- *Inwentaryzacja* > *Hosty* > *Szczegóły inwentaryzacji hosta*
- *Zbieranie danych* > *Hosty* (zobacz kolumnę „Status")



Szczegóły konserwacji są wyświetlane po umieszczeniu wskaźnika myszy nad ikoną.

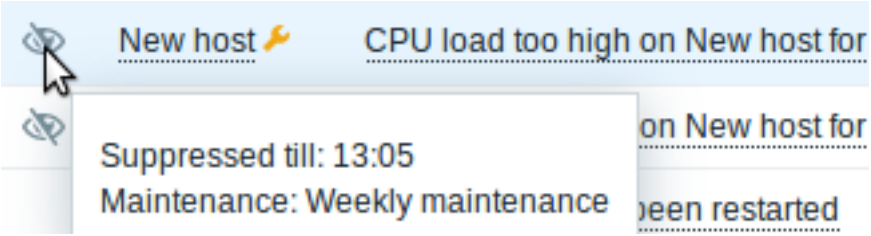
Dodatkowo hosty w konserwacji mają pomarańczowe tło w *Monitoring* > *Mapy*.

Wyświetlanie stłumionych problemów

Zwykle problemy dla hostów w konserwacji są stłumione, tj. nie są wyświetlane we frontend. Można jednak również skonfigurować wyświetlanie stłumionych problemów, wybierając opcję *Pokaż stłumione problemy* w następujących miejscach:

- *Pulpity* (w konfiguracji widżetów *Hosty z problemami*, *Problemy*, *Problemy według ważności*, *Przegląd wyzwalaczy*)
- *Monitorowanie* > *Problemy* (w filtrze)
- *Monitorowanie* > *Mapy* (w konfiguracji mapy)
- Globalne powiadomienia (w konfiguracji profilu użytkownika)

Gdy stłumione problemy są wyświetlane, pokazywana jest następująca ikona: . Najechanie kursorem myszy na ikonę powoduje wyświetlenie dodatkowych szczegółów.



Obliczanie kolejek podczas konserwacji Kolejki wyświetlane w frontendzie Zabbix (Administration > Queue) są obliczane przez serwer Zabbix. Nie obejmują one pozycji objętych konserwacją bez zbierania danych — długość kolejki dla tych pozycji jest zawsze równa zero, nawet jeśli ich wartości są opóźnione. Opóźnione pozycje w konserwacji ze zbieraniem danych są nadal uwzględniane w kolejce.

Zabbix proxy nie jest świadomy okresów konserwacji, ponieważ nie ma synchronizacji konfiguracji konserwacji między serwerem Zabbix a proxy. Kontrole wewnętrzne obliczane na proxy Zabbix (na przykład `zabbix[queue,,]` i `zabbix[stats,,,queue,,]`) zgłaszają opóźnione pozycje niezależnie od statusu konserwacji na serwerze Zabbix.

W rezultacie frontend Zabbix i kontrole wewnętrzne na proxy Zabbix mogą raportować różne długości kolejek dla tych samych pozycji objętych konserwacją bez zbierania danych.

10 Wyrażenia regularne

Przegląd Wyrażenia regularne zgodne z Perlem (PCRE, PCRE2) są obsługiwane w Zabbix.

Istnieją dwa sposoby używania wyrażeń regularnych w Zabbix:

- ręczne wprowadzanie wyrażenia regularnego
- użycie globalnego wyrażenia regularnego utworzonego w Zabbix

Wyrażenia regularne W obsługiwanych miejscach można ręcznie wprowadzić wyrażenie regularne. Należy pamiętać, że wyrażenie nie może zaczynać się od znaku @, ponieważ symbol ten jest używany w Zabbix do odwoływania się do globalnych wyrażeń regularnych.

> **Warning:**
> Podczas używania wyrażeń regularnych może dojść do przepełnienia stosu. Więcej informacji można znaleźć na stronie podręcznika pcrestack man page.

Należy pamiętać, że przy dopasowywaniu wielowierszowym kotwice ^ i $ dopasowują się odpowiednio do początku/końca każdej linii, a nie do początku/końca całego ciągu znaków.

Zobacz także przykłady poprawnego użycia znaków ucieczki w różnych kontekstach.

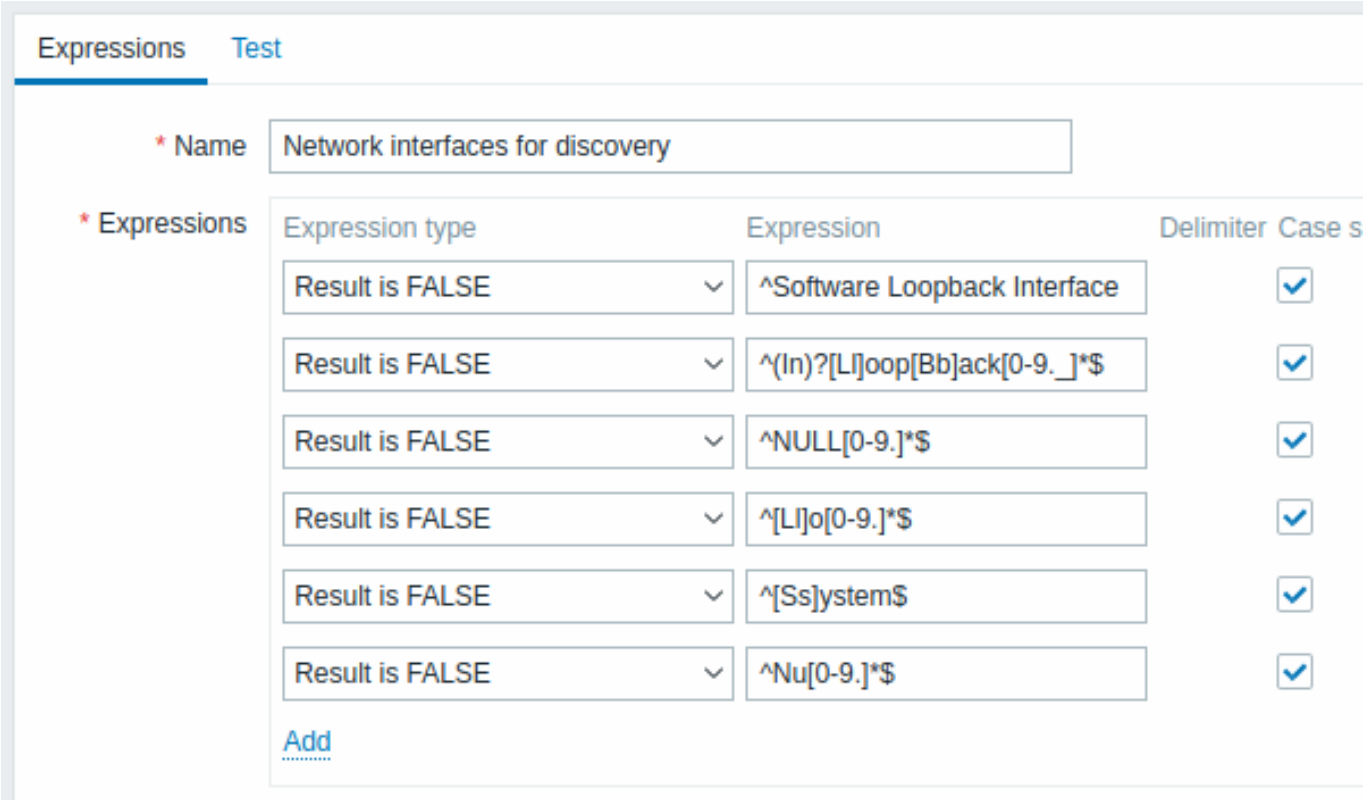
Globalne wyrażenia regularne W Zabbix frontend dostępny jest zaawansowany edytor do tworzenia i testowania złożonych wyrażeń regularnych.

Po utworzeniu wyrażenia regularnego w ten sposób można go używać w kilku miejscach we frontend, odwołując się do jego nazwy poprzedzonej znakiem @, na przykład *@mycustomregexp*.

Aby utworzyć globalne wyrażenie regularne:

- Przejdź do: *Administration* → *General*
- Wybierz *Regular expressions* z listy rozwijanej
- Kliknij *New regular expression*

Karta **Expressions** umożliwia ustawienie nazwy wyrażenia regularnego i dodanie podwyrażeń.



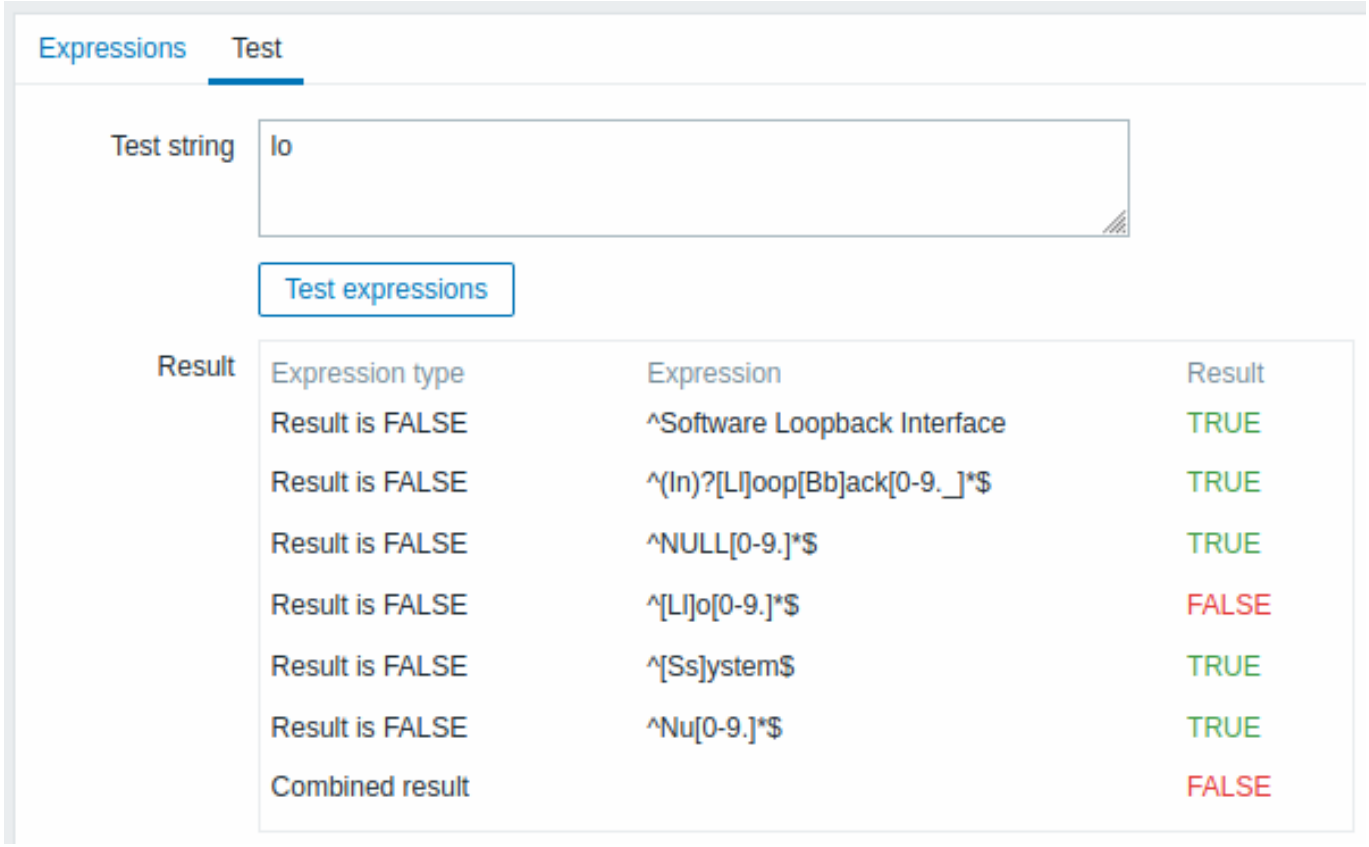
Wszystkie wymagane pola wejściowe są oznaczone czerwoną gwiazdką.

Parameter	Description
Name	Ustaw nazwę wyrażenia regularnego. Dozwolone są dowolne znaki Unicode.
Expressions	Kliknij *Add* w bloku Expressions, aby dodać nowe podwyrażenie.
Expression type	Wybierz typ wyrażenia: **Character string included** - dopasowuje podciąg **Any character string included** - dopasowuje dowolny podciąg z listy rozdzielanej separatorem. Lista rozdzielana separatorem może zawierać przecinek (,), kropkę (.) lub ukośnik (/). **Character string not included** - dopasowuje dowolny ciąg z wyjątkiem podciągu **Result is TRUE** - dopasowuje wyrażenie regularne **Result is FALSE** - nie dopasowuje wyrażenia regularnego
Expression	Wprowadź podciąg/wyrażenie regularne.
Delimiter	Przecinek (,), kropka (.) lub ukośnik (/) służące do rozdzielania ciągów tekstowych w wyrażeniu regularnym. Ten parametr jest aktywny tylko wtedy, gdy wybrano typ wyrażenia *"Any character string included"*.
Case sensitive	Pole wyboru określające, czy wyrażenie regularne rozróżnia wielkość liter.

Ukośnik (/) w wyrażeniu jest traktowany dosłownie, a nie jako separator. Dzięki temu można zapisywać wyrażenia zawierające ukośnik bez błędów.

Attention:
Niestandardowa nazwa wyrażenia regularnego w Zabbix może zawierać przecinki, spacje itd. W przypadkach, gdy może to prowadzić do błędnej interpretacji podczas odwoływania się do niej (na przykład przecinek w parametrze klucza pozycji), całe odwołanie można ująć w cudzysłów w następujący sposób: *"@My custom regexp for purpose1, purpose2"*.
Nazwy wyrażeń regularnych nie mogą być ujmowane w cudzysłów w innych miejscach (na przykład we właściwościach reguły LLD).

Na karcie **Test** wyrażenie regularne i jego podwyrażenia można przetestować, podając ciąg testowy.



Wyniki pokazują status każdego podwyrażenia oraz łączny status niestandardowego wyrażenia.

Łączny status niestandardowego wyrażenia jest określany jako *Combined result*. Jeśli zdefiniowano kilka podwyrażeń, Zabbix używa operatora logicznego AND do obliczenia *Combined result*. Oznacza to, że jeśli co najmniej jeden wynik ma wartość False, *Combined result* również ma status False.

Domyślne globalne wyrażenia regularne Zabbix zawiera kilka globalnych wyrażeń regularnych w swoim domyślnym zestawie danych.

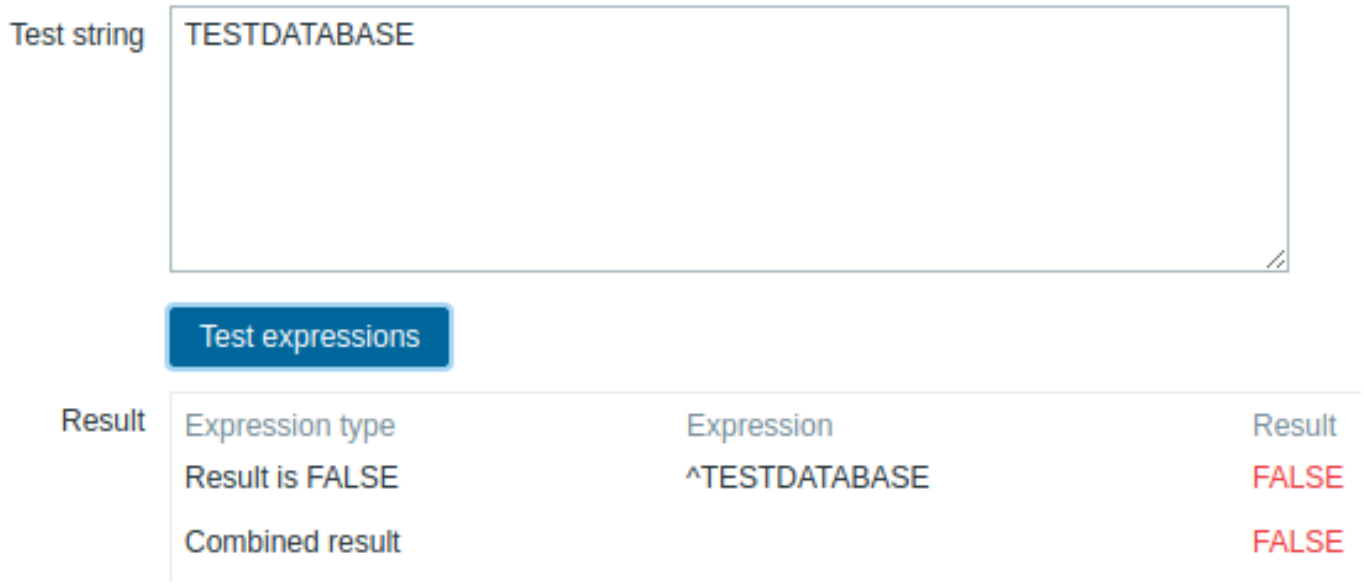
Name	Expression	Matches
Systemy plików do wykrywania	`^(btrfs|ext2|ext3|ext4|jfs|reiser|xfs|ffs|ufs|jfs|jfs2|vxfs|hfs|refs|apfs|ntfs|fat32|zfs)$`	”btrfs” lub ”ext2” lub ”ext3” lub ”ext4” lub ”jfs” lub ”reiser” lub ”xfs” lub ”ffs” lub ”ufs” lub ”jfs” lub ”jfs2” lub ”vxfs” lub ”hfs” lub ”refs” lub ”apfs” lub ”ntfs” lub ”fat32” lub ”zfs”
Interfejsy sieciowe do wykrywania	`^Software Loopback Interface`	Ciągi znaków zaczynające się od ”Software Loopback Interface”.
	`^lo$`	”lo”
	`^(In)?[Ll]oop[Bb]ack[0-9._]*$`	Ciągi znaków, które opcjonalnie zaczynają się od ”In”, następnie mają ”L” lub ”l”, potem ”oop”, następnie ”B” lub ”b”, potem ”ack”, po czym opcjonalnie może występować dowolna liczba cyfr, kropek lub podkreśleń.
	`^NULL[0-9.]*$`	Ciągi znaków zaczynające się od ”NULL”, po których opcjonalnie występuje dowolna liczba cyfr lub kropek.
	`^[Ll]o[0-9.]*$`	Ciągi znaków zaczynające się od ”Lo” lub ”lo”, po których opcjonalnie występuje dowolna liczba cyfr lub kropek.
	`^[Ss]ystem$`	”System” lub ”system”
	`^Nu[0-9.]*$`	Ciągi znaków zaczynające się od ”Nu”, po których opcjonalnie występuje dowolna liczba cyfr lub kropek.

Name	Expression	Matches
Urządzenia pamięci masowej do wykrywania SNMP	`^(Physical memory|Virtual memory|Memory buffers|Cached memory|Swap space)$`	”Physical memory” lub ”Virtual memory” lub ”Memory buffers” lub ”Cached memory” lub ”Swap space”
Nazwy usług Windows do wykrywania	`^(MMCSS|gupdate|SysmonLog|clr_optimization_v4.0.30319_32)$`	”MMCSS”, ”gupdate” lub ”SysmonLog” lub ciągi znaków takie jak ”clr_optimization_v2.0.50727_32” i ”clr_optimization_v4.0.30319_32”, gdzie zamiast kropek można wstawić dowolny znak z wyjątkiem znaku nowej linii.
Stany uruchamiania usług Windows do wykrywania	`^(automatic|automatic delayed)$`	”automatic” lub ”automatic delayed”

Przykłady Przykład 1

Użycie następującego wyrażenia w wykrywaniu niskiego poziomu do wykrywania baz danych z wyjątkiem bazy danych o określonej nazwie:

`^TESTDATABASE$`

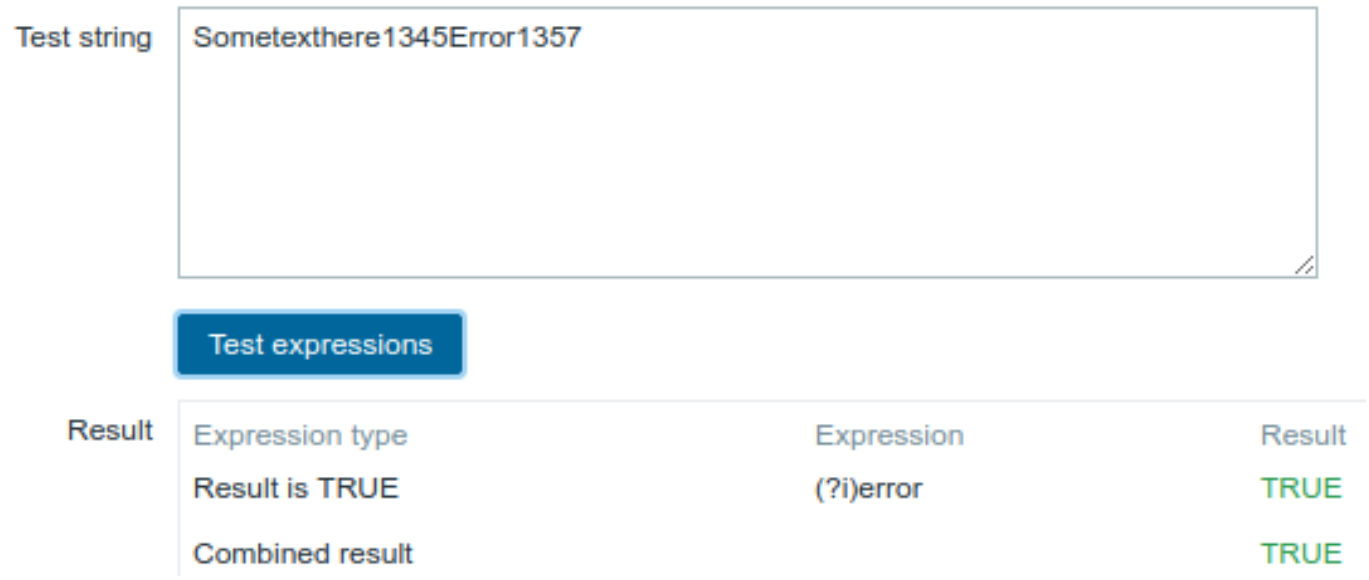


Wybrany *Typ wyrażenia*: „Wynik to FALSE”. Nie pasuje do nazwy zawierającej ciąg „*TESTDATABASE*”.

Przykład z modyfikatorem regex w linii

Użycie następującego wyrażenia regularnego, zawierającego modyfikator w linii (?i), do dopasowania znaków „error”:

`(?i)error`



Wybrany *Typ wyrażenia*: „Wynik to TRUE”. Znaki „error” są dopasowane.

Kolejny przykład z modyfikatorem regex inline

Użycie następującego wyrażenia regularnego zawierającego wiele modyfikatorów inline do dopasowania znaków po określonej linii:

```
(?<=match (?i)everything(?-i) after this line\n)(?sx).*# dodajemy modyfikator s, aby umożliwić dopasowanie
```



Wybrany typ wyrażenia: „Wynik to TRUE”. Znaki po określonej linii są dopasowywane.

Attention:
Modyfikator **g** nie może być określony w linii. Lista dostępnych modyfikatorów znajduje się na stronie podręcznika pcresyntax. Więcej informacji o składni PCRE można znaleźć w dokumentacji HTML PCRE.

Obsługa wyrażeń regularnych według lokalizacji

Lokalizacja	Wyrażenie regularne	Globalne wyrażenie regularne	Dopasowanie wielowierszowe	Komentarze
Pozycje agenta				
eventlog[]	Tak	Tak	Tak	parametry `regexp`, `severity`, `source`, `eventid`
eventlog.count[]				parametry `regexp`, `severity`, `source`, `eventid`
log[]				parametr `regexp`
log.count[]				
logrt[]		Tak/Nie		parametr `regexp` obsługuje oba typy, parametr `file_regexp` obsługuje tylko wyrażenia nieglobalne
logrt.count[]				

Lokalizacja	Wyrażenie regularne	Globalne wyrażenie regularne	Dopasowanie wielowierszowe	Komentarze
proc.cpu.util[]		Nie	Nie	parametr `cmdline`
proc.get[]				
proc.mem[]				
proc.num[]				
sensor[]				parametry `device` i `sensor` w systemie Linux 2.4
system.hw.macaddr[]				parametr `interface`
system.sw.packages[]				parametr `regexp`
system.sw.packages.get[]				parametr `regexp`
vfs.dir.count[]				parametry `regex_incl`, `regex_excl`, `regex_excl_dir`
vfs.dir.get[]				parametry `regex_incl`, `regex_excl`, `regex_excl_dir`
vfs.dir.size[]				parametry `regex_incl`, `regex_excl`, `regex_excl_dir`
vfs.file.regexp[]			Tak	parametr `regexp`
vfs.file.regmatch[]				
web.page.regexp[]				
Pułapki SNMP				
snmptrap[]	Tak	Tak	Nie	parametr `regexp`
Wstępne przetwarzanie wartości pozycji	Tak	Nie	Nie	parametr `pattern`
Funkcje dla wyzwalaczy/pozycji obliczanych				
count()	Tak	Tak	Tak	parametr `pattern`, jeśli parametr `operator` ma wartość *regexp* lub *iregexp*
countunique()	Tak	Tak		
find()	Tak	Tak		
logeventid()	Tak	Tak	Nie	parametr `pattern`
logsource()				
Wykrywanie niskiego poziomu				
Filtry	Tak	Tak	Nie	pole *Regular expression*
Nadpisania	Tak	Nie		W opcjach *matches*, *does not match* dla warunków *Operation*
Warunki akcji	Tak	Nie	Nie	W opcjach *matches*, *does not match* dla warunków autorejestracji *Host name* i *Host metadata*
Skrypty	Tak	Tak	Nie	pole *Input validation rule*
Monitorowanie WWW	Tak	Nie	Tak	*Variables* z prefiksem **regex:** pole *Required string*
Kontekst makra użytkownika	Tak	Nie	Nie	W kontekście makra z prefiksem **regex:**
Funkcje makr				
regsub()	Tak	Nie	Nie	parametr `pattern`
iregsub()				

Lokalizacja	Wyrażenie regularne	Globalne wyrażenie regularne	Dopasowanie wielowierszowe	Komentarze
Wskaźniki łączy na mapach	Tak	Nie	Nie	pole *Pattern* (dla pozycji tekstowych)
Mapowanie ikon	Tak	Tak	Nie	pole *Expression*
Mapowanie wartości	Tak	Nie	Nie	pole *Value*, jeśli typ mapowania to `regexp`

11 Potwierdzanie problemu

Przegląd Zdarzenia problemów w Zabbix mogą być potwierdzane przez użytkowników.

Jeśli użytkownik otrzyma powiadomienie o zdarzeniu problemu, może przejść do frontend Zabbix, otworzyć wyskakujące okno aktualizacji problemu dla tego problemu, korzystając z jednego ze sposobów wymienionych poniżej, i potwierdzić problem. Podczas potwierdzania może dodać komentarz, informując, że pracuje nad problemem lub wpisując cokolwiek innego, co uzna za stosowne.

Dzięki temu, jeśli inny użytkownik systemu zauważy ten sam problem, od razu zobaczy, czy został on potwierdzony, oraz dotychczasowe komentarze.

W ten sposób proces rozwiązywania problemów przez więcej niż jednego użytkownika systemu może przebiegać w skoordynowany sposób.

Status potwierdzenia jest również używany podczas definiowania operacji akcji. Można na przykład zdefiniować, że powiadomienie zostanie wysłane do menedżera wyższego szczebla tylko wtedy, gdy zdarzenie nie zostanie potwierdzone przez pewien czas.

Aby potwierdzać zdarzenia i komentować je, użytkownik musi mieć co najmniej uprawnienia do odczytu dla odpowiednich wyzwalaczy. Aby zmienić ważność problemu lub zamknąć problem, użytkownik musi mieć uprawnienia do odczytu i zapisu dla odpowiednich wyzwalaczy.

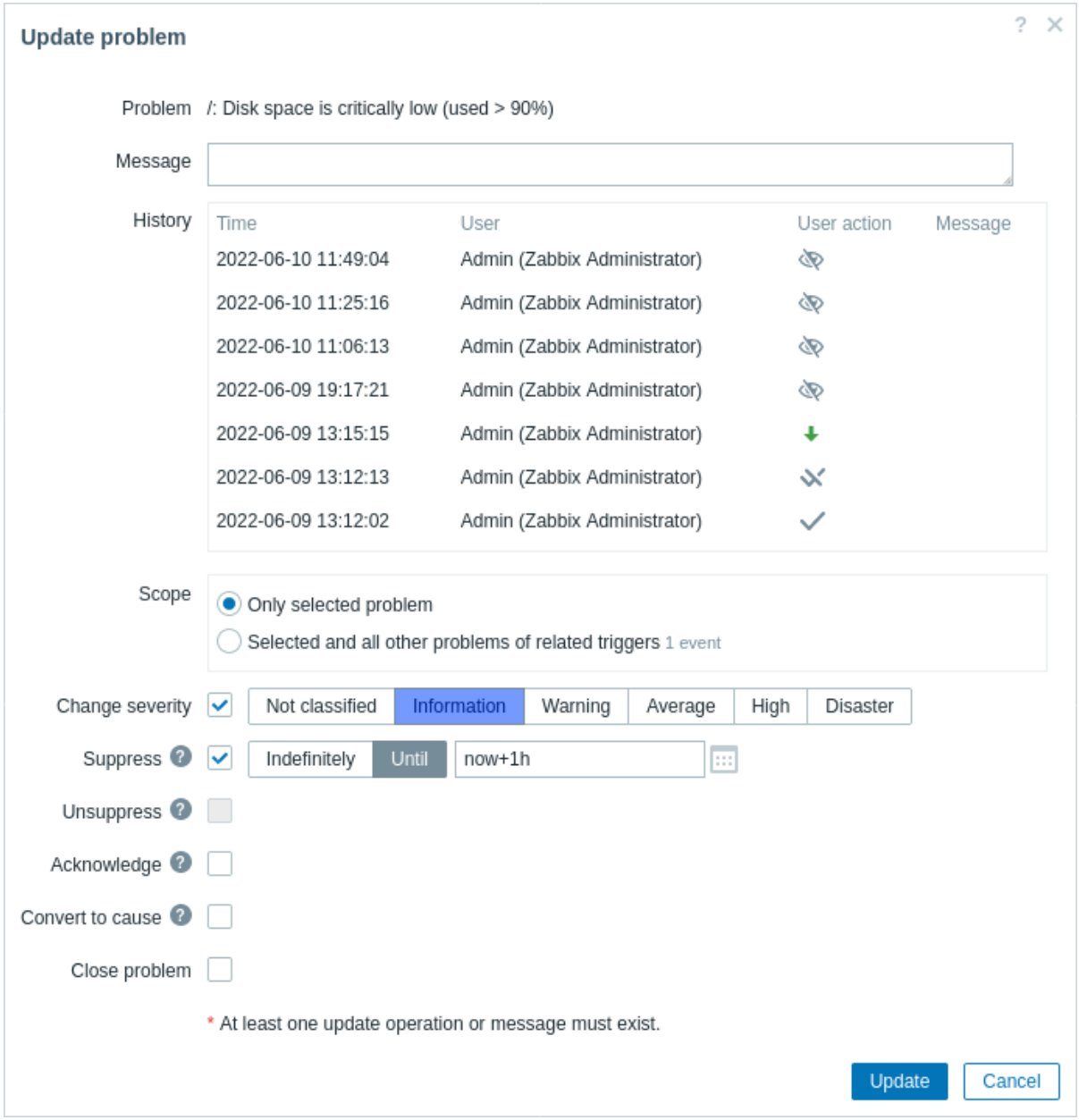
Istnieje **kilka** sposobów uzyskania dostępu do wyskakującego okna aktualizacji problemu, które umożliwia potwierdzenie problemu.

- Możesz wybrać problemy w *Monitoring* → *Problems*, a następnie kliknąć *Mass update* pod listą
- Możesz kliknąć *Update* w kolumnie *Update* problemu w:
  - *Dashboards* (widżety *Problems* i *Problems by severity*)
  - *Monitoring* → *Problems*
  - *Monitoring* → *Problems* → *Event details*
- Możesz kliknąć komórkę nierozwiązanego problemu w:
  - *Dashboards* (widżet *Trigger overview*)

Menu podręczne zawiera opcję *Update*, która przeniesie Cię do okna aktualizacji problemu.

Aktualizowanie problemów Wyskakujące okno aktualizacji problemu umożliwia:

- dodanie komentarza do problemu
- wyświetlenie dotychczasowych komentarzy i działań
- zmianę ważności problemu
- stłumienie/usunięcie stłumienia problemu
- potwierdzenie/cofnięcie potwierdzenia problemu
- zmianę problemu objawowego na problem przyczynowy
- ręczne zamknięcie problemu



Wszystkie wymagane pola wejściowe są oznaczone czerwoną gwiazdką.

Parametr	Opis
Problem	Jeśli wybrano tylko jeden problem, wyświetlana jest nazwa problemu. Jeśli wybrano kilka problemów, wyświetlany jest tekst *Wybrano N problemów*.
Message	Wprowadź tekst komentarza do problemu (maksymalnie 2048 znaków).
History	Wyświetlana jest lista wcześniejszych działań i komentarzy dotyczących problemu wraz z czasem i danymi użytkownika. Znaczenie ikon używanych do oznaczania działań użytkownika opisano na stronie szczegółów zdarzenia. Należy pamiętać, że historia jest wyświetlana tylko wtedy, gdy do aktualizacji wybrano jeden problem.
Scope	Określ zakres działań takich jak zmiana ważności, potwierdzanie lub ręczne zamykanie problemów: **Only selected problem** - wpłynie tylko na to zdarzenie **Selected and all other problems of related triggers** - w przypadku potwierdzenia/zamknięcia problemu wpłynie na to zdarzenie oraz wszystkie inne problemy, które nie zostały jeszcze potwierdzone/zamknięte. Jeśli zakres obejmuje problemy już potwierdzone lub zamknięte, nie zostaną one potwierdzone/zamknięte ponownie. Z drugiej strony liczba operacji dodawania wiadomości i zmiany ważności nie jest ograniczona.

Parametr	Opis
Change severity	Zaznacz pole wyboru i kliknij przycisk ważności, aby zaktualizować ważność problemu. Pole wyboru zmiany ważności jest dostępne, jeśli istnieją uprawnienia do odczytu i zapisu dla co najmniej jednego z wybranych problemów. Po kliknięciu *Update* zaktualizowane zostaną tylko te problemy, dla których dostępny jest odczyt i zapis. Jeśli dla żadnego z wybranych wyzwalaczy nie istnieją uprawnienia do odczytu i zapisu, pole wyboru jest wyłączone.
Suppress	Zaznacz pole wyboru, aby stłumić problem: **Indefinitely** - stłum bezterminowo **Until** - stłum do określonego czasu. Obsługiwane są formaty czasu bezwzględnego i względnego, na przykład: `now+1d` - na jeden dzień od teraz (domyślnie) `now/w` - do końca bieżącego tygodnia `2022-05-28 12:00:00` - do bezwzględnej daty/godziny Należy pamiętać, że prosty okres (np. `1d`, `1w`) nie jest obsługiwany. Dostępność tej opcji zależy od ustawień roli użytkownika „Suppress problems". Zobacz także: Stłumienie problemów
Unsuppress	Zaznacz pole wyboru, aby usunąć stłumienie problemu. To pole wyboru jest aktywne tylko wtedy, gdy co najmniej jeden z wybranych problemów jest stłumiony. Dostępność tej opcji zależy od ustawień roli użytkownika „Suppress problems".
Acknowledge	Zaznacz pole wyboru, aby potwierdzić problem. To pole wyboru jest dostępne, jeśli wśród wybranych znajduje się co najmniej jeden niepotwierdzony problem. Nie można dodać kolejnego potwierdzenia do już potwierdzonego problemu (można jednak dodać kolejny komentarz).
Unacknowledge	Zaznacz pole wyboru, aby cofnąć potwierdzenie problemu. To pole wyboru jest dostępne, jeśli wśród wybranych znajduje się co najmniej jeden potwierdzony problem.
Convert to cause	Zaznacz pole wyboru, aby przekształcić problem(y) objawowy(e) w problem(y) przyczynowy(e).
Close problem	Zaznacz pole wyboru, aby ręcznie zamknąć wybrany problem(y). Pole wyboru zamknięcia problemu jest dostępne, jeśli opcja *Allow manual close* jest zaznaczona w konfiguracji wyzwalacza dla co najmniej jednego z wybranych problemów. Po kliknięciu *Update* zamknięte zostaną tylko te problemy, które można zamknąć. Jeśli żadnego problemu nie można zamknąć ręcznie, pole wyboru jest wyłączone. Problemy już zamknięte nie zostaną zamknięte ponownie.

Wyświetlanie Na podstawie informacji o potwierdzeniach można skonfigurować sposób wyświetlania liczby problemów na pulpicie lub mapach. Aby to zrobić, należy dokonać wyboru w opcji *Wyświetlanie problemów*, dostępnej zarówno w konfiguracji mapy, jak i w widżecie pulpitu *Problemy według ważności* dashboard. Możliwe jest wyświetlanie całkowitej liczby problemów, liczby niepotwierdzonych problemów oddzielnie od całości lub wyłącznie liczby niepotwierdzonych problemów.

Na podstawie informacji o aktualizacji problemu (potwierdzenie itp.) można skonfigurować operacje aktualizacji — wysłanie wiadomości lub wykonanie zdalnych poleceń.

1 Tłumienie problemów

Przegląd

Wyciszenie problemu umożliwia tymczasowe ukrycie problemu, którym można zająć się później. Jest to przydatne do uporządkowania listy problemów, aby nadać najwyższy priorytet najpilniejszym kwestiom. Na przykład czasami problem może pojawić się w weekend i nie być na tyle pilny, aby zajmować się nim natychmiast, więc można go „odłożyć" do poniedziałkowego poranka.

Wyciszenie problemu pozwala ukryć *pojedynczy* problem, w przeciwieństwie do wyciszenia problemów poprzez konserwację hosta, gdy ukrywane są wszystkie problemy hosta objętego konserwacją.

Operacje dla akcji wyzwalaczy będą wstrzymane dla wyciszonych problemów w taki sam sposób, jak ma to miejsce w przypadku konserwacji hosta.

Konfiguracja

Problem można stłumić za pomocą okna **aktualizacja problemu**, gdzie stłumienie jest jedną z opcji aktualizacji problemu, obok komentowania, zmiany powagi, potwierdzania znajomości itd.

Problem można również przywrócić za pomocą tego samego okna aktualizacji problemu.

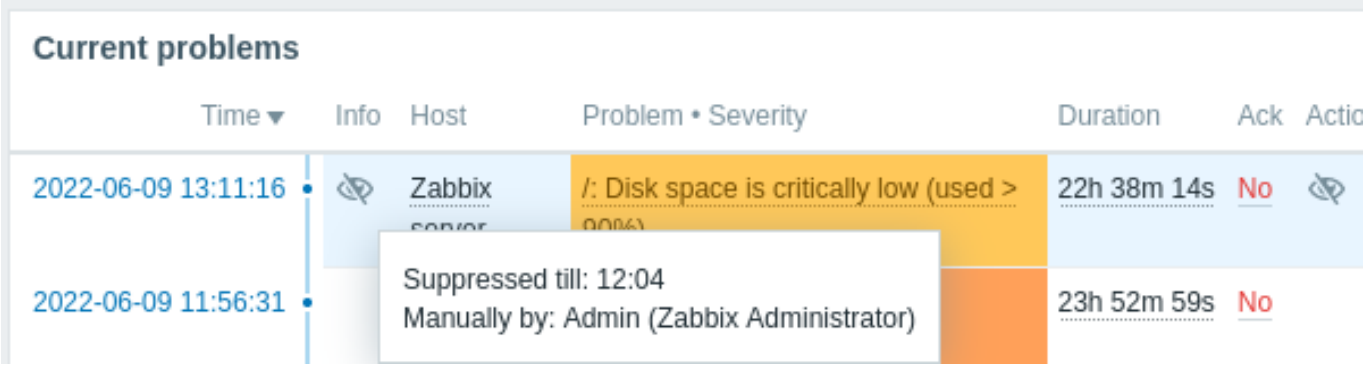
Wyświetlanie

Po wyciszeniu problem jest oznaczany migającą ikoną wyciszenia w kolumnie *Info*, zanim zostanie ukryty.

Ikona wyciszenia miga, gdy zadanie wyciszenia znajduje się na liście oczekujących. Gdy menedżer zadań wyciszy problem, ikona przestanie migać. Jeśli ikona wyciszenia miga przez dłuższy czas, może to wskazywać na problem z serwerem, na przykład gdy serwer jest niedostępny i menedżer zadań nie może ukończyć zadania. Ta sama logika dotyczy cofnięcia wyciszenia. W krótkim czasie po przesłaniu zadania, gdy serwer jeszcze go nie ukończył, ikona cofnięcia wyciszenia miga.

Wyciszony problem może być zarówno ukryty, jak i wyświetlany, w zależności od ustawień filtra problemów/widgetu.

Gdy jest wyświetlany na liście problemów, wyciszony problem jest oznaczony ikoną wyciszenia, a szczegóły wyciszenia są wyświetlane po najechaniu kursorem:



Szczegóły wyciszenia są również wyświetlane w wyskakującym oknie po najechaniu kursorem na ikonę wyciszenia w kolumnie *Actions*.

12 Eksport/import konfiguracji

Przegląd Funkcjonalność eksportu/importu w Zabbix umożliwia wymianę różnych elementów konfiguracji między jednym systemem Zabbix a drugim.

Typowe przypadki użycia tej funkcjonalności:

- udostępnianie szablonów lub map sieciowych — użytkownicy Zabbix mogą udostępniać swoje parametry konfiguracji
- przesyłanie szablonu do Zabbix Community templates. Następnie inni mogą pobrać szablon i zaimportować plik do Zabbix.
- integracja z narzędziami innych firm — uniwersalne formaty YAML, XML i JSON umożliwiają integrację oraz import/eksport danych za pomocą narzędzi i aplikacji innych firm

Co można eksportować/importować

Obiekty, które można eksportować/importować to:

- Grupy hostów (*tylko przez Zabbix API*)
- Grupy szablonów (*tylko przez Zabbix API*)
- Szablony
- Hosty
- Mapy sieci
- Typy mediów
- Obrazy

Format eksportu

Dane można eksportować za pomocą interfejsu użytkowania Zabbix lub Zabbix API. Obsługiwane formaty eksportu to YAML, XML i JSON.

Szczegóły eksportu

- Wszystkie obsługiwane elementy są eksportowane do jednego pliku.
- Encje hosta i szablonu (pozycje, wyzwalacze, wykresy, reguły wykrywania), które są dziedziczone z podłączonych szablonów, nie są eksportowane. Wszelkie zmiany wprowadzone w tych encjach na poziomie hosta (takie jak zmieniony interwał pozycji, zmodyfikowane wyrażenie regularne lub dodane prototypy do reguły wykrywania niskiego poziomu) zostaną utracone

podczas eksportu; podczas importu wszystkie encje z podłączonych szablonów są odtwarzane tak jak w oryginalnym podłączonym szablonie.
- Encje utworzone przez wykrywanie niskiego poziomu oraz wszelkie encje od nich zależne nie są eksportowane. Na przykład wyzwalacz utworzony dla pozycji wygenerowanej przez regułę LLD nie zostanie wyeksportowany.
- Jeśli eksportowany host/szablon zawiera encje obsługujące limity czasu, wartości limitu czasu zostaną wyeksportowane, jeśli dla tych encji skonfigurowano własne limity czasu.

Szczegóły dotyczące importu

- Import zatrzymuje się przy pierwszym błędzie.
- Podczas aktualizacji istniejących obrazów w trakcie importu obrazów pole "imagetype" jest ignorowane, tj. nie można zmienić typu obrazu za pomocą importu.
- Podczas importowania hostów/szablonów z użyciem opcji "Delete missing" makra hosta/szablonu, które nie są obecne w pliku importu, zostaną usunięte z
hosta/szablonu po imporcie.
- Puste tagi dla pozycji, wyzwalaczy, wykresów, discoveryRules, itemPrototypes, triggerPrototypes, graphPrototypes nie mają znaczenia, tj. to tak, jakby ich brakowało.
- Jeśli encje importowanego hosta/szablonu mają skonfigurowane własne limity czasu, zostaną one zastosowane; w przeciwnym razie zostaną zastosowane limity czasu proxy/globalne.
- Import obsługuje YAML, XML i JSON, a plik importu musi mieć poprawne rozszerzenie pliku: .yaml i .yml dla YAML, .xml dla XML oraz .json dla JSON. Zobacz informacje o kompatybilności dotyczące obsługiwanych wersji XML.
- Import obsługuje pliki konfiguracyjne wyłącznie w kodowaniu UTF-8 (z BOM lub bez); inne kodowania (UTF16LE, UTF16BE, UTF32LE, UTF32BE itd.) spowodują błąd konwersji podczas importu.

Podstawowy format YAML Format eksportu YAML zawiera następujące węzły:

- Węzeł główny eksportu Zabbix YAML
- Wersja eksportu

```
zabbix_export:
  version: '8.0'
```

Pozostałe węzły zależą od eksportowanych obiektów.

Format XML Format eksportu XML zawiera następujące tagi:

- Domyślny nagłówek dla dokumentów XML
- Główny tag dla eksportu XML Zabbix
- Wersja eksportu

```
<?xml version="1.0" encoding="UTF-8"?>
<zabbix_export>
    <version>8.0</version>
</zabbix_export>
```

Pozostałe tagi zależą od eksportowanych obiektów.

Format JSON Format eksportu JSON zawiera następujące obiekty:

- Obiekt główny eksportu JSON Zabbix
- Wersja eksportu

```
{
    "zabbix_export": {
        "version": "8.0"
    }
}
```

Pozostałe obiekty zależą od eksportowanych obiektów.

1 Grupy szablonów

Przegląd

W frontend grupy szablonów mogą być eksportowane tylko razem z eksportem szablonów. Gdy szablon jest eksportowany, wszystkie grupy, do których należy, są eksportowane wraz z nim automatycznie.

API umożliwia eksportowanie grup szablonów niezależnie od szablonów.

Format eksportu

```
  template_groups:
    - uuid: 36bff6c29af64692839d077febfc7079
      name: 'Urządzenia sieciowe'
```

Wyeksportowane elementy

Element	Type	Description
uuid	string	Unikalny identyfikator tej grupy szablonów.
name	string	Nazwa grupy.

2 Grupy hostów

Przegląd

W interfejsie użytkownika grupy hostów mogą być eksportowane tylko za pomocą eksportu hosta. Gdy host jest eksportowany, wszystkie grupy, do których należy, są automatycznie eksportowane wraz z nim.

API umożliwia eksportowanie grup hostów niezależnie od hostów.

Format eksportu

```
host_groups:
- uuid: 6f6799aa69e844b4b3918f779f2abf08
name: 'Serwery Zabbix'
```

Eksportowane elementy

Element	Typ	Opis
uuid	string	Unikalny identyfikator grupy hostów.
name	string	Nazwa grupy.

###3 Szablony {#manual-xml_export_import-templates}

Przegląd

Szablony są eksportowane wraz z wieloma powiązanymi obiektami i relacjami między obiektami.

Eksport szablonu zawiera:

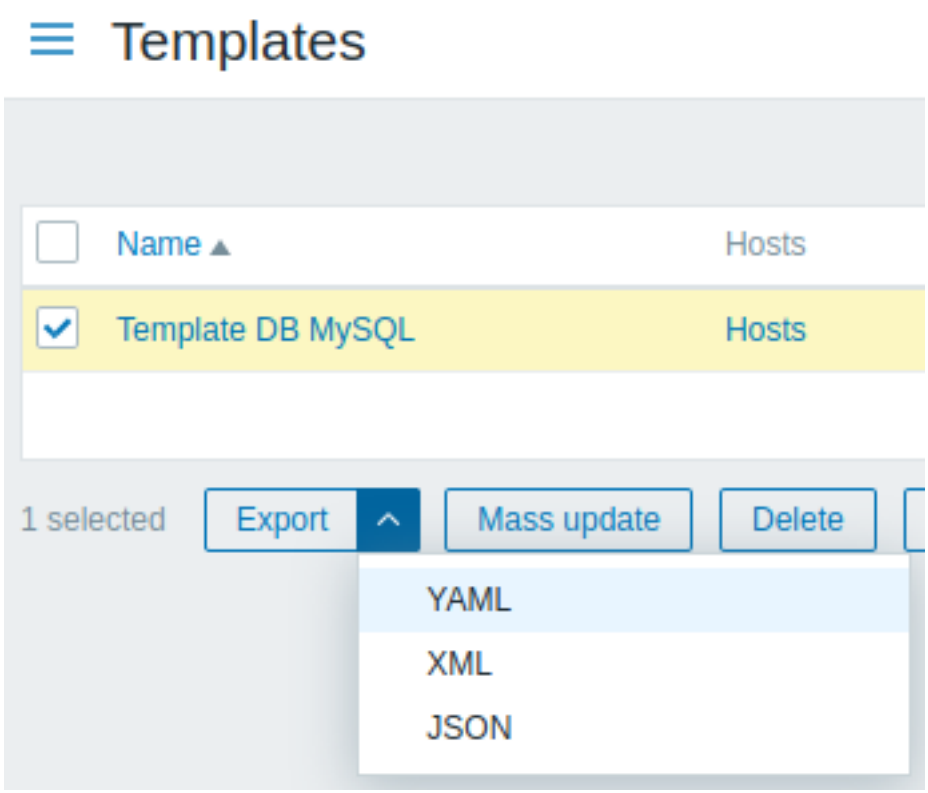
- Powiązane grupy szablonów
- Powiązane grupy hostów (jeśli są używane w konfiguracji prototypu hosta)
- Dane szablonu
- Powiązania z innymi szablonami
- Powiązania z grupami szablonów
- Bezpośrednio powiązane pozycje
- Bezpośrednio powiązane wyzwalacze
- Bezpośrednio powiązane wykresy
- Bezpośrednio powiązane pulpity
- Bezpośrednio powiązane reguły wykrywania ze wszystkimi prototypami
- Bezpośrednio powiązane scenariusze WWW
- Mapy wartości

Eksportowanie

Aby wyeksportować szablony, wykonaj następujące czynności:

1. Przejdź do *Data collection* → *Templates*.
2. Zaznacz pola wyboru szablonów do wyeksportowania.

3. Kliknij *Export* poniżej listy.



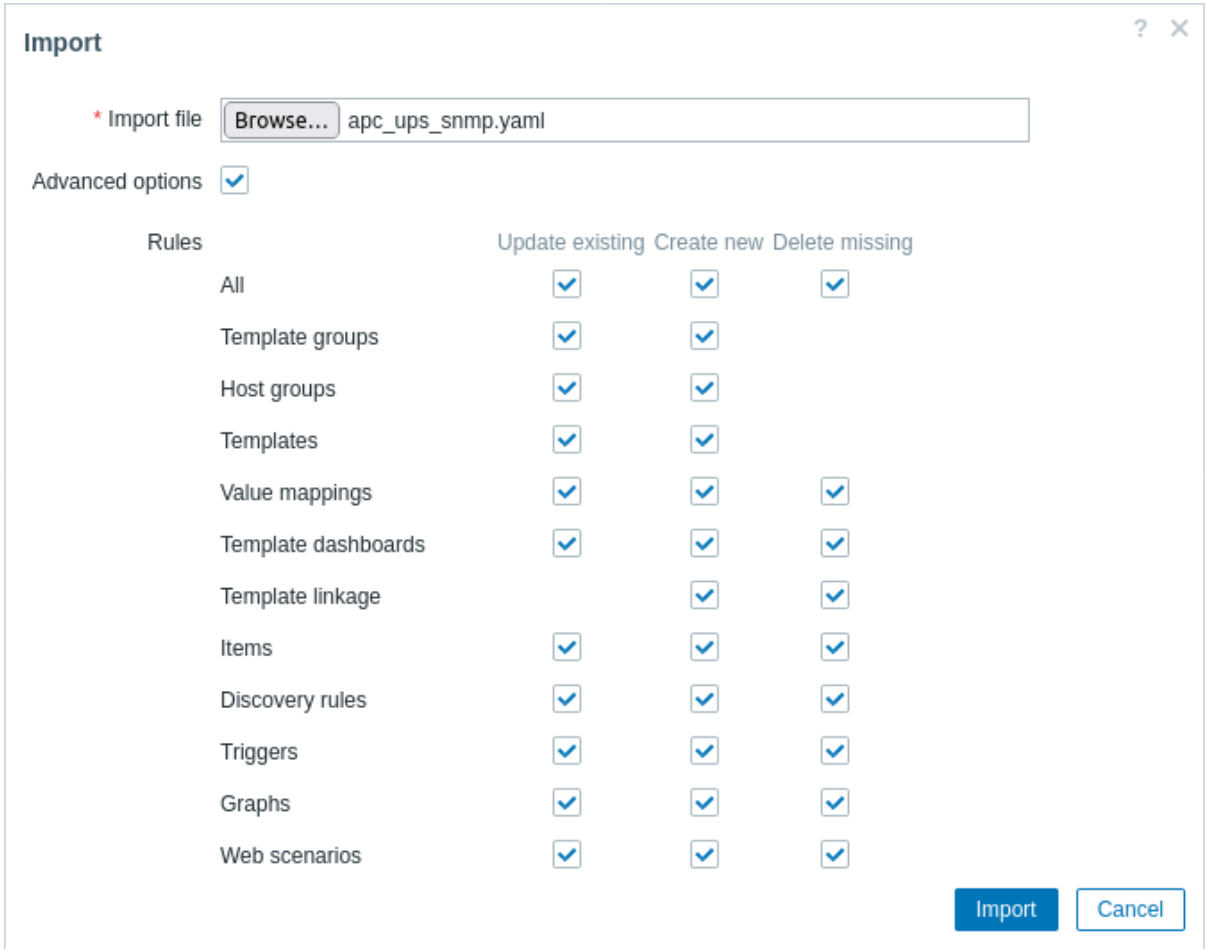
W zależności od wybranego formatu szablony są eksportowane do pliku lokalnego z domyślną nazwą:

- `zabbix_export_templates.yaml` — w eksporcie YAML (domyślna opcja eksportu);
- `zabbix_export_templates.xml` — w eksporcie XML;
- `zabbix_export_templates.json` — w eksporcie JSON.

Importowanie

Aby zaimportować szablony, wykonaj następujące czynności:

1. Przejdź do *Data collection* → *Templates*.
2. Kliknij *Import* w prawym górnym rogu.
3. Wybierz plik importu.
4. Kliknij *Import* w prawym dolnym rogu formularza konfiguracji.



Jeśli zaznaczysz pole wyboru *Advanced options*, zostanie wyświetlona szczegółowa lista wszystkich elementów, które można importować — zaznacz lub odznacz każdą regułę importu zgodnie z potrzebami.

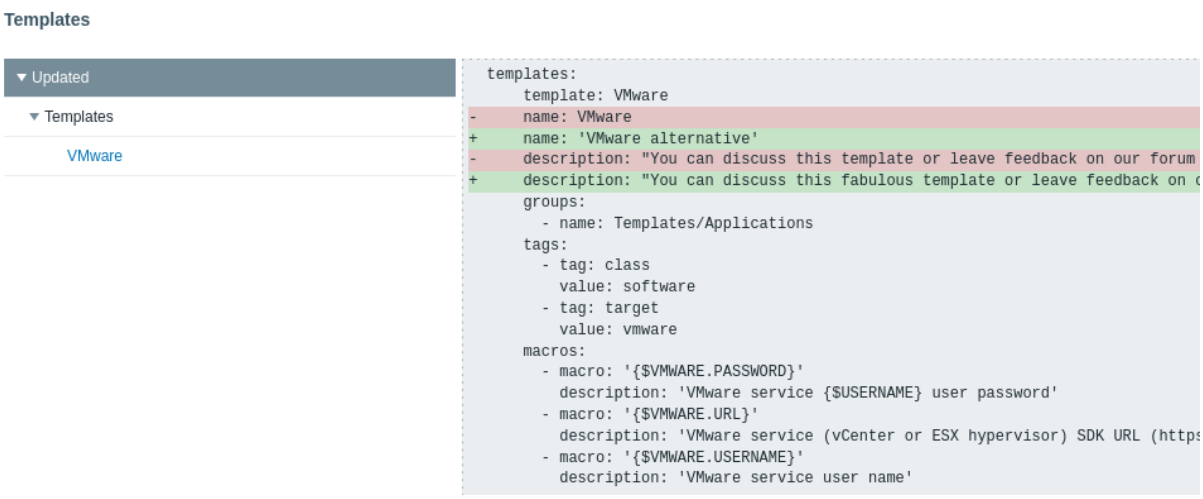
Jeśli klikniesz pole wyboru w wierszu *All*, wszystkie elementy poniżej zostaną zaznaczone/odznaczone.

Reguły importu:

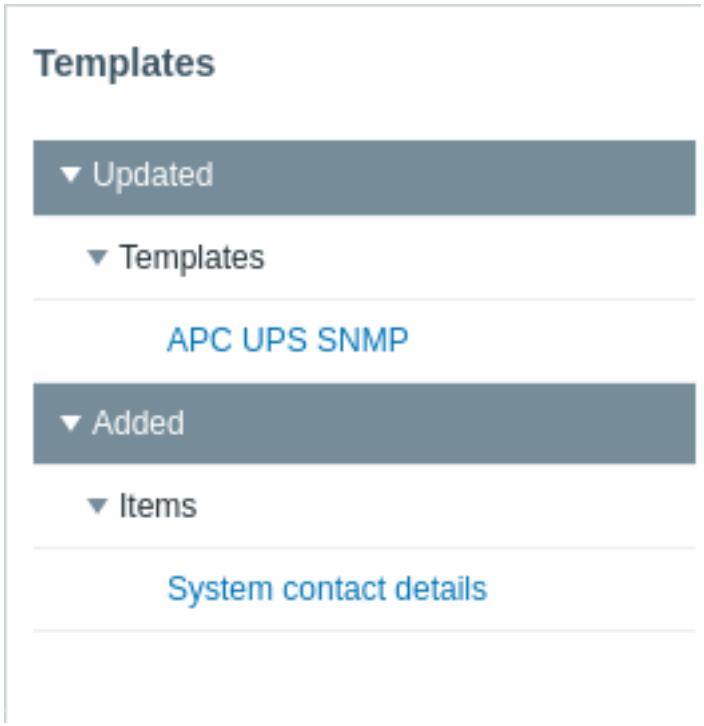
Rule	Description
Update existing	Istniejące elementy zostaną zaktualizowane przy użyciu danych z pliku importu. W przeciwnym razie nie zostaną zaktualizowane.
Create new	Nowe elementy zostaną utworzone przy użyciu danych z pliku importu. W przeciwnym razie nie zostaną utworzone.
Delete missing	Istniejące elementy, których nie ma w pliku importu, zostaną usunięte. W przeciwnym razie nie zostaną usunięte. Jeśli opcja *Delete missing* jest zaznaczona dla *Template linkage*, bieżące powiązania szablonów, których nie ma w pliku importu, zostaną odłączone. Encje (pozycje, wyzwalacze, wykresy itd.) dziedziczone z odłączonych szablonów nie zostaną usunięte (chyba że opcja *Delete missing* zostanie również zaznaczona dla każdej encji).

Attention:
Jeśli szablony o tych samych nazwach już istnieją, podczas importu należy zaznaczyć opcje *Delete missing*, aby uzyskać czysty import. W ten sposób stare pozycje, których nie ma już w zaktualizowanym szablonie, zostaną usunięte (należy pamiętać, że będzie to oznaczać utratę historii tych starych pozycji).

Na następnym ekranie będzie można wyświetlić zawartość importowanego szablonu. Jeśli jest to nowy szablon, wszystkie elementy będą wyświetlane na zielono. W przypadku aktualizacji istniejącego szablonu nowe elementy szablonu będą wyróżnione na zielono; usunięte elementy szablonu będą wyróżnione na czerwono; elementy, które nie uległy zmianie, będą wyświetlane na szarym tle.



Menu po lewej stronie może służyć do poruszania się po liście zmian. Sekcja *Updated* wyróżnia wszystkie zmiany wprowadzone w istniejących elementach szablonu. Sekcja *Added* zawiera listę nowych elementów szablonu. Elementy w każdej sekcji są pogrupowane według typu elementu; kliknij szarą strzałkę, aby rozwinąć lub zwinąć grupę elementów.



Przejrzyj zmiany w szablonie, a następnie kliknij *Import*, aby wykonać import szablonu. W frontend zostanie wyświetlony komunikat o powodzeniu lub niepowodzeniu importu.

Format eksportu Po wyeksportowaniu szablonu Zabbix generuje uporządkowany format YAML, JSON lub XML. Eksport obejmuje elementy szablonu, takie jak metadane szablonu, pozycje, makra, wyzwalacze, pulpity i inne.

Każdy element pełni określoną funkcję i może zawierać elementy zagnieżdżone.

Poniższe sekcje opisują każdy element w formacie eksportu. W przykładach użyto szablonu Linux by Zabbix agent.

Wielokropek (`...`) oznacza elementy pominięte dla zwięzłości. Uwaga (`see table below`) jest używana, gdy dany element jest wyjaśniony bardziej szczegółowo w dalszych sekcjach.

```
zabbix_export:
  version: '8.0'
  template_groups:
    - uuid: 846977d1dfed4968bc5f8bdb363285bc
      name: 'Templates/Operating systems'
  templates: (zobacz tabelę poniżej)
```

```
  triggers: (zobacz tabelę poniżej)
  graphs: (zobacz tabelę poniżej)
```

Metadane szablonu

Element	Type	Opis
version	string	(wymagane) Wersja eksportu.
template_groups		(wymagane) Element główny dla grup szablonów.
uuid	string	(wymagane) Unikalny identyfikator tej grupy szablonów.
name	string	(wymagane) Nazwa grupy szablonów.
host_groups		Element główny dla grup hostów używanych przez prototypy hostów.
uuid	string	(wymagane) Unikalny identyfikator tej grupy hostów.
name	string	(wymagane) Nazwa grupy hostów.
templates		Element główny dla szablonów.
triggers		Element główny dla elementów wyzwalaczy szablonu, które są takie same jak dla wyzwalaczy pozycji szablonu.
graphs		Element główny dla elementów wykresów szablonu, które są takie same jak dla wykresów hosta.

```
zabbix_export:
  (...)
  templates:
    - uuid: f8f7908280354f2abeed07dc788c3747
      template: 'Linux by Zabbix agent'
      name: 'Linux by Zabbix agent'
      description: |
        To jest oficjalny szablon Linux. Wymaga Zabbix agent 8.0 lub nowszego. (...)
      wizard_ready: 'YES'
      readme: |
        ## Przegląd

        To jest oficjalny szablon Linux. Wymaga Zabbix agent 8.0 lub nowszego. (...)
      vendor:
        name: Zabbix
        version: 8.0-2
      groups:
        - name: 'Templates/Operating systems'
      items: (zobacz tabelę poniżej)
      discovery_rules: (zobacz tabelę poniżej)
      tags:
        - tag: class
          value: os
        - tag: target
          value: linux
      macros:
        - macro: '{$AGENT.TIMEOUT}'
          value: 3m
          description: 'Limit czasu, po którym agent jest uznawany za niedostępny. Działa tylko dla agentó
          config: (zobacz tabelę poniżej)
        - macro: '{$CPU.UTIL.CRIT}'
          value: '90'
          description: 'Próg krytyczny wykorzystania CPU wyrażony w %.'
          config: (zobacz tabelę poniżej)
        (...)
      dashboards: (zobacz tabelę poniżej)
      valuemaps: (zobacz tabelę poniżej)
    (...)
```

Szablony

Element	Type	Opis
uuid	string	(wymagane) Unikalny identyfikator tego szablonu.
template	string	(wymagane) Unikalna nazwa szablonu.
name	string	Widoczna nazwa szablonu.
description	text	Opis szablonu.
wizard_ready	text	Czy szablon jest dostępny do wyboru w Kreatorze hosta. Możliwe wartości:[1] NO (0, domyślnie), YES (1). Zobacz także: Obiekt szablonu (`wizard_ready`).
readme	text	Instrukcje konfiguracji specyficzne dla szablonu, wyświetlane w Kreatorze hosta. Obsługuje formatowanie Markdown.
vendor		Element główny dla dostawcy szablonu (obecny, jeśli eksportowany szablon zawiera dane dostawcy).
name	string	(wymagane) Nazwa dostawcy szablonu.
version	string	(wymagane) Wersja szablonu. Dla gotowych szablonów wersja jest wyświetlana w następujący sposób: główna wersja Zabbix, separator (”-”), numer rewizji (zwiększany z każdą nową wersją szablonu i resetowany przy każdej głównej wersji Zabbix). Na przykład 7.0-0, 7.0-3, 8.0-0, 8.0-3.
templates		Element główny dla podlinkowanych szablonów.
name	string	(wymagane) Nazwa szablonu.
groups		Element główny dla grup szablonów.
name	string	(wymagane) Nazwa grupy szablonów.
items		Element główny dla pozycji szablonu.
discovery_rules		Element główny dla reguł niskopoziomowego wykrywania szablonu.
httptests		Element główny dla scenariuszy WWW szablonu.
tags		Element główny dla tagów szablonu.
tag	string	(wymagane) Nazwa tagu.
value	string	Wartość tagu.
macros		Element główny dla makr użytkownika szablonu.
macro	string	(wymagane) Nazwa makra użytkownika.
type	string	Typ makra użytkownika. Możliwe wartości:[1] TEXT (0, domyślnie), SECRET_TEXT (1), VAULT (2). Zobacz także: Obiekt makra użytkownika (`type`).
value	string	Wartość makra użytkownika.
description	string	Opis makra użytkownika.
config		Element główny dla konfiguracji makra szablonu, odpowiedzialnej za sposób wyświetlania makra w Kreatorze hosta.
dashboards		Element główny dla pulpitów szablonu.
valuemaps		Element główny dla map wartości szablonu.

Pozycje szablonu

```
zabbix_export:
  (...)
  templates:
    (...)
      items:
        - uuid: f94f9f4699e94c369e6c98b2a2f485ce
          name: 'Ping agenta Zabbix'
          key: agent.ping
          description: 'Agent zawsze zwraca "1" dla tej pozycji. Może być używana w połączeniu z `nodata()
          valuemap:
            name: 'Status pingu agenta Zabbix'
          tags:
            - tag: component
              value: system
        (...)
        - uuid: 58818005e76d46dda14d6592f601ab00
          name: 'Liczba zainstalowanych pakietów'
          key: system.sw.packages.get
          delay: 1h
          preprocessing: (zobacz tabelę poniżej)
          tags:
```

```
      - tag: component
        value: os
    triggers: (zobacz tabelę poniżej)
  - uuid: 403cebed115441369e94d35d070ca7b8
    name: 'Wykorzystanie pamięci'
    type: DEPENDENT
    key: vm.memory.utilization
    value_type: FLOAT
    units: '%'
    description: 'Procent użytej pamięci jest obliczany jako `100-pavailable`.'
    preprocessing: (zobacz tabelę poniżej)
    master_item:
      key: 'vm.memory.size[pavailable]'
    tags:
      - tag: component
        value: memory
    triggers: (zobacz tabelę poniżej)
  (...)
```

Element	Type	Opis
uuid	string	(wymagane) Unikalny identyfikator tej pozycji.
name	string	(wymagane) Nazwa pozycji.
type	string	Typ pozycji. Możliwe wartości:[1] ZABBIX_PASSIVE (0, domyślnie), TRAP (2), SIMPLE (3), INTERNAL (5), ZABBIX_ACTIVE (7), EXTERNAL (10), ODBC (11), IPMI (12), SSH (13), TELNET (14), CALCULATED (15), JMX (16), SNMP_TRAP (17), DEPENDENT (18), HTTP_AGENT (19), SNMP_AGENT (20), ITEM_TYPE_SCRIPT (21), ITEM_TYPE_BROWSER (22).
snmp_oid	string	(wymagane dla pozycji SNMP_AGENT) ID obiektu SNMP.
key	string	(wymagane) Klucz pozycji.
delay	string	Interwał aktualizacji pozycji. Domyślnie: 1m. Dla pozycji TRAP wartość zawsze będzie wynosić 0.
history	string	Okres czasu (z użyciem sufiksu czasu, makra użytkownika lub makra LLD), przez jaki dane historii powinny być przechowywane. Domyślnie: 31d.
trends	string	Okres czasu (z użyciem sufiksu czasu, makra użytkownika lub makra LLD), przez jaki dane trendów powinny być przechowywane. Domyślnie: 365d.
status	string	Status pozycji. Możliwe wartości:[1] ENABLED (0, domyślnie), DISABLED (1).
value_type	string	Typ otrzymywanej wartości. Możliwe wartości:[1] FLOAT (0), CHAR (1), LOG (2), UNSIGNED (3, domyślnie), TEXT (4), BINARY (5), JSON (6).
allowed_hosts	string	Lista adresów IP hostów, oddzielonych przecinkami, którym wolno wysyłać dane dla tej pozycji. Obsługiwane dla pozycji TRAP i HTTP_AGENT.
units	string	Jednostki otrzymywanej wartości (bps, B itp.).
params	text	Dodatkowe parametry zależne od typu pozycji (wykonywany skrypt dla pozycji SSH i TELNET; zapytanie SQL dla pozycji ODBC; formuła dla pozycji CALCULATED; skrypt dla pozycji ITEM_TYPE_SCRIPT i ITEM_TYPE_BROWSER).
ipmi_sensor	string	Czujnik IPMI. Obsługiwane dla pozycji IPMI.
authtype	string	Typ uwierzytelniania. Obsługiwane dla pozycji SSH i HTTP_AGENT. Możliwe wartości dla pozycji SSH:[1] PASSWORD (0, domyślnie), PUBLIC_KEY (1). Możliwe wartości dla pozycji HTTP_AGENT:[1] NONE (0, domyślnie), BASIC (1), NTLM (2), Kerberos (3) lub Digest (4).
username	string	(wymagane dla pozycji SSH i TELNET) Nazwa użytkownika do uwierzytelniania. Obsługiwane dla pozycji SIMPLE, ODBC, JMX i HTTP_AGENT. W przypadku użycia dla pozycji JMX należy również określić `password` (zobacz poniżej) albo pozostawić oba elementy puste.

Element	Type	Opis
password	string	(wymagane dla pozycji SSH i TELNET) Hasło do uwierzytelniania. Obsługiwane dla pozycji SIMPLE, ODBC, JMX i HTTP_AGENT. W przypadku użycia dla pozycji JMX należy również określić `username` (zobacz powyżej) albo pozostawić oba elementy puste.
publickey	string	(wymagane dla pozycji SSH) Nazwa pliku klucza publicznego.
privatekey	string	(wymagane dla pozycji SSH) Nazwa pliku klucza prywatnego.
description	text	Opis pozycji.
inventory_link	string	Pole inwentarza hosta, które jest wypełniane przez tę pozycję. Możliwe wartości:[1] NONE (0), ALIAS (4) itd. (obsługiwane pola można znaleźć w Inwentarz hosta).
valuemap		Element główny dla map wartości pozycji.
name	string	(wymagane) Nazwa mapy wartości używanej dla pozycji.
logtimefmt	string	Format czasu we wpisach logu. Obsługiwane dla pozycji typu wartości LOG.
preprocessing		Element główny dla wstępnego przetwarzania wartości pozycji.
step		Element główny dla kroków wstępnego przetwarzania wartości pozycji szablonu.
jmx_endpoint	string	Punkt końcowy JMX. Obsługiwane dla pozycji JMX.
master_item		(wymagane dla pozycji DEPENDENT) Element główny dla pozycji nadrzędnej pozycji zależnej.
key	string	(wymagane) Klucz pozycji nadrzędnej pozycji zależnej.
timeout	string	Limit czasu żądania odpytywania danych pozycji. Obsługiwane dla listy typów pozycji w Timeouts.
url	string	(wymagane dla pozycji HTTP_AGENT) Ciąg URL.
query_fields		Element główny dla parametrów zapytania. Obsługiwane dla pozycji HTTP_AGENT.
name	string	(wymagane dla pozycji HTTP_AGENT) Nazwa parametru zapytania.
value	string	Wartość parametru zapytania. Obsługiwane dla pozycji HTTP_AGENT.
parameters		Element główny dla parametrów zdefiniowanych przez użytkownika. Obsługiwane dla pozycji ITEM_TYPE_SCRIPT i ITEM_TYPE_BROWSER.
name	string	(wymagane dla pozycji ITEM_TYPE_SCRIPT i ITEM_TYPE_BROWSER) Nazwa parametru zdefiniowanego przez użytkownika.
value	string	Wartość parametru zdefiniowanego przez użytkownika. Obsługiwane dla pozycji ITEM_TYPE_SCRIPT i ITEM_TYPE_BROWSER.
posts	string	Dane treści żądania HTTP(S). Obsługiwane dla pozycji HTTP_AGENT.
status_codes	string	Zakresy wymaganych kodów statusu HTTP, oddzielone przecinkami. Obsługiwane dla pozycji HTTP_AGENT.
follow_redirects	string	Czy podążać za przekierowaniami odpowiedzi podczas odpytywania danych. Obsługiwane dla pozycji HTTP_AGENT. Możliwe wartości:[1] NO (0), YES (1, domyślnie).
post_type	string	Typ treści danych wysyłanych metodą POST. Obsługiwane dla pozycji HTTP_AGENT. Możliwe wartości:[1] RAW (0, domyślnie), JSON (2), XML (3).
http_proxy	string	Ciąg połączenia proxy HTTP(S). Obsługiwane dla pozycji HTTP_AGENT.
headers		Element główny dla nagłówków żądania HTTP(S). Obsługiwane dla pozycji HTTP_AGENT.
name	string	(wymagane dla pozycji HTTP_AGENT) Nazwa nagłówka.
value	string	(wymagane dla pozycji HTTP_AGENT) Wartość nagłówka.
retrieve_mode	string	Która część odpowiedzi ma być przechowywana. Obsługiwane dla pozycji HTTP_AGENT. Możliwe wartości:[1] BODY (0, domyślnie), HEADERS (1), BOTH (2).
request_method	string	Typ metody żądania. Obsługiwane dla pozycji HTTP_AGENT. Możliwe wartości:[1] GET (0, domyślnie), POST (1), PUT (2), HEAD (3).
output_format	string	Sposób przetwarzania odpowiedzi. Obsługiwane dla pozycji HTTP_AGENT. Możliwe wartości:[1] RAW (0, domyślnie), JSON (1).

Element	Type	Opis
allow_traps	string	Zezwala na wypełnianie wartości podobnie jak w pozycji trapper. Obsługiwane dla pozycji HTTP_AGENT. Możliwe wartości:[1] NO (0, domyślnie), YES (1).
ssl_cert_file	string	Ścieżka do pliku publicznego klucza SSL. Obsługiwane dla pozycji HTTP_AGENT.
ssl_key_file	string	Ścieżka do pliku prywatnego klucza SSL. Obsługiwane dla pozycji HTTP_AGENT.
ssl_key_password	string	Hasło do pliku klucza SSL. Obsługiwane dla pozycji HTTP_AGENT.
verify_peer	string	Czy weryfikować, że certyfikat hosta jest autentyczny. Obsługiwane dla pozycji HTTP_AGENT. Możliwe wartości:[1] NO (0, domyślnie), YES (1).
verify_host	string	Czy weryfikować, że nazwa hosta dla połączenia odpowiada nazwie w certyfikacie hosta. Obsługiwane dla pozycji HTTP_AGENT. Możliwe wartości:[1] NO (0, domyślnie), YES (1).
tags		Element główny dla tagów pozycji.
tag	string	(wymagane) Nazwa tagu.
value	string	Wartość tagu.
triggers		Element główny dla wyzwalaczy pozycji szablonu.

Note:
Zobacz także: Item object (odwołaj się do odpowiedniej właściwości o pasującej nazwie).

Kroki wstępnego przetwarzania wartości pozycji szablonu

```
zabbix_export:
  (...)
  templates:
    (...)
      items:
        (...)
        - uuid: 58818005e76d46dda14d6592f601ab00
          (...)
          preprocessing:
            - type: JSONPATH
              parameters:
                - $.length()
            - type: DISCARD_UNCHANGED_HEARTBEAT
              parameters:
                - 12h
          (...)
```

Element	Type	Opis
type	string	(wymagane) Typ kroku wstępnego przetwarzania wartości pozycji. Możliwe wartości:[1] MULTIPLIER (1), RTRIM (2), LTRIM (3), TRIM (4), REGEX (5), BOOL_TO_DECIMAL (6), OCTAL_TO_DECIMAL (7), HEX_TO_DECIMAL (8), SIMPLE_CHANGE (9, obliczane: otrzymana wartość - poprzednia wartość), CHANGE_PER_SECOND (10, obliczane: (otrzymana wartość - poprzednia wartość)/(bieżący czas - czas ostatniego sprawdzenia)), XMLPATH (11), JSONPATH (12), IN_RANGE (13), MATCHES_REGEX (14), NOT_MATCHES_REGEX (15), CHECK_JSON_ERROR (16), CHECK_XML_ERROR (17), CHECK_REGEX_ERROR (18), DISCARD_UNCHANGED (19), DISCARD_UNCHANGED_HEARTBEAT (20), JAVASCRIPT (21), PROMETHEUS_PATTERN (22), PROMETHEUS_TO_JSON (23), CSV_TO_JSON (24), STR_REPLACE (25), CHECK_NOT_SUPPORTED (26), XML_TO_JSON (27), SNMP_WALK_VALUE (28), SNMP_WALK_TO_JSON (29), SNMP_GET_VALUE (30).
parameters		(wymagane) Element główny dla parametrów kroku wstępnego przetwarzania wartości pozycji.
parameter	string	Indywidualny parametr kroku wstępnego przetwarzania wartości pozycji.

Element	Type	Opis
error_handler	string	Typ akcji używany w przypadku niepowodzenia kroku wstępnego przetwarzania. Możliwe wartości:[1] ORIGINAL_ERROR (0, domyślnie), DISCARD_VALUE (1), CUSTOM_VALUE (2), CUSTOM_ERROR (3).
error_handler_params	string	Parametry obsługi błędów.

Note:
Zobacz także: Item preprocessing object (odpowiednia właściwość o pasującej nazwie).

Wyzwalacze pozycji szablonu

```
zabbix_export:
  (...)
  templates:
    (...)
      items:
        (...)
        - uuid: 58818005e76d46dda14d6592f601ab00
          (...)
          triggers:
            - uuid: b950c306394f4b3c902060a8273cbcde
              expression: 'change(/Linux by Zabbix agent/system.sw.packages.get)<>0'
              name: 'Linux: Liczba zainstalowanych pakietów uległa zmianie'
              priority: WARNING
              manual_close: 'YES'
              tags:
                - tag: scope
                  value: notice
        (...)
        - uuid: 403cebed115441369e94d35d070ca7b8
          (...)
          triggers:
            - uuid: cfd395b1cde74ef18a5e5f840bd5142a
              expression: 'min(/Linux by Zabbix agent/vm.memory.utilization,5m)>{$MEMORY.UTIL.MAX}'
              name: 'Linux: Wysokie wykorzystanie pamięci'
              event_name: 'Linux: Wysokie wykorzystanie pamięci (>{$MEMORY.UTIL.MAX}% przez 5m)'
              priority: AVERAGE
              description: 'Systemowi kończy się wolna pamięć.'
              dependencies:
                - name: 'Linux: Brak dostępnej pamięci'
                  expression: 'max(/Linux by Zabbix agent/vm.memory.size[available],5m)<{$MEMORY.AVAILABLE
              tags:
                - tag: scope
                  value: capacity
                - tag: scope
                  value: performance
        (...)
```

Element	Type	Opis
uuid	string	(wymagane) Unikalny identyfikator tego wyzwalacza.
expression	string	(wymagane) Wyrażenie wyzwalacza.
recovery_mode	string	Podstawa generowania zdarzeń OK. Możliwe wartości:[1] EXPRESSION (0, domyślnie), RECOVERY_EXPRESSION (1), NONE (2).
recovery_expression	string	Wyrażenie odzyskiwania wyzwalacza.
correlation_mode	string	Tryb korelacji (brak korelacji zdarzeń lub korelacja zdarzeń według tagu). Możliwe wartości:[1] DISABLED (0, domyślnie), TAG_VALUE (1).
correlation_tag	string	Nazwa tagu używanego do korelacji zdarzeń.
name	string	(wymagane) Nazwa wyzwalacza.
event_name	string	Nazwa zdarzenia.
opdata	string	Dane operacyjne.
url_name	string	Etykieta adresu URL powiązanego z wyzwalaczem.

Element	Type	Opis
url	string	Adres URL powiązany z wyzwalaczem.
status	string	Status wyzwalacza. Możliwe wartości:[1] ENABLED (0, domyślnie), DISABLED (1).
priority	string	Poziom ważności wyzwalacza. Możliwe wartości:[1] NOT_CLASSIFIED (0, domyślnie), INFO (1), WARNING (2), AVERAGE (3), HIGH (4), DISASTER (5).
description	text	Opis wyzwalacza.
type	string	Typ generowania zdarzeń (pojedyncze zdarzenie problemu lub wiele zdarzeń problemu). Możliwe wartości:[1] SINGLE (0, domyślnie), MULTIPLE (1).
manual_close	string	Ręczne zamykanie zdarzeń problemu. Możliwe wartości:[1] NO (0, domyślnie), YES (1).
dependencies		Element główny dla zależności.
name	string	(wymagane) Nazwa zależnego wyzwalacza.
expression	string	(wymagane) Wyrażenie zależnego wyzwalacza.
recovery_expression	string	Wyrażenie odzyskiwania zależnego wyzwalacza.
tags		Element główny dla tagów wyzwalacza.
tag	string	(wymagane) Nazwa tagu.
value	string	Wartość tagu.

Note:
Zobacz także: Trigger object (odnieś się do odpowiedniej właściwości o pasującej nazwie).

Reguły wykrywania niskiego poziomu szablonu

```
zabbix_export:
  (...)
  templates:
    (...)
      discovery_rules:
        - uuid: acfdea9c46ef48c68e6636f43b8f96a2
          name: 'Wykrywanie interfejsów sieciowych'
          key: net.if.discovery
          delay: 1h
          filter: (zobacz tabelę poniżej)
          description: 'Wykrywanie interfejsów sieciowych.'
          item_prototypes: (zobacz tabelę poniżej)
          trigger_prototypes: (zobacz tabelę poniżej)
          graph_prototypes: (zobacz tabelę poniżej)
        (...)
```

Attention:
Większość elementów reguł wykrywania niskiego poziomu szablonu jest taka sama jak w przypadku pozycji szablonu. Poniższa tabela opisuje te elementy, które różnią się od pozycji szablonu.

Element	Type	Opis
type	string	Typ pozycji. Możliwe wartości:[1] ZABBIX_PASSIVE (0, domyślnie), TRAP (2), SIMPLE (3), INTERNAL (5), ZABBIX_ACTIVE (7), EXTERNAL (10), ODBC (11), IPMI (12), SSH (13), TELNET (14), JMX (16), DEPENDENT (18), HTTP_AGENT (19), SNMP_AGENT (20), ITEM_TYPE_SCRIPT (21), ITEM_TYPE_BROWSER (22).
key	string	(wymagane) Klucz reguły wykrywania niskiego poziomu.
filter		Element główny dla filtrów reguł wykrywania niskiego poziomu szablonu.
lifetime	string	Okres czasu (z użyciem sekund, sufiksu czasu lub makra użytkownika), po którym zasoby, które nie są już wykrywane, zostaną usunięte. Domyślnie: 7d.
lifetime_type	string	Scenariusz usuwania utraconych zasobów LLD. Możliwe wartości: DELETE_NEVER, DELETE_IMMEDIATELY, DELETE_AFTER.
enabled_lifetime	string	Okres czasu (z użyciem sekund, sufiksu czasu lub makra użytkownika), po którym zasoby, które nie są już wykrywane, zostaną wyłączone.

Element	Type	Opis
enabled_lifetime_type	string	Scenariusz wyłączania utraconych zasobów LLD. Możliwe wartości: DISABLE_NEVER, DISABLE_IMMEDIATELY, DISABLE_AFTER.
item_prototypes		Element główny dla elementów prototypów pozycji szablonu, które są takie same jak dla pozycji szablonu.
trigger_prototypes		Element główny dla elementów prototypów wyzwalaczy szablonu, które są takie same jak dla wyzwalaczy pozycji szablonu.
graph_prototypes		Element główny dla elementów prototypów wykresów szablonu, które są takie same jak dla wykresów hosta.
host_prototypes		Element główny dla elementów prototypów hostów szablonu, które są takie same jak dla hostów.
parent_discovery_rule		Element główny dla nadrzędnej reguły wykrywania niskiego poziomu (lub prototypu reguły) prototypu reguły wykrywania niskiego poziomu. Ta właściwość oznacza, że jest to prototyp reguły LLD, będący bezpośrednim elementem podrzędnym wskazanej reguły/prototypu reguły.
key	string	(wymagane) Klucz nadrzędnej reguły wykrywania niskiego poziomu (lub prototypu reguły).
master_item	string	(wymagane dla reguł DEPENDENT) Element główny dla pozycji nadrzędnej reguły zależnej.
lld_macro_paths		Element główny dla ścieżek makr reguły wykrywania niskiego poziomu.
lld_macro	string	(wymagane) Nazwa makra reguły wykrywania niskiego poziomu.
path	string	(wymagane) Selektor wartości, która zostanie przypisana do odpowiedniego makra.
preprocessing		Element główny dla wstępnego przetwarzania wartości reguły wykrywania niskiego poziomu.
step		Element główny dla elementów kroków wstępnego przetwarzania wartości reguły wykrywania niskiego poziomu, które są takie same jak dla kroków wstępnego przetwarzania wartości pozycji szablonu, z wyjątkiem mniejszej liczby możliwych wartości. Zobacz także: obiekt przetwarzania wstępnego reguły LLD.
overrides		Element główny dla reguł nadpisywania reguły wykrywania niskiego poziomu.
name	string	(wymagane) Unikalna nazwa nadpisania.
step	string	(wymagane) Unikalny numer kolejności nadpisania.
stop	string	Zatrzymaj przetwarzanie kolejnych nadpisań, jeśli pasuje.
filter		Element główny dla elementów filtrów reguł nadpisywania reguły wykrywania niskiego poziomu szablonu, które są takie same jak dla filtrów reguł wykrywania niskiego poziomu szablonu.
operations		Element główny dla operacji nadpisywania reguły wykrywania niskiego poziomu szablonu.

Note:
Zobacz także: obiekt reguły LLD (odnieś się do odpowiedniej właściwości o pasującej nazwie).

Filtry reguł wykrywania niskiego poziomu szablonu

```
zabbix_export:
  (...)
  templates:
    (...)
      discovery_rules:
        - uuid: acfdea9c46ef48c68e6636f43b8f96a2
          (...)
          filter:
            evaltype: AND
            conditions:
              - macro: '{#IFNAME}'
                value: '{$NET.IF.IFNAME.MATCHES}'
              - macro: '{#IFNAME}'
                value: '{$NET.IF.IFNAME.NOT_MATCHES}'
                operator: NOT_MATCHES_REGEX
          (...)
        - uuid: 2bbdc79f082d4c618e01bec625e9c90a
          (...)
          filter:
```

```
            evaltype: AND
            conditions:
              - macro: '{#DEVNAME}'
                value: '{$VFS.DEV.DEVNAME.MATCHES}'
              - macro: '{#DEVNAME}'
                value: '{$VFS.DEV.DEVNAME.NOT_MATCHES}'
                operator: NOT_MATCHES_REGEX
              - macro: '{#DEVTYPE}'
                value: disk
          (...)
```

Element	Type	Opis
evaltype	string	Zastąp metodę oceny warunków filtra. Możliwe wartości:[1] AND_OR (0, domyślnie), AND (1), OR (2), FORMULA (3).
formula	string	Niestandardowa formuła obliczeniowa dla warunków filtra.
conditions		Element główny dla warunków filtra.
macro	string	(wymagane) Nazwa makra wykrywania niskiego poziomu, dla którego ma zostać wykonane sprawdzenie.
value	string	Wartość do porównania.
operator	string	Operator warunku. Możliwe wartości:[1] MATCHES_REGEX (8, domyślnie), NOT_MATCHES_REGEX (9).
formulaid	string	(wymagane) Dowolny unikalny identyfikator używany do odwoływania się do warunku z wyrażenia niestandardowego. Może zawierać wyłącznie wielkie litery. Identyfikator musi zostać zdefiniowany przez użytkownika podczas modyfikowania warunków filtra, ale zostanie wygenerowany ponownie przy późniejszym żądaniu tych warunków.

Note:
Zobacz także: LLD rule filter object (odnieś się do odpowiedniej właściwości o pasującej nazwie).

Operacje nadpisania reguły wykrywania niskiego poziomu szablonu

Element	Type	Opis
operationobject	string	Obiekt, do którego stosowana jest operacja. Możliwe wartości:[1] ITEM_PROTOTYPE (0), TRIGGER_PROTOTYPE (1), GRAPH_PROTOTYPE (2), HOST_PROTOTYPE (3).
operator	string	Operator warunku nadpisania. Możliwe wartości:[1] EQUAL (1), NOT_EQUAL (2), LIKE (3), NOT_LIKE (4), REGEXP (5), NOT_REGEXP (6).
value	string	Wyrażenie regularne lub ciąg znaków dla operatora warunku nadpisania.
status	string	Status obiektu po operacji nadpisania.
discover	string	Czy obiekt jest dodawany w wyniku wykrywania.
delay	string	Interwał aktualizacji ustawiony dla prototypu pozycji po operacji nadpisania.
history	string	Okres przechowywania historii ustawiony dla prototypu pozycji po operacji nadpisania.
trends	string	Okres przechowywania trendów ustawiony dla prototypu pozycji po operacji nadpisania.
severity	string	Ważność prototypu wyzwalacza ustawiona po operacji nadpisania.
tags		Element główny dla tagów ustawionych dla obiektu po operacji nadpisania.
tag	string	(wymagane) Nazwa tagu.
value	string	Wartość tagu.
templates		Element główny dla szablonów podłączonych do prototypu hosta po operacji nadpisania.
name	string	(wymagane) Nazwa szablonu.
inventory_mode	string	Tryb inwentarza prototypu hosta ustawiony po operacji nadpisania.

Note:
Zobacz także: obiekt operacji nadpisania reguły LLD (odnieś się do odpowiedniej właściwości o pasującej nazwie).

Scenariusze WWW szablonu

Element	Type	Opis
uuid	string	(wymagane) Unikalny identyfikator tego scenariusza WWW.
name	string	(wymagane) Nazwa scenariusza WWW.
delay	string	Częstotliwość wykonywania scenariusza WWW (z użyciem sekund, sufiksu czasu lub makra użytkownika). Domyślnie: 1m.
attempts	integer	Liczba prób wykonania kroków scenariusza WWW. Możliwe wartości:[1] 1-10 (domyślnie: 1).
agent	string	agent klienta. Zabbix będzie udawał wybraną przeglądarkę. Jest to przydatne, gdy strona internetowa zwraca różną zawartość dla różnych przeglądarek. Domyślnie: Zabbix.
http_proxy	string	proxy, który będzie używany przez scenariusz WWW, podany w postaci: `http://[username[:password]@]proxy.example.com[:port]`
variables		Element główny dla zmiennych scenariusza WWW, które mogą być używane w krokach scenariusza.
name	string	(wymagane) Nazwa zmiennej.
value	text	(wymagane) Wartość zmiennej.
headers		Element główny dla nagłówków HTTP wysyłanych podczas wykonywania żądania. Nagłówki powinny być wymienione przy użyciu tej samej składni, w jakiej występują w protokole HTTP.
name	string	(wymagane) Nazwa nagłówka.
value	text	(wymagane) Wartość nagłówka.
status	string	Status scenariusza WWW. Możliwe wartości:[1] ENABLED (0, domyślnie), DISABLED (1).
authentication	string	Metoda uwierzytelniania. Możliwe wartości:[1] NONE (0, domyślnie), BASIC (1), NTLM (2), Kerberos (3) lub Digest (4).
http_user	string	Nazwa użytkownika używana do uwierzytelniania BASIC (HTTP), NTLM, Kerberos lub Digest.
http_password	string	Hasło używane do uwierzytelniania BASIC (HTTP), NTLM, Kerberos lub Digest.
verify_peer	string	Weryfikacja certyfikatu SSL serwera WWW. Możliwe wartości:[1] NO (0, domyślnie), YES (1).
verify_host	string	Weryfikacja zgodności pola *Common Name* lub pola *Subject Alternate Name* certyfikatu serwera WWW. Możliwe wartości:[1] NO (0, domyślnie), YES (1).
ssl_cert_file	string	Nazwa pliku certyfikatu SSL używanego do uwierzytelniania klienta (musi być w formacie PEM).
ssl_key_file	string	Nazwa pliku klucza prywatnego SSL używanego do uwierzytelniania klienta (musi być w formacie PEM).
ssl_key_password	string	Hasło pliku klucza prywatnego SSL.
steps		(wymagane) Element główny dla kroków scenariusza WWW szablonu.
tags		Element główny dla tagów scenariusza WWW.
tag	string	(wymagane) Nazwa tagu.
value	string	Wartość tagu.

Note:
Zobacz także: Obiekt scenariusza WWW (odwołaj się do odpowiedniej właściwości o pasującej nazwie).

Kroki scenariusza WWW szablonu

Element	Type	Opis
name	string	(wymagane) Nazwa kroku scenariusza WWW.
url	string	(wymagane) URL do monitorowania.
query_fields		Element główny parametrów zapytania (tablica pól HTTP, które mają zostać dodane do URL podczas wykonywania żądania).
name	string	(wymagane) Nazwa parametru zapytania.
value	string	Wartość parametru zapytania.
posts		Element główny zmiennych HTTP POST (ciąg znaków (surowe dane POST) lub tablica pól HTTP (dane pól formularza)).

Element	Type	Opis
name	string	(wymagane) Nazwa pola POST.
value	string	(wymagane) Wartość pola POST.
variables		Element główny zmiennych na poziomie kroku (makr), które powinny zostać zastosowane po tym kroku. Jeśli wartość zmiennej ma prefiks 'regex:', jej wartość jest wyodrębniana z danych zwróconych przez ten krok zgodnie ze wzorcem wyrażenia regularnego następującym po prefiksie 'regex:'
name	string	(wymagane) Nazwa zmiennej.
value	text	(wymagane) Wartość zmiennej.
headers		Element główny nagłówków HTTP, które mają zostać wysłane podczas wykonywania żądania.
name	string	(wymagane) Nazwa nagłówka.
value	text	(wymagane) Wartość nagłówka.
follow_redirects	string	Podążanie za przekierowaniami HTTP. Możliwe wartości:[1] NO (0), YES (1, domyślnie).
retrieve_mode	string	Tryb pobierania odpowiedzi HTTP. Możliwe wartości:[1] BODY (0, domyślnie), HEADERS (1), BOTH (2).
timeout	string	Limit czasu wykonania kroku (z użyciem sekund, sufiksu czasu lub makra użytkownika). Domyślnie: 15s.
required	string	Tekst, który musi występować w odpowiedzi (ignorowany, jeśli pusty).
status_codes	string	Rozdzielana przecinkami lista akceptowanych kodów statusu HTTP (np. 200-201,210-299; ignorowana, jeśli pusta).

Note:
Zobacz także: Obiekt kroku scenariusza WWW (odnieś się do odpowiedniej właściwości o pasującej nazwie).

Konfiguracja makr szablonu

```
zabbix_export:
  (...)
  templates:
    - uuid: f8f7908280354f2abeed07dc788c3747
      (...)
      macros:
        - macro: '{$AGENT.TIMEOUT}'
          (...)
          config:
            type: TEXT
            priority: '1'
            label: 'Liczba sekund od ostatniego wykrycia agenta Zabbix'
            description: 'Limit czasu, po którym agent jest uznawany za niedostępny.'
        - macro: '{$CPU.UTIL.CRIT}'
          (...)
          config:
            type: TEXT
            priority: '2'
            section_name: Progi
            label: 'Próg wykorzystania CPU wyrażony'
            description: 'Krytyczny próg wykorzystania CPU wyrażony w %. W zakresie od 0 do 100 włącznie.'
            regex: '^-?([0-9]+|(([0-9]+)\.([0-9]+)))$'
        (...)
        - macro: '{$IFCONTROL}'
          (...)
          config:
            type: CHECKBOX
            priority: '19'
            label: 'Kontrola interfejsów'
            description: 'Uruchom wyzwalacz, gdy stan operacyjny interfejsu zmieni się na "Link down".'
            options:
              - checked: '1'
```

```
                unchecked: '0'
        (...)
```

Element	Type	Opis
type	string	(wymagane) Typ pola wejściowego makra. Możliwe wartości:[1] NOCONF (0), TEXT (1), LIST (2), CHECKBOX (3).
priority	string	Pozycja makra na liście makr.
section_name	string	Etykieta zwijanej sekcji, w której makro jest grupowane.
label	string	(wymagane dla makr TEXT, LIST, CHECKBOX) Etykieta makra.
description	text	Tekst pomocy makra. Obsługuje formatowanie Markdown.
required	string	Oznacza makro jako obowiązkowe. Możliwe wartości:[1] NO (0), YES (1). Obsługiwane dla makr TEXT i LIST.
regex	string	Wyrażenie regularne do walidacji danych wejściowych użytkownika w polu tekstowym. Obsługiwane dla makr TEXT.
options		Element główny dla elementów LIST lub wartości CHECKBOX.
value	string	(wymagane dla makr LIST) Wartość elementu LIST.
text	string	(wymagane dla makr LIST) Tekst elementu LIST.
checked	string	(wymagane dla makr CHECKBOX) Wartość reprezentująca stan zaznaczony. Możliwe wartości:[1] 0 (false), 1 (true). Obsługiwane dla makr CHECKBOX.
unchecked	string	(wymagane dla makr CHECKBOX) Wartość reprezentująca stan niezaznaczony. Możliwe wartości:[1] 0 (false), 1 (true). Obsługiwane dla makr CHECKBOX.

Note:
Zobacz także: Macro configuration object (odpowiednia właściwość o pasującej nazwie).

Pulpity szablonów

```
zabbix_export:
  (...)
  templates:
    (...)
      dashboards:
        - uuid: c689ad3115fd46a4b927d1f70ee2e5a4
          name: Filesystems
          pages:
            - name: Overview
              widgets: (zobacz tabelę poniżej)
        (...)
```

Element	Type	Opis
uuid	string	(wymagane) Unikalny identyfikator tego pulpitu.
name	string	(wymagane) Nazwa pulpitu szablonu.
display pe- riod	integer	Okres wyświetlania stron pulpitu.
auto_start	string	Automatyczne uruchamianie pokazu slajdów. Możliwe wartości:[1] NO (0), YES (1, domyślnie).
pages		Element główny dla stron pulpitu szablonu.
name	string	Nazwa strony.
display period	integer	Okres wyświetlania strony.
sortorder	integer	Kolejność sortowania strony.
widgets		Element główny dla widgetów pulpitu szablonu.

Note:
Zobacz także: obiekt pulpitu szablonu (odpowiednia właściwość o pasującej nazwie).

Widżety pulpitu szablonu

```
zabbix_export:
  (...)
  templates:
    (...)
      dashboards:
        - uuid: c689ad3115fd46a4b927d1f70ee2e5a4
          name: Filesystems
          pages:
            - name: Overview
              widgets:
                - type: graphprototype
                  width: '72'
                  height: '5'
                  fields:
                    - type: INTEGER
                      name: columns
                      value: '3'
                    - type: GRAPH_PROTOTYPE
                      name: graphid.0
                      value:
                        host: 'Linux by Zabbix agent'
                        name: 'FS [{#FSTYPE}({#FSNAME})]: Space utilization chart (relative to total)'
                    - type: STRING
                      name: reference
                      value: AAAEB
                - type: graphprototype
                  'y': '5'
                  width: '72'
                  height: '5'
                  fields:
                    - type: INTEGER
                      name: columns
                      value: '1'
                    - type: GRAPH_PROTOTYPE
                      name: graphid.0
                      value:
                        host: 'Linux by Zabbix agent'
                        name: 'FS [{#FSTYPE}({#FSNAME})]: Space usage graph, in % (relative to max availab
                    - type: STRING
                      name: reference
                      value: AAAEC
        (...)
```

Element	Type	Opis
type	string	(wymagane) Typ widżetu.
name	string	Nazwa widżetu.
x	integer	Pozycja pozioma od lewej strony pulpitu szablonu. Możliwe wartości:[1] 0-71.
y	integer	Pozycja pionowa od górnej krawędzi pulpitu szablonu. Możliwe wartości:[1] 0-63.
width	integer	Szerokość widżetu. Możliwe wartości:[1] 1-72.
height	integer	Wysokość widżetu. Możliwe wartości:[1] 1-64.
hide_header	string	Ukryj nagłówek widżetu. Możliwe wartości:[1] NO (0, domyślnie), YES (1).
fields		Element główny dla pól widżetu pulpitu szablonu.
type	string	(wymagane) Typ pola widżetu. Możliwe wartości:[1] INTEGER (0), STRING (1), ITEM (4), ITEM_PROTOTYPE (5), GRAPH (6), GRAPH_PROTOTYPE (7), MAP (8), SERVICE (9), SLA (10), USER (11), ACTION (12), MEDIA_TYPE (13).

Element	Type	Opis
name	string	(wymagane) Nazwa pola widżetu.
value	mixed	(wymagane) Wartość pola widżetu, zależna od typu pola.

Note:
Zobacz także: Template dashboard widget object (odwołaj się do odpowiedniej właściwości o pasującej nazwie).

Mapowania wartości szablonu

```
zabbix_export:
  (...)
  templates:
    (...)
      valuemaps:
        - uuid: 8c048c6cca8248f2860c208e8db0f59e
          name: ifOperStatus
          mappings:
            - value: '0'
              newvalue: unknown
            - value: '1'
              newvalue: notpresent
            - value: '2'
              newvalue: down
            - value: '3'
              newvalue: lowerlayerdown
            - value: '4'
              newvalue: testing
            - value: '5'
              newvalue: dormant
            - value: '6'
              newvalue: up
        (...)
```

Element	Type	Opis
uuid	string	(wymagane) Unikalny identyfikator tego mapowania wartości.
name	string	(wymagane) Nazwa mapowania wartości.
mapping		Element główny dla mapowań.
type	string	Typ dopasowania mapowania. Możliwe wartości:[1] EQUAL (0, domyślnie), GREATER_OR_EQUAL (2), LESS_OR_EQUAL (3), IN_RANGE (4), REGEXP (5), DEFAULT (6).
value	string	Wartość oryginalna.
newvalue	string	(wymagane) Wartość, na którą mapowana jest wartość oryginalna.

Note:
Zobacz także: Value map object (odnieś się do odpowiedniej właściwości o pasującej nazwie).

Przypisy [1] Wartości całkowite API w nawiasach, na przykład ENABLED (0), są podane wyłącznie w celach informacyjnych. Więcej informacji można znaleźć na stronie powiązanego obiektu API wskazanej w odpowiednim wpisie tabeli lub na końcu każdej sekcji.

4 Hosty

Przegląd

Hosty są eksportowane z wieloma powiązanymi obiektami i relacjami obiektów.

Eksport hosta zawiera:

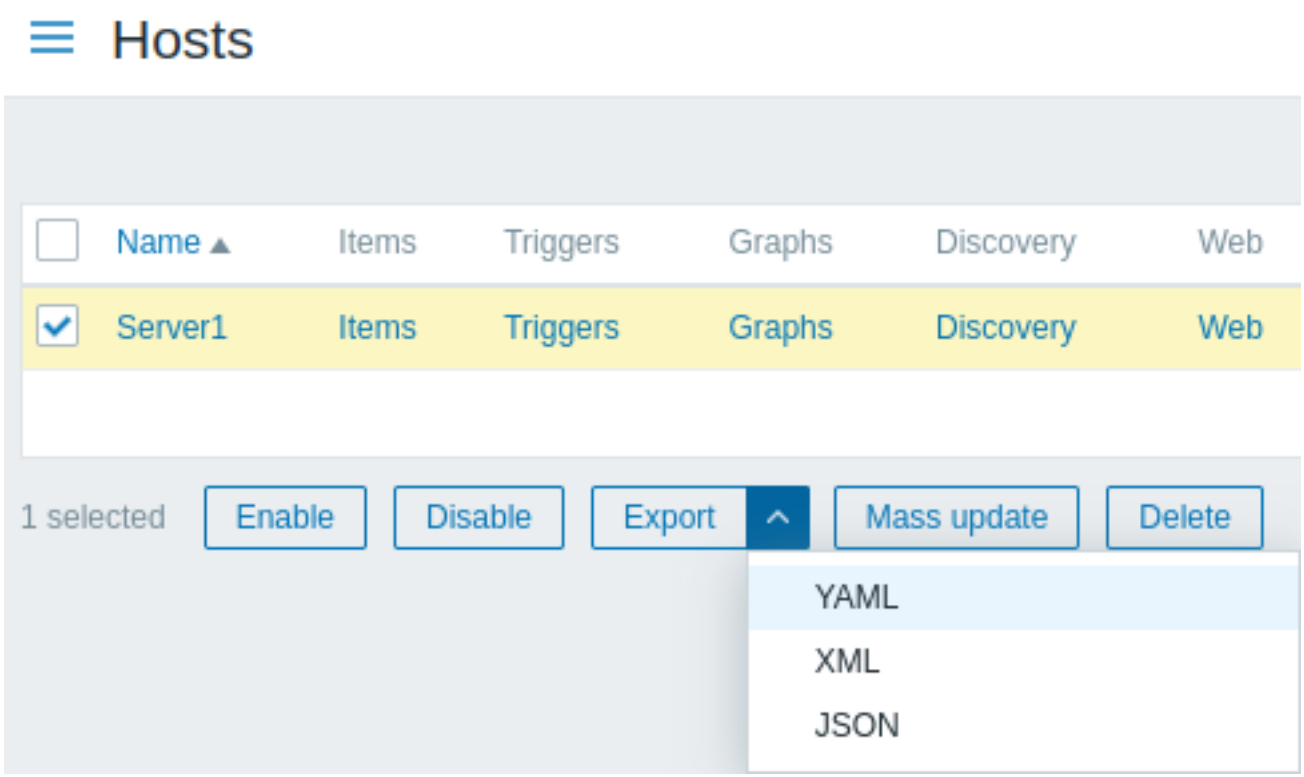
- Połączone grupy hostów

- Dane hosta
- Powiązanie szablonu
- Powiązanie grupy hosta
- Interfejsy hosta
- Bezpośrednio połączone pozycje
- Bezpośrednio połączone wyzwalacze
- Bezpośrednio połączone reguły wykrywania ze wszystkimi prototypami
- Bezpośrednio połączone scenariusze sieci WWW
- Makra hosta
- Dane inwentarza hosta
- Mapy wartości
- Połączone wykresy

Eksportowanie

Aby wyeksportować hosty, wykonaj następujące kroki:

1. Przejdź do *Data collection* → *Hosts*.
2. Zaznacz pola wyboru hostów, które chcesz wyeksportować.
3. Kliknij *Export* pod listą.



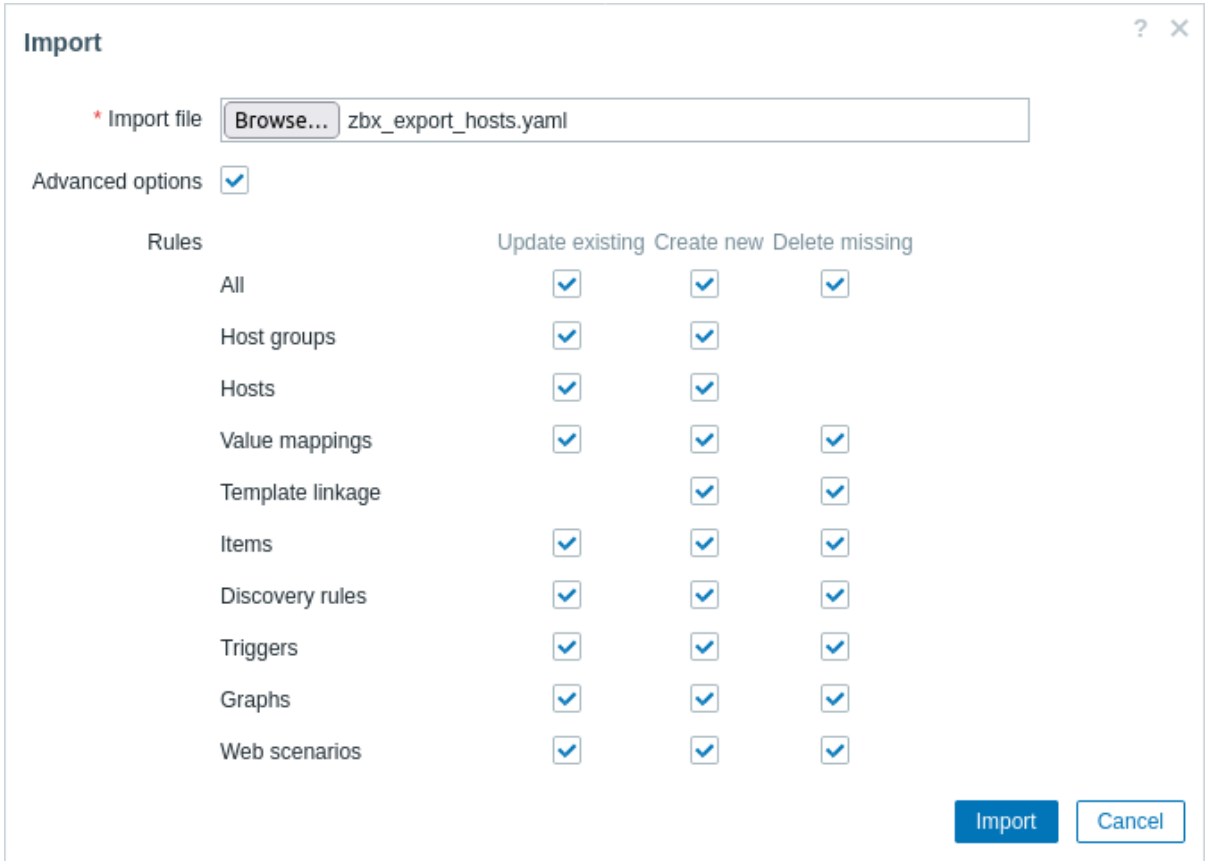
W zależności od wybranego formatu hosty są eksportowane do pliku lokalnego z domyślną nazwą:

- `zabbix_export_hosts.yaml` — w eksporcie YAML (domyślna opcja eksportu);
- `zabbix_export_hosts.xml` — w eksporcie XML;
- `zabbix_export_hosts.json` — w eksporcie JSON.

Importowanie

Aby zaimportować hosty, wykonaj następujące czynności:

1. Przejdź do *Data collection* → *Hosts*.
2. Kliknij *Import* w prawym górnym rogu.
3. Wybierz plik importu.
4. Kliknij *Import* w prawym dolnym rogu formularza konfiguracji.



Jeśli zaznaczysz pole wyboru *Advanced options*, zostanie wyświetlona szczegółowa lista wszystkich elementów możliwych do importu — zaznacz lub odznacz każdą regułę importu zgodnie z potrzebami.

Jeśli klikniesz pole wyboru w wierszu *All*, wszystkie elementy poniżej zostaną zaznaczone/odznaczone.

Reguły importu:

Reguła	Opis
Update existing	Istniejące elementy zostaną zaktualizowane przy użyciu danych z pliku importu. W przeciwnym razie nie zostaną zaktualizowane.
Create new	Nowe elementy zostaną utworzone przy użyciu danych z pliku importu. W przeciwnym razie nie zostaną utworzone.
Delete missing	Istniejące elementy, które nie są obecne w pliku importu, zostaną usunięte. W przeciwnym razie nie zostaną usunięte. Jeśli opcja *Delete missing* jest zaznaczona dla *Template linkage*, bieżące powiązania z szablonami, których nie ma w pliku importu, zostaną odłączone. Encje (pozycje, wyzwalacze, wykresy itp.) dziedziczone z odłączonych szablonów nie zostaną usunięte (chyba że opcja *Delete missing* zostanie również wybrana dla każdej encji).

Komunikat o powodzeniu lub niepowodzeniu importu zostanie wyświetlony we frontend.

Format eksportu

Gdy host jest eksportowany, Zabbix generuje uporządkowany format YAML, JSON lub XML. Eksport obejmuje elementy hosta, takie jak metadane hosta, pozycje, makra, wyzwalacze i inne.

Każdy element pełni określoną funkcję i może zawierać elementy zagnieżdżone.

W kolejnych sekcjach opisano każdy element w formacie eksportu. W przykładach użyto hosta z szablonem MySQL by Zabbix agent 2. Na potrzeby demonstracji elementów szablon jest odłączany po utworzeniu hosta. Odłączenie zachowuje wszystkie elementy w konfiguracji (w przeciwieństwie do odłączenia i wyczyszczenia, które je usuwa).

Wielokropek (`...`) oznacza elementy pominięte dla zwięzłości. Uwaga (`see table below`) jest używana, gdy dany element jest bardziej szczegółowo wyjaśniony w dalszych sekcjach.

```
zabbix_export:
  version: '8.0'
```

```
  host_groups:
    - uuid: 748ad4d098d447d492bb935c907f652f
      name: Databases
  hosts: (zobacz tabelę poniżej)
  graphs: (zobacz tabelę poniżej)
```

Metadane hosta

Element		Type	Description
version		string	(wymagane) Wersja Zabbix.
host_groups			(wymagane) Element główny dla grup hostów.
	uuid	string	(wymagane) Unikalny identyfikator tej grupy hostów.
	name	string	(wymagane) Nazwa grupy hostów.
hosts			Element główny dla hostów.
graphs			Element główny dla wykresów hosta.

```
zabbix_export:
  (...)
  hosts:
    - host: 'MySQL server'
      name: 'MySQL server'
      groups:
        - name: Databases
      interfaces: (zobacz tabelę poniżej)
      items: (zobacz tabelę poniżej)
      discovery_rules: (zobacz tabelę poniżej)
      tags:
        - tag: location
          value: Riga
      macros:
        (...)
        - macro: '{$MYSQL.DSN}'
          value: 192.0.2.0
        (...)
        - macro: '{$MYSQL.PASSWORD}'
          type: SECRET_TEXT
          description: 'Hasło użytkownika MySQL.'
        (...)
      valuemaps: (zobacz tabelę poniżej)
  (...)
```

Hosty

Element	Type	Opis
host	string	(wymagane) Unikalna nazwa hosta.
name	string	Widoczna nazwa hosta.
description	text	Opis hosta.
monitored_by	string	Sposób monitorowania hosta. Możliwe wartości:[1] SERVER (0, domyślnie), PROXY (1) lub PROXY_GROUP (2).
proxy		Element główny dla proxy.
name	string	(wymagane) Nazwa proxy (jeśli istnieje), który monitoruje hosta.
proxy_group		Element główny dla grupy proxy.
name	string	(wymagane) Nazwa grupy proxy (jeśli istnieje), która jest używana do monitorowania hosta.
status	string	Status hosta. Możliwe wartości:[1] ENABLED (0, domyślnie), DISABLED (1).
ipmi_authtype	string	Typ uwierzytelniania sesji IPMI. Możliwe wartości:[1] DEFAULT (-1, domyślnie), NONE (0), MD2 (1), MD5 (2), STRAIGHT (4), OEM (5), RMCP_PLUS (6).

Element	Type	Opis
ipmi_privilege	string	Poziom uprawnień sesji IPMI. Możliwe wartości:[1] CALLBACK (1), USER (2, domyślnie), OPERATOR (3), ADMIN (4), OEM (5).
ipmi_username	string	Nazwa użytkownika dla kontroli IPMI.
ipmi_password	string	Hasło dla kontroli IPMI.
templates		Element główny dla podłączonych szablonów.
name	string	(wymagane) Nazwa szablonu.
groups		Element główny dla grup hostów, do których należy host.
name	string	(wymagane) Nazwa grupy hostów.
interfaces		Element główny dla interfejsów hosta.
items		Element główny dla pozycji hosta.
discovery_rules		Element główny dla reguł niskopoziomowego wykrywania hosta.
http_tests		Element główny dla scenariuszy WWW hosta.
tags		Element główny dla tagów hosta.
tag	string	(wymagane) Nazwa tagu.
value	string	Wartość tagu.
macros		Element główny dla makr hosta.
macro	string	(wymagane) Nazwa makra użytkownika.
type	string	Typ makra użytkownika. Możliwe wartości:[1] TEXT (0, domyślnie), SECRET_TEXT (1), VAULT (2).
value	string	Wartość makra użytkownika.
description	string	Opis makra użytkownika.
inventory		Element główny dla inwentarza hosta.
<inventory_property>	string	Właściwość inwentarza. Wszystkie właściwości mają odpowiadający im element (`type`, `name`, `os` itd.; przykład można znaleźć w Export format).
inventory_mode	string	Tryb inwentarza. Możliwe wartości:[1] DISABLED (-1), MANUAL (0, domyślnie), AUTOMATIC (1).
valuemaps		Element główny dla map wartości hosta.

Note:
Zobacz także: Host object (odnieś się do odpowiedniej właściwości o pasującej nazwie).

Interfejsy hosta

```
zabbix_export:
  (...)
  hosts:
    - host: 'MySQL server'
      (...)
      interfaces:
        - ip: 192.0.2.0
          interface_ref: if1
      (...)
```

Element	Type	Opis
default	string	Czy jest to podstawowy interfejs hosta. Należy pamiętać, że na hoście może istnieć tylko jeden podstawowy interfejs danego typu. Możliwe wartości:[1] NO (0), YES (1, domyślnie).
type	string	Typ interfejsu. Możliwe wartości:[1] ZABBIX (1, domyślnie), SNMP (2), IPMI (3), JMX (4).
useip	string	Czy używać adresu IP jako interfejsu do łączenia z hostem (w przeciwnym razie zostanie użyty DNS). Możliwe wartości:[1] NO (0), YES (1, domyślnie).
ip	string	(wymagane dla połączeń IP) Adres IP (IPv4 lub IPv6).
dns	string	(wymagane dla połączeń DNS) Nazwa DNS.
port	string	Numer portu.
details		Element główny dla szczegółów interfejsu.
version	string	Użyj tej wersji SNMP. Możliwe wartości:[1] SNMPV1 (1), SNMP_V2C (2, domyślnie), SNMP_V3 (3).
community	string	(wymagane dla pozycji SNMPv1 i SNMPv2) Społeczność SNMP.

Element	Type	Opis
max_repetitions	string	Maksymalna wartość powtórzeń dla natywnych żądań zbiorczych SNMP (GetBulkRequest-PDUs). Obsługiwane dla pozycji SNMPv2 i SNMPv3 (pozycje `discovery[]` i `walk[]`). Domyślnie: 10.
contextname	string	Nazwa kontekstu SNMPv3. Obsługiwane dla pozycji SNMPv3.
securityname	string	Nazwa zabezpieczeń SNMPv3. Obsługiwane dla pozycji SNMPv3.
securitylevel	string	Poziom zabezpieczeń SNMPv3. Obsługiwane dla pozycji SNMPv3. Możliwe wartości:[1] NOAUTHNOPRIV (0, domyślnie), AUTHNOPRIV (1), AUTHPRIV (2).
authprotocol	string	Protokół uwierzytelniania SNMPv3. Obsługiwane dla pozycji SNMPv3. Możliwe wartości:[1] MD5 (0, domyślnie), SHA1 (1), SHA224 (2), SHA256 (3), SHA384 (4), SHA512 (5).
authpassphrase	string	Hasło uwierzytelniania SNMPv3. Obsługiwane dla pozycji SNMPv3.
privprotocol	string	Protokół prywatności SNMPv3. Obsługiwane dla pozycji SNMPv3. Możliwe wartości:[1] DES (0, domyślnie), AES128 (1), AES192 (2), AES256 (3), AES192C (4), AES256C (5).
privpassphrase	string	Hasło prywatności SNMPv3. Obsługiwane dla pozycji SNMPv3.
bulk	string	Używaj żądań zbiorczych dla SNMP. Możliwe wartości:[1] NO (0), YES (1, domyślnie).
interface_ref	string	Nazwa referencyjna interfejsu używana w pozycjach (format: `if<N>`).

Note:
Zobacz także: Host interface object (odpowiednia właściwość o pasującej nazwie).

Pozycje hosta

```
zabbix_export:
  (...)
  hosts:
    - host: 'MySQL server'
      (...)
      items:
        (...)
        - name: 'Binlog cache disk use'
          type: DEPENDENT
          key: mysql.binlog_cache_disk_use
          value_type: FLOAT
          description: 'Liczba transakcji, które użyły tymczasowej pamięci podręcznej na dysku, ponieważ n
          preprocessing: (zobacz tabelę poniżej)
          master_item:
            key: 'mysql.get_status_variables["{$MYSQL.DSN}","{$MYSQL.USER}","{$MYSQL.PASSWORD}"]'
          tags:
            - tag: component
              value: cache
        (...)
        - name: 'Buffer pool utilization'
          type: CALCULATED
          key: mysql.buffer_pool_utilization
          value_type: FLOAT
          units: '%'
          params: |
            ( last(//mysql.innodb_buffer_pool_pages_total) -
            last(//mysql.innodb_buffer_pool_pages_free) ) /
            ( last(//mysql.innodb_buffer_pool_pages_total) +
            ( last(//mysql.innodb_buffer_pool_pages_total) = 0 ) ) * 100 *
```

```
        ( last(//mysql.innodb_buffer_pool_pages_total) > 0 )
      description: 'Stosunek używanych stron do całkowitej liczby stron w puli buforów.'
      tags:
        - tag: component
          value: memory
      triggers: (zobacz tabelę poniżej)
    (...)
    - name: Uptime
      type: DEPENDENT
      key: mysql.uptime
      units: uptime
      description: 'Liczba sekund, przez które serwer działał.'
      preprocessing: (zobacz tabelę poniżej)
      master_item:
        key: 'mysql.get_status_variables["{$MYSQL.DSN}","{$MYSQL.USER}","{$MYSQL.PASSWORD}"]'
      tags:
        - tag: component
          value: application
      triggers: (zobacz tabelę poniżej)
    (...)
```

Element	Type	Opis
name	string	(wymagane) Nazwa pozycji.
type	string	Typ pozycji. Możliwe wartości:[1] ZABBIX_PASSIVE (0, domyślnie), TRAP (2), SIMPLE (3), INTERNAL (5), ZABBIX_ACTIVE (7), EXTERNAL (10), ODBC (11), IPMI (12), SSH (13), TELNET (14), CALCULATED (15), JMX (16), SNMP_TRAP (17), DEPENDENT (18), HTTP_AGENT (19), SNMP_AGENT (20), ITEM_TYPE_SCRIPT (21), ITEM_TYPE_BROWSER (22), ITEM_TYPE_NESTED (23).
snmp_oid	string	(wymagane dla pozycji SNMP_AGENT) ID obiektu SNMP.
key	string	(wymagane) Klucz pozycji.
delay	string	Interwał aktualizacji pozycji. Domyślnie: 1m. Wartość będzie zawsze wynosić 0 dla pozycji TRAP.
history	string	Okres czasu (z użyciem sufiksu czasu, makra użytkownika lub makra LLD) określający, jak długo dane historii powinny być przechowywane. Domyślnie: 31d.
trends	string	Okres czasu (z użyciem sufiksu czasu, makra użytkownika lub makra LLD) określający, jak długo dane trendów powinny być przechowywane. Domyślnie: 365d.
status	string	Status pozycji. Możliwe wartości:[1] ENABLED (0, domyślnie), DISABLED (1).
value_type	string	Typ otrzymywanej wartości. Możliwe wartości:[1] FLOAT (0), CHAR (1), LOG (2), UNSIGNED (3, domyślnie), TEXT (4), BINARY (5), JSON (6).
allowed_hosts	string	Lista adresów IP hostów rozdzielonych przecinkami, którym wolno wysyłać dane dla pozycji. Obsługiwane dla pozycji TRAP i HTTP_AGENT.
units	string	Jednostki otrzymywanej wartości (bps, B itp.).
params	text	Dodatkowe parametry zależne od typu pozycji (wykonywany skrypt dla pozycji SSH i TELNET; zapytanie SQL dla pozycji ODBC; formuła dla pozycji CALCULATED; skrypt dla pozycji ITEM_TYPE_SCRIPT i ITEM_TYPE_BROWSER).
ipmi_sensor	string	Czujnik IPMI. Obsługiwane dla pozycji IPMI.
authtype	string	Typ uwierzytelniania. Obsługiwane dla pozycji SSH i HTTP_AGENT. Możliwe wartości dla pozycji SSH:[1] PASSWORD (0, domyślnie), PUBLIC_KEY (1). Możliwe wartości dla pozycji HTTP_AGENT:[1] NONE (0, domyślnie), BASIC (1), NTLM (2), Kerberos (3) lub Digest (4).
username	string	(wymagane dla pozycji SSH i TELNET) Nazwa użytkownika do uwierzytelniania. Obsługiwane dla pozycji SIMPLE, ODBC, JMX i HTTP_AGENT. W przypadku użycia dla pozycji JMX należy również określić `password` (zobacz poniżej) albo pozostawić oba elementy puste.

Element	Type	Opis
password	string	(wymagane dla pozycji SSH i TELNET) Hasło do uwierzytelniania. Obsługiwane dla pozycji SIMPLE, ODBC, JMX i HTTP_AGENT. W przypadku użycia dla pozycji JMX należy również określić `username` (zobacz powyżej) albo pozostawić oba elementy puste.
publickey	string	(wymagane dla pozycji SSH) Nazwa pliku klucza publicznego.
privatekey	string	(wymagane dla pozycji SSH) Nazwa pliku klucza prywatnego.
description	text	Opis pozycji.
inventory_link	string	Pole inwentarza hosta, które jest wypełniane przez pozycję. Możliwe wartości:[1] NONE (0), ALIAS (4) itd. (obsługiwane pola można znaleźć w Inwentarz hosta).
valuemap		Element główny dla map wartości pozycji.
name	string	(wymagane) Nazwa mapy wartości używanej dla pozycji.
logtimefmt	string	Format czasu we wpisach dziennika. Obsługiwane dla pozycji o typie wartości LOG.
preprocessing		Element główny dla wstępnego przetwarzania wartości pozycji.
step		Element główny dla kroków wstępnego przetwarzania wartości pozycji hosta.
interface_ref	string	Odwołanie do interfejsu hosta (format: `if<N>`).
jmx_endpoint	string	Punkt końcowy JMX. Obsługiwane dla pozycji JMX.
master_item		(wymagane dla pozycji DEPENDENT) Element główny dla pozycji nadrzędnej pozycji zależnej.
key	string	(wymagane) Klucz pozycji nadrzędnej pozycji zależnej.
timeout	string	Limit czasu żądania odpytywania danych pozycji. Obsługiwane dla listy typów pozycji Timeouts.
url	string	(wymagane dla pozycji HTTP_AGENT) Ciąg URL.
query_fields		Element główny dla parametrów zapytania. Obsługiwane dla pozycji HTTP_AGENT.
name	string	(wymagane dla pozycji HTTP_AGENT) Nazwa parametru zapytania.
value	string	Wartość parametru zapytania. Obsługiwane dla pozycji HTTP_AGENT.
parameters		Element główny dla parametrów zdefiniowanych przez użytkownika. Obsługiwane dla pozycji ITEM_TYPE_SCRIPT i ITEM_TYPE_BROWSER.
name	string	(wymagane dla pozycji ITEM_TYPE_SCRIPT i ITEM_TYPE_BROWSER) Nazwa parametru zdefiniowanego przez użytkownika.
value	string	Wartość parametru zdefiniowanego przez użytkownika. Obsługiwane dla pozycji ITEM_TYPE_SCRIPT i ITEM_TYPE_BROWSER.
posts	string	Dane treści żądania HTTP(S). Obsługiwane dla pozycji HTTP_AGENT.
status_codes	string	Zakresy wymaganych kodów statusu HTTP, rozdzielone przecinkami. Obsługiwane dla pozycji HTTP_AGENT.
follow_redirects	string	Czy podążać za przekierowaniami odpowiedzi podczas odpytywania danych. Obsługiwane dla pozycji HTTP_AGENT. Możliwe wartości:[1] NO (0), YES (1, domyślnie).
post_type	string	Typ treści danych wysyłanych metodą POST. Obsługiwane dla pozycji HTTP_AGENT. Możliwe wartości:[1] RAW (0, domyślnie), JSON (2), XML (3).
http_proxy	string	Ciąg połączenia proxy HTTP(S). Obsługiwane dla pozycji HTTP_AGENT.
headers		Element główny dla nagłówków żądania HTTP(S). Obsługiwane dla pozycji HTTP_AGENT.
name	string	(wymagane dla pozycji HTTP_AGENT) Nazwa nagłówka.
value	string	(wymagane dla pozycji HTTP_AGENT) Wartość nagłówka.
retrieve_mode	string	Która część odpowiedzi ma być przechowywana. Obsługiwane dla pozycji HTTP_AGENT. Możliwe wartości:[1] BODY (0, domyślnie), HEADERS (1), BOTH (2).
request_method	string	Typ metody żądania. Obsługiwane dla pozycji HTTP_AGENT. Możliwe wartości:[1] GET (0, domyślnie), POST (1), PUT (2), HEAD (3).
output_format	string	Sposób przetwarzania odpowiedzi. Obsługiwane dla pozycji HTTP_AGENT. Możliwe wartości:[1] RAW (0, domyślnie), JSON (1).

Element	Type	Opis
allow_traps	string	Zezwala na wypełnianie wartości podobnie jak w pozycji trapper. Obsługiwane dla pozycji HTTP_AGENT. Możliwe wartości:[1] NO (0, domyślnie), YES (1).
ssl_cert_file	string	Ścieżka do pliku publicznego klucza SSL. Obsługiwane dla pozycji HTTP_AGENT.
ssl_key_file	string	Ścieżka do pliku prywatnego klucza SSL. Obsługiwane dla pozycji HTTP_AGENT.
ssl_key_password	string	Hasło do pliku klucza SSL. Obsługiwane dla pozycji HTTP_AGENT.
verify_peer	string	Czy weryfikować, że certyfikat hosta jest autentyczny. Obsługiwane dla pozycji HTTP_AGENT. Możliwe wartości:[1] NO (0, domyślnie), YES (1).
verify_host	string	Czy weryfikować, że nazwa hosta dla połączenia odpowiada nazwie w certyfikacie hosta. Obsługiwane dla pozycji HTTP_AGENT. Możliwe wartości:[1] NO (0, domyślnie), YES (1).
tags		Element główny dla tagów pozycji.
tag	string	(wymagane) Nazwa tagu.
value	string	Wartość tagu.
triggers		Element główny dla wyzwalaczy pozycji hosta.

Note:
Zobacz także: Item object (odwołaj się do odpowiedniej właściwości o pasującej nazwie).

Kroki wstępnego przetwarzania wartości pozycji hosta

```
zabbix_export:
  (...)
  hosts:
    - host: 'MySQL server'
      (...)
      items:
        (...)
        - name: 'Binlog cache disk use'
          (...)
          preprocessing:
            - type: JSONPATH
              parameters:
                - $.Binlog_cache_disk_use
            - type: DISCARD_UNCHANGED_HEARTBEAT
              parameters:
                - 6h
          (...)
```

Element	Type	Description
type	string	(wymagane) Typ kroku wstępnego przetwarzania wartości pozycji. Możliwe wartości:[1] MULTIPLIER (1), RTRIM (2), LTRIM (3), TRIM (4), REGEX (5), BOOL_TO_DECIMAL (6), OCTAL_TO_DECIMAL (7), HEX_TO_DECIMAL (8), SIMPLE_CHANGE (9, obliczane: otrzymana wartość - poprzednia wartość), CHANGE_PER_SECOND (10, obliczane: (otrzymana wartość - poprzednia wartość)/(bieżący czas - czas ostatniego sprawdzenia)), XMLPATH (11), JSONPATH (12), IN_RANGE (13), MATCHES_REGEX (14), NOT_MATCHES_REGEX (15), CHECK_JSON_ERROR (16), CHECK_XML_ERROR (17), CHECK_REGEX_ERROR (18), DISCARD_UNCHANGED (19), DISCARD_UNCHANGED_HEARTBEAT (20), JAVASCRIPT (21), PROMETHEUS_PATTERN (22), PROMETHEUS_TO_JSON (23), CSV_TO_JSON (24), STR_REPLACE (25), CHECK_NOT_SUPPORTED (26), XML_TO_JSON (27), SNMP_WALK_VALUE (28), SNMP_WALK_TO_JSON (29), SNMP_GET_VALUE (30).
parameters		(wymagane) Element główny dla parametrów kroku wstępnego przetwarzania wartości pozycji.
parameter	string	Indywidualny parametr kroku wstępnego przetwarzania wartości pozycji.

Element	Type	Description
error_handler	string	Typ akcji używany w przypadku niepowodzenia kroku wstępnego przetwarzania. Możliwe wartości:[1] ORIGINAL_ERROR (0, domyślnie), DISCARD_VALUE (1), CUSTOM_VALUE (2), CUSTOM_ERROR (3).
error_handler_params	string	Parametry obsługi błędów.

Note:
Zobacz także: Item preprocessing object (odnieś się do odpowiedniej właściwości o pasującej nazwie).

Wyzwalacze pozycji hosta

```
zabbix_export:
  (...)
  hosts:
    - host: 'MySQL server'
      (...)
      items:
        (...)
        - name: Uptime
          (...)
          triggers:
            - expression: 'nodata(/MySQL server/mysql.uptime,30m)=1'
              name: 'MySQL: Failed to fetch info data'
              event_name: 'MySQL: Failed to fetch info data (or no data for 30m)'
              priority: INFO
              description: 'Zabbix has not received any data for items for the last 30 minutes.'
              dependencies:
                - name: 'MySQL: Service is down'
                  expression: 'last(/MySQL server/mysql.ping["{$MYSQL.DSN}","{$MYSQL.USER}","{$MYSQL.PASSW
              tags:
                - tag: scope
                  value: availability
            - expression: 'last(/MySQL server/mysql.uptime)<10m'
              name: 'MySQL: Service has been restarted'
              event_name: 'MySQL: Service has been restarted (uptime < 10m)'
              priority: INFO
              description: 'MySQL uptime is less than 10 minutes.'
              tags:
                - tag: scope
                  value: notice
        (...)
```

Element	Type	Opis
uuid	string	(wymagane) Unikalny identyfikator tego wyzwalacza.
expression	string	(wymagane) Wyrażenie wyzwalacza.
recovery_mode	string	Podstawa generowania zdarzeń OK. Możliwe wartości:[1] EXPRESSION (0, domyślnie), RECOVERY_EXPRESSION (1), NONE (2).
recovery_expression	string	Wyrażenie odzyskiwania wyzwalacza.
correlation_mode	string	Tryb korelacji (brak korelacji zdarzeń lub korelacja zdarzeń według tagu). Możliwe wartości:[1] DISABLED (0, domyślnie), TAG_VALUE (1).
correlation_tag	string	Nazwa tagu używana do korelacji zdarzeń.
name	string	(wymagane) Nazwa wyzwalacza.
event_name	string	Nazwa zdarzenia.
opdata	string	Dane operacyjne.
url_name	string	Etykieta adresu URL powiązanego z wyzwalaczem.
url	string	Adres URL powiązany z wyzwalaczem.
status	string	Status wyzwalacza. Możliwe wartości:[1] ENABLED (0, domyślnie), DISABLED (1).
priority	string	Poziom ważności wyzwalacza. Możliwe wartości:[1] NOT_CLASSIFIED (0, domyślnie), INFO (1), WARNING (2), AVERAGE (3), HIGH (4), DISASTER (5).

Element	Type	Opis
description	text	Opis wyzwalacza.
type	string	Typ generowania zdarzeń (pojedyncze zdarzenie problemu lub wiele zdarzeń problemu). Możliwe wartości:[1] SINGLE (0, domyślnie), MULTIPLE (1).
manual_close	string	Ręczne zamykanie zdarzeń problemu. Możliwe wartości:[1] NO (0, domyślnie), YES (1).
dependencies		Element główny dla zależności.
name	string	(wymagane) Nazwa wyzwalacza zależności.
expression	string	(wymagane) Wyrażenie wyzwalacza zależności.
recovery_expression	string	Wyrażenie odzyskiwania wyzwalacza zależności.
tags		Element główny dla tagów wyzwalacza.
tag	string	(wymagane) Nazwa tagu.
value	string	Wartość tagu.

Note:
Zobacz także: Trigger object (odnieś się do odpowiedniej właściwości o pasującej nazwie).

Reguły wykrywania niskiego poziomu hosta

```
zabbix_export:
  (...)
  hosts:
    - host: 'MySQL server'
      (...)
      discovery_rules:
        - name: 'Database discovery'
          key: 'mysql.db.discovery["{$MYSQL.DSN}","{$MYSQL.USER}","{$MYSQL.PASSWORD}"]'
          delay: 1h
          filter: (see table below)
          description: 'Scanning databases in DBMS.'
          interface_ref: if1
          item_prototypes:
            - name: 'Size of database {#DATABASE}'
              key: 'mysql.db.size["{$MYSQL.DSN}","{$MYSQL.USER}","{$MYSQL.PASSWORD}","{#DATABASE}"]'
              delay: 5m
              units: B
              description: 'Database size.'
              preprocessing:
                - type: DISCARD_UNCHANGED_HEARTBEAT
                  parameters:
                    - 1h
              interface_ref: if1
              tags:
                - tag: component
                  value: storage
                - tag: database
                  value: '{#DATABASE}'
          lld_macro_paths:
            - lld_macro: '{#DATABASE}'
              path: $.Database
          preprocessing:
            - type: DISCARD_UNCHANGED_HEARTBEAT
              parameters:
                - 1d
        (...)
```

Attention:
Większość elementów reguł wykrywania niskiego poziomu hosta jest taka sama jak w przypadku pozycji hosta. Poniższa tabela opisuje te elementy, które różnią się od pozycji hosta.

Element	Type	Opis
type	string	Typ pozycji. Możliwe wartości:[1] ZABBIX_PASSIVE (0, domyślnie), TRAP (2), SIMPLE (3), INTERNAL (5), ZABBIX_ACTIVE (7), EXTERNAL (10), ODBC (11), IPMI (12), SSH (13), TELNET (14), JMX (16), DEPENDENT (18), HTTP_AGENT (19), SNMP_AGENT (20), ITEM_TYPE_SCRIPT (21), ITEM_TYPE_BROWSER (22).
key	string	(wymagane) Klucz reguły wykrywania niskiego poziomu.
filter		Element główny dla filtrów reguł wykrywania niskiego poziomu hosta.
lifetime	string	Okres czasu (z użyciem sekund, sufiksu czasu lub makra użytkownika), po którym zasoby, które nie są już wykrywane, zostaną usunięte. Domyślnie: 7d.
lifetime_type	string	Scenariusz usuwania utraconych zasobów LLD. Możliwe wartości: DELETE_NEVER, DELETE_IMMEDIATELY, DELETE_AFTER.
enabled_lifetime	string	Okres czasu (z użyciem sekund, sufiksu czasu lub makra użytkownika), po którym zasoby, które nie są już wykrywane, zostaną wyłączone.
enabled_lifetime_type	string	Scenariusz wyłączania utraconych zasobów LLD. Możliwe wartości: DISABLE_NEVER, DISABLE_IMMEDIATELY, DISABLE_AFTER.
item_prototypes		Element główny dla elementów prototypów pozycji hosta, które są takie same jak dla pozycji hosta.
trigger_prototypes		Element główny dla elementów prototypów wyzwalaczy hosta, które są takie same jak dla wyzwalaczy pozycji hosta.
graph_prototypes		Element główny dla prototypów wykresów hosta, które są takie same jak dla wykresów hosta.
host_prototypes		Element główny dla prototypów hosta, które są takie same jak dla hostów.
parent_discovery_rule		Element główny dla nadrzędnej reguły wykrywania niskiego poziomu (lub prototypu reguły) prototypu reguły wykrywania niskiego poziomu. Ta właściwość oznacza, że jest to prototyp reguły LLD, będący bezpośrednim elementem podrzędnym wskazanej reguły/prototypu reguły.
key	string	(wymagane) Klucz nadrzędnej reguły wykrywania niskiego poziomu (lub prototypu reguły).
master_item	string	(wymagane dla reguł DEPENDENT) Element główny dla pozycji nadrzędnej reguły zależnej.
lld_macro_paths		Element główny dla ścieżek makr reguły wykrywania niskiego poziomu.
lld_macro	string	(wymagane) Nazwa makra reguły wykrywania niskiego poziomu.
path	string	(wymagane) Selektor wartości, która zostanie przypisana do odpowiedniego makra.
preprocessing		Element główny dla wstępnego przetwarzania wartości reguły wykrywania niskiego poziomu.
step		Element główny dla elementów kroków wstępnego przetwarzania wartości reguły wykrywania niskiego poziomu, które są takie same jak dla kroków wstępnego przetwarzania wartości pozycji hosta, z wyjątkiem mniejszej liczby możliwych wartości. Zobacz także: obiekt wstępnego przetwarzania reguły LLD.
overrides		Element główny dla reguł nadpisywania reguły wykrywania niskiego poziomu.
name	string	(wymagane) Unikalna nazwa nadpisania.
step	string	(wymagane) Unikalny numer kolejności nadpisania.
stop	string	Zatrzymaj przetwarzanie kolejnych nadpisań, jeśli pasuje.
filter		Element główny dla elementów filtra reguły nadpisywania reguły wykrywania niskiego poziomu, które są takie same jak dla filtrów reguł wykrywania niskiego poziomu hosta.
operations		Element główny dla operacji nadpisywania reguły wykrywania niskiego poziomu hosta.

Note:
Zobacz także: obiekt reguły LLD (odnieś się do odpowiedniej właściwości o pasującej nazwie).

Filtry reguły wykrywania niskiego poziomu hosta

```
zabbix_export:
  (...)
  hosts:
    - host: 'MySQL server'
      (...)
      discovery_rules:
        - name: 'Database discovery'
          (...)
```

```
        filter:
          evaltype: AND
          conditions:
            - macro: '{#DATABASE}'
              value: '{$MYSQL.DBNAME.MATCHES}'
            - macro: '{#DATABASE}'
              value: '{$MYSQL.DBNAME.NOT_MATCHES}'
              operator: NOT_MATCHES_REGEX
        (...)
```

Element	Type	Opis
evaltype	string	Nadpisuje metodę oceny warunków filtra. Możliwe wartości:[1] AND_OR (0, domyślnie), AND (1), OR (2), FORMULA (3).
formula	string	Niestandardowa formuła obliczeniowa dla warunków filtra.
conditions		Element główny dla warunków filtra.
macro	string	(wymagane) Nazwa makra wykrywania niskiego poziomu, dla którego ma zostać wykonane sprawdzenie.
value	string	Wartość do porównania.
operator	string	Operator warunku. Możliwe wartości:[1] MATCHES_REGEX (8, domyślnie), NOT_MATCHES_REGEX (9).
formulaid	string	(wymagane) Dowolny unikalny identyfikator używany do odwoływania się do warunku z poziomu wyrażenia niestandardowego. Może zawierać wyłącznie wielkie litery. Identyfikator musi zostać zdefiniowany przez użytkownika podczas modyfikowania warunków filtra, ale zostanie wygenerowany ponownie przy późniejszym żądaniu ich pobrania.

Note:
Zobacz także: obiekt filtra reguły LLD (odnieś się do odpowiedniej właściwości o pasującej nazwie).

Operacje nadpisania reguły wykrywania niskopoziomowego hosta

Element	Type	Opis
operationobject	string	Obiekt, do którego stosowana jest operacja. Możliwe wartości:[1] ITEM_PROTOTYPE (0), TRIGGER_PROTOTYPE (1), GRAPH_PROTOTYPE (2), HOST_PROTOTYPE (3), DISCOVERY_PROTOTYPE (4).
operator	string	Operator warunku nadpisania. Możliwe wartości:[1] EQUAL (1), NOT_EQUAL (2), LIKE (3), NOT_LIKE (4), REGEXP (5), NOT_REGEXP (6).
value	string	Wyrażenie regularne lub ciąg znaków dla operatora warunku nadpisania.
status	string	Status obiektu po operacji nadpisania.
discover	string	Czy obiekt jest dodawany w wyniku wykrywania.
delay	string	Interwał aktualizacji ustawiony dla prototypu pozycji po operacji nadpisania.
history	string	Okres przechowywania historii ustawiony dla prototypu pozycji po operacji nadpisania.
trends	string	Okres przechowywania trendów ustawiony dla prototypu pozycji po operacji nadpisania.
severity	string	Istotność prototypu wyzwalacza ustawiona po operacji nadpisania.
tags		Element główny dla tagów ustawionych dla obiektu po operacji nadpisania.
tag	string	(wymagane) Nazwa tagu.
value	string	Wartość tagu.
templates		Element główny dla szablonów podłączonych do prototypu hosta po operacji nadpisania.
name	string	(wymagane) Nazwa szablonu.
inventory_mode	string	Tryb inwentaryzacji prototypu hosta ustawiony po operacji nadpisania.

Note:
Zobacz także: Obiekt operacji nadpisania reguły LLD (odnieś się do odpowiedniej właściwości o pasującej nazwie).

Scenariusze WWW hosta

Element	Type	Opis
uuid	string	(wymagane) Unikalny identyfikator tego scenariusza WWW.
name	string	(wymagane) Nazwa scenariusza WWW.
delay	string	Częstotliwość wykonywania scenariusza WWW (z użyciem sekund, sufiksu czasu lub makra użytkownika). Domyślnie: 1m.
attempts	integer	Liczba prób wykonania kroków scenariusza WWW. Możliwe wartości: 1-10 (domyślnie: 1).
agent	string	Agent klienta. Zabbix będzie udawał wybraną przeglądarkę. Jest to przydatne, gdy witryna zwraca różną zawartość dla różnych przeglądarek. Domyślnie: Zabbix.
http_proxy	string	Proxy, który będzie używany przez scenariusz WWW, podany w postaci: `http://[username[:password]@]proxy.example.com[:port]`
variables		Element główny dla zmiennych scenariusza WWW, które mogą być używane w krokach scenariusza.
name	string	(wymagane) Nazwa zmiennej.
value	text	(wymagane) Wartość zmiennej.
headers		Element główny dla nagłówków HTTP wysyłanych podczas wykonywania żądania. Nagłówki powinny być podane z użyciem tej samej składni, w jakiej występują w protokole HTTP.
name	string	(wymagane) Nazwa nagłówka.
value	text	(wymagane) Wartość nagłówka.
status	string	Status scenariusza WWW. Możliwe wartości:[1] ENABLED (0, domyślnie), DISABLED (1).
authentication	string	Metoda uwierzytelniania. Możliwe wartości:[1] NONE (0, domyślnie), BASIC (1), NTLM (2), Kerberos (3) lub Digest (4).
http_user	string	Nazwa użytkownika używana do uwierzytelniania BASIC (HTTP), NTLM, Kerberos lub Digest.
http_password	string	Hasło używane do uwierzytelniania BASIC (HTTP), NTLM, Kerberos lub Digest.
verify_peer	string	Weryfikacja certyfikatu SSL serwera WWW. Możliwe wartości:[1] NO (0, domyślnie), YES (1).
verify_host	string	Weryfikacja zgodności pola *Common Name* lub pola *Subject Alternate Name* certyfikatu serwera WWW. Możliwe wartości:[1] NO (0, domyślnie), YES (1).
ssl_cert_file	string	Nazwa pliku certyfikatu SSL używanego do uwierzytelniania klienta (musi być w formacie PEM).
ssl_key_file	string	Nazwa pliku klucza prywatnego SSL używanego do uwierzytelniania klienta (musi być w formacie PEM).
ssl_key_password	string	Hasło pliku klucza prywatnego SSL.
steps		(wymagane) Element główny dla kroków scenariusza WWW hosta.
tags		Element główny dla tagów scenariusza WWW.
tag	string	(wymagane) Nazwa tagu.
value	string	Wartość tagu.

Note:
Zobacz także: Obiekt scenariusza WWW (odnieś się do odpowiedniej właściwości o pasującej nazwie).

Kroki scenariusza WWW hosta

Element	Type	Opis
name	string	(wymagane) Nazwa kroku scenariusza WWW.
url	string	(wymagane) URL do monitorowania.
query_fields		Element główny parametrów zapytania (tablica pól HTTP, które mają zostać dodane do URL podczas wykonywania żądania).
name	string	(wymagane) Nazwa parametru zapytania.
value	string	Wartość parametru zapytania.
posts		Element główny zmiennych HTTP POST (ciąg znaków (surowe dane POST) lub tablica pól HTTP (dane pól formularza)).
name	string	(wymagane) Nazwa pola POST.

Element	Type	Opis
value	string	(wymagane) Wartość pola POST.
variables		Element główny zmiennych na poziomie kroku (makr), które powinny zostać zastosowane po tym kroku. Jeśli wartość zmiennej ma prefiks 'regex:', to jej wartość jest wyodrębniana z danych zwróconych przez ten krok zgodnie ze wzorcem wyrażenia regularnego następującym po prefiksie 'regex:'
name	string	(wymagane) Nazwa zmiennej.
value	text	(wymagane) Wartość zmiennej.
headers		Element główny nagłówków HTTP, które mają zostać wysłane podczas wykonywania żądania.
name	string	(wymagane) Nazwa nagłówka.
value	text	(wymagane) Wartość nagłówka.
follow_redirects	string	Podążanie za przekierowaniami HTTP. Możliwe wartości:[1] NO (0), YES (1, domyślnie).
retrieve_mode	string	Tryb pobierania odpowiedzi HTTP. Możliwe wartości:[1] BODY (0, domyślnie), HEADERS (1), BOTH (2).
timeout	string	Limit czasu wykonania kroku (z użyciem sekund, sufiksu czasu lub makra użytkownika). Domyślnie: 15s.
required	string	Tekst, który musi występować w odpowiedzi (ignorowany, jeśli pusty).
status_codes	string	Lista akceptowanych kodów statusu HTTP rozdzielonych przecinkami (np. 200-201,210-299; ignorowana, jeśli pusta).

Note:
Zobacz także: Obiekt kroku scenariusza WWW (odnieś się do odpowiedniej właściwości o pasującej nazwie).

Wykresy hosta

```
zabbix_export:
  (...)
  graphs:
    - name: 'MySQL: Bandwidth'
      graph_items: (zobacz tabelę poniżej)
    (...)
```

Element	Type	Opis
uuid	string	Unikalny identyfikator wykresu.
name	string	(wymagane) Nazwa wykresu.
width	integer	Szerokość wykresu w pikselach. Używana do podglądu oraz dla wykresów kołowych/rozsuniętych. Możliwe wartości:[1] 20-65535 (domyślnie: 900).
height	integer	Wysokość wykresu w pikselach. Używana do podglądu oraz dla wykresów kołowych/rozsuniętych. Możliwe wartości:[1] 20-65535 (domyślnie: 900).
yaxismin	double	Wartość minimum osi Y. Obsługiwane dla STAŁEJ wartości minimalnej osi Y. Domyślnie: 0.
yaxismax	double	Wartość maksimum osi Y. Obsługiwane dla STAŁEJ wartości minimalnej osi X. Domyślnie: 0.
show_work_period	string	Wyróżnij godziny poza czasem pracy. Obsługiwane dla wykresów NORMAL i STACKED. Możliwe wartości:[1] NO (0), YES (1, domyślnie).
show_triggers	string	Wyświetl proste wartości wyzwalaczy jako linię. Obsługiwane dla wykresów NORMAL i STACKED. Możliwe wartości:[1] NO (0), YES (1, domyślnie).
type	string	Typ wykresu. Możliwe wartości:[1] NORMAL (0, domyślnie), STACKED (1), PIE (2), EXPLODED (3).
show_legend	string	Wyświetl legendę wykresu. Możliwe wartości:[1] NO (0), YES (1, domyślnie).

Element	Type	Opis
show_3d	string	Włącz styl 3D. Obsługiwane dla wykresów NORMAL i STACKED. Możliwe wartości:[1] NO (0, domyślnie), YES (1).
percent_left	double	Pokaż linię percentyla dla lewej osi. Obsługiwane dla wykresów NORMAL. Domyślnie: 0.
percent_right	double	Pokaż linię percentyla dla prawej osi. Obsługiwane dla wykresów NORMAL. Domyślnie: 0.
ymin_type_1	string	Minimalna wartość osi Y. Obsługiwane dla wykresów NORMAL i STACKED. Możliwe wartości:[1] CALCULATED (0, domyślnie), FIXED (1), ITEM (2).
ymin_item_1		(wymagane, jeśli `ymin_type_1` jest ustawione na `ITEM`) Element główny dla szczegółów indywidualnej pozycji.
host	string	(wymagane) Host pozycji.
key	string	(wymagane) Klucz pozycji.
ymax_type_1	string	Maksymalna wartość osi Y. Obsługiwane dla wykresów NORMAL i STACKED. Możliwe wartości:[1] CALCULATED (0, domyślnie), FIXED (1), ITEM (2).
ymax_item_1		(wymagane, jeśli `ymax_type_1` jest ustawione na `ITEM`) Element główny dla szczegółów indywidualnej pozycji.
host	string	(wymagane) Host pozycji.
key	string	(wymagane) Klucz pozycji.
graph_items		(wymagane) Element główny dla pozycji wykresu hosta.

Note:
Zobacz także: Graph object (odnieś się do odpowiedniej właściwości o pasującej nazwie).

Pozycje wykresu hosta

```
zabbix_export:
  (...)
  graphs:
    - name: 'MySQL: Bandwidth'
      graph_items:
        - drawtype: GRADIENT_LINE
          color: 199C0D
          item:
            host: 'MySQL server'
            key: mysql.bytes_received.rate
        - sortorder: '1'
          drawtype: GRADIENT_LINE
          color: F63100
          item:
            host: 'MySQL server'
            key: mysql.bytes_sent.rate
    (...)
```

Element	Type	Opis
sortorder	integer	Kolejność rysowania. Mniejsza wartość jest rysowana jako pierwsza. Może być używana do rysowania linii lub obszarów za (lub przed) innym elementem.
drawtype	string	Styl rysowania pozycji wykresu. Obsługiwane dla wykresów NORMAL. Możliwe wartości:[1] SINGLE_LINE (0, domyślnie), FILLED_REGION (1), BOLD_LINE (2), DOTTED_LINE (3), DASHED_LINE (4), GRADIENT_LINE (5).
color	string	Kolor elementu (6 znaków, hex).
yaxisside	string	Strona wykresu, po której będzie rysowana skala Y pozycji wykresu. Obsługiwane dla wykresów NORMAL i STACKED graphs.

Element	Type	Opis
calc_fnc	string	Dane do narysowania, jeśli dla pozycji istnieje więcej niż jedna wartość. Możliwe wartości:[1] MIN (1), AVG (2, domyślnie), MAX (4), ALL (7; minimum, średnia i maksimum; obsługiwane dla wykresów prostych), LAST (9, obsługiwane dla wykresów kołowych/rozsuniętych).
type	string	Typ pozycji wykresu. Możliwe wartości:[1] SIMPLE (0, domyślnie), GRAPH_SUM (2; wartość pozycji reprezentuje cały wykres kołowy; obsługiwane dla wykresów kołowych/rozsuniętych).
item		(wymagane) Indywidualna pozycja.
host	string	(wymagane) Host pozycji.
key	string	(wymagane) Klucz pozycji.

Note:
Zobacz także: Graph item object (odpowiednia właściwość o pasującej nazwie).

Mapy wartości hosta

```
zabbix_export:
  (...)
  hosts:
    - host: 'MySQL server'
      (...)
      valuemaps:
        - name: Przykładowa mapa wartości
          mappings:
            - value: '1'
              newvalue: Przykładowa wartość
  (...)
```

Element	Type	Opis
uuid	string	(wymagane) Unikalny identyfikator tej mapy wartości.
name	string	(wymagane) Nazwa mapy wartości.
mapping		Element główny dla mapowań.
type	string	Typ dopasowania mapowania. Możliwe wartości:[1] EQUAL (0, domyślnie), GREATER_OR_EQUAL (2), LESS_OR_EQUAL (3), IN_RANGE (4), REGEXP (5), DEFAULT (6).
value	string	Wartość oryginalna.
newvalue	string	(wymagane) Wartość, na którą mapowana jest wartość oryginalna.

Note:
Zobacz także: Value map object (odpowiednia właściwość o pasującej nazwie).

Przypisy [1] Wartości całkowite API w nawiasach, na przykład ENABLED (0), są podane wyłącznie w celach informacyjnych. Więcej informacji można znaleźć na stronie powiązanego obiektu API wskazanej w odpowiednim wpisie tabeli lub na końcu każdej sekcji.

5 Mapy sieciowe

Przegląd

Export mapy sieci zawiera:

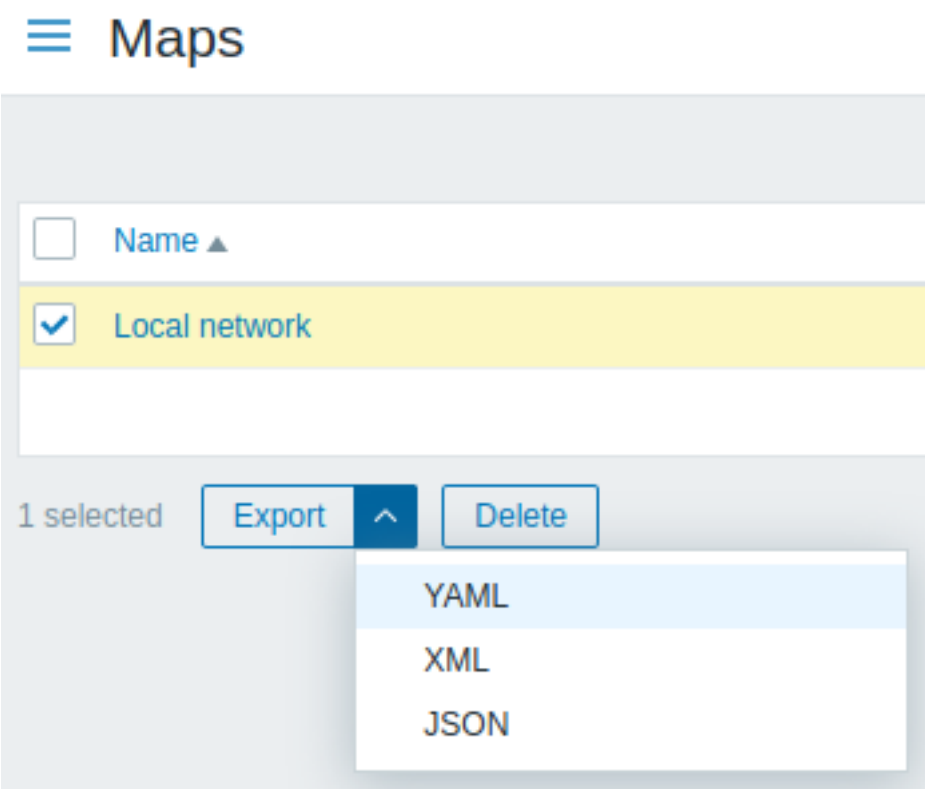
- Wszystkie powiązane obrazy
- Strukturę mapy (wszystkie ustawienia mapy, wszystkie zawarte elementy wraz z ich ustawieniami, łącza mapy oraz wskaźniki statusu łączy mapy)

Warning:
Żadne grupy hostów, hosty, wyzwalacze, inne mapy ani inne elementy, które mogą być powiązane z eksportowaną mapą, nie są eksportowane. Dlatego jeśli brakuje co najmniej jednego z elementów, do których odwołuje się mapa, jej import się nie powiedzie.

Eksportowanie

Aby wyeksportować mapy sieci, wykonaj następujące czynności:

1. Przejdź do *Monitoring* → *Maps*.
2. Zaznacz pola wyboru map sieci, które chcesz wyeksportować.
3. Kliknij *Export* pod listą.



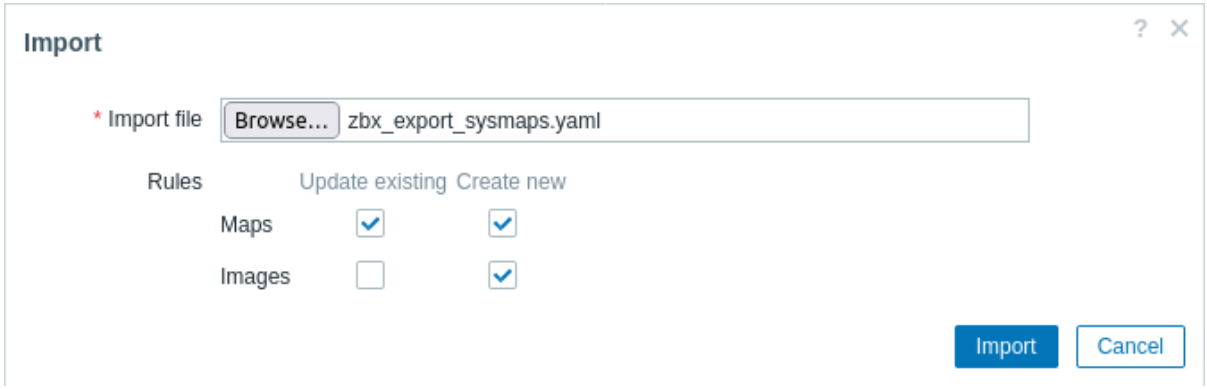
W zależności od wybranego formatu mapy są eksportowane do pliku lokalnego z domyślną nazwą:

- `zabbix_export_maps.yaml` — w eksporcie YAML (domyślna opcja eksportu);
- `zabbix_export_maps.xml` — w eksporcie XML;
- `zabbix_export_maps.json` — w eksporcie JSON.

Importowanie

Aby zaimportować mapy sieci, wykonaj następujące czynności:

1. Przejdź do *Monitoring* → *Maps*.
2. Kliknij *Import* w prawym górnym rogu.
3. Wybierz plik importu.
4. Zaznacz wymagane opcje w regułach importu.
5. Kliknij *Import* w prawym dolnym rogu formularza konfiguracji.



Reguły importu:

Reguła	Opis
Update existing	Istniejące mapy zostaną zaktualizowane przy użyciu danych z pliku importu. W przeciwnym razie nie zostaną zaktualizowane.
Create new	Nowe mapy zostaną utworzone przy użyciu danych z pliku importu. W przeciwnym razie nie zostaną utworzone.

Jeśli odznaczysz obie opcje map i zaznaczysz odpowiednie opcje dla obrazów, zaimportowane zostaną tylko obrazy. Importowanie obrazów jest dostępne tylko dla użytkowników *Super admin*.

W frontend zostanie wyświetlony komunikat o powodzeniu lub niepowodzeniu importu.

Warning:
Jeśli zastąpisz istniejący obraz, wpłynie to na wszystkie mapy, które używają tego obrazu.

Format eksportu

Eksport do YAML:

```
zabbix_export:
  version: '8.0'
  images:
    - name: Zabbix_server_3D_(128)
      imagetype: '1'
      encodedImage: iVBOR...5CYII=
  maps:
    - name: 'Sieć lokalna'
      width: '680'
      height: '200'
      label_type: '0'
      label_location: '0'
      highlight: '1'
      expandproblem: '1'
      markelements: '1'
      show_unack: '0'
      severity_min: '0'
      show_suppressed: '0'
      grid_size: '50'
      grid_show: '1'
      grid_align: '1'
      label_format: '0'
      label_type_host: '2'
      label_type_hostgroup: '2'
      label_type_trigger: '2'
      label_type_map: '2'
      label_type_image: '2'
      label_string_host: ''
      label_string_hostgroup: ''
      label_string_trigger: ''
```

```
    label_string_map: ''
    label_string_image: ''
    expand_macros: '1'
    background: {  }
    iconmap: {  }
    urls: {  }
    selements:
      - elementtype: '0'
        elements:
          - host: 'Serwer Zabbix'
        label: |
          {HOST.NAME}
          {HOST.CONN}
        label_location: '0'
        x: '111'
        'y': '61'
        elementsubtype: '0'
        areatype: '0'
        width: '200'
        height: '200'
        viewtype: '0'
        use_iconmap: '0'
        selementid: '1'
        icon_off:
          name: Zabbix_server_3D_(128)
        icon_on: {  }
        icon_disabled: {  }
        icon_maintenance: {  }
        urls: {  }
        evaltype: '0'
    shapes:
      - type: '0'
        x: '0'
        'y': '0'
        width: '680'
        height: '15'
        text: '{MAP.NAME}'
        font: '9'
        font_size: '11'
        font_color: '000000'
        text_halign: '0'
        text_valign: '0'
        border_type: '0'
        border_width: '0'
        border_color: '000000'
        background_color: ''
        zindex: '0'
    lines: {  }
    links: {  }
```

Eksportowane elementy Wyeksportowane elementy są objaśnione w poniższej tabeli.

Element	Type	Description
images		Element główny dla obrazów.
name	string	Unikalna nazwa obrazu.
imagetype	integer	Typ obrazu. Możliwe wartości: 1 - Obraz; 2 - Tło.
encodedImage	string	Obraz zakodowany w Base64.
maps		Element główny dla map.

Mapy

Element	Type	Opis
name	string	Unikalna nazwa mapy.
width	integer	Szerokość mapy w pikselach.
height	integer	Wysokość mapy w pikselach.
label_type	integer	Typ etykiety elementu mapy. Możliwe wartości: 0 - Etykieta; 1 - Adres IP hosta; 2 - Nazwa elementu; 3 - Tylko status; 4 - Nic.
label_location	integer	Domyślne położenie etykiety elementu mapy. Możliwe wartości: 0 - Dół; 1 - Lewo; 2 - Prawo; 3 - Góra.
highlight	integer	Włącz podświetlanie ikon dla aktywnych wyzwalaczy i statusów hostów. Możliwe wartości: 0 - Nie; 1 - Tak.
expandproblem	integer	Wyświetlaj wyzwalacz problemu dla elementów z pojedynczym problemem. Możliwe wartości: 0 - Nie; 1 - Tak.
markelements	integer	Podświetlaj elementy mapy, których status ostatnio się zmienił. Możliwe wartości: 0 - Nie; 1 - Tak.
show_unack	integer	Wyświetlanie problemów. Możliwe wartości: 0 - Liczba wszystkich problemów; 1 - Liczba niepotwierdzonych problemów; 2 - Liczba potwierdzonych i niepotwierdzonych problemów osobno.
severity_min	integer	Minimalny poziom ważności wyzwalacza wyświetlany domyślnie na mapie. Możliwe wartości: 0 - Niesklasyfikowany; 1 - Informacja; 2 - Ostrzeżenie; 3 - Średni; 4 - Wysoki; 5 - Katastrofa.
show_suppressed	integer	Wyświetlaj problemy, które w przeciwnym razie byłyby wyciszone (niewyświetlane) z powodu konserwacji hosta. Możliwe wartości: 0 - Nie; 1 - Tak.
grid_size	integer	Rozmiar komórki siatki mapy w pikselach. Obsługiwane, jeśli `grid_show` jest ustawione na 0. Możliwe wartości: 20, 40, 50, 75 lub 100.
grid_show	integer	Wyświetlaj siatkę w konfiguracji mapy. Możliwe wartości: 0 - Tak; 1 - Nie.
grid_align	integer	Automatycznie wyrównuj ikony w konfiguracji mapy. Możliwe wartości: 0 - Tak; 1 - Nie.

Element	Type	Opis
label_format	integer	Użyj zaawansowanej konfiguracji etykiet. Możliwe wartości: 0 - Nie; 1 - Tak.
label_type_host	integer	Wyświetlaj etykietę jako etykietę hosta. Obsługiwane, jeśli `label_format` jest ustawione na 1. Możliwe wartości: 0 - Etykieta; 1 - Adres IP hosta; 2 - Nazwa elementu; 3 - Tylko status; 4 - Nic; 5 - Etykieta niestandardowa.
label_type_hostgroup	integer	Wyświetlaj etykietę jako etykietę grupy hostów. Obsługiwane, jeśli `label_format` jest ustawione na 1. Możliwe wartości: 0 - Etykieta; 2 - Nazwa elementu; 3 - Tylko status; 4 - Nic; 5 - Etykieta niestandardowa.
label_type_trigger	integer	Wyświetlaj etykietę jako etykietę wyzwalacza. Obsługiwane, jeśli `label_format` jest ustawione na 1. Możliwe wartości: 0 - Etykieta; 2 - Nazwa elementu; 3 - Tylko status; 4 - Nic; 5 - Etykieta niestandardowa.
label_type_map	integer	Wyświetlaj etykietę jako etykietę mapy. Obsługiwane, jeśli `label_format` jest ustawione na 1. Możliwe wartości: 0 - Etykieta; 2 - Nazwa elementu; 3 - Tylko status; 4 - Nic; 5 - Etykieta niestandardowa.
label_type_image	integer	Wyświetlaj etykietę jako etykietę obrazu. Obsługiwane, jeśli `label_format` jest ustawione na 1. Możliwe wartości: 0 - Etykieta; 2 - Nazwa elementu; 4 - Nic; 5 - Etykieta niestandardowa.
label_string_host	string	Etykieta niestandardowa dla elementów hosta. Obsługiwane, jeśli `label_type_host` jest ustawione na 5.
label_string_hostgroup	string	Etykieta niestandardowa dla elementów grupy hostów. Obsługiwane, jeśli `label_type_hostgroup` jest ustawione na 5.
label_string_trigger	string	Etykieta niestandardowa dla elementów wyzwalacza. Obsługiwane, jeśli `label_type_trigger` jest ustawione na 5.
label_string_map	string	Etykieta niestandardowa dla elementów mapy. Obsługiwane, jeśli `label_type_map` jest ustawione na 5.
label_string_image	string	Etykieta niestandardowa dla elementów obrazu. Obsługiwane, jeśli `label_type_image` jest ustawione na 5.
expand_macros	integer	Rozwijaj makra w etykietach w konfiguracji mapy. Możliwe wartości: 0 - Nie; 1 - Tak.
background		Element główny obrazu tła (jeśli istnieje). Obsługiwane, jeśli `imagetype` jest ustawione na 2.
name	string	Nazwa obrazu tła.

Element		Type	Opis
iconmap			Element główny mapowania ikon (jeśli istnieje).
	name	string	Nazwa mapowania ikon.
urls			Element główny adresów URL używanych przez mapy lub każdy element mapy.
	name	string	Nazwa linku.
	url	string	Adres URL linku.
	elementtype	integer	Typ pozycji mapy, do którego należy link. Możliwe wartości: 0 - Host; 1 - Mapa; 2 - Wyzwalacz; 3 - Grupa hostów; 4 - Obraz.
selements			Element główny dla selements mapy.
shapes			Element główny dla kształtów mapy.
	type	integer	Typ kształtu. Możliwe wartości: 0 - Prostokąt; 1 - Elipsa.
	x	integer	Współrzędne X kształtu w pikselach.
	y	integer	Współrzędne Y kształtu w pikselach.
	width	integer	Szerokość kształtu.
	height	integer	Wysokość kształtu.
	text	string	Tekst wewnątrz kształtu.
	font	integer	Styl czcionki tekstu. Możliwe wartości: 0 - Georgia, serif; 1 - ”Palatino Linotype”, ”Book Antiqua”, Palatino, serif; 2 - ”Times New Roman”, Times, serif; 3 - Arial, Helvetica, sans-serif; 4 - ”Arial Black”, Gadget, sans-serif; 5 - ”Comic Sans MS”, cursive, sans-serif; 6 - Impact, Charcoal, sans-serif; 7 - ”Lucida Sans Unicode”, ”Lucida Grande”, sans-serif; 8 - Tahoma, Geneva, sans-serif; 9 - ”Trebuchet MS”, Helvetica, sans-serif; 10 - Verdana, Geneva, sans-serif; 11 - ”Courier New”, Courier, monospace; 12 - ”Lucida Console”, Monaco, monospace.
	font_size	integer	Rozmiar czcionki w pikselach.
	font_color	string	Kolor czcionki przedstawiony w kodzie szesnastkowym.
	text_halign	integer	Wyrównanie poziome tekstu. Możliwe wartości: 0 - Środek; 1 - Lewo; 2 - Prawo.
	text_valign	integer	Wyrównanie pionowe tekstu. Możliwe wartości: 0 - Środek; 1 - Góra; 2 - Dół.
	border_type	integer	Typ obramowania kształtu. Możliwe wartości: 0 - Brak; 1 - Linia pogrubiona; 2 - Linia kropkowana; 3 - Linia przerywana.
	border_width	integer	Szerokość obramowania w pikselach.
	border_color	string	Kolor obramowania przedstawiony w kodzie szesnastkowym.
	background_color	string	Kolor tła (wypełnienia) przedstawiony w kodzie szesnastkowym.
	zindex	integer	Wartość określająca kolejność wszystkich kształtów i linii (z-index).
lines			Element główny dla linii mapy.

Element	Type	Opis
x1	integer	Współrzędne X punktu 1 linii w pikselach.
y1	integer	Współrzędne Y punktu 1 linii w pikselach.
x2	integer	Współrzędne X punktu 2 linii w pikselach.
y2	integer	Współrzędne Y punktu 2 linii w pikselach.
line_type	integer	Typ linii. Możliwe wartości: 0 - Brak; 1 - Linia pogrubiona; 2 - Linia kropkowana; 3 - Linia przerywana.
line_width	integer	Szerokość linii w pikselach.
line_color	string	Kolor linii przedstawiony w kodzie szesnastkowym.
zindex	integer	Wartość określająca kolejność wszystkich kształtów i linii (z-index).
links		Element główny dla połączeń między elementami mapy.
drawtype	integer	Styl połączenia. Możliwe wartości: 0 - Linia; 2 - Linia pogrubiona; 3 - Linia kropkowana; 4 - Linia przerywana.
color	string	Kolor połączenia (6 znaków, hex).
label	string	Etykieta połączenia.
selementid1	id	ID jednego elementu do połączenia.
selementid2	id	ID drugiego elementu do połączenia.
linktriggers		Element główny dla wskaźników statusu połączeń.

Note:
Zobacz także: Map object (odwołaj się do odpowiedniej właściwości o pasującej nazwie).

Selementy mapy

Element	Type	Opis
elementtype	integer	Typ elementu mapy. Możliwe wartości: 0 - Host; 1 - Mapa; 2 - Wyzwalacz; 3 - Grupa hostów; 4 - Obraz.
elements		Element główny dla encji Zabbix (host, grupa hostów, mapa itp.), które są reprezentowane na mapie. Wszystkie encje mają swoje odpowiednie elementy (`host` itp.; zobacz na przykład Format eksportu).
label	string	Etykieta ikony.
label_location	integer	Położenie etykiety. Możliwe wartości: -1 - Użyj wartości domyślnej mapy; 0 - Dół; 1 - Lewo; 2 - Prawo; 3 - Góra.
x	integer	Położenie na osi X.
y	integer	Położenie na osi Y.
elementsubtype	integer	Podtyp elementu. Obsługiwane, jeśli `elementtype` jest ustawione na 3. Możliwe wartości: 0 - Pojedyncza grupa hostów; 1 - Wszystkie grupy hostów.

Element	Type	Opis
areatype	integer	Rozmiar obszaru. Obsługiwane, jeśli `elementtype` jest ustawione na 1. Możliwe wartości: 0 - Taki sam jak cała mapa; 1 - Rozmiar niestandardowy.
width	integer	Szerokość obszaru. Obsługiwane, jeśli `areatype` jest ustawione na 1.
height	integer	Wysokość obszaru. Obsługiwane, jeśli `areatype` jest ustawione na 1.
viewtype	integer	Algorytm rozmieszczania obszaru. Obsługiwane, jeśli `elementsubtype` jest ustawione na 1. Możliwe wartości: 0 - Rozmieść równomiernie w obszarze.
use_iconmap	integer	Użyj mapowania ikon dla tego elementu. Ma znaczenie tylko wtedy, gdy mapowanie ikon jest aktywowane na poziomie mapy. Możliwe wartości: 0 - Nie; 1 - Tak.
selementid	id	Unikalny identyfikator rekordu elementu.
icon_off		Element główny obrazu używanego, gdy element jest w stanie `OK`.
name	string	Unikalna nazwa obrazu.
icon_on		Element główny obrazu używanego, gdy element jest w stanie `Problem`.
name	string	Unikalna nazwa obrazu.
icon_disabled		Element główny obrazu używanego, gdy element jest wyłączony.
name	string	Unikalna nazwa obrazu.
icon_maintenance		Element główny obrazu używanego, gdy element jest w konserwacji.
name	string	Unikalna nazwa obrazu.
urls		Element główny dla adresów URL używanych przez mapy lub każdy element mapy.
name	string	Nazwa linku.
url	string	Adres URL linku.
evaltype	integer	Typ oceny dla tagów.
tags		Element główny dla tagów problemów (dla elementów hosta i grupy hostów). Jeśli podano tagi, na mapie będą wyświetlane tylko problemy z tymi tagami.
tag	string	Nazwa tagu.
value	string	Wartość tagu.
operator	integer	Operator.

Note:
Zobacz także: Obiekt elementu mapy (odnieś się do odpowiedniej właściwości o pasującej nazwie).

Wskaźniki statusu łącza mapy

Element	Type	Opis
drawtype	integer	Styl łącza, gdy wyzwalacz jest w stanie „Problem”. Możliwe wartości: 0 - Linia; 2 - Linia pogrubiona; 3 - Linia kropkowana; 4 - Linia kreskowana.
color	string	Kolor łącza (6 znaków, hex), gdy wyzwalacz jest w stanie „Problem”.
trigger		Element główny dla wyzwalacza używanego do wskazywania statusu łącza.
description	string	Nazwa wyzwalacza.
expression	string	Wyrażenie wyzwalacza.
recovery_expression	string	Wyrażenie odzyskiwania wyzwalacza.

Note:
Zobacz także: Obiekt wyzwalacza łącza mapy (odpowiednia właściwość o pasującej nazwie).

6 Typy mediów

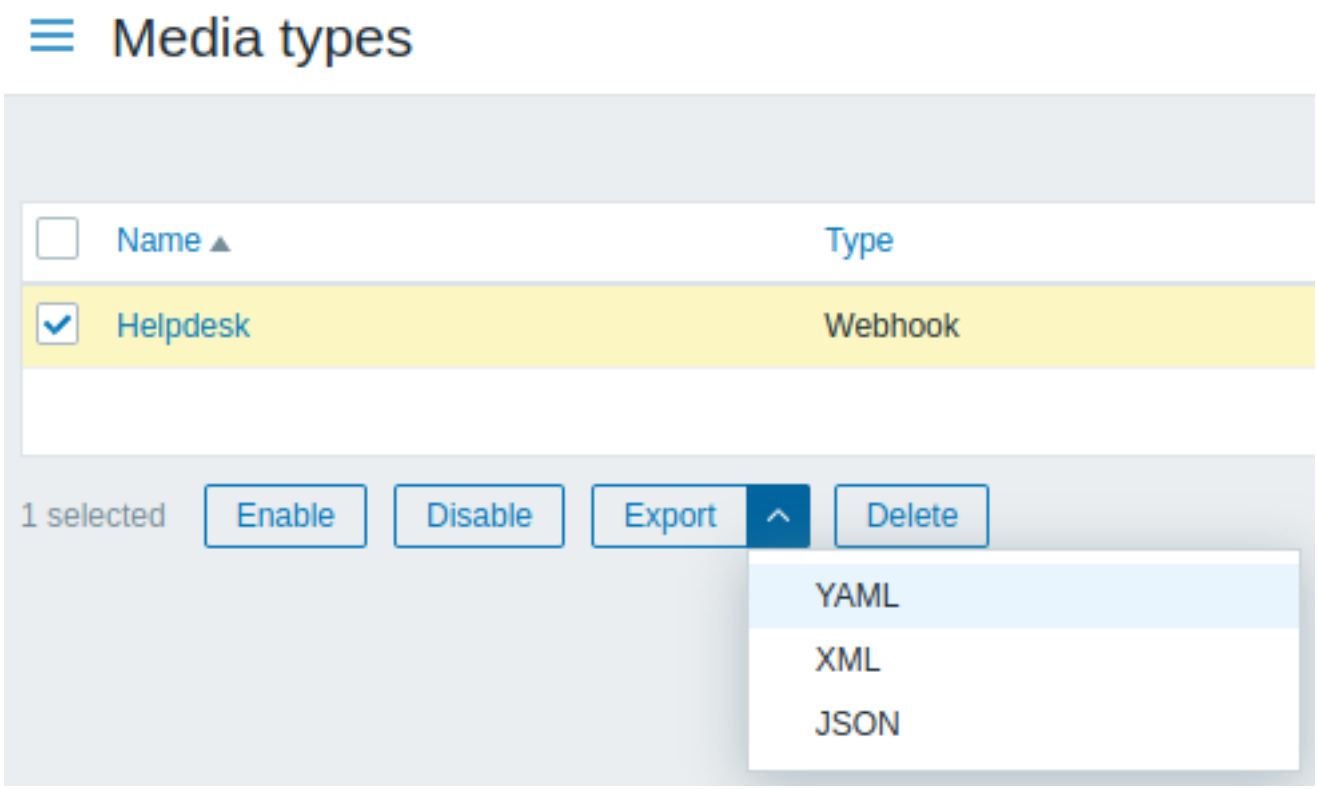
Przegląd

Typy mediów są eksportowane ze wszystkimi powiązanymi obiektami i relacjami obiektów.

Eksportowanie

Aby wyeksportować typy mediów, wykonaj następujące czynności:

1. Przejdź do *Alerty* → *Typy mediów*.
2. Zaznacz pola wyboru typów mediów, które chcesz wyeksportować.
3. Kliknij *Eksportuj* poniżej listy.



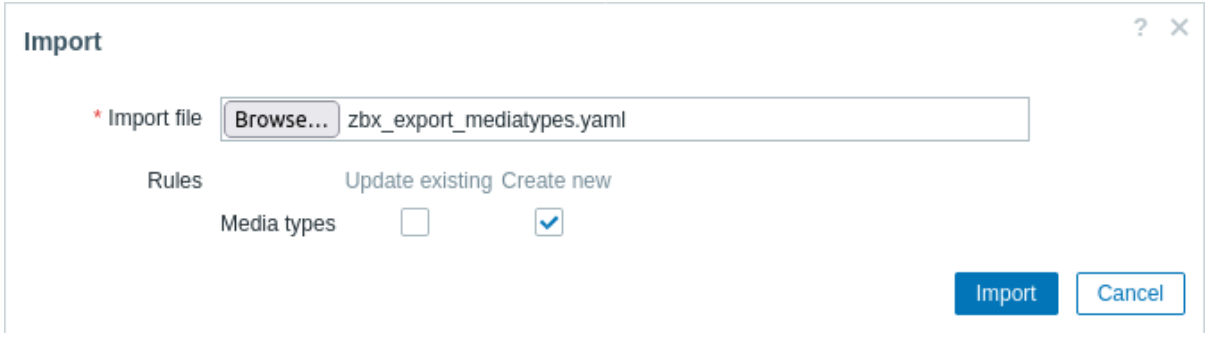
W zależności od wybranego formatu typy mediów są eksportowane do pliku lokalnego, który posiada domyślną nazwię:

- `zabbix_export_mediatypes.yaml` - przy eksporcie do YAML (domyślna opcja eksportu);
- `zabbix_export_mediatypes.xml` - przy eksporcie do XML;
- `zabbix_export_mediatypes.json` - przy eksporcie do JSON.

Importowanie

Aby zaimportować typy mediów, wykonaj następujące kroki:

1. Przejdź do *Alerts* → *Media types*.
2. Kliknij *Import* w prawym górnym rogu.
3. Wybierz plik importu.
4. Zaznacz wymagane opcje w regułach importu.
5. Kliknij *Import* w prawym dolnym rogu formularza konfiguracji.



Reguły importu:

Rule	Description
Update existing	Istniejące elementy zostaną zaktualizowane przy użyciu danych z pliku importu. W przeciwnym razie nie zostaną zaktualizowane.
Create new	Nowe elementy zostaną utworzone przy użyciu danych z pliku importu. W przeciwnym razie nie zostaną utworzone.

W frontend zostanie wyświetlony komunikat o powodzeniu lub niepowodzeniu importu.

Format eksportu

Eksport do YAML:

```yaml
zabbix_export:
  version: '8.0'
  media_types:
    - name: Pushover
      type: WEBHOOK
      parameters:
        - name: endpoint
          value: 'https://api.pushover.net/1/messages.json'
        - name: eventid
          value: '{EVENT.ID}'
        - name: event_nseverity
          value: '{EVENT.NSEVERITY}'
        - name: event_source
          value: '{EVENT.SOURCE}'
        - name: event_value
          value: '{EVENT.VALUE}'
        - name: expire
          value: '1200'
        - name: message
          value: '{ALERT.MESSAGE}'
        - name: priority_average
          value: '0'
        - name: priority_default
          value: '0'
        - name: priority_disaster
          value: '0'
        - name: priority_high
          value: '0'
        - name: priority_information
          value: '0'
        - name: priority_not_classified
          value: '0'
        - name: priority_warning
          value: '0'
        - name: retry
          value: '60'
        - name: title
          value: '{ALERT.SUBJECT}'
        - name: token
          value: '<PUSHOVER TOKEN HERE>'
        - name: triggerid
          value: '{TRIGGER.ID}'
        - name: url
          value: '{$ZABBIX.URL}'
        - name: url_title
          value: Zabbix
        - name: user
          value: '{ALERT.SENDTO}'
      status: DISABLED
```

```
    max_sessions: '0'
    script: |
      try {
          var params = JSON.parse(value),
              request = new HttpRequest(),
              data,
              response,
              severities = [
                  {name: 'not_classified', color: '#97AAB3'},
                  {name: 'information', color: '#7499FF'},
                  {name: 'warning', color: '#FFC859'},
                  {name: 'average', color: '#FFA059'},
                  {name: 'high', color: '#E97659'},
                  {name: 'disaster', color: '#E45959'},
                  {name: 'resolved', color: '#009900'},
                  {name: 'default', color: '#000000'}
              ],
              priority;

          if (typeof params.HTTPProxy === 'string' && params.HTTPProxy.trim() !== '') {
              request.setProxy(params.HTTPProxy);
          }

          if ([0, 1, 2, 3].indexOf(parseInt(params.event_source)) === -1) {
              throw 'Incorrect "event_source" parameter given: "' + params.event_source + '".\nMust be 0
          }

          if (params.event_value !== '0' && params.event_value !== '1'
              && (params.event_source === '0' || params.event_source === '3')) {
              throw 'Incorrect "event_value" parameter given: ' + params.event_value + '\nMust be 0 or 1
          }

          if ([0, 1, 2, 3, 4, 5].indexOf(parseInt(params.event_nseverity)) === -1) {
              params.event_nseverity = '7';
          }

          if (params.event_value === '0') {
              params.event_nseverity = '6';
          }

          priority = params['priority_' + severities[params.event_nseverity].name] || params.priority_de

          if (isNaN(priority) || priority < -2 || priority > 2) {
              throw '"priority" should be -2..2';
          }

          if (params.event_source === '0' && isNaN(params.triggerid)) {
              throw 'field "triggerid" is not a number';
          }

          if (isNaN(params.eventid)) {
              throw 'field "eventid" is not a number';
          }

          if (typeof params.message !== 'string' || params.message.trim() === '') {
              throw 'field "message" cannot be empty';
          }

          data = {
              token: params.token,
              user: params.user,
              title: params.title,
```

```
            message: params.message,
            url: (params.event_source === '0')
                ? params.url + '/tr_events.php?triggerid=' + params.triggerid + '&eventid=' + params.e
                : params.url,
            url_title: params.url_title,
            priority: priority
        };

        if (priority == 2) {
            if (isNaN(params.retry) || params.retry < 30) {
                throw 'field "retry" should be a number with value of at least 30 if "priority" is set

            if (isNaN(params.expire) || params.expire > 10800) {
                throw 'field "expire" should be a number with value of at most 10800 if "priority" is

            data.retry = params.retry;
            data.expire = params.expire;
        }

        data = JSON.stringify(data);
        Zabbix.log(4, '[ Pushover Webhook ] Sending request: ' + params.endpoint + '\n' + data);

        request.addHeader('Content-Type: application/json');
        response = request.post(params.endpoint, data);

        Zabbix.log(4, '[ Pushover Webhook ] Received response with status code ' + request.getStatus()

        if (response !== null) {
            try {
                response = JSON.parse(response);
            }
            catch (error) {
                Zabbix.log(4, '[ Pushover Webhook ] Failed to parse response received from Pushover');
                response = null;
            }
        }

        if (request.getStatus() != 200 || response === null || typeof response !== 'object' || respons
            if (response !== null && typeof response === 'object' && typeof response.errors === 'objec
                    && typeof response.errors[0] === 'string') {
                throw response.errors[0];
            }
            else {
                throw 'Unknown error. Check debug log for more information.';
            }
        }

        return 'OK';
    }
    catch (error) {
        Zabbix.log(4, '[ Pushover Webhook ] Pushover notification failed: ' + error);
        throw 'Pushover notification failed: ' + error;
    }
description: |
    Zapoznaj się z przewodnikiem konfiguracji tutaj: https://git.zabbix.com/projects/ZBX/repos/zabbix/

    Ustaw parametr token na klucz aplikacji Pushover.
    Podczas przypisywania nośnika Pushover do użytkownika Zabbix - dodaj klucz użytkownika w polu wyśl
message_templates:
    - event_source: TRIGGERS
      operation_mode: PROBLEM
```

```
      subject: 'Problem: {EVENT.NAME}'
      message: |
        Problem rozpoczął się o {EVENT.TIME} dnia {EVENT.DATE}
        Nazwa problemu: {EVENT.NAME}
        Host: {HOST.NAME}
        Ważność: {EVENT.SEVERITY}
        Dane operacyjne: {EVENT.OPDATA}
        ID oryginalnego problemu: {EVENT.ID}
        {TRIGGER.URL}
    - event_source: TRIGGERS
      operation_mode: RECOVERY
      subject: 'Rozwiązano w {EVENT.DURATION}: {EVENT.NAME}'
      message: |
        Problem został rozwiązany o {EVENT.RECOVERY.TIME} dnia {EVENT.RECOVERY.DATE}
        Nazwa problemu: {EVENT.NAME}
        Czas trwania problemu: {EVENT.DURATION}
        Host: {HOST.NAME}
        Ważność: {EVENT.SEVERITY}
        ID oryginalnego problemu: {EVENT.ID}
        {TRIGGER.URL}
    - event_source: TRIGGERS
      operation_mode: UPDATE
      subject: 'Zaktualizowano problem po {EVENT.AGE}: {EVENT.NAME}'
      message: |
        {USER.FULLNAME} {EVENT.UPDATE.ACTION} problem dnia {EVENT.UPDATE.DATE} o {EVENT.UPDATE.TIME}.
        {EVENT.UPDATE.MESSAGE}

        Bieżący stan problemu to {EVENT.STATUS}, wiek to {EVENT.AGE}, potwierdzono: {EVENT.ACK.STATUS}
    - event_source: DISCOVERY
      operation_mode: PROBLEM
      subject: 'Wykrywanie: {DISCOVERY.DEVICE.STATUS} {DISCOVERY.DEVICE.IPADDRESS}'
      message: |
        Reguła wykrywania: {DISCOVERY.RULE.NAME}

        IP urządzenia: {DISCOVERY.DEVICE.IPADDRESS}
        DNS urządzenia: {DISCOVERY.DEVICE.DNS}
        Stan urządzenia: {DISCOVERY.DEVICE.STATUS}
        Czas działania urządzenia: {DISCOVERY.DEVICE.UPTIME}

        Nazwa usługi urządzenia: {DISCOVERY.SERVICE.NAME}
        Port usługi urządzenia: {DISCOVERY.SERVICE.PORT}
        Stan usługi urządzenia: {DISCOVERY.SERVICE.STATUS}
        Czas działania usługi urządzenia: {DISCOVERY.SERVICE.UPTIME}
    - event_source: AUTOREGISTRATION
      operation_mode: PROBLEM
      subject: 'Autorejestracja: {HOST.HOST}'
      message: |
        Nazwa hosta: {HOST.HOST}
        IP hosta: {HOST.IP}
        Port agenta: {HOST.PORT}
```

Elementy eksportowane

Eksportowane elementy są wyjaśnione w poniższej tabeli.

Element	Typ	Opis
name	string	(wymagane) Nazwa typu mediów.
type	string	(wymagane) Typ komunikacji używany przez typ mediów. Możliwe wartości:[1] EMAIL (0), SMS (1), SCRIPT (2), WEBHOOK (4).
status	string	Czy typ mediów jest włączony. Możliwe wartości:[1] ENABLED (0, domyślne), DISABLED (1)

Element	Typ	Opis
max_sessions	integer	Maksymalna liczba alertów, które można przetwarzać równolegle. Możliwe wartości dla wiadomości SMS:[1] 1 (domyślnie). Możliwe wartości dla innych typów mediów:[1] 0-100 (gdzie 0 — bez ograniczeń).
attempts	integer	Maksymalna liczba prób wysłania alertu. Możliwe wartości:[1] 1-10 (domyślnie: 3).
attempt_interval	string	Interwał (z użyciem sekund lub przyrostka czasu) między kolejnymi próbami. Możliwe wartości:[1] 0-60 s (domyślnie: 10 s).
description	string	Opis typu mediów.
message_templates		Element główny szablonu wiadomości dla typu mediów.
event_source	string	(wymagane) Źródło zdarzenia. Możliwe wartości:[1] TRIGGERS (0), DISCOVERY (1), AUTOREGISTRATION (2), INTERNAL (3), SERVICE (4).
operation_mode	string	Tryb działania. Możliwe wartości:[1] PROBLEM (0), RECOVERY (1), UPDATE (2).
subject	string	Temat wiadomości.
message	string	Treść wiadomości.

Note:
Zobacz także: Obiekt typu mediów (odnieś się do odpowiedniej właściwości o pasującej nazwie).

E-mail

Następujące dodatkowe elementy są eksportowane tylko dla typu nośnika *E-mail*.

Element	Type	Opis
provider	string	Dostawca poczty e-mail.
smtp_server	string	Serwer SMTP.
smtp_port	integer	Port serwera SMTP, z którym ma zostać nawiązane połączenie. Domyślnie: 25.
smtp_helo	string	HELO SMTP.
smtp_email	string	Adres e-mail, z którego będą wysyłane powiadomienia.
smtp_security	string	Poziom zabezpieczeń połączenia SMTP do użycia. Możliwe wartości:[1] NONE (0, domyślnie), STARTTLS (1), SSL_OR_TLS (2).
smtp_verify_host	string	Weryfikacja hosta SSL dla SMTP. Możliwe wartości:[1] NO (0, domyślnie), YES (1).
smtp_verify_peer	string	Weryfikacja peera SSL dla SMTP. Możliwe wartości:[1] NO (0, domyślnie), YES (1).
smtp_authentication	string	Metoda uwierzytelniania SMTP do użycia. Możliwe wartości:[1] NONE (0, domyślnie), PASSWORD (1), OAUTH (2).
username	string	Nazwa użytkownika.
password	string	Hasło uwierzytelniające.
redirection_url	string	Adres URL frontendu Zabbix, do którego nastąpi przekierowanie po autoryzacji OAuth.
client_id	string	Identyfikator klienta zarejestrowany na serwerze autoryzacji OAuth.
authorization_url	string	Adres URL OAuth wraz z parametrami służący do uzyskania tokenów dostępu i odświeżania.
token_url	string	Adres URL OAuth służący do wymiany tokenu autoryzacyjnego na tokeny dostępu i odświeżania.
message_format	string	Format wiadomości. Możliwe wartości:[1] TEXT (0), HTML (1, domyślnie).

Note:
Zobacz także: Media type object (odpowiednia właściwość o pasującej nazwie).

SMS

Następujące dodatkowe elementy są eksportowane tylko dla typu mediów *SMS*.

Element	Typ	Opis
gsm_modem	string	(wymagane) Nazwa urządzenia szeregowego modemu GSM.

Note:
Zobacz także: Obiekt typu mediów (sprawdź odpowiednią właściwość z pasującą nazwą).

Skrypt

Następujące dodatkowe elementy są eksportowane tylko dla typu nośnika *Skrypt*.

Element	Typ	Opis
nazwa skryptu	string	(wymagane) Nazwa skryptu.
parametry		Element główny dla parametrów skryptu.
sortorder	string	(wymagane) Kolejność parametrów skryptu przekazywanych do skryptu jako argumenty wiersza poleceń.
wartość	string	Wartość parametru skryptu.

Note:
Zobacz także: Obiekt typu nośnika (sprawdź odpowiednią właściwość o pasującej nazwie).

Webhook

Następujące dodatkowe elementy są eksportowane tylko dla typu mediów *Webhook*.

Element	Typ	Opis
script	string	Skrypt.
timeout	string	Limitu czasu żądania HTTP dla skryptu JavaScript. Możliwe wartości:[1] 1-60s (domyślnie: 30s).
process_tags	string	Czy przetwarzać zwrócone tagi. Możliwe wartości:[1] NIE (0, domyślnie), TAK (1).
show_event_menu	string	Wskaż obecność wpisu w menu zdarzeń„ jeśli makro {EVENT.TAGS.*} zostało pomyślnie przetworzone w polach `event_menu_url` i `event_menu_name`. Możliwe wartości:[1] NIE (0, domyślnie), TAK (1).
event_menu_url	string	Adres URL wpisu menu zdarzeń. Obsługuje makro {EVENT.TAGS.*}.
event_menu_name	string	Nazwa wpisu menu zdarzeń. Obsługuje makro {EVENT.TAGS.*}.
parameters		Element główny dla parametrów typu mediów webhook.
name	string	(wymagane) Nazwa parametru webhook.
value	string	Wartość parametru webhook.

Note:
Zobacz także: Obiekt typu media (odnieś się do odpowiedniej właściwości o pasującej nazwie).

Przypisy

[1] Wartości liczb całkowitych API w nawiasach, na przykład ENABLED (0), są wymienione tylko w celach informacyjnych. Aby uzyskać więcej informacji, zobacz powiązaną stronę obiektu API w tabeli lub na końcu każdej sekcji.

13 Wykrywanie

Użyj panelu bocznego, aby uzyskać dostęp do treści w sekcji Wykrywanie.

1 Wykrywanie sieci

Przegląd

Zabbix oferuje funkcję automatycznego wykrywania sieci, która jest skuteczna i bardzo elastyczna.

Przy prawidłowo skonfigurowanym wykrywaniu sieci można:

- przyspieszyć wdrożenie Zabbix
- uprościć administrację
- używać Zabbix w szybko zmieniających się środowiskach bez nadmiernych nakładów administracyjnych

Wykrywanie sieci w Zabbix opiera się na następujących informacjach:

- zakresy adresów IP
- dostępność usług zewnętrznych (FTP, SSH, WEB, POP3, IMAP, TCP itp.)
- informacje otrzymane od Zabbix agent (obsługiwany jest tylko tryb nieszyfrowany)
- informacje otrzymane od agenta SNMP

Nie zapewnia ono:

- wykrywania topologii sieci

Wykrywanie sieci zasadniczo składa się z dwóch faz: wykrywania i działań.

Wykrywanie

Zabbix okresowo skanuje zakresy IP zdefiniowane w regułach wykrywania sieci. Częstotliwość sprawdzania można skonfigurować indywidualnie dla każdej reguły.

Każda reguła ma zdefiniowany zestaw kontroli usług do wykonania dla zakresu IP.

Reguły wykrywania są przetwarzane przez menedżera wykrywania. Menedżer wykrywania tworzy zadanie dla każdej reguły z listą zadań cząstkowych (kontroli sieciowych). Kontrole sieciowe są wykonywane równolegle przez dostępne procesy robocze wykrywania (ich liczba jest konfigurowalna w frontendzie dla każdej reguły). Tylko kontrole z tym samym adresem IP i portem są planowane sekwencyjnie, ponieważ niektóre urządzenia nie akceptują równoległych połączeń na tym samym porcie.

Rozmiar kolejki kontroli sieciowych jest ograniczony do 2000000 lub około 4 GB pamięci. Jeśli kolejka się zapełni, reguła wykrywania zostanie pominięta, a w logu zostanie zapisany komunikat ostrzegawczy. Możesz użyć wewnętrznej pozycji `zabbix[discovery_queue]`, aby monitorować liczbę kontroli wykrywania w kolejce.

Kontrole wykrywania są przetwarzane niezależnie od innych kontroli. Jeśli jakiekolwiek kontrole nie znajdą usługi (lub zakończą się niepowodzeniem), pozostałe kontrole nadal będą przetwarzane.

> **Note:**
> Jeśli reguła wykrywania zostanie zmieniona podczas wykonywania, bieżące wykonanie wykrywania zostanie przerwane.

Każda kontrola usługi i hosta (IP) wykonywana przez moduł wykrywania sieci generuje zdarzenie wykrywania.

Zdarzenie	Wynik kontroli usługi
Usługa wykryta	Usługa jest „up” po tym, jak była „down”, lub gdy została wykryta po raz pierwszy.
Usługa up	Usługa jest „up” po tym, jak była już „up”.
Usługa utracona	Usługa jest „down” po tym, jak była „up”.
Usługa down	Usługa jest „down” po tym, jak była już „down”.
Host wykryty	Co najmniej jedna usługa hosta jest „up” po tym, jak wszystkie usługi tego hosta były „down”, lub została wykryta usługa należąca do niezarejestrowanego hosta.
Host up	Co najmniej jedna usługa hosta jest „up” po tym, jak co najmniej jedna usługa była już „up”.
Host utracony	Wszystkie usługi hosta są „down” po tym, jak co najmniej jedna była „up”.
Host down	Wszystkie usługi hosta są „down” po tym, jak były już „down”.

Akcje

Zdarzenia wykrywania mogą stanowić podstawę odpowiednich akcji, takich jak:

- Wysyłanie powiadomień
- Dodawanie/usuwanie hostów
- Włączanie/wyłączanie hostów

- Dodawanie hostów do grupy
- Usuwanie hostów z grupy
- Dodawanie tagów do hosta
- Usuwanie tagów z hosta
- Podłączanie szablonu do hostów/odłączanie szablonu od hostów
- Wykonywanie zdalnych skryptów

Akcje te można skonfigurować z uwzględnieniem typu urządzenia, adresu IP, statusu, czasu działania/przestoju itd. Pełne informacje na temat konfigurowania akcji dla zdarzeń opartych na wykrywaniu sieci można znaleźć na stronach operacji i warunków akcji.

Ponieważ akcje wykrywania sieci są oparte na zdarzeniach, będą uruchamiane zarówno wtedy, gdy wykryty host jest online, jak i wtedy, gdy jest offline. Zdecydowanie zaleca się dodanie warunku akcji *Discovery status: up*, aby uniknąć uruchamiania takich akcji jak *Add host* przy zdarzeniach *Service Lost*/*Service Down*. W przeciwnym razie, jeśli wykryty host zostanie usunięty ręcznie, nadal będzie generował zdarzenia *Service Lost*/*Service Down* i zostanie odtworzony podczas następnego cyklu wykrywania.

Note:
Podłączanie szablonów do wykrytego hosta zakończy się zbiorczym niepowodzeniem, jeśli którykolwiek z szablonów możliwych do podłączenia zawiera unikalną encję (np. klucz pozycji), która jest taka sama jak unikalna encja (np. klucz pozycji) już istniejąca na hoście lub w innym z szablonów możliwych do podłączenia.

Tworzenie hosta

Host jest dodawany, jeśli wybrano operację *Add host*. Host jest również dodawany, nawet jeśli brakuje operacji *Add host*, jeśli wybierzesz operacje skutkujące działaniami na hoście. Takimi operacjami są:

- włącz host
- wyłącz host
- dodaj host do grupy hostów
- podłącz szablon do hosta

Utworzone hosty są dodawane do grupy *Discovered hosts* (domyślnie, z możliwością konfiguracji w *Administration* > *General* > *Other*). Jeśli chcesz, aby hosty były dodawane do innej grupy, dodaj operację *Remove from host groups* (określając „Discovered hosts”) oraz operację *Add to host groups* (określając inną grupę hostów), ponieważ host musi należeć do grupy hostów.

Adres IP wykrytego urządzenia, wraz ze źródłem wykrywania (serwer Zabbix, proxy Zabbix lub grupa proxy) oraz typem interfejsu, jest używany jako kryterium wyszukiwania hosta w systemie. Jeśli host z tym samym adresem IP, typem interfejsu i źródłem wykrywania już istnieje, ten host będzie celem wykonywania operacji. Jeśli źródło wykrywania jest inne, wykryty obiekt jest traktowany jako inny host i może zostać utworzony nowy host.

Jeśli adres IP wykrytego hosta zostanie zmieniony lub interfejs zostanie usunięty, przy następnym wykryciu zostanie utworzony nowy host.

Nadawanie nazw hostom

Podczas dodawania hostów nazwa hosta jest wynikiem odwrotnego wyszukiwania DNS lub adresem IP, jeśli odwrotne wyszukiwanie się nie powiedzie. Wyszukiwanie jest wykonywane z serwera Zabbix lub proxy Zabbix, w zależności od tego, który z nich wykonuje wykrywanie. Jeśli wyszukiwanie nie powiedzie się na proxy, nie jest ponawiane na serwerze. Jeśli host o takiej nazwie już istnieje, do nazwy kolejnego hosta zostanie dodane **_2**, następnie **_3** itd.

Możliwe jest również zastąpienie wyszukiwania DNS/IP i użycie zamiast tego wartości pozycji jako nazwy hosta, na przykład:

- Można wykryć wiele serwerów z uruchomionym agent Zabbix przy użyciu pozycji agenta Zabbix do wykrywania i automatycznie przypisać im odpowiednie nazwy na podstawie wartości tekstowej zwróconej przez tę pozycję
- Można wykryć wiele urządzeń sieciowych SNMP przy użyciu pozycji agenta SNMP do wykrywania i automatycznie przypisać im odpowiednie nazwy na podstawie wartości tekstowej zwróconej przez tę pozycję

Jeśli nazwa hosta została ustawiona przy użyciu wartości pozycji, nie jest aktualizowana podczas kolejnych kontroli wykrywania. Jeśli nie można ustawić nazwy hosta przy użyciu wartości pozycji, używana jest wartość domyślna (nazwa DNS).

Jeśli host z wykrytym adresem IP już istnieje, a źródło wykrywania (serwer Zabbix, proxy lub grupa proxy) nie uległo zmianie, nowy host nie jest tworzony. Jeśli źródło wykrywania jest inne, wykryta jednostka jest traktowana jako odrębna i może zostać utworzony nowy host. Jednak jeśli akcja wykrywania zawiera operacje (podłączenie szablonu, dodanie do grupy hostów itp.), są one wykonywane na istniejącym hoście dopasowanym według adresu IP, typu interfejsu i źródła wykrywania.

Usuwanie hostów

Hosty wykryte przez regułę wykrywania sieci są usuwane automatycznie z *Monitoring* > *Discovery*, jeśli wykryta jednostka nie znajduje się już w zakresie adresów IP tej reguły. Hosty są usuwane natychmiast.

Tworzenie interfejsów podczas dodawania hostów

Gdy hosty są dodawane w wyniku wykrywania sieci, ich interfejsy są tworzone zgodnie z następującymi zasadami:

- Wykryte usługi — na przykład, jeśli sprawdzenie SNMP zakończyło się powodzeniem, zostanie utworzony interfejs SNMP.
- Jeśli host odpowiedział zarówno na żądania agenta Zabbix, jak i SNMP, zostaną utworzone oba typy interfejsów.
- Jeśli kryteriami unikalności są dane zwrócone przez agenta Zabbix lub SNMP, pierwszy interfejs znaleziony dla hosta zostanie utworzony jako domyślny. Pozostałe adresy IP zostaną dodane jako dodatkowe interfejsy. Warunki akcji (takie jak IP hosta) nie mają wpływu na dodawanie interfejsów. *Należy pamiętać*, że będzie to działać, jeśli wszystkie interfejsy zostaną wykryte przez tę samą regułę wykrywania. Jeśli inna reguła wykrywania wykryje inny interfejs tego samego hosta, zostanie dodany dodatkowy host.
- Jeśli host odpowiadał tylko na sprawdzenia agenta, zostanie utworzony tylko z interfejsem agenta. Jeśli później zacznie odpowiadać na SNMP, zostaną dodane dodatkowe interfejsy SNMP.
- Jeśli początkowo zostały utworzone 3 oddzielne hosty, wykryte na podstawie kryteriów unikalności „IP", a następnie reguła wykrywania zostanie zmodyfikowana tak, że hosty A, B i C będą miały identyczny wynik kryteriów unikalności, hosty B i C zostaną utworzone jako dodatkowe interfejsy dla A, pierwszego hosta. Poszczególne hosty B i C pozostaną. W *Monitoring > Discovery* dodane interfejsy będą wyświetlane w kolumnie „Discovered device", czarną czcionką i z wcięciem, ale kolumna „Monitored host" będzie wyświetlać tylko A, pierwszego utworzonego hosta. „Uptime/Downtime" nie jest mierzone dla adresów IP, które są traktowane jako dodatkowe interfejsy.

Zmiana ustawienia proxy

Hosty wykryte przez różne proxy nie zawsze są traktowane jako różne hosty. Wykrywanie i sprawdzanie unikalności zależą od struktury grup proxy: gdy proxy uruchamia regułę wykrywania i tworzy host, ten host jest dodawany do nadrzędnej grupy proxy danego proxy, a nie przypisywany do samego proxy. Gdy Zabbix podczas wykrywania sprawdza unikalność adresu IP, sprawdza hosty monitorowane przez nadrzędną grupę proxy. Hosty monitorowane przez poszczególne proxy w tej grupie (w tym proxy, które uruchomiło wykrywanie) są pomijane podczas sprawdzania unikalności, co może skutkować zduplikowanymi hostami, jeśli wiele proxy monitoruje nakładające się podsieci.

Chociaż takie zachowanie pozwala na działanie wykrywania w nakładających się zakresach adresów IP używanych przez różne podsieci, zmiana proxy przypisanego do już monitorowanej podsieci jest bardziej skomplikowana, ponieważ zmiany proxy muszą zostać spójnie zastosowane do wykrytych hostów oraz do członkostwa w nadrzędnej grupie proxy, aby uniknąć duplikatów.

Na przykład kroki wymagane do zastąpienia proxy w regule wykrywania:

1. wyłącz regułę wykrywania
2. zsynchronizuj konfigurację proxy
3. zastąp proxy w regule wykrywania
4. zastąp proxy dla wszystkich hostów wykrytych przez tę regułę (upewnij się, że hosty w nadrzędnej grupie proxy oraz wszelkie hosty monitorowane przez poszczególne proxy w tej grupie zostały zaktualizowane, aby uniknąć duplikatów)
5. włącz regułę wykrywania

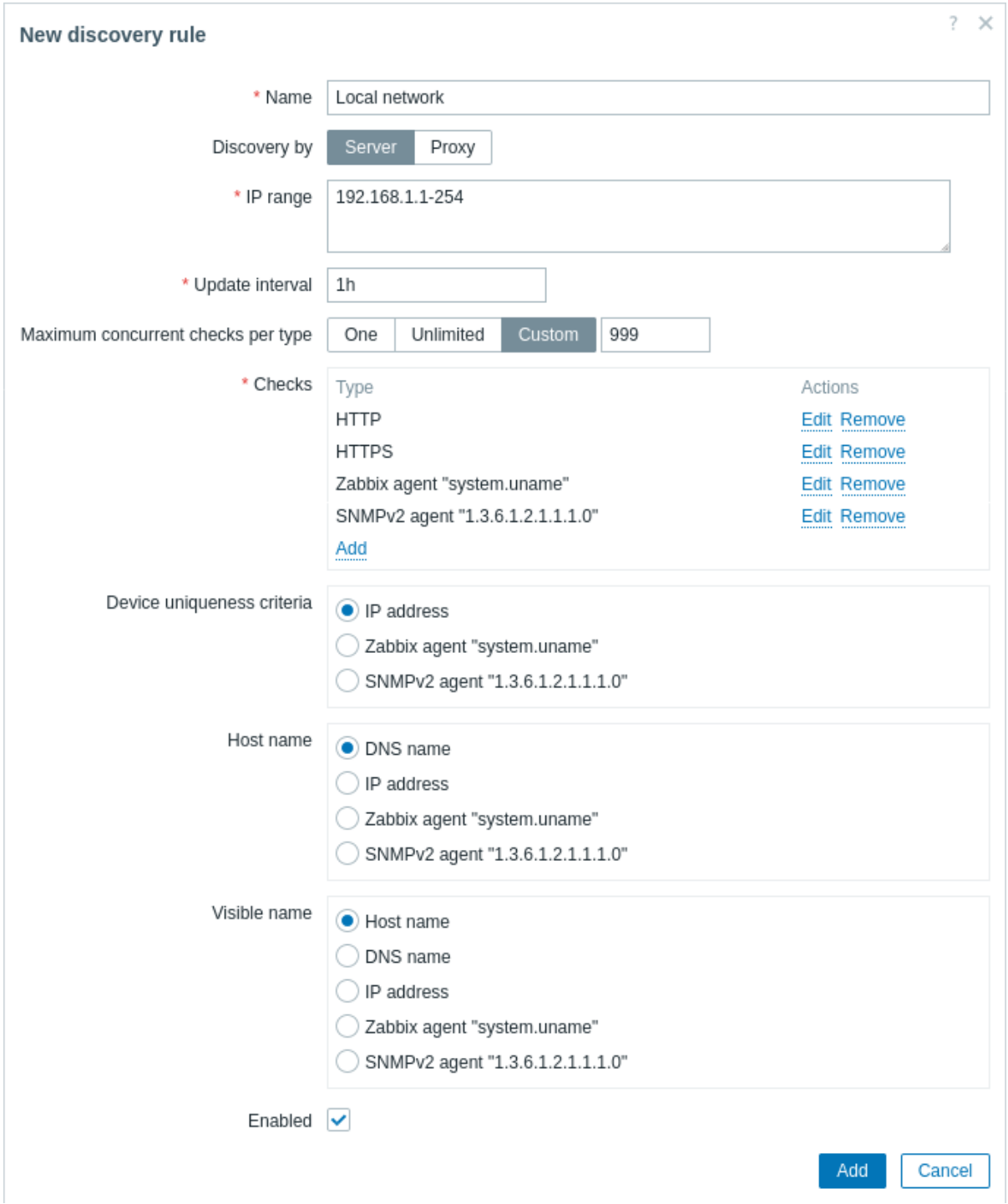
1 Konfigurowanie reguły wykrywania sieci

Przegląd

Aby skonfigurować regułę wykrywania sieci używaną przez Zabbix do wykrywania hostów i usług:

- Przejdź do *Data collection → Discovery*
- Kliknij *Create discovery rule* (lub nazwę reguły, aby edytować istniejącą)
- Edytuj atrybuty reguły wykrywania

Atrybuty reguły



Wszystkie obowiązkowe pola wejściowe są oznaczone czerwoną gwiazdką.

Parametr	Opis
Name	Unikalna nazwa reguły. Na przykład „Local network”.
Discovery by	Wykrywanie jest wykonywane przez: **Server** - przez serwer Zabbix **Proxy** - przez proxy Zabbix (wybrane w polu nazwy proxy)
IP range	Zakres adresów IP do wykrywania. Może mieć następujące formaty: Pojedynczy adres IP: 192.168.1.33 Zakres adresów IP: 192.168.1-10.1-255. Zakres jest ograniczony całkowitą liczbą objętych adresów (mniej niż 64K). Maska IP: 192.168.4.0/24 obsługiwane maski IP: /16 - /30 dla adresów IPv4 /112 - /128 dla adresów IPv6 Lista: 192.168.1.1-255, 192.168.2.1-100, 192.168.2.200, 192.168.4.0/24 To pole obsługuje spacje, tabulatory i wiele wierszy.

Parametr	Opis
Update interval	Ten parametr określa, jak często Zabbix będzie wykonywać regułę. Interwał jest liczony po zakończeniu wykonywania poprzedniego wystąpienia wykrywania, więc nie dochodzi do nakładania się. Obsługiwane są sufiksy czasu, np. 30s, 1m, 2h, 1d. Obsługiwane są makra użytkownika. *Uwaga*: jeśli używane jest makro użytkownika i jego wartość zostanie zmieniona (np. 1w → 1h), następne sprawdzenie zostanie wykonane zgodnie z poprzednią wartością (w podanym przykładzie — znacznie później).
Maximum concurrent checks per type	Ustaw maksymalną liczbę wątków wykrywania (workerów) na sprawdzenie usługi do równoległego przetwarzania sprawdzeń wykrywania: **One** - jeden wątek **Unlimited** - nieograniczona liczba wątków (ale nie większa niż w parametrze StartDiscoverers) **Custom** - ustaw własną liczbę wątków (0-999) Zwróć uwagę, że wszystkie reguły wykrywania ze sprawdzeniami usług asynchronicznych SNMPv3 są przetwarzane przez jeden worker ze względu na specyfikę implementacji libsnmp, tj. zwiększenie liczby workerów nie zwiększy szybkości wykrywania.
Checks	Zabbix użyje tej listy sprawdzeń do wykrywania. Kliknij Add, aby skonfigurować nowe sprawdzenie w wyskakującym oknie. Obsługiwane sprawdzenia: SSH, LDAP, SMTP, FTP, HTTP, HTTPS, POP, NNTP, IMAP, TCP, Telnet, agent Zabbix, agent SNMPv1, agent SNMPv2, agent SNMPv3, ICMP ping. Wykrywanie oparte na protokole używa funkcjonalności **net.tcp.service[]** do testowania każdego hosta, z wyjątkiem SNMP, które odpytuje OID SNMP. agent Zabbix jest testowany przez odpytywanie pozycji w trybie nieszyfrowanym. Więcej szczegółów znajduje się w sekcji pozycje agenta. Parametr „Ports” może mieć jedną z następujących postaci: Pojedynczy port: 22 Zakres portów: 22-45 Lista: 22-45,55,60-70 Od Zabbix 7.0 wszystkie sprawdzenia usług są wykonywane asynchronicznie, z wyjątkiem sprawdzeń LDAP. Od Zabbix 7.0 sprawdzanie HTTP/HTTPs odbywa się przez libcurl. Jeśli serwer/proxy Zabbix został skompilowany bez libcurl, sprawdzenia HTTP będą działać jak w poprzednich wersjach (tj. jako sprawdzenia TCP), ale sprawdzenia HTTPS nie będą działać.
Device uniqueness criteria	Kryteria unikalności mogą być następujące: **IP address** - nie przetwarzaj wielu urządzeń z pojedynczym adresem IP. Jeśli urządzenie z tym samym adresem IP już istnieje, zostanie uznane za już wykryte i nowy host nie zostanie dodany. **<discovery check>** - sprawdzenie agenta Zabbix lub agenta SNMP. Zwróć uwagę, że kryteria unikalności używane podczas wykrywania nie są tym samym co identyfikacja hosta w systemie podczas wykonywania akcji. Kryteria unikalności podczas wykrywania określają, czy dwa lub więcej wykrytych urządzeń to to samo urządzenie (lub różne urządzenia), podczas gdy jedynym kryterium identyfikacji hosta w Zabbix jest adres IP (zobacz Tworzenie hosta).
Host name	Ustaw techniczną nazwę hosta tworzonego hosta, używając: **DNS name** - nazwa DNS (domyślnie) **IP address** - adres IP **<discovery check>** - odebrana wartość tekstowa sprawdzenia wykrywania (np. agent Zabbix, sprawdzenie agenta SNMP) Zobacz także: Nazewnictwo hostów.
Visible name	Ustaw widoczną nazwę tworzonego hosta, używając: **Host name** - techniczna nazwa hosta (domyślnie) **DNS name** - nazwa DNS **IP address** - adres IP **<discovery check>** - odebrana wartość tekstowa sprawdzenia wykrywania (np. agent Zabbix, sprawdzenie agenta SNMP) Zobacz także: Nazewnictwo hostów.
Enabled	Po zaznaczeniu pola wyboru reguła jest aktywna i będzie wykonywana przez serwer Zabbix. Jeśli pole nie jest zaznaczone, reguła nie jest aktywna. Nie będzie wykonywana.

Przekroczenie limitu deskryptorów plików

W przypadku dużej liczby równoczesnych kontroli możliwe jest wyczerpanie limitu deskryptorów plików dla discovery manager.

Liczba deskryptorów plików wymaganych do wykrywania jest równa liczbie discovery workers * 1000. Domyślnie istnieje 5 discovery workers, podczas gdy miękki limit systemu wynosi około 1024.

Jeśli ten limit zostanie osiągnięty, Zabbix zmniejszy domyślną liczbę równoczesnych kontroli na typ dla każdego workera i zapisze ostrzeżenie do pliku dziennika. Jeśli jednak użytkownik ustawił wyższą wartość dla *Maximum concurrent checks per type* niż wartość obliczona przez Zabbix, Zabbix użyje wartości zdefiniowanej przez użytkownika dla jednego workera.

Przykład z życia

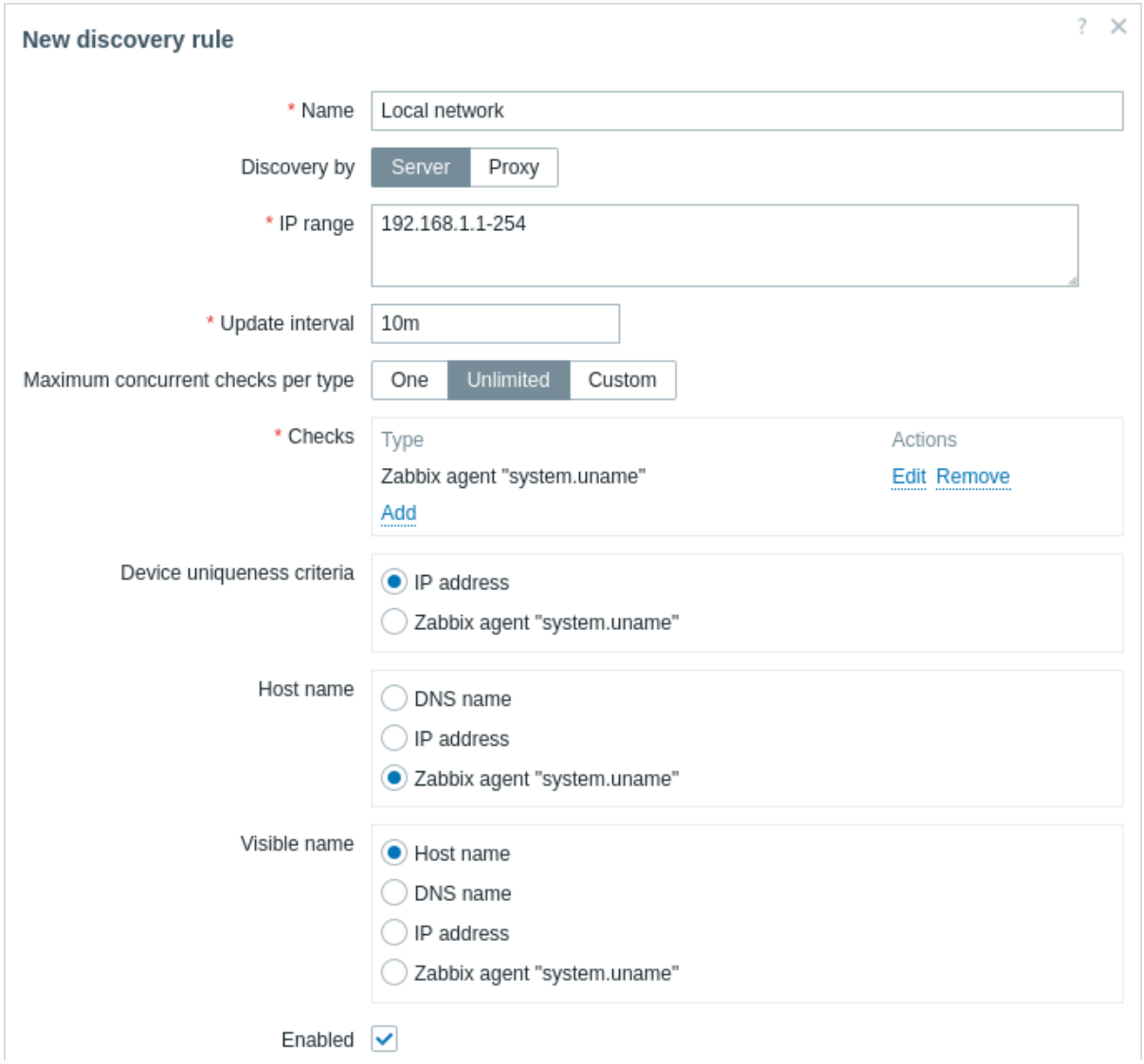
W tym przykładzie chcemy skonfigurować wykrywanie sieci dla sieci lokalnej o zakresie adresów IP 192.168.1.1-192.168.1.254.

W naszym scenariuszu chcemy:

- wykrywać te hosty, na których działa agent Zabbix
- uruchamiać wykrywanie co 10 minut
- dodać host do monitorowania, jeśli czas działania hosta wynosi więcej niż 1 godzinę
- usuwać hosty, jeśli czas niedostępności hosta przekracza 24 godziny
- dodawać hosty z systemem Linux do grupy ”Linux servers”
- dodawać hosty z systemem Windows do grupy ”Windows servers”
- używać szablonu *Linux* dla hostów z systemem Linux
- używać szablonu *Windows* dla hostów z systemem Windows

Krok 1

Definiowanie reguły wykrywania sieci dla naszego zakresu adresów IP.



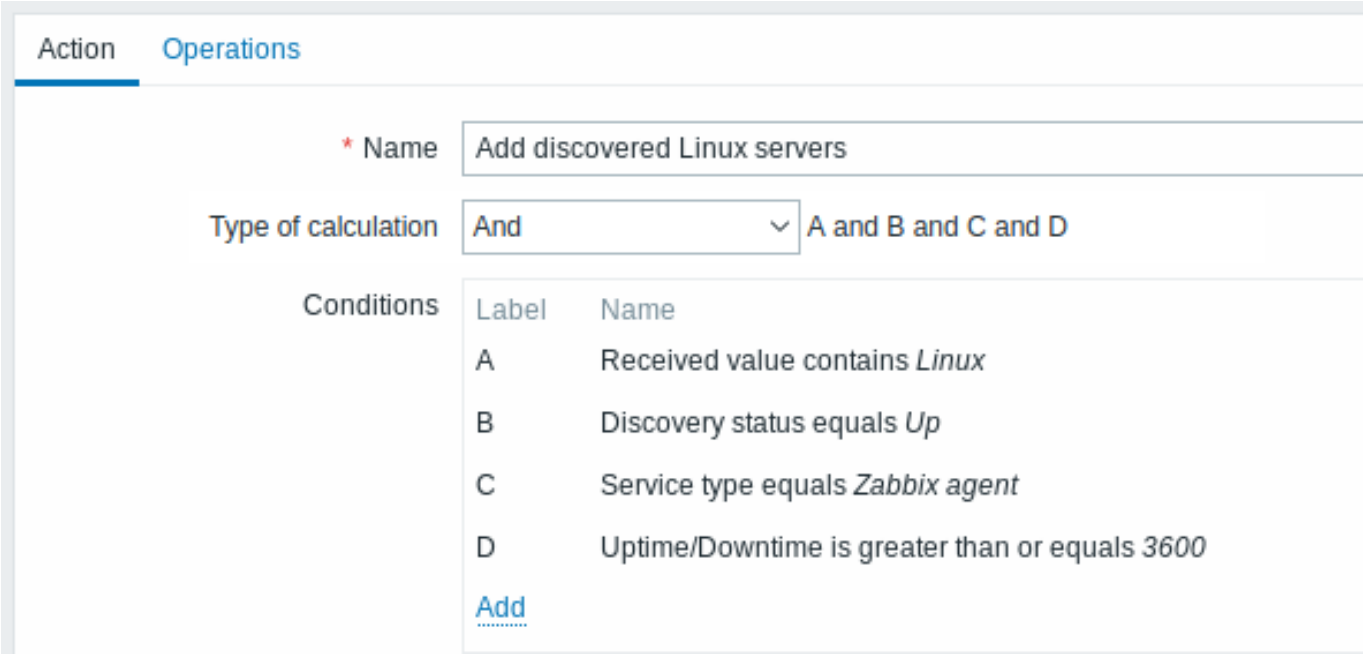
Zabbix spróbuje wykryć hosty w zakresie adresów IP 192.168.1.1-192.168.1.254, łącząc się z agentami Zabbix i pobierając wartość z klucza **system.uname**. Wartość otrzymana od agent może zostać użyta do nadania nazw hostom, a także do zastosowania różnych akcji dla różnych systemów operacyjnych. Na przykład powiązać serwery Windows z szablonem *Windows*, a serwery Linux z szablonem *Linux*.

Reguła będzie wykonywana co 10 minut.

Po dodaniu tej reguły Zabbix automatycznie rozpocznie wykrywanie i generowanie zdarzeń opartych na wykrywaniu do dalszego przetwarzania.

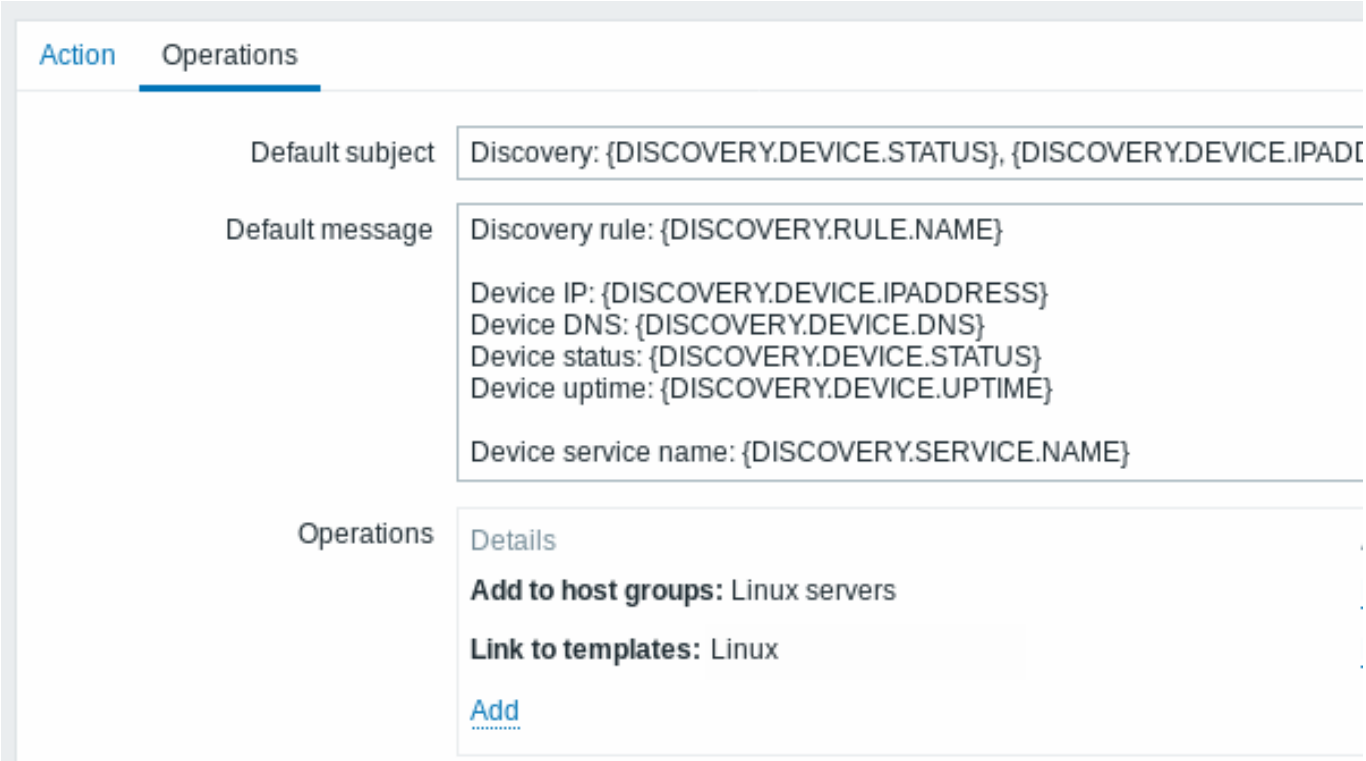
Krok 2

Definiowanie akcji wykrywania do dodawania wykrytych serwerów Linux do odpowiedniej grupy/szablonu.



Akcja zostanie uruchomiona, jeśli:

- usługa „Zabbix agent” ma stan „up”
- wartość system.uname (klucz Zabbix agent użyty przez nas w definicji reguły) zawiera „Linux”
- czas działania wynosi 1 godzinę (3600 sekund) lub więcej

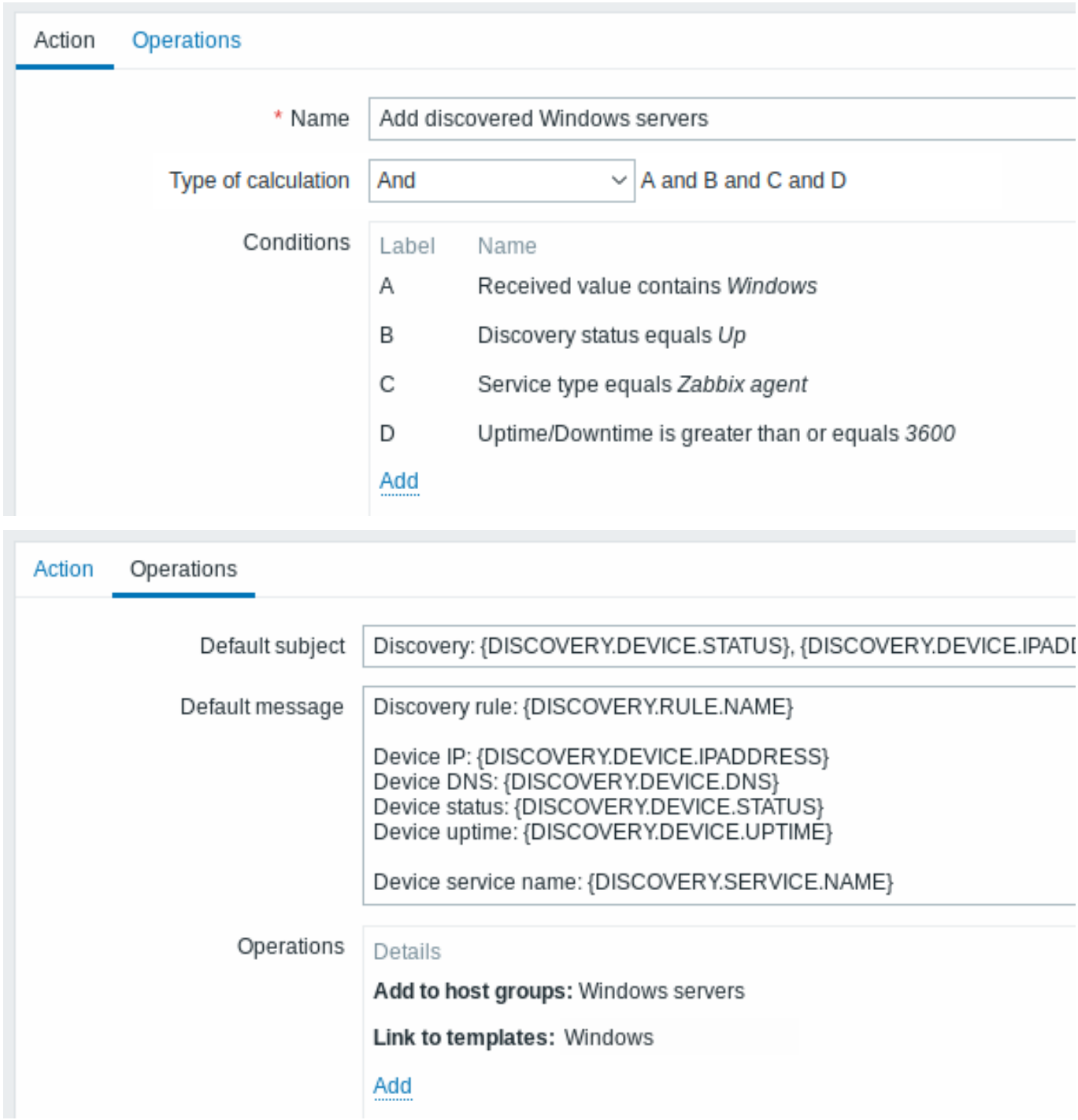


Akcja wykona następujące operacje:

- doda wykryty host do grupy „Linux servers” (a także doda host, jeśli nie został dodany wcześniej)
- podłączy host do szablonu *Linux*. Zabbix automatycznie rozpocznie monitorowanie hosta przy użyciu pozycji i wyzwalaczy z szablonu „Linux”.

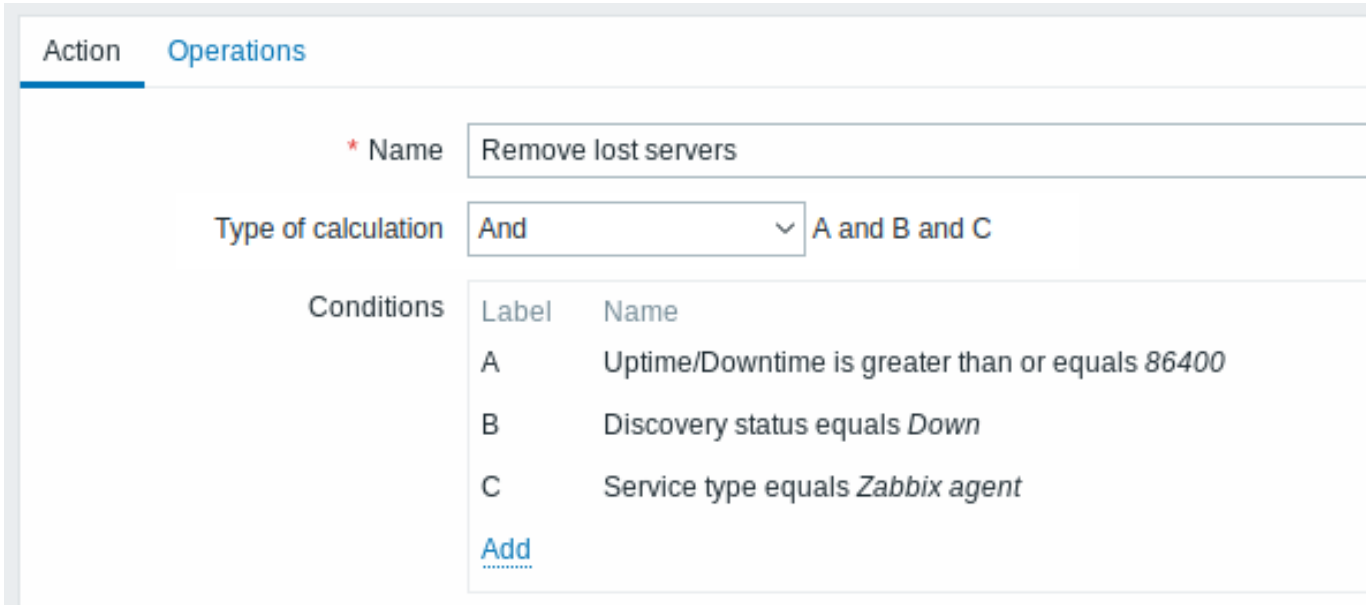
Krok 3

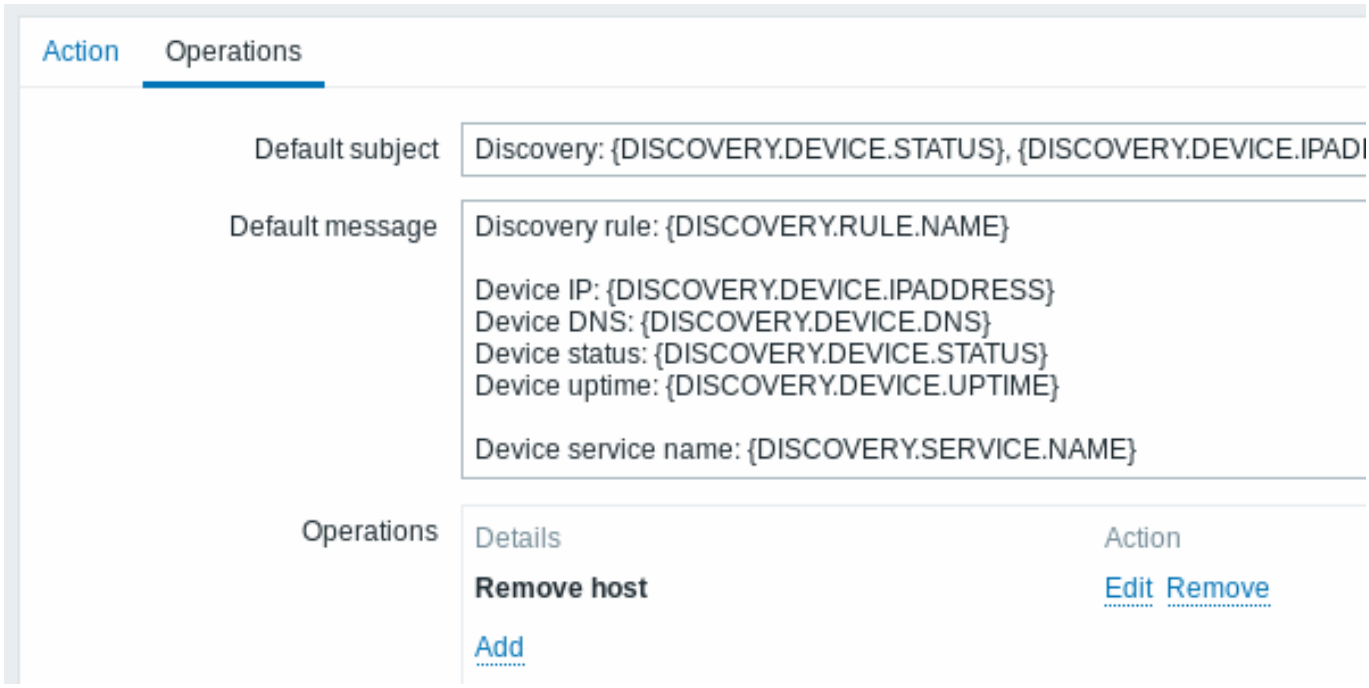
Definiowanie akcji wykrywania służącej do dodawania wykrytych serwerów Windows do odpowiedniej grupy/szablonu.



Krok 4

Definiowanie akcji wykrywania do usuwania utraconych serwerów.





Serwer zostanie usunięty, jeśli usługa „Zabbix agent” będzie w stanie „down” przez ponad 24 godziny (86400 sekund).

2 Autorejestracja agenta aktywnego

Przegląd

Możliwe jest włączenie automatycznej rejestracji aktywnego Zabbix agent, po czym serwer może rozpocząć ich monitorowanie. W ten sposób nowe hosty mogą być dodawane do monitorowania bez ręcznej konfiguracji na serwerze.

Automatyczna rejestracja może nastąpić, gdy wcześniej nieznany aktywny agent poprosi o testy.

Funkcja ta może być bardzo przydatna do automatycznego monitorowania nowych węzłów Cloud. Gdy tylko w Cloud pojawi się nowy węzeł, Zabbix automatycznie rozpocznie zbieranie danych o wydajności i dostępności hosta.

Automatyczna rejestracja aktywnego agent obsługuje również monitorowanie dodanych hostów za pomocą testów pasywnych. Gdy aktywny agent prosi o testy, pod warunkiem że ma zdefiniowane w pliku konfiguracyjnym parametry konfiguracyjne `ListenIP` lub `ListenPort`, są one również przesyłane do serwera. Jeśli określono wiele adresów IP, do serwera wysyłany jest pierwszy z nich.

Serwer, dodając nowy automatycznie zarejestrowany host, używa otrzymanego adresu IP i portu do skonfigurowania agent. Jeśli nie zostanie odebrana wartość adresu IP, używany jest adres wykorzystany dla połączenia przychodzącego. Jeśli nie zostanie odebrana wartość portu, używany jest port 10050.

Można określić, że host powinien zostać automatycznie zarejestrowany z nazwą DNS jako domyślnym interfejsem agent.

Automatyczna rejestracja jest uruchamiana ponownie:

- jeśli zmienią się informacje o metadanych hosta:
  - z powodu zmiany HostMetadata i ponownego uruchomienia agent
  - z powodu zmiany wartości zwracanej przez HostMetadataItem
- dla hostów utworzonych ręcznie, jeśli brakuje metadanych
- jeśli host zostanie ręcznie zmieniony tak, aby był monitorowany przez inny Zabbix proxy
- jeśli automatyczna rejestracja dla tego samego hosta pochodzi z nowego Zabbix proxy

Interwał heartbeat automatycznej rejestracji aktywnego agent dla Zabbix server i Zabbix proxy wynosi 120 sekund. Dlatego w przypadku usunięcia wykrytego hosta automatyczna rejestracja zostanie uruchomiona ponownie po 120 sekundach.

Konfiguracja

Określ serwer

Upewnij się, że serwer Zabbix jest wskazany w pliku konfiguracyjnym agenta - `zabbix_agentd.conf`:

```
ServerActive=10.0.0.1
```

Jeśli nie zdefiniujesz jawnie parametru *Hostname* w `zabbix_agentd.conf`, serwer użyje nazwy systemowej hosta z lokalizacji agenta do nazwania hosta. Nazwę systemową hosta w systemie Linux można uzyskać, uruchamiając polecenie `hostname`.

Jeśli parametr *Hostname* jest zdefiniowany w konfiguracji agenta Zabbix jako lista hostów rozdzielona przecinkami, hosty zostaną utworzone dla wszystkich wymienionych nazw hostów.

Po wprowadzeniu jakichkolwiek zmian w pliku konfiguracyjnym uruchom ponownie agenta.

Akcja dla aktywnej autorejestracji agent

Gdy serwer otrzyma żądanie autorejestracji od agent, wywołuje akcję. Dla autorejestracji agent musi być skonfigurowana akcja ze źródłem zdarzeń „Autorejestracja".

> **Note:**
> Konfigurowanie wykrywania sieci nie jest wymagane, aby aktywne agenty mogły się autorejestrować.

W frontend Zabbix przejdź do *Alerty → Akcje*, wybierz *Akcje autorejestracji* i kliknij *Utwórz akcję*:

- Na karcie Akcja nadaj swojej akcji nazwę
- Opcjonalnie określ warunki. Możesz użyć dopasowania podciągu lub wyrażenia regularnego w warunkach dla nazwy hosta/metadanych hosta. Jeśli zamierzasz użyć warunku „Metadane hosta", zobacz następną sekcję.
- Na karcie Operacje dodaj odpowiednie operacje, takie jak: „Dodaj host", „Dodaj do grupy hostów" (na przykład *Discovered hosts*), „Podłącz szablony" itd.

> **Note:**
> Jeśli hosty, które będą się autorejestrować, prawdopodobnie będą obsługiwane wyłącznie przez aktywne monitorowanie (na przykład hosty odgrodzone zaporą od serwera Zabbix), możesz utworzyć specjalny szablon, taki jak *Template_Linux-active*, do podłączenia.

Utworzone hosty są dodawane do grupy *Discovered hosts* (domyślnie; można to skonfigurować w *Administracja > Ogólne > Inne*). Jeśli chcesz, aby hosty były dodawane do innej grupy, dodaj operację *Usuń z grupy hostów* (wskazując „Discovered hosts"), a także operację *Dodaj do grupy hostów* (wskazując inną grupę hostów), ponieważ host musi należeć do grupy hostów.

Bezpieczna autorejestracja

Bezpieczny sposób autorejestracji jest możliwy dzięki skonfigurowaniu uwierzytelniania opartego na PSK z szyfrowanymi połączeniami.

Poziom szyfrowania jest konfigurowany globalnie w *Administracja > Ogólne > Autorejestracja*. Można wybrać brak szyfrowania, szyfrowanie TLS z uwierzytelnianiem PSK lub obie opcje jednocześnie (tak aby niektóre hosty mogły rejestrować się bez szyfrowania, a inne z użyciem szyfrowania).

Uwierzytelnianie za pomocą PSK jest weryfikowane przez serwer Zabbix przed dodaniem hosta. Jeśli zakończy się powodzeniem, host zostanie dodany, a ustawienie *Połączenia z/do hosta* zostanie ustawione wyłącznie na „PSK", z tożsamością/kluczem współdzielonym takim samym jak w globalnym ustawieniu autorejestracji.

Attention:
Aby zapewnić bezpieczeństwo autorejestracji w instalacjach korzystających z proxy, należy włączyć szyfrowanie między serwerem Zabbix a proxy.

Używanie DNS jako domyślnego interfejsu

Parametry konfiguracyjne HostInterface i HostInterfaceItem configuration parameters umożliwiają określenie niestandardowej wartości interfejsu hosta podczas autorejestracji.

Dokładniej mówiąc, są one przydatne, jeśli host ma zostać automatycznie zarejestrowany z nazwą DNS jako domyślnym interfejsem agent zamiast jego adresu IP. W takim przypadku nazwa DNS powinna zostać określona lub zwrócona jako wartość parametru HostInterface albo HostInterfaceItem. Jeśli wartość jednego z tych parametrów zmieni się — na przykład z adresu IP na nazwę DNS lub odwrotnie — domyślny interfejs automatycznie zarejestrowanego hosta zostanie odpowiednio zaktualizowany. Ta aktualizacja jest stosowana do istniejącego hosta, a nie przez utworzenie nowego. Aby wysłać nową wartość, agent musi zostać uruchomiony ponownie, tak aby ponownie zainicjował proces autorejestracji.

Note:
Jeśli parametry HostInterface lub HostInterfaceItem nie są skonfigurowane, zamiast nich używany jest parametr listen_dns. Ta wartość jest określana przez wykonanie odwrotnego wyszukiwania DNS dla adresu IP agenta. Jeśli odwrotne DNS nie jest poprawnie skonfigurowane lub zwraca nieprawidłową nazwę, może to skutkować nieprawidłową lub nieudaną autorejestracją z powodu nieprawidłowej wartości interfejsu.

Używanie metadanych hosta

Gdy agent wysyła do serwera żądanie autorejestracji, przesyła swoją nazwę hosta. W niektórych przypadkach (na przykład węzły chmury Amazon) nazwa hosta nie wystarcza, aby serwer Zabbix mógł rozróżnić wykryte hosty. Metadane hosta mogą być opcjonalnie używane do przesyłania innych informacji z agenta do serwera.

Metadane hosta konfiguruje się w pliku konfiguracyjnym agenta - `zabbix_agentd.conf`. Istnieją 2 sposoby określenia metadanych hosta w pliku konfiguracyjnym:

```
HostMetadata
HostMetadataItem
```

Opis tych opcji znajduje się pod powyższym linkiem.

Parametr HostMetadataItem może zwrócić maksymalnie 65535 punktów kodowych UTF-8. Dłuższa wartość zostanie obcięta.

Należy pamiętać, że w MySQL efektywna maksymalna długość w znakach będzie mniejsza, jeśli zwracana wartość zawiera znaki wielobajtowe. Na przykład wartość zawierająca wyłącznie znaki 3-bajtowe będzie ograniczona łącznie do 21844 znaków, natomiast wartość zawierająca wyłącznie znaki 4-bajtowe będzie ograniczona do 16383 znaków.

Attention:
Próba autorejestracji następuje za każdym razem, gdy aktywny agent wysyła do serwera żądanie odświeżenia aktywnych kontroli. Opóźnienie między żądaniami jest określone w parametrze RefreshActiveChecks agenta. Pierwsze żądanie jest wysyłane natychmiast po ponownym uruchomieniu agenta.

Przykłady

Autorejestracja według systemu operacyjnego przy użyciu HostMetadata

Załóżmy, że chcesz, aby hosty były automatycznie rejestrowane przez serwer Zabbix. W swojej sieci masz aktywne agenty Zabbix (zobacz sekcję „Configuration" powyżej). W sieci znajdują się hosty z systemem Windows i Linux, a w frontendzie Zabbix masz dostępne szablony „Linux by Zabbix agent" i „Windows by Zabbix agent". Dlatego podczas rejestracji hosta chcesz, aby do rejestrowanego hosta został zastosowany odpowiedni szablon Linux/Windows. Domyślnie podczas autorejestracji do serwera wysyłana jest tylko nazwa hosta, co może nie być wystarczające. Aby mieć pewność, że do hosta zostanie zastosowany właściwy szablon, należy użyć metadanych hosta.

Konfiguracja frontendu

Pierwszą rzeczą, którą należy zrobić, jest skonfigurowanie frontendu. Utwórz 2 akcje. Pierwsza akcja:

- Nazwa: Automatyczna rejestracja hosta Linux
- Warunki: Metadane hosta zawierają *Linux*
- Operacje: Podłącz szablony: Linux by Zabbix agent

Note:
W tym przypadku można pominąć operację „Dodaj host”. Podłączenie szablonu do hosta wymaga najpierw dodania hosta, więc serwer zrobi to automatycznie.

Druga akcja:

- Nazwa: Automatyczna rejestracja hosta Windows
- Warunki: Metadane hosta zawierają *Windows*
- Operacje: Podłącz szablony: Windows by Zabbix agent

Konfiguracja agenta

Teraz należy skonfigurować agenty. Dodaj następujący wiersz do plików konfiguracyjnych agenta:

```
HostMetadataItem=system.uname
```

W ten sposób masz pewność, że metadane hosta będą zawierać „Linux” lub „Windows” w zależności od hosta, na którym uruchomiony jest agent. Przykład metadanych hosta w tym przypadku:

```
Linux: Linux server3 3.2.0-4-686-pae #1 SMP Debian 3.2.41-2 i686 GNU/Linux
Windows: Windows WIN-0PXGGSTYNHO 6.0.6001 Windows Server 2008 Service Pack 1 Intel IA-32
```

Nie zapomnij zrestartować agenta po wprowadzeniu jakichkolwiek zmian w pliku konfiguracyjnym.

Używanie HostMetadata do kontrolowania autorejestracji i szablonów

Krok 1 — Chroń rejestrację za pomocą HostMetadata

Użycie metadanych hosta pozwala zapewnić podstawową ochronę przed rejestracją niepożądanych hostów.

Konfiguracja frontendu

Utwórz akcję we frontendzie, używając trudnego do odgadnięcia tajnego kodu, aby nie dopuścić niepożądanych hostów:

- Nazwa: Akcja autorejestracji Linux
- Warunki:
  - Typ obliczeń: AND
  - Warunek (A): Metadane hosta zawierają //Linux//
  - Warunek (B): Metadane hosta zawierają //21df83bf21bf0be663090bb8d4128558ab9b95fba66a6dbf834f8b91ae5e08ae//
- Operacje:
  - Wyślij wiadomość do użytkowników: Admin przez wszystkie media
  - Dodaj do grup hostów: Serwery Linux
  - Podłącz szablony: Linux by Zabbix agent

Należy pamiętać, że sama ta metoda nie zapewnia silnej ochrony, ponieważ dane są przesyłane otwartym tekstem. Aby zmiany zaczęły obowiązywać natychmiast, wymagane jest przeładowanie pamięci podręcznej konfiguracji.

Konfiguracja agenta

Dodaj następujący wiersz do pliku konfiguracyjnego agenta:

```
HostMetadata=Linux    21df83bf21bf0be663090bb8d4128558ab9b95fba66a6dbf834f8b91ae5e08ae
```

gdzie „Linux” to platforma, a pozostała część ciągu to trudny do odgadnięcia tajny tekst.

Nie zapomnij zrestartować agenta po wprowadzeniu jakichkolwiek zmian w pliku konfiguracyjnym.

Krok 2 — Dodaj szablon do zarejestrowanego hosta

Możliwe jest dodanie dodatkowych szablonów do już zarejestrowanego hosta. W takim przypadku szablon MySQL by Zabbix agent zostanie podłączony tylko do hostów, których HostMetadata zawiera token `MySQL`.

Konfiguracja frontend

Zaktualizuj akcję we frontend:

- Nazwa: Akcja autorejestracji Linux
- Warunki:
  - Typ obliczania: AND
  - Warunek (A): Metadane host zawierają Linux
  - Warunek (B): Metadane host zawierają 21df83bf21bf0be663090bb8d4128558ab9b95fba66a6dbf834f8b91ae5e08ae
  - Warunek (C): Metadane host zawierają MySQL
- Operacje:
  - Wyślij wiadomość do użytkowników: Admin przez wszystkie media

- Dodaj do grup hostów: Serwery Linux
- Podłącz szablony: Linux by Zabbix agent
- Podłącz szablony: MySQL by Zabbix Agent

Konfiguracja agenta

Zaktualizuj następną linię w pliku konfiguracyjnym agenta:

```
HostMetadata=MySQL on Linux 21df83bf21bf0be663090bb8d4128558ab9b95fba66a6dbf834f8b91ae5e08ae
```

Nie zapomnij zrestartować agenta po wprowadzeniu jakichkolwiek zmian w pliku konfiguracyjnym.

3 Odkrywanie niskiego poziomu

Przegląd Low-level discovery (LLD) zapewnia sposób automatycznego tworzenia pozycji, wyzwalaczy i wykresów dla różnych encji na hoście. Na przykład Zabbix może automatycznie rozpocząć monitorowanie systemów plików lub interfejsów sieciowych na Twojej maszynie, bez konieczności ręcznego tworzenia pozycji dla każdego systemu plików lub interfejsu sieciowego. LLD może również tworzyć hosty, na przykład w celu uzupełnienia listy maszyn wirtualnych wykrytych na hiperwizorze, a także zagnieżdżone reguły wykrywania, umożliwiające wielopoziomowe wykrywanie. Dodatkowo możliwe jest skonfigurowanie Zabbix tak, aby automatycznie usuwał niepotrzebne encje na podstawie rzeczywistych wyników okresowo wykonywanego wykrywania.

Użytkownik może zdefiniować własne typy wykrywania, pod warunkiem że są zgodne z określonym protokołem JSON.

Ogólna architektura procesu wykrywania wygląda następująco.

Najpierw użytkownik tworzy regułę wykrywania w *Data collection* > *Templates*, w kolumnie *Discovery*. Reguła wykrywania składa się z (1) pozycji, która wykrywa wymagane encje (na przykład systemy plików lub interfejsy sieciowe), oraz (2) prototypów pozycji, wyzwalaczy i wykresów, które mają zostać utworzone na podstawie wartości tej pozycji.

Pozycja wykrywająca wymagane encje jest podobna do zwykłej pozycji spotykanej w innych miejscach: serwer żąda od agenta Zabbix (lub innego komponentu, zależnie od ustawionego typu pozycji) wartości tej pozycji, a agent odpowiada wartością tekstową. Różnica polega na tym, że wartość zwracana przez agenta powinna zawierać listę wykrytych encji w formacie JSON. Chociaż szczegóły tego formatu są istotne tylko dla implementatorów niestandardowych kontroli wykrywania, warto wiedzieć, że zwracana wartość zawiera listę par makro → wartość. Na przykład pozycja ”net.if.discovery” może zwrócić dwie pary: ”{#IFNAME}” → ”lo” oraz ”{#IFNAME}” → ”eth0”.

Te makra są używane w nazwach, kluczach i innych polach prototypów, gdzie są następnie zastępowane otrzymanymi wartościami w celu utworzenia rzeczywistych pozycji, wyzwalaczy, wykresów, a nawet hostów dla każdej wykrytej encji. Zobacz pełną listę opcji użycia makr LLD.

Gdy serwer otrzyma wartość dla pozycji wykrywania, analizuje pary makro → wartość i dla każdej pary generuje rzeczywiste pozycje, wyzwalacze i wykresy na podstawie ich prototypów. W powyższym przykładzie z ”net.if.discovery” serwer wygenerowałby jeden zestaw pozycji, wyzwalaczy i wykresów dla interfejsu pętli zwrotnej ”lo” oraz drugi zestaw dla interfejsu ”eth0”.

Należy pamiętać, że od **Zabbix 4.2** zmienił się format JSON zwracanego przez reguły low-level discovery. Nie oczekuje się już, że JSON będzie zawierał obiekt ”data”. Low-level discovery akceptuje teraz zwykły JSON zawierający tablicę, aby obsługiwać nowe funkcje, takie jak preprocessing wartości pozycji oraz niestandardowe ścieżki do wartości makr low-level discovery w dokumencie JSON.

Wbudowane klucze wykrywania zostały zaktualizowane tak, aby zwracały tablicę wierszy LLD w katalogu głównym dokumentu JSON. Zabbix automatycznie wyodrębni makro i wartość, jeśli pole tablicy używa składni {#MACRO} jako klucza. Wszelkie nowe natywne kontrole wykrywania będą używać nowej składni bez elementów ”data”. Podczas przetwarzania wartości low-level discovery najpierw lokalizowany jest katalog główny (tablica pod `$.` lub `$.data`).

Chociaż element ”data” został usunięty ze wszystkich natywnych pozycji związanych z wykrywaniem, ze względu na zgodność wsteczną Zabbix nadal będzie akceptował notację JSON z elementem ”data”, choć jej użycie nie jest zalecane. Jeśli JSON zawiera obiekt tylko z jednym elementem tablicy ”data”, zawartość tego elementu zostanie automatycznie wyodrębniona przy użyciu JSONPath `$.data`. Low-level discovery akceptuje teraz opcjonalne makra LLD zdefiniowane przez użytkownika z niestandardową ścieżką określoną w składni JSONPath.

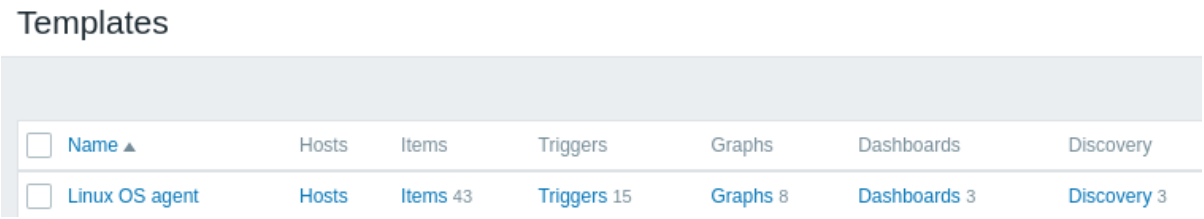
> **Warning:**
> W rezultacie powyższych zmian nowsze agenty nie będą już mogły współpracować ze starszym serwerem Zabbix.

Zobacz także: Wykryte encje

Konfigurowanie wykrywania niskiego poziomu Przedstawimy wykrywanie niskiego poziomu na przykładzie wykrywania systemów plików.

Aby skonfigurować wykrywanie, wykonaj następujące czynności:

- Przejdź do: *Zbieranie danych* > *Szablony* lub *Hosty*.
- Kliknij *Wykrywanie* w wierszu odpowiedniego szablonu/hosta.



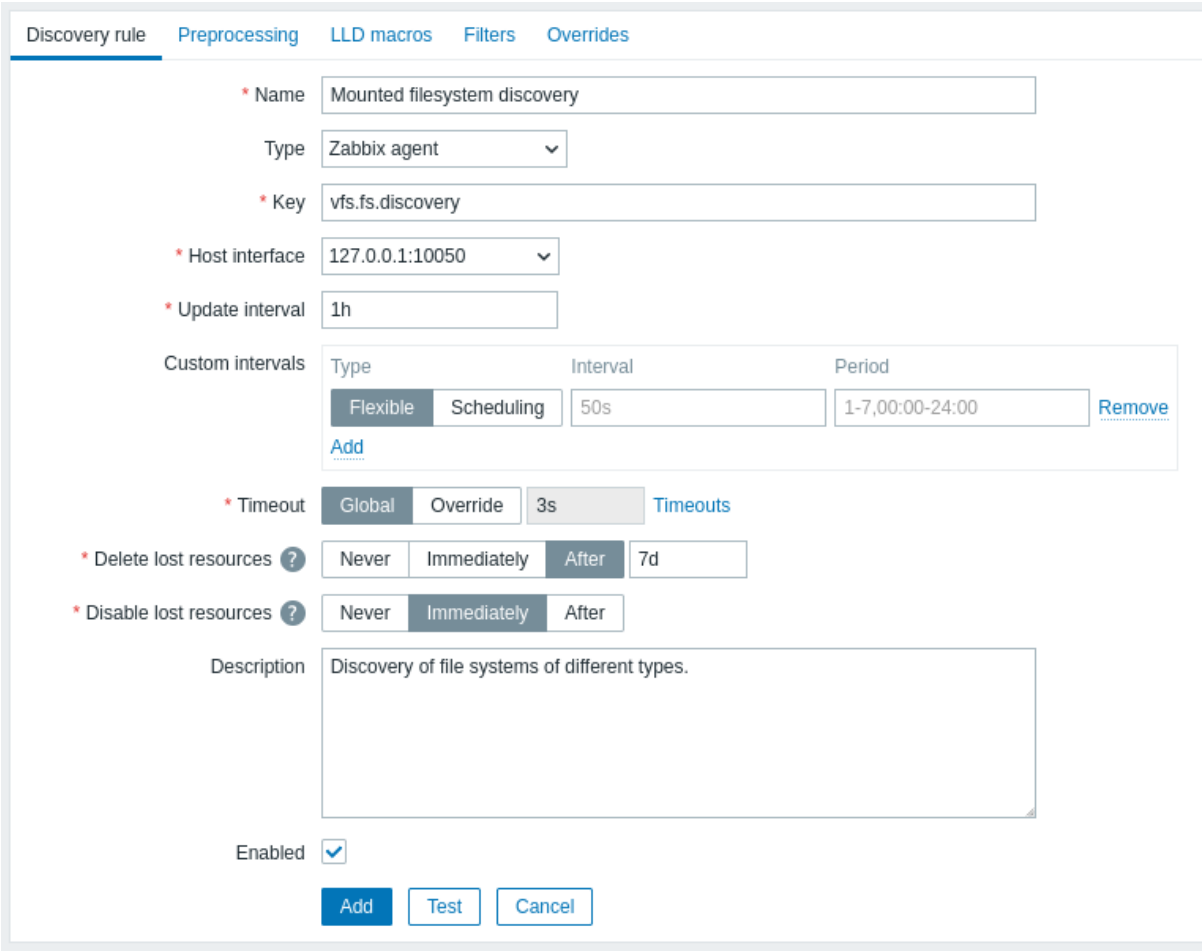
- Kliknij *Utwórz regułę wykrywania* w prawym górnym rogu ekranu.
- Uzupełnij formularz reguły wykrywania, podając wymagane informacje.

Reguła wykrywania

Formularz reguły wykrywania zawiera pięć zakładek, które od lewej do prawej przedstawiają przepływ danych podczas wykrywania:

- *Reguła wykrywania* — określa przede wszystkim wbudowaną pozycję lub niestandardowy skrypt służący do pobierania danych wykrywania.
- *Przetwarzanie wstępne* — stosuje przetwarzanie wstępne do wykrytych danych.
- *Makra LLD* — umożliwia wyodrębnienie wartości makr do użycia w wykrytych pozycjach, wyzwalaczach itd.
- *Filtry* — umożliwia filtrowanie wykrytych wartości.
- *Nadpisania* — umożliwia modyfikację pozycji, wyzwalaczy, wykresów lub prototypów hostów podczas stosowania do określonych wykrytych obiektów.

Zakładka **Reguła wykrywania** zawiera klucz pozycji używany do wykrywania (a także niektóre ogólne atrybuty reguły wykrywania):



Wszystkie wymagane pola wejściowe są oznaczone czerwoną gwiazdką.

Parameter	Description
Name	Nazwa reguły wykrywania.
Type	Typ sprawdzenia używanego do wykrywania. W tym przykładzie używamy typu pozycji *Zabbix agent*. Reguła wykrywania może być także pozycją zależną, zależną od zwykłej pozycji. Nie może zależeć od innej reguły wykrywania. W przypadku pozycji zależnej wybierz odpowiedni typ (*Dependent item*) i określ pozycję nadrzędną w polu „Master item". Pozycja nadrzędna musi istnieć.
Key	Wprowadź klucz pozycji wykrywania (do 2048 znaków). Na przykład możesz użyć wbudowanego klucza pozycji „vfs.fs.discovery", aby zwrócić ciąg JSON z listą systemów plików obecnych na komputerze, ich typami i opcjami montowania. Zwróć uwagę, że inną opcją wykrywania systemów plików jest użycie wyników wykrywania przez klucz agenta „vfs.fs.get" (zobacz przykład).
Update interval	To pole określa, jak często Zabbix wykonuje wykrywanie. Na początku, gdy dopiero konfigurujesz wykrywanie systemów plików, możesz chcieć ustawić krótki interwał, ale gdy już wiesz, że działa, możesz ustawić 30 minut lub więcej, ponieważ systemy plików zwykle nie zmieniają się zbyt często. Obsługiwane są sufiksy czasu, np. 30s, 1m, 2h, 1d. Obsługiwane są makra użytkownika. *Uwaga*: Interwał aktualizacji można ustawić na „0" tylko wtedy, gdy istnieją niestandardowe interwały z wartością różną od zera. Jeśli ustawiono „0" i istnieje niestandardowy interwał (elastyczny lub harmonogram) z wartością różną od zera, pozycja będzie odpytywana w czasie trwania niestandardowego interwału. Nowe reguły wykrywania zostaną sprawdzone w ciągu 60 sekund od ich utworzenia, chyba że mają Harmonogram lub Elastyczny interwał aktualizacji, a *Update interval* jest ustawiony na 0. *Uwaga*, że w przypadku istniejącej reguły wykrywania wykrywanie można wykonać natychmiast, naciskając przycisk *Execute now*.
Custom intervals	Możesz utworzyć niestandardowe reguły sprawdzania pozycji: **Flexible** — utwórz wyjątek od *Update interval* (interwał z inną częstotliwością) **Scheduling** — utwórz niestandardowy harmonogram odpytywania. Szczegółowe informacje można znaleźć w sekcji Custom intervals.
Timeout	Ustaw limit czasu sprawdzenia wykrywania. Wybierz opcję limitu czasu: **Global** — używany jest limit czasu proxy/globalny (wyświetlany w wyszarzonym polu *Timeout*); **Override** — używany jest niestandardowy limit czasu (ustawiany w polu *Timeout*; dozwolony zakres: 1 - 600s). Obsługiwane są sufiksy czasu, np. 30s, 1m, oraz makra użytkownika. Kliknięcie odnośnika *Timeouts* umożliwia skonfigurowanie limitów czasu proxy lub limitów globalnych (jeśli proxy nie jest używany). Zwróć uwagę, że odnośnik *Timeouts* jest widoczny tylko dla użytkowników typu *Super admin* z uprawnieniami do sekcji frontend *Administration > General* lub *Administration > Proxies*.
Delete lost resources	Określ, jak szybko wykryta jednostka zostanie usunięta, gdy jej status wykrywania zmieni się na „Not discovered anymore": *Never* — nie zostanie usunięta; *Immediately* — zostanie usunięta natychmiast; *After* — zostanie usunięta po określonym czasie. Wartość musi być większa niż wartość *Disable lost resources*. Obsługiwane są sufiksy czasu, np. 2h, 1d. Obsługiwane są makra użytkownika. *Uwaga*: Używanie opcji „Immediately" nie jest zalecane, ponieważ nawet błędna edycja filtra może spowodować usunięcie jednostki wraz ze wszystkimi danymi historycznymi. Zwróć uwagę, że zasoby wyłączone ręcznie nie zostaną usunięte przez wykrywanie niskiego poziomu.
Disable lost resources	Określ, jak szybko wykryta jednostka zostanie wyłączona, gdy jej status wykrywania zmieni się na „Not discovered anymore": *Never* — nie zostanie wyłączona; *Immediately* — zostanie wyłączona natychmiast; *After* — zostanie wyłączona po określonym czasie. Wartość powinna być większa niż interwał aktualizacji reguły wykrywania. Zwróć uwagę, że zasoby wyłączone automatycznie zostaną ponownie włączone, jeśli zostaną ponownie wykryte przez wykrywanie niskiego poziomu. Zasoby wyłączone ręcznie nie zostaną ponownie włączone po ponownym wykryciu. To pole nie jest wyświetlane, jeśli *Delete lost resources* jest ustawione na „Immediately". Obsługiwane są sufiksy czasu, np. 2h, 1d. Obsługiwane są makra użytkownika.

Parameter	Description
Description	Wprowadź opis.
Enabled	Jeśli zaznaczone, reguła będzie przetwarzana.

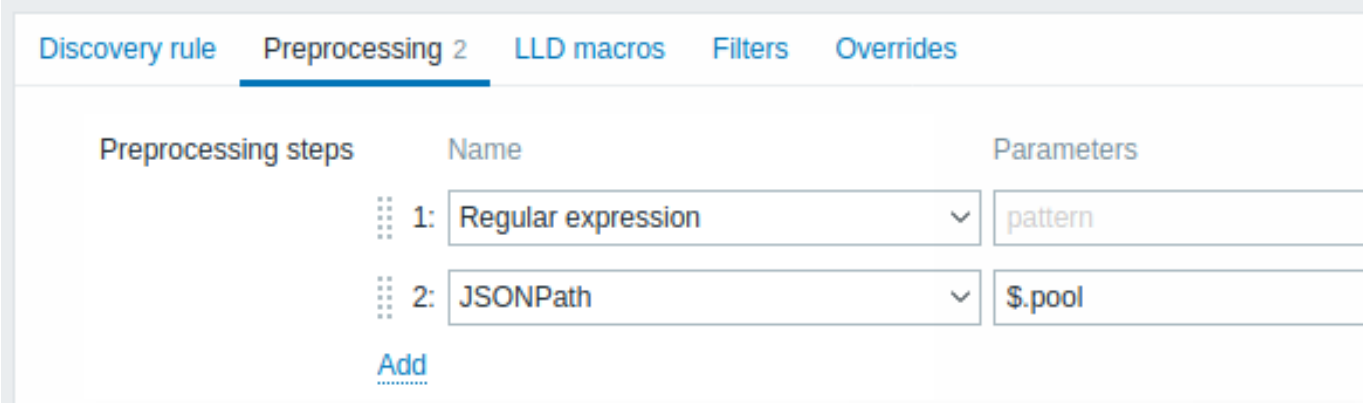
Note:
Historia reguły wykrywania nie jest zachowywana.

Wstępne przetwarzanie

Zakładka **Wstępne przetwarzanie** umożliwia zdefiniowanie reguł transformacji stosowanych do wyniku wykrywania. Na tym etapie możliwa jest jedna lub wiele transformacji. Transformacje są wykonywane w kolejności, w jakiej zostały zdefiniowane. Całe wstępne przetwarzanie jest wykonywane przez serwer Zabbix.

Zobacz także:

- Szczegóły wstępnego przetwarzania
- Testowanie wstępnego przetwarzania



Type	*Transformacja*	Opis
Text	*Wyrażenie regularne*	Dopasuj otrzymaną wartość do wyrażenia regularnego <pattern> i zastąp wartość wyodrębnionym <output>. Wyrażenie regularne obsługuje wyodrębnianie maksymalnie 10 przechwyconych grup za pomocą sekwencji \N. Parametry: **pattern** - wyrażenie regularne **output** - szablon formatowania danych wyjściowych. Sekwencja ucieczki \N (gdzie N=1...9) jest zastępowana N-tą dopasowaną grupą. Sekwencja ucieczki \0 jest zastępowana dopasowanym tekstem. Jeśli zaznaczysz pole wyboru *Custom on fail*, możliwe jest określenie niestandardowych opcji obsługi błędów: odrzucenie wartości, ustawienie określonej wartości lub ustawienie określonego komunikatu błędu.
	Zastąp	Znajdź wyszukiwany ciąg i zastąp go innym (lub niczym). Wszystkie wystąpienia wyszukiwanego ciągu zostaną zastąpione. Parametry: **search string** - ciąg do znalezienia i zastąpienia, z rozróżnianiem wielkości liter (wymagane) **replacement** - ciąg, którym zostanie zastąpiony wyszukiwany ciąg. Ciąg zastępujący może być również pusty, co w praktyce pozwala usunąć wyszukiwany ciąg po jego znalezieniu. Możliwe jest użycie sekwencji ucieczki do wyszukiwania lub zastępowania znaków nowej linii, powrotu karetki, tabulatorów i spacji: ”\n \r \t \s”; ukośnik odwrotny można zapisać jako ”\\”, a sekwencje ucieczki można zapisać jako ”\\n”. Uciekanie znaków nowej linii, powrotu karetki i tabulatorów jest wykonywane automatycznie podczas wykrywania niskiego poziomu.
Structured data	*JSONPath*	Wyodrębnij wartość lub fragment z danych JSON przy użyciu funkcjonalności JSONPath. Jeśli zaznaczysz pole wyboru *Custom on fail*, możliwe jest określenie niestandardowych opcji obsługi błędów: odrzucenie wartości, ustawienie określonej wartości lub ustawienie określonego komunikatu błędu.

Type	

XML XPath	Wyodrębnij wartość lub fragment z danych XML przy użyciu funkcjonalności XPath.
	Aby ta opcja działała, serwer Zabbix musi być skompilowany z obsługą libxml.
	Przykłady:
	`number(/document/item/value)` wyodrębni 10 z `<document><item><value>10</value></item></document>`
	`number(/document/item/@attribute)` wyodrębni 10 z `<document><item attribute="10"></item></document>`
	`/document/item` wyodrębni `<item><value>10</value></item>` z `<document><item><value>10</value></item></document>`
	Pamiętaj, że przestrzenie nazw nie są obsługiwane.
	Jeśli zaznaczysz pole wyboru *Custom on fail*, możliwe jest określenie niestandardowych opcji obsługi błędów: odrzucenie wartości, ustawienie określonej wartości lub ustawienie określonego komunikatu błędu.

CSV do JSON	Konwertuj dane pliku CSV do formatu JSON. Więcej informacji znajdziesz tutaj: Wstępne przetwarzanie CSV do JSON.
XML do JSON	Konwertuj dane w formacie XML do JSON. Więcej informacji znajdziesz tutaj: Reguły serializacji. Jeśli zaznaczysz pole wyboru *Custom on fail*, możliwe jest określenie niestandardowych opcji obsługi błędów: odrzucenie wartości, ustawienie określonej wartości lub ustawienie określonego komunikatu błędu.
SNMP	
Wartość SNMP walk	Wyodrębnij wartość według określonej nazwy OID/MIB i zastosuj opcje formatowania: **Unchanged** - zwróć Hex-STRING jako nieuciekany ciąg szesnastkowy (*uwaga*: wskazówki wyświetlania są nadal stosowane); **UTF-8 from Hex-STRING** - konwertuj Hex-STRING do ciągu UTF-8; **MAC from Hex-STRING** - konwertuj Hex-STRING do ciągu adresu MAC (w którym `' '` zostanie zastąpione przez `':'`); **Integer from BITS** - konwertuj pierwsze 8 bajtów ciągu bitowego wyrażonego jako sekwencja znaków szesnastkowych (np. ”1A 2B 3C 4D”) na 64-bitową liczbę całkowitą bez znaku. W ciągach bitowych dłuższych niż 8 bajtów kolejne bajty zostaną zignorowane. Jeśli zaznaczysz pole wyboru *Custom on fail*, możliwe jest określenie niestandardowych opcji obsługi błędów: odrzucenie wartości, ustawienie określonej wartości lub ustawienie określonego komunikatu błędu.
SNMP walk do JSON	Konwertuj wartości SNMP do JSON. Określ nazwę pola w JSON oraz odpowiadającą jej ścieżkę SNMP OID. Wartości pól zostaną wypełnione wartościami z określonej ścieżki SNMP OID. Możesz użyć tego kroku wstępnego przetwarzania do wykrywania SNMP OID. Dostępne są podobne opcje formatowania wartości jak w kroku *Wartość SNMP walk*. Jeśli zaznaczysz pole wyboru *Custom on fail*, możliwe jest określenie niestandardowych opcji obsługi błędów: odrzucenie wartości, ustawienie określonej wartości lub ustawienie określonego komunikatu błędu.
Wartość SNMP get	Zastosuj opcje formatowania do wartości pobranej przez SNMP get: **UTF-8 from Hex-STRING** - konwertuj Hex-STRING do ciągu UTF-8; **MAC from Hex-STRING** - konwertuj Hex-STRING do ciągu adresu MAC (w którym `' '` zostanie zastąpione przez `':'`); **Integer from BITS** - konwertuj pierwsze 8 bajtów ciągu bitowego wyrażonego jako sekwencja znaków szesnastkowych (np. ”1A 2B 3C 4D”) na 64-bitową liczbę całkowitą bez znaku. W ciągach bitowych dłuższych niż 8 bajtów kolejne bajty zostaną zignorowane. Jeśli zaznaczysz pole wyboru *Custom on fail*, możliwe jest określenie niestandardowych opcji obsługi błędów: odrzucenie wartości, ustawienie określonej wartości lub ustawienie określonego komunikatu błędu.
Custom scripts	
JavaScript	Wprowadź kod JavaScript w modalnym edytorze, który otwiera się po kliknięciu w polu parametru lub ikonie ołówka obok niego. Pamiętaj, że dostępna długość kodu JavaScript zależy od używanej bazy danych. Więcej informacji znajdziesz tutaj: Wstępne przetwarzanie JavaScript
Validation	
Nie pasuje do wyrażenia regularnego	Określ wyrażenie regularne, do którego wartość nie może pasować. Np. `Error:(.*?)\.` Jeśli zaznaczysz pole wyboru *Custom on fail*, możliwe jest określenie niestandardowych opcji obsługi błędów: odrzucenie wartości, ustawienie określonej wartości lub ustawienie określonego komunikatu błędu.

Type	
Sprawdź błąd w JSON	Sprawdź komunikat błędu na poziomie aplikacji znajdujący się pod JSONPath. Zatrzymaj przetwarzanie, jeśli operacja się powiedzie i komunikat nie jest pusty; w przeciwnym razie kontynuuj przetwarzanie z wartością sprzed tego kroku wstępnego przetwarzania. Pamiętaj, że te błędy usług zewnętrznych są zgłaszane użytkownikowi w niezmienionej postaci, bez dodawania informacji o kroku wstępnego przetwarzania. Np. `$.errors`. Jeśli zostanie odebrany JSON taki jak `{"errors":"e1"}`, następny krok wstępnego przetwarzania nie zostanie wykonany. Jeśli zaznaczysz pole wyboru *Custom on fail*, możliwe jest określenie niestandardowych opcji obsługi błędów: odrzucenie wartości, ustawienie określonej wartości lub ustawienie określonego komunikatu błędu.
Sprawdź błąd w XML	Sprawdź komunikat błędu na poziomie aplikacji znajdujący się pod XPath. Zatrzymaj przetwarzanie, jeśli operacja się powiedzie i komunikat nie jest pusty; w przeciwnym razie kontynuuj przetwarzanie z wartością sprzed tego kroku wstępnego przetwarzania. Pamiętaj, że te błędy usług zewnętrznych są zgłaszane użytkownikowi w niezmienionej postaci, bez dodawania informacji o kroku wstępnego przetwarzania. W przypadku niepowodzenia parsowania nieprawidłowego XML nie zostanie zgłoszony żaden błąd. Jeśli zaznaczysz pole wyboru *Custom on fail*, możliwe jest określenie niestandardowych opcji obsługi błędów: odrzucenie wartości, ustawienie określonej wartości lub ustawienie określonego komunikatu błędu.
Pasuje do wyrażenia regularnego	Określ wyrażenie regularne, do którego wartość musi pasować. Jeśli zaznaczysz pole wyboru *Custom on fail*, możliwe jest określenie niestandardowych opcji obsługi błędów: odrzucenie wartości, ustawienie określonej wartości lub ustawienie określonego komunikatu błędu.
Throttling	
Odrzuć niezmienione z heartbeat	Odrzuć wartość, jeśli nie zmieniła się w zdefiniowanym okresie czasu (w sekundach). Obsługiwane są dodatnie wartości całkowite określające sekundy (minimum - 1 sekunda). W tym polu można używać sufiksów czasu (np. 30s, 1m, 2h, 1d). W tym polu można używać makr użytkownika i makr wykrywania niskiego poziomu. Dla discovery item można określić tylko jedną opcję ograniczania częstotliwości. Np. `1m`. Jeśli identyczny tekst zostanie przekazany do tej reguły dwa razy w ciągu 60 sekund, zostanie odrzucony. *Uwaga*: Zmiana prototypów pozycji nie resetuje ograniczania częstotliwości. Ograniczanie częstotliwości jest resetowane tylko wtedy, gdy zmienią się kroki wstępnego przetwarzania.
Prometheus	
Prometheus do JSON	Konwertuj wymagane metryki Prometheus do JSON. Szczegóły znajdziesz w sekcji Kontrole Prometheus.

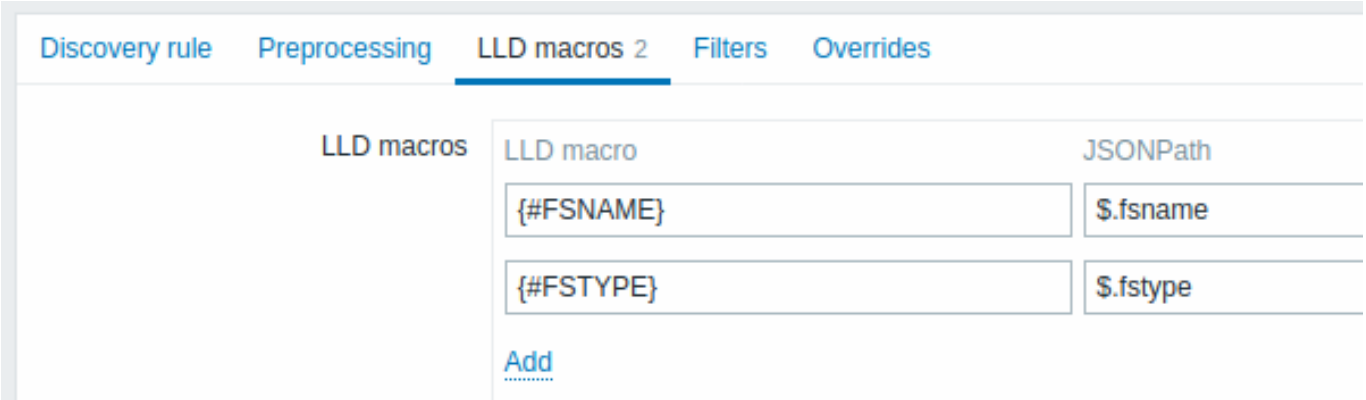
Pamiętaj, że jeśli reguła wykrywania została zastosowana do hosta przez szablon, zawartość tej zakładki jest tylko do odczytu.

Makra niestandardowe

Zakładka **Makra LLD** umożliwia określenie niestandardowych makr wykrywania niskiego poziomu.

Makra niestandardowe są przydatne w przypadkach, gdy zwrócony JSON nie ma już zdefiniowanych wymaganych makr. Na przykład:

- Natywny klucz `vfs.fs.discovery` do wykrywania systemów plików zwraca JSON z pewnymi wstępnie zdefiniowanymi makrami LLD, takimi jak {#FSNAME}, {#FSTYPE}. Te makra mogą być używane bezpośrednio w prototypach pozycji i wyzwalaczy (zobacz kolejne sekcje strony); definiowanie makr niestandardowych nie jest potrzebne;
- Pozycja agenta `vfs.fs.get` również zwraca JSON z danymi systemu plików, ale bez żadnych wstępnie zdefiniowanych makr LLD. W takim przypadku możesz samodzielnie zdefiniować makra i odwzorować je na wartości w JSON za pomocą JSONPath:

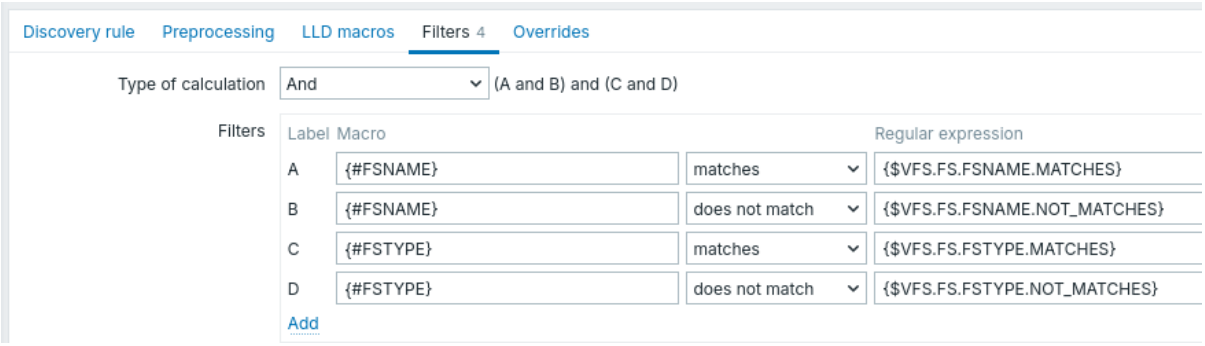


Wyodrębnione wartości mogą być używane w wykrytych pozycjach, wyzwalaczach itd. Pamiętaj, że wartości będą wyodrębniane z wyniku wykrywania oraz wszystkich dotychczasowych kroków przetwarzania wstępnego.

Parameter	Description
Makro LLD *JSONPath*	Nazwa makra wykrywania niskiego poziomu, z użyciem następującej składni: {#MACRO}. Ścieżka używana do wyodrębnienia wartości makra LLD z wiersza LLD, z użyciem składni JSONPath. Wartości wyodrębnione ze zwróconego JSON są używane do zastępowania makr LLD w polach prototypów pozycji, wyzwalaczy itd. JSONPath można określić przy użyciu notacji kropkowej lub notacji nawiasowej. Notacja nawiasowa powinna być używana w przypadku znaków specjalnych i Unicode, na przykład `$['unicode + special chars #1']['unicode + special chars #2']`. Na przykład `$.foo` wyodrębni „bar” i „baz” z tego JSON: `[{"foo":"bar"}, {"foo":"baz"}]` Zwróć uwagę, że `$.foo` wyodrębni „bar” i „baz” również z tego JSON: `{"data":[{"foo":"bar"}, {"foo":"baz"}]}` ponieważ pojedynczy obiekt „data” jest przetwarzany automatycznie (dla zgodności wstecznej z implementacją wykrywania niskiego poziomu w wersjach Zabbix wcześniejszych niż 4.2).

Filtr

Filtr może być użyty do generowania rzeczywistych pozycji, wyzwalaczy i wykresów tylko dla encji spełniających kryteria. Karta **Filtry** zawiera definicje filtrów reguły wykrywania, umożliwiające filtrowanie wartości wykrywania:



Parametr	Opis
Typ obliczania	Dostępne są następujące opcje obliczania filtrów: **And** - wszystkie filtry muszą zostać spełnione; **Or** - wystarczy, jeśli jeden filtr zostanie spełniony; **And/Or** - używa *And* dla różnych nazw makr i *Or* dla tej samej nazwy makra; **Custom expression** - oferuje możliwość zdefiniowania własnego sposobu obliczania filtrów. Formuła musi zawierać wszystkie filtry z listy. Ograniczenie do 255 znaków.

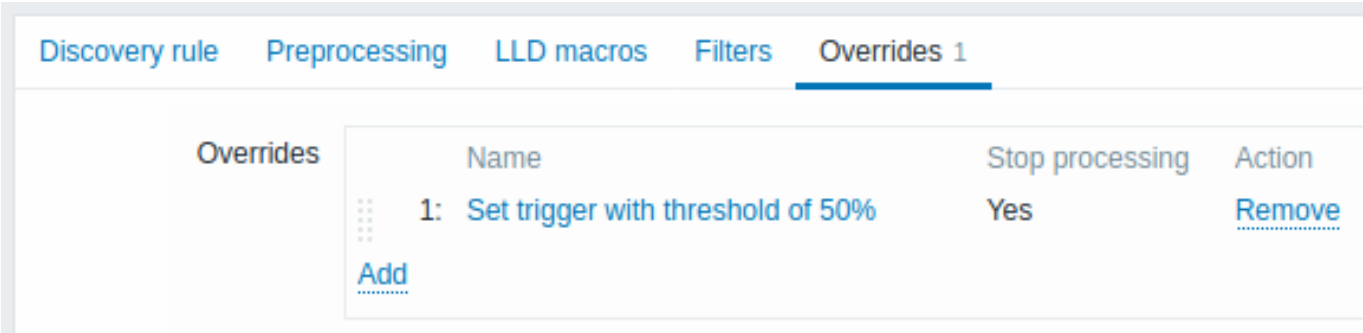
Parametr	Opis
Filtry	Dostępne są następujące operatory warunków filtra: *matches*, *does not match*, *exists*, *does not exist*. Operatory *matches* i *does not match* oczekują wyrażenia regularnego zgodnego z Perl (PCRE). Na przykład, jeśli interesują Cię tylko systemy plików C:, D: i E:, możesz wpisać {#FSNAME} w polu „Macro”, a wyrażenie regularne ”^C|^D|^E” w polu tekstowym „Regular expression”. Filtrowanie jest również możliwe według typów systemów plików przy użyciu makra {#FSTYPE} (np. ”^ext|^reiserfs”) oraz według typów dysków (obsługiwane tylko przez agent Windows) przy użyciu makra {#FSDRIVETYPE} (np. ”fixed”). W polu „Regular expression” można wprowadzić wyrażenie regularne lub odwołać się do globalnego wyrażenia regularnego. Aby przetestować wyrażenie regularne, można użyć „grep -E”, na przykład: `for f in ext2 nfs reiserfs smbfs; do echo $f | grep -E '^ext|^reiserfs' || echo "SKIP: $f"; done` Operatory *exists* i *does not exist* umożliwiają filtrowanie encji na podstawie obecności lub braku określonego makra LLD w odpowiedzi. Zwróć uwagę, że jeśli makro z filtra nie występuje w odpowiedzi, znaleziona encja zostanie zignorowana, chyba że dla tego makra określono warunek „does not exist”. Wyświetlone zostanie ostrzeżenie, jeśli brak makra wpływa na wynik wyrażenia. Na przykład, jeśli brakuje {#B} w: {#A} matches 1 and {#B} matches 2 - spowoduje ostrzeżenie {#A} matches 1 or {#B} matches 2 - bez ostrzeżenia

Warning:
Błąd lub literówka w wyrażeniu regularnym użytym w regule LLD (na przykład nieprawidłowe wyrażenie regularne „File systems for discovery”) może spowodować usunięcie tysięcy elementów konfiguracji, wartości historycznych i zdarzeń dla wielu hostów.

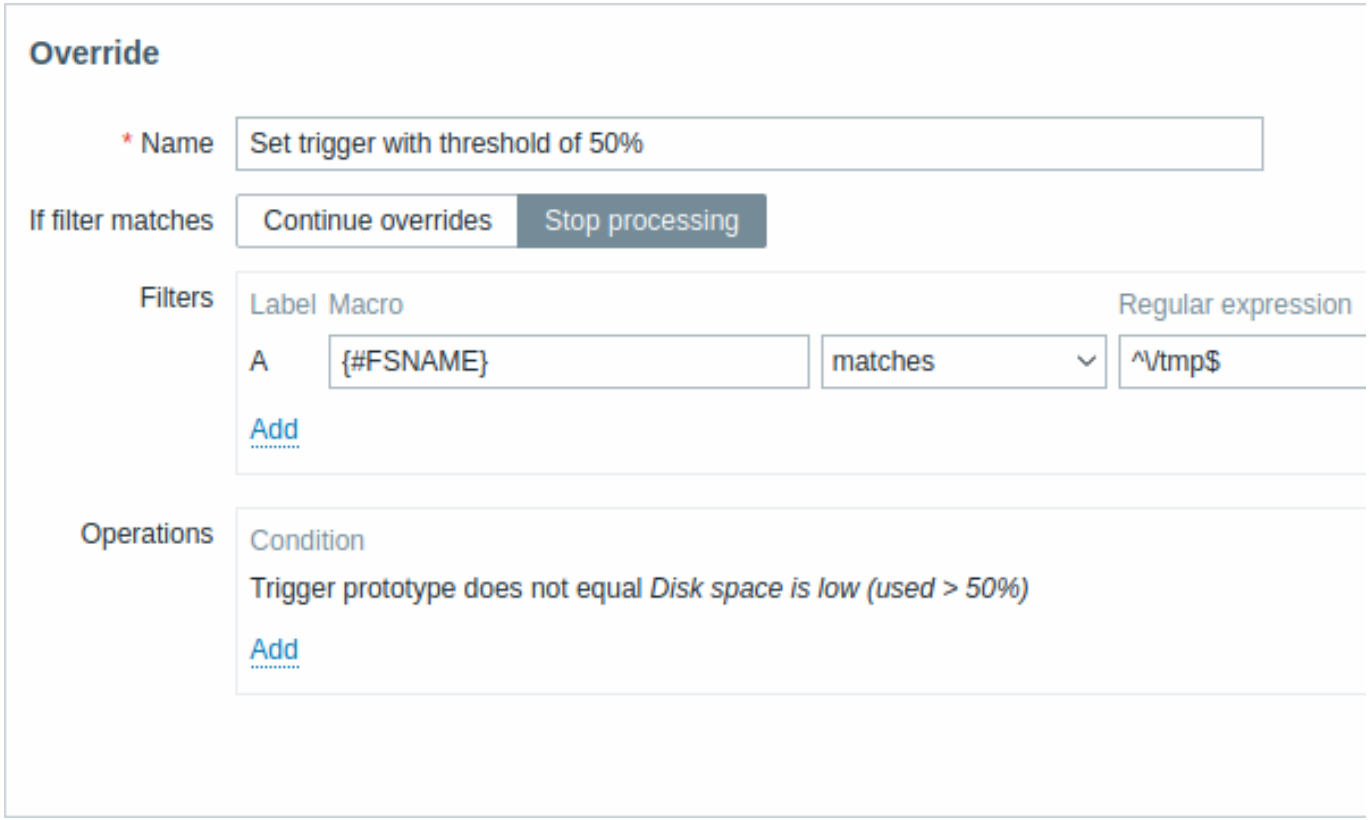
Attention:
Baza danych Zabbix w MySQL musi zostać utworzona z rozróżnianiem wielkości liter, jeśli nazwy systemów plików różniące się wyłącznie wielkością liter mają być wykrywane poprawnie.

Nadpisanie

Karta **Overrides** umożliwia ustawienie reguł modyfikujących listę prototypów pozycji, wyzwalaczy, wykresów, hostów i wykrywania lub ich atrybuty dla wykrytych obiektów spełniających podane kryteria.



Nadpisania (jeśli istnieją) są wyświetlane na liście z możliwością zmiany kolejności metodą przeciągnij i upuść i są wykonywane w kolejności, w jakiej zostały zdefiniowane. Aby skonfigurować szczegóły nowego nadpisania, kliknij Add w bloku *Overrides*. Aby edytować istniejące nadpisanie, kliknij nazwę nadpisania. Otworzy się wyskakujące okno umożliwiające edycję szczegółów reguły nadpisania.

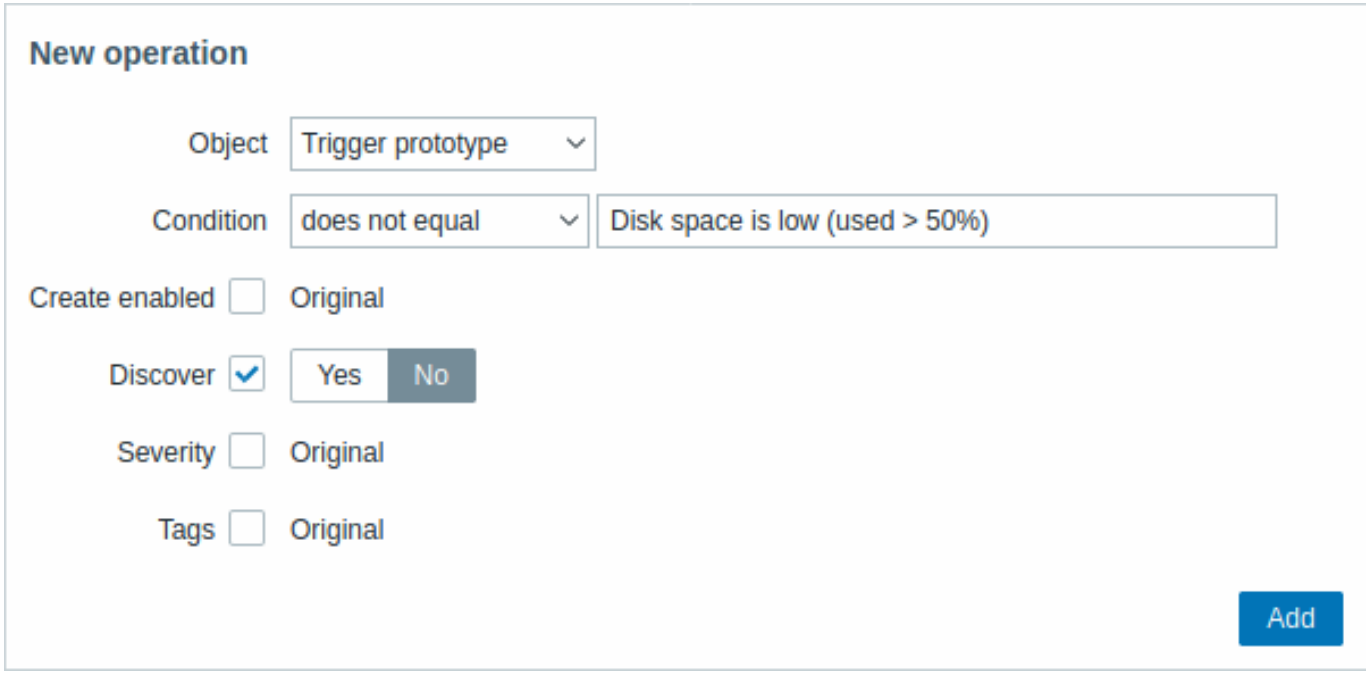


Wszystkie obowiązkowe parametry są oznaczone czerwonymi gwiazdkami.

Parameter	Description
Name	Unikalna (w obrębie reguły LLD) nazwa nadpisania.
If filter matches	Określa, czy kolejne nadpisania powinny być przetwarzane po spełnieniu warunków filtra: **Continue overrides** - kolejne nadpisania będą przetwarzane. **Stop processing** - operacje z poprzednich nadpisań (jeśli istnieją) oraz z tego nadpisania zostaną wykonane, a kolejne nadpisania zostaną zignorowane dla pasujących wierszy LLD.
Filters	Określa, do których wykrytych encji ma zostać zastosowane nadpisanie. Filtry nadpisania są przetwarzane po filtrach reguły wykrywania i mają tę samą funkcjonalność.
Operations	Operacje nadpisania są wyświetlane z następującymi szczegółami: **Condition** - typ obiektu i warunek, który musi zostać spełniony dla nazwy obiektu; na przykład: Prototyp wyzwalacza nie jest równy *Disk space is low (used > 50%)*. **Actions** - wyświetlane są odnośniki do edycji i usunięcia operacji.

Konfigurowanie operacji

Aby skonfigurować szczegóły nowej operacji, kliknij Add w bloku Operations. Aby edytować istniejącą operację, kliknij Edit obok operacji. Otworzy się wyskakujące okno, w którym można edytować szczegóły operacji.



Parameter	Description
Object	Dostępnych jest pięć typów obiektów: Prototyp pozycji Prototyp wyzwalacza Prototyp wykresu Prototyp hosta Prototyp wykrywania
Condition	Umożliwia filtrowanie encji, do których operacja ma zostać zastosowana.
Operator	Obsługiwane operatory: **equals** - zastosuj do tego prototypu **does not equal** - zastosuj do wszystkich prototypów oprócz tego **contains** - zastosuj, jeśli nazwa prototypu zawiera ten ciąg **does not contain** - zastosuj, jeśli nazwa prototypu nie zawiera tego ciągu **matches** - zastosuj, jeśli nazwa prototypu pasuje do wyrażenia regularnego **does not match** - zastosuj, jeśli nazwa prototypu nie pasuje do wyrażenia regularnego
Pattern	Wyrażenie regularne lub ciąg do wyszukania.
Object: *Item prototype*	
Create enabled	Po zaznaczeniu pola wyboru pojawią się przyciski umożliwiające nadpisanie oryginalnych ustawień prototypu pozycji: *Yes* - pozycja zostanie dodana w stanie włączonym. *No* - pozycja zostanie dodana do wykrytej encji, ale w stanie wyłączonym.
Discover	Po zaznaczeniu pola wyboru pojawią się przyciski umożliwiające nadpisanie oryginalnych ustawień prototypu pozycji: *Yes* - pozycja zostanie dodana. *No* - pozycja nie zostanie dodana.
Update interval	Po zaznaczeniu pola wyboru pojawią się dwie opcje umożliwiające ustawienie innego interwału dla pozycji: *Delay* - interwał aktualizacji pozycji. Obsługiwane są makra użytkownika i sufiksy czasu (np. 30s, 1m, 2h, 1d). Należy ustawić na 0, jeśli używany jest *Custom interval*. *Custom interval* - kliknij Add, aby określić elastyczne/planowane interwały. Szczegółowe informacje można znaleźć w sekcji Custom intervals.

Parameter		Description
	History	Po zaznaczeniu pola wyboru pojawią się przyciski umożliwiające ustawienie innego okresu przechowywania historii dla pozycji: *Do not store* - jeśli wybrane, historia nie będzie przechowywana. *Store up to* - jeśli wybrane, po prawej stronie pojawi się pole wejściowe do określenia okresu przechowywania. Obsługiwane są makra użytkownika i makra LLD.
	Trends	Po zaznaczeniu pola wyboru pojawią się przyciski umożliwiające ustawienie innego okresu przechowywania trendów dla pozycji: *Do not store* - jeśli wybrane, trendy nie będą przechowywane. *Store up to* - jeśli wybrane, po prawej stronie pojawi się pole wejściowe do określenia okresu przechowywania. Obsługiwane są makra użytkownika i makra LLD.
	Tags	Po zaznaczeniu pola wyboru pojawi się nowy blok umożliwiający określenie par tag-wartość. Te tagi zostaną dołączone do tagów określonych w prototypie pozycji, nawet jeśli nazwy tagów są takie same.
Object: *Trigger prototype*		
	Create enabled	Po zaznaczeniu pola wyboru pojawią się przyciski umożliwiające nadpisanie oryginalnych ustawień prototypu wyzwalacza: *Yes* - wyzwalacz zostanie dodany w stanie włączonym. *No* - wyzwalacz zostanie dodany do wykrytej encji, ale w stanie wyłączonym.
	Discover	Po zaznaczeniu pola wyboru pojawią się przyciski umożliwiające nadpisanie oryginalnych ustawień prototypu wyzwalacza: *Yes* - wyzwalacz zostanie dodany. *No* - wyzwalacz nie zostanie dodany.
	Severity	Po zaznaczeniu pola wyboru pojawią się przyciski ważności wyzwalacza, umożliwiające modyfikację ważności wyzwalacza.
	Tags	Po zaznaczeniu pola wyboru pojawi się nowy blok umożliwiający określenie par tag-wartość. Te tagi zostaną dołączone do tagów określonych w prototypie wyzwalacza, nawet jeśli nazwy tagów są takie same.
Object: *Graph prototype*		
	Discover	Po zaznaczeniu pola wyboru pojawią się przyciski umożliwiające nadpisanie oryginalnych ustawień prototypu wykresu: *Yes* - wykres zostanie dodany. *No* - wykres nie zostanie dodany.
Object: *Host prototype*		
	Create enabled	Po zaznaczeniu pola wyboru pojawią się przyciski umożliwiające nadpisanie oryginalnych ustawień prototypu hosta: *Yes* - host zostanie utworzony w stanie włączonym. *No* - host zostanie utworzony w stanie wyłączonym.
	Discover	Po zaznaczeniu pola wyboru pojawią się przyciski umożliwiające nadpisanie oryginalnych ustawień prototypu hosta: *Yes* - host zostanie wykryty. *No* - host nie zostanie wykryty.
	Link templates	Po zaznaczeniu pola wyboru pojawi się pole wejściowe do określenia szablonów. Zacznij wpisywać nazwę szablonu lub kliknij *Select* obok pola i wybierz szablony z listy w wyskakującym oknie. Szablony z tego nadpisania są dodawane do wszystkich szablonów już podłączonych do prototypu hosta.

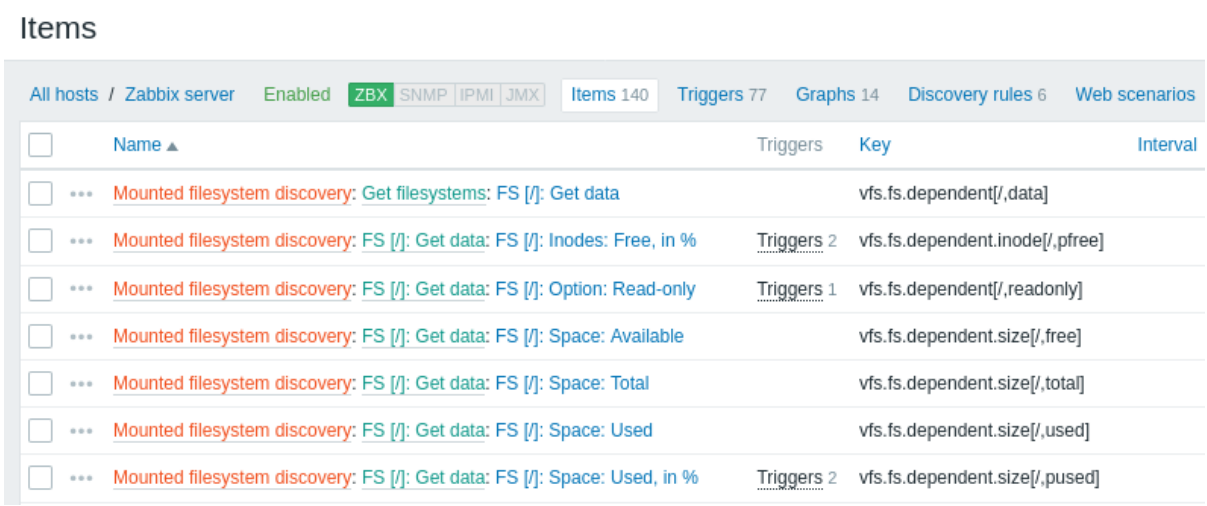
Parameter	Description
Tags	Po zaznaczeniu pola wyboru pojawi się nowy blok umożliwiający określenie par tag-wartość. Te tagi zostaną dołączone do tagów określonych w prototypie hosta, nawet jeśli nazwy tagów są takie same.
Host inventory	Po zaznaczeniu pola wyboru pojawią się przyciski umożliwiające wybór innego trybu inwentarza dla prototypu hosta: *Disabled* - nie wypełniaj inwentarza hosta *Manual* - podaj szczegóły ręcznie *Automated* - automatycznie wypełnij dane inwentarza hosta na podstawie zebranych metryk.

Przyciski formularza

Przyciski na dole formularza umożliwiają wykonanie kilku operacji.

Add	Dodaj regułę wykrywania. Ten przycisk jest dostępny tylko dla nowych reguł wykrywania.
Update	Zaktualizuj właściwości reguły wykrywania. Ten przycisk jest dostępny tylko dla istniejących reguł wykrywania.
Clone	Utwórz kolejną regułę wykrywania na podstawie właściwości bieżącej reguły wykrywania.
Execute now	Wykonaj wykrywanie natychmiast na podstawie reguły wykrywania. Reguła wykrywania musi już istnieć. Zobacz więcej szczegółów. *Uwaga:* podczas natychmiastowego wykonywania wykrywania pamięć podręczna konfiguracji nie jest aktualizowana, dlatego wynik nie będzie odzwierciedlał bardzo niedawnych zmian w konfiguracji reguły wykrywania.
Test	Przetestuj konfigurację reguły wykrywania. Użyj tego przycisku, aby zweryfikować ustawienia konfiguracji (takie jak łączność i poprawność parametrów) bez trwałego stosowania jakichkolwiek zmian.
Delete	Usuń regułę wykrywania.
Cancel	Anuluj edycję właściwości reguły wykrywania.

Odkryte encje Poniższe zrzuty ekranu ilustrują, jak odkryte pozycje, wyzwalacze i wykresy wyglądają w konfiguracji hosta. Odkryte encje są poprzedzone pomarańczowym odnośnikiem do reguły wykrywania, z której pochodzą.



Należy pamiętać, że odkryte encje nie zostaną utworzone, jeśli istnieją już encje o tych samych kryteriach unikalności, na przykład pozycja z takim samym kluczem lub wykres o tej samej nazwie. W takim przypadku w frontend jest wyświetlany komunikat o

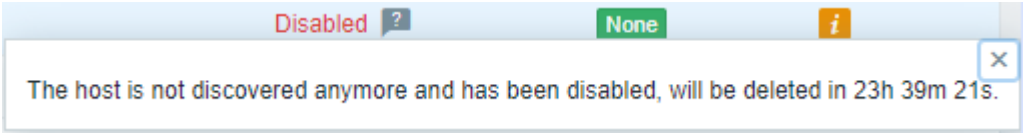
błędzie informujący, że reguła wykrywania niskiego poziomu nie mogła utworzyć niektórych encji. Sama reguła wykrywania nie stanie się jednak nieobsługiwana tylko dlatego, że nie udało się utworzyć jakiejś encji i trzeba było ją pominąć. Reguła wykrywania będzie nadal tworzyć/aktualizować inne encje.

Jeśli odkryta encja (host, system plików, interfejs itp.) przestanie być wykrywana (lub nie przejdzie już filtra), encje utworzone na jej podstawie mogą zostać automatycznie wyłączone, a ostatecznie usunięte.

Utracone zasoby mogą być automatycznie wyłączane na podstawie wartości parametru *Disable lost resources*. Dotyczy to utraconych hostów, pozycji i wyzwalaczy.

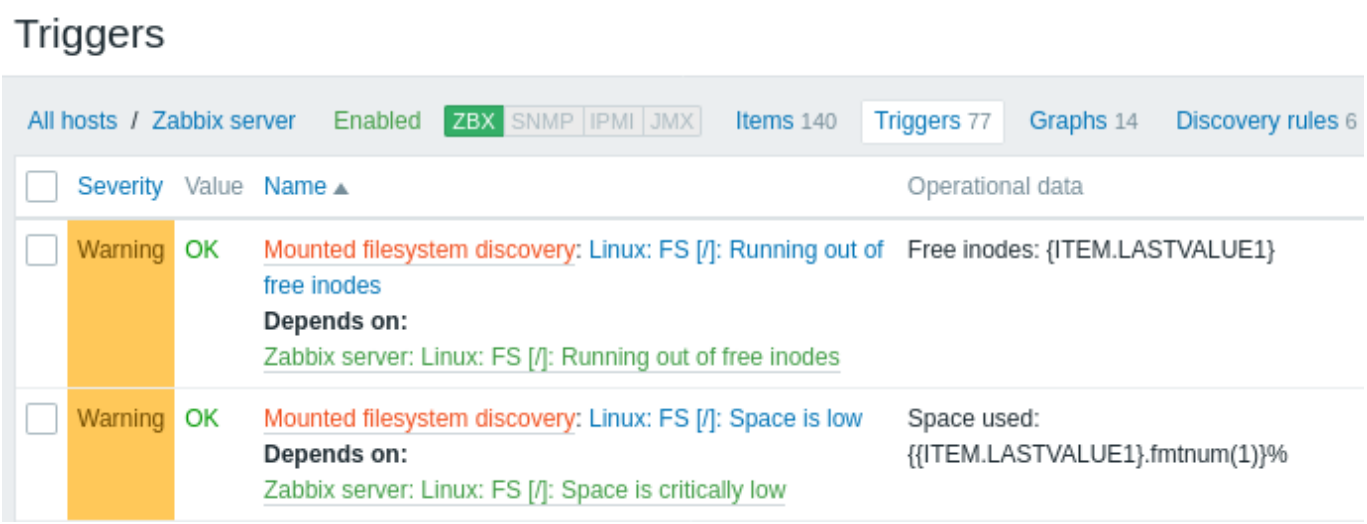
Utracone zasoby mogą być automatycznie usuwane na podstawie wartości parametru *Delete lost resources*. Dotyczy to utraconych hostów, grup hostów, pozycji, wyzwalaczy i wykresów.

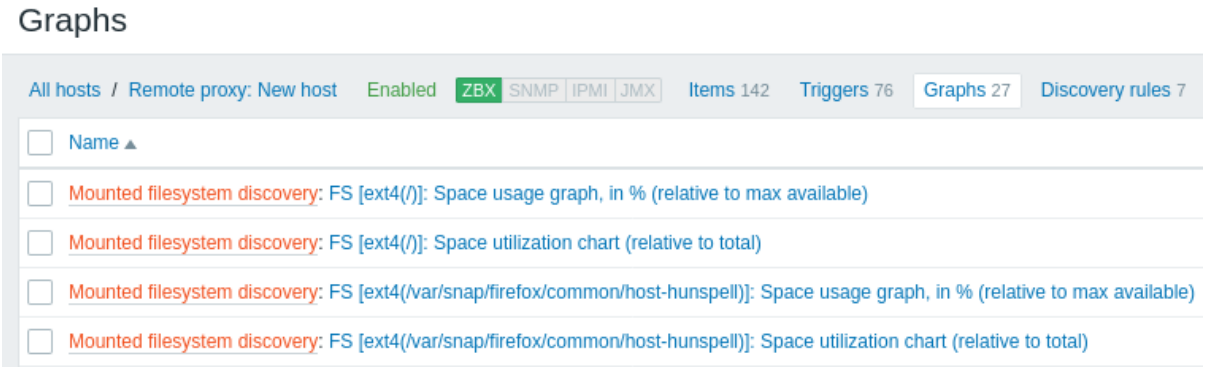
Gdy odkryte encje przechodzą do stanu „Not discovered anymore", na liście encji wyświetlany jest wskaźnik czasu życia. Po najechaniu na niego kursorem myszy zostanie wyświetlony komunikat zawierający szczegóły statusu.



Jeśli encje zostały oznaczone do usunięcia, ale nie zostały usunięte w oczekiwanym czasie (wyłączona reguła wykrywania lub host pozycji), zostaną usunięte przy następnym przetwarzaniu reguły wykrywania.

Encje zawierające inne encje oznaczone do usunięcia nie będą aktualizowane, jeśli zostaną zmienione na poziomie reguły wykrywania. Na przykład wyzwalacze oparte na LLD nie będą aktualizowane, jeśli zawierają pozycje oznaczone do usunięcia.





Inne typy wykrywania Więcej szczegółów oraz instrukcje dotyczące innych gotowych typów wykrywania są dostępne w następujących sekcjach:

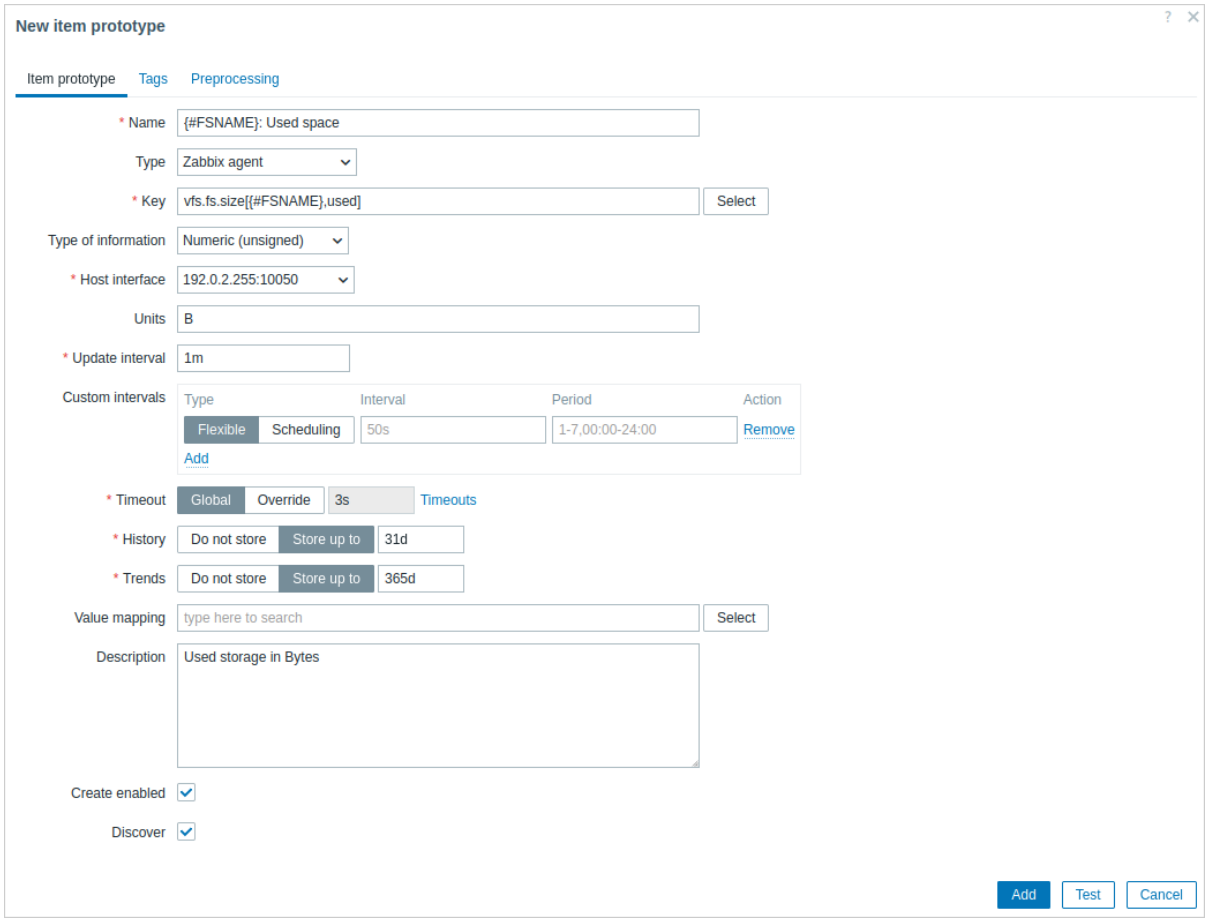
- wykrywanie interfejsów sieciowych
- wykrywanie procesorów i rdzeni CPU
- wykrywanie OID-ów SNMP
- wykrywanie obiektów JMX;
- wykrywanie przy użyciu zapytań SQL ODBC
- wykrywanie usług Windows
- wykrywanie interfejsów hosta w Zabbix

Więcej szczegółów na temat formatu JSON dla pozycji wykrywania oraz przykład implementacji własnego mechanizmu wykrywania systemu plików jako skryptu Perl można znaleźć w sekcji tworzenie niestandardowych reguł LLD.

1 Prototypy pozycji

Po utworzeniu reguły przejdź do pozycji dla tej reguły i naciśnij „Utwórz prototyp pozycji”, aby utworzyć prototyp pozycji.

Zwróć uwagę, jak makro {#FSNAME} jest używane tam, gdzie wymagana jest nazwa systemu plików. Użycie makra low-level discovery jest obowiązkowe w kluczu pozycji, aby mieć pewność, że wykrywanie zostanie przetworzone poprawnie. Gdy reguła wykrywania zostanie przetworzona, to makro zostanie zastąpione wykrytym systemem plików.



Note:
Gdy parametry klucza pozycji nie są używane, umieść makro LLD wewnątrz nawiasów klucza pozycji `[...]` (na przykład `v_[{#MACRO}]`).

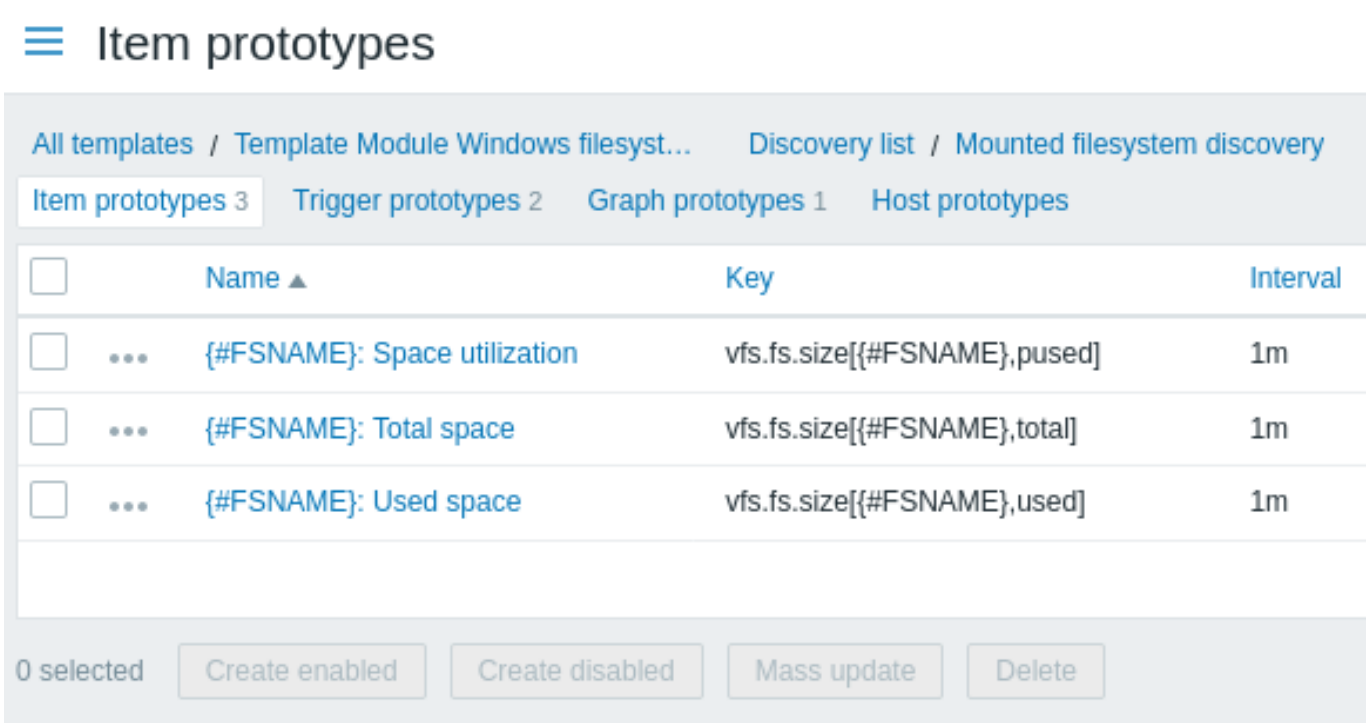
Makra low-level discovery macros oraz makra użytkownika macros są obsługiwane w konfiguracji prototypu pozycji oraz w parametrach wstępnego przetwarzania wartości pozycji. Zwróć uwagę, że w przypadku użycia w interwałach aktualizacji pojedyncze makro musi wypełniać całe pole. Wiele makr w jednym polu lub makra połączone z tekstem nie są obsługiwane.

Note:
Dla bezpiecznego użycia w parametrach wstępnego przetwarzania wyrażeń regularnych i XPath wykonywane jest odpowiednie dla kontekstu maskowanie makr low-level discovery.

Atrybuty specyficzne dla prototypów pozycji:

Parameter	Description
Create enabled	Jeśli zaznaczone, pozycja zostanie dodana w stanie włączonym. Jeśli odznaczone, pozycja zostanie dodana do wykrytego obiektu, ale w stanie wyłączonym.
Discover	Jeśli zaznaczone (domyślnie), pozycja zostanie dodana do wykrytego obiektu. Jeśli odznaczone, pozycja nie zostanie dodana do wykrytego obiektu, chyba że to ustawienie zostanie nadpisane w regule wykrywania.

Możemy utworzyć kilka prototypów pozycji dla każdej metryki systemu plików, która nas interesuje:



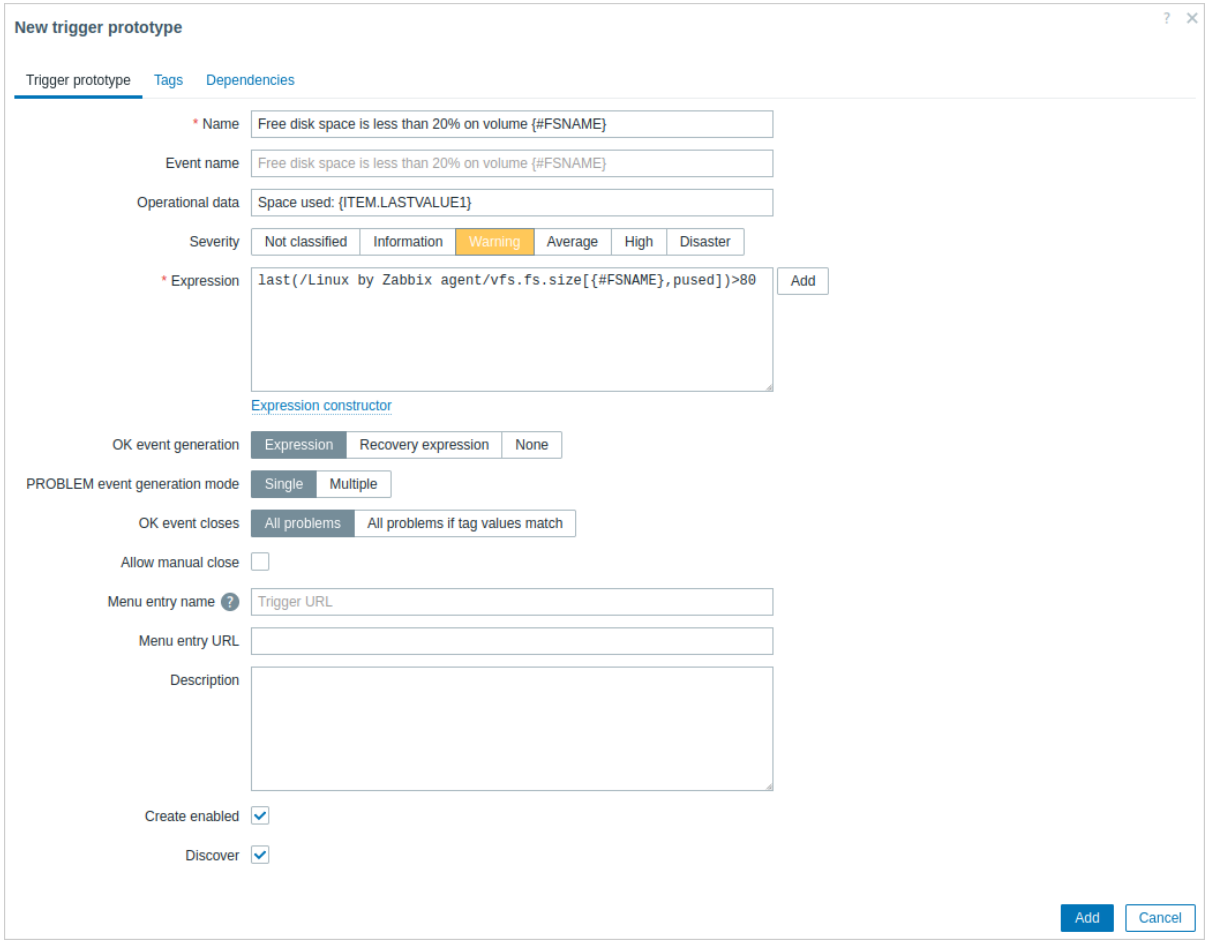
Kliknij ikonę z trzema kropkami, aby otworzyć menu dla konkretnego prototypu pozycji z następującymi opcjami:

- *Create trigger prototype* - utwórz prototyp wyzwalacza na podstawie tego prototypu pozycji
- *Trigger prototypes* - kliknij, aby zobaczyć listę z odnośnikami do już skonfigurowanych prototypów wyzwalaczy tego prototypu pozycji
- *Create dependent item* - utwórz pozycję zależną dla tego prototypu pozycji

Opcja *Mass update* jest dostępna, jeśli chcesz jednocześnie zaktualizować właściwości kilku prototypów pozycji.

2 Prototypy wyzwalaczy

Prototypy wyzwalaczy tworzy się w podobny sposób jak prototypy pozycji:

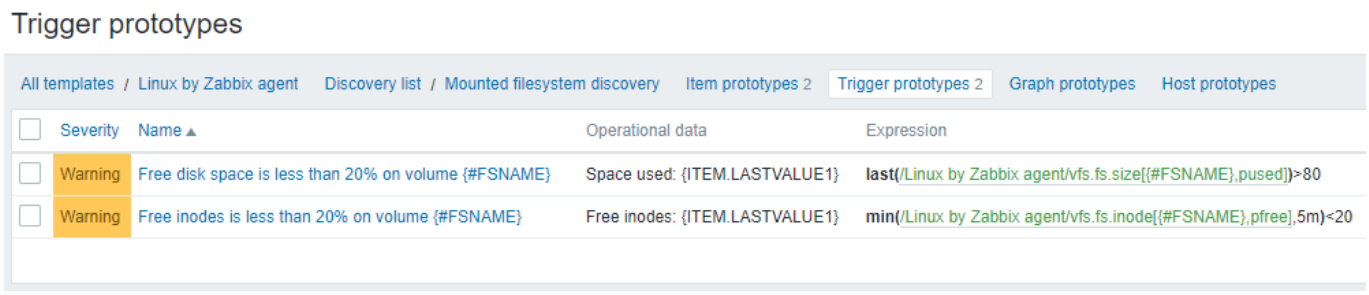


Atrybuty specyficzne dla prototypów wyzwalaczy:

Parametr	Opis
Create enabled	Jeśli zaznaczone, wyzwalacz zostanie dodany w stanie włączonym. Jeśli odznaczone, wyzwalacz zostanie dodany do wykrytego obiektu, ale w stanie wyłączonym.
Discover	Jeśli zaznaczone (domyślnie), wyzwalacz zostanie dodany do wykrytego obiektu. Jeśli odznaczone, wyzwalacz nie zostanie dodany do wykrytego obiektu, chyba że to ustawienie zostanie nadpisane w regule wykrywania.

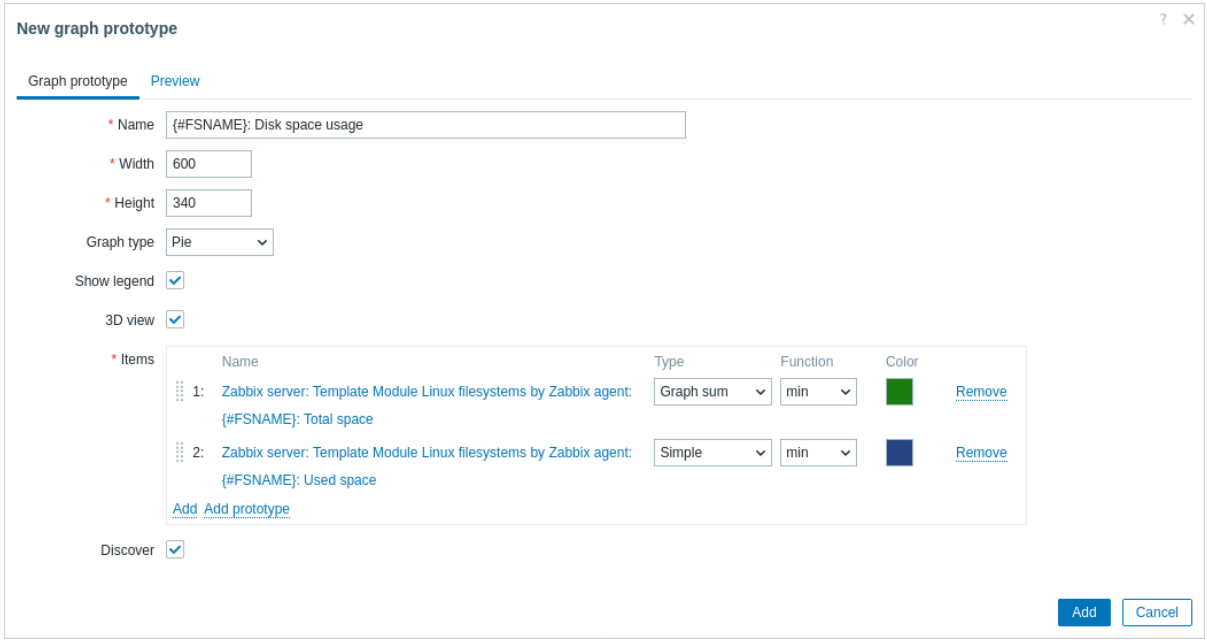
Gdy z prototypów tworzone są rzeczywiste wyzwalacze, może pojawić się potrzeba elastycznego określenia, jaka stała („20” w naszym przykładzie) ma być użyta do porównania w wyrażeniu. Zobacz, jak makra użytkownika z kontekstem mogą być przydatne do uzyskania takiej elastyczności.

Można zdefiniować zależności między prototypami wyzwalaczy. Aby to zrobić, przejdź do zakładki *Dependencies*. Prototyp wyzwalacza może zależeć od innego prototypu wyzwalacza z tej samej reguły wykrywania niskiego poziomu (LLD) lub od zwykłego wyzwalacza. Prototyp wyzwalacza nie może zależeć od prototypu wyzwalacza z innej reguły LLD ani od wyzwalacza utworzonego z prototypu wyzwalacza. Prototyp wyzwalacza hosta nie może zależeć od wyzwalacza z szablonu.



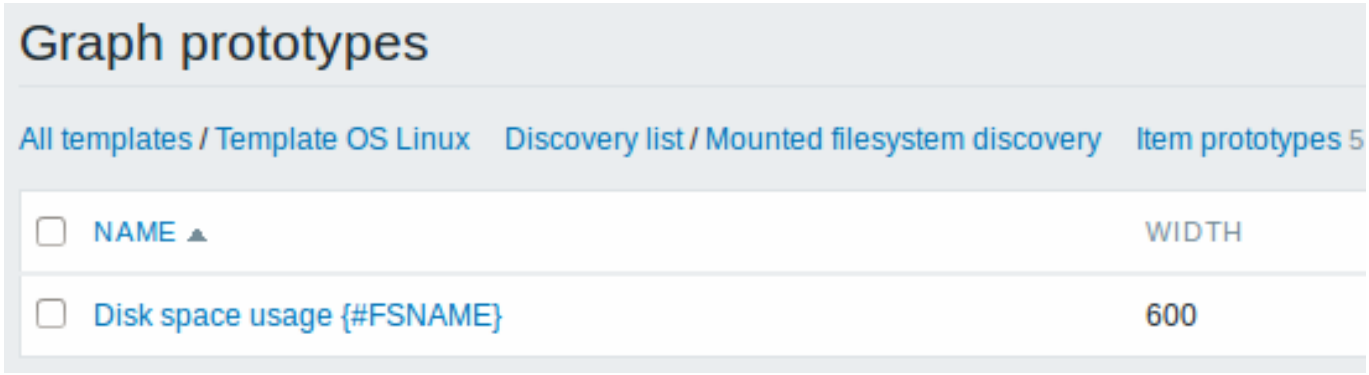
3 Prototypy wykresów

Możemy również tworzyć prototypy wykresów:

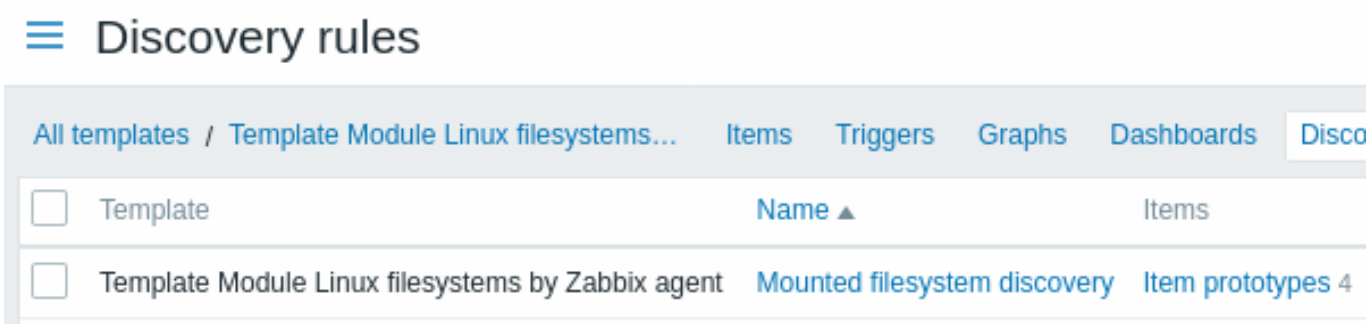


Atrybuty specyficzne dla prototypów wykresów:

Parametr	Opis
Discover	Jeśli zaznaczone (domyślnie), wykres zostanie dodany do wykrytego obiektu. Jeśli odznaczone, wykres nie zostanie dodany do wykrytego obiektu, chyba że to ustawienie zostanie nadpisane w regule wykrywania.



Na koniec utworzyliśmy regułę wykrywania, która wygląda jak pokazano poniżej. Ma ona pięć prototypów pozycji, dwa prototypy wyzwalaczy i jeden prototyp wykresu.



4 Prototypy hostów

Prototypy hostów są wzorcami do tworzenia hostów za pomocą reguł odkrywania niskiego poziomu. Zanim zostaną odkryte jako hosty, te prototypy nie mogą mieć pozycji ani wyzwalaczy, z wyjątkiem tych podłączonych z szablonów.

Konfiguracja

Prototypy hostów są konfigurowane w ramach reguł wykrywania niskiego poziomu.

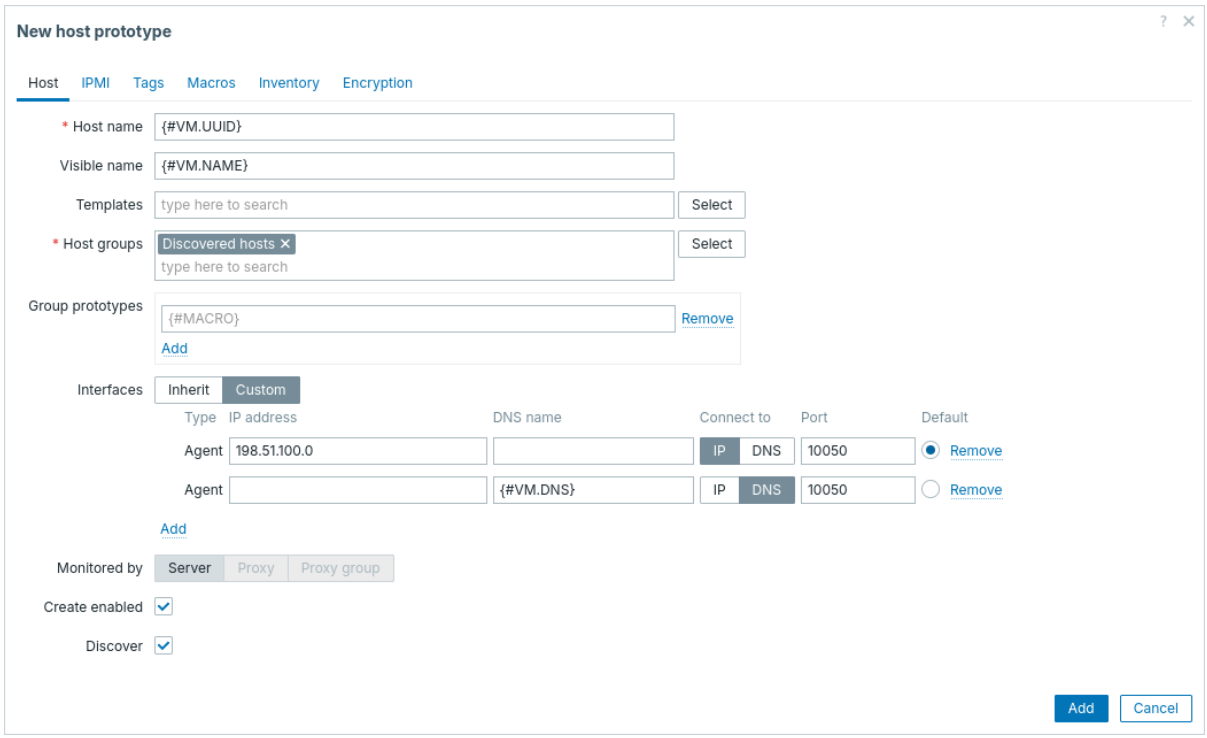
Aby utworzyć prototyp hosta:

1. Przejdź do *Data collection → Hosts*.

2. Kliknij *Discovery* dla wymaganego hosta, aby przejść do listy reguł wykrywania niskiego poziomu skonfigurowanych dla tego hosta.

3. Kliknij *Host prototypes* dla wymaganej reguły wykrywania.

4. Kliknij przycisk *Create host prototype* w prawym górnym rogu i uzupełnij formularz konfiguracji.



Wszystkie wymagane pola wejściowe są oznaczone czerwoną gwiazdką.

Parametr	Opis
Host name	Ten parametr musi zawierać co najmniej jedno makro wykrywania niskiego poziomu, aby zapewnić unikalne nazwy hostów dla tworzonych hostów.
Visible name	Obsługiwane są makra wykrywania niskiego poziomu.
Group prototypes	Umożliwia określenie prototypów grup hostów przy użyciu makr wykrywania niskiego poziomu. Na podstawie określonych prototypów grup grupy hostów zostaną wykryte, utworzone i podłączone do utworzonych hostów; wykryte grupy, które zostały już utworzone przez inne reguły wykrywania niskiego poziomu, również zostaną podłączone do utworzonych hostów. Jednak wykryte grupy hostów, które odpowiadają grupom hostów utworzonym ręcznie, nie zostaną podłączone do utworzonych hostów.
Interfaces	Ustaw, czy wykryte hosty dziedziczą adres IP po hoście, do którego należy reguła wykrywania (domyślnie), czy otrzymują niestandardowe interfejsy. Obsługiwane są makra wykrywania niskiego poziomu i makra użytkownika.
Monitored by	To pole jest synchronizowane automatycznie z odpowiednim polem w konfiguracji hosta.
Create enabled	Ustaw status wykrytych hostów; jeśli pole nie jest zaznaczone, hosty zostaną utworzone jako wyłączone.
Discover	Ustaw, czy hosty będą tworzone z prototypu hosta; jeśli pole nie jest zaznaczone, hosty nie będą tworzone z prototypu hosta (chyba że to ustawienie zostanie nadpisane w regule wykrywania niskiego poziomu).

Note:
Makra wykrywania niskiego poziomu są również obsługiwane dla wartości tagów i wartości makr użytkownika prototypu hosta.
 Mapowania wartości nie są obsługiwane dla prototypów hostów.

Przykład konfiguracji prototypu hosta znajduje się w sekcji *Virtual machine monitoring*.

Interfejsy hosta

Aby dodać niestandardowe interfejsy, przełącz selektor *Interfaces* z „Inherit” na „Custom”. Kliknij Add i wybierz typ interfejsu — Zabbix agent, SNMP, JMX, IPMI.

Note:
Jeśli wybrano *Custom*, ale nie ustawiono żadnych interfejsów, hosty zostaną utworzone bez interfejsów.
 Jeśli wybrano *Inherit* i prototyp hosta należy do szablonu, wszystkie wykryte hosty odziedziczą interfejs hosta od hosta, do którego podłączony jest szablon.

Jeśli określono wiele niestandardowych interfejsów, podstawowy interfejs można ustawić w kolumnie *Default*.

Przykład konfiguracji niestandardowego interfejsu hosta znajduje się w *przykładzie konfiguracji monitorowania VMware*.

Warning:
Host zostanie utworzony tylko wtedy, gdy interfejs hosta zawiera poprawne dane.

Wykryte hosty

Na liście hostów wykryte hosty są poprzedzone nazwą reguły wykrywania, która je utworzyła.

Wykryte hosty dziedziczą większość parametrów z prototypów hostów jako *tylko do odczytu*. Skonfigurować można tylko następujące parametry wykrytego hosta:

- *Szablony* - połączyć nowe szablony lub odłączyć dodane ręcznie. Szablonów odziedziczonych z prototypu hosta nie można odłączyć.
- *Opis* - dodać lub edytować opis hosta.
- *Status* - włączyć lub wyłączyć host.
- *Tagi* - dodać nowe tagi lub usunąć dodane ręcznie. Tagów odziedziczonych z prototypu hosta nie można usunąć. Należy pamiętać, że tagi nie mogą się powielać (tagi o tej samej nazwie i wartości). Jeśli do prototypu hosta zostanie dodany nowy tag i będzie on odpowiadał tagowi dodanemu ręcznie w wykrytym hoście, podczas wykrywania tag dodany ręcznie zostanie zastąpiony tagiem odziedziczonym.
- *Makra* - dodać nowe makra hosta lub usunąć dodane ręcznie, a także te odziedziczone z prototypu hosta; zmienić wartości makr i typy.

Note:
Wykryte hosty dziedziczą również makra użytkownika z hosta, na którym skonfigurowano regułę wykrywania. Te odziedziczone makra można usunąć, a ich wartości i typy można zmienić.

Wykryte hosty mogą również wykrywać inne hosty. Na przykład, jeśli prototyp hosta (używany do wykrywania hiperwizorów) ma podłączony szablon zawierający regułę wykrywania niskiego poziomu z własnym prototypem hosta (używanym do wykrywania maszyn wirtualnych), Zabbix wykryje zarówno hiperwizory, jak i ich maszyny wirtualne. Aby dodatkowo wykrywać kontenery na tych maszynach wirtualnych, można utworzyć reguły wykrywania niskiego poziomu lub podłączyć nowy szablon z prototypami hostów do wykrytych maszyn wirtualnych, albo wstępnie skonfigurować prototyp hosta maszyny wirtualnej przez podłączenie szablonu, który sam zawiera prototypy hostów.

Wykryte hosty można usuwać ręcznie. Należy jednak pamiętać, że zostaną wykryte ponownie, jeśli wykrywanie będzie dla nich włączone.

Hosty, które nie są już wykrywane, mogą zostać:

- automatycznie wyłączone (na podstawie wartości *Disable lost resources* reguły wykrywania)
- automatycznie usunięte (na podstawie wartości *Delete lost resources* reguły wykrywania).

5 Prototypy wykrywania

Przegląd

Prototypy wykrywania to **zagnieżdżone reguły wykrywania niskiego poziomu** w ramach „nadrzędnej” reguły wykrywania, umożliwiające tworzenie wielopoziomowego wykrywania obiektów z ich własnymi pozycjami, wyzwalaczami itp. Na przykład możesz chcieć wykryć wszystkie instancje bazy danych na serwerze bazy danych, następnie wykryć przestrzenie tabel dla każdej instancji, a potem wykryć tabele dla każdej przestrzeni tabel.

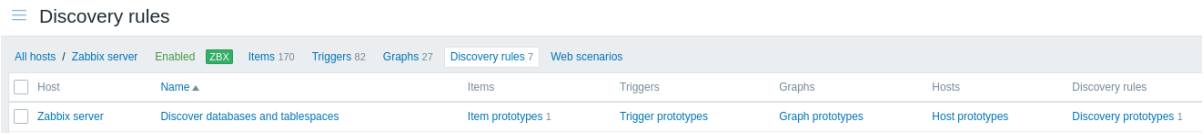
Prototypy wykrywania mają własne prototypy pozycji, wyzwalaczy, wykresów, hostów i wykrywania. Zagnieżdżony prototyp wykrywania będzie używać tej samej wartości JSON co reguła nadrzędna, jeśli określisz typ *Nested*.

Liczba poziomów zagnieżdżenia dla prototypów wykrywania jest nieograniczona.

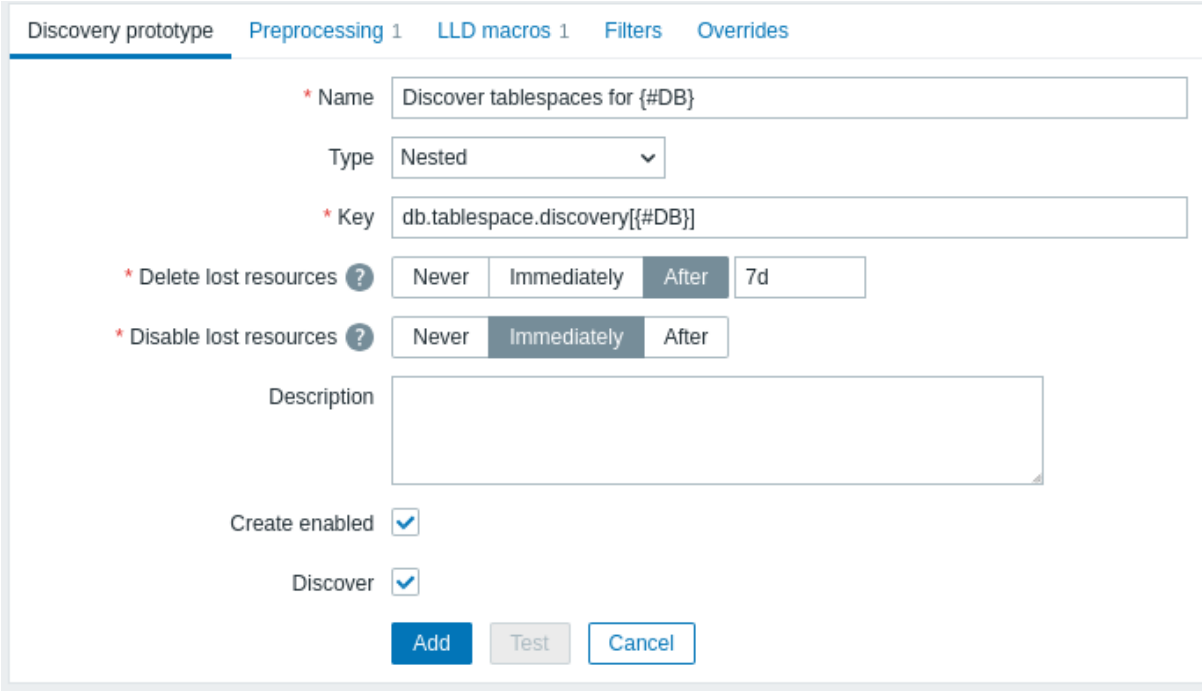
Konfiguracja

Aby utworzyć prototyp wykrywania:

- Kliknij *Discovery prototypes* w wierszu istniejącej reguły wykrywania



- Kliknij *Create discovery prototype*



Pola konfiguracyjne tego formularza są wspólne ze standardowym wykrywaniem niskiego poziomu.

Jeśli w otwartym formularzu prototypu wykrywania wybierzesz „Nested" jako *Type*, reguły wykrywania (z prototypu wykrywania) będą generowane na podstawie obiektu JSON z tej samej wartości JSON co nadrzędna reguła wykrywania. Na przykład, jeśli oryginalny JSON ma postać [<object A>, <object B>] i istnieje jeden prototyp zagnieżdżonej reguły wykrywania, wówczas zostaną wygenerowane dwie reguły wykrywania odpowiednio na podstawie danych obiektu A i obiektu B.

W takim przypadku prototyp wykrywania jest aktywowany w tym samym czasie co reguła nadrzędna. Dzięki temu reguła zagnieżdżona może używać przetwarzania wstępnego, aby pracować na innym „wycinku" tych samych danych, już pobranych przez regułę nadrzędną.

Makra LLD z nadrzędnej reguły LLD są dostępne dla zagnieżdżonych reguł wykrywania.

Zagnieżdżone reguły LLD na wykrytych hostach

Zagnieżdżona reguła wykrywania niskiego poziomu może być używana w szablonie hosta przypisanym do prototypu hosta. Jeśli na wykrytym hoście istnieje *zagnieżdżona* reguła wykrywania, wówczas obiekt JSON użyty do wykrycia hosta jest również przekazywany do wszystkich reguł LLD typu zagnieżdżonego na tym hoście. Więcej szczegółów znajduje się w przykładzie.

Makra LLD z reguły wykrywania, która utworzyła host, są dostępne dla zagnieżdżonych reguł wykrywania.

Przykład

Zilustrujmy możliwe zastosowanie prototypów wykrywania na podstawie otrzymania następującego przykładu wielopoziomowego JSON.

```
[
  {
    "database": "db1",
    "created_at": "2024-02-01T12:30:00Z",
    "encoding": "UTF8",
    "tablespaces": [
      { "name": "ts1", "max_size": "10GB" },
      { "name": "ts2", "max_size": "20GB" },
      { "name": "ts3", "max_size": "15GB" }
    ]
```

```
  },
  {
    "database": "db2",
    "created_at": "2023-11-15T08:45:00Z",
    "encoding": "UTF16",
    "tablespaces": [
      { "name": "ts1", "max_size": "5GB" },
      { "name": "ts2", "max_size": "25GB" },
      { "name": "ts3", "max_size": "30GB" }
    ]
  },
  {
    "database": "db3",
    "created_at": "2024-01-05T15:10:00Z",
    "encoding": "UTF8",
    "tablespaces": [
      { "name": "ts1", "max_size": "12GB" },
      { "name": "ts2", "max_size": "18GB" },
      { "name": "ts3", "max_size": "22GB" }
    ]
  }
]
```

Przypadek 1

Wykrywanie instancji baz danych na serwerze bazodanowym, a następnie wykrywanie tablespace dla każdej instancji.

1. Masz co najmniej jeden host powiązany z wykrywaniem serwera bazodanowego.
2. Utwórz regułę LLD dla tego hosta o nazwie *Wykryj bazy danych i tablespace*.
3. Przejdź do zakładki *Makra LLD* w tej regule i dodaj makro `{#DB}=$.database`.
4. Dodaj prototyp pozycji dla tej reguły o nazwie *Aktywne połączenia do {#DB}* (Typ: Agent, Klucz: `db.connections[{#DB}]`).
5. Zostaną wykryte pozycje powiązane z każdą bazą danych:

```
Active connections to db1, Active connections to db2, Active connections to db3.
```

6. Utwórz prototyp wykrywania dla tej reguły o nazwie *Wykryj tablespace dla {#DB}* (Typ: Zagnieżdżony, Klucz: `db.tablespace.discovery[{#DB}]`).
7. Przejdź do zakładki *Przetwarzanie wstępne* tego prototypu wykrywania i dodaj krok `JSONPath=$.tablespaces`.
8. Przejdź do zakładki *Makra LLD* tego prototypu wykrywania i dodaj makro `{#TSNAME}=$.name`.
9. Utwórz prototyp pozycji dla tego prototypu wykrywania o nazwie *Rozmiar tablespace {#TSNAME} dla {#DB}* (Typ: Agent, Klucz: `db.ts.size[{#DB}, {#TSNAME}]`).
10. Zostaną wykryte pozycje powiązane z każdym tablespace każdej bazy danych:

```
Size of tablespace ts1 for db1, Size of tablespace ts2 for db1, Size of tablespace ts3 for db1,
Size of tablespace ts1 for db2, Size of tablespace ts2 for db2, Size of tablespace ts3 for db2,
Size of tablespace ts1 for db3, Size of tablespace ts2 for db3, Size of tablespace ts3 for db3.
```

z kluczami `db.ts.size[db1,ts1]`, `db.ts.size[db1,ts2]`, ... `db.ts.size[db3,ts3]`.

Przypadek 2

Wykrywanie instancji baz danych na serwerze bazy danych poprzez reprezentowanie ich jako wykrytych hostów, a następnie wykrywanie tablespace dla każdej instancji.

1. Masz co najmniej jeden host (host główny) powiązany z wykrywaniem serwera bazy danych.
2. Utwórz szablon do wykrywania tablespace dla każdej bazy danych.
3. Utwórz w tym szablonie pozycję o nazwie *Aktywne połączenia do {#DB}* (Typ: Agent, Klucz: `db.connections[{#DB}]`).
4. Utwórz regułę LLD dla tego szablonu o nazwie *Wykryj tablespace* (Typ: Zagnieżdżony).
5. Przejdź do zakładki *Preprocessing* tej reguły i dodaj krok `JSONPath=$.tablespaces`.
6. Przejdź do zakładki *LLD Macros* tej reguły, dodaj makro `{#TSNAME}=$.name`.

7. Utwórz prototyp pozycji dla tej reguły o nazwie *Rozmiar tablespace {#TSNAME} dla {#DB}* (Typ: Agent, Klucz: `db.ts.size[{#DB}, {#TSNAME}]`).
8. Wróć do hosta głównego i utwórz regułę LLD dla tego hosta o nazwie *Wykryj bazy danych i tablespace*.
9. Przejdź do zakładki *LLD Macros* tej reguły, dodaj makro `{#DB}=$.database`.
10. Dodaj prototyp hosta dla tej reguły o nazwie *Host dla bazy danych {#DB}*.
11. Przejdź do zakładki *Macros* tego prototypu hosta, dodaj makro `{$DB}={#DB}` (dla nazwy i klucza pozycji z kroku 3).
12. Podłącz szablon z kroku 2 do tego prototypu hosta.
13. Wykryte hosty zawierają wykryte pozycje powiązane z każdą bazą danych i jej tablespace:

Host	Pozycje
Host dla bazy danych db1	Aktywne połączenia do db1
	Rozmiar tablespace ts1 dla db1
	Rozmiar tablespace ts2 dla db1
	Rozmiar tablespace ts3 dla db1
Host dla bazy danych db2	Aktywne połączenia do db2
	Rozmiar tablespace ts1 dla db2
	Rozmiar tablespace ts2 dla db2
	Rozmiar tablespace ts3 dla db2
Host dla bazy danych db3	Aktywne połączenia do db3
	Rozmiar tablespace ts1 dla db3
	Rozmiar tablespace ts2 dla db3
	Rozmiar tablespace ts3 dla db3

6 Uwagi dotyczące wykrywania niskiego poziomu

Używanie makr LLD w kontekstach makr użytkownika

Makra LLD mogą być używane wewnątrz kontekstu makr użytkownika, na przykład w prototypach wyzwalaczy.

Wiele reguł LLD dla tej samej pozycji

Możliwe jest zdefiniowanie kilku reguł wykrywania niskiego poziomu z tą samą pozycją wykrywania.

Aby to zrobić, należy zdefiniować parametr agenta Alias parameter, który pozwala używać zmodyfikowanych kluczy pozycji wykrywania w różnych regułach wykrywania, na przykład `vfs.fs.discovery[foo]`, `vfs.fs.discovery[bar]` itd.

Limity danych dla wartości zwracanych

Nie ma limitu dla danych JSON reguły wykrywania niskiego poziomu, jeśli są one odbierane bezpośrednio przez serwer Zabbix. Wynika to z tego, że wartości zwracane są przetwarzane bez zapisywania ich w bazie danych.

Nie ma również limitu dla niestandardowych reguł wykrywania niskiego poziomu. Jeśli jednak dane niestandardowej reguły wykrywania niskiego poziomu są pobierane przy użyciu parametru użytkownika, obowiązuje limit wartości zwracanej dla parametru użytkownika.

Jeśli dane muszą przejść przez proxy Zabbix, proxy musi zapisać te dane w bazie danych. W takim przypadku obowiązują limity bazy danych.

7 Reguły wykrywania

Skorzystaj z paska bocznego, aby zobaczyć przykłady konfiguracji reguł wykrywania dla różnych przypadków.

1 Wykrywanie zamontowanych systemów plików

Przegląd

Możliwe jest wykrywanie zamontowanych systemów plików i ich właściwości:

- nazwa punktu montowania
- typ systemu plików
- rozmiar systemu plików
- statystyki inode

- opcje montowania

Aby to zrobić, można użyć połączenia:

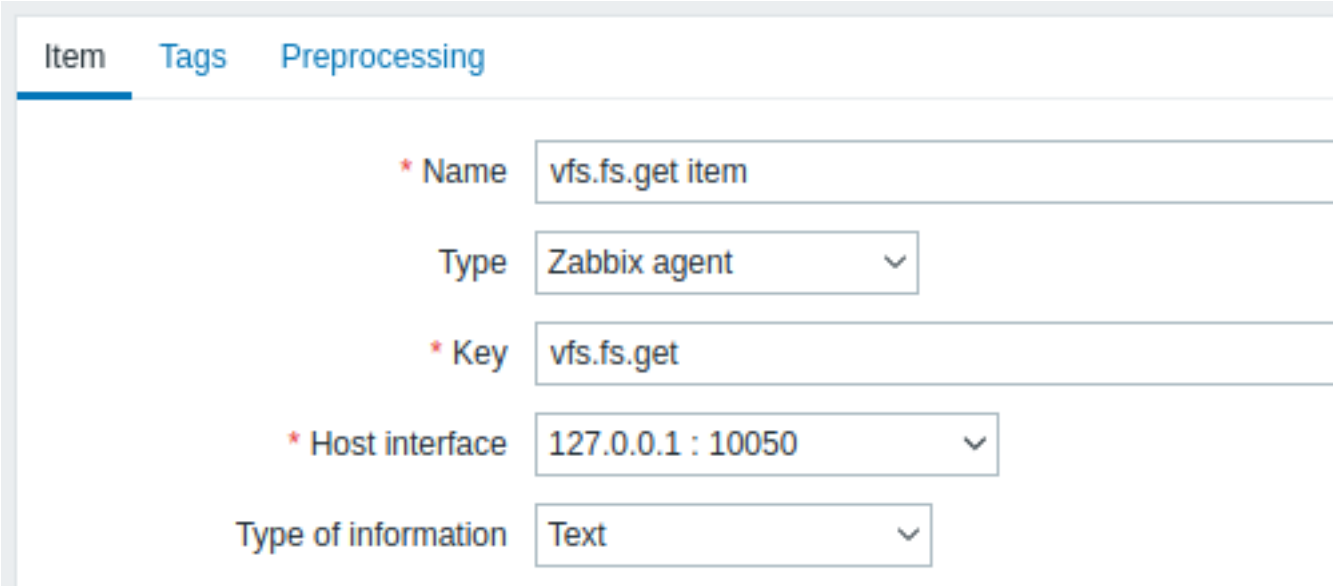
- pozycji agent `vfs.fs.get` jako pozycji nadrzędnej
- zależnej reguły wykrywania niskiego poziomu oraz prototypów pozycji

Konfiguracja

Główna pozycja

Utwórz pozycję agenta Zabbix, używając następującego klucza:

`vfs.fs.get`



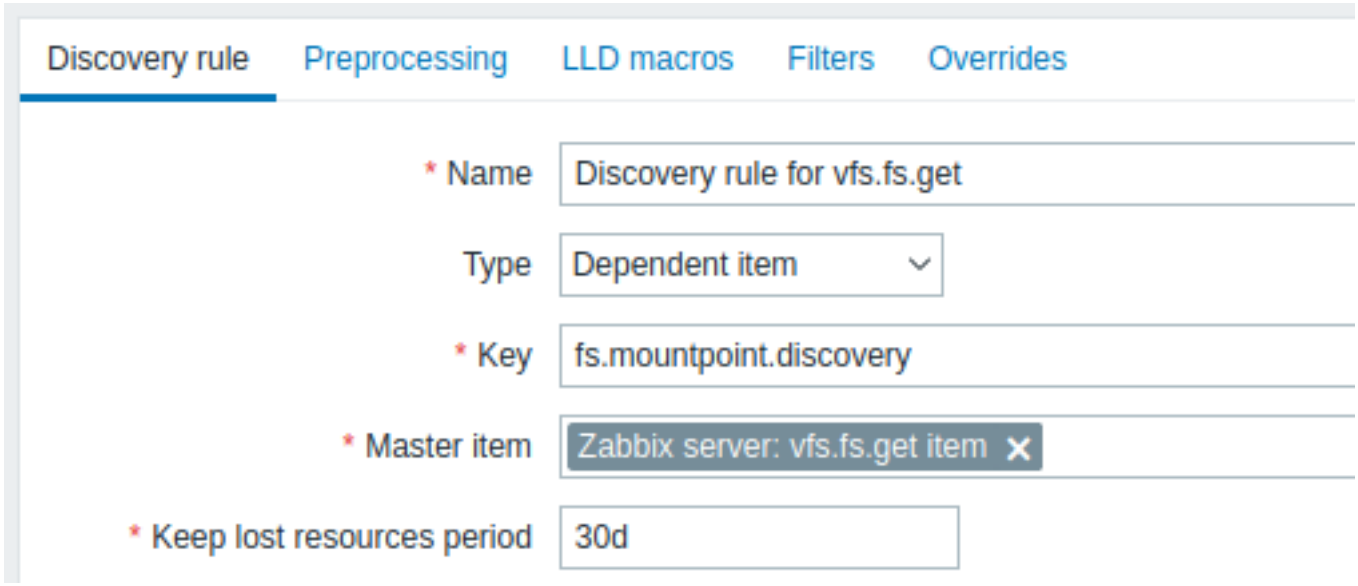
Ustaw typ informacji na „Tekst” dla potencjalnie dużych danych JSON.

Dane zwracane przez tę pozycję będą zawierać coś podobnego do poniższego dla zamontowanego systemu plików:

```
[
  {
    "fsname": "/",
    "fstype": "ext4",
    "bytes": {
      "total": 249405239296,
      "free": 24069537792,
      "used": 212595294208,
      "pfree": 10.170306,
      "pused": 89.829694
    },
    "inodes": {
      "total": 15532032,
      "free": 12656665,
      "used": 2875367,
      "pfree": 81.487503,
      "pused": 18.512497
    },
    "options": "rw,noatime,errors=remount-ro"
  }
]
```

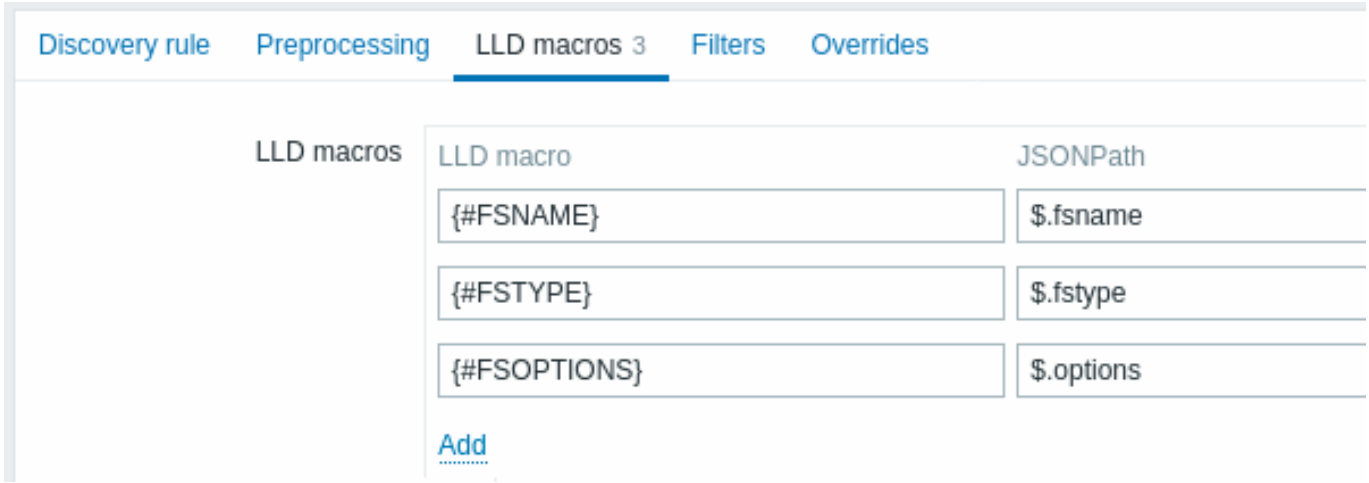
Zależna reguła LLD

Utwórz regułę wykrywania niskiego poziomu typu „Dependent item”:

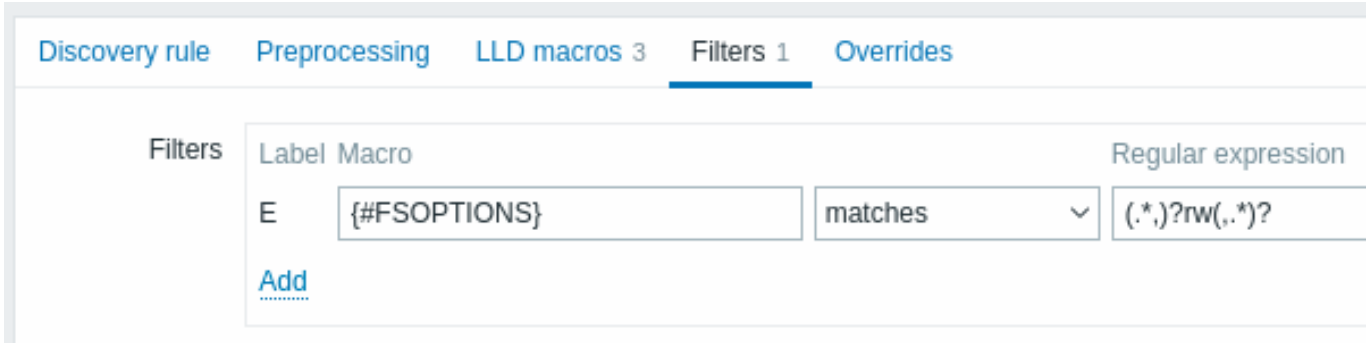


Jako pozycję nadrzędną wybierz utworzoną przez nas pozycję `vfs.fs.get`.

Na karcie „LLD macros” zdefiniuj własne makra z odpowiadającymi im ścieżkami JSONPath:

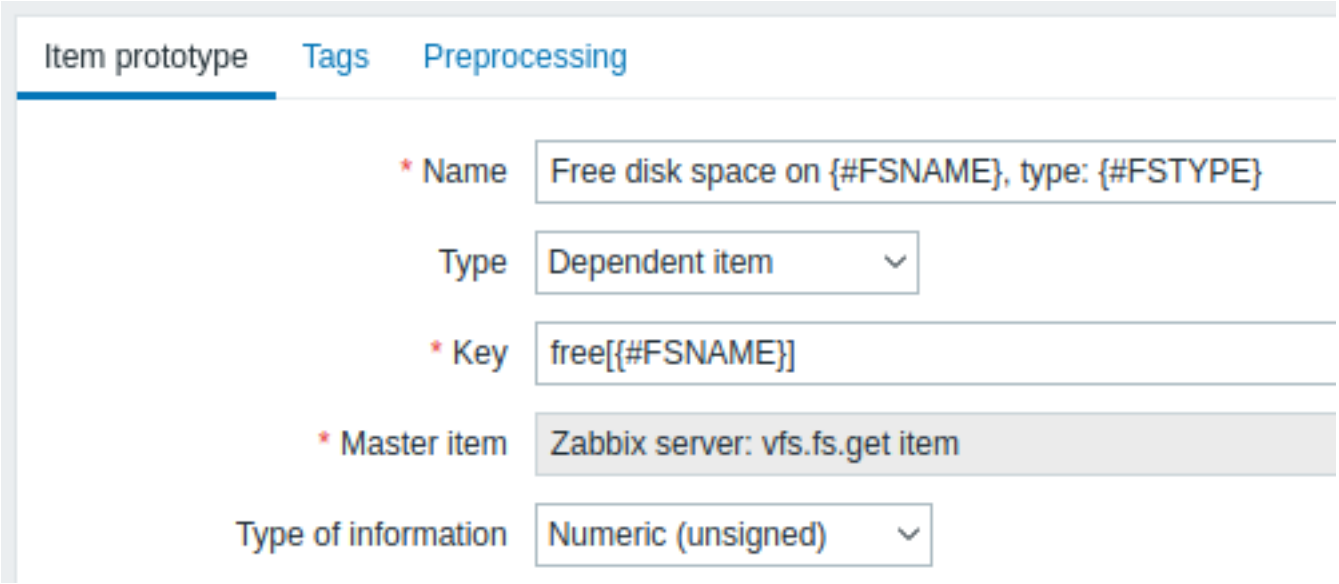


Na karcie „Filters” możesz dodać wyrażenie regularne, które odfiltruje tylko systemy plików **do odczytu i zapisu**:



Zależna pozycja prototypu

Utwórz prototyp pozycji z typem „Dependent item” w tej regule LLD. Jako pozycję nadrzędną dla tego prototypu wybierz utworzoną przez nas pozycję `vfs.fs.get`.



Zwróć uwagę na użycie własnych makr w nazwie i kluczu prototypu pozycji:

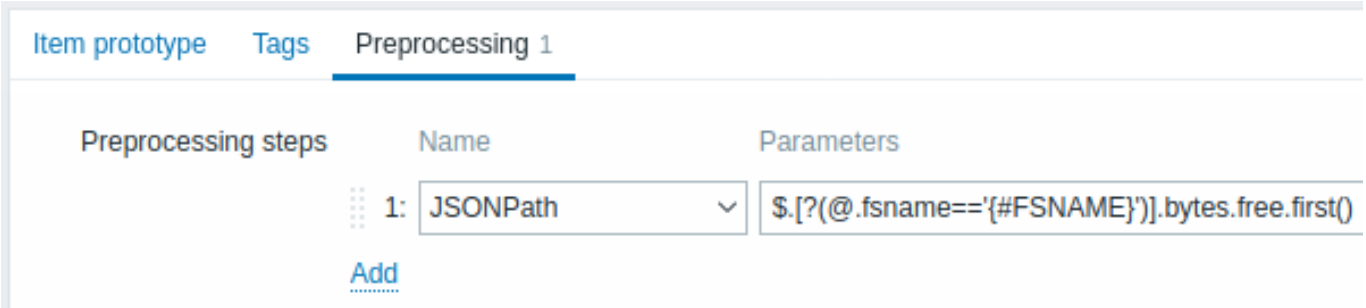
- *Nazwa*: Wolne miejsce na dysku na {#FSNAME}, typ: {#FSTYPE}
- *Klucz*: Free[{#FSNAME}]

Jako typ informacji użyj:

- *Numeric (unsigned)* dla metryk takich jak „free”, „total”, „used”
- *Numeric (float)* dla metryk takich jak „pfree”, „pused” (procent)

Na karcie „Preprocessing” prototypu pozycji wybierz JSONPath i użyj następującego wyrażenia JSONPath jako parametru:

```
$.[?(@.fsname=='{#FSNAME}')].bytes.free.first()
```



Po rozpoczęciu wykrywania zostanie utworzona jedna pozycja dla każdego punktu montowania. Ta pozycja będzie zwracała liczbę wolnych bajtów dla danego punktu montowania.

2 Wykrywanie interfejsów sieciowych

Podobnie jak wykrywane są systemy plików, możliwe jest również wykrywanie interfejsów sieciowych.

Klucz pozycji

Klucz pozycji używany w regule odkrywania to

```
net.if.discovery
```

Obsługiwane makra

Możesz użyć makra {#IFNAME} w filtrze reguły wykrywania oraz w prototypach pozycji, wyzwalaczy i wykresów.

Przykłady prototypów pozycji, które możesz chcieć utworzyć na podstawie ”net.if.discovery”:

- ”net.if.in[{#IFNAME},bytes]”,
- ”net.if.out[{#IFNAME},bytes]”.

Zwróć uwagę, że w systemie Windows zwracane jest również {#IFGUID}.

3 Wykrywanie procesorów CPU i rdzeni CPU

Podobnie jak wykrywane są systemy plików, możliwe jest również wykrywanie procesorów CPU i rdzeni CPU.

Klucz pozycji

Klucz pozycji używany w regule odkrywania to

`system.cpu.discovery`

Obsługiwane makra

Ten klucz wykrywania zwraca dwa makra - {#CPU.NUMBER} oraz {#CPU.STATUS}, identyfikujące odpowiednio numer porządkowy CPU i jego stan. Wylicza procesory od 0 do N - 1, gdzie N jest całkowitą liczbą procesorów.

```
[
    {
        "{#CPU.NUMBER}": 0,
        "{#CPU.STATUS}": "online"
    },
    {
        "{#CPU.NUMBER}": 1,
        "{#CPU.STATUS}": "offline"
    },
    {
        "{#CPU.NUMBER}": 2,
        "{#CPU.STATUS}": "unknown" /* "unknown" występuje tylko w systemie Windows */
    },
    {
        "{#CPU.NUMBER}": 3,
        "{#CPU.STATUS}": "online"
    }
]
```

Należy pamiętać, że nie da się jednoznacznie rozróżnić rzeczywistych, fizycznych procesorów, rdzeni i wątków hyper-threading. {#CPU.STATUS} w systemach Linux, UNIX i BSD zwraca stan procesora, który może mieć wartość "online" lub "offline". W systemach Windows to samo makro może przyjmować trzecią wartość - "unknown" - co oznacza, że procesor został wykryty, ale nie zebrano jeszcze o nim żadnych informacji.

Wykrywanie CPU opiera się na procesie collectora agenta, aby zachować spójność z danymi dostarczanymi przez collector i oszczędzać zasoby podczas pozyskiwania danych. Powoduje to, że ten klucz pozycji nie działa z flagą wiersza poleceń test (-t) pliku binarnego agenta, która zwróci stan NOT_SUPPORTED wraz z komunikatem informującym, że proces collectora nie został uruchomiony.

Prototypy pozycji, które można utworzyć na podstawie wykrywania CPU, obejmują na przykład:

- `system.cpu.util[{#CPU.NUMBER},<type>,<mode>]`
- `system.hw.cpu[{#CPU.NUMBER},<info>]`

Szczegółowy opis kluczy pozycji można znaleźć w sekcji klucze pozycji agenta Zabbix.

Uwagi dotyczące wykrytych pozycji liczników wydajności w systemach NUMA

Niektóre liczniki wydajności Windows mogą nie być dostępne dla części procesorów logicznych w systemach NUMA.

Na przykład pozycje wykryte za pomocą prototypu pozycji z poniższym kluczem mogą działać tylko dla pierwszego węzła NUMA. Pozycje dla pozostałych węzłów NUMA mogą być w stanie nieobsługiwanym.

`perf_counter[\Processor({#CPU.NUMBER})\% Processor Time,60]`

Ponadto reguła wykrywania z kluczem "system.cpu.discovery" nie dostarcza żadnych wartości makr wykrywania niskiego poziomu, które można by podstawić do takich liczników wydajności jak:

`perf_counter["\Processor Information(<NUMA node index>,<CPU index in NUMA node>)\% Processor Time",60]`

Natomiast pozycje system.cpu.util opierają się na innych licznikach wydajności do monitorowania procentowego wykorzystania CPU, w zależności od liczby grup procesorów i liczby procesorów. Występuje również rzadki błąd związany z grupami procesorów w Windows.

4 Odkrywanie OID-ów SNMP

Przegląd

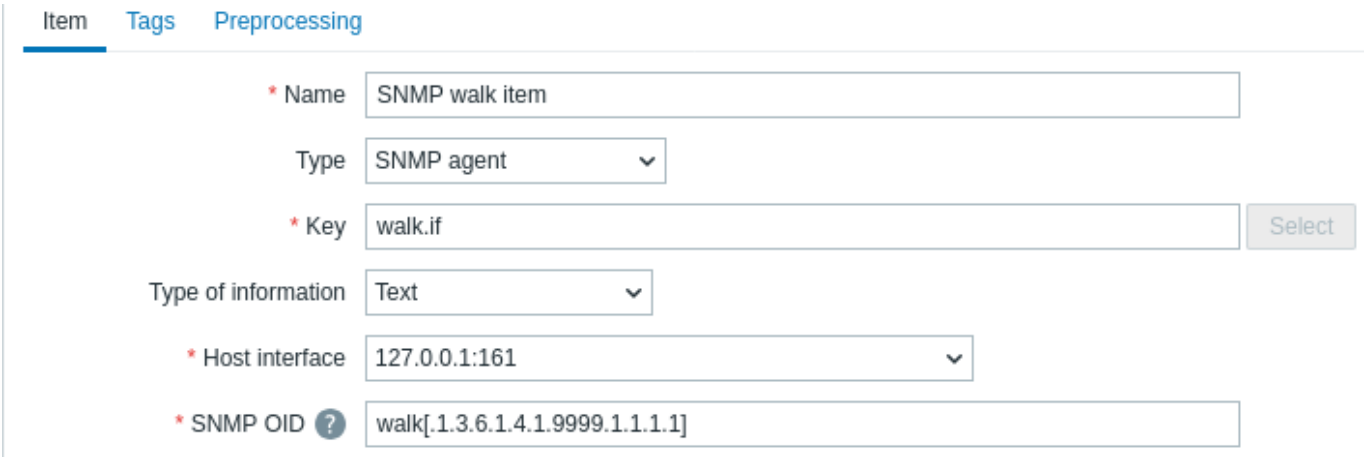
W tej sekcji przeprowadzimy odkrywanie niskiego poziomu na urządzeniu SNMP.

Ta metoda odkrywania OID SNMP jest obsługiwana od wersji 6.4 serwera/proxy Zabbix.

Przykładowa konfiguracja

1. Utwórz pozycję agenta SNMP z kluczem takim jak:

```
walk[.1.3.6.1.4.1.9999.1.1.1.1]
```



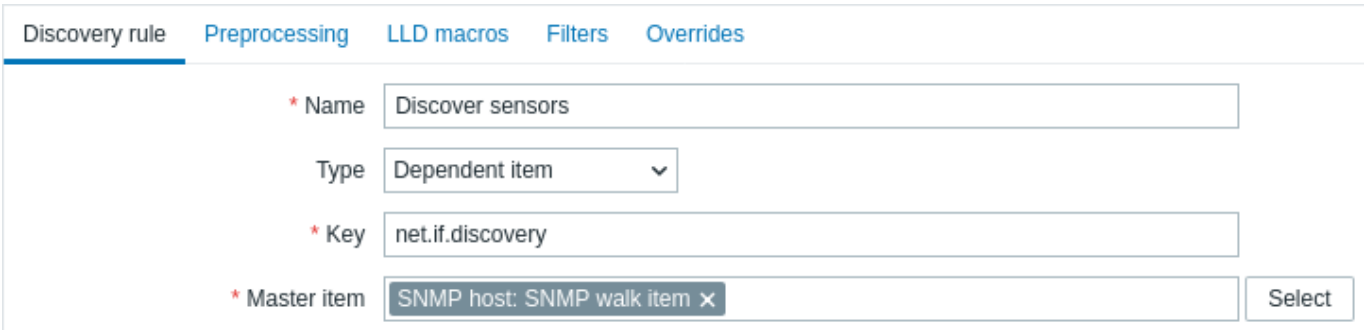
Ta pozycja wykonuje pojedyncze przejście po tabeli SNMP i zwraca wszystkie wpisy tabeli w jednym żądaniu, w formacie odpowiadającym danym wyjściowym narzędzia `snmpwalk` z opcjami formatowania `-Oe -Ot -On`.

Zwróci następującą wielowierszową wartość tekstową:

```
.1.3.6.1.4.1.9999.1.1.1.1.1.1 = STRING: "Temperature Sensor"
.1.3.6.1.4.1.9999.1.1.1.1.2.1 = STRING: "temp"
.1.3.6.1.4.1.9999.1.1.1.1.3.1 = 100
.1.3.6.1.4.1.9999.1.1.1.1.1.2 = STRING: "Humidity Sensor"
.1.3.6.1.4.1.9999.1.1.1.1.2.2 = STRING: "humidity"
.1.3.6.1.4.1.9999.1.1.1.1.3.2 = 200
```

2. Utwórz regułę wykrywania:

- W polu *Name* wprowadź opisową nazwę reguły wykrywania (np. „Wykryj czujniki”).
- W polu *Type* wybierz „Dependent item”.
- W polu *Key* wprowadź opisowy klucz (np. „net.if.discovery”).
- W polu *Master item* wybierz „SNMP walk item”.



3. Na karcie *Preprocessing* dodaj krok przetwarzania wstępnego z opcją „SNMP walk to JSON” wybraną na liście rozwijanej *Name* i z 3 parametrami:

- *Field name*: ”{#SENSORNAME}”; *OID prefix*: ”.1.3.6.1.4.1.9999.1.1.1.1.1”: *Format*: ”Unchanged”.
- *Field name*: ”{#SENSORTYPE}”; *OID prefix*: ”.1.3.6.1.4.1.9999.1.1.1.1.2”: *Format*: ”Unchanged”.
- *Field name*: ”{#SENSORVALUE}”; *OID prefix*: ”.1.3.6.1.4.1.9999.1.1.1.1.3”: *Format*: ”Unchanged”.

Po przetwarzaniu wstępnym reguła wykrywania zwraca tablicę JSON zestawów makr.

Na przykład:

```
[
    {
        "{#SNMPINDEX}": "1",
        "{#SENSORNAME}": "Temperature Sensor",
        "{#SENSORTYPE}": "temp",
        "{#SENSORVALUE}": "100"
    },
    {
        "{#SNMPINDEX}": "2",
        "{#SENSORNAME}": "Humidity Sensor",
        "{#SENSORTYPE}": "humidity",
        "{#SENSORVALUE}": "200"
    }
]
```

Każdy obiekt reprezentuje jeden wykryty czujnik i udostępnia makra takie jak {#SNMPINDEX}, {#SENSORNAME}, {#SENSORTYPE} oraz {#SENSORVALUE}.

Są one grupowane według indeksu SNMP, który jest numerycznym sufiksem na końcu każdego OID (np. .1, .2) — ten indeks jednoznacznie identyfikuje każdy wiersz w tabeli SNMP i jest automatycznie wyodrębniany jako {#SNMPINDEX}.

4. W ramach reguły wykrywania utwórz jeden lub więcej prototypów pozycji (z regułą wykrywania jako pozycją nadrzędną).

Na przykład zależna pozycja wartości czujnika:

- W polu *Name* wprowadź „Sensor {#SNMPINDEX}: {#SENSORNAME}”.
- W polu *Type* wybierz „Dependent item”.
- W polu *Key* wprowadź „sensor.value[{#SNMPINDEX}]”.
- W polu *Master item* wybierz „SNMP walk item”.



Na karcie *Preprocessing* dodaj krok przetwarzania wstępnego o nazwie „SNMP walk value” z OID ”.1.3.6.1.4.1.9999.1.1.1.1.3.{#SNMPINDEX}” w polu *Parameter*. *Format*: ”Unchanged”.

Zostaną wykryte następujące pozycje:

Name	Key	OID from which value is extracted	Item value
Sensor 1: Temperature Sensor	sensor.value[1]	.1.3.6.1.4.1.9999.1.1.1.1.3.1	100
Sensor 2: Humidity Sensor	sensor.value[2]	.1.3.6.1.4.1.9999.1.1.1.1.3.2	200

Po uruchomieniu reguły wykrywania zostaną utworzone pozycje takie jak `sensor.value[1]`, `sensor.value[2]`.

Każda pozycja zależna wyodrębnia swoją wartość z wyniku SNMP walk pozycji nadrzędnej przy użyciu przetwarzania wstępnego, bez wykonywania osobnych żądań SNMP.

5. Odwołuj się do prototypów pozycji zależnych w prototypach wyzwalaczy, używając tych samych makr z reguły wykrywania. Przykład:

```
{Template_Sensor:sensor.value[{#SNMPINDEX}].last()} > 75
```

Powoduje to utworzenie wyzwalacza dla każdego wykrytego czujnika (na przykład sensor.value[1], sensor.value[2]) i jego uruchomienie, jeśli najnowsza wartość (temperatury lub wilgotności) przekroczy 75.

6. Uwzględnij pozycje zależne dla każdej wykrytej jednostki. Przykładowy klucz elementu wykresu:

```
sensor.value[{#SNMPINDEX}]
```

Dla każdego {#SNMPINDEX} tworzony jest jeden wykres, przedstawiający temperaturę i wilgotność w czasie.

Ta konfiguracja wykonuje tylko jedno żądanie SNMP walk na cykl odpytywania, niezależnie od liczby wykrytych pozycji. Wszystkie pozycje zależne wyodrębniają swoje wartości z nadrzędnego wyniku SNMP walk przy użyciu przetwarzania wstępnego, co znacząco zmniejsza ruch SNMP i obciążenie.

Dynamiczne indeksy z walk[]

Dynamiczne indeksy (na przykład indeksy interfejsów) mogą się zmieniać po rekonfiguracji sprzętu. Aby uwzględnić takie zachowanie, tworzona jest nadrzędna reguła wykrywania SNMP walk z kluczem takim jak:

```
walk[1.3.6.1.2.1.2.2.1.10]
```

Po przetwarzaniu wstępnym SNMP walk do JSON wynik może wyglądać następująco:

```
[
    {
        "{#SNMPINDEX}": "2",
        "{#VALUE}": "123456"
    },
    {
        "{#SNMPINDEX}": "3",
        "{#VALUE}": "654321"
    }
]
```

Prototyp pozycji zależnej używa makra {#SNMPINDEX} do zbudowania klucza:

```
net.if.in[{#SNMPINDEX}]
```

Przetwarzanie wstępne dla tego prototypu obejmuje nazwę „SNMP walk value" z OID „1.3.6.1.2.1.2.2.1.10.{#SNMPINDEX}" w polu *Parameter*. *Format*: „Unchanged".

W czasie działania tworzone są rzeczywiste pozycje, takie jak `net.if.in[2]` i `net.if.in[3]`. Jeśli dany indeks interfejsu ulegnie zmianie (na przykład jeśli indeks 2 zostanie zastąpiony przez 5 w tabeli SNMP), to przy następnym uruchomieniu reguły wykrywania:

- Stara zależna pozycja net.if.in[2] zostanie oznaczona jako „lost" lub usunięta i nie będą już zbierane dla niej nowe dane.
- Zostanie utworzona nowa zależna pozycja net.if.in[5], rozpoczynająca z pustą historią.
- Dane historyczne z net.if.in[2] nie są automatycznie przenoszone do net.if.in[5].

Przykład prototypu wyzwalacza:

```
{Template_Interface:net.if.in[{#SNMPINDEX}].last()} > 1000000000
```

Przykład prototypu wykresu obejmuje pozycje:

```
net.if.in[{#SNMPINDEX}]
net.if.out[{#SNMPINDEX}]
```

Ta konfiguracja zapewnia niezawodne monitorowanie tabel z dynamicznymi indeksami przy jednoczesnym zminimalizowaniu ruchu SNMP — wymagany jest tylko jeden SNMP walk na cykl odpytywania, a prototypy pozycji zależnych wyodrębniają potrzebne wartości.

Wykryte encje

Gdy serwer jest uruchomiony, utworzy rzeczywiste zależne pozycje, wyzwalacze i wykresy na podstawie wartości zwracanych przez regułę wykrywania SNMP.

5 Odkrywanie OID-ów SNMP (starsza wersja)

Przegląd

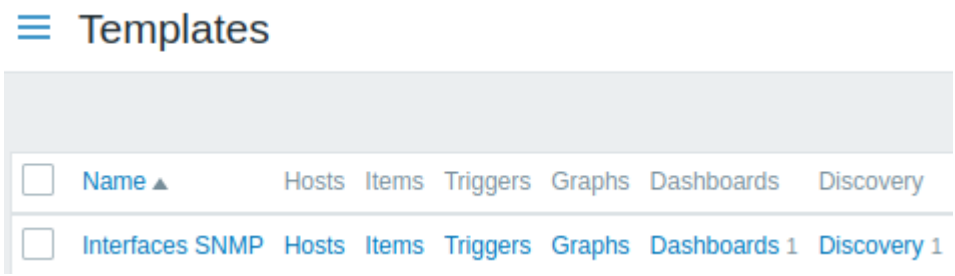
W tej sekcji przeprowadzimy wykrywanie SNMP na przełączniku.

Klucz pozycji

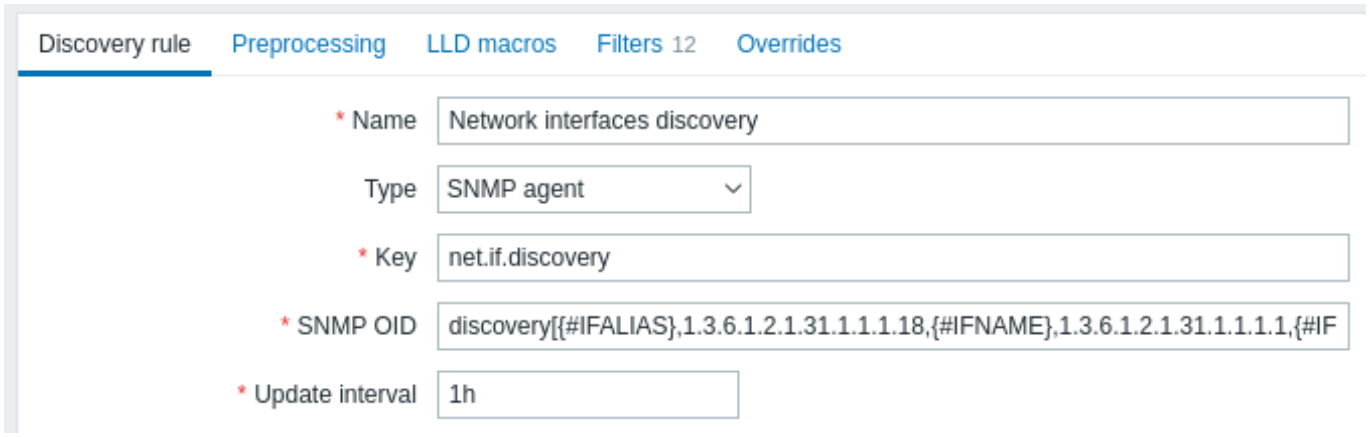
W przeciwieństwie do wykrywania systemów plików i interfejsów sieciowych, pozycja niekoniecznie musi mieć klucz "snmp.discovery" — wystarczy typ pozycji SNMP agent.

Aby skonfigurować regułę wykrywania, wykonaj następujące kroki:

- Przejdź do: *Data collection* → *Templates*
- Kliknij *Discovery* w wierszu odpowiedniego szablonu



- Kliknij *Create discovery rule* w prawym górnym rogu ekranu
- Wypełnij formularz reguły wykrywania wymaganymi danymi, jak pokazano na zrzucie ekranu poniżej



Wszystkie obowiązkowe pola wejściowe są oznaczone czerwoną gwiazdką.

OID-y do wykrycia są definiowane w polu SNMP OID w następującym formacie: `discovery[{#MACRO1}, oid1, {#MACRO2}, oid2, …,]`

gdzie *{#MACRO1}*, *{#MACRO2}* ... są prawidłowymi nazwami makr lld, a *oid1*, *oid2*... są OID-ami zdolnymi do generowania znaczących wartości dla tych makr. Wbudowane makro *{#SNMPINDEX}*, zawierające indeks wykrytego OID, jest stosowane do wykrytych encji. Wykryte encje są grupowane według wartości makra *{#SNMPINDEX}*.

Oto przykład, w którym na przełączniku wykonywanych jest kilka poleceń snmpwalk:

```
$ snmpwalk -v 2c -c public 192.168.1.1 IF-MIB::ifDescr
IF-MIB::ifDescr.1 = STRING: WAN
IF-MIB::ifDescr.2 = STRING: LAN1
IF-MIB::ifDescr.3 = STRING: LAN2

$ snmpwalk -v 2c -c public 192.168.1.1 IF-MIB::ifPhysAddress
IF-MIB::ifPhysAddress.1 = STRING: 8:0:27:90:7a:75
IF-MIB::ifPhysAddress.2 = STRING: 8:0:27:90:7a:76
IF-MIB::ifPhysAddress.3 = STRING: 8:0:27:2b:af:9e
```

A SNMP OID jest ustawiony na: `discovery[{#IFDESCR}, ifDescr, {#IFPHYSADDRESS}, ifPhysAddress]`

Teraz ta reguła wykryje encje z makrami {#IFDESCR} ustawionymi na **WAN**, **LAN1** i **LAN2**, makrami {#IFPHYSADDRESS} ustawionymi na **8:0:27:90:7a:75**, **8:0:27:90:7a:76** oraz **8:0:27:2b:af:9e**, a makrami {#SNMPINDEX} ustawionymi na indeksy wykrytych OID-ów **1**, **2** i **3**:

```
[
    {
        "{#SNMPINDEX}": "1",
        "{#IFDESCR}": "WAN",
        "{#IFPHYSADDRESS}": "8:0:27:90:7a:75"
```

```
    },
    {
        "{#SNMPINDEX}": "2",
        "{#IFDESCR}": "LAN1",
        "{#IFPHYSADDRESS}": "8:0:27:90:7a:76"
    },
    {
        "{#SNMPINDEX}": "3",
        "{#IFDESCR}": "LAN2",
        "{#IFPHYSADDRESS}": "8:0:27:2b:af:9e"
    }
]
```

Jeśli encja nie ma określonego OID, odpowiednie makro zostanie pominięte dla tej encji. Na przykład, jeśli mamy następujące dane:

```
ifDescr.1 "Interface #1"
ifDescr.2 "Interface #2"
ifDescr.4 "Interface #4"

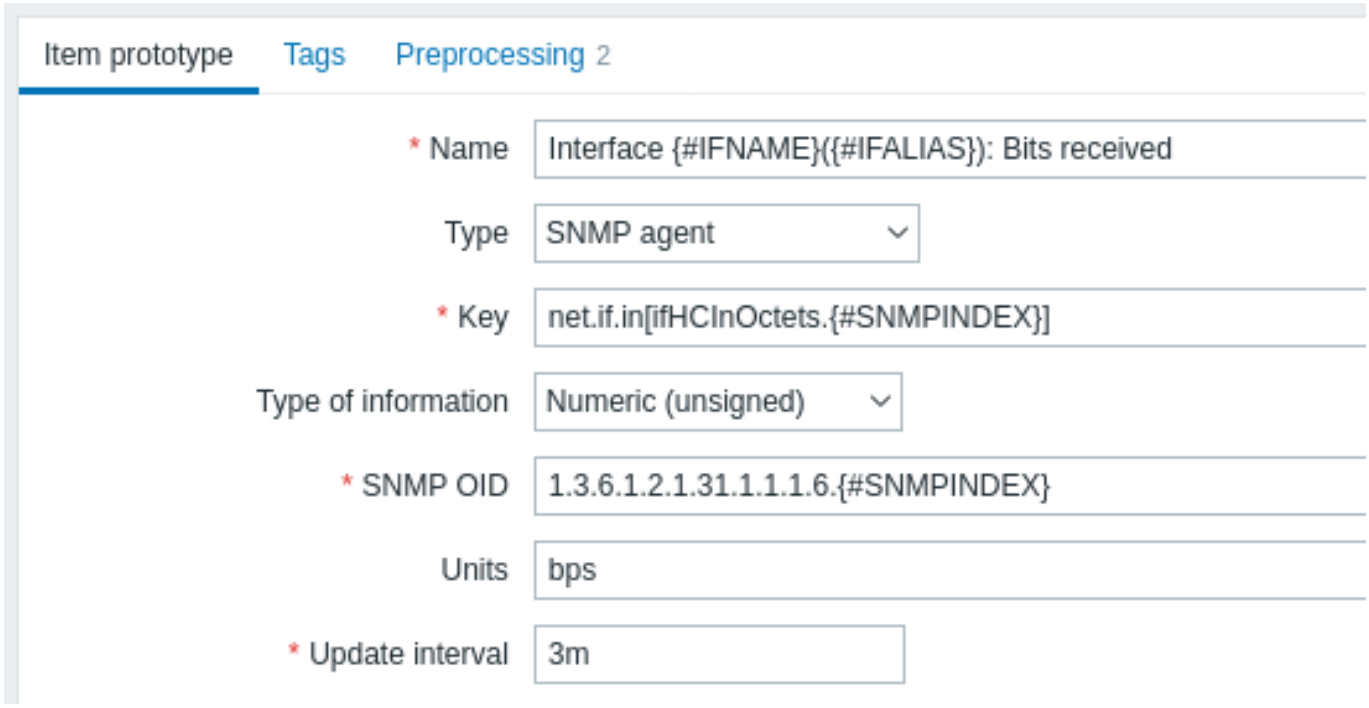
ifAlias.1 "eth0"
ifAlias.2 "eth1"
ifAlias.3 "eth2"
ifAlias.5 "eth4"
```

W takim przypadku wykrywanie SNMP `discovery[{#IFDESCR}, ifDescr, {#IFALIAS}, ifAlias]` zwróci następującą strukturę:

```
[
    {
        "{#SNMPINDEX}": 1,
        "{#IFDESCR}": "Interface #1",
        "{#IFALIAS}": "eth0"
    },
    {
        "{#SNMPINDEX}": 2,
        "{#IFDESCR}": "Interface #2",
        "{#IFALIAS}": "eth1"
    },
    {
        "{#SNMPINDEX}": 3,
        "{#IFALIAS}": "eth2"
    },
    {
        "{#SNMPINDEX}": 4,
        "{#IFDESCR}": "Interface #4"
    },
    {
        "{#SNMPINDEX}": 5,
        "{#IFALIAS}": "eth4"
    }
]
```

Prototypy pozycji

Poniższy zrzut ekranu pokazuje, jak można używać tych makr w prototypach pozycji:



Możesz utworzyć tyle prototypów pozycji, ile potrzeba:

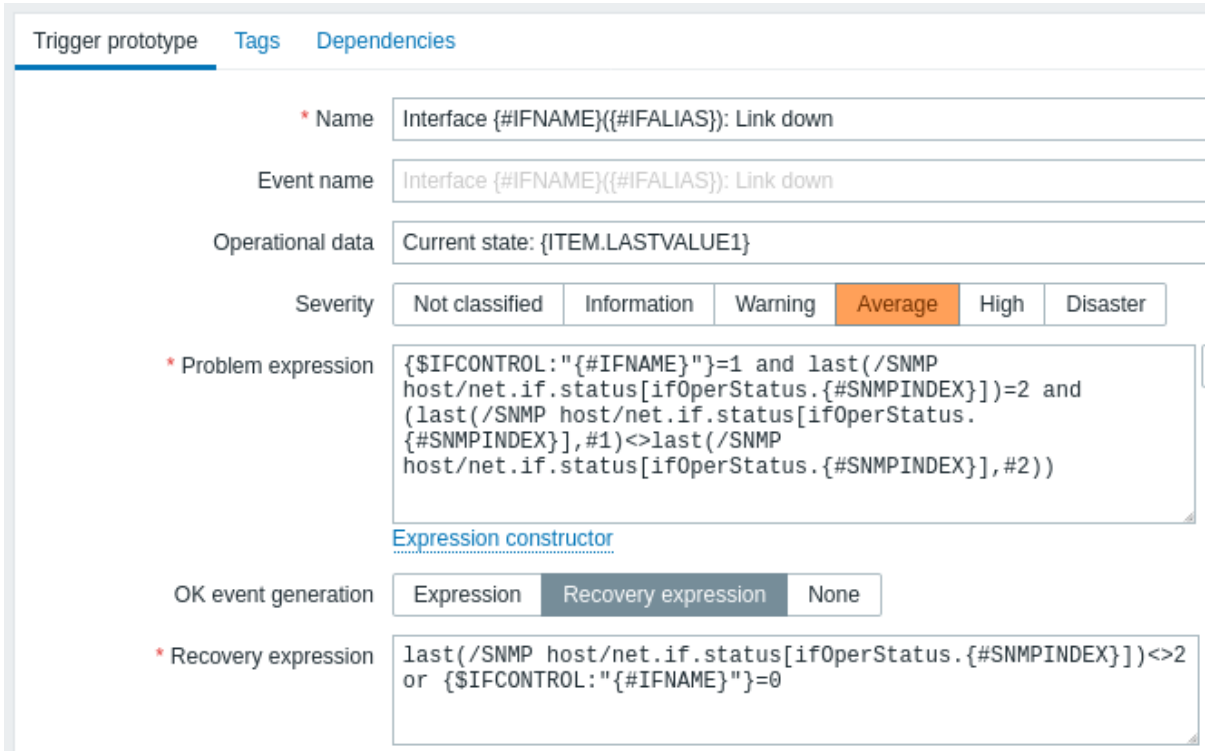
Item prototypes

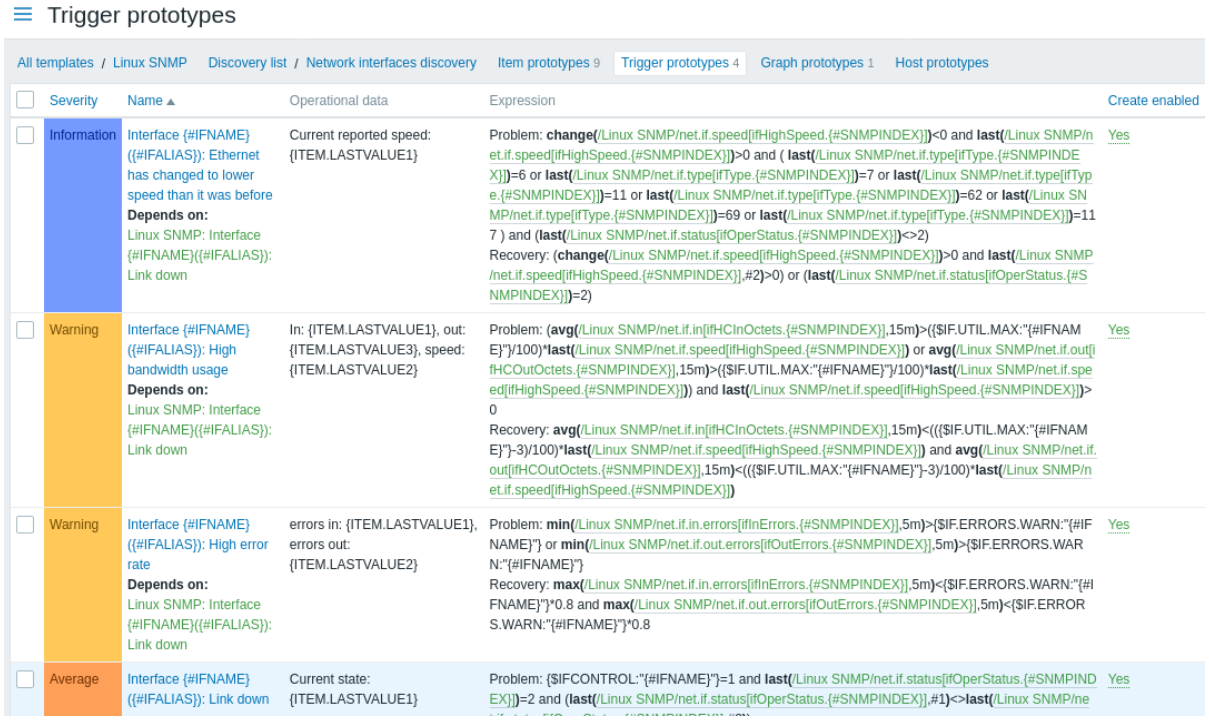
All templates / Linux SNMP Discovery list / Network interfaces discovery Item prototypes 9 Trigger prototypes 4 Graph prototypes 1 Host prototypes

Name ▲	Key	Interval	History	Trends	Type	Create enabled
Interface {#IFNAME}({#IFALIAS}): Bits received	net.if.in[ifHCInOctets.{#SNMPINDEX}]	3m	7d	365d	SNMP agent	Yes
Interface {#IFNAME}({#IFALIAS}): Bits sent	net.if.out[ifHCOutOctets.{#SNMPINDEX}]	3m	7d	365d	SNMP agent	Yes
Interface {#IFNAME}({#IFALIAS}): Inbound packets discarded	net.if.in.discards[ifInDiscards.{#SNMPINDEX}]	3m	7d	365d	SNMP agent	Yes
Interface {#IFNAME}({#IFALIAS}): Inbound packets with errors	net.if.in.errors[ifInErrors.{#SNMPINDEX}]	3m	7d	365d	SNMP agent	Yes
Interface {#IFNAME}({#IFALIAS}): Interface type	net.if.type[ifType.{#SNMPINDEX}]	1h	7d	0d	SNMP agent	Yes
Interface {#IFNAME}({#IFALIAS}): Operational status	net.if.status[ifOperStatus.{#SNMPINDEX}]	1m	7d	0	SNMP agent	Yes
Interface {#IFNAME}({#IFALIAS}): Outbound packets discarded	net.if.out.discards[ifOutDiscards.{#SNMPINDEX}]	3m	7d	365d	SNMP agent	Yes
Interface {#IFNAME}({#IFALIAS}): Outbound packets with errors	net.if.out.errors[ifOutErrors.{#SNMPINDEX}]	3m	7d	365d	SNMP agent	Yes
Interface {#IFNAME}({#IFALIAS}): Speed	net.if.speed[ifHighSpeed.{#SNMPINDEX}]	5m	7d	0d	SNMP agent	Yes

Prototypy wyzwalaczy

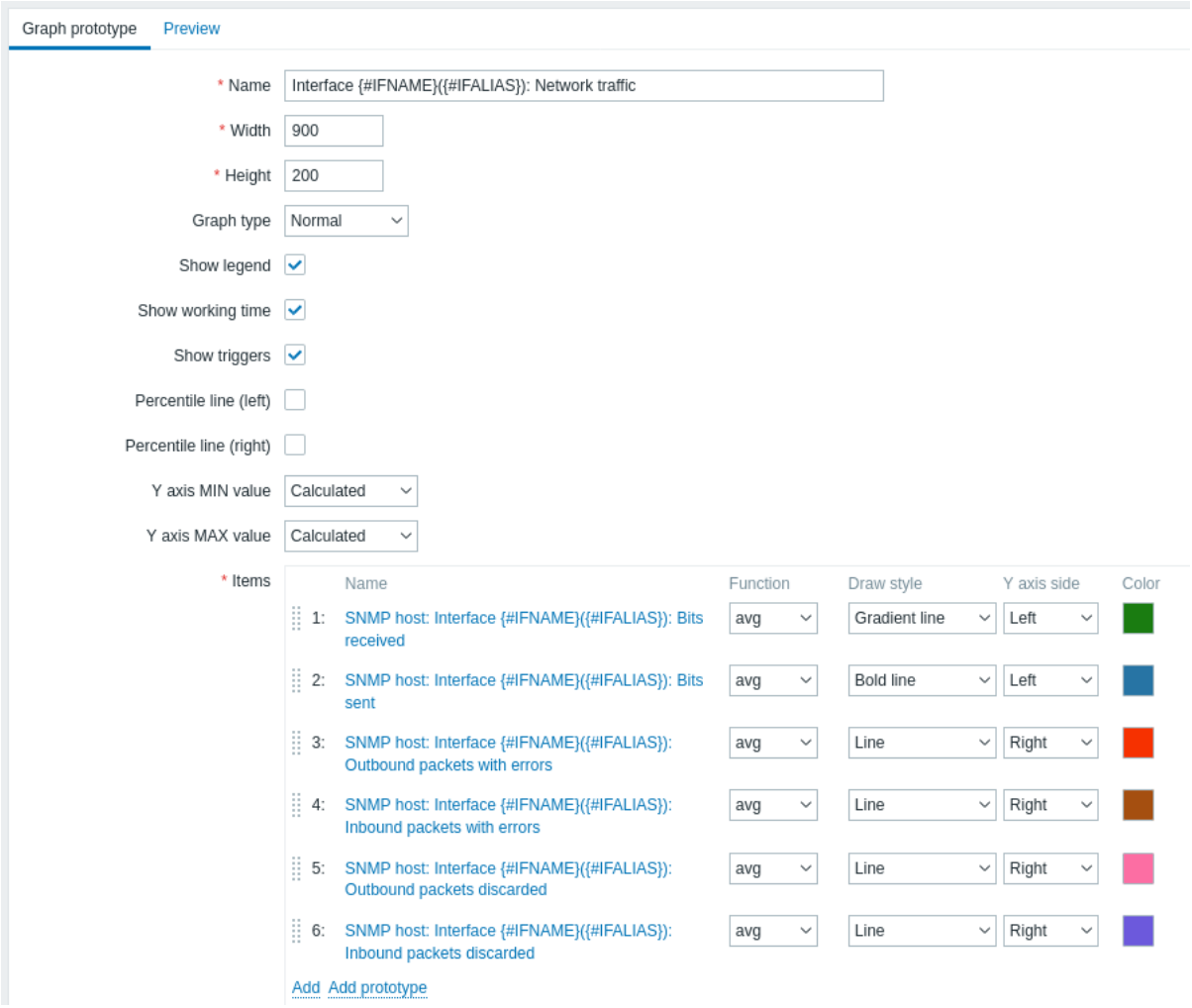
Poniższy zrzut ekranu ilustruje, jak możemy używać tych makr w prototypach wyzwalaczy:

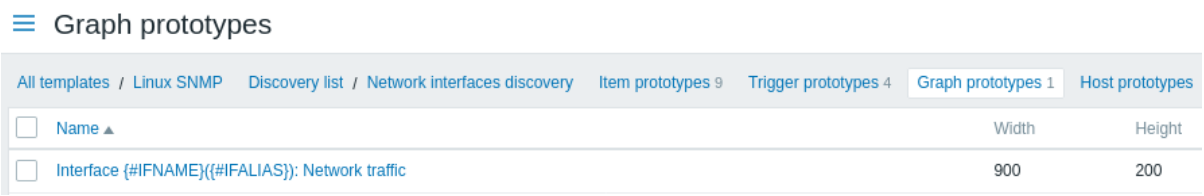




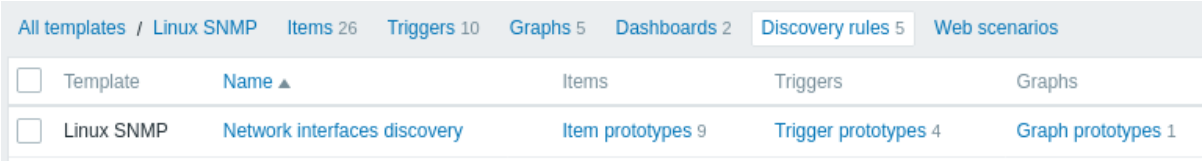
Prototypy wykresów

Poniższy zrzut ekranu pokazuje, jak możemy używać tych makr w prototypach wykresów:





Podsumowanie naszej reguły wykrywania:



Wykryte encje

Gdy serwer jest uruchomiony, utworzy rzeczywiste pozycje, wyzwalacze i wykresy na podstawie wartości zwracanych przez regułę wykrywania SNMP. W konfiguracji hosta są one poprzedzone pomarańczowym odnośnikiem do reguły wykrywania, z której pochodzą.

Items

All hosts / SNMP host Enabled SNMP Items 81 Triggers 23 Graphs 14 Discovery rules 6 Web scenarios

Name ▲	Triggers	Key	Interval	History	Trends	Type	Status
Network interfaces discovery: Interface enp4s0(): Bits received	Triggers 1	net.if.in[ifHCInOctets.2]	3m	7d	365d	SNMP agent	Enabled
Network interfaces discovery: Interface enp4s0(): Bits sent	Triggers 1	net.if.out[ifHCOutOctets.2]	3m	7d	365d	SNMP agent	Enabled
Network interfaces discovery: Interface enp4s0(): Inbound packets discarded		net.if.in.discards[ifInDiscards.2]	3m	7d	365d	SNMP agent	Enabled
Network interfaces discovery: Interface enp4s0(): Inbound packets with errors	Triggers 1	net.if.in.errors[ifInErrors.2]	3m	7d	365d	SNMP agent	Enabled
Network interfaces discovery: Interface enp4s0(): Interface type	Triggers 1	net.if.type[ifType.2]	1h	7d	0d	SNMP agent	Enabled
Network interfaces discovery: Interface enp4s0(): Operational status	Triggers 2	net.if.status[ifOperStatus.2]	1m	7d	0	SNMP agent	Enabled
Network interfaces discovery: Interface enp4s0(): Outbound packets discarded		net.if.out.discards[ifOutDiscards.2]	3m	7d	365d	SNMP agent	Enabled
Network interfaces discovery: Interface enp4s0(): Outbound packets with errors	Triggers 1	net.if.out.errors[ifOutErrors.2]	3m	7d	365d	SNMP agent	Enabled
Network interfaces discovery: Interface enp4s0(): Speed	Triggers 2	net.if.speed[ifHighSpeed.2]	5m	7d	0d	SNMP agent	Enabled

Triggers

All hosts / SNMP host Enabled SNMP Items 81 Triggers 23 Graphs 14 Discovery rules 6 Web scenarios

Severity	Value	Name ▲	Operational data	Expression
Information	OK	Network interfaces discovery: Interface enp4s0(): Ethernet has changed to lower speed than it was before **Depends on:** SNMP host: Interface enp4s0(): Link down	Current reported speed: {ITEM.LASTVALUE1}	Problem: **change(**/SNMP host/net.if.speed[ifHighSpeed.2]**)**<0 and **last(**/SNMP host/net.if.speed[ifHighSpeed.2]**)**>0 and (**last(**/SNMP host/net.if.type[ifType.2]**)**=6 or **last(**/SNMP host/net.if.type[ifType.2]**)**=7 or **last(**/SNMP host/net.if.type[ifType.2]**)**=11 or **last(**/SNMP host/net.if.type[ifType.2]**)**=62 or **last(**/SNMP host/net.if.type[ifType.2]**)**=69 or **last(**/SNMP host/net.if.type[ifType.2]**)**=117) and (**last(**/SNMP host/net.if.status[ifOperStatus.2]**)**<>2) Recovery: (**change(**/SNMP host/net.if.speed[ifHighSpeed.2]**)**>0 and **last(**/SNMP host/net.if.speed[ifHighSpeed.2],#2**)**>0) or (**last(**/SNMP host/net.if.status[ifOperStatus.2]**)**=2)
Warning	OK	Network interfaces discovery: Interface enp4s0(): High bandwidth usage **Depends on:** SNMP host: Interface enp4s0(): Link down	In: {ITEM.LASTVALUE1}, out: {ITEM.LASTVALUE3}, speed: {ITEM.LASTVALUE2}	Problem: (**avg(**/SNMP host/net.if.in[ifHCInOctets.2],15m**)**>({$IF.UTIL.MAX:"enp4s0"}/100)***last(**/SNMP host/net.if.speed[ifHighSpeed.2]**)**) or **avg(**/SNMP host/net.if.out[ifHCOutOctets.2],15m**)**>({$IF.UTIL.MAX:"enp4s0"}/100)***last(**/SNMP host/net.if.speed[ifHighSpeed.2]**)**) and **last(**/SNMP host/net.if.speed[ifHighSpeed.2]**)**>0 Recovery: **avg(**/SNMP host/net.if.in[ifHCInOctets.2],15m**)**<(({$IF.UTIL.MAX:"enp4s0"}-3)/100)***last(**/SNMP host/net.if.speed[ifHighSpeed.2]**)** and **avg(**/SNMP host/net.if.out[ifHCOutOctets.2],15m**)**<(({$IF.UTIL.MAX:"enp4s0"}-3)/100)***last(**/SNMP host/net.if.speed[ifHighSpeed.2]**)**
Warning	OK	Network interfaces discovery: Interface enp4s0(): High error rate **Depends on:** SNMP host: Interface enp4s0(): Link down	errors in: {ITEM.LASTVALUE1}, errors out: {ITEM.LASTVALUE2}	Problem: **min(**/SNMP host/net.if.in.errors[ifInErrors.2],5m**)**>{$IF.ERRORS.WARN:"enp4s0"} or **min(**/SNMP host/net.if.out.errors[ifOutErrors.2],5m**)**>{$IF.ERRORS.WARN:"enp4s0"} Recovery: **max(**/SNMP host/net.if.in.errors[ifInErrors.2],5m**)**<{$IF.ERRORS.WARN:"enp4s0"}*0.8 and **max(**/SNMP host/net.if.out.errors[ifOutErrors.2],5m**)**<{$IF.ERRORS.WARN:"enp4s0"}*0.8
Average	OK	Network interfaces discovery: Interface enp4s0(): Link down	Current state: {ITEM.LASTVALUE1}	Problem: {$IFCONTROL:"enp4s0"}=1 and **last(**/SNMP host/net.if.status[ifOperStatus.2]**)**=2 and (**last(**/SNMP host/net.if.status[ifOperStatus.2],#1**)**<>**last(**/SNMP host/net.if.status[ifOperStatus.2],#2**)**) Recovery: **last(**/SNMP host/net.if.status[ifOperStatus.2]**)**<>2 or {$IFCONTROL:"enp4s0"}=0

Graphs

All hosts / SNMP host Enabled SNMP Items 81 Triggers 23 Graphs 14 Discovery rules 6 Web scenarios

Name ▲
Mounted filesystem discovery: /: Disk space usage
Linux SNMP: CPU jumps
CPU discovery: CPU usage
CPU discovery: CPU utilization
Network interfaces discovery: Interface enp4s0(): Network traffic

6 Wykrywanie obiektów JMX

Przegląd

Możliwe jest wykrywanie wszystkich JMX MBeanów lub atrybutów MBeanów albo określenie wzorca do wykrywania tych obiektów.

Dla konfiguracji reguły wykrywania konieczne jest zrozumienie różnicy między MBeanem a atrybutami MBeana. MBean jest obiektem, który może reprezentować urządzenie, aplikację lub dowolny zasób, który wymaga zarządzania.

Na przykład istnieje MBean reprezentujący serwer WWW. Jego atrybutami są liczba połączeń, liczba wątków, limit czasu żądania, pamięć podręczna plików HTTP, użycie pamięci itp. Wyrażając tę myśl w języku bardziej zrozumiałym dla człowieka, możemy zdefiniować ekspres do kawy jako MBean, który ma następujące atrybuty do monitorowania: ilość wody na filiżankę, średnie zużycie wody w określonym czasie, liczba ziaren kawy wymagana na filiżankę, czas uzupełniania ziaren kawy i wody itp.

Klucz pozycji

W konfiguracji reguły wykrywania wybierz **JMX agent** w polu *Typ*.

Obsługiwane są dwa klucze pozycji do wykrywania obiektów JMX - jmx.discovery[] oraz jmx.get[]:

Klucz pozycji	Wartość zwracana	Parametry	Komentarz
jmx.discovery[<tryb wykrywania>,<nazwa obiektu>,<unikalny krótki opis>]	Ta pozycja zwraca tablicę JSON z makrami LLD opisującymi obiekty MBean lub ich atrybuty.	**tryb wykrywania** - jedna z następujących wartości: *attributes* (pobiera atrybuty JMX MBean, domyślnie) lub *beans* (pobiera JMX MBeans) **nazwa obiektu** - wzorzec nazwy obiektu (zobacz documentation) identyfikujący nazwy MBean do pobrania (domyślnie puste, co powoduje pobranie wszystkich zarejestrowanych beanów) **unikalny krótki opis** - unikalny opis umożliwiający użycie wielu pozycji JMX z tym samym trybem wykrywania i nazwą obiektu na hoście (opcjonalnie)	Przykłady: → jmx.discovery - pobierz wszystkie atrybuty JMX MBean → jmx.discovery[beans] - pobierz wszystkie JMX MBeans → jmx.discovery[attributes,"*:type=GarbageCollector,name - pobierz wszystkie atrybuty garbage collectora → jmx.discovery[beans,"*:type=GarbageCollector,name=* - pobierz wszystkie garbage collectory Istnieją pewne ograniczenia dotyczące tego, jakie właściwości MBean ta pozycja może zwracać, ze względu na ograniczony zestaw znaków obsługiwanych przy generowaniu nazw makr (obsługiwane znaki można opisać za pomocą następującego wyrażenia regularnego: `A-Z0-9_\.`). Dlatego na przykład, aby wykrywać właściwości MBean zawierające słowo z łącznikiem lub znaki spoza ASCII, należy użyć `jmx.get[]`.
jmx.get[<tryb wykrywania>,<nazwa obiektu>,<unikalny krótki opis>]			

Klucz pozycji			
	Ta pozycja zwraca tablicę JSON z obiektami MBean lub ich atrybutami. W porównaniu do `jmx.discovery[]` nie definiuje makr LLD.	**tryb wykrywania** - jedna z następujących wartości: *attributes* (pobiera atrybuty JMX MBean, domyślnie) lub *beans* (pobiera JMX MBeans) **nazwa obiektu** - wzorzec nazwy obiektu (zobacz documentation) identyfikujący nazwy MBean do pobrania (domyślnie puste, co powoduje pobranie wszystkich zarejestrowanych beanów) **unikalny krótki opis** - unikalny opis umożliwiający użycie wielu pozycji JMX z tym samym trybem wykrywania i nazwą obiektu na hoście (opcjonalnie)	W przypadku użycia tej pozycji należy zdefiniować niestandardowe makra wykrywania niskiego poziomu, wskazujące wartości wyodrębnione ze zwróconego JSON przy użyciu JSONPath.

Attention:
Jeśli nie zostaną przekazane żadne parametry, żądane są wszystkie atrybuty MBean z JMX. Niepodanie parametrów dla wykrywania JMX lub próba pobrania wszystkich atrybutów dla szerokiego zakresu, takiego jak `*:type=*,name=*`, może prowadzić do potencjalnych problemów z wydajnością.

Użycie jmx.discovery

Ta pozycja zwraca obiekt JSON z makrami wykrywania niskiego poziomu opisującymi obiekty MBean lub atrybuty. Na przykład przy wykrywaniu atrybutów MBean (przeformatowano dla przejrzystości):

```
[
    {
        "{#JMXVALUE}":"0",
        "{#JMXTYPE}":"java.lang.Long",
        "{#JMXOBJ}":"java.lang:type=GarbageCollector,name=PS Scavenge",
        "{#JMXDESC}":"java.lang:type=GarbageCollector,name=PS Scavenge,CollectionCount",
        "{#JMXATTR}":"CollectionCount"
    },
    {
        "{#JMXVALUE}":"0",
        "{#JMXTYPE}":"java.lang.Long",
        "{#JMXOBJ}":"java.lang:type=GarbageCollector,name=PS Scavenge",
        "{#JMXDESC}":"java.lang:type=GarbageCollector,name=PS Scavenge,CollectionTime",
        "{#JMXATTR}":"CollectionTime"
    },
    {
        "{#JMXVALUE}":"true",
        "{#JMXTYPE}":"java.lang.Boolean",
        "{#JMXOBJ}":"java.lang:type=GarbageCollector,name=PS Scavenge",
        "{#JMXDESC}":"java.lang:type=GarbageCollector,name=PS Scavenge,Valid",
        "{#JMXATTR}":"Valid"
    },
    {
        "{#JMXVALUE}":"PS Scavenge",
        "{#JMXTYPE}":"java.lang.String",
        "{#JMXOBJ}":"java.lang:type=GarbageCollector,name=PS Scavenge",
        "{#JMXDESC}":"java.lang:type=GarbageCollector,name=PS Scavenge,Name",
        "{#JMXATTR}":"Name"
    },
    {
        "{#JMXVALUE}":"java.lang:type=GarbageCollector,name=PS Scavenge",
        "{#JMXTYPE}":"javax.management.ObjectName",
```

```
        "{#JMXOBJ}":"java.lang:type=GarbageCollector,name=PS Scavenge",
        "{#JMXDESC}":"java.lang:type=GarbageCollector,name=PS Scavenge,ObjectName",
        "{#JMXATTR}":"ObjectName"
    }
]
```

Przy wykrywaniu MBeanów (przeformatowano dla przejrzystości):

```
[
    {
        "{#JMXDOMAIN}":"java.lang",
        "{#JMXTYPE}":"GarbageCollector",
        "{#JMXOBJ}":"java.lang:type=GarbageCollector,name=PS Scavenge",
        "{#JMXNAME}":"PS Scavenge"
    }
]
```

Obsługiwane makra

Następujące makra są obsługiwane do użycia w filtrze reguły wykrywania oraz w prototypach pozycji, wyzwalaczy i wykresów:

Makro	Opis
Wykrywanie atrybutów MBean	
{#JMXVALUE}	Wartość atrybutu.
{#JMXTYPE}	Typ atrybutu.
{#JMXOBJ}	Nazwa obiektu.
{#JMXDESC}	Nazwa obiektu wraz z nazwą atrybutu.
{#JMXATTR}	Nazwa atrybutu.
Wykrywanie MBeanów	
{#JMXDOMAIN}	Domena MBean. (*Nazwa zastrzeżona przez Zabbix*)
{#JMXOBJ}	Nazwa obiektu. (*Nazwa zastrzeżona przez Zabbix*)
{#JMX<key property>}	Właściwości MBean (takie jak {#JMXTYPE}, {#JMXNAME}) (zobacz Ograniczenia poniżej).

Ograniczenia

Istnieją pewne ograniczenia związane z algorytmem tworzenia nazw makr LLD z nazw właściwości MBean:

- nazwy atrybutów są zmieniane na wielkie litery
- nazwy atrybutów są ignorowane (nie są generowane żadne makra LLD), jeśli składają się z znaków nieobsługiwanych w nazwach makr LLD. Obsługiwane znaki można opisać za pomocą następującego wyrażenia regularnego: `A-Z0-9_\.`
- jeśli atrybut ma nazwę ”obj” lub ”domain”, zostanie zignorowany z powodu nakładania się z wartościami zastrzeżonych właściwości Zabbix {#JMXOBJ} i {#JMXDOMAIN}

Proszę rozważyć ten przykład jmx.discovery (w trybie ”beans”). MBean ma zdefiniowane następujące właściwości (niektóre z nich zostaną zignorowane; patrz niżej):

```
name=test
  =Type
attributes []=1,2,3
Name=NameOfTheTest
domAin=some
```

W wyniku wykrywania JMX zostaną wygenerowane następujące makra LLD:

- {#JMXDOMAIN} - wewnętrzne Zabbix, opisujące domenę MBean
- {#JMXOBJ} - wewnętrzne Zabbix, opisujące obiekt MBean
- {#JMXNAME} - utworzone z właściwości ”name”

Ignorowane właściwości to:

- тип : jego nazwa zawiera nieobsługiwane znaki (spoza ASCII)
- attributes[] : jego nazwa zawiera nieobsługiwane znaki (nawiasy kwadratowe nie są obsługiwane)
- Name : jest już zdefiniowana (name=test)
- domAin : jest to nazwa zastrzeżona przez Zabbix

Przykłady

Przyjrzyjmy się jeszcze dwóm praktycznym przykładom tworzenia reguły LLD z wykorzystaniem MBean. Aby lepiej zrozumieć różnicę między regułą LLD zbierającą MBeans a regułą LLD zbierającą atrybuty MBean, prosimy spojrzeć na poniższą tabelę:

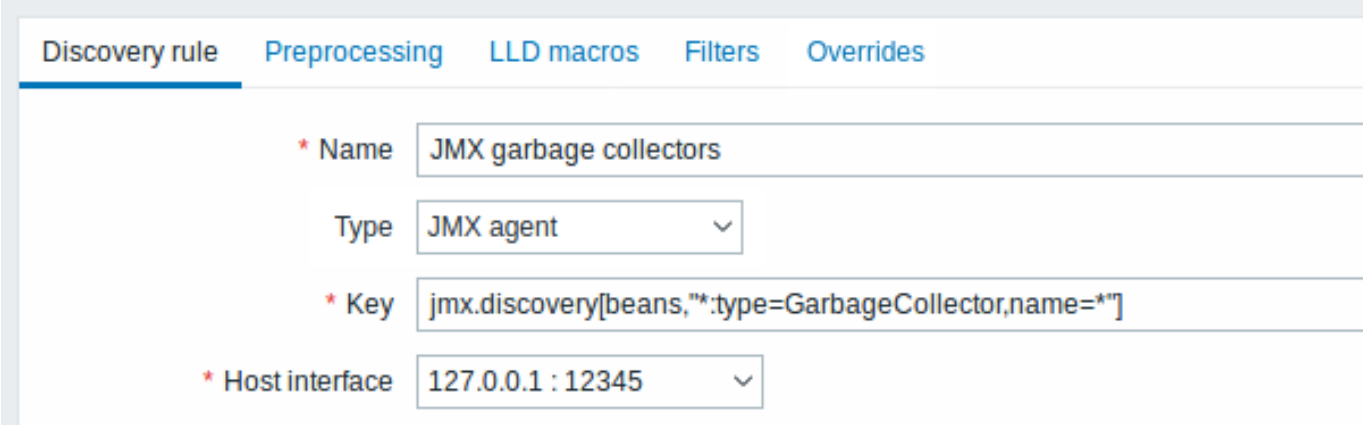
MBean1	**MBean2**	**MBean3**
MBean1Attribute1	MBean2Attribute1	MBean3Attribute1
MBean1Attribute2	MBean2Attribute2	MBean3Attribute2
MBean1Attribute3	MBean2Attribute3	MBean3Attribute3

Przykład 1: Odkrywanie MBeanów

Ta reguła zwróci 3 obiekty: górny wiersz kolumny: MBean1, MBean2, MBean3.

Więcej informacji o obiektach można znaleźć w tabeli obsługiwanych makr, w sekcji *Odkrywanie MBeanów*.

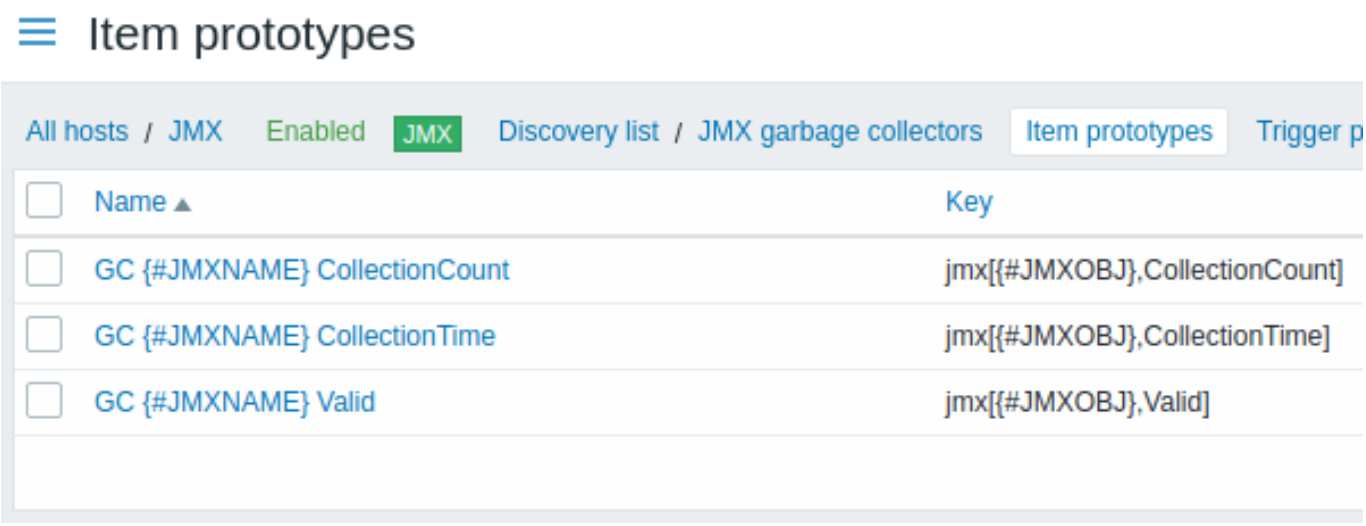
Konfiguracja reguły odkrywania zbierającej MBeany (bez atrybutów) wygląda następująco:



Użyty tutaj klucz:

```
jmx.discovery[beans,"*:type=GarbageCollector,name=*"]
```

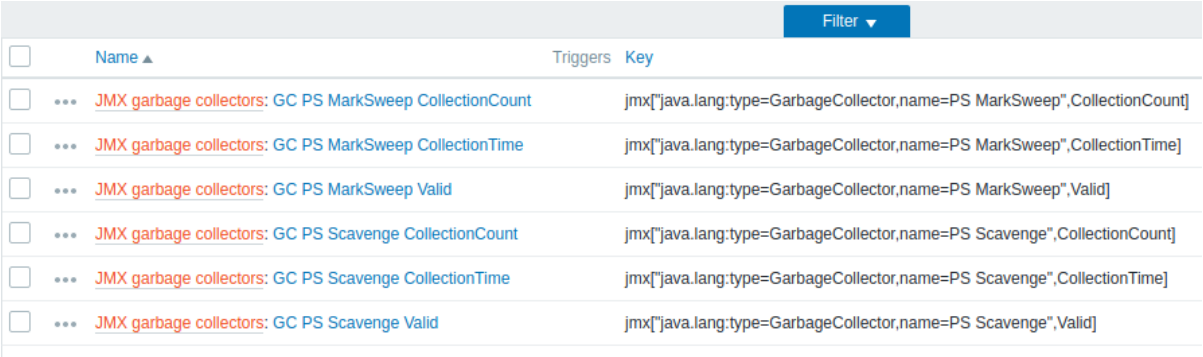
Zostaną odkryte wszystkie garbage collectory bez atrybutów. Ponieważ garbage collectory mają ten sam zestaw atrybutów, możemy użyć żądanych atrybutów w prototypach pozycji w następujący sposób:



Użyte tutaj klucze:

```
jmx[{#JMXOBJ},CollectionCount]
jmx[{#JMXOBJ},CollectionTime]
jmx[{#JMXOBJ},Valid]
```

Reguła odkrywania LLD da wynik zbliżony do poniższego (pozycje są odkrywane dla dwóch garbage collectorów):

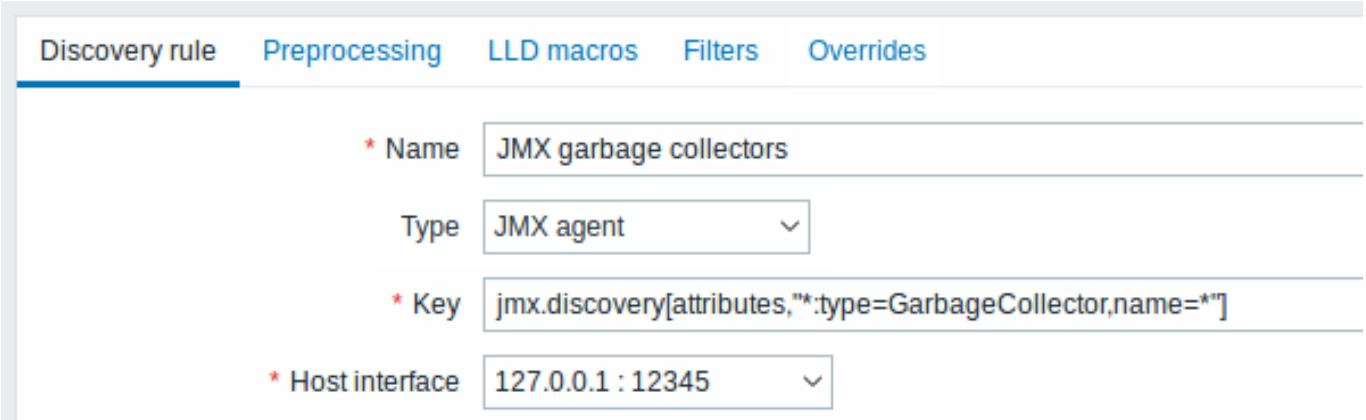


Przykład 2: Odkrywanie atrybutów MBean

Ta reguła zwróci 9 obiektów z następującymi polami: MBean1Attribute1, MBean2Attribute1, MBean3Attribute1,MBean1Attribute2,MBean2Attri MBean3Attribute2, MBean1Attribute3, MBean2Attribute3, MBean3Attribute3.

Aby uzyskać więcej informacji o obiektach, zobacz tabelę supported macros, sekcja *Discovery of MBean attributes*.

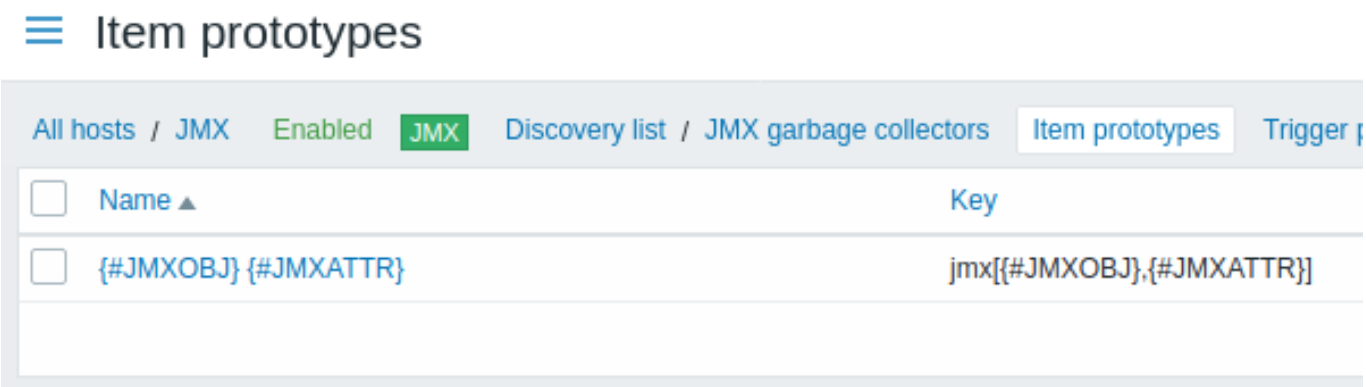
Konfiguracja reguły wykrywania zbierającej atrybuty MBean wygląda następująco:



Użyty tutaj klucz:

```
jmx.discovery[attributes,"*:type=GarbageCollector,name=*"]
```

Wszyscy garbage collectory z atrybutem pojedynczej pozycji zostaną wykryci.



W tym konkretnym przypadku dla każdego atrybutu MBean zostanie utworzona pozycja z prototypu. Główną wadą tej konfiguracji jest to, że tworzenie wyzwalaczy z prototypów wyzwalaczy jest niemożliwe, ponieważ istnieje tylko jeden prototyp pozycji dla wszystkich atrybutów. Dlatego ta konfiguracja może być używana do zbierania danych, ale nie jest zalecana do automatycznego monitorowania.

Używanie jmx.get

`jmx.get[]` jest podobna do pozycji `jmx.discovery[]`, ale nie zamienia właściwości obiektów Java na nazwy makr wykrywania niskiego poziomu i dlatego może zwracać wartości bez ograniczeń, które są związane z generowaniem nazw makr LLD, takich jak myślniki lub znaki spoza ASCII.

Podczas używania `jmx.get[]` do wykrywania makra wykrywania niskiego poziomu mogą być zdefiniowane oddzielnie na niestandardowej karcie makr LLD w konfiguracji reguły wykrywania, z użyciem JSONPath do wskazania wymaganych wartości.

Odkrywanie MBeans

Pozycja wykrywania: `jmx.get[beans,"com.example:type=*,*"]`

Odpowiedź:

```
[
    {
        "object": "com.example:type=Hello,data-src=data-base,  =    ",
        "domain": "com.example",
        "properties": {
            "data-src": "data-base",
            "  ": "    ",
            "type": "Hello"
        }
    },
    {
        "object": "com.example:type=Atomic",
        "domain": "com.example",
        "properties": {
            "type": "Atomic"
        }
    }
]
```

Odkrywanie atrybutów MBean

Pozycja odkrywania: `jmx.get[attributes,"com.example:type=*,*"]`

Odpowiedź:

```
[
    {
        "object": "com.example:type=*",
        "domain": "com.example",
        "properties": {
            "type": "Simple"
        }
    },
    {
        "object": "com.zabbix:type=yes,domain=zabbix.com,data-source=/dev/rand,  =    ,obj=true",
        "domain": "com.zabbix",
        "properties": {
            "type": "Hello",
            "domain": "com.example",
            "data-source": "/dev/rand",
            "  ": "    ",
            "obj": true
        }
    }
]
```

7 Wykrywanie sensorów IPMI

Przegląd

Możliwe jest automatyczne wykrywanie sensorów IPMI.

Aby to zrobić, można użyć kombinacji:

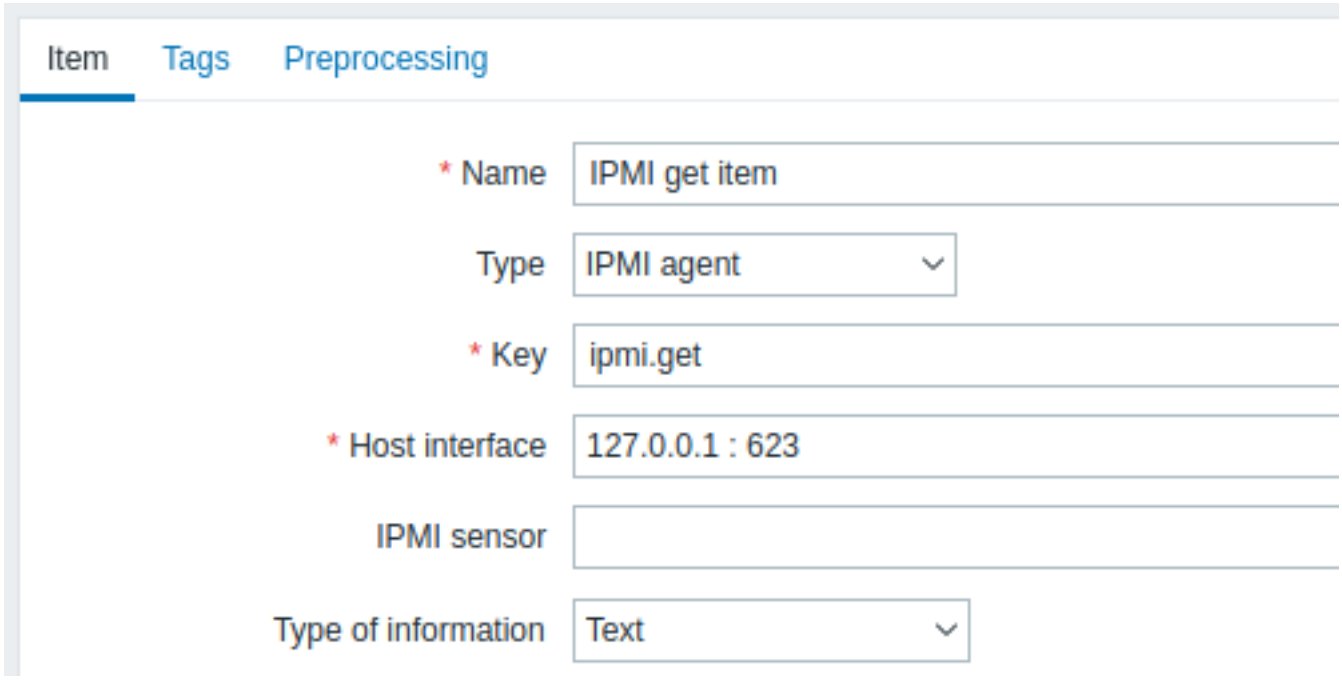
- pozycji IPMI `ipmi.get` jako pozycji nadrzędnej
- zależnej reguły wykrywania niskiego poziomu oraz prototypów pozycji

Konfiguracja

Główna pozycja

Utwórz pozycję IPMI przy użyciu następującego klucza:

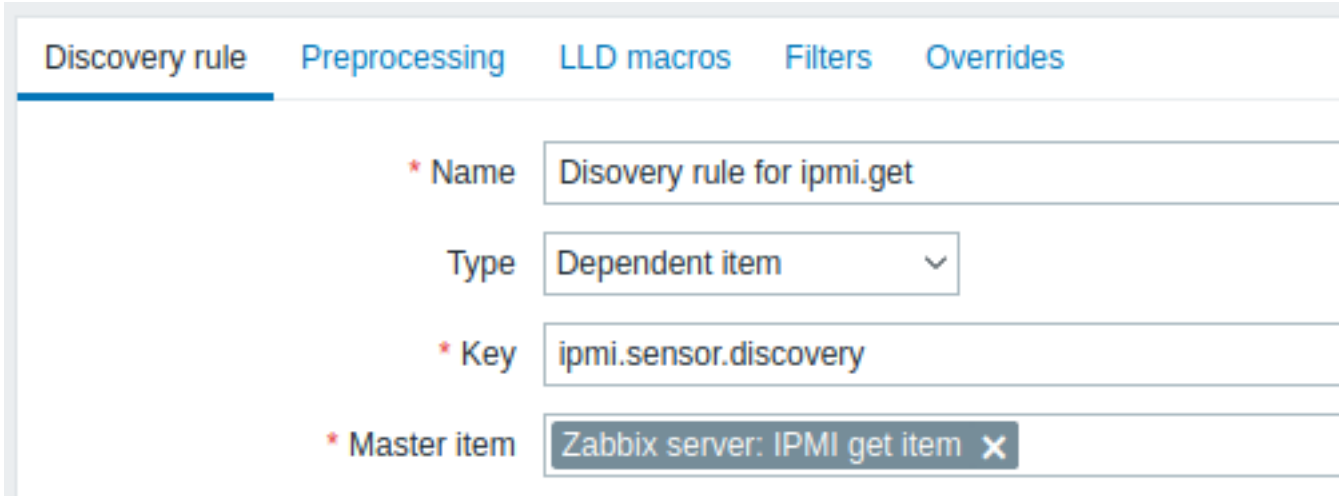
`ipmi.get`



Ustaw typ informacji na „Tekst” dla potencjalnie dużych danych JSON.

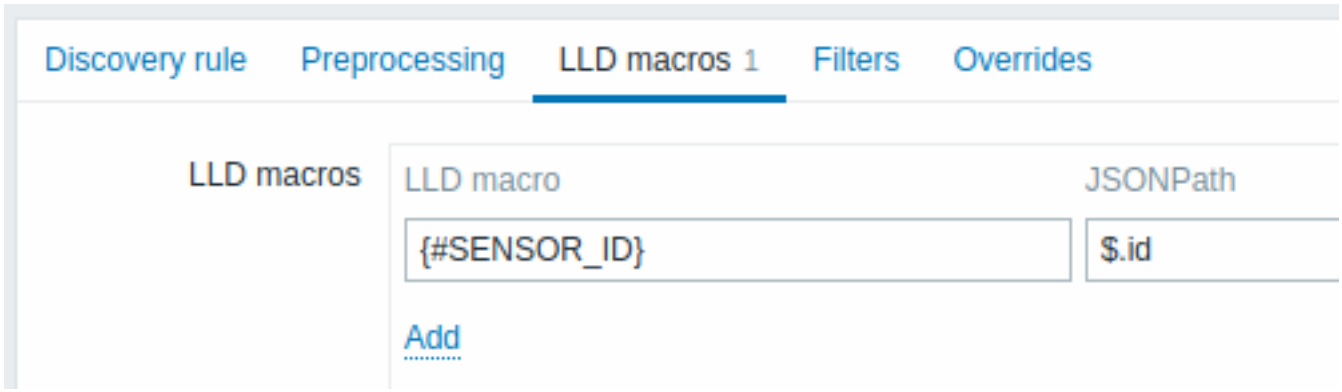
Zależna reguła LLD

Utwórz regułę wykrywania niskiego poziomu typu „Dependent item”:



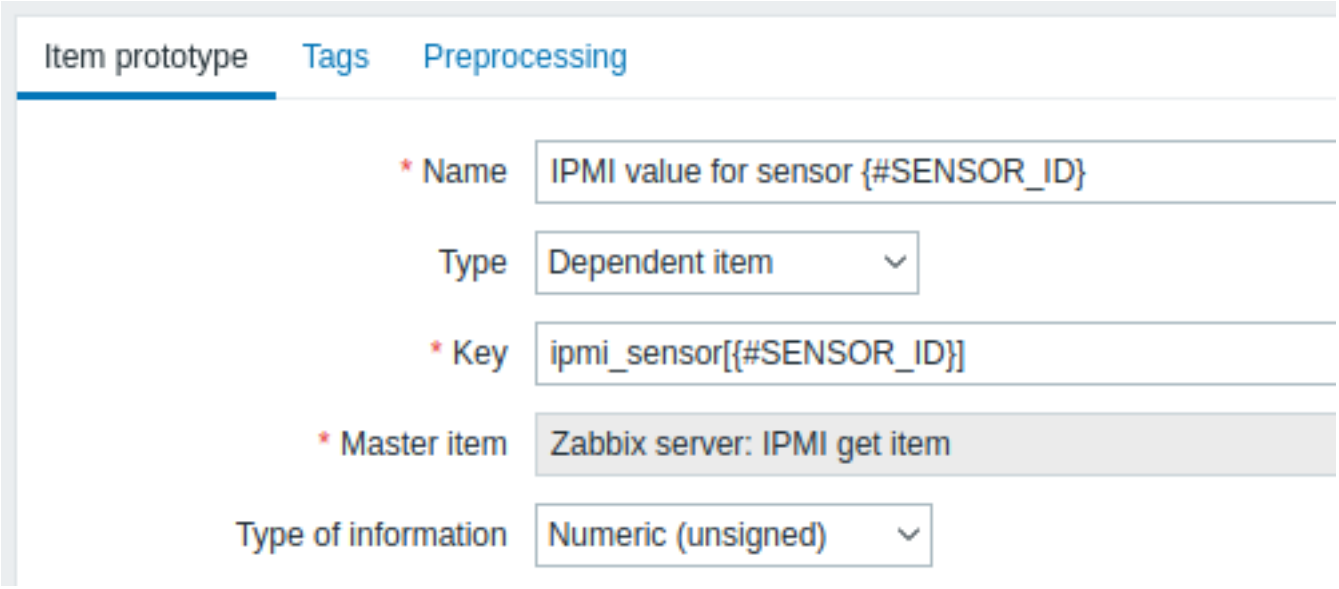
Jako nadrzędną pozycja wybierz utworzoną przez nas pozycja `ipmi.get`.

Na karcie „LLD macros” zdefiniuj niestandardowe makro z odpowiadającym JSONPath:



Prototyp pozycji zależnej

Utwórz prototyp pozycji typu „Dependent item” w tej regule LLD. Jako pozycję nadrzędną dla tego prototypu wybierz pozycję `ipmi.get`, którą utworzyliśmy.



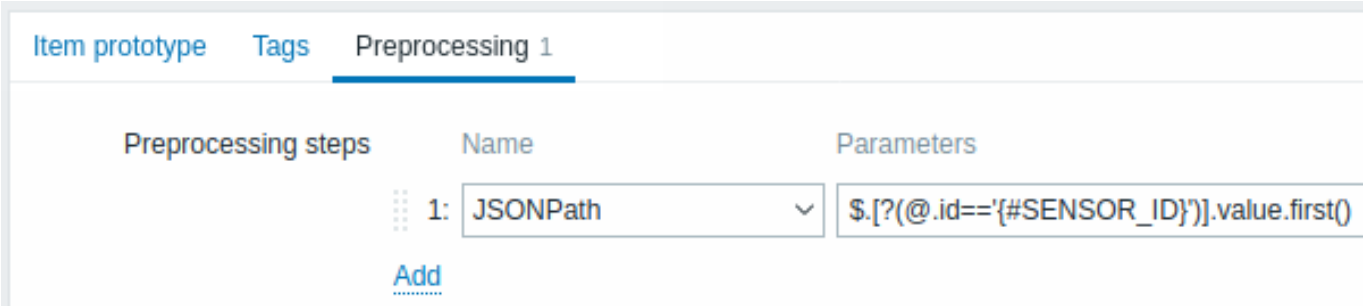
Zwróć uwagę na użycie makra {#SENSOR_ID} w nazwie i kluczu prototypu pozycji:

- *Nazwa*: Wartość IPMI dla sensora {#SENSOR_ID}
- *Klucz*: ipmi_sensor[{#SENSOR_ID}]

Jako typ informacji wybierz *Numeric (unsigned)*.

Na karcie „Preprocessing" prototypu pozycji wybierz JSONPath i użyj następującego wyrażenia JSONPath jako parametru:

```
$.[?(@.id=='{#SENSOR_ID}')].value.first()
```



Po rozpoczęciu wykrywania zostanie utworzona jedna pozycja dla każdego sensora IPMI. Ta pozycja będzie zwracać wartość całkowitą dla danego sensora.

8 Wykrywanie usług systemd

Przegląd

Możliwe jest wykrywanie jednostek systemd (domyślnie usług) za pomocą Zabbix.

Klucz pozycji

Pozycja używana w regule wykrywania to

```
systemd.unit.discovery
```

Attention:
Ten klucz pozycji jest obsługiwany tylko w Zabbix agent 2.

Ta pozycja zwraca JSON z informacjami o jednostkach systemd, na przykład:

```
[{
    "{#UNIT.NAME}": "mysqld.service",
    "{#UNIT.DESCRIPTION}": "MySQL Server",
    "{#UNIT.LOADSTATE}": "loaded",
    "{#UNIT.ACTIVESTATE}": "active",
    "{#UNIT.SUBSTATE}": "running",
    "{#UNIT.FOLLOWED}": "",
```

```
    "{#UNIT.PATH}": "/org/freedesktop/systemd1/unit/mysqld_2eservice",
    "{#UNIT.JOBID}": 0,
    "{#UNIT.JOBTYPE}": "",
    "{#UNIT.JOBPATH}": "/",
    "{#UNIT.UNITFILESTATE}": "enabled"
    "{#UNIT.SERVICETYPE}": "simple"
}, {
    "{#UNIT.NAME}": "systemd-journald.socket",
    "{#UNIT.DESCRIPTION}": "Journal Socket",
    "{#UNIT.LOADSTATE}": "loaded",
    "{#UNIT.ACTIVESTATE}": "active",
    "{#UNIT.SUBSTATE}": "running",
    "{#UNIT.FOLLOWED}": "",
    "{#UNIT.PATH}": "/org/freedesktop/systemd1/unit/systemd_2djournald_2esocket",
    "{#UNIT.JOBID}": 0,
    "{#UNIT.JOBTYPE}": "",
    "{#UNIT.JOBPATH}": "/",
    "{#UNIT.UNITFILESTATE}": "enabled"
}]
```

Wykrywanie wyłączonych jednostek systemd

Możliwe jest również wykrywanie **wyłączonych** jednostek systemd. W takim przypadku w wynikowym JSON zwracane są trzy makra:

- {#UNIT.PATH}
- {#UNIT.ACTIVESTATE}
- {#UNIT.UNITFILESTATE}.

Attention:
Aby pozycje i wyzwalacze były tworzone z prototypów dla wyłączonych jednostek systemd, upewnij się, że dostosowano (lub usunięto) blokujące filtry LLD dla {#UNIT.ACTIVESTATE} i {#UNIT.UNITFILESTATE}.

Obsługiwane makra

Następujące makra są obsługiwane do użycia w filtrze reguły wykrywania oraz w prototypach pozycji, wyzwalaczy i wykresów:

Macro	Description
{#UNIT.NAME}	Podstawowa nazwa jednostki.
{#UNIT.DESCRIPTION}	Opis czytelny dla człowieka.
{#UNIT.LOADSTATE}	Stan załadowania (tj. czy plik jednostki został pomyślnie załadowany).
{#UNIT.ACTIVESTATE}	Stan aktywności (tj. czy jednostka jest obecnie uruchomiona, czy nie).
{#UNIT.SUBSTATE}	Stan podrzędny (bardziej szczegółowa wersja stanu aktywności, specyficzna dla typu jednostki, w przeciwieństwie do stanu aktywności).
{#UNIT.FOLLOWED}	Jednostka, której stan jest śledzony przez tę jednostkę, jeśli taka istnieje; w przeciwnym razie pusty ciąg.
{#UNIT.PATH}	Ścieżka obiektu jednostki.
{#UNIT.JOBID}	Numeryczny identyfikator zadania, jeśli dla jednostki zadania znajduje się zadanie w kolejce; w przeciwnym razie 0.
{#UNIT.JOBTYPE}	Typ zadania.
{#UNIT.JOBPATH}	Ścieżka obiektu zadania.
{#UNIT.UNITFILESTATE}	Stan instalacji pliku jednostki.
{#UNIT.SERVICETYPE}	Typ jednostki usługi (np. `simple`, `forking`, `oneshot`, `idle` itd.). To makro jest zwracane tylko wtedy, gdy jednostka jest usługą.

Prototypy pozycji

Prototypy pozycji, które można utworzyć na podstawie wykrywania usług systemd, obejmują na przykład:

- Nazwa pozycji: `{#UNIT.DESCRIPTION} active state info`; klucz pozycji: `systemd.unit.info["{#UNIT.NAME}"]`
- Nazwa pozycji: `{#UNIT.DESCRIPTION} load state info`; klucz pozycji: `systemd.unit.info["{#UNIT.NAME}",LoadState]`

9 Wykrywanie usług Windows

Przegląd

Podobnie jak wykrywane są systemy plików, możliwe jest również wykrywanie usług systemu Windows.

Klucz pozycji

Pozycja używana w regule odkrywania to

`service.discovery`

Obsługiwane makra

Następujące makra są obsługiwane do użycia w filtrze reguły wykrywania oraz w prototypach pozycji, wyzwalaczy i wykresów:

Makro	Opis
{#SERVICE.NAME}	Nazwa usługi.
{#SERVICE.DISPLAYNAME}	Wyświetlana nazwa usługi.
{#SERVICE.DESCRIPTION}	Opis usługi.
{#SERVICE.STATE}	Wartość liczbowa stanu usługi. Szczegóły znajdują się w pozycji service.info.
{#SERVICE.STATENAME}	Nazwa stanu usługi. Szczegóły znajdują się w pozycji service.info.
{#SERVICE.PATH}	Ścieżka usługi.
{#SERVICE.USER}	Użytkownik usługi.
{#SERVICE.STARTUP}	Wartość liczbowa typu uruchamiania usługi. Szczegóły znajdują się w pozycji service.info.
{#SERVICE.STARTUPNAME}	Nazwa typu uruchamiania usługi. Szczegóły znajdują się w pozycji service.info.
{#SERVICE.STARTUPTRIGGER}	Wartość liczbowa wskazująca, czy typ uruchamiania usługi ma: 0 - brak wyzwalaczy uruchamiania 1 - ma wyzwalacze uruchamiania Jest to przydatne do wykrywania takich typów uruchamiania usług jak *Automatyczny (uruchamianie wyzwalane)*, *Automatyczny opóźniony (uruchamianie wyzwalane)* oraz *Ręczny (uruchamianie wyzwalane).*

Na podstawie wykrywania usług Windows można utworzyć prototyp pozycji taki jak

`service.info[{#SERVICE.NAME},<param>]`

gdzie `param` przyjmuje następujące wartości: *state*, *displayname*, *path*, *user*, *startup* lub *description*.

Na przykład, aby pobrać wyświetlaną nazwę usługi, można użyć pozycji "service.info[{#SERVICE.NAME},displayname]". Jeśli wartość `param` nie zostanie określona ("service.info[{#SERVICE.NAME}]"), używany jest domyślny parametr *state*.

10 Odkrywanie instancji liczników wydajności systemu Windows

Przegląd

Możliwe jest wykrywanie instancji obiektów liczników wydajności systemu Windows. Jest to przydatne w przypadku liczników wydajności z wieloma instancjami.

Klucz pozycji

Aby skonfigurować regułę wykrywania, użyj następującej pozycji:

- `perf_instance.discovery[object]`

Zwróć uwagę, że nazwa obiektu może być zlokalizowana. Na przykład:

```
perf_instance.discovery[Processor] # Nazwa obiektu jest w języku angielskim.
perf_instance.discovery[Processador] # Nazwa obiektu jest w języku portugalskim.
```

Alternatywnie, aby mieć pewność, że nazwa obiektu jest podawana w języku angielskim, niezależnie od lokalizacji systemu operacyjnego, użyj następującej pozycji:

- `perf_instance_en.discovery[object]`

Na przykład:

```
perf_instance_en.discovery[Processor]
perf_instance_en.discovery[Memory]
```

Obsługiwane makra

Proces wykrywania zwróci wszystkie instancje określonego obiektu w makrze {#INSTANCE}:

```
[
    {"{#INSTANCE}":"0"},
    {"{#INSTANCE}":"1"},
    {"{#INSTANCE}":"_Total"}
]
```

To makro może być używane w prototypach pozycji perf_counter[] i perf_counter_en[].

Na przykład, jeśli kluczem pozycji użytym w regule wykrywania jest perf_instance.discovery[Processor], możesz utworzyć następujący prototyp pozycji:

```
perf_counter["\Processor({#INSTANCE})\% Processor Time"]
```

Uwaga:

- Jeśli określony obiekt nie zostanie znaleziony lub nie obsługuje zmiennych instancji, pozycja wykrywania otrzyma stan NOT-SUPPORTED.
- Jeśli określony obiekt obsługuje zmienne instancje, ale obecnie nie ma żadnych instancji, zostanie zwrócona pusta tablica JSON.
- Zduplikowane instancje zostaną pominięte.

11 Wykrywanie przy użyciu zapytań WMI

Przegląd

WMI to potężny interfejs w systemie Windows, który może być używany do pobierania różnych informacji o komponentach Windows, usługach, stanie systemu oraz zainstalowanym oprogramowaniu.

Może być używany do wykrywania dysków fizycznych i zbierania danych o ich wydajności, wykrywania interfejsów sieciowych, wykrywania gości Hyper-V, monitorowania usług Windows oraz wielu innych zadań w systemie operacyjnym Windows.

Ten typ wykrywania niskiego poziomu jest realizowany przy użyciu zapytań WQL, których wyniki są automatycznie przekształcane w obiekt JSON odpowiedni do wykrywania niskiego poziomu.

Klucz pozycji

Pozycja używana w regule wykrywania to

```
wmi.getall[<namespace>,<query>]
```

Ta pozycja przekształca wynik zapytania w tablicę JSON. Na przykład:

```
select * from Win32_DiskDrive where Name like '%PHYSICALDRIVE%'
```

może zwrócić coś takiego:

```
[
    {
        "DeviceID" : "\\.\PHYSICALDRIVE0",
        "BytesPerSector" : 512,
        "Capabilities" : [
            3,
            4
        ],
        "CapabilityDescriptions" : [
            "Random Access",
            "Supports Writing"
        ],
        "Caption" : "VBOX HARDDISK ATA Device",
        "ConfigManagerErrorCode" : 0,
        "ConfigManagerUserConfig" : "False",
        "CreationClassName" : "Win32_DiskDrive",
        "Description" : "Disk drive",
```

```
        "FirmwareRevision" : "1.0",
        "Index" : 0,
        "InterfaceType" : "IDE"
    },
    {
        "DeviceID" : "\\.\PHYSICALDRIVE1",
        "BytesPerSector" : 512,
        "Capabilities" : [
            3,
            4
        ],
        "CapabilityDescriptions" : [
            "Random Access",
            "Supports Writing"
        ],
        "Caption" : "VBOX HARDDISK ATA Device",
        "ConfigManagerErrorCode" : 0,
        "ConfigManagerUserConfig" : "False",
        "CreationClassName" : "Win32_DiskDrive",
        "Description" : "Disk drive",
        "FirmwareRevision" : "1.0",
        "Index" : 1,
        "InterfaceType" : "IDE"
    }
]
```


Makra wykrywania niskiego poziomu

Mimo że w zwróconym JSON nie są tworzone żadne makra wykrywania niskiego poziomu, makra te mogą zostać zdefiniowane przez użytkownika jako dodatkowy krok, z użyciem funkcji niestandardowych makr LLD, gdzie JSONPath wskazuje na wykryte wartości w zwróconym JSON.

Makra te mogą następnie zostać użyte do tworzenia prototypów pozycji, wyzwalaczy itp.

12 Wykrywanie za pomocą zapytań SQL poprzez ODBC

Przegląd

Ten typ wykrywania niskiego poziomu jest realizowany przy użyciu zapytań SQL, których wyniki są automatycznie przekształcane w obiekt JSON odpowiedni do wykrywania niskiego poziomu.

Klucz pozycji

Zapytania SQL są wykonywane przy użyciu typu pozycji „Database monitor". Dlatego większość instrukcji na stronie monitoring ODBC ma zastosowanie, aby uzyskać działającą regułę wykrywania „Database monitor".

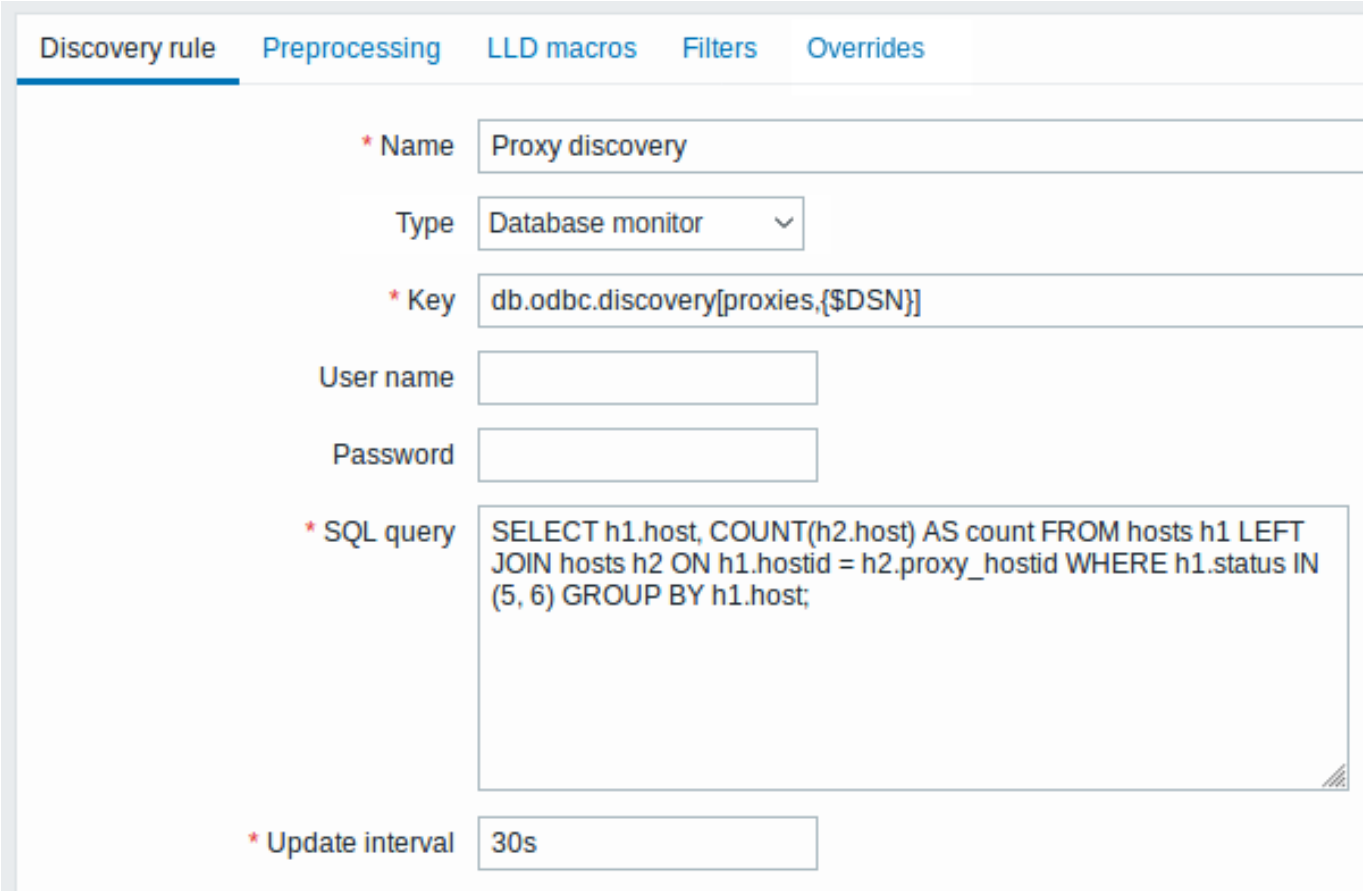
W regułach wykrywania „Database monitor" można używać dwóch kluczy pozycji:

- **db.odbc.discovery**[<unique short description>,<dsn>,<connection string>] - ta pozycja przekształca wynik zapytania SQL w tablicę JSON, zamieniając nazwy kolumn z wyniku zapytania na nazwy makr wykrywania niskiego poziomu sparowane z wykrytymi wartościami pól. Makra te mogą być używane podczas tworzenia prototypów pozycji, wyzwalaczy itp. Zobacz także: Using db.odbc.discovery.
- **db.odbc.get**[<unique short description>,<dsn>,<connection string>] - ta pozycja przekształca wynik zapytania SQL w tablicę JSON, zachowując oryginalne nazwy kolumn z wyniku zapytania jako nazwy pól w JSON sparowane z wykrytymi wartościami. W porównaniu z `db.odbc.discovery[]` ta pozycja nie tworzy makr wykrywania niskiego poziomu w zwracanym JSON, dlatego nie ma potrzeby sprawdzania, czy nazwy kolumn mogą być prawidłowymi nazwami makr. Makra wykrywania niskiego poziomu można zdefiniować jako dodatkowy krok w razie potrzeby, używając funkcji custom LLD macro z JSONPath wskazującym wykryte wartości w zwracanym JSON. Zobacz także: Using db.odbc.get.

Użycie db.odbc.discovery

Poniższy przykład pokazuje, jak zapytanie SQL jest przekształcane do formatu JSON przy użyciu wykrywania niskiego poziomu proxy Zabbix, na podstawie zapytania ODBC do bazy danych Zabbix. Jest to przydatne do automatycznego tworzenia "zabbix[proxy,<name>,lastaccess]" pozycji wewnętrznych w celu monitorowania, które proxy są aktywne.

Zacznij od konfiguracji reguły wykrywania:



Wszystkie wymagane pola wejściowe są oznaczone czerwoną gwiazdką.

Tutaj używane jest następujące bezpośrednie zapytanie do bazy danych Zabbix w celu wybrania wszystkich proxy Zabbix wraz z liczbą hostów, które monitorują. Liczba hostów może zostać użyta na przykład do odfiltrowania pustych proxy:

```
mysql> SELECT h1.host, COUNT(h2.host) AS count FROM hosts h1 LEFT JOIN hosts h2 ON h1.hostid = h2.proxyid
+---------+-------+
| host    | count |
+---------+-------+
| Japan 1 |     5 |
| Japan 2 |    12 |
| Latvia  |     3 |
+---------+-------+
3 rows in set (0.01 sec)
```

Dzięki wewnętrznemu działaniu pozycji "db.odbc.discovery[,{$DSN}]" wynik tego zapytania jest automatycznie przekształcany do następującego formatu JSON:

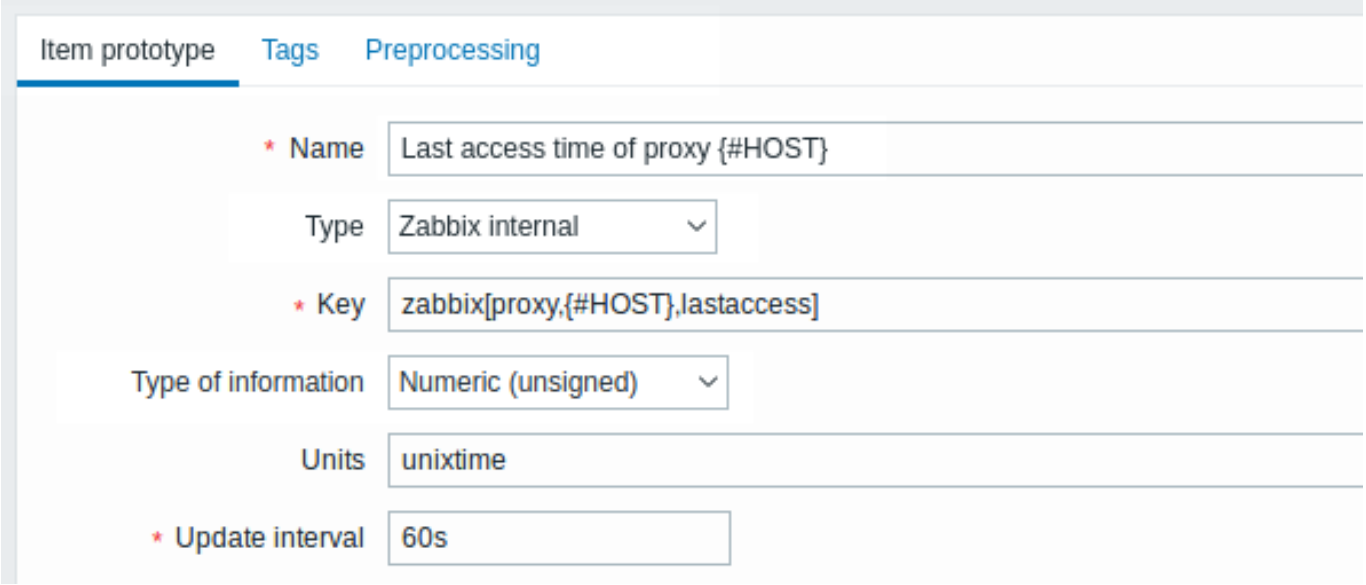
```
[
    {
        "{#HOST}": "Japan 1",
        "{#COUNT}": "5"
    },
    {
        "{#HOST}": "Japan 2",
        "{#COUNT}": "12"
    },
    {
        "{#HOST}": "Latvia",
        "{#COUNT}": "3"
    }
]
```

Jak widać, nazwy kolumn stają się nazwami makr, a wybrane wiersze stają się wartościami tych makr.

Note:
Jeśli nie jest oczywiste, w jaki sposób nazwa kolumny zostanie przekształcona w nazwę makra, zaleca się użycie aliasów kolumn, takich jak "COUNT(h2.host) AS count" w powyższym przykładzie.
Jeśli nazwa kolumny nie może zostać przekonwertowana na prawidłową nazwę makra, reguła wykrywania stanie się nieobsługiwana, a komunikat błędu będzie zawierał numer problematycznej kolumny. Jeśli potrzebna jest dodatkowa pomoc, uzyskane nazwy kolumn są podawane przy DebugLevel=4 w pliku dziennika serwera Zabbix:

```
$ grep db.odbc.discovery /tmp/zabbix_server.log
 ...
 23876:20150114:153410.856 In db_odbc_discovery() query:'SELECT h1.host, COUNT(h2.host) FROM hosts h1 L
 23876:20150114:153410.860 db_odbc_discovery() column[1]:'host'
 23876:20150114:153410.860 db_odbc_discovery() column[2]:'COUNT(h2.host)'
 23876:20150114:153410.860 End of db_odbc_discovery():NOTSUPPORTED
 23876:20150114:153410.860 Item [Zabbix server:db.odbc.discovery[proxies,{$DSN}]] error: Cannot convert
```

Teraz, gdy rozumiemy, jak zapytanie SQL jest przekształcane w obiekt JSON, możemy użyć makra {#HOST} w prototypach pozycji:



Po wykonaniu wykrywania zostanie utworzona pozycja dla każdego proxy:



Używanie `db.odbc.get`

Używając `db.odbc.get[,{$DSN}]` oraz poniższego przykładu SQL:

```
mysql> SELECT h1.host, COUNT(h2.host) AS count FROM hosts h1 LEFT JOIN hosts h2 ON h1.hostid = h2.proxyid
+---------+-------+
| host    | count |
+---------+-------+
| Japan 1 |     5 |
| Japan 2 |    12 |
| Latvia  |     3 |
+---------+-------+
3 rows in set (0.01 sec)
```

zostanie zwrócony następujący JSON:

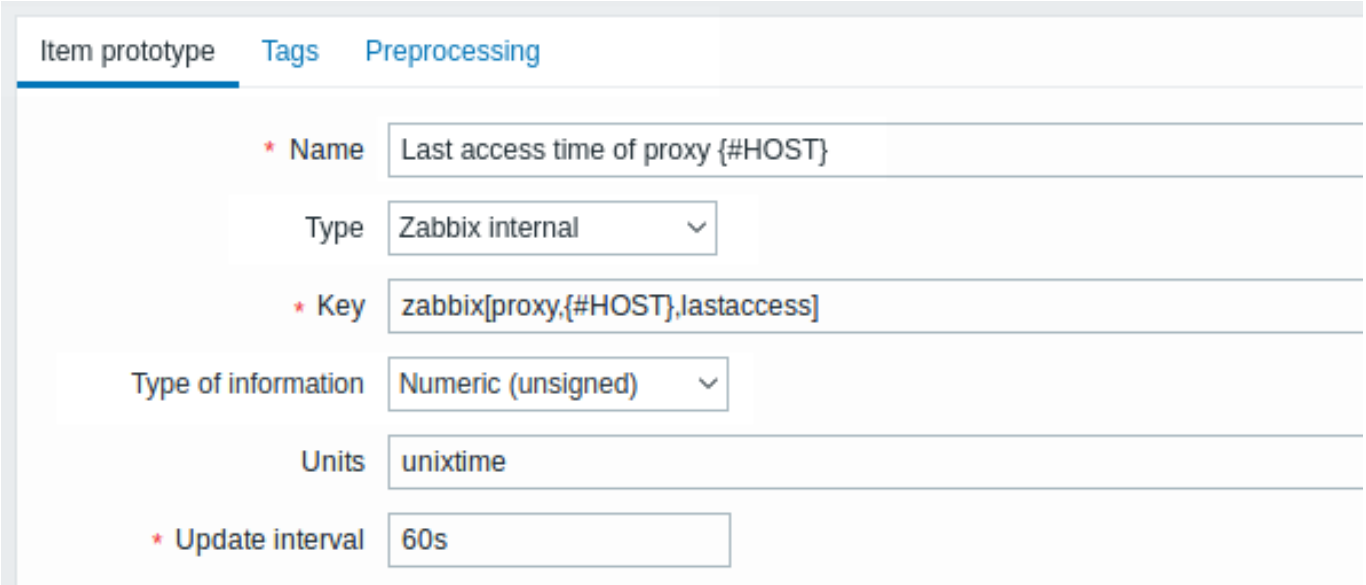
```
[
    {
```

```
        "host": "Japan 1",
        "count": "5"
    },
    {
        "host": "Japan 2",
        "count": "12"
    },
    {
        "host": "Latvia",
        "count": "3"
    }
]
```

Jak widać, nie ma tam makr niskopoziomowego wykrywania. Jednak własne makra niskopoziomowego wykrywania można utworzyć na karcie LLD macros reguły wykrywania przy użyciu JSONPath, na przykład:

```
{#HOST} → $.host
```

Teraz to makro {#HOST} może być używane w prototypach pozycji:



13 Wykrywanie przy użyciu danych Prometheus

Przegląd

Dane dostarczone w formacie linii Prometheus mogą być używane do odkrywania niskiego poziomu.

Szczegółowe informacje o tym, jak zaimplementowano odpytywanie danych Prometheus w Zabbix, można znaleźć w sekcji Prometheus checks.

Konfiguracja

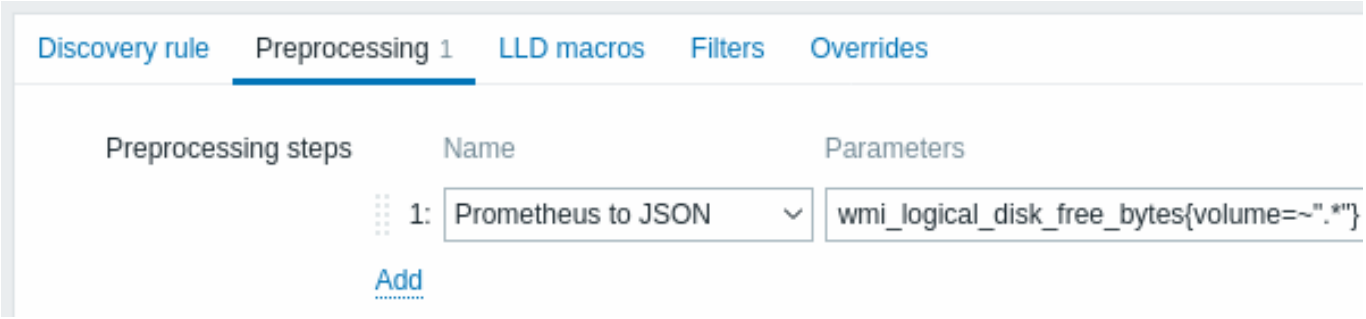
Reguła wykrywania niskiego poziomu powinna zostać utworzona jako pozycja zależna względem nadrzędnej pozycji HTTP, która zbiera dane Prometheus.

Prometheus do JSON

W regule wykrywania przejdź do zakładki Preprocessing i wybierz opcję przetwarzania wstępnego *Prometheus do JSON*. Dane w formacie JSON są potrzebne do wykrywania, a opcja przetwarzania wstępnego *Prometheus do JSON* zwróci dokładnie takie dane z następującymi atrybutami:

- nazwa metryki
- wartość metryki
- help (jeśli występuje)
- type (jeśli występuje)
- labels (jeśli występują)
- surowy wiersz

Na przykład zapytanie `wmi_logical_disk_free_bytes`:



z tych wierszy Prometheus:

```
# HELP wmi_logical_disk_free_bytes Free space in bytes (LogicalDisk.PercentFreeSpace)
# TYPE wmi_logical_disk_free_bytes gauge
wmi_logical_disk_free_bytes{volume="C:"} 3.5180249088e+11
wmi_logical_disk_free_bytes{volume="D:"} 2.627731456e+09
wmi_logical_disk_free_bytes{volume="HarddiskVolume4"} 4.59276288e+08
```

zwróci:

```
[
    {
        "name": "wmi_logical_disk_free_bytes",
        "help": "Free space in bytes (LogicalDisk.PercentFreeSpace)",
        "type": "gauge",
        "labels": {
            "volume": "C:"
         },
        "value": "3.5180249088e+11",
        "line_raw": "wmi_logical_disk_free_bytes{volume=\"C:\"} 3.5180249088e+11"
    },
    {
        "name": "wmi_logical_disk_free_bytes",
        "help": "Free space in bytes (LogicalDisk.PercentFreeSpace)",
        "type": "gauge",
        "labels": {
            "volume": "D:"
         },
        "value": "2.627731456e+09",
        "line_raw": "wmi_logical_disk_free_bytes{volume=\"D:\"} 2.627731456e+09"
    },
    {
        "name": "wmi_logical_disk_free_bytes",
        "help": "Free space in bytes (LogicalDisk.PercentFreeSpace)",
        "type": "gauge",
        "labels": {
            "volume": "HarddiskVolume4"
         },
        "value": "4.59276288e+08",
        "line_raw": "wmi_logical_disk_free_bytes{volume=\"HarddiskVolume4\"} 4.59276288e+08"
    }
]
```

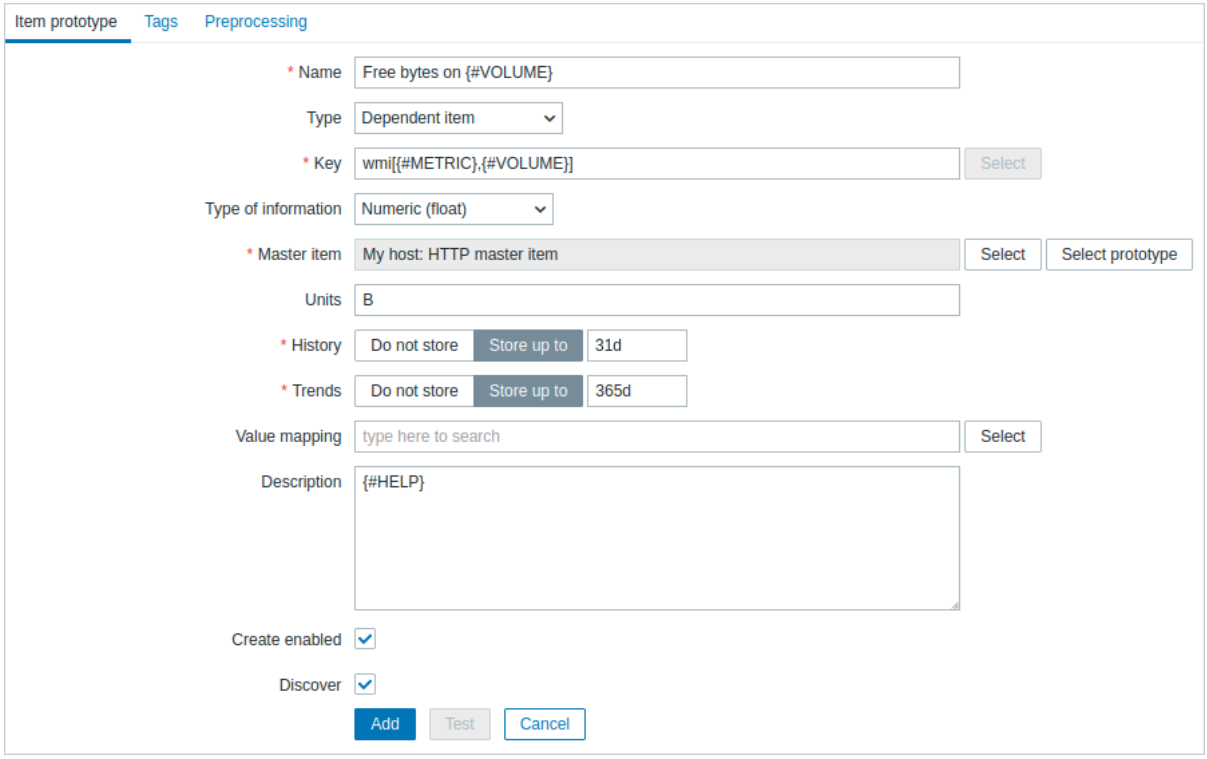
Mapowanie makr LLD

Następnie należy przejść do zakładki makr LLD i utworzyć następujące mapowania:

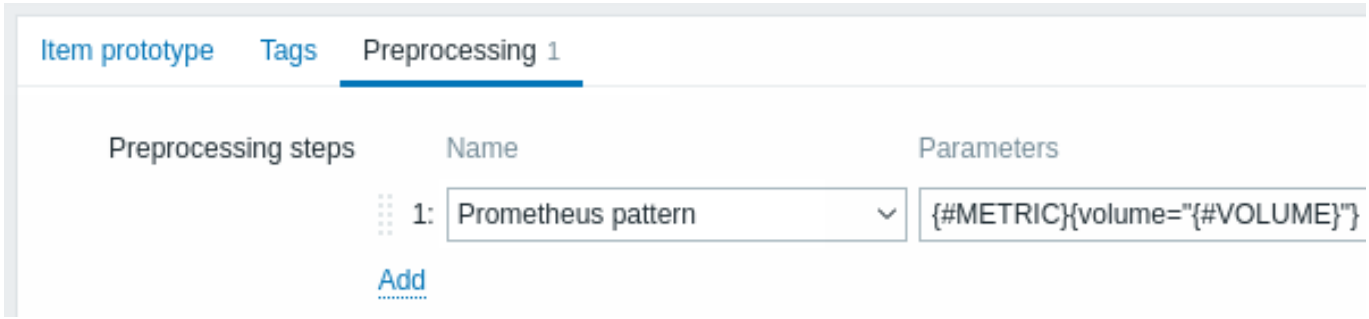
```
{#VOLUME}=$.labels['volume']
{#METRIC}=$['name']
{#HELP}=$['help']
```

Prototyp pozycji

Możesz chcieć utworzyć prototyp pozycji w taki sposób:



z opcjami przetwarzania wstępnego:



14 Wykrywanie urządzeń blokowych

Podobnie jak wykrywane są systemy plików, możliwe jest również wykrywanie urządzeń blokowych oraz ich typu.

Klucz pozycji

Klucz pozycji do użycia w regule wykrywania to

`vfs.dev.discovery`

Ta pozycja jest obsługiwana tylko na platformach Linux.

Możesz tworzyć reguły wykrywania przy użyciu tej pozycji wykrywania oraz:

- filtra: **{#DEVNAME} pasuje do** `sd[\D]$` — aby wykrywać urządzenia o nazwach „sd0”, „sd1”, „sd2”, ...
- filtra: **{#DEVTYPE} pasuje do** `disk` **ORAZ {#DEVNAME} nie pasuje do** `^loop.*` — aby wykrywać urządzenia typu dysk, których nazwa nie zaczyna się od „loop”

Obsługiwane makra

Ten klucz wykrywania zwraca dwa makra - {#DEVNAME} i {#DEVTYPE}, identyfikujące odpowiednio nazwę i typ urządzenia blokowego, na przykład:

```
[
   {
      "{#DEVNAME}":"loop1",
      "{#DEVTYPE}":"disk"
   },
   {
      "{#DEVNAME}":"dm-0",
```

```
        "{#DEVTYPE}":"disk"
    },
    {
        "{#DEVNAME}":"sda",
        "{#DEVTYPE}":"disk"
    },
    {
        "{#DEVNAME}":"sda1",
        "{#DEVTYPE}":"partition"
    }
]
```

Wykrywanie urządzeń blokowych pozwala używać pozycji `vfs.dev.read[]` i `vfs.dev.write[]` do tworzenia prototypów pozycji z użyciem makra {#DEVNAME}, na przykład:

- ”vfs.dev.read[{#DEVNAME},sps]”
- ”vfs.dev.write[{#DEVNAME},sps]”

Makro {#DEVTYPE} jest przeznaczone do filtrowania urządzeń.

15 Odkrywanie interfejsów hosta w Zabbix

Przegląd

Możliwe jest wykrywanie wszystkich interfejsów skonfigurowanych w frontend Zabbix dla hosta.

Klucz pozycji

Pozycją używaną w regule wykrywania jest wewnętrzna pozycja Zabbix:

`zabbix[host,discovery,interfaces]`

Ta pozycja zwraca JSON z opisem interfejsów, w tym:

- adres IP/nazwę hosta DNS (w zależności od ustawienia hosta „Połącz z”)
- numer portu
- typ interfejsu (agent Zabbix, SNMP, JMX, IPMI)
- informację, czy jest to interfejs domyślny, czy nie
- informację, czy funkcja żądań zbiorczych jest włączona — tylko dla interfejsów SNMP.

Na przykład:

```
[{"{#IF.CONN}":"192.168.3.1","{#IF.IP}":"192.168.3.1","{#IF.DNS}":"","{#IF.PORT}":"10050","{#IF.TYPE}":"AG
```

W przypadku wielu interfejsów ich rekordy w JSON są uporządkowane według:

- typu interfejsu,
- domyślności — interfejs domyślny jest umieszczany przed interfejsami niedomyślnymi,
- ID interfejsu (w kolejności rosnącej).

Obsługiwane makra

Następujące makra są obsługiwane do użycia w filtrze reguły wykrywania oraz w prototypach pozycji, wyzwalaczy i wykresów:

Macro	Description
{#IF.CONN}	Adres IP interfejsu lub nazwa hosta DNS.
{#IF.IP}	Adres IP interfejsu.
{#IF.DNS}	Nazwa hosta DNS interfejsu.
{#IF.PORT}	Numer portu interfejsu.
{#IF.TYPE}	Typ interfejsu („AGENT”, „SNMP”, „JMX” lub „IPMI”).
{#IF.DEFAULT}	Status domyślny interfejsu: 0 - interfejs niedomyślny 1 - interfejs domyślny
{#IF.SNMP.BULK}	Status przetwarzania zbiorczego SNMP dla interfejsu: 0 - wyłączone 1 - włączone To makro jest zwracane tylko wtedy, gdy typ interfejsu to „SNMP”.

8 Własne reguły LLD

Przegląd

Możliwe jest również utworzenie całkowicie niestandardowej reguły LLD, wykrywającej dowolny typ encji — na przykład bazy danych na serwerze bazodanowym.

W tym celu należy utworzyć niestandardową pozycja, która zwraca ciąg JSON, określający znalezione obiekty oraz opcjonalnie — niektóre ich właściwości. Liczba makr na encję nie jest ograniczona — podczas gdy wbudowane reguły wykrywania zwracają jedno lub dwa makra (na przykład dwa dla wykrywania systemów plików), możliwe jest zwrócenie większej liczby.

Przykład

Wymagany format ciągu JSON najlepiej zilustrować na przykładzie. Załóżmy, że używasz starego agenta Zabbix 1.8 (takiego, który nie obsługuje klucza vfs.fs.discovery), ale nadal musisz wykrywać systemy plików. Poniżej znajduje się prosty skrypt Perl dla Linuksa, który wykrywa zamontowane systemy plików i zwraca dane w formacie JSON, zawierające zarówno nazwę, jak i typ systemu plików. Jednym ze sposobów jego użycia byłoby zastosowanie go jako UserParameter z kluczem "vfs.fs.discovery_perl":

```
####!/usr/bin/perl

$first = 1;

print "[\n";

for (`cat /proc/mounts`)
{
    ($fsname, $fstype) = m/\S+ (\S+) (\S+)/;

    print "\t,\n" if not $first;
    $first = 0;

    print "\t{\n";
    print "\t\t\"{#FSNAME}\":\"$fsname\",\n";
    print "\t\t\"{#FSTYPE}\":\"$fstype\"\n";
    print "\t}\n";
}

print "]\n";
```

Attention:
Dozwolone symbole w nazwach makr LLD to **0-9** , **A-Z** , **_** , **.** Małe litery nie są obsługiwane w nazwach.

Przykład danych wyjściowych (przeformatowany dla czytelności) pokazano poniżej. JSON dla niestandardowych kontroli wykrywania musi mieć ten sam format.

```
[
    { "{#FSNAME}":"/",                          "{#FSTYPE}":"rootfs"   },
    { "{#FSNAME}":"/sys",                       "{#FSTYPE}":"sysfs"    },
    { "{#FSNAME}":"/proc",                      "{#FSTYPE}":"proc"     },
    { "{#FSNAME}":"/dev",                       "{#FSTYPE}":"devtmpfs" },
    { "{#FSNAME}":"/dev/pts",                   "{#FSTYPE}":"devpts"   },
    { "{#FSNAME}":"/lib/init/rw",               "{#FSTYPE}":"tmpfs"    },
    { "{#FSNAME}":"/dev/shm",                   "{#FSTYPE}":"tmpfs"    },
    { "{#FSNAME}":"/home",                      "{#FSTYPE}":"ext3"     },
    { "{#FSNAME}":"/tmp",                       "{#FSTYPE}":"ext3"     },
    { "{#FSNAME}":"/usr",                       "{#FSTYPE}":"ext3"     },
    { "{#FSNAME}":"/var",                       "{#FSTYPE}":"ext3"     },
    { "{#FSNAME}":"/sys/fs/fuse/connections",   "{#FSTYPE}":"fusectl"  }
]
```

W poprzednim przykładzie wymagane jest, aby klucze odpowiadały nazwom makr LLD używanym w prototypach; alternatywnie można wyodrębnić wartości makr LLD za pomocą JSONPath `{#FSNAME}` → `$.fsname` oraz `{#FSTYPE}` → `$.fstype`, co umożliwia użycie takiego skryptu:

```
####!/usr/bin/perl
```

```
$first = 1;

print "[\n";

for (`cat /proc/mounts`)
{
    ($fsname, $fstype) = m/\S+ (\S+) (\S+)/;

    print "\t,\n" if not $first;
    $first = 0;

    print "\t{\n";
    print "\t\t\"fsname\":\"$fsname\",\n";
    print "\t\t\"fstype\":\"$fstype\"\n";
    print "\t}\n";
}

print "]\n";
```

Przykład danych wyjściowych (przeformatowany dla czytelności) pokazano poniżej.

```
[
    { "fsname":"/",                          "fstype":"rootfs"   },
    { "fsname":"/sys",                       "fstype":"sysfs"    },
    { "fsname":"/proc",                      "fstype":"proc"     },
    { "fsname":"/dev",                       "fstype":"devtmpfs" },
    { "fsname":"/dev/pts",                   "fstype":"devpts"   },
    { "fsname":"/lib/init/rw",               "fstype":"tmpfs"    },
    { "fsname":"/dev/shm",                   "fstype":"tmpfs"    },
    { "fsname":"/home",                      "fstype":"ext3"     },
    { "fsname":"/tmp",                       "fstype":"ext3"     },
    { "fsname":"/usr",                       "fstype":"ext3"     },
    { "fsname":"/var",                       "fstype":"ext3"     },
    { "fsname":"/sys/fs/fuse/connections",   "fstype":"fusectl"  }
]
```

Następnie w polu *Filter* reguły wykrywania możesz określić "{#FSTYPE}" jako makro, a "rootfs|ext3" jako wyrażenie regularne.

Note:
Nie musisz używać nazw makr takich jak FSNAME/FSTYPE w niestandardowych regułach LLD; możesz używać dowolnych nazw. Jeśli używany jest JSONPath, wówczas wiersz LLD będzie elementem tablicy, który może być obiektem, ale może też być inną tablicą albo wartością.

Pamiętaj, że w przypadku użycia parametru użytkownika wartość zwracana jest ograniczona do 16 MB. Więcej szczegółów znajdziesz w sekcji limity danych dla wartości zwracanych LLD.

14 Monitorowanie rozproszone

Przegląd Zabbix zapewnia skuteczny i niezawodny sposób monitorowania rozproszonej infrastruktury IT przy użyciu proxy.

Proxy mogą być używane do lokalnego zbierania danych w imieniu scentralizowanego serwera Zabbix, a następnie przekazywania tych danych do serwera.

Funkcje proxy

Przy podejmowaniu decyzji o użyciu lub nieużyciu proxy należy wziąć pod uwagę kilka kwestii.

	Proxy
Lekki	**Tak**
GUI	Nie
Działa niezależnie	**Tak**

	Proxy
Łatwe utrzymanie	**Tak**
Automatyczne tworzenie bazy danych	**Tak**[1]
Lokalna administracja	Nie
Gotowy do użycia na sprzęcie wbudowanym	**Tak**
Jednokierunkowe połączenia TCP	**Tak**
Scentralizowana konfiguracja	**Tak**
Generuje powiadomienia	Nie

[1] Funkcja automatycznego tworzenia bazy danych działa tylko z SQLite. Inne obsługiwane bazy danych wymagają ręcznej konfiguracji.

Attention:
Proxy Zabbix nie uwzględnia okresów konserwacji; szczegóły znajdują się w sekcji Obliczanie kolejek podczas konserwacji.

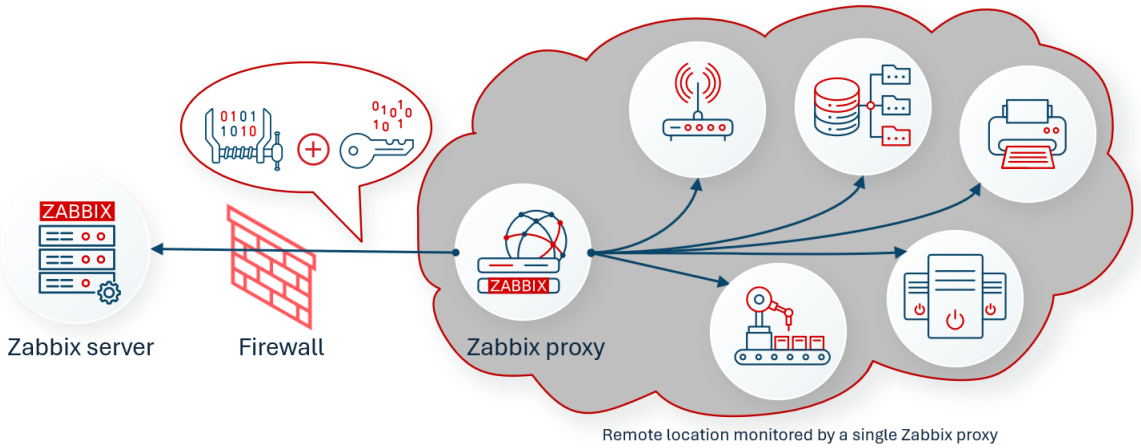
1 Proxy

Przegląd Proxy Zabbix może zbierać dane o wydajności i dostępności w imieniu serwera Zabbix. W ten sposób proxy może przejąć część obciążenia związanego ze zbieraniem danych i odciążyć serwer Zabbix.

Ponadto użycie proxy jest najprostszym sposobem wdrożenia monitorowania scentralizowanego i rozproszonego, gdy wszystkie agenty i proxy raportują do jednego serwera Zabbix, a wszystkie dane są zbierane centralnie.

Proxy Zabbix może być używany do:

- Monitorowania zdalnych lokalizacji
- Monitorowania lokalizacji z zawodną komunikacją
- Odciążenia serwera Zabbix podczas monitorowania tysięcy urządzeń
- Uproszczenia utrzymania monitorowania rozproszonego



Proxy wymaga tylko jednego połączenia TCP z serwerem Zabbix. Dzięki temu łatwiej jest ominąć zaporę sieciową, ponieważ trzeba skonfigurować tylko jedną regułę zapory.

Attention:
Proxy Zabbix musi używać oddzielnej bazy danych. Wskazanie bazy danych serwera Zabbix spowoduje uszkodzenie konfiguracji.

Wszystkie dane zebrane przez proxy są przechowywane lokalnie przed przesłaniem ich do serwera. Dzięki temu żadne dane nie zostaną utracone z powodu tymczasowych problemów z komunikacją z serwerem. Parametry *ProxyLocalBuffer* i *ProxyOfflineBuffer* w pliku konfiguracyjnym proxy określają, jak długo dane są przechowywane lokalnie.

Attention:
Może się zdarzyć, że proxy, który otrzymuje najnowsze zmiany konfiguracji bezpośrednio z bazy danych serwera Zabbix, ma bardziej aktualną konfigurację niż serwer Zabbix, którego konfiguracja może nie być aktualizowana tak szybko ze względu na wartość CacheUpdateFrequency. W rezultacie proxy może rozpocząć zbieranie danych i wysyłać je do serwera Zabbix, który te dane zignoruje.

Proxy Zabbix jest kolektorem danych. Nie oblicza wyzwalaczy, nie przetwarza zdarzeń ani nie wysyła alertów. Aby uzyskać przegląd funkcjonalności proxy, zapoznaj się z poniższą tabelą:

Funkcja		Obsługiwane przez proxy
Pozycje		
	Kontrole agenta Zabbix	**Tak**
	Kontrole agenta Zabbix (aktywne)	**Tak** [1]
	Kontrole proste	**Tak**
	Pozycje trappera	**Tak**
	Kontrole SNMP	**Tak**
	Pułapki SNMP	**Tak**
	Kontrole IPMI	**Tak**
	Kontrole JMX	**Tak**
	Monitorowanie plików dziennika	**Tak**
	Kontrole wewnętrzne	**Tak**
	Kontrole SSH	**Tak**
	Kontrole Telnet	**Tak**
	Kontrole zewnętrzne	**Tak**
	Pozycje zależne	**Tak**
	Pozycje skryptowe	**Tak**
	Pozycje przeglądarkowe	**Tak**
Wbudowane monitorowanie WWW		**Tak**
Wstępne przetwarzanie wartości pozycji		**Tak**
Wykrywanie sieci		**Tak**
Autorejestracja aktywnego agenta		**Tak**
Odkrywanie niskiego poziomu		**Tak** [2]
Polecenia zdalne		**Tak**
Obliczanie wyzwalaczy		*Nie*
Przetwarzanie zdarzeń		*Nie*
Korelacja zdarzeń		*Nie*
Wysyłanie alertów		*Nie*

Note:
[1] Aby mieć pewność, że agent pyta proxy (a nie serwer) o aktywne kontrole, proxy musi być wymieniony w parametrze **ServerActive** w pliku konfiguracyjnym agenta.
 [2] W przypadku LLD proxy Zabbix tylko zbiera i wstępnie przetwarza dane, a następnie wysyła je do serwera Zabbix w celu dalszego przetwarzania.

Ochrona przed przeciążeniem

Jeśli serwer Zabbix był przez pewien czas niedostępny, a proxy zgromadziły dużo danych, po uruchomieniu serwera może dojść do jego przeciążenia (wykorzystanie cache historii przez pewien czas utrzymuje się na poziomie 95-100%). Takie przeciążenie może skutkować spadkiem wydajności, przez co kontrole są przetwarzane wolniej, niż powinny. Aby uniknąć problemów wynikających z przeciążenia cache historii, zaimplementowano mechanizm ochrony przed takim scenariuszem.

Gdy cache historii serwera Zabbix jest pełny, dostęp do zapisu w cache historii jest ograniczany, co wstrzymuje procesy zbierania danych przez serwer. Najczęstszy przypadek przeciążenia cache historii występuje po przestoju serwera, gdy proxy przesyłają zebrane dane. Aby temu zapobiec, dodano ograniczanie proxy (obecnie nie można go wyłączyć).

Gdy wykorzystanie cache historii osiąga 80%, serwer Zabbix przechodzi w tryb ograniczania. W trybie ograniczania serwer akceptuje dane z proxy tylko wtedy, gdy wykorzystanie cache historii spadnie poniżej 60%, rotacyjnie wybierając akceptowane proxy. Gdy wykorzystanie cache historii spadnie poniżej 20%, serwer przełącza się z powrotem do trybu normalnego.

Dodatkowo, w trybie normalnym serwer Zabbix ogranicza poszczególne proxy wysyłające bardzo duże pakiety (ponad 10 000 rekordów), jeśli wykorzystanie cache historii przekracza 60%. Decyzja ta jest podejmowana w momencie, gdy serwer ocenia przesyłanie danych przez proxy, dlatego nie zawsze może być natychmiast widoczna na wykresach wykorzystania cache historii (wewnętrzna pozycja `zabbix[wcache,history,pused]` i jej interwał aktualizacji mogą nie uchwycić krótkotrwałych skoków).

Ten tryb ograniczania będzie trwał do momentu, gdy wykorzystanie cache ponownie osiągnie 80%, spadnie do 20% albo lista ograniczania będzie pusta. W pierwszym przypadku serwer ponownie przestanie akceptować dane z proxy. W pozostałych dwóch przypadkach serwer zacznie działać normalnie, akceptując dane ze wszystkich proxy.

Powyższe informacje można zilustrować w poniższej tabeli:

Wykorzystanie cache zapisu historii	Tryb serwera Zabbix	Działanie serwera Zabbix
Osiąga 80%	Oczekiwanie	Przestaje akceptować dane z proxy, ale utrzymuje *listę ograniczania* (uporządkowaną listę proxy, z którymi należy skontaktować się później).
Osiąga 60%	Normalny, ale gotowy do ograniczania	Może odrzucać bardzo duże przesyłania z proxy (ponad 10 tys. rekordów) podczas podejmowania decyzji o akceptacji danych; nadal akceptuje inne dane z proxy.
Spada do 20%	Normalny	Usuwa listę ograniczania i zaczyna normalnie akceptować dane z proxy.

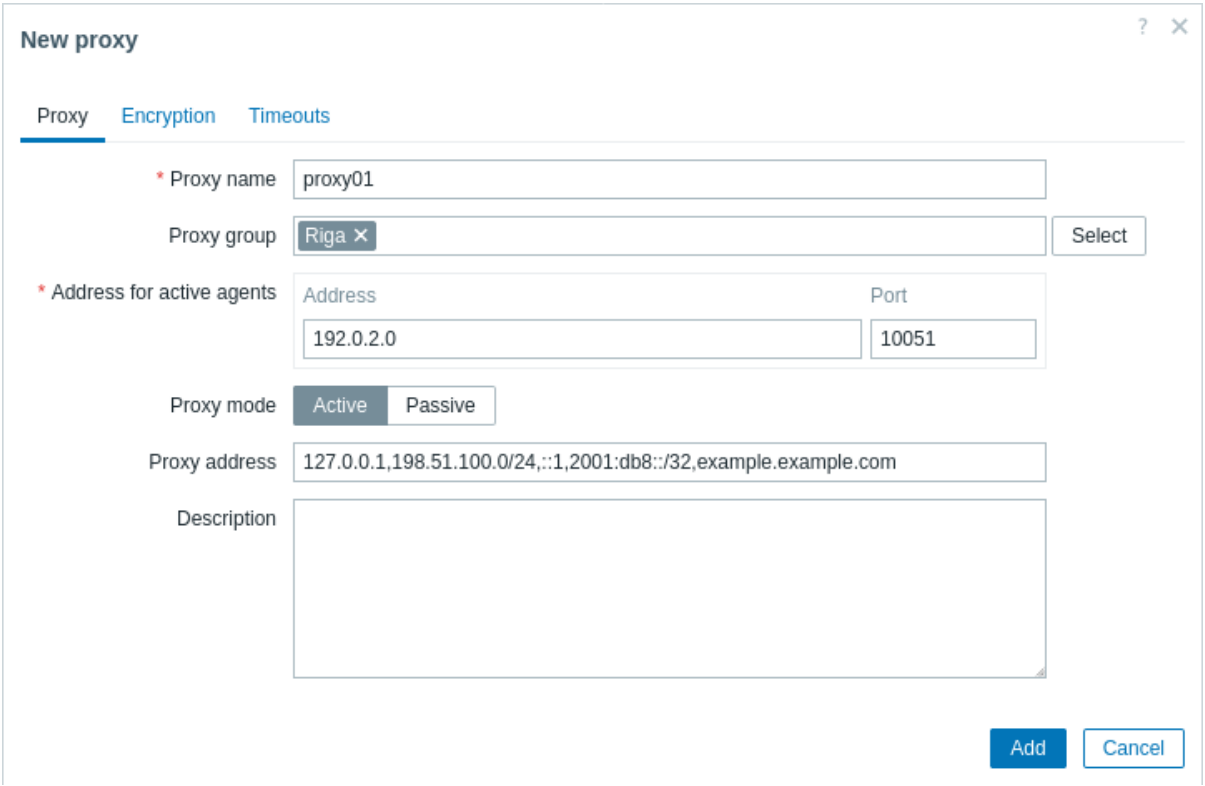
Możesz użyć wewnętrznej pozycji zabbix[wcache,history,pused], aby powiązać to zachowanie serwera Zabbix z metryką.

Konfiguracja Po zainstalowaniu i skonfigurowaniu proxy nadszedł czas, aby skonfigurować go we frontendzie Zabbix.

Dodawanie proxy

Aby skonfigurować proxy w frontend Zabbix:

- Przejdź do: *Administracja* > *Proxy*
- Kliknij *Utwórz proxy*



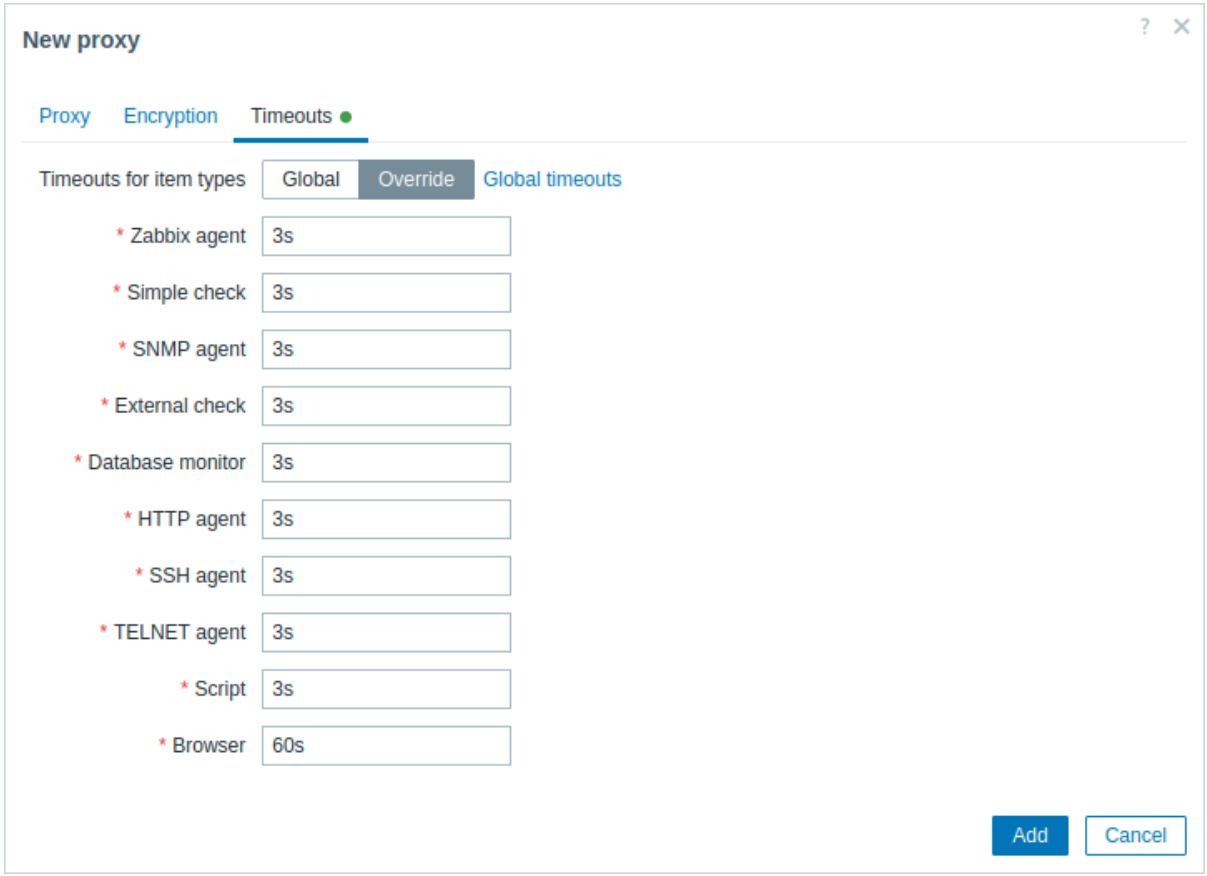
Parametr	Opis
Nazwa proxy	Wprowadź nazwę proxy. Musi to być taka sama nazwa jak w parametrze *Hostname* w pliku konfiguracyjnym proxy.
Grupa proxy	Wybierz jedną grupę proxy dla równoważenia obciążenia/wysokiej dostępności proxy.

Parametr	Opis
Adres dla aktywnych agentów	Wprowadź adres, z którym mają się łączyć monitorowane aktywne agenty lub sendery. Obsługiwane **tylko** dla agentów Zabbix 7.0 lub nowszych. Ten adres jest używany do łączenia zarówno z aktywnymi, jak i pasywnymi proxy. To pole jest dostępne tylko wtedy, gdy w polu *Grupa proxy* wybrano grupę proxy.
Adres	Adres IP/nazwa DNS, z którym należy się połączyć.
Port	Numer portu TCP (domyślnie 10051), z którym należy się połączyć. Obsługiwane są makra użytkownika.
Tryb proxy	Wybierz tryb proxy. **Aktywny** — proxy połączy się z serwer Zabbix i zażąda danych konfiguracyjnych **Pasywny** — serwer Zabbix łączy się z proxy Zwróć uwagę, że bez szyfrowanej komunikacji dane konfiguracyjne proxy (wrażliwe) mogą stać się dostępne dla stron mających dostęp do portu trappera serwer Zabbix podczas korzystania z aktywnego proxy. Jest to możliwe, ponieważ każdy może podszyć się pod aktywne proxy i zażądać danych konfiguracyjnych, jeśli nie odbywa się uwierzytelnianie lub adresy proxy nie są ograniczone w polu *Adres proxy*.
Adres proxy	Jeśli określono, żądania aktywnego proxy są akceptowane tylko z tej listy adresów IP rozdzielonych przecinkami, opcjonalnie w notacji CIDR, lub nazw DNS aktywnego proxy Zabbix. To pole jest dostępne tylko wtedy, gdy w polu *Tryb proxy* wybrano aktywne proxy. Makra nie są obsługiwane.
Interfejs	Wprowadź szczegóły interfejsu dla pasywnego proxy. To pole jest dostępne tylko wtedy, gdy w polu Tryb proxy wybrano pasywne proxy.
Adres	Adres IP/nazwa DNS pasywnego proxy.
Port	Numer portu TCP pasywnego proxy (domyślnie 10051). Obsługiwane są makra użytkownika.
Opis	Wprowadź opis proxy.

Karta **Szyfrowanie** umożliwia wymaganie szyfrowanych połączeń z proxy.

Parametr	Opis
Połączenia do proxy	Sposób, w jaki serwer łączy się z pasywnym proxy: bez szyfrowania (domyślnie), przy użyciu PSK (klucza współdzielonego) lub certyfikatu.
Połączenia z proxy	Wybierz, jaki typ połączeń jest dozwolony z aktywnego proxy. Jednocześnie można wybrać kilka typów połączeń (przydatne do testowania i przełączania na inny typ połączenia). Domyślnie ustawione jest „Bez szyfrowania”.
Wystawca	Dozwolony wystawca certyfikatu. Certyfikat jest najpierw weryfikowany przez CA (urząd certyfikacji). Jeśli jest prawidłowy i podpisany przez CA, pole *Wystawca* może zostać użyte do dalszego ograniczenia dozwolonego CA. To pole jest opcjonalne i przeznaczone do użycia, jeśli instalacja Zabbix korzysta z certyfikatów od wielu CA.
Temat	Dozwolony temat certyfikatu. Certyfikat jest najpierw weryfikowany przez CA. Jeśli jest prawidłowy i podpisany przez CA, pole *Temat* może zostać użyte do dopuszczenia tylko jednej wartości ciągu *Temat*. Jeśli to pole jest puste, akceptowany jest dowolny prawidłowy certyfikat podpisany przez skonfigurowany CA.
Tożsamość PSK	Ciąg identyfikujący klucz współdzielony. Nie umieszczaj poufnych informacji w tożsamości PSK, ponieważ jest ona przesyłana przez sieć bez szyfrowania, aby poinformować odbiorcę, którego PSK użyć.
PSK	Klucz współdzielony (ciąg szesnastkowy). Maksymalna długość: 512 cyfr szesnastkowych (256-bajtowy PSK), jeśli Zabbix używa biblioteki GnuTLS lub OpenSSL, 64 cyfry szesnastkowe (32-bajtowy PSK), jeśli Zabbix używa biblioteki mbed TLS (PolarSSL). Przykład: 1f87b595725ac58dd977beef14b97461a7c1045b9a1c963065002c5473194952

Karta **Limity czasu** umożliwia zastąpienie globalnych limitów czasu dla typów pozycji, które to obsługują.



Parametr	Opis
Limity czasu dla typów pozycji	Ustaw limit czasu pozycji (na podstawie jej typu): **Globalne** — użyj globalnego limitu czasu (wyświetlanego w wyszarzonym polu *Limit czasu* dla każdego typu pozycji); **Zastąp** — ustaw niestandardowy limit czasu (w polu *Limit czasu* dla każdego typu pozycji). Dozwolony zakres: 1 - 600 s (domyślnie: dziedziczone z globalnych limitów czasu). Obsługiwane są sufiksy czasu, np. 30s, 1m, oraz makra użytkownika. Kliknięcie odnośnika *Globalne limity czasu* umożliwia skonfigurowanie globalnych limitów czasu. Zwróć uwagę, że odnośnik *Globalne limity czasu* jest widoczny tylko dla użytkowników typu *Super admin* z uprawnieniami do sekcji frontend *Administracja* > *Ogólne*. Zwróć uwagę, że chociaż limity czasu na poziomie proxy zastępują limity globalne, same zostaną zastąpione przez indywidualne limity czasu pozycji, jeśli zostały skonfigurowane.

Note:
Jeśli główna wersja proxy nie jest zgodna z główną wersją serwer, obok *Limitów czasu dla typów pozycji* zostanie wyświetlona ikona z komunikatem po najechaniu „Limity czasu wyłączone, ponieważ wersje proxy i serwer nie są zgodne”. W takich przypadkach proxy będzie używać parametru `Timeout` z pliku konfiguracyjnego proxy.

Formularz edycji istniejącego proxy ma następujące dodatkowe przyciski:

- *Odśwież konfigurację* — odśwież konfigurację proxy
- *Klonuj* — utwórz nowe proxy na podstawie właściwości istniejącego proxy
- *Usuń* — usuń proxy

Konfiguracja hosta

Możesz określić, że dany host ma być monitorowany przez proxy lub grupę proxy w formularzu konfiguracji hosta, używając pola *Monitored by*.



Masowa aktualizacja hostów to kolejny sposób określenia, że hosty mają być monitorowane przez proxy lub grupę proxy.

1 Synchronizacja konfiguracji monitoringu

Przegląd

Ta strona zawiera szczegółowe informacje o aktualizacji konfiguracji monitorowania dla proxy, tj. o tym, jak zmiany wprowadzone w konfiguracji monitorowania na serwerze są synchronizowane z proxy.

Aktualizacja przyrostowa

Aktualizacja konfiguracji proxy jest przyrostowa. Podczas synchronizacji konfiguracji aktualizowane są tylko zmodyfikowane encje (zatem jeśli żadne encje nie zostały zmodyfikowane, nic nie zostanie wysłane). Takie podejście pozwala oszczędzać zasoby i ustawić krótszy interwał aktualizacji konfiguracji proxy (niemal natychmiastowy).

Zmiany konfiguracji proxy są śledzone za pomocą numerów rewizji. Tylko encje z rewizjami większymi niż rewizja konfiguracji proxy są uwzględniane w danych konfiguracyjnych wysyłanych do proxy.

Encje objęte synchronizacją konfiguracji są następujące:

Encja	Szczegóły
dane TLS autorejestracji	Wszystkie dane TLS autorejestracji.
wyrażenia	Wszystkie wyrażenia (wyrażenia regularne, tabele wyrażeń).
konfiguracja globalna	Konfiguracja globalna zdefiniowana w tabeli 'config'
host	Wszystkie właściwości, interfejsy, inwentarz, pozycje, preprocessing pozycji, parametry pozycji, scenariusze WWW hosta.
makra hosta	Wszystkie makra zdefiniowane dla hosta oraz wszystkie identyfikatory szablonów z nim powiązanych.
reguła wykrywania proxy	Reguły wykrywania i kontrole przypisane do proxy.

Oznacza to, że:

- Jeśli pozycja zostanie zmieniona na **hoście**, zsynchronizowana zostanie cała konfiguracja tego hosta.
- Jeśli **wyrażenie regularne** zostanie zmienione, zsynchronizowane zostaną wszystkie wyrażenia.

Wyjątkiem są makra hosta, które są wysyłane również wtedy, gdy cokolwiek na hoście zostało zmienione.

Polecenie `-R config_cache_reload` na proxy również zainicjuje aktualizację przyrostową.

Należy pamiętać, że pełna synchronizacja konfiguracji zostanie przeprowadzona przy uruchomieniu/ponownym uruchomieniu proxy, przełączeniu awaryjnym HA, jeśli token sesji uległ zmianie lub jeśli aktualizacja konfiguracji nie powiodła się na proxy, na przykład gdy połączenie zostało przerwane podczas odbierania danych konfiguracyjnych.

Parametry konfiguracji

Parametr **ProxyConfigFrequency** określa, jak często konfiguracja proxy jest synchronizowana z serwerem (domyślnie co 10 sekund).

Należy pamiętać, że ProxyConfigFrequency jest:

- parametrem serwera dla pasywnych proxy
- parametrem proxy dla aktywnych proxy

W aktywnych proxy parametr ProxyConfigFrequency jest nowym parametrem od wersji Zabbix 6.4 i musi być używany zamiast obecnie przestarzałego parametru ConfigFrequency.

Attention:
Jeśli używane są jednocześnie ProxyConfigFrequency i ConfigFrequency, proxy zapisze błąd w logu i zakończy działanie.

Obliczanie kolejek podczas konserwacji

Attention:
Proxy Zabbix nie jest świadomy okresów konserwacji; szczegóły znajdują się w sekcji Obliczanie kolejek podczas konserwacji.

2 Równoważenie obciążenia proxy i wysoka dostępność

Przegląd

Proxy Zabbix mogą być organizowane w grupy proxy, aby umożliwić równoważenie obciążenia proxy i wysoką dostępność.

Równoważenie obciążenia proxy i wysoka dostępność to automatyczna redystrybucja hostów między proxy w ramach grupy proxy:

- Jeśli proxy przejdzie w tryb offline, jego hosty zostaną przeniesione do innych proxy, co pozwoli utrzymać wysoką dostępność proxy.
- Jeśli proxy ma znacznie większą/mniejszą liczbę hostów niż inne proxy, jego hosty zostaną przeniesione do innych proxy w celu zrównoważenia obciążenia proxy.

Redystrybucja hostów działa tylko między proxy w grupie, które spełniają następujące warunki:

- Proxy działają w wersji Zabbix 7.0 lub nowszej.
- Wersja proxy jest zgodna z wersją serwera Zabbix. W przypadku używania Zabbix agent (passive) wersja proxy musi być zgodna z wersją agenta. Aktywne agenty wymagają jedynie Zabbix 7.0 lub nowszego.
- Grupa proxy ma stan online.
- Hosty są skonfigurowane do monitorowania przez grupę proxy, a nie przez pojedyncze proxy.

Note:
Stan grupy proxy można monitorować za pomocą sprawdzeń wewnętrznych przez dowolny host przypisany do grupy proxy. Jednak aby monitorować stan pojedynczego proxy w grupie, przypisz host do tego proxy; w przeciwnym razie wyniki mogą być niespójne.

Redystrybucja hostów

Równoważenie obciążenia proxy i wysoka dostępność są zarządzane przez serwer Zabbix za pomocą menedżera grup proxy, który stale monitoruje stan wszystkich proxy w każdej grupie proxy oraz rozkład ich hostów.

Wysoka dostępność proxy w obrębie grupy jest zapewniana przez mechanizm przełączania awaryjnego proxy: gdy proxy przechodzi w tryb offline, jego hosty są natychmiast redystrybuowane do innych proxy. Równoważenie obciążenia proxy również ma miejsce, ponieważ hosty są ponownie przypisywane do proxy z najmniejszą liczbą przypisanych hostów.

Dodatkowo równoważenie obciążenia proxy jest uruchamiane, gdy liczba hostów na proxy różni się od średniej grupowej o co najmniej 10 hostów oraz współczynnik 2 (nadmiar hostów lub niedobór hostów). Jeśli nierównowaga utrzymuje się po okresie karencji (10 x opóźnienie przełączenia awaryjnego), grupa proxy jest umieszczana w kolejce do redystrybucji hostów.

Menedżer grup proxy redystrybuuje hosty zgodnie z następującą logiką:

1. Oblicz średnią liczbę hostów na proxy.
2. Dla proxy z nadmiarem hostów — przenieś nadmiarowe hosty do nieprzypisanej puli proxy.
3. Dla proxy z niedoborem hostów — oblicz, ile hostów jest potrzebnych do osiągnięcia równowagi.
4. Usuń wymaganą liczbę hostów z proxy mających najwięcej hostów.
5. Przenieś nieprzypisane hosty do proxy mających najmniej hostów.

Przykłady redystrybucji hostów:

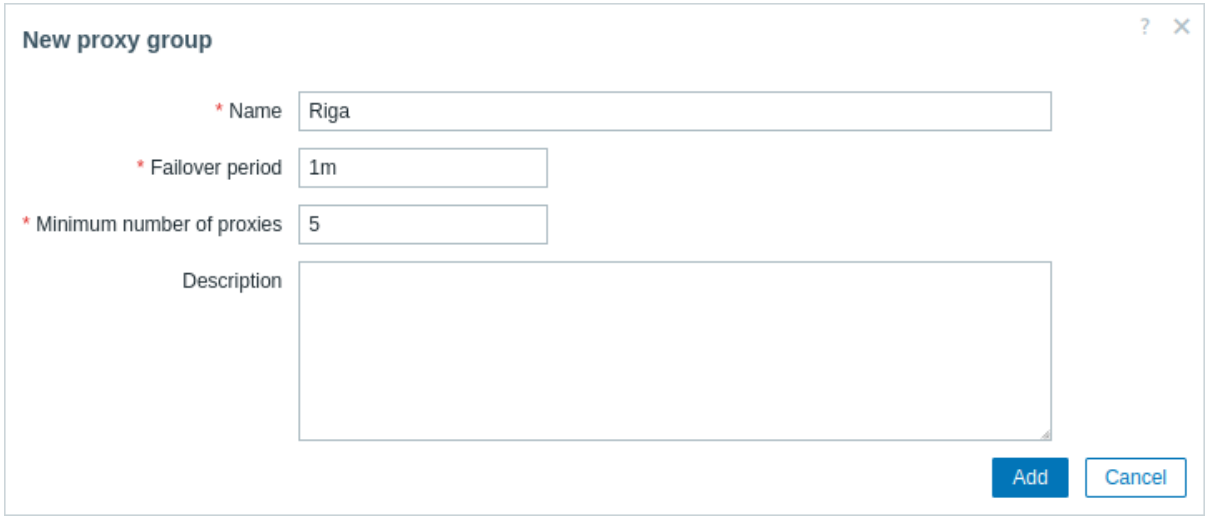
Hosty na proxy	Średnia grupowa	Ponowne przypisanie hostów
100	50	Tak
60	50	Nie
40	50	Nie
25	50	Tak
15	5	Tak
10	5	Nie

Attention:
Posiadanie mniej niż 10 hostów monitorowanych przez grupę proxy może prowadzić do nierównomiernego rozkładu hostów między proxy w grupie.

Konfigurowanie grupy proxy

Aby skonfigurować grupę proxy w Zabbix frontend:

1. Przejdź do *Administration* > *Proxy groups*
2. Kliknij *Create proxy group*



Parametr	Opis
Name	Nazwa grupy proxy.
Failover period	Okres w sekundach, w którym proxy w grupie proxy musi komunikować się z serwer Zabbix, aby był uznawany za online (domyślnie: 1m; zakres: 10s–15m). Jeśli proxy nie komunikuje się w tym okresie, stan proxy zmienia się na *Offline*, a jego hosty są natychmiast redystrybuowane do innych proxy. Równoważenie obciążenia proxy rozpoczyna się po 10 x tego okresu. Obsługuje sufiksy czasu (np. 30s, 1m) oraz makra użytkownika.
Minimum number of proxies	Minimalna liczba proxy online wymagana do utrzymania grupy proxy online (domyślnie: 1; zakres: 1–1000). Obsługuje makra użytkownika. Ta wartość powinna być mniejsza niż całkowita liczba proxy w grupie. Na przykład w grupie 10 proxy ustawienie minimum na 10 spowoduje przejście grupy w stan offline, jeśli jakiekolwiek proxy ulegnie awarii. Należy pamiętać, że proxy online w grupie offline nadal działają normalnie, ale równoważenie obciążenia/wysoka dostępność nie będą realizowane.
Description	Opis grupy proxy.
Proxies	Wyświetla listę maksymalnie pięciu proxy (jako linki lub zwykły tekst, w zależności od uprawnień użytkownika do proxy) podczas edycji grupy zawierającej proxy.

Konfigurowanie równoważenia obciążenia proxy

Aby używać równoważenia obciążenia proxy, należy skonfigurować grupę proxy w Zabbix frontend (zobacz wyżej) i upewnić się, że hosty są monitorowane przez grupę proxy, a nie przez pojedyncze proxy (można użyć masowej aktualizacji hostów, aby przenieść hosty z proxy do grupy proxy).

W przypadku korzystania z Zabbix agent należy również skonfigurować go w następujący sposób:

- Dla kontroli pasywnych należy wymienić wszystkie proxy z grupy proxy w parametrze Server.
- Dla kontroli aktywnych zaleca się wymienienie wszystkich proxy z grupy proxy lub serwera Zabbix w parametrze ServerActive. Należy pamiętać, że tylko Zabbix agent 7.0 (lub nowszy) będzie działać z grupami proxy w trybie aktywnym.

Jeśli parametr `ServerActive` zawiera tylko jedno proxy z grupy proxy (lub serwer Zabbix), agent nadal będzie mógł połączyć się z właściwym proxy. Gdy usługa agenta uruchomi się i połączy z określonym proxy, agent otrzyma i zapisze w pamięci podręcznej pełną listę adresów IP proxy oraz ich bieżące obciążenie w grupie. Następnie kontrole aktywne zostaną przekierowane do właściwego dostępnego proxy dla hosta, na podstawie bieżącego przypisania proxy-host w grupie proxy.

Warning:
Podanie tylko jednego proxy w parametrze `ServerActive` Zabbix agent może prowadzić do utraty danych monitorowania, jeśli agent zostanie uruchomiony/zrestartowany, gdy wskazane proxy będzie niedostępne.

Note:
Podczas korzystania z Zabbix sender żądania danych są również przekierowywane do właściwego dostępnego proxy dla hosta, na podstawie bieżącego przypisania proxy-host w grupie proxy. Jeśli jednak wysyłasz wartości wielu hostów z pliku wejściowego, użyj opcji −g, aby zapobiec wysłaniu danych do niewłaściwego proxy.

Zabbix agent musi również mieć możliwość łączenia się przez zaporę sieciową ze wszystkimi proxy w grupie proxy. W przeciwnym razie kontrole aktywne mogą zawieszać się lub kończyć niepowodzeniem podczas przekierowania albo przełączenia awaryjnego. Na przykład:

- Podczas kontroli aktywnych proxy może przekierować agenta do innego proxy. Jeśli to proxy jest blokowane przez zaporę sieciową, komunikacja zawiesi się podczas oczekiwania na odpowiedź.
- W stabilnych konfiguracjach wysokiej dostępności bez niedawnego równoważenia agenty mogą nigdy nie kontaktować się z zapasowymi proxy. Jeśli reguły zapory sieciowej uległy zmianie i nie zostały przetestowane, przełączenie awaryjne może się nie powieść.

Testowanie równoważenia obciążenia proxy

Aby przetestować równoważenie obciążenia proxy:

1. Skonfiguruj grupę proxy.
2. Upewnij się, że grupa proxy ma stan online.
3. Upewnij się, że hosty są monitorowane przez grupę proxy, a nie przez pojedyncze proxy (możesz użyć masowej aktualizacji, aby przenieść hosty z proxy do grupy proxy).
4. Odczekaj kilka sekund na aktualizację konfiguracji i dystrybucję hostów między proxy w grupie proxy. Obserwuj zmianę, odświeżając listę hostów w *Administracja* > *Proxy*.

Ważne uwagi

- Pułapki SNMP nie są obsługiwane przez proxy w grupie proxy.
- Kontrole zależne od konfiguracji zewnętrznej (np. skrypty dla kontroli zewnętrznych lub konfiguracja ODBC dla kontroli bazy danych) muszą mieć taką samą konfigurację na wszystkich proxy w grupie proxy.
- Kontrole bazy danych wymagają rozszerzonych uprawnień do obiektu bazy danych/serwera.
- Hosty VMware monitorowane przez grupę proxy będą losowo rozdzielane między proxy w grupie. Powoduje to, że każdy proxy buforuje wszystkie dane VMware, co skutkuje dodatkowym obciążeniem vCenter.
- Hosty utworzone na podstawie danych autorejestracji z proxy w grupie proxy są ustawiane jako monitorowane przez tę grupę proxy. Jednak hosty utworzone na podstawie danych wykrywania sieci z proxy w grupie proxy są ustawiane jako monitorowane przez ten proxy.

15 Szyfrowanie

Przegląd Zabbix obsługuje szyfrowaną komunikację między komponentami Zabbix z użyciem protokołu Transport Layer Security (TLS) w wersji 1.2 i 1.3 (w zależności od biblioteki kryptograficznej). Obsługiwane jest szyfrowanie oparte na certyfikatach oraz na kluczach współdzielonych.

Szyfrowanie można skonfigurować dla połączeń:

- Między Zabbix server, Zabbix proxy, Zabbix agent, usługą Zabbix web service oraz narzędziami zabbix_sender i zabbix_get
- Z bazą danych Zabbix z poziomu Zabbix frontend oraz server/proxy
- Między Zabbix frontend a Zabbix server

Szyfrowanie jest opcjonalne i można je skonfigurować dla poszczególnych komponentów:

- Niektóre proxy i agenty mogą być skonfigurowane do używania szyfrowania opartego na certyfikatach w komunikacji z serwerem, podczas gdy inne mogą używać szyfrowania opartego na kluczach współdzielonych, a jeszcze inne mogą nadal korzystać z nieszyfrowanej komunikacji (jak dotychczas).
- Serwer (proxy) może używać różnych konfiguracji szyfrowania dla różnych hostów.

Programy daemon Zabbix używają jednego portu nasłuchującego zarówno dla szyfrowanych, jak i nieszyfrowanych połączeń przychodzących. Dodanie szyfrowania nie wymaga otwierania nowych portów w zaporach sieciowych.

Ograniczenia

- Klucze prywatne są przechowywane w postaci zwykłego tekstu w plikach dostępnych do odczytu przez komponenty Zabbix podczas uruchamiania.

- Klucze współdzielone są wprowadzane w Zabbix frontend i przechowywane w bazie danych Zabbix w postaci zwykłego tekstu.
- Wbudowane szyfrowanie nie chroni komunikacji między serwerem WWW uruchamiającym Zabbix frontend a przeglądarką internetową użytkownika.
- Obecnie każde szyfrowane połączenie jest otwierane z pełnym uzgadnianiem TLS; nie są zaimplementowane buforowanie sesji ani bilety.
- Dodanie szyfrowania wydłuża czas sprawdzania pozycji i wykonywania akcji, w zależności od opóźnień sieciowych:
  - Na przykład, jeśli opóźnienie pakietów wynosi 100 ms, to otwarcie połączenia TCP i wysłanie niezaszyfrowanego żądania zajmuje około 200 ms. Przy szyfrowaniu dochodzi około 1000 ms na ustanowienie połączenia TLS.
  - Może być konieczne zwiększenie limitów czasu; w przeciwnym razie niektóre pozycje i akcje uruchamiające zdalne skrypty na agentach mogą działać przy połączeniach nieszyfrowanych, ale kończyć się błędem przekroczenia limitu czasu przy połączeniach szyfrowanych.
- Szyfrowanie nie jest obsługiwane przez wykrywanie sieci. Kontrole Zabbix agent wykonywane przez wykrywanie sieci będą nieszyfrowane, a jeśli Zabbix agent jest skonfigurowany tak, aby odrzucać nieszyfrowane połączenia, takie kontrole nie zakończą się powodzeniem.

Kompilowanie Zabbix z obsługą szyfrowania Aby obsługiwać szyfrowanie, Zabbix musi zostać skompilowany i połączony z jedną z obsługiwanych bibliotek kryptograficznych:

- GnuTLS - od wersji 3.1.18
- OpenSSL - wersje 1.0.1, 1.0.2, 1.1.0, 1.1.1, 3.0.x
- LibreSSL - testowano z wersjami 2.7.4, 2.8.2:
  - LibreSSL 2.6.x nie jest obsługiwany
  - LibreSSL jest obsługiwany jako kompatybilny zamiennik OpenSSL; nowe funkcje API `tls_*()` specyficzne dla LibreSSL nie są używane. Komponenty Zabbix skompilowane z LibreSSL nie będą mogły używać PSK, będzie można używać wyłącznie certyfikatów.

Note:
Więcej informacji o konfiguracji SSL dla frontend Zabbix można znaleźć w tych najlepszych praktykach.

Bibliotekę wybiera się przez podanie odpowiedniej opcji do skryptu „configure”:

- `--with-gnutls[=DIR]`
- `--with-openssl[=DIR]` (używane również dla LibreSSL)

Na przykład, aby skonfigurować źródła dla serwer i agent z użyciem *OpenSSL*, można użyć polecenia podobnego do poniższego:

```
./configure --enable-server --enable-agent --with-mysql --enable-ipv6 --with-net-snmp --with-libcurl --wit
```

Różne komponenty Zabbix mogą być kompilowane z różnymi bibliotekami kryptograficznymi (np. serwer z *OpenSSL*, agent z *GnuTLS*).

Attention:
Jeśli planujesz używać kluczy współdzielonych (PSK), rozważ użycie bibliotek *GnuTLS* lub *OpenSSL 1.1.0* (albo nowszych) w komponentach Zabbix korzystających z PSK. Biblioteki *GnuTLS* i *OpenSSL 1.1.0* obsługują pakiety szyfrów PSK z Perfect Forward Secrecy. Starsze wersje biblioteki *OpenSSL* (1.0.1, 1.0.2c) również obsługują PSK, ale dostępne pakiety szyfrów PSK nie zapewniają Perfect Forward Secrecy.

Zarządzanie szyfrowaniem połączeń Połączenia w Zabbix mogą używać:

- braku szyfrowania (domyślnie)
- szyfrowania opartego na certyfikatach RSA
- szyfrowania opartego na PSK

Istnieją dwa ważne parametry używane do określania szyfrowania między komponentami Zabbix:

- TLSConnect - określa, jakiego szyfrowania używać dla połączeń wychodzących (bez szyfrowania, PSK lub certyfikat)
- TLSAccept - określa, jakie typy połączeń są dozwolone dla połączeń przychodzących (bez szyfrowania, PSK lub certyfikat). Można podać jedną lub więcej wartości.

`TLSConnect` jest używany w plikach konfiguracyjnych Zabbix proxy (w trybie aktywnym określa tylko połączenia do serwer) oraz Zabbix agent (dla aktywnych kontroli). W Zabbix frontend odpowiednikiem TLSConnect jest pole *Connections to host* na karcie *Data collection → Hosts → <some host> → Encryption* oraz pole *Connections to proxy* na karcie *Administration → Proxies → <some proxy> → Encryption*. Jeśli skonfigurowany typ szyfrowania dla połączenia zawiedzie, żadne inne typy szyfrowania nie będą próbowane.

`TLSAccept` jest używany w plikach konfiguracyjnych Zabbix proxy (w trybie pasywnym określa tylko połączenia z serwer) oraz Zabbix agent (dla pasywnych kontroli). W Zabbix frontend odpowiednikiem TLSAccept jest pole *Connections from host* na karcie

Data collection → *Hosts* → *<some host>* → *Encryption* oraz pole *Connections from proxy* na karcie *Administration* → *Proxies* → *<some proxy>* → *Encryption*.

Zwykle konfiguruje się tylko jeden typ szyfrowania dla połączeń przychodzących. Możesz jednak chcieć zmienić typ szyfrowania, np. z braku szyfrowania na szyfrowanie oparte na certyfikatach, przy minimalnym czasie niedostępności i z możliwością wycofania zmian. Aby to osiągnąć:

- Ustaw `TLSAccept=unencrypted,cert` w pliku konfiguracyjnym agent i uruchom ponownie Zabbix agent
- Przetestuj połączenie z agent za pomocą zabbix_get, używając certyfikatu. Jeśli działa, możesz ponownie skonfigurować szyfrowanie dla tego agent w Zabbix frontend na karcie *Data collection* → *Hosts* → *<some host>* → *Encryption*, ustawiając *Connections to host* na "Certificate".
- Gdy pamięć podręczna konfiguracji serwer zostanie zaktualizowana (a konfiguracja proxy również zostanie zaktualizowana, jeśli host jest monitorowany przez proxy), połączenia z tym agent będą szyfrowane
- Jeśli wszystko działa zgodnie z oczekiwaniami, możesz ustawić `TLSAccept=cert` w pliku konfiguracyjnym agent i uruchomić ponownie Zabbix agent. Teraz agent będzie akceptował tylko szyfrowane połączenia oparte na certyfikatach. Połączenia bez szyfrowania oraz oparte na PSK będą odrzucane.

W podobny sposób działa to na serwer i proxy. Jeśli w Zabbix frontend w konfiguracji host pole *Connections from host* jest ustawione na "Certificate", to od agent (aktywne kontrole) i zabbix_sender (trapper pozycja) będą akceptowane tylko szyfrowane połączenia oparte na certyfikatach.

Najprawdopodobniej skonfigurujesz połączenia przychodzące i wychodzące tak, aby używały tego samego typu szyfrowania albo w ogóle bez szyfrowania. Technicznie jednak możliwa jest konfiguracja asymetryczna, np. szyfrowanie oparte na certyfikatach dla połączeń przychodzących i oparte na PSK dla połączeń wychodzących.

Konfiguracja szyfrowania dla każdego host jest wyświetlana w Zabbix frontend, w *Data collection* → *Hosts* w kolumnie *Agent encryption*. Na przykład:

Przykład	Connections to host	Allowed connections from host	Rejected connections from host
NONE	Bez szyfrowania	Bez szyfrowania	Szyfrowane, oparte na certyfikatach i oparte na PSK
CERT NONE PSK CERT	Szyfrowane, oparte na certyfikatach	Szyfrowane, oparte na certyfikatach	Bez szyfrowania i szyfrowane oparte na PSK
PSK NONE PSK CERT	Szyfrowane, oparte na PSK	Szyfrowane, oparte na PSK	Bez szyfrowania i szyfrowane oparte na certyfikatach
PSK NONE PSK CERT	Szyfrowane, oparte na PSK	Bez szyfrowania i szyfrowane oparte na PSK	Szyfrowane oparte na certyfikatach
CERT NONE PSK CERT	Szyfrowane, oparte na certyfikatach	Bez szyfrowania, szyfrowane oparte na PSK lub oparte na certyfikatach	-

Attention:
Połączenia domyślnie nie są szyfrowane. Szyfrowanie musi być skonfigurowane indywidualnie dla każdego host i proxy.

zabbix_get i zabbix_sender z szyfrowaniem Informacje o używaniu zabbix_get i zabbix_sender z szyfrowaniem można znaleźć w ich stronach podręcznika man.

Pakiety szyfrów Pakiety szyfrów są domyślnie konfigurowane wewnętrznie podczas uruchamiania Zabbix.

Obsługiwane są również pakiety szyfrów konfigurowane przez użytkownika dla GnuTLS i OpenSSL. Użytkownicy mogą skonfigurować pakiety szyfrów zgodnie ze swoimi politykami bezpieczeństwa. Korzystanie z tej funkcji jest opcjonalne (wbudowane domyślne pakiety szyfrów nadal działają).

W przypadku bibliotek kryptograficznych skompilowanych z ustawieniami domyślnymi wbudowane reguły Zabbix zwykle skutkują następującymi pakietami szyfrów (w kolejności od wyższego do niższego priorytetu):

Biblioteka	Pakiety szyfrów certyfikatów	Pakiety szyfrów PSK
GnuTLS 3.1.18	TLS_ECDHE_RSA_AES_128_GCM_SHA256 TLS_ECDHE_RSA_AES_128_CBC_SHA256 TLS_ECDHE_RSA_AES_128_CBC_SHA1 TLS_RSA_AES_128_GCM_SHA256 TLS_RSA_AES_128_CBC_SHA256 TLS_RSA_AES_128_CBC_SHA1	TLS_ECDHE_PSK_AES_128_CBC_SHA256 TLS_ECDHE_PSK_AES_128_CBC_SHA1 TLS_PSK_AES_128_GCM_SHA256 TLS_PSK_AES_128_CBC_SHA256 TLS_PSK_AES_128_CBC_SHA1

Biblioteka	Pakiety szyfrów certyfikatów	Pakiety szyfrów PSK
OpenSSL 1.0.2c	ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA256 ECDHE-RSA-AES128-SHA AES128-GCM-SHA256 AES128-SHA256 AES128-SHA	PSK-AES128-CBC-SHA
OpenSSL 1.1.0	ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA256 ECDHE-RSA-AES128-SHA AES128-GCM-SHA256 AES128-CCM8 AES128-CCM AES128-SHA256 AES128-SHA	ECDHE-PSK-AES128-CBC-SHA256 ECDHE-PSK-AES128-CBC-SHA PSK-AES128-GCM-SHA256 PSK-AES128-CCM8 PSK-AES128-CCM PSK-AES128-CBC-SHA256 PSK-AES128-CBC-SHA
OpenSSL 1.1.1d	TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 TLS_AES_128_GCM_SHA256 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA256 ECDHE-RSA-AES128-SHA AES128-GCM-SHA256 AES128-CCM8 AES128-CCM AES128-SHA256 AES128-SHA	TLS_CHACHA20_POLY1305_SHA256 TLS_AES_128_GCM_SHA256 ECDHE-PSK-AES128-CBC-SHA256 ECDHE-PSK-AES128-CBC-SHA PSK-AES128-GCM-SHA256 PSK-AES128-CCM8 PSK-AES128-CCM PSK-AES128-CBC-SHA256 PSK-AES128-CBC-SHA

Pakiety szyfrów skonfigurowane przez użytkownika Wbudowane kryteria wyboru pakietów szyfrów mogą zostać nadpisane przez pakiety szyfrów skonfigurowane przez użytkownika.

> **Attention:**
> Pakiety szyfrów skonfigurowane przez użytkownika to funkcja przeznaczona dla zaawansowanych użytkowników, którzy rozumieją pakiety szyfrów TLS, ich bezpieczeństwo oraz konsekwencje błędów, a także dobrze radzą sobie z rozwiązywaniem problemów z TLS.

Wbudowane kryteria wyboru pakietów szyfrów można nadpisać za pomocą następujących parametrów:

Zakres nadpisania	Parametr	Wartość	Opis
Wybór pakietów szyfrów dla certyfikatów	TLSCipherCert13	Prawidłowe cipher strings OpenSSL 1.1.1 dla protokołu TLS 1.3 (ich wartości są przekazywane do funkcji OpenSSL `SSL_CTX_set_ciphersuites()`).	Kryteria wyboru pakietów szyfrów opartych na certyfikatach dla TLS 1.3 Tylko OpenSSL 1.1.1 lub nowszy.
	TLSCipherCert	Prawidłowe cipher strings OpenSSL dla TLS 1.2 lub prawidłowe priority strings GnuTLS. Ich wartości są przekazywane odpowiednio do funkcji `SSL_CTX_set_cipher_list()` lub `gnutls_priority_init()`.	Kryteria wyboru pakietów szyfrów opartych na certyfikatach dla TLS 1.2/1.3 (GnuTLS), TLS 1.2 (OpenSSL)
Wybór pakietów szyfrów dla PSK	TLSCipherPSK13	Prawidłowe cipher strings OpenSSL 1.1.1 dla protokołu TLS 1.3 (ich wartości są przekazywane do funkcji OpenSSL `SSL_CTX_set_ciphersuites()`).	Kryteria wyboru pakietów szyfrów opartych na PSK dla TLS 1.3 Tylko OpenSSL 1.1.1 lub nowszy.
	TLSCipherPSK	Prawidłowe cipher strings OpenSSL dla TLS 1.2 lub prawidłowe priority strings GnuTLS. Ich wartości są przekazywane odpowiednio do funkcji `SSL_CTX_set_cipher_list()` lub `gnutls_priority_init()`.	Kryteria wyboru pakietów szyfrów opartych na PSK dla TLS 1.2/1.3 (GnuTLS), TLS 1.2 (OpenSSL)

Zakres nadpisania	Parametr	Wartość	Opis
Połączona lista pakietów szyfrów dla certyfikatu i PSK	TLSCipherAll13	Prawidłowe cipher strings OpenSSL 1.1.1 dla protokołu TLS 1.3 (ich wartości są przekazywane do funkcji OpenSSL `SSL_CTX_set_ciphersuites()`).	Kryteria wyboru pakietów szyfrów dla TLS 1.3 Tylko OpenSSL 1.1.1 lub nowszy.
	TLSCipherAll	Prawidłowe cipher strings OpenSSL dla TLS 1.2 lub prawidłowe priority strings GnuTLS. Ich wartości są przekazywane odpowiednio do funkcji `SSL_CTX_set_cipher_list()` lub `gnutls_priority_init()`.	Kryteria wyboru pakietów szyfrów dla TLS 1.2/1.3 (GnuTLS), TLS 1.2 (OpenSSL)

Aby nadpisać wybór pakietów szyfrów w narzędziach zabbix_get i zabbix_sender, użyj parametrów wiersza poleceń:

- `--tls-cipher13`
- `--tls-cipher`

Nowe parametry są opcjonalne. Jeśli parametr nie zostanie określony, zostanie użyta wewnętrzna wartość domyślna. Jeśli parametr jest zdefiniowany, nie może być pusty.

Jeśli ustawienie wartości TLSCipher* w bibliotece kryptograficznej zakończy się niepowodzeniem, serwer, proxy lub agent nie uruchomi się, a błąd zostanie zapisany w logu.

Ważne jest, aby rozumieć, kiedy każdy parametr ma zastosowanie.

Połączenia wychodzące

Najprostszy przypadek to połączenia wychodzące:

- Dla połączeń wychodzących z certyfikatem użyj TLSCipherCert13 lub TLSCipherCert
- Dla połączeń wychodzących z PSK użyj TLSCipherPSK13 lub TLSCipherPSK
- W przypadku narzędzi zabbix_get i zabbix_sender można użyć parametrów wiersza poleceń `--tls-cipher13` lub `--tls-cipher` (szyfrowanie jest jednoznacznie określone parametrem `--tls-connect`)

Połączenia przychodzące

W przypadku połączeń przychodzących jest to nieco bardziej skomplikowane, ponieważ reguły są specyficzne dla komponentów i konfiguracji.

Dla Zabbix **agent**:

Konfiguracja połączenia agenta	Konfiguracja szyfrów
TLSConnect=cert	TLSCipherCert, TLSCipherCert13
TLSConnect=psk	TLSCipherPSK, TLSCipherPSK13
TLSAccept=cert	TLSCipherCert, TLSCipherCert13
TLSAccept=psk	TLSCipherPSK, TLSCipherPSK13
TLSAccept=cert,psk	TLSCipherAll, TLSCipherAll13

Dla Zabbix **serwer** i **proxy**:

Konfiguracja połączenia	Konfiguracja szyfrów
Połączenia wychodzące używające PSK	TLSCipherPSK, TLSCipherPSK13
Połączenia przychodzące używające certyfikatów	TLSCipherAll, TLSCipherAll13
Połączenia przychodzące używające PSK, jeśli serwer nie ma certyfikatu	TLSCipherPSK, TLSCipherPSK13
Połączenia przychodzące używające PSK, jeśli serwer ma certyfikat	TLSCipherAll, TLSCipherAll13

W dwóch powyższych tabelach można zauważyć pewną prawidłowość:

- TLSCipherAll i TLSCipherAll13 mogą być określone tylko wtedy, gdy używana jest połączona lista pakietów szyfrujących opartych na certyfikatach **i** PSK. Występuje to w dwóch przypadkach: serwer (proxy) ze skonfigurowanym certyfikatem (pakiety szyfrujące PSK są zawsze konfigurowane na serwerze, proxy, jeśli biblioteka kryptograficzna obsługuje PSK), agent skonfigurowany do akceptowania zarówno przychodzących połączeń opartych na certyfikatach, jak i na PSK
- w pozostałych przypadkach wystarczające są TLSCipherCert* i/lub TLSCipherPSK*

Poniższe tabele pokazują wbudowane wartości domyślne `TLSCipher*`. Mogą one być dobrym punktem wyjścia do zdefiniowania własnych wartości niestandardowych.

Parametr	GnuTLS 3.6.12
TLSCipherCert	NONE:+VERS-TLS1.2:+ECDHE-RSA:+RSA:+AES-128-GCM:+AES-128-CBC:+AEAD:+SHA256:+SHA1:+CURVE-ALL:+COMP-NULL:+SIGN-ALL:+CTYPE-X.509
TLSCipherPSK	NONE:+VERS-TLS1.2:+ECDHE-PSK:+PSK:+AES-128-GCM:+AES-128-CBC:+AEAD:+SHA256:+SHA1:+CURVE-ALL:+COMP-NULL:+SIGN-ALL
TLSCipherAll	NONE:+VERS-TLS1.2:+ECDHE-RSA:+RSA:+ECDHE-PSK:+PSK:+AES-128-GCM:+AES-128-CBC:+AEAD:+SHA256:+SHA1:+CURVE-ALL:+COMP-NULL:+SIGN-ALL:+CTYPE-X.509

Parametr	OpenSSL 1.1.1d [1]
TLSCipherCert13	
TLSCipherCert	EECDH+aRSA+AES128:RSA+aRSA+AES128
TLSCipherPSK13	TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256
TLSCipherPSK	kECDHEPSK+AES128:kPSK+AES128
TLSCipherAll13	
TLSCipherAll	EECDH+aRSA+AES128:RSA+aRSA+AES128:kECDHEPSK+AES128:kPSK+AES128

[1] Wartości domyślne są inne dla starszych wersji OpenSSL (1.0.1, 1.0.2, 1.1.0), dla LibreSSL oraz jeśli OpenSSL został skompilowany bez obsługi PSK.

Przykłady pakietów szyfrujących skonfigurowanych przez użytkownika

Poniżej przedstawiono przykłady pakietów szyfrujących skonfigurowanych przez użytkownika:

- Testowanie ciągów szyfrów i zezwalanie tylko na pakiety szyfrujące z PFS
- Przełączanie z AES128 na AES256

Testowanie ciągów szyfrów i zezwalanie tylko na pakiety szyfrów PFS

Aby zobaczyć, które pakiety szyfrów zostały wybrane, należy ustawić `DebugLevel=4` w pliku konfiguracyjnym lub użyć opcji `-vv` dla zabbix_sender.

Przed uzyskaniem żądanych pakietów szyfrów może być konieczne poeksperymentowanie z parametrami `TLSCipher*`. Wielokrotne restartowanie serwera Zabbix, proxy lub agent tylko po to, aby dostosować parametry `TLSCipher*`, jest niewygodne. Wygodniejszymi opcjami są użycie zabbix_sender lub polecenia `openssl`. Pokażmy oba sposoby.

1. Użycie zabbix_sender.

Utwórzmy testowy plik konfiguracyjny, na przykład `/home/zabbix/test.conf`, ze składnią pliku `zabbix_agentd.conf`:

```
Hostname=nonexisting
ServerActive=nonexisting

TLSConnect=cert
TLSCAFile=/home/zabbix/ca.crt
TLSCertFile=/home/zabbix/agent.crt
TLSKeyFile=/home/zabbix/agent.key
TLSPSKIdentity=nonexisting
TLSPSKFile=/home/zabbix/agent.psk
```

Do tego przykładu potrzebne są prawidłowe certyfikaty CA i agent oraz PSK. Dostosuj ścieżki i nazwy plików certyfikatów oraz PSK do swojego środowiska.

Jeśli nie używasz certyfikatów, a tylko PSK, możesz utworzyć prostszy plik testowy:

```
Hostname=nonexisting
ServerActive=nonexisting
```

```
TLSConnect=psk
TLSPSKIdentity=nonexisting
TLSPSKFile=/home/zabbix/agentd.psk
```

Wybrane pakiety szyfrów można zobaczyć, uruchamiając zabbix_sender (przykład skompilowany z OpenSSL 1.1.d):

```
$ zabbix_sender -vv -c /home/zabbix/test.conf -k nonexisting_item -o 1 2>&1 | grep ciphersuites
zabbix_sender [41271]: DEBUG: zbx_tls_init_child() certificate ciphersuites: TLS_AES_256_GCM_SHA384 TLS_
zabbix_sender [41271]: DEBUG: zbx_tls_init_child() PSK ciphersuites: TLS_CHACHA20_POLY1305_SHA256 TLS_AE
zabbix_sender [41271]: DEBUG: zbx_tls_init_child() certificate and PSK ciphersuites: TLS_AES_256_GCM_SHA
```

Tutaj widać pakiety szyfrów wybrane domyślnie. Te wartości domyślne zostały dobrane tak, aby zapewnić interoperacyjność z agentami Zabbix działającymi w systemach ze starszymi wersjami OpenSSL (od 1.0.1).

W nowszych systemach można zwiększyć bezpieczeństwo, zezwalając tylko na kilka pakietów szyfrów, np. tylko na pakiety szyfrów z PFS (Perfect Forward Secrecy). Spróbujmy zezwolić tylko na pakiety szyfrów z PFS przy użyciu parametrów `TLSCipher*`.

Attention:
Wynik nie będzie interoperacyjny z systemami używającymi OpenSSL 1.0.1 i 1.0.2, jeśli używany jest PSK. Szyfrowanie oparte na certyfikatach powinno działać.

Dodaj dwie linie do pliku konfiguracyjnego `test.conf`:

```
TLSCipherCert=EECDH+aRSA+AES128
TLSCipherPSK=kECDHEPSK+AES128
```

i przetestuj ponownie:

```
$ zabbix_sender -vv -c /home/zabbix/test.conf -k nonexisting_item -o 1 2>&1 | grep ciphersuites
zabbix_sender [42892]: DEBUG: zbx_tls_init_child() certificate ciphersuites: TLS_AES_256_GCM_SHA384 TLS_
zabbix_sender [42892]: DEBUG: zbx_tls_init_child() PSK ciphersuites: TLS_CHACHA20_POLY1305_SHA256 TLS_AE
zabbix_sender [42892]: DEBUG: zbx_tls_init_child() certificate and PSK ciphersuites: TLS_AES_256_GCM_SHA
```

Listy „certificate ciphersuites" i „PSK ciphersuites" uległy zmianie — są krótsze niż wcześniej i zawierają tylko pakiety szyfrów TLS 1.3 oraz pakiety szyfrów TLS 1.2 ECDHE-*, zgodnie z oczekiwaniami.

2. TLSCipherAll i TLSCipherAll13 nie mogą być testowane za pomocą zabbix_sender; nie wpływają one na wartość „certificate and PSK ciphersuites" pokazaną w powyższym przykładzie. Aby dostroić TLSCipherAll i TLSCipherAll13, trzeba eksperymentować z agent, proxy lub serwer.

Aby więc zezwolić tylko na pakiety szyfrów PFS, może być konieczne dodanie maksymalnie trzech parametrów

```
TLSCipherCert=EECDH+aRSA+AES128
TLSCipherPSK=kECDHEPSK+AES128
TLSCipherAll=EECDH+aRSA+AES128:kECDHEPSK+AES128
```

do zabbix_agentd.conf, zabbix_proxy.conf i zabbix_server_conf, jeśli każdy z nich ma skonfigurowany certyfikat, a agent ma również PSK.

Jeśli środowisko Zabbix używa wyłącznie szyfrowania opartego na PSK i nie używa certyfikatów, wystarczy tylko jeden parametr:

```
TLSCipherPSK=kECDHEPSK+AES128
```

Teraz, gdy już rozumiesz, jak to działa, możesz testować wybór pakietów szyfrów nawet poza Zabbix, za pomocą polecenia `openssl`. Przetestujmy wszystkie trzy wartości parametrów `TLSCipher*`:

```
$ openssl ciphers EECDH+aRSA+AES128 | sed 's/:/ /g'
TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 TLS_AES_128_GCM_SHA256 ECDHE-RSA-AES128-GCM-SHA256 E
$ openssl ciphers kECDHEPSK+AES128 | sed 's/:/ /g'
TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 TLS_AES_128_GCM_SHA256 ECDHE-PSK-AES128-CBC-SHA256 E
$ openssl ciphers EECDH+aRSA+AES128:kECDHEPSK+AES128 | sed 's/:/ /g'
TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 TLS_AES_128_GCM_SHA256 ECDHE-RSA-AES128-GCM-SHA256 E
```

Możesz preferować `openssl ciphers` z opcją `-V`, aby uzyskać bardziej szczegółowe dane wyjściowe:

```
$ openssl ciphers -V EECDH+aRSA+AES128:kECDHEPSK+AES128
           0x13,0x02 - TLS_AES_256_GCM_SHA384  TLSv1.3 Kx=any      Au=any  Enc=AESGCM(256) Mac=AEAD
           0x13,0x03 - TLS_CHACHA20_POLY1305_SHA256 TLSv1.3 Kx=any      Au=any  Enc=CHACHA20/POLY1305(256
           0x13,0x01 - TLS_AES_128_GCM_SHA256  TLSv1.3 Kx=any      Au=any  Enc=AESGCM(128) Mac=AEAD
           0xC0,0x2F - ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH     Au=RSA  Enc=AESGCM(128) Mac=AEAD
           0xC0,0x27 - ECDHE-RSA-AES128-SHA256 TLSv1.2 Kx=ECDH     Au=RSA  Enc=AES(128)  Mac=SHA256
```

```
0xC0,0x13 - ECDHE-RSA-AES128-SHA     TLSv1 Kx=ECDH     Au=RSA  Enc=AES(128)  Mac=SHA1
0xC0,0x37 - ECDHE-PSK-AES128-CBC-SHA256 TLSv1 Kx=ECDHEPSK Au=PSK  Enc=AES(128)  Mac=SHA256
0xC0,0x35 - ECDHE-PSK-AES128-CBC-SHA TLSv1 Kx=ECDHEPSK Au=PSK  Enc=AES(128)  Mac=SHA1
```

Podobnie można testować ciągi priorytetów dla GnuTLS:

```
$ gnutls-cli -l --priority=NONE:+VERS-TLS1.2:+ECDHE-RSA:+AES-128-GCM:+AES-128-CBC:+AEAD:+SHA256:+CURVE-A
Cipher suites for NONE:+VERS-TLS1.2:+ECDHE-RSA:+AES-128-GCM:+AES-128-CBC:+AEAD:+SHA256:+CURVE-ALL:+COMP-
TLS_ECDHE_RSA_AES_128_GCM_SHA256                        0xc0, 0x2f      TLS1.2
TLS_ECDHE_RSA_AES_128_CBC_SHA256                        0xc0, 0x27      TLS1.2

Protocols: VERS-TLS1.2
Ciphers: AES-128-GCM, AES-128-CBC
MACs: AEAD, SHA256
Key Exchange Algorithms: ECDHE-RSA
Groups: GROUP-SECP256R1, GROUP-SECP384R1, GROUP-SECP521R1, GROUP-X25519, GROUP-X448, GROUP-FFDHE2048, GR
PK-signatures: SIGN-RSA-SHA256, SIGN-RSA-PSS-SHA256, SIGN-RSA-PSS-RSAE-SHA256, SIGN-ECDSA-SHA256, SIGN-E
```

Przełączanie z AES128 na AES256

Zabbix używa AES128 jako wbudowanego domyślnego szyfrowania danych. Załóżmy, że używasz certyfikatów i chcesz przełączyć się na AES256 w OpenSSL 1.1.1.

Można to osiągnąć, dodając odpowiednie parametry w `zabbix_server.conf`:

```
TLSCAFile=/home/zabbix/ca.crt
TLSCertFile=/home/zabbix/server.crt
TLSKeyFile=/home/zabbix/server.key
TLSCipherCert13=TLS_AES_256_GCM_SHA384
TLSCipherCert=EECDH+aRSA+AES256:-SHA1:-SHA384
TLSCipherPSK13=TLS_CHACHA20_POLY1305_SHA256
TLSCipherPSK=kECDHEPSK+AES256:-SHA1
TLSCipherAll13=TLS_AES_256_GCM_SHA384
TLSCipherAll=EECDH+aRSA+AES256:-SHA1:-SHA384
```

Attention:
Chociaż używane będą tylko pakiety szyfrów związane z certyfikatami, parametry `TLSCipherPSK*` również są zdefiniowane, aby uniknąć ich wartości domyślnych, które obejmują mniej bezpieczne szyfry dla szerszej interoperacyjności. Pakietów szyfrów PSK nie można całkowicie wyłączyć na serwer/proxy.

A w `zabbix_agentd.conf`:

```
TLSConnect=cert
TLSAccept=cert
TLSCAFile=/home/zabbix/ca.crt
TLSCertFile=/home/zabbix/agent.crt
TLSKeyFile=/home/zabbix/agent.key
TLSCipherCert13=TLS_AES_256_GCM_SHA384
TLSCipherCert=EECDH+aRSA+AES256:-SHA1:-SHA384
```

1 Korzystanie z certyfikatów

Przegląd

Zabbix może używać certyfikatów RSA w formacie PEM, podpisanych przez publiczny lub wewnętrzny urząd certyfikacji (CA).

Weryfikacja certyfikatu jest wykonywana względem wstępnie skonfigurowanego certyfikatu CA. Opcjonalnie można używać list unieważnionych certyfikatów (CRL).

Każdy komponent Zabbix może mieć skonfigurowany tylko jeden certyfikat.

Aby uzyskać więcej informacji na temat konfigurowania i obsługi wewnętrznego CA, generowania i podpisywania żądań certyfikatów oraz unieważniania certyfikatów, zapoznaj się z samouczkami, takimi jak OpenSSL PKI Tutorial v2.0.

Dokładnie rozważ i przetestuj rozszerzenia swoich certyfikatów. Więcej szczegółów znajduje się w sekcji Ograniczenia dotyczące używania rozszerzeń certyfikatów X.509 v3.

Parametry konfiguracji certyfikatów

Poniższe parametry konfiguracji są obsługiwane przy konfigurowaniu certyfikatów w komponentach Zabbix.

Parametr	Wymagany	Opis
TLSCAFile	tak	Pełna ścieżka do pliku zawierającego certyfikaty nadrzędnego urzędu(ów) certyfikacji (CA) do weryfikacji certyfikatu strony komunikacji. W przypadku używania łańcucha certyfikatów z wieloma elementami należy uporządkować certyfikaty tak, aby najpierw znajdowały się certyfikaty CA niższego poziomu, a następnie certyfikaty CA wyższego poziomu. Certyfikaty z wielu urzędów certyfikacji mogą być zawarte w jednym pliku.
TLSCRLFile	nie	Pełna ścieżka do pliku zawierającego listy unieważnionych certyfikatów (CRL).
TLSCertFile	tak	Pełna ścieżka do pliku zawierającego certyfikat. W przypadku używania łańcucha certyfikatów z wieloma elementami należy uporządkować certyfikaty tak, aby najpierw znajdował się certyfikat serwera, proxy lub agenta, następnie certyfikaty CA niższego poziomu, a na końcu certyfikaty CA wyższego poziomu.
TLSKeyFile	tak	Pełna ścieżka do pliku zawierającego klucz prywatny. Należy upewnić się, że plik ten jest dostępny do odczytu wyłącznie dla użytkownika Zabbix, ustawiając odpowiednie prawa dostępu.
TLSServerCertIssuer	nie	Dozwolony wystawca certyfikatu serwera.
TLSServerCertSubject	nie	Dozwolony podmiot certyfikatu serwera.

Przykłady konfiguracji

Po skonfigurowaniu wymaganych certyfikatów skonfiguruj komponenty Zabbix tak, aby używały szyfrowania opartego na certyfikatach.

Poniżej znajdują się szczegółowe kroki konfiguracji dla:

- serwera Zabbix
- proxy Zabbix
- agenta Zabbix

Serwer Zabbix

1. Przygotuj plik certyfikatu CA.

Aby weryfikować certyfikaty partnera, serwer Zabbix musi mieć dostęp do pliku zawierającego certyfikaty głównych, samopodpisanych głównych urzędów certyfikacji CA. Na przykład, jeśli wymagane są certyfikaty z dwóch niezależnych głównych urzędów CA, umieść je w pliku `/home/zabbix/zabbix_ca_file.crt`:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: DC=com, DC=zabbix, O=Zabbix SIA, OU=Development group, CN=Root1 CA
            ...
        Subject: DC=com, DC=zabbix, O=Zabbix SIA, OU=Development group, CN=Root1 CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
            ...
        X509v3 extensions:
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE
            ...
-----BEGIN CERTIFICATE-----
MIID2jCCAsKgAwIBAgIBATANBgkqhkiG9w0BAQUFADB+MRMwEQYKCZImiZPyLGQB
....
9wEzdN8uTrqoyU78gi12npLj08LegRKjb5hFTVmO
-----END CERTIFICATE-----
Certificate:
```

```
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: DC=com, DC=zabbix, O=Zabbix SIA, OU=Development group, CN=Root2 CA
            ...
        Subject: DC=com, DC=zabbix, O=Zabbix SIA, OU=Development group, CN=Root2 CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
            ....
        X509v3 extensions:
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE
            ....
-----BEGIN CERTIFICATE-----
MIID3DCCAsSgAwIBAgIBATANBgkqhkiG9w0BAQUFADB/MRMwEQYKCZImiZPyLGQB
...
vdGNYoSfvu41GQAR5Vj5FnRJRzv5XQOZ3B6894GY1zY=
-----END CERTIFICATE-----
```

2. Umieść certyfikat/łańcuch certyfikatów serwera Zabbix w pliku, na przykład w `/home/zabbix/zabbix_server.crt`. Pierwszy certyfikat to certyfikat serwera Zabbix, po którym następuje certyfikat pośredniego urzędu CA:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: DC=com, DC=zabbix, O=Zabbix SIA, OU=Development group, CN=Signing CA
        ...
        Subject: DC=com, DC=zabbix, O=Zabbix SIA, OU=Development group, CN=Zabbix server
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                ...
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Basic Constraints:
                CA:FALSE
            ...
-----BEGIN CERTIFICATE-----
MIIECDCCAvCgAwIBAgIBATANBgkqhkiG9w0BAQUFADCBgTETMBEGCgmSJomT8ixk
...
h02u1GHiy46GI+xfR3LsPwFKlkTaaLaL/6aaoQ==
-----END CERTIFICATE-----
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 2 (0x2)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: DC=com, DC=zabbix, O=Zabbix SIA, OU=Development group, CN=Root1 CA
        ...
        Subject: DC=com, DC=zabbix, O=Zabbix SIA, OU=Development group, CN=Signing CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
            ...
        X509v3 extensions:
            X509v3 Key Usage: critical
```

```
                Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
        ...
-----BEGIN CERTIFICATE-----
MIID4TCCAsmgAwIBAgIBAjANBgkqhkiG9w0BAQUFADB+MRMwEQYKCZImiZPyLGQB
...
dyCeWnvL7u5sd6ffo8iRny0QzbHKmQt/wUtcVIvWXdMIFJM0Hw==
-----END CERTIFICATE-----
```

Note:
Używaj wyłącznie atrybutów wymienionych powyżej zarówno dla certyfikatów klienta, jak i serwera, aby nie wpływać na proces weryfikacji certyfikatu. Na przykład OpenSSL może nie ustanowić szyfrowanego połączenia, jeśli używane są rozszerzenia *X509v3 Subject Alternative Name* lub *Netscape Cert Type*. Więcej informacji znajduje się w sekcji Ograniczenia dotyczące używania rozszerzeń certyfikatów X.509 v3.

3. Umieść klucz prywatny serwera Zabbix w pliku, na przykład w `/home/zabbix/zabbix_server.key`:

```
-----BEGIN PRIVATE KEY-----
MIIEwAIBADANBgkqhkiG9w0BAQEFAASCBKowggSmAgEAAoIBAQC9tIXIJoVnNXDl
...
IJLkhbybBYEf47MLhffWa7XvZTY=
-----END PRIVATE KEY-----
```

4. Edytuj parametry konfiguracji TLS w pliku konfiguracyjnym serwera Zabbix:

```
TLSCAFile=/home/zabbix/zabbix_ca_file.crt
TLSCertFile=/home/zabbix/zabbix_server.crt
TLSKeyFile=/home/zabbix/zabbix_server.key
```

Zabbix proxy

1. Przygotuj pliki z certyfikatami głównego urzędu certyfikacji (CA), certyfikatem/łańcuchem certyfikatów Zabbix proxy oraz kluczem prywatnym, zgodnie z opisem w sekcji Zabbix server. Następnie odpowiednio edytuj parametry `TLSCAFile`, `TLSCertFile` i `TLSKeyFile` w pliku konfiguracyjnym Zabbix proxy.

2. Edytuj dodatkowe parametry TLS w pliku konfiguracyjnym Zabbix proxy:

- Dla aktywnego proxy: `TLSConnect=cert`
- Dla pasywnego proxy: `TLSAccept=cert`

Note:
Aby zwiększyć bezpieczeństwo proxy, możesz również ustawić parametry `TLSServerCertIssuer` i `TLSServerCertSubject`. Więcej informacji znajduje się w sekcji Ograniczanie dozwolonego wystawcy i podmiotu certyfikatu.

Parametry TLS w końcowym pliku konfiguracyjnym proxy mogą wyglądać następująco:

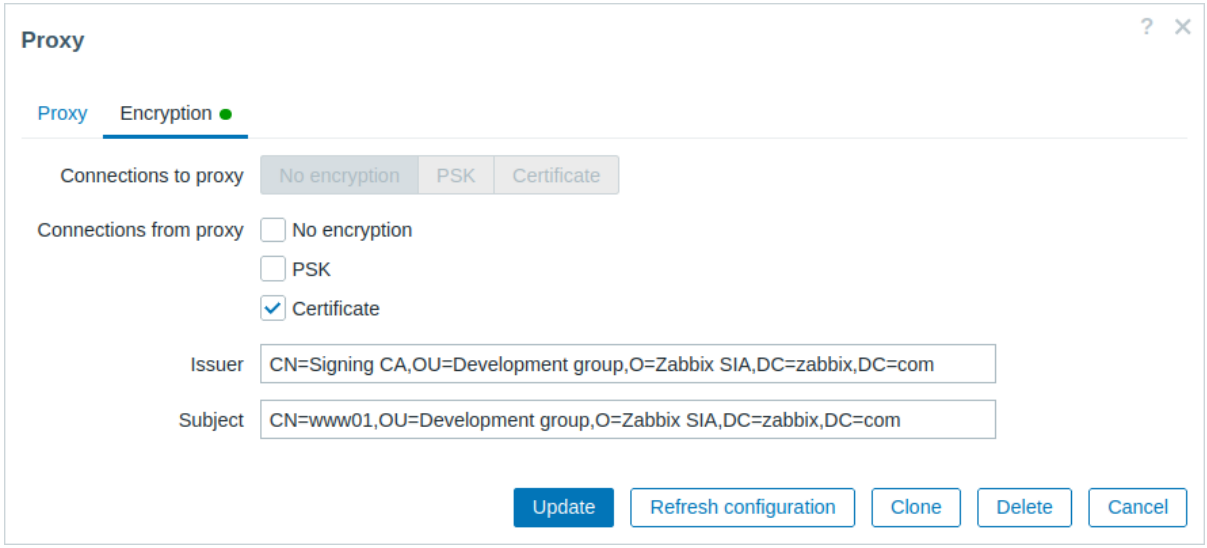
```
TLSConnect=cert
TLSAccept=cert
TLSCAFile=/home/zabbix/zabbix_ca_file.crt
TLSServerCertIssuer=CN=Signing CA,OU=Development group,O=Zabbix SIA,DC=zabbix,DC=com
TLSServerCertSubject=CN=Zabbix server,OU=Development group,O=Zabbix SIA,DC=zabbix,DC=com
TLSCertFile=/home/zabbix/zabbix_proxy.crt
TLSKeyFile=/home/zabbix/zabbix_proxy.key
```

3. Skonfiguruj szyfrowanie dla tego proxy w Zabbix frontend:

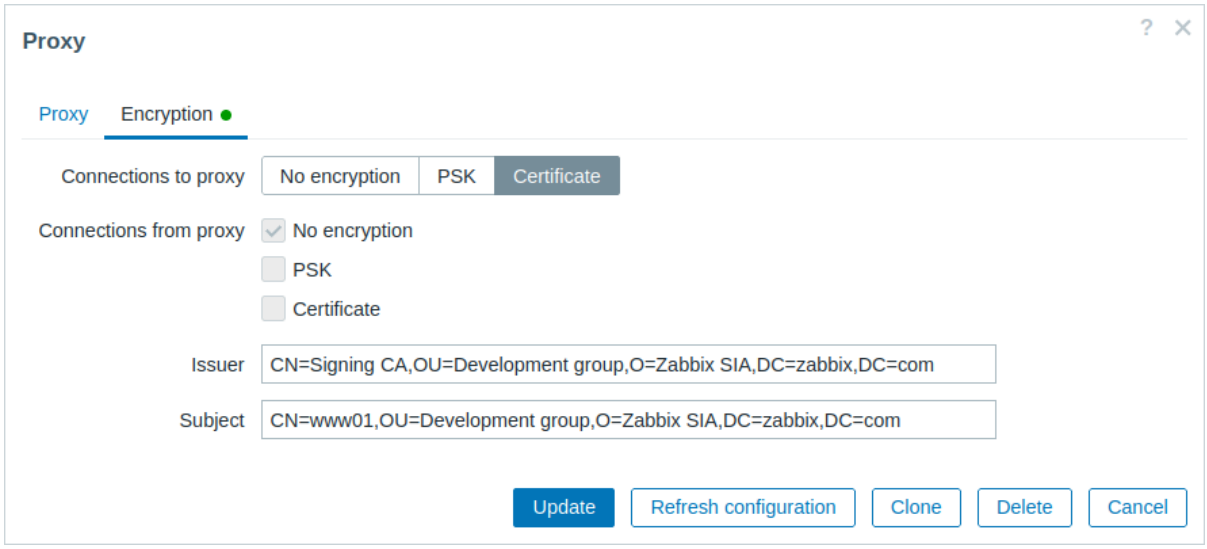
- Przejdź do: *Administracja* → *Proxy*.
- Wybierz proxy i kliknij kartę *Szyfrowanie*.

W poniższych przykładach pola *Issuer* i *Subject* są wypełnione. Więcej informacji o tym, dlaczego i jak używać tych pól, znajduje się w sekcji Ograniczanie dozwolonego wystawcy i podmiotu certyfikatu.

Dla aktywnego proxy:



Dla pasywnego proxy:



Zabbix agent

1. Przygotuj pliki z certyfikatami CA najwyższego poziomu, certyfikatem/łańcuchem certyfikatów Zabbix agent oraz kluczem prywatnym, zgodnie z opisem w sekcji Zabbix server. Następnie odpowiednio edytuj parametry `TLSCAFile`, `TLSCertFile` i `TLSKeyFile` w pliku konfiguracyjnym Zabbix agent.

2. Edytuj dodatkowe parametry TLS w pliku konfiguracyjnym Zabbix agent:

- Dla aktywnego agent: `TLSConnect=cert`
- Dla pasywnego agent: `TLSAccept=cert`

Note:
Aby zwiększyć bezpieczeństwo agent, możesz ustawić parametry `TLSServerCertIssuer` i `TLSServerCertSubject`. Więcej informacji znajdziesz w sekcji Ograniczanie dozwolonego wystawcy i podmiotu certyfikatu.

Parametry TLS w końcowym pliku konfiguracyjnym agent mogą wyglądać następująco. Zwróć uwagę, że przykład zakłada, iż host jest monitorowany przez proxy, dlatego zostało ono określone jako Subject certyfikatu:

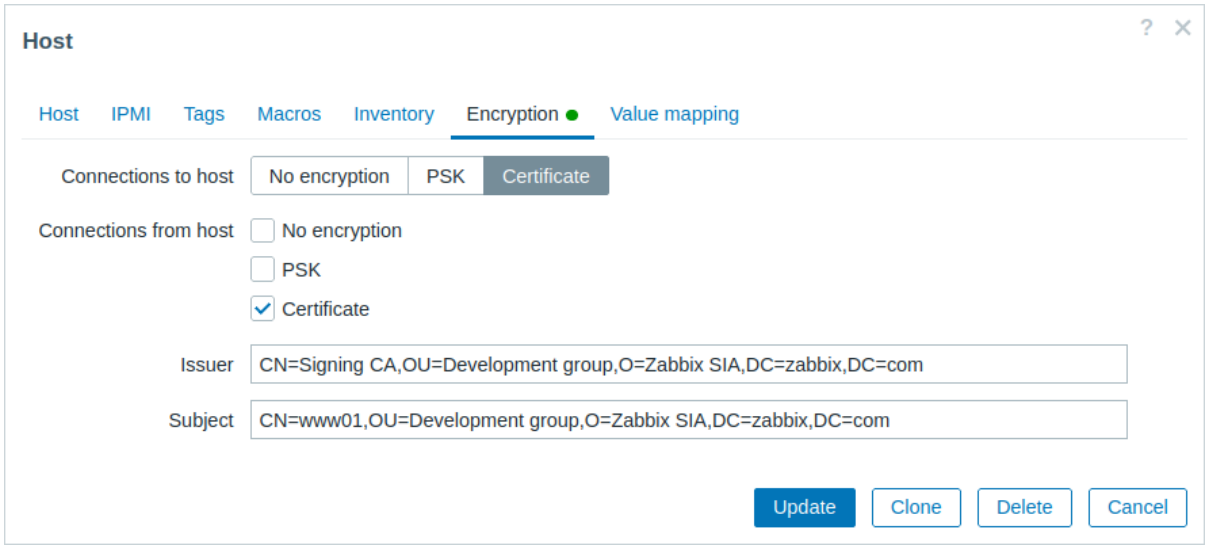
```
TLSConnect=cert
TLSAccept=cert
TLSCAFile=/home/zabbix/zabbix_ca_file.crt
TLSServerCertIssuer=CN=Signing CA,OU=Development group,O=Zabbix SIA,DC=zabbix,DC=com
TLSServerCertSubject=CN=Zabbix proxy,OU=Development group,O=Zabbix SIA,DC=zabbix,DC=com
TLSCertFile=/home/zabbix/zabbix_agentd.crt
TLSKeyFile=/home/zabbix/zabbix_agentd.key
```

3. Skonfiguruj szyfrowanie w Zabbix frontend dla hosta monitorowanego przez ten agent.

- Przejdź do: *Data collection* → *Hosts*.

- Wybierz host i kliknij kartę *Encryption*.

W poniższym przykładzie pola *Issuer* i *Subject* są wypełnione. Więcej informacji o tym, dlaczego i jak używać tych pól, znajdziesz w sekcji Ograniczanie dozwolonego wystawcy i podmiotu certyfikatu.



Usługa internetowa Zabbix

1. Przygotuj pliki z certyfikatami głównego urzędu certyfikacji (CA), certyfikatem/łańcuchem certyfikatów usługi internetowej Zabbix oraz kluczem prywatnym, zgodnie z opisem w sekcji serwer Zabbix. Następnie odpowiednio edytuj parametry `TLSCAFile`, `TLSCertFile` i `TLSKeyFile` w pliku konfiguracyjnym usługi internetowej Zabbix.

2. Edytuj dodatkowy parametr TLS w pliku konfiguracyjnym usługi internetowej Zabbix: `TLSAccept=cert`

Parametry TLS w końcowym pliku konfiguracyjnym usługi internetowej mogą wyglądać następująco:

```
TLSAccept=cert
TLSCAFile=/home/zabbix/zabbix_ca_file.crt
TLSCertFile=/home/zabbix/zabbix_web_service.crt
TLSKeyFile=/home/zabbix/zabbix_web_service.key
```

3. Skonfiguruj serwer Zabbix tak, aby łączył się z usługą internetową Zabbix skonfigurowaną do używania TLS, edytując parametr `WebServiceURL` w pliku konfiguracyjnym serwera Zabbix:

```
WebServiceURL=https://example.com:443/report
```

Ograniczanie dozwolonego wystawcy i podmiotu certyfikatu

Gdy dwa komponenty Zabbix (na przykład serwer i agent) ustanawiają połączenie TLS, weryfikują wzajemnie swoje certyfikaty. Jeśli certyfikat strony zdalnej jest podpisany przez zaufany urząd certyfikacji (z wcześniej skonfigurowanym certyfikatem głównym w `TLSCAFile`), jest prawidłowy, nie wygasł i przechodzi inne kontrole, komunikacja między komponentami może być kontynuowana. W tym najprostszym przypadku wystawca i podmiot certyfikatu nie są weryfikowani.

Jednak stwarza to ryzyko: każdy, kto ma ważny certyfikat, może podszyć się pod kogokolwiek innego (na przykład certyfikat hosta może zostać użyty do podszycia się pod serwer). Choć może to być akceptowalne w małych środowiskach, gdzie certyfikaty są podpisywane przez dedykowany wewnętrzny urząd certyfikacji, a ryzyko podszycia się jest niskie, w większych środowiskach lub środowiskach o wyższych wymaganiach bezpieczeństwa może to być niewystarczające.

Jeśli Twój główny urząd certyfikacji wystawia certyfikaty, które nie powinny być akceptowane przez Zabbix, lub jeśli chcesz zmniejszyć ryzyko podszycia się, możesz ograniczyć dozwolone certyfikaty, określając ich wystawcę i podmiot.

Na przykład w pliku konfiguracyjnym Zabbix proxy można określić:

```
TLSServerCertIssuer=CN=Signing CA,OU=Development group,O=Zabbix SIA,DC=zabbix,DC=com
TLSServerCertSubject=CN=Zabbix server,OU=Development group,O=Zabbix SIA,DC=zabbix,DC=com
```

Przy tych ustawieniach aktywny proxy nie będzie komunikował się z serwerem Zabbix, którego certyfikat ma innego wystawcę lub podmiot. Podobnie pasywny proxy nie będzie akceptował żądań od takiego serwera.

Zasady dopasowywania ciągów `Issuer` i `Subject`

Zasady dopasowywania ciągów `Issuer` i `Subject` są następujące:

- Ciągi `Issuer` i `Subject` są sprawdzane niezależnie. Oba są opcjonalne.
- Nieokreślony ciąg oznacza, że akceptowany jest dowolny ciąg.

- Ciągi są porównywane *tak jak są* i muszą być identyczne.
- Znaki UTF-8 są obsługiwane. Jednak symbole wieloznaczne (*) ani wyrażenia regularne nie są obsługiwane.
- Zaimplementowano następujące wymagania RFC 4514 — znaki wymagające poprzedzenia znakiem ucieczki (odwrotnym ukośnikiem '\', U+005C):
  - w dowolnym miejscu ciągu: '"' (U+0022), '+' (U+002B), ',' (U+002C), ';' (U+003B), '<' (U+003C), '>' (U+003E), '\\' (U+005C);
  - na początku ciągu: spacja (' ', U+0020) lub znak kratki ('#', U+0023);
  - na końcu ciągu: spacja (' ', U+0020).
- Znaki null (U+0000) nie są obsługiwane. Jeśli zostanie napotkany znak null, dopasowanie zakończy się niepowodzeniem.
- Standardy RFC 4517 i RFC 4518 nie są obsługiwane.

Na przykład, jeśli ciągi organizacji (O) w `Issuer` i `Subject` zawierają końcowe spacje, a ciąg jednostki organizacyjnej (OU) w `Subject` zawiera podwójne cudzysłowy, znaki te muszą być poprzedzone znakiem ucieczki:

```
TLSServerCertIssuer=CN=Signing CA,OU=Development head,O=\ Example SIA\ ,DC=example,DC=com
TLSServerCertSubject=CN=Zabbix server,OU=Development group \"5\",O=\ Example SIA\ ,DC=example,DC=com
```

Kolejność pól i formatowanie

Zabbix stosuje się do zaleceń RFC 4514, które określają „odwrotną" kolejność tych pól, zaczynając od pól najniższego poziomu (CN), przechodząc do pól poziomu pośredniego (OU, O) i kończąc na polach najwyższego poziomu (DC).

```
TLSServerCertIssuer=CN=Signing CA,OU=Development group,O=Zabbix SIA,DC=zabbix,DC=com
TLSServerCertSubject=CN=Zabbix proxy,OU=Development group,O=Zabbix SIA,DC=zabbix,DC=com
```

Natomiast OpenSSL domyślnie wyświetla ciągi `Issuer` i `Subject` w kolejności od najwyższego do najniższego poziomu. W poniższym przykładzie pola `Issuer` i `Subject` zaczynają się od najwyższego poziomu (DC) i kończą na polu najniższego poziomu (CN). Formatowanie ze spacjami i separatorami pól również różni się w zależności od użytych opcji, dlatego nie będzie zgodne z formatem wymaganym przez Zabbix.

```
$ openssl x509 -noout -in /home/zabbix/zabbix_proxy.crt -issuer -subject
issuer= /DC=com/DC=zabbix/O=Zabbix SIA/OU=Development group/CN=Signing CA
subject= /DC=com/DC=zabbix/O=Zabbix SIA/OU=Development group/CN=Zabbix proxy

$ openssl x509 -noout -text -in /home/zabbix/zabbix_proxy.crt
Certificate:
    ...
        Issuer: DC=com, DC=zabbix, O=Zabbix SIA, OU=Development group, CN=Signing CA
        ...
        Subject: DC=com, DC=zabbix, O=Zabbix SIA, OU=Development group, CN=Zabbix proxy
```

Aby poprawnie sformatować ciągi *Issuer* i *Subject* dla Zabbix, uruchom OpenSSL z następującymi opcjami:

```
$ openssl x509 -noout -issuer -subject \
    -nameopt esc_2253,esc_ctrl,utf8,dump_nostr,dump_unknown,dump_der,sep_comma_plus,dn_rev,sname\
    -in /home/zabbix/zabbix_proxy.crt
```

Dane wyjściowe będą wtedy w odwrotnej kolejności, rozdzielone przecinkami i gotowe do użycia w plikach konfiguracyjnych Zabbix oraz we frontend:

```
issuer=CN=Signing CA,OU=Development group,O=Zabbix SIA,DC=zabbix,DC=com
subject=CN=Zabbix proxy,OU=Development group,O=Zabbix SIA,DC=zabbix,DC=com
```

Ograniczenia dotyczące używania rozszerzeń certyfikatów X.509 v3

Podczas wdrażania certyfikatów X.509 v3 w Zabbix niektóre rozszerzenia mogą nie być w pełni obsługiwane lub mogą powodować niespójne działanie.

Rozszerzenie Subject Alternative Name

Zabbix nie obsługuje rozszerzenia *Subject Alternative Name*, które służy do określania alternatywnych nazw DNS, takich jak adresy IP lub adresy e-mail. Zabbix może weryfikować wyłącznie wartość w polu *Subject* certyfikatu (zobacz Ograniczanie dozwolonego wystawcy i podmiotu certyfikatu). Jeśli certyfikaty zawierają pole `subjectAltName`, wynik weryfikacji certyfikatu może się różnić w zależności od konkretnych zestawów narzędzi kryptograficznych użytych do kompilacji komponentów Zabbix. W rezultacie Zabbix może zarówno akceptować, jak i odrzucać certyfikaty w zależności od tych kombinacji.

Rozszerzenie Extended Key Usage

Zabbix obsługuje rozszerzenie *Extended Key Usage*. Jednak jeśli jest ono używane, zazwyczaj wymagane jest określenie zarówno atrybutu *clientAuth* (do uwierzytelniania klienta TLS WWW), jak i *serverAuth* (do uwierzytelniania serwera TLS WWW). Na przykład:

- W przypadku kontroli pasywnych, gdzie agent działa jako serwer TLS, atrybut *serverAuth* musi być zawarty w certyfikacie agenta.
- W przypadku kontroli aktywnych, gdzie agent działa jako klient TLS, atrybut *clientAuth* musi być zawarty w certyfikacie agenta.

Chociaż GnuTLS może zgłaszać ostrzeżenie o naruszeniu użycia klucza, zwykle pozwala kontynuować komunikację mimo tych ostrzeżeń.

Rozszerzenie Name Constraints

Obsługa rozszerzenia *Name Constraints* różni się w zależności od zestawu narzędzi kryptograficznych. Upewnij się, że wybrany zestaw narzędzi obsługuje to rozszerzenie. To rozszerzenie może uniemożliwić Zabbix załadowanie certyfikatów CA, jeśli ta sekcja jest oznaczona jako krytyczna, w zależności od używanego zestawu narzędzi.

Listy unieważnionych certyfikatów (CRL)

Jeśli certyfikat zostanie skompromitowany, urząd certyfikacji (CA) może go unieważnić, umieszczając certyfikat na liście unieważnionych certyfikatów (CRL). Listy CRL są zarządzane za pomocą plików konfiguracyjnych i mogą być określone przy użyciu parametru `TLSCRLFile` w plikach konfiguracyjnych serwera, proxy i agenta. Na przykład:

```
TLSCRLFile=/home/zabbix/zabbix_crl_file.crt
```

W tym przypadku `zabbix_crl_file.crt` może zawierać listy CRL z wielu urzędów certyfikacji i może wyglądać następująco:

```
-----BEGIN X509 CRL-----
MIIB/DCB5QIBATANBgkqhkiG9w0BAQUFADCBgTETMBEGCgmSJomT8ixkARkWA2Nv
...
treZeUPjb7LSmZ3K2hpbZN7SoOZcAoHQ3GWd9npuctg=
-----END X509 CRL-----
-----BEGIN X509 CRL-----
MIIB+TCB4gIBATANBgkqhkiG9w0BAQUFADB/MRMwEQYKCZImiZPyLGQBGRYDY29t
...
CAEebS2CND3ShBedZ8YSil59O6JvaDP61lR5lNs=
-----END X509 CRL-----
```

Plik CRL jest wczytywany tylko podczas uruchamiania Zabbix. Aby zaktualizować listę CRL, uruchom ponownie Zabbix.

Attention:
Jeśli komponenty Zabbix są skompilowane z OpenSSL i używane są listy CRL, upewnij się, że każdy główny i pośredni urząd certyfikacji w łańcuchach certyfikatów ma odpowiadającą mu listę CRL (nawet jeśli jest pusta) dołączoną w `TLSCRLFile`.

2 Używanie kluczy współdzielonych z wyprzedzeniem

Przegląd

Każdy klucz pre-shared key (PSK) w Zabbix jest w rzeczywistości parą składającą się z:

- jawnego ciągu identyfikatora PSK,
- tajnej wartości ciągu PSK.

Ciąg identyfikatora PSK jest niepustym ciągiem UTF-8. Na przykład „PSK ID 001 Zabbix agentd”. Jest to unikalna nazwa, za pomocą której ten konkretny PSK jest identyfikowany przez komponenty Zabbix. Nie umieszczaj poufnych informacji w ciągu identyfikatora PSK — jest on przesyłany przez sieć bez szyfrowania.

Wartość PSK to trudny do odgadnięcia ciąg cyfr szesnastkowych, na przykład „e560cb0d918d26d31b4f642181f5f570ad89a390931102e5391d

Ograniczenia rozmiaru

W Zabbix obowiązują ograniczenia rozmiaru dla tożsamości i wartości PSK; w niektórych przypadkach biblioteka kryptograficzna może mieć niższy limit:

Komponent	Maksymalny rozmiar tożsamości PSK	Minimalny rozmiar wartości PSK	Maksymalny rozmiar wartości PSK
Zabbix	128 znaków UTF-8	128 bitów (16-bajtowy PSK, wprowadzany jako 32 cyfry szesnastkowe)	2048 bitów (256-bajtowy PSK, wprowadzany jako 512 cyfr szesnastkowych)

Komponent	Maksymalny rozmiar tożsamości PSK	Minimalny rozmiar wartości PSK	Maksymalny rozmiar wartości PSK
GnuTLS	128 bajtów (może zawierać znaki UTF-8)	-	2048 bitów (256-bajtowy PSK, wprowadzany jako 512 cyfr szesnastkowych)
OpenSSL 1.0.x, 1.1.0	127 bajtów (może zawierać znaki UTF-8)	-	2048 bitów (256-bajtowy PSK, wprowadzany jako 512 cyfr szesnastkowych)
OpenSSL 1.1.1	127 bajtów (może zawierać znaki UTF-8)	-	512 bitów (64-bajtowy PSK, wprowadzany jako 128 cyfr szesnastkowych)
OpenSSL 1.1.1a i nowsze	127 bajtów (może zawierać znaki UTF-8)	-	2048 bitów (256-bajtowy PSK, wprowadzany jako 512 cyfr szesnastkowych)

Attention:
Zabbix frontend umożliwia skonfigurowanie ciągu tożsamości PSK o długości do 128 znaków oraz PSK o długości 2048 bitów, niezależnie od używanych bibliotek kryptograficznych.
Jeśli niektóre komponenty Zabbix obsługują niższe limity, obowiązkiem użytkownika jest skonfigurowanie tożsamości i wartości PSK o długości dozwolonej dla tych komponentów.
Przekroczenie limitów długości skutkuje błędami komunikacji między komponentami Zabbix.

Zanim serwer Zabbix połączy się z agent przy użyciu PSK, serwer wyszukuje w bazie danych tożsamość PSK i wartość PSK skonfigurowane dla tego agent (w rzeczywistości w pamięci podręcznej konfiguracji). Po odebraniu połączenia agent używa tożsamości PSK i wartości PSK ze swojego pliku konfiguracyjnego. Jeśli obie strony mają ten sam ciąg tożsamości PSK i tę samą wartość PSK, połączenie może się powieść.

Attention:
Każda tożsamość PSK musi być powiązana tylko z jedną wartością. Obowiązkiem użytkownika jest upewnienie się, że nie istnieją dwa PSK z tym samym ciągiem tożsamości, ale różnymi wartościami. Niedopełnienie tego może prowadzić do nieprzewidywalnych błędów lub zakłóceń komunikacji między komponentami Zabbix używającymi PSK z tym ciągiem tożsamości PSK.

Generowanie PSK

Na przykład 256-bitowy (32 bajty) PSK można wygenerować za pomocą następujących poleceń:

- przy użyciu *OpenSSL*:

```
$ openssl rand -hex 32
af8ced32dfe8714e548694e2d29e1a14ba6fa13f216cb35c19d0feb1084b0429
```

- przy użyciu *GnuTLS*:

```
$ psktool -u psk_identity -p database.psk -s 32
Generating a random key for user 'psk_identity'
Key stored to database.psk

$ cat database.psk
psk_identity:9b8eafedfaae00cece62e85d5f4792c7d9c9bcc851b23216a1d300311cc4f7cb
```

Należy pamiętać, że powyższe polecenie „psktool” generuje plik bazy danych zawierający tożsamość PSK oraz skojarzony z nią PSK. Zabbix oczekuje w pliku PSK wyłącznie samego PSK, dlatego z pliku należy usunąć ciąg tożsamości oraz dwukropek (':').

Konfigurowanie PSK do komunikacji serwer-agent (przykład)

Na hoście agenta zapisz wartość PSK do pliku, na przykład `/home/zabbix/zabbix_agentd.psk`. Plik musi zawierać PSK w pierwszym ciągu tekstowym, na przykład:

```
1f87b595725ac58dd977beef14b97461a7c1045b9a1c963065002c5473194952
```

Ustaw prawa dostępu do pliku PSK — musi on być czytelny tylko dla użytkownika Zabbix.

Edytuj parametry TLS w pliku konfiguracyjnym agenta `zabbix_agentd.conf`, na przykład ustaw:

```
TLSConnect=psk
TLSAccept=psk
```

```
TLSPSKFile=/home/zabbix/zabbix_agentd.psk
TLSPSKIdentity=PSK 001
```

agent będzie łączył się z serwerem (aktywne testy) i akceptował od serwera oraz `zabbix_get` tylko połączenia używające PSK. Tożsamość PSK będzie miała wartość „PSK 001”.

Uruchom ponownie agent. Teraz możesz przetestować połączenie za pomocą `zabbix_get`, na przykład:

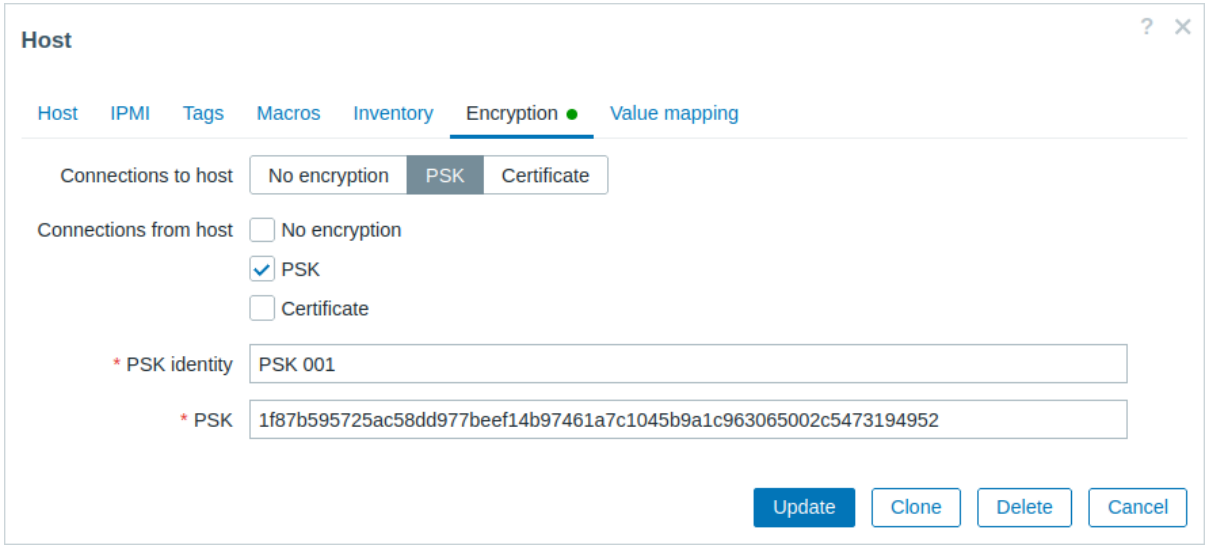
```
zabbix_get -s 127.0.0.1 -k "system.cpu.load[all,avg1]" --tls-connect=psk --tls-psk-identity="PSK 001" --tl
```

(Aby zminimalizować przestój, zobacz, jak zmienić typ połączenia w zarządzaniu szyfrowaniem połączeń).

Skonfiguruj szyfrowanie PSK dla tego agenta w Zabbix frontend:

- Przejdź do: *Data collection → Hosts*
- Wybierz host i kliknij kartę **Encryption**

Przykład:



Wszystkie wymagane pola wejściowe są oznaczone czerwoną gwiazdką.

Gdy pamięć podręczna konfiguracji zostanie zsynchronizowana z bazą danych, nowe połączenia będą używać PSK. Sprawdź pliki dziennika serwera i agenta pod kątem komunikatów o błędach.

Konfigurowanie PSK dla komunikacji serwer - aktywny proxy (przykład)

Na proxy zapisz wartość PSK do pliku, na przykład `/home/zabbix/zabbix_proxy.psk`. Plik musi zawierać PSK w pierwszym wierszu tekstu, na przykład:

```
e560cb0d918d26d31b4f642181f5f570ad89a390931102e5391d08327ba434e9
```

Ustaw prawa dostępu do pliku PSK - musi on być czytelny tylko dla użytkownika Zabbix.

Edytuj parametry TLS w pliku konfiguracyjnym proxy `zabbix_proxy.conf`, na przykład ustaw:

```
TLSConnect=psk
TLSPSKFile=/home/zabbix/zabbix_proxy.psk
TLSPSKIdentity=PSK 002
```

Proxy będzie łączyć się z serwerem przy użyciu PSK. Tożsamość PSK będzie miała wartość ”PSK 002”.

(Aby zminimalizować przestój, zobacz jak zmienić typ połączenia w zarządzaniu szyfrowaniem połączeń).

Skonfiguruj PSK dla tego proxy w Zabbix frontend. Przejdź do *Administration→Proxies*, wybierz proxy, przejdź do zakładki ”Encryption”. W polu ”Connections from proxy” zaznacz PSK. Wklej do pola ”PSK identity” wartość ”PSK 002”, a do pola ”PSK” wartość ”e560cb0d918d26d31b4f642181f5f570ad89a390931102e5391d08327ba434e9”. Kliknij ”Update”.

Uruchom ponownie proxy. Zacznie on używać połączeń szyfrowanych opartych na PSK z serwerem. Sprawdź pliki dziennika serwera i proxy pod kątem komunikatów o błędach.

W przypadku pasywnego proxy procedura jest bardzo podobna. Jedyna różnica - ustaw `TLSAccept=psk` w pliku konfiguracyjnym proxy i ustaw ”Connections to proxy” w Zabbix frontend na PSK.

3 Rozwiązywanie problemów

Ogólne zalecenia

- Zacznij od ustalenia, który komponent działa jako klient TLS, a który jako serwer TLS w danym problematycznym przypadku.
  Serwer Zabbix, proxy i agenty, w zależności od interakcji między nimi, mogą działać zarówno jako serwery TLS, jak i klienci.
  Na przykład serwer Zabbix łączący się z agent w celu wykonania pasywnego sprawdzenia działa jako klient TLS. Agent pełni rolę serwera TLS.
  Agent Zabbix, żądający listy aktywnych sprawdzeń od proxy, działa jako klient TLS. Proxy pełni rolę serwera TLS.
  Narzędzia `zabbix_get` i `zabbix_sender` zawsze działają jako klienci TLS.
- Zabbix używa wzajemnego uwierzytelniania.
  Każda strona weryfikuje swojego partnera i może odrzucić połączenie.
  Na przykład serwer Zabbix łączący się z agent może natychmiast zamknąć połączenie, jeśli certyfikat agent jest nieprawidłowy. I odwrotnie — agent Zabbix przyjmujący połączenie od serwera może zamknąć połączenie, jeśli serwer nie jest zaufany przez agent.
- Sprawdź pliki dziennika po obu stronach — po stronie klienta TLS i serwera TLS.
  Strona, która odrzuca połączenie, może zapisać dokładny powód odrzucenia. Druga strona często zgłasza raczej ogólny błąd (np. „Connection closed by peer", „connection was non-properly terminated").
- Czasami błędnie skonfigurowane szyfrowanie skutkuje mylącymi komunikatami o błędach, które w żaden sposób nie wskazują rzeczywistej przyczyny.
  W poniższych podsekcjach staramy się przedstawić zbiór komunikatów i możliwych przyczyn (daleki od wyczerpującego), który może pomóc w rozwiązywaniu problemów.
  Należy pamiętać, że różne biblioteki kryptograficzne (OpenSSL, GnuTLS) często generują różne komunikaty o błędach w tych samych sytuacjach problemowych.
  Czasami komunikaty o błędach zależą nawet od konkretnej kombinacji bibliotek kryptograficznych po obu stronach.

1 Problemy z typem połączenia lub uprawnieniami

Serwer jest skonfigurowany do łączenia się z agent przy użyciu PSK, ale agent akceptuje tylko połączenia nieszyfrowane

W logu serwera lub proxy (z *GnuTLS* 3.3.16)

```
Get value from agent failed: zbx_tls_connect(): gnutls_handshake() failed: \
    -110 The TLS connection was non-properly terminated.
```

W logu serwera lub proxy (z *OpenSSL* 1.0.2c)

```
Get value from agent failed: TCP connection successful, cannot establish TLS to [[127.0.0.1]:10050]: \
    Connection closed by peer. Check allowed connection types and access rights
```

Jedna strona łączy się przy użyciu certyfikatu, ale druga strona akceptuje tylko PSK lub odwrotnie

W dowolnym logu (z *GnuTLS*):

```
nie udało się zaakceptować połączenia przychodzącego: z 127.0.0.1: zbx_tls_accept(): gnutls_handshake() ni
    -21 Nie można było uzgodnić obsługiwanego zestawu szyfrów.
```

W dowolnym logu (z *OpenSSL* 1.0.2c):

```
nie udało się zaakceptować połączenia przychodzącego: z 127.0.0.1: uzgadnianie TLS zwróciło kod błędu 1:\
    plik .\ssl\s3_srvr.c linia 1411: error:1408A0C1:procedury SSL:ssl3_get_client_hello:brak wspólnego szy
    zapis TLS krytycznego alertu „handshake failure"
```

Próba użycia Zabbix sender skompilowanego z obsługą TLS do wysyłania danych do serwera/proxy Zabbix skompilowanego bez obsługi TLS

W logu po stronie nawiązującej połączenie:

Linux:

```
...In zbx_tls_init_child()
...Biblioteka OpenSSL (wersja OpenSSL 1.1.1  11 Sep 2018) zainicjalizowana
...
...In zbx_tls_connect(): psk_identity:"PSK test sender"
...End of zbx_tls_connect():FAIL error:'połączenie zamknięte przez peer'
...błąd wysyłania wartości: TCP zakończone powodzeniem, nie można ustanowić TLS do [[localhost]:10051]: po
```

Windows:

```
...Biblioteka OpenSSL (wersja OpenSSL 1.1.1a  20 Nov 2018) zainicjalizowana
...
...In zbx_tls_connect(): psk_identity:"PSK test sender"
...zbx_psk_client_cb() requested PSK identity "PSK test sender"
...End of zbx_tls_connect():FAIL error:'SSL_connect() błąd wejścia/wyjścia: [0x00000000] Operacja zakończo
...błąd wysyłania wartości: TCP zakończone powodzeniem, nie można ustanowić TLS do [[192.168.1.2]:10051]:
```

W logu po stronie akceptującej:

```
...nie udało się zaakceptować połączenia przychodzącego: z 127.0.0.1: obsługa TLS nie została skompilowana
```

Jedna strona łączy się przy użyciu PSK, ale druga strona używa LibreSSL lub została skompilowana bez obsługi szyfrowania

LibreSSL nie obsługuje PSK.

W logu strony nawiązującej połączenie:

```
...TCP successful, cannot establish TLS to [[192.168.1.2]:10050]: SSL_connect() I/O error: [0] Success
```

W logu strony akceptującej połączenie:

```
...failed to accept an incoming connection: from 192.168.1.2: support for PSK was not compiled in
```

W Zabbix frontend:

```
Get value from agent failed: TCP successful, cannot establish TLS to [[192.168.1.2]:10050]: SSL_connect()
```

Jedna strona łączy się z użyciem PSK, ale druga strona używa OpenSSL z wyłączoną obsługą PSK

W logu strony nawiązującej połączenie:

```
...TCP successful, cannot establish TLS to [[192.168.1.2]:10050]: SSL_connect() set result code to SSL_ERR
```

W logu strony akceptującej połączenie:

```
...failed to accept an incoming connection: from 192.168.1.2: TLS handshake set result code to 1: file ssl
```

2 Problemy z certyfikatem

OpenSSL używany z listami CRL i dla części CA w łańcuchu certyfikatów ich CRL nie jest dołączona w TLSCRLFile

W logu serwera TLS w przypadku peera *OpenSSL*:

```
failed to accept an incoming connection: from 127.0.0.1: TLS handshake with 127.0.0.1 returned error code
    file s3_srvr.c line 3251: error:14089086: SSL routines:ssl3_get_client_certificate:certificate verify
    TLS write fatal alert "unknown CA"
```

W logu serwera TLS w przypadku peera *GnuTLS*:

```
failed to accept an incoming connection: from 127.0.0.1: TLS handshake with 127.0.0.1 returned error code
    file rsa_pk1.c line 103: error:0407006A: rsa routines:RSA_padding_check_PKCS1_type_1:\
    block type is not 01 file rsa_eay.c line 705: error:04067072: rsa routines:RSA_EAY_PUBLIC_DECRYPT:padd
```

Lista CRL wygasła lub wygasa podczas działania serwera

OpenSSL, w logu serwera:

- przed wygaśnięciem:

```
cannot connect to proxy "proxy-openssl-1.0.1e": TCP successful, cannot establish TLS to [[127.0.0.1]:20004
    SSL_connect() returned SSL_ERROR_SSL: file s3_clnt.c line 1253: error:14090086:\
    SSL routines:ssl3_get_server_certificate:certificate verify failed:\
    TLS write fatal alert "certificate revoked"
```

- po wygaśnięciu:

```
cannot connect to proxy "proxy-openssl-1.0.1e": TCP successful, cannot establish TLS to [[127.0.0.1]:20004
    SSL_connect() returned SSL_ERROR_SSL: file s3_clnt.c line 1253: error:14090086:\
    SSL routines:ssl3_get_server_certificate:certificate verify failed:\
    TLS write fatal alert "certificate expired"
```

Chodzi o to, że przy prawidłowej liście CRL unieważniony certyfikat jest zgłaszany jako ”certificate revoked”. Gdy lista CRL wygaśnie, komunikat o błędzie zmienia się na ”certificate expired”, co jest dość mylące.

GnuTLS, w logu serwera:

- przed i po wygaśnięciu tak samo:

```
cannot connect to proxy "proxy-openssl-1.0.1e": TCP successful, cannot establish TLS to [[127.0.0.1]:20004
      invalid peer certificate: The certificate is NOT trusted. The certificate chain is revoked.
```

Certyfikat z podpisem własnym, nieznane CA

OpenSSL, w logu:

```
error:'self signed certificate: SSL_connect() set result code to SSL_ERROR_SSL: file ../ssl/statem/statem_
      line 1924: error:1416F086:SSL routines:tls_process_server_certificate:certificate verify failed:\
      TLS write fatal alert "unknown CA"'
```

Zaobserwowano to, gdy certyfikat serwera przez pomyłkę miał taki sam ciąg znaków Issuer i Subject, mimo że został podpisany przez CA. Issuer i Subject są równe w certyfikacie głównego CA, ale nie mogą być równe w certyfikacie serwera. (To samo dotyczy certyfikatów proxy i agent.)

Aby sprawdzić, czy certyfikat zawiera takie same wpisy Issuer i Subject, uruchom:

```
openssl x509 -in <yourcertificate.crt> -noout -text
```

Dopuszczalne jest, aby certyfikat root (najwyższego poziomu) miał identyczne wartości Issuer i Subject.

3 Problemy z PSK

PSK zawiera nieparzystą liczbę cyfr szesnastkowych

Proxy lub agent nie uruchamia się, komunikat w logu proxy lub agent:

```
nieprawidłowy PSK w pliku "/home/zabbix/zabbix_proxy.psk"
```

Ciąg tożsamości PSK dłuższy niż 128 bajtów jest przekazywany do GnuTLS

W logu po stronie klienta TLS:

```
gnutls_handshake() failed: -110 The TLS connection was non-properly terminated.
```

W logu po stronie serwera TLS.

```
gnutls_handshake() failed: -90 The SRP username supplied is illegal.
```

Zbyt długa wartość PSK używana z OpenSSL 1.1.1

W logu strony nawiązującej połączenie:

```
...OpenSSL library (version OpenSSL 1.1.1  11 Sep 2018) initialized
...
...In zbx_tls_connect(): psk_identity:"PSK 1"
...zbx_psk_client_cb() requested PSK identity "PSK 1"
...End of zbx_tls_connect():FAIL error:'SSL_connect() set result code to SSL_ERROR_SSL: file ssl\statem\ex
```

W logu strony akceptującej połączenie:

```
...Message from 123.123.123.123 is missing header. Message ignored.
```

Ten problem zwykle występuje podczas aktualizacji OpenSSL z wersji 1.0.x lub 1.1.0 do 1.1.1, jeśli wartość PSK jest dłuższa niż 512 bitów (64-bajtowy PSK, wprowadzony jako 128 cyfr szesnastkowych).

Zobacz także: Ograniczenia rozmiaru wartości

16 Interfejs webowy

Przegląd Aby zapewnić łatwy dostęp do Zabbix z dowolnego miejsca i z dowolnej platformy, udostępniono interfejs oparty na sieci WWW.

> **Note:**
> Jeśli używasz więcej niż jednej instancji frontend, upewnij się, że ustawienia regionalne i biblioteki (LDAP, SAML itp.) są zainstalowane i skonfigurowane identycznie dla wszystkich frontendów.

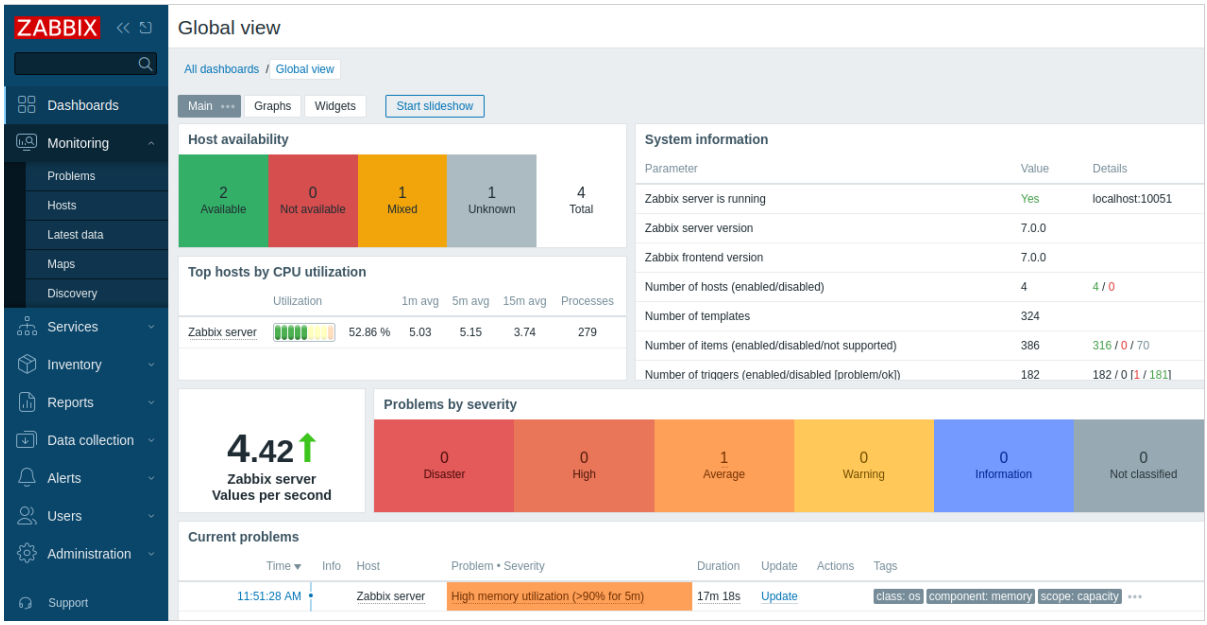
Pomoc frontend Łącze pomocy ? jest dostępne w formularzach frontend Zabbix i zawiera bezpośrednie odnośniki do odpowiednich części dokumentacji.

1 Menu

Przegląd

Pionowe menu na pasku bocznym zapewnia dostęp do różnych sekcji frontendu Zabbix.

Domyślny motyw posiada ciemnoniebieskie menu.

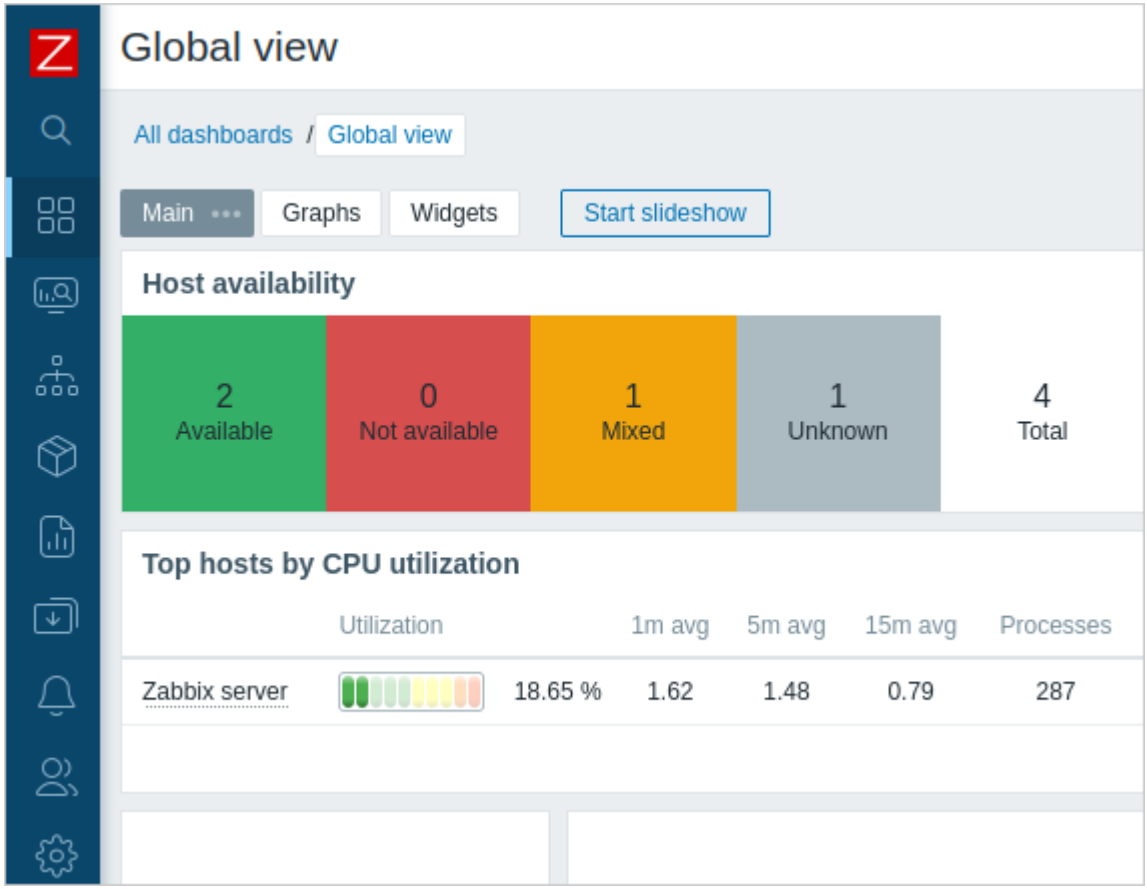


Praca z menu

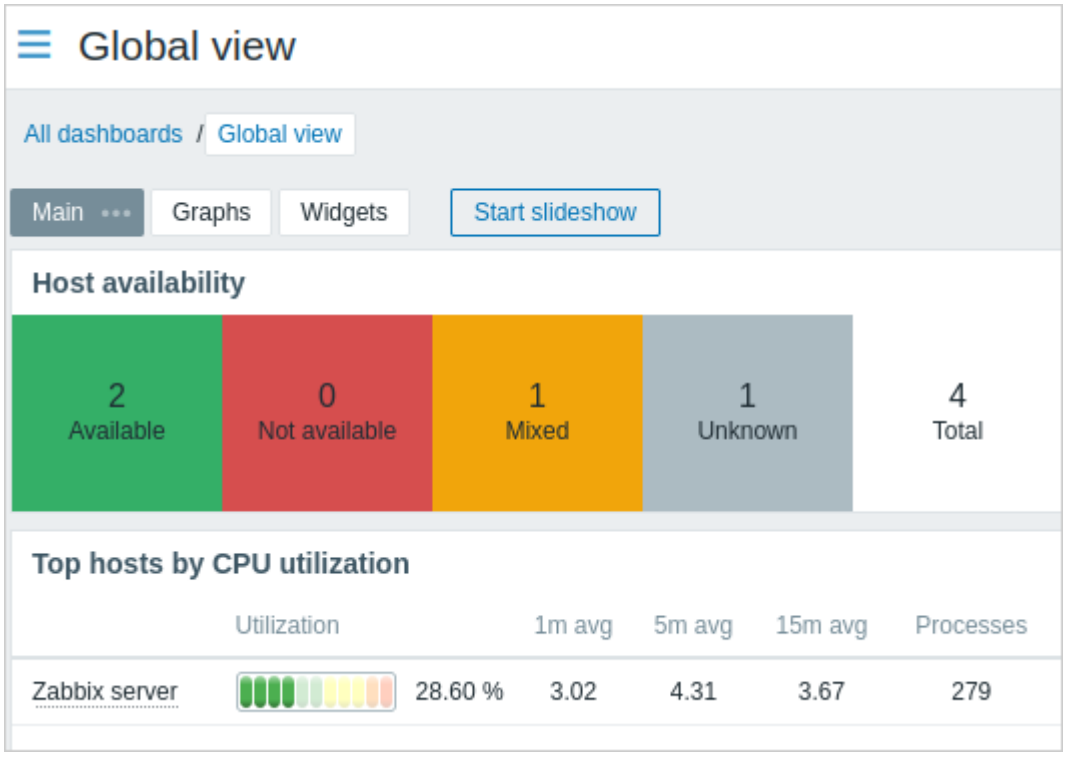
Pole wyszukiwania globalnego znajduje się poniżej logo Zabbix.

Menu można zwinąć lub całkowicie ukryć:

- Aby zwinąć, kliknij obok logo Zabbix. W zwiniętym menu widoczne są tylko ikony.



- Aby ukryć, kliknij  obok logo Zabbix. W ukrytym menu wszystko jest niewidoczne.



Collapsed menu

When the menu is collapsed to icons only, a full menu reappears as soon as the mouse cursor is placed upon it. Note that it reappears over page content; to move page content to the right you have to click on the expand button. If the mouse cursor again is placed outside the full menu, the menu will collapse again after two seconds.

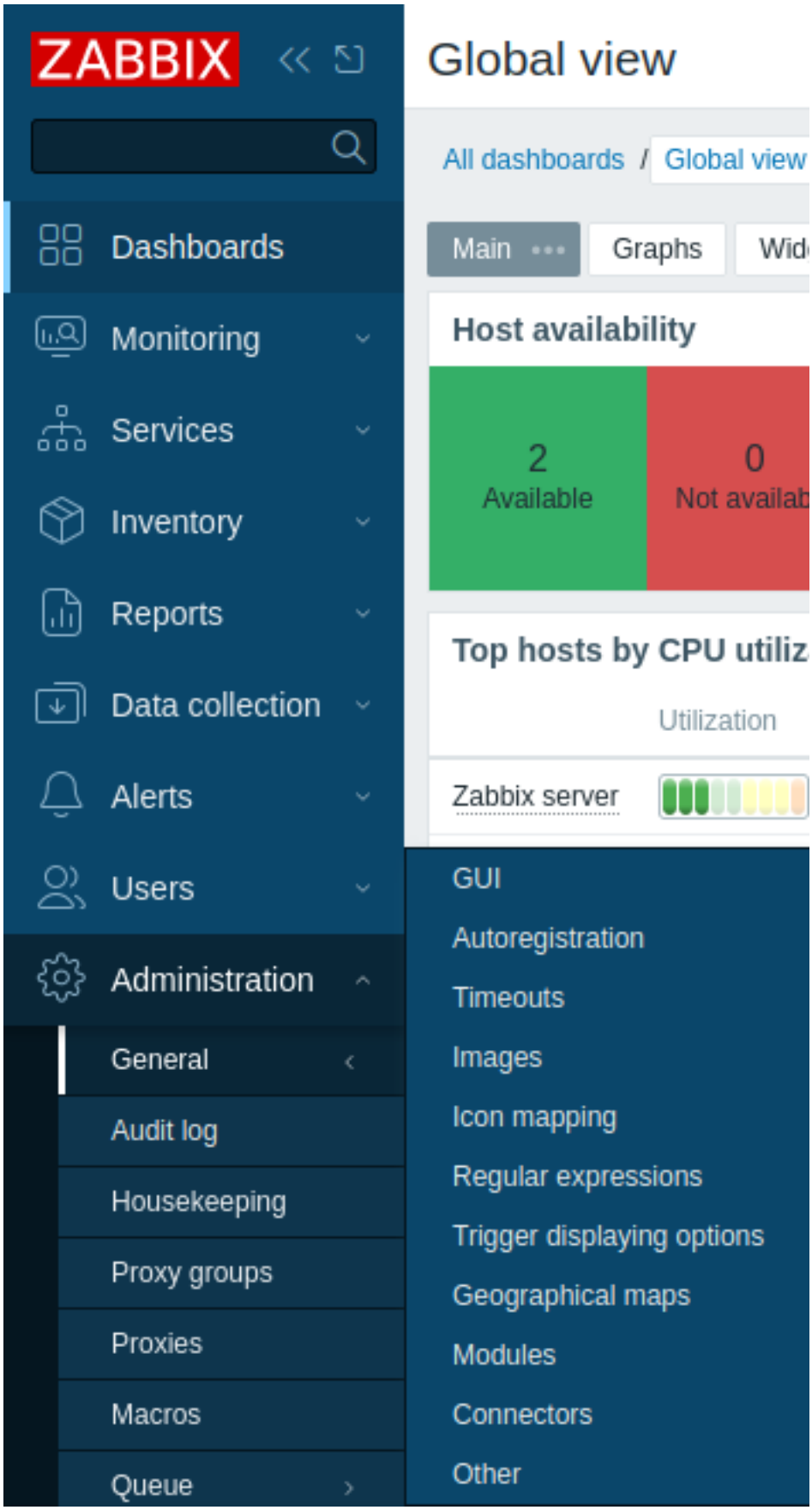
You can also make a collapsed menu reappear fully by hitting the Tab key. Hitting the Tab key repeatedly will allow to focus on the next menu element.

Ukryte menu

Nawet gdy menu jest całkowicie ukryte, pełne menu jest dostępne po jednym kliknięciu myszą — po kliknięciu ikony burgera . Należy pamiętać, że pojawia się ono ponownie nad zawartością strony; aby przesunąć zawartość strony w prawo, trzeba odkryć menu, klikając przycisk pokazania paska bocznego.

Poziomy menu

W menu są maksymalnie trzy poziomy.



Menu kontekstowe

Oprócz menu głównego Zabbix udostępnia menu kontekstowe dla hosta, pozycji oraz zdarzenia, zapewniające szybki dostęp do często używanych elementów, takich jak najnowsze wartości, prosty wykres, formularz konfiguracji, powiązane skrypty lub linki zewnętrzne.

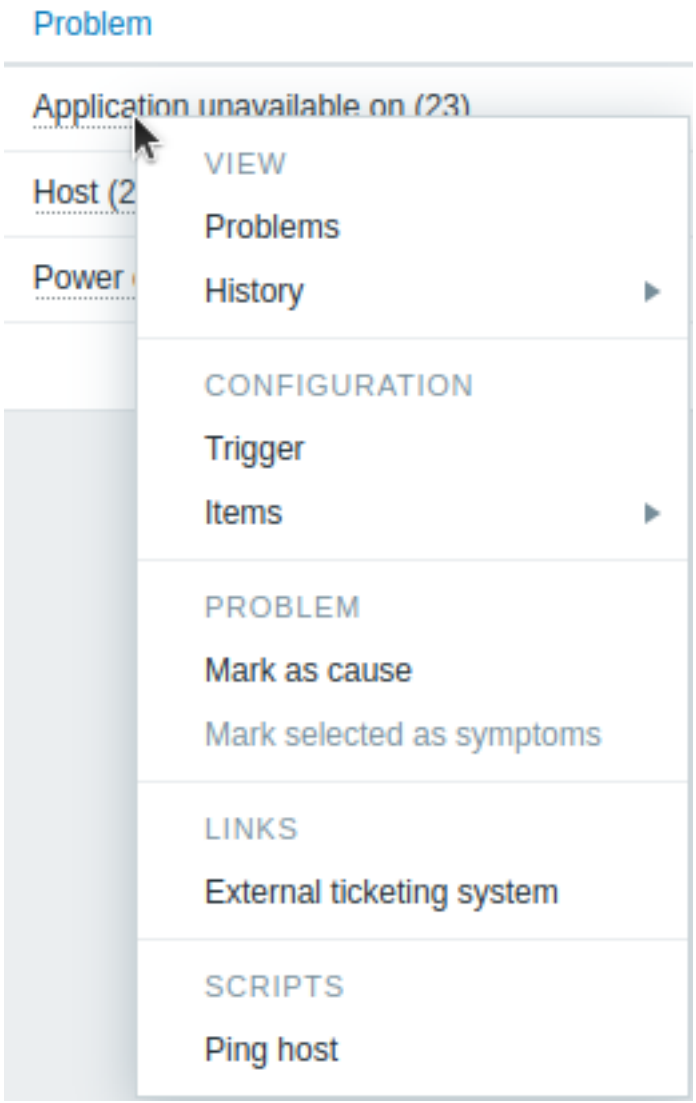
Menu kontekstowe są dostępne po kliknięciu nazwy hosta, pozycji lub problemu/wyzwalacza w obsługiwanych lokalizacjach.

1 Menu Zdarzenia

Przegląd

Menu zdarzenia zawiera skróty do działań lub sekcji frontend, które są często wymagane dla zdarzenia.

Menu zdarzenia można otworzyć, klikając nazwę zdarzenia.



Zawartość

Menu kontekstowe zdarzenia ma sześć sekcji: *Widok*, *Akcje*, *Konfiguracja*, *Problem*, *Linki* i *Skrypty*. Dla encji, które nie są skonfigurowane, linki są wyłączone i wyświetlane na szaro. Sekcje *Skrypty* i *Linki* są wyświetlane, jeśli ich encje są skonfigurowane.

Sekcja *Widok* zawiera linki do:

- **Problemy** - otwiera listę nierozwiązanych problemów powiązanych z bazowym wyzwalacz;
- **Historia** - prowadzi do wykresu/historii pozycja(i) w *Najnowsze dane* dla bazowej pozycji (bazowych pozycji). Jeśli wyzwalacz używa kilku pozycji, linki będą dostępne dla każdej z nich.

Sekcja *Akcje* jest dostępna tylko w widżetach *Przegląd wyzwalaczy*. Zawiera link do:

- **Aktualizuj problem** - otwiera ekran aktualizacji problemu.

Sekcja *Konfiguracja* zawiera linki do konfiguracji:

- **Wyzwalacza**, który wywołał problem;
- **Pozycji** użytych w wyrażeniu wyzwalacza.

Note:
Należy pamiętać, że sekcja konfiguracji jest dostępna tylko dla użytkowników typu Admin i Super admin.

Sekcja *Problem* zawiera opcje umożliwiające:

- **Oznacz jako przyczynę** - oznaczenie problemu jako przyczyny;
- **Oznacz wybrane jako symptomy** - oznaczenie wybranych problemów jako symptomów tego problemu.

Sekcja *Linki* zawiera linki do:

- dostępu do skonfigurowanego URL wyzwalacza;
- dostępu do niestandardowych linków skonfigurowanych w Skryptach globalnych (z zakresem „Ręczna akcja zdarzenia" i typem „URL");
- dostępu do skonfigurowanego zewnętrznego zgłoszenia dla problemu (zobacz opcję *Include event menu entry* podczas konfigurowania webhooków).

Sekcja *Skrypty* zawiera linki do wykonania globalnego skryptu (z zakresem *Ręczna akcja zdarzenia*). Ta funkcja może być przydatna do uruchamiania skryptów używanych do zarządzania zgłoszeniami problemów w systemach zewnętrznych.

Obsługiwane lokalizacje

Menu kontekstowe zdarzenia jest dostępne po kliknięciu problemu lub nazwy zdarzenia w różnych sekcjach frontend, na przykład:

- Widgety pulpitów, takie jak widget *Problemy*, widget *Przegląd wyzwalaczy* itp.
- Monitorowanie → Problemy
- Monitorowanie → Problemy → Szczegóły zdarzenia
- Raporty → Top 100 wyzwalaczy (skrypty globalne i dostęp do zewnętrznego zgłoszenia nie są obsługiwane w tej lokalizacji)

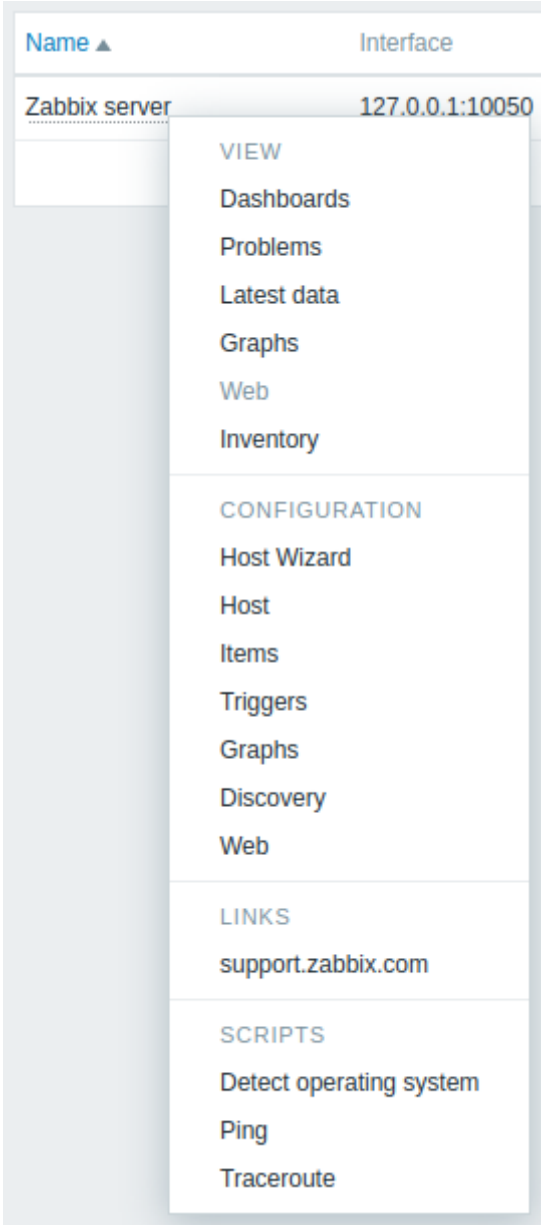
2 Menu hosta

Przegląd

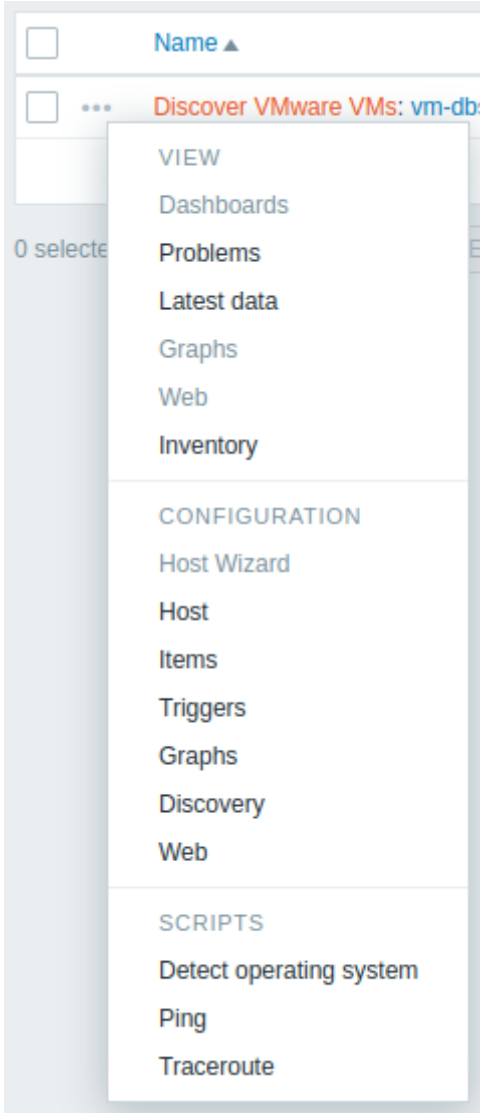
Menu hosta zawiera skróty do działań lub sekcji frontendu, które są często wymagane dla hosta.

Menu hosta można otworzyć, klikając nazwę hosta lub ikonę trzech kropek, w zależności od sekcji frontendu, na przykład:

Monitoring → Najnowsze dane



Zbieranie danych → Hosty



Zawartość

Menu kontekstowe hosta ma cztery sekcje: *Widok*, *Konfiguracja*, *Linki* i *Skrypty*. Dla encji, które nie są skonfigurowane, linki są wyłączone i wyświetlane na szaro. Sekcje *Skrypty* i *Linki* są wyświetlane, jeśli ich encje są skonfigurowane.

Sekcja *Widok* zawiera linki do:

- **Pulpity** - otwiera widżety i wykresy.
- **Problemy** - otwiera sekcję *Problemy* z listą nierozwiązanych problemów bazowego wyzwalacza.
- **Najnowsze dane** - otwiera sekcję *Najnowsze dane* z listą wszystkich najnowszych danych bieżącego hosta.
- **Wykresy** - otwiera proste wykresy bieżącego hosta.
- **WWW** - otwiera link do skonfigurowanych scenariuszy WWW.
- **Inwentaryzacja** - otwiera link do inwentaryzacji bieżącego hosta.

Sekcja *Konfiguracja* zawiera linki do:

- **Host Wizard** - otwiera Host Wizard dla bieżącego hosta (wyłączone dla hostów wykrytych automatycznie).
- **Host** - formularz konfiguracji bieżącego hosta.
- **Pozycje** - lista pozycji bieżącego hosta.
- **Wyzwalacze** - lista wyzwalaczy bieżącego hosta.
- **Wykresy** - proste wykresy bieżącego hosta.
- **Odkrywanie** - lista reguł odkrywania niskiego poziomu bieżącego hosta.
- **WWW** - lista scenariuszy WWW bieżącego hosta.

Note:
Należy pamiętać, że sekcja konfiguracji jest dostępna tylko dla użytkowników typu Admin i Super admin.

Sekcja *Linki* zawiera linki do:

- dostępu do skonfigurowanego URL wyzwalacza.
- dostępu do niestandardowych linków skonfigurowanych w Skryptach globalnych (o zakresie *Manual host action* i typie „URL").

Sekcja *Skrypty* umożliwia wykonywanie skryptów globalnych skonfigurowanych dla bieżącego hosta. Aby były dostępne w menu hosta, skrypty te muszą mieć zdefiniowany zakres jako *Manual host action*.

Obsługiwane lokalizacje

Menu hosta jest dostępne po kliknięciu nazwy hosta w różnych sekcjach frontend, na przykład:

- Widżety pulpitów, takie jak Problemy, Najpopularniejsze pozycje, Przegląd wyzwalaczy itp.
- Monitorowanie → Problemy
- Monitorowanie → Problemy → Szczegóły zdarzenia
- Monitorowanie → Hosty
- Monitorowanie → Hosty → Monitorowanie WWW
- Monitorowanie → Najnowsze dane
- Monitorowanie → Mapy
- Inwentaryzacja → Hosty
- Raporty → 100 najpopularniejszych wyzwalaczy

Menu hosta jest dostępne po kliknięciu ikony trzech kropek w sekcji Zbieranie danych → Hosty.

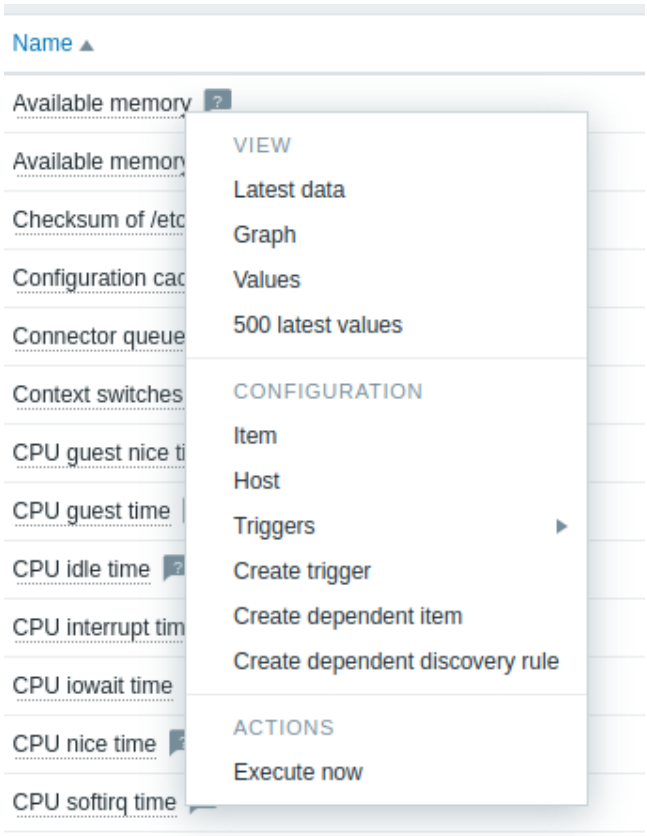
3 Menu pozycji

Przegląd

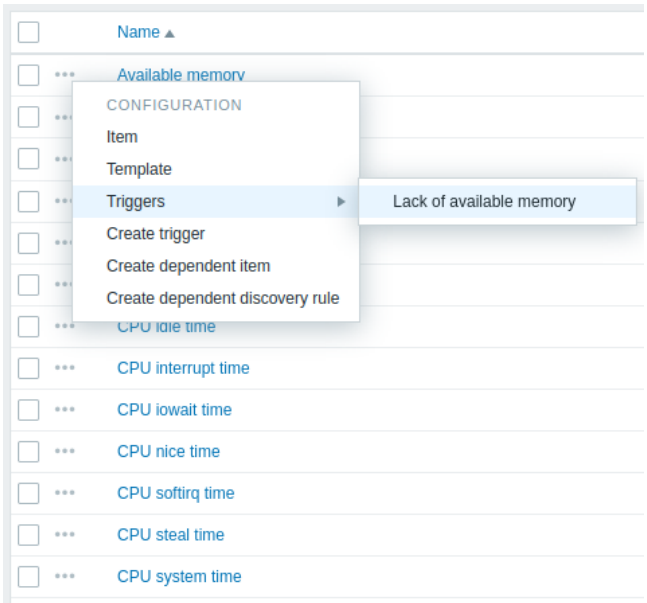
Menu pozycji zawiera skróty do działań lub sekcji frontend, które są często wymagane dla pozycji.

Menu pozycji można otworzyć, klikając nazwę pozycji lub ikonę z trzema kropkami, w zależności od sekcji frontend, na przykład:

Monitoring → Najnowsze dane



Zbieranie danych → Szablony → Pozycje



Zawartość

Menu pozycji ma trzy sekcje: *Widok*, *Konfiguracja* i *Działania*.

Sekcja *Widok* zawiera następujące opcje:

- **Najnowsze dane** - otwiera sekcję *Najnowsze dane* przefiltrowaną według bieżącego hosta i pozycji;
- **Wykres** - otwiera prosty wykres bieżącej pozycji;
- **Wartości** - otwiera listę wszystkich wartości odebranych dla bieżącej pozycji w ciągu ostatnich 60 minut;
- **500 najnowszych wartości** - otwiera listę 500 najnowszych wartości dla bieżącej pozycji.

Sekcja *Konfiguracja* (dostępna tylko dla użytkowników typu *Admin* i *Super admin*) zawiera następujące opcje:

- **Pozycja** - otwiera formularz konfiguracji pozycji bieżącej pozycji;
- **Szablon** - otwiera formularz konfiguracji szablonu szablonu, do którego należy pozycja (dostępne tylko wtedy, gdy menu pozycji jest otwierane z *Zbieranie danych* → *Szablony* → *Pozycje*);
- **Host** - otwiera formularz konfiguracji hosta hosta, do którego należy pozycja;
- **Wyzwalacze** - po najechaniu kursorem otwiera listę wyzwalaczy pozycji, jeśli istnieją; kliknięcie wyzwalacza otwiera jego formularz konfiguracji wyzwalacza;
- **Utwórz wyzwalacz** - otwiera formularz konfiguracji wyzwalacza w celu utworzenia wyzwalacza dla tej pozycji;
- **Utwórz pozycję zależną** - otwiera formularz konfiguracji pozycji w celu utworzenia pozycji zależnej, z bieżącą pozycją jako pozycją nadrzędną;
- **Utwórz zależną regułę wykrywania** - otwiera formularz konfiguracji reguły wykrywania w celu utworzenia zależnej reguły wykrywania, z bieżącą pozycją jako pozycją nadrzędną.

Sekcja *Działania* zawiera następującą opcję:

- **Wykonaj teraz** - natychmiast wykonuje sprawdzenie w celu pobrania nowej wartości pozycji.

Obsługiwane lokalizacje

Menu pozycji jest dostępne po kliknięciu nazwy pozycji w różnych sekcjach frontend, na przykład:

- Monitoring → Najnowsze dane
- Zbieranie danych → Hosts → Pozycje
- Zbieranie danych → Hosts → Reguły wykrywania → Prototypy pozycji

Menu pozycji jest dostępne po kliknięciu wartości pozycji w widżecie pulpitu Top items.

2 Sekcje frontend

Struktura menu Menu frontendu Zabbix ma następującą strukturę:

- Pulpity
- Monitorowanie
  - Problemy
  - Hosty
  - Najnowsze dane
  - Mapy
  - Odkrywanie
- Usługi
  - Usługi
  - SLA
  - Raport SLA
- Inwentaryzacja
  - Przegląd
  - Hosty
- Raporty
  - Informacje o systemie
  - Raporty cykliczne
  - Raport dostępności
  - 100 najważniejszych wyzwalaczy
  - Dziennik audytu
  - Dziennik działań
  - Powiadomienia
- Zbieranie danych
  - Grupy szablonów
  - Grupy hostów

    - Szablony
    - Hosty
    - Konserwacja
    - Korelacja zdarzeń
    - Odkrywanie
- Alerty
    - Działania
        * Działania wyzwalaczy
        * Działania usług
        * Działania odkrywania
        * Działania autorejestracji
        * Działania wewnętrzne
    - Typy mediów
    - Skrypty
- Użytkownicy
    - Grupy użytkowników
    - Role użytkowników
    - Użytkownicy
    - Tokeny API
    - Uwierzytelnianie
- Administracja
    - Ogólne
        * GUI
        * Autorejestracja
        * Limity czasu
        * Obrazy
        * Mapowanie ikon
        * Wyrażenia regularne
        * Opcje wyświetlania wyzwalaczy
        * Mapy geograficzne
        * Moduły
        * Konektory
        * Inne
    - Dziennik audytu
    - Porządkowanie
    - Grupy proxy
    - Proxy
    - Makra
    - Kolejka
        * Przegląd kolejki
        * Przegląd kolejki według proxy
        * Szczegóły kolejki

1 Pulpity

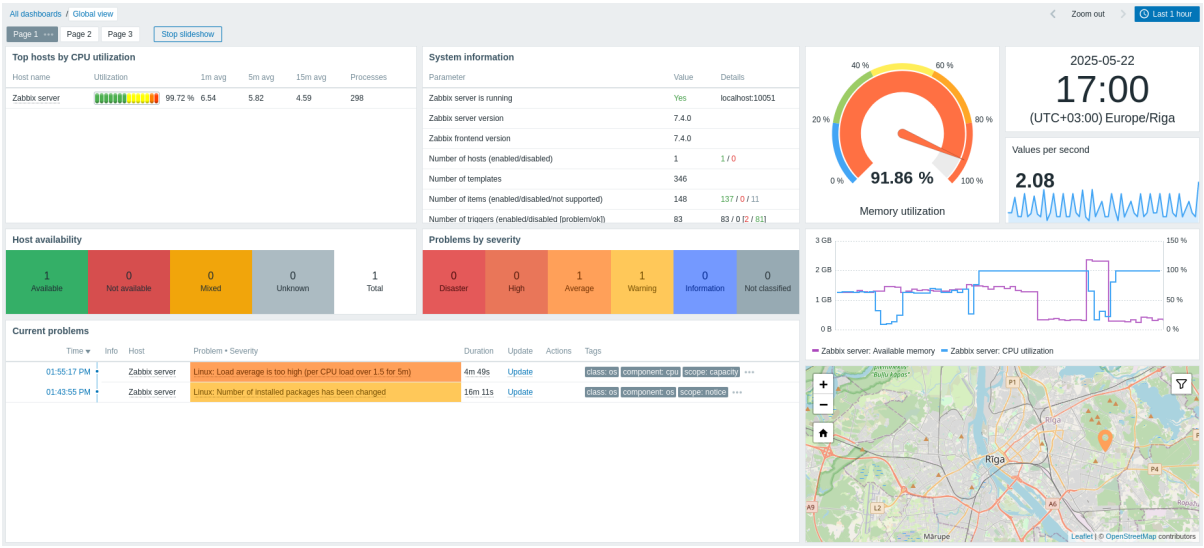
Przegląd

Sekcja *Pulpity* służy do wyświetlania podsumowań wszystkich ważnych informacji na **pulpicie**.

Chociaż w danym momencie może być wyświetlany tylko jeden pulpit, możliwe jest skonfigurowanie kilku pulpitów. Każdy pulpit może zawierać jedną lub kilka stron, które mogą być przełączane w formie pokazu slajdów.

Strona pulpitu składa się z widżetów, a każdy widżet jest przeznaczony do wyświetlania informacji określonego rodzaju i z określonego źródła, takich jak podsumowanie, mapa, wykres, zegar itp.

Dostęp do hostów w widżetach zależy od uprawnień do hostów.



Strony i widżety są dodawane do pulpitu oraz edytowane w trybie edycji pulpitu. Strony mogą być wyświetlane i przełączane w trybie widoku.

Okres czasu wyświetlany w widżetach wykresów jest kontrolowany przez selektor okresu czasu znajdujący się nad widżetami. Jego etykieta wyświetla aktualnie wybrany okres czasu. Kliknięcie etykiety umożliwia rozwinięcie i zwinięcie selektora okresu czasu.

Rozmiar pulpitu

Minimalna szerokość pulpitu wynosi 1200 pikseli. Pulpit nie zmniejszy się poniżej tej szerokości; zamiast tego zostanie wyświetlony poziomy pasek przewijania, jeśli okno przeglądarki będzie mniejsze.

Maksymalna szerokość pulpitu jest równa szerokości okna przeglądarki. Widgety pulpitu rozciągają się poziomo, aby dopasować się do okna. Jednocześnie widget pulpitu nie może zostać rozciągnięty poziomo poza granice okna.

W poziomie pulpit składa się z 72 kolumn o zawsze jednakowej szerokości, które dynamicznie się rozszerzają/zwężają (ale nie do mniej niż łącznie 1200 pikseli).

W pionie pulpit może zawierać maksymalnie 64 wiersze; każdy wiersz ma stałą wysokość 70 pikseli.

Widget może więc mieć maksymalnie 72 kolumny szerokości i 64 wiersze wysokości.

Wyświetlanie pulpitów

Aby wyświetlić wszystkie skonfigurowane pulpity, kliknij *All dashboards* tuż pod tytułem sekcji.



Pulpity są wyświetlane z etykietą udostępniania:

- *My* — oznacza pulpit należący do bieżącego użytkownika
- *Shared* — oznacza pulpit publiczny lub pulpit prywatny udostępniony dowolnemu użytkownikowi albo grupie użytkowników

Należy pamiętać, że etykiety udostępniania są wyświetlane tylko dla pulpitów należących do bieżącego użytkownika. Pulpity należące do innych użytkowników są wyświetlane bez etykiet udostępniania.

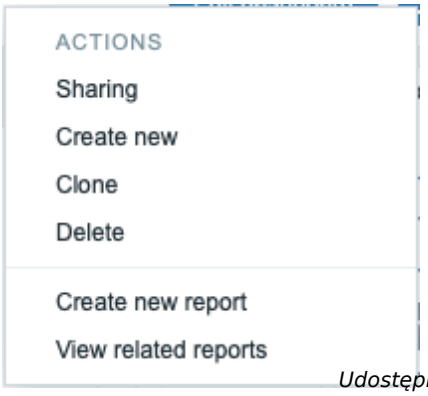
Filtr znajdujący się po prawej stronie nad listą umożliwia filtrowanie pulpitów według nazwy oraz według tych utworzonych przez bieżącego użytkownika.

Aby usunąć jeden lub kilka pulpitów, zaznacz pola wyboru odpowiednich pulpitów i kliknij *Delete* pod listą.

Wyświetlanie pulpitu

Aby wyświetlić pojedynczy pulpit, kliknij jego nazwę na liście pulpitów.

Podczas **wyświetlania** pulpitu dostępne są następujące opcje:

Edit dashboard	Przełącz do trybu **edycji** pulpitu. Tryb edycji jest również otwierany podczas tworzenia nowego pulpitu oraz po kliknięciu przycisku edycji widżetu.
	Otwórz menu działań (zobacz opisy działań poniżej).
	*Udostępnianie* - edytuj ustawienia udostępniania dla pulpitu. *Utwórz nowy* - utwórz nowy pulpit. *Klonuj* - utwórz nowy pulpit, kopiując właściwości istniejącego. Najpierw zostaniesz poproszony o wprowadzenie parametrów pulpitu. Następnie nowy pulpit otworzy się w trybie edycji ze wszystkimi widżetami oryginalnego pulpitu. *Usuń* - usuń pulpit. *Utwórz nowy raport* - otwórz wyskakujące okno z formularzem konfiguracji raportu. Opcja niedostępna, jeśli użytkownik nie ma uprawnień do zarządzania raportami cyklicznymi. *Wyświetl powiązane raporty* - otwórz wyskakujące okno z listą istniejących raportów opartych na bieżącym pulpicie. Opcja niedostępna, jeśli nie ma powiązanych raportów lub użytkownik nie ma uprawnień do wyświetlania raportów cyklicznych.
	Wyświetlaj tylko zawartość strony (tryb kiosk). Do trybu kiosk można również przejść za pomocą następujących parametrów URL: `/zabbix.php?action=dashboard.view&kiosk=1`. Aby wrócić do trybu normalnego: `/zabbix.php?action=dashboard.view&kiosk=0`.

Udostępnianie

Pulpity można ustawić jako publiczne lub prywatne.

Publiczne pulpity są widoczne dla wszystkich użytkowników. Prywatne pulpity są widoczne tylko dla ich właściciela oraz dla użytkowników/grup użytkowników dodanych w ustawieniach udostępniania.

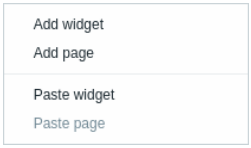
Aby edytować status udostępniania pulpitu, kliknij opcję *Udostępnianie* w menu działań podczas wyświetlania pojedynczego pulpitu:

Parameter	Description
Type	Wybierz typ pulpitu: **Prywatny** — pulpit jest widoczny tylko dla wybranych grup użytkowników i użytkowników. **Publiczny** — pulpit jest widoczny dla wszystkich.
List of user group shares	Wybierz grupy użytkowników, którym pulpit ma być dostępny. Możesz zezwolić na dostęp tylko do odczytu lub do odczytu i zapisu.
List of user shares	Wybierz użytkowników, którym pulpit ma być dostępny. Możesz zezwolić na dostęp tylko do odczytu lub do odczytu i zapisu.

Zobacz Uprawnienia do pulpitów, aby dowiedzieć się, jak opcje udostępniania ograniczają działania dostępne dla użytkowników.

Edycja pulpitu

Podczas **edycji** pulpitu dostępne są następujące opcje:

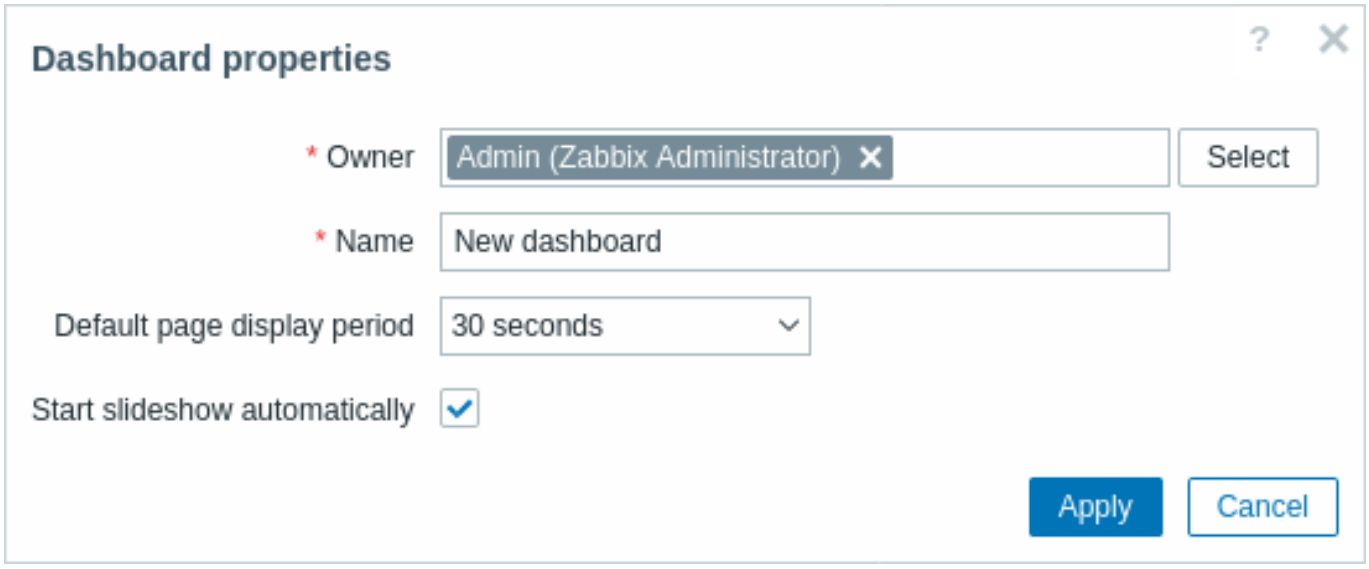
	Edytuj ogólne parametry pulpitu. Dodaj nowy widżet. Kliknięcie przycisku strzałki otworzy menu działań (zobacz opisy działań poniżej).
	*Dodaj widżet* - dodaj nowy widżet. *Dodaj stronę* - dodaj nową stronę. *Wklej widżet* - wklej skopiowany widżet. Ta opcja jest wyszarzona, jeśli nie skopiowano żadnego widżetu. W danym momencie można skopiować tylko jeden obiekt (widżet lub stronę). *Wklej stronę* - wklej skopiowaną stronę. Ta opcja jest wyszarzona, jeśli nie skopiowano żadnej strony.
	Zapisz zmiany pulpitu.
	Anuluj zmiany pulpitu.

Tworzenie pulpitu

Nowy pulpit można utworzyć na dwa sposoby:

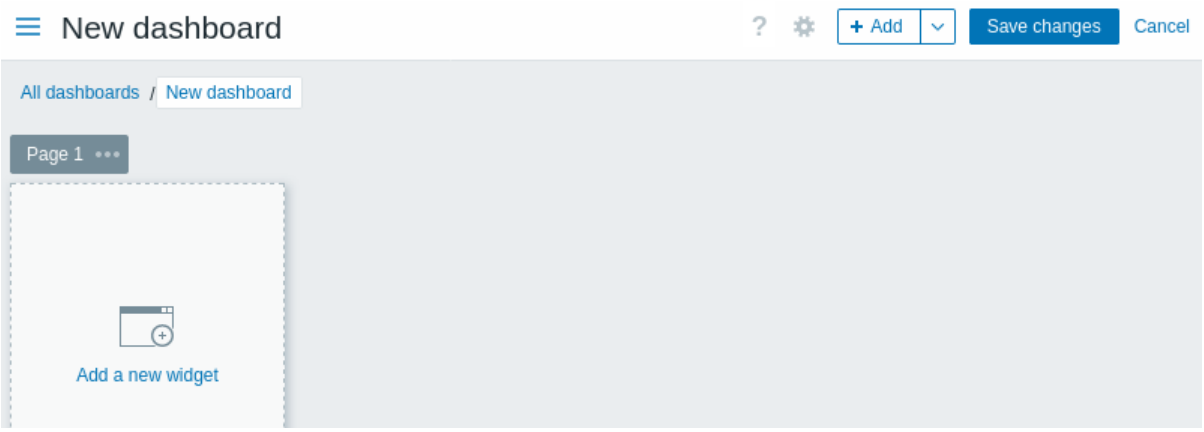
- Kliknij *Utwórz pulpit*, podczas przeglądania wszystkich pulpitów
- Wybierz *Utwórz nowy* z menu działań, podczas przeglądania pojedynczego pulpitu

Najpierw zostaniesz poproszony o wprowadzenie ogólnych parametrów pulpitu:



Parameter	Description
Właściciel	Wybierz użytkownika systemowego, który będzie właścicielem pulpitu.
Nazwa	Wprowadź nazwę pulpitu.
Domyślny okres wyświetlania strony	Wybierz okres, przez jaki strona pulpitu będzie wyświetlana przed przejściem do następnej strony w pokazie slajdów.
Uruchom pokaz slajdów automatycznie	Zaznacz to pole wyboru, aby automatycznie uruchomić pokaz slajdów, gdy istnieje więcej niż jedna strona pulpitu.

Po kliknięciu *Zastosuj* zostanie otwarty pusty pulpit:



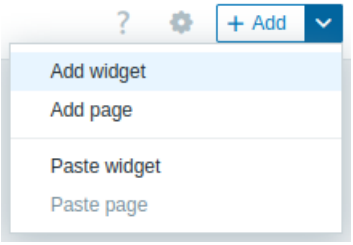
Aby wypełnić pulpit, możesz dodać widżety i strony.

Kliknij przycisk *Zapisz zmiany*, aby zapisać pulpit. Jeśli klikniesz *Anuluj*, pulpit nie zostanie utworzony.

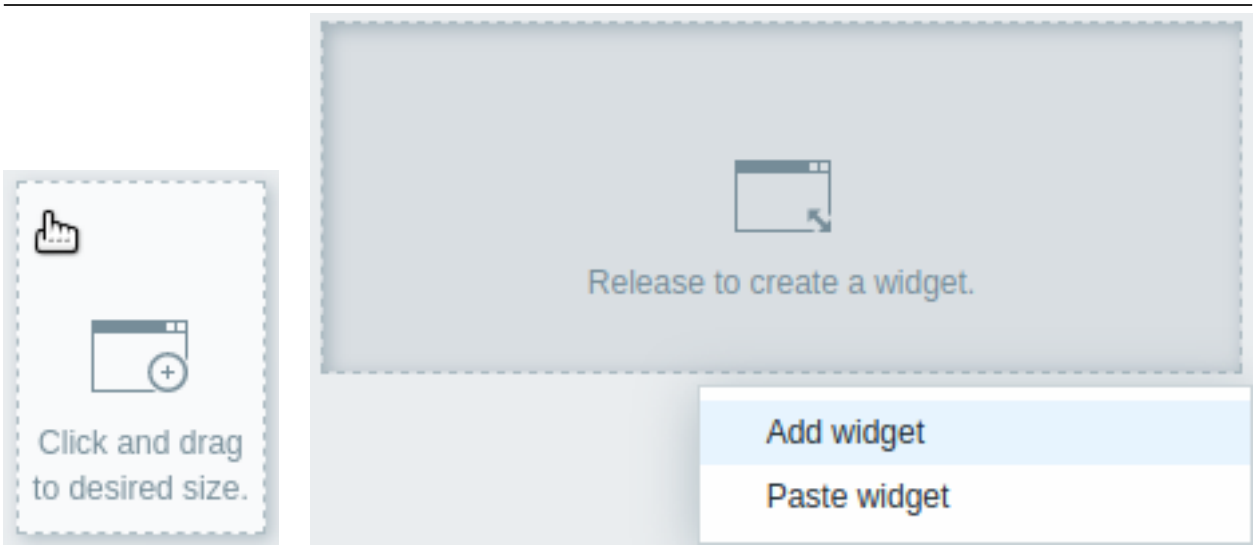
Dodawanie widgetów

Do pulpitu można dodawać różne widgety (dziennik działań, Zegar, status wykrywania itp.). Widgety można dodawać na dwa sposoby:

- Kliknij przycisk *Dodaj* lub strzałkę obok niego, a następnie wybierz *Dodaj widget* z menu działań. Po skonfigurowaniu widget zostanie dodany w domyślnym rozmiarze i umieszczony za wszystkimi istniejącymi widgetami.

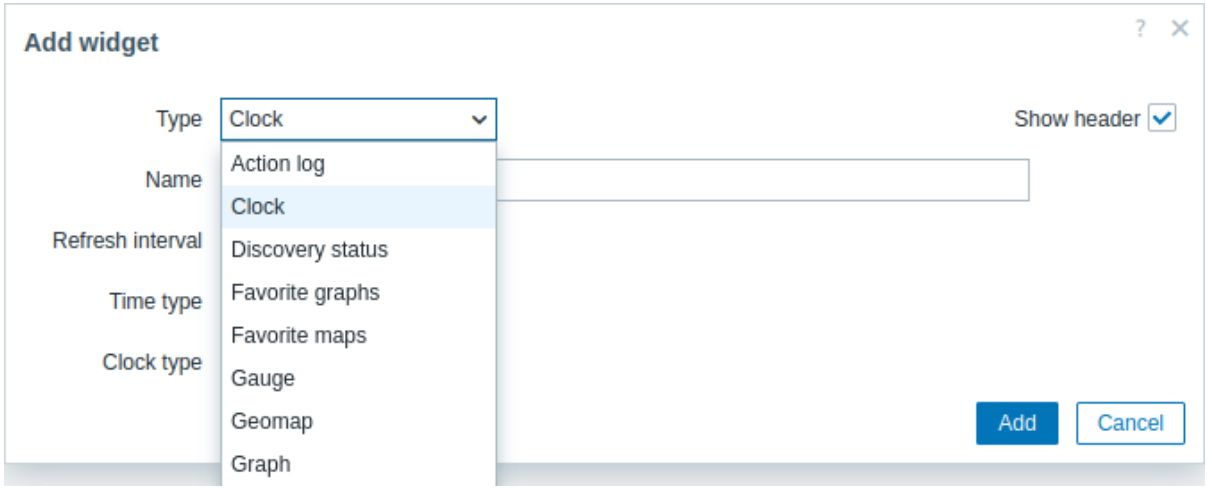


- Przesuń kursor myszy na puste miejsce na pulpicie. Zauważ, że pojawi się symbol zastępczy, a następnie kliknij go, aby otworzyć formularz konfiguracji widgetu. Po skonfigurowaniu widget zostanie dodany w domyślnym rozmiarze lub jego rozmiar zostanie zmieniony tak, aby pasował do dostępnej przestrzeni. Alternatywnie przeciągnij symbol zastępczy, aby określić rozmiar widgetu, i zwolnij go, aby otworzyć formularz konfiguracji widgetu (jeśli widget został skopiowany do schowka, najpierw pojawi się monit o wybór między *Dodaj widget* a *Wklej widget*).



W formularzu konfiguracji widgetu:

1. Wybierz typ widgetu.
2. Skonfiguruj parametry widgetu.
3. Kliknij *Dodaj*, aby dodać widget do pulpitu.



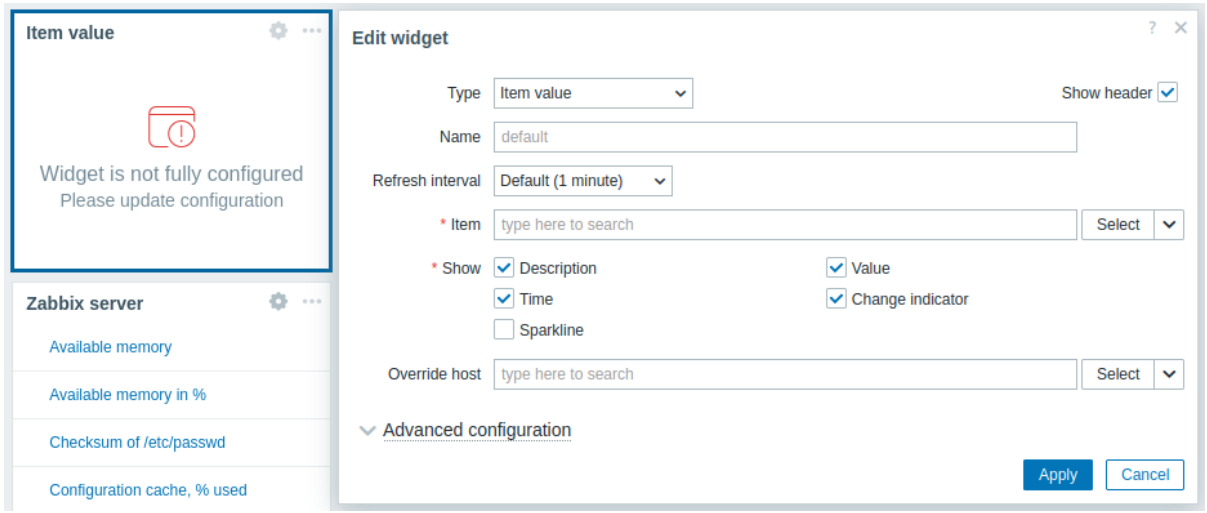
Edytowanie widgetów

Rozmiar widgetów można zmieniać, a ich położenie na pulpicie można modyfikować w trybie edycji, przeciągając ich pasek tytułu. Możesz także zmieniać położenie formularza konfiguracji widgetu, przeciągając jego pasek tytułu.

Każdy widget zawiera elementy sterujące w prawym górnym rogu:

-  - edytuj widget
- - otwórz menu widgetu

Podczas edycji widget jest podświetlony, a zmiany są wyświetlane w podglądzie w czasie rzeczywistym. Jeśli wymagane parametry widgetu nie są skonfigurowane, widget przechodzi do stanu *Widget is not fully configured*.



Po zakończeniu edycji kliknij *Zastosuj* w widżecie, a następnie *Zapisz zmiany* w prawym górnym rogu pulpitu, aby zastosować zmiany.

Kopiowanie/wklejanie widgetów

Możesz kopiować i wklejać widgety pulpitu, aby szybko tworzyć nowe widgety z tą samą konfiguracją. Widgety można kopiować i wklejać w obrębie tego samego pulpitu lub między pulpitami otwartymi w różnych kartach.

Aby skopiować widget, użyj menu widgetu. Aby wkleić skopiowany widget (dostępne w trybie edycji pulpitu):

- Kliknij strzałkę obok przycisku *Dodaj* i wybierz *Wklej widget*.
- Alternatywnie kliknij pusty obszar pulpitu i wybierz *Wklej widget*.

Możesz także wkleić skopiowany widget na istniejący widget, używając opcji *Wklej* w jego menu widgetu.

Tworzenie pokazu slajdów

Pokaz slajdów będzie uruchamiany automatycznie, jeśli dashboard zawiera co najmniej dwie strony (zobacz Dodawanie stron) oraz jeśli spełniony jest jeden z poniższych warunków:

- Opcja *Uruchom pokaz slajdów automatycznie* jest zaznaczona we właściwościach dashboardu
- URL dashboardu zawiera parametr `slideshow=1`

Strony są przełączane zgodnie z interwałami określonymi we właściwościach dashboardu i poszczególnych stron. Kliknij:

- *Zatrzymaj pokaz slajdów* - aby zatrzymać pokaz slajdów
- *Uruchom pokaz slajdów* - aby uruchomić pokaz slajdów



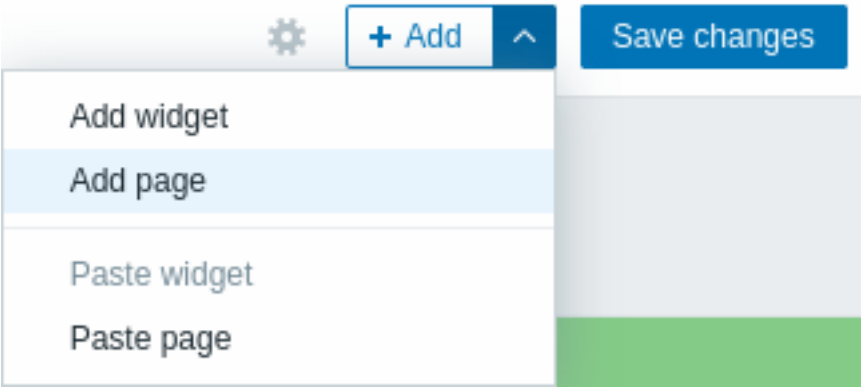
Elementy sterujące związane z pokazem slajdów są również dostępne w trybie kiosku (w którym wyświetlana jest tylko zawartość strony):

-  - zatrzymaj pokaz slajdów
-  - uruchom pokaz slajdów
-  - wróć o jedną stronę
-  - przejdź do następnej strony

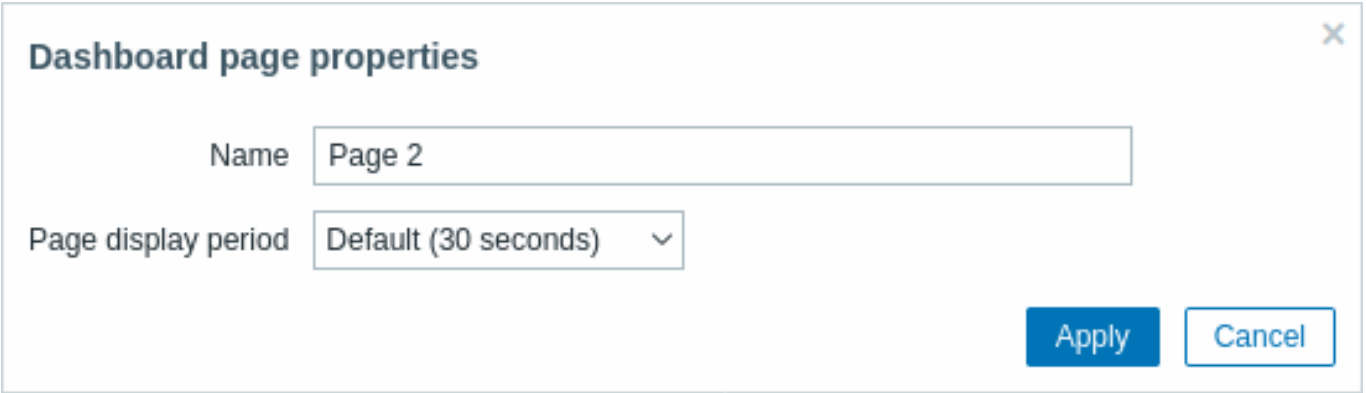
Dodawanie stron

Aby dodać nową stronę do pulpitu:

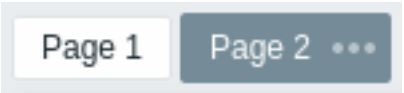
- Upewnij się, że pulpit znajduje się w trybie edycji
- Kliknij strzałkę obok przycisku *Dodaj* i wybierz opcję *Dodaj stronę*



- Wypełnij ogólne parametry strony i kliknij *Zastosuj*. Jeśli pozostawisz nazwę pustą, strona zostanie dodana z nazwą `Page N`, gdzie „N” jest kolejnym numerem strony. Okres wyświetlania strony pozwala dostosować, jak długo strona jest wyświetlana w pokazie slajdów.



Zostanie dodana nowa strona, oznaczona nową kartą (*Page 2*).



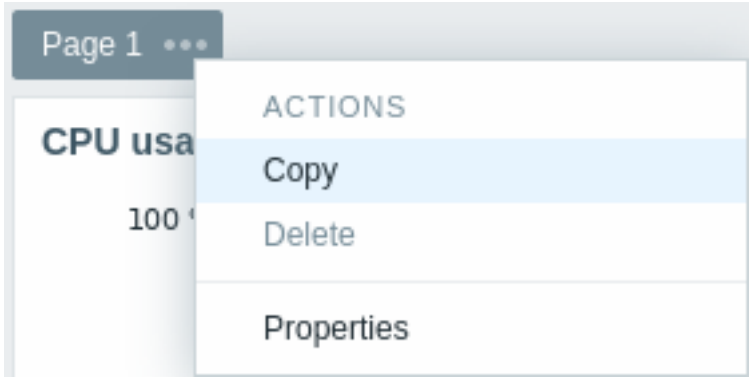
Strony można zmieniać kolejnością metodą przeciągnij i upuść, przeciągając karty stron. Zmiana kolejności zachowuje oryginalne nazewnictwo stron. Zawsze można przejść do każdej strony, klikając jej kartę.

Po dodaniu nowej strony jest ona pusta. Możesz dodać do niej widgety, jak opisano powyżej.

Kopiowanie/wklejanie stron

Strony pulpitu mogą być kopiowane i wklejane, co pozwala utworzyć nową stronę z właściwościami istniejącej. Można je wklejać z tego samego pulpitu lub z innego pulpitu.

Aby wkleić istniejącą stronę do pulpitu, najpierw skopiuj ją, używając menu strony:

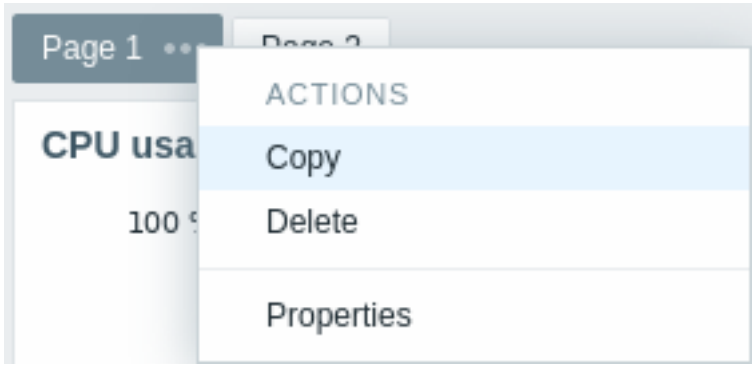


Aby wkleić skopiowaną stronę:

- Upewnij się, że pulpit jest w trybie edycji
- Kliknij strzałkę obok przycisku *Dodaj* i wybierz opcję *Wklej stronę*

Menu strony

Menu strony można otworzyć, klikając trzy kropki  obok nazwy strony:

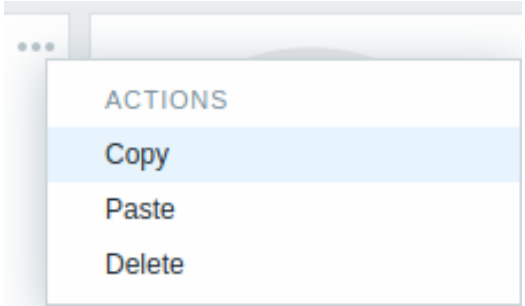


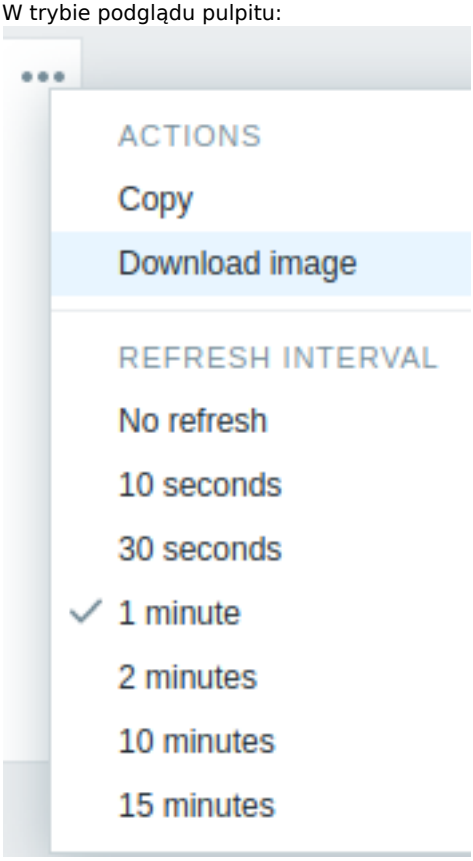
Zawiera ono następujące opcje:

- *Kopiuj* - skopiuj stronę
- *Usuń* - usuń stronę (strony można usuwać tylko w trybie edycji pulpitu)
- *Właściwości* - dostosuj parametry strony (nazwę i czas wyświetlania strony w pokazie slajdów)

Menu widgetu

Menu widgetu zawiera różne opcje w zależności od tego, czy pulpit znajduje się w trybie edycji, czy podglądu:

Menu widgetu	Opcje
W trybie edycji pulpitu: 	*Kopiuj* - skopiuj widget. *Wklej* - wklej skopiowany widget w miejsce tego widgetu. Ta opcja jest wyszarzona, jeśli nie skopiowano żadnego widgetu. *Usuń* - usuń widget.

Menu widgetu	Opcje
W trybie podglądu pulpitu: 	*Kopiuj* - skopiuj widget. *Pobierz obraz* - pobierz widget jako obraz PNG. Ta opcja jest dostępna dla widgetów, które obsługują tę funkcję (zobacz strony poszczególnych widgetów). W zależności od ustawień przeglądarki obraz jest automatycznie zapisywany w folderze Pobrane lub otwierane jest okno dialogowe zapisu, umożliwiające wybór lokalizacji. *Interwał odświeżania* - wybierz częstotliwość odświeżania zawartości widgetu

Uprawnienia do pulpitów

Uprawnienia do pulpitów dla zwykłych użytkowników oraz użytkowników typu „Admin” (pod warunkiem, że dostęp do pulpitów oraz opcja *Create and edit dashboards* są włączone dla roli użytkownika, która jest im przypisana) są ograniczone w sposób opisany poniżej.

- Mogą wyświetlać i klonować publiczny pulpit, nawet jeśli w ustawieniach udostępniania pulpitu nie dodano żadnych użytkowników ani grup użytkowników.
- Mogą wyświetlać i klonować prywatny pulpit, jeśli mają do niego co najmniej uprawnienia *Read* ustawione za pomocą ustawień udostępniania.
- Mogą edytować i usuwać pulpit tylko wtedy, gdy mają do niego uprawnienia *Read-write* ustawione za pomocą ustawień udostępniania.
- Nie mogą zmienić właściciela pulpitu.

1 Widżety pulpitu nawigacyjnego

Przegląd

Zabbix udostępnia różnorodne widgety pulpitu, które wizualizują i podsumowują dane monitoringu, zapewniając przejrzysty przegląd wydajności i dostępności systemu.

Poniżej znajduje się przegląd wszystkich widgetów, pogrupowanych według ich głównego przeznaczenia.

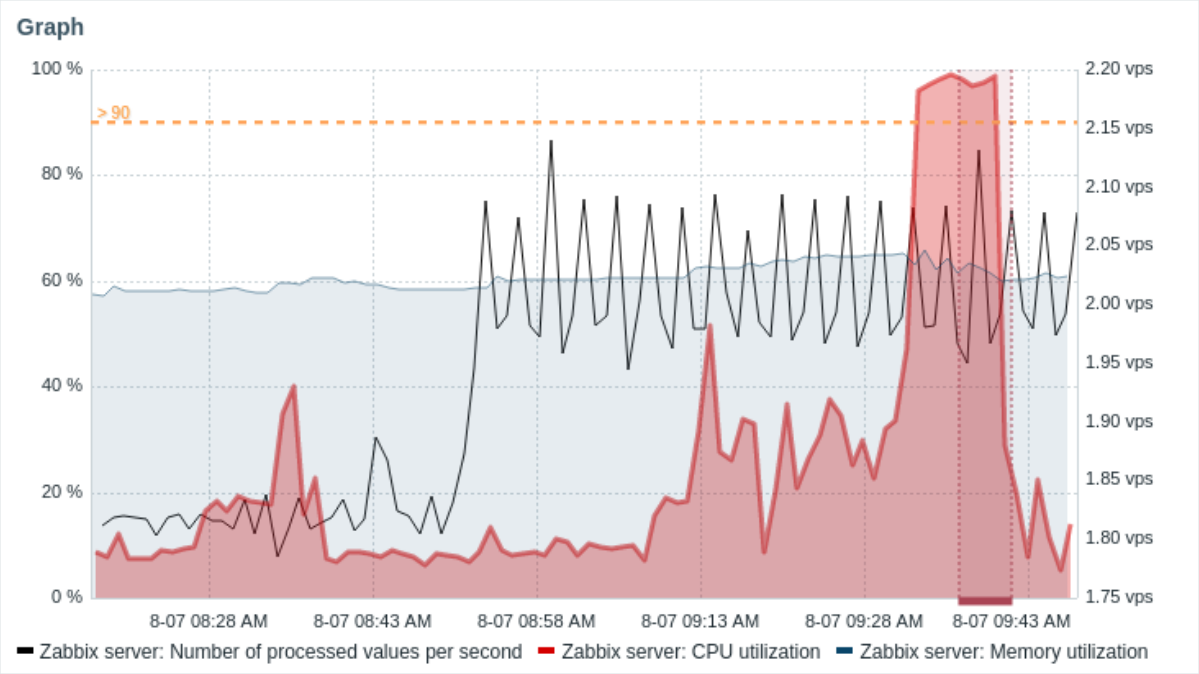
Szczegółowe informacje dotyczące konfiguracji widgetów można znaleźć w sekcji Parametry widgetów pulpitu.

Wizualizacja danych

Te widżety prezentują dane w różnych formatach wizualnych, pomagając monitorować dane i problemy na różne sposoby.

Wykres

Widżet Graph wyświetla dane numeryczne pozycji w postaci wykresu wektorowego. Może pomóc w śledzeniu metryk, wykrywaniu problemów oraz porównywaniu wartości w czasie i pomiędzy hostami.

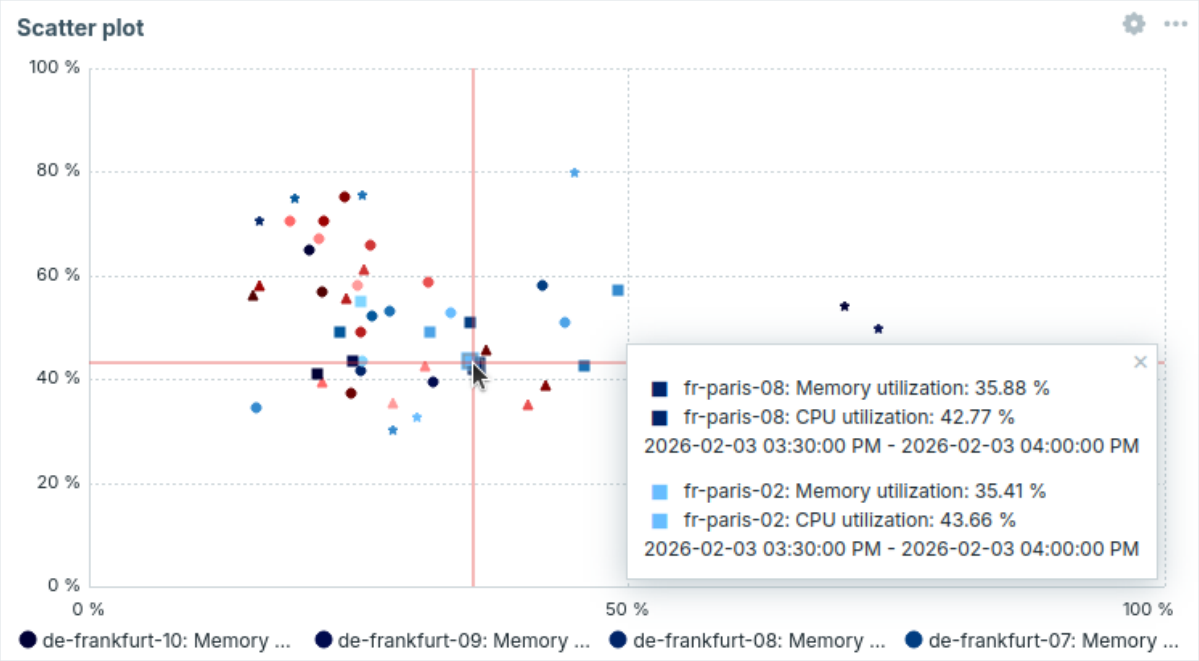


Zobacz także:

- Graph (classic) — starszy widżet Graph, który wyświetla dane numeryczne pozycji w postaci wykresu opartego na obrazie.
- Graph prototype — wyświetla siatkę automatycznie tworzonych niestandardowych wykresów na podstawie prototypów wykresów lub prototypów pozycji z reguły wykrywania niskiego poziomu.
- Favorite graphs — wyświetla alfabetyczną listę skrótów do wykresów oznaczonych przez bieżącego użytkownika jako ulubione.

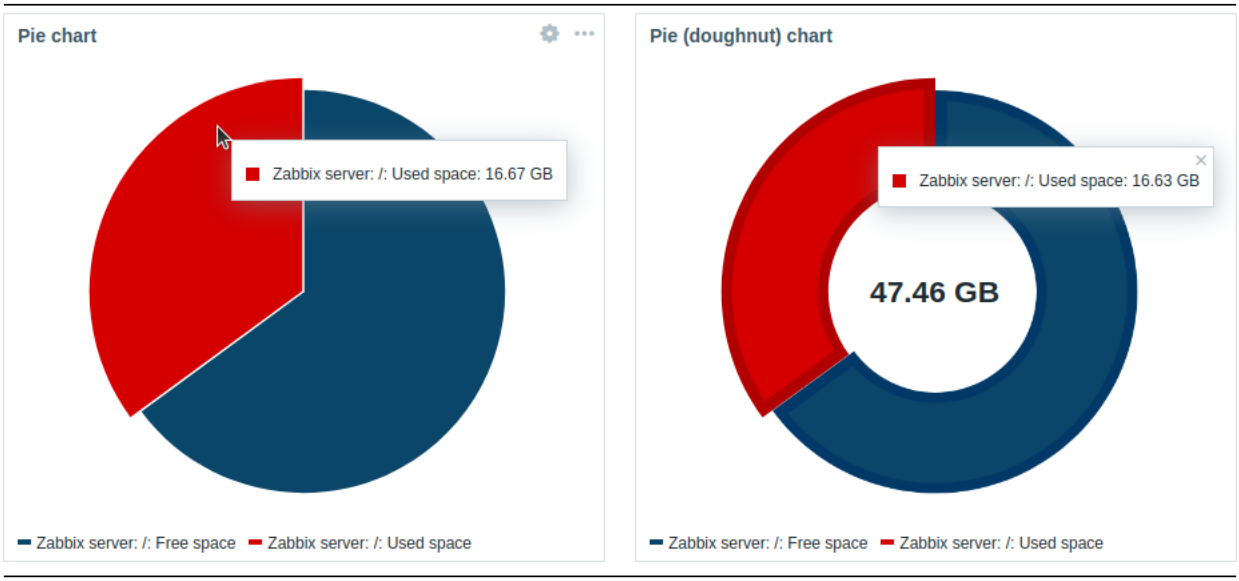
Wykres punktowy

Widżet Scatter plot wyświetla zależność między dwiema metrykami, nanosząc pojedyncze punkty danych wzdłuż osi X i Y. Pomaga to ujawnić wzorce, skupiska, korelacje i wartości odstające w zbiorze danych.



Wykres kołowy

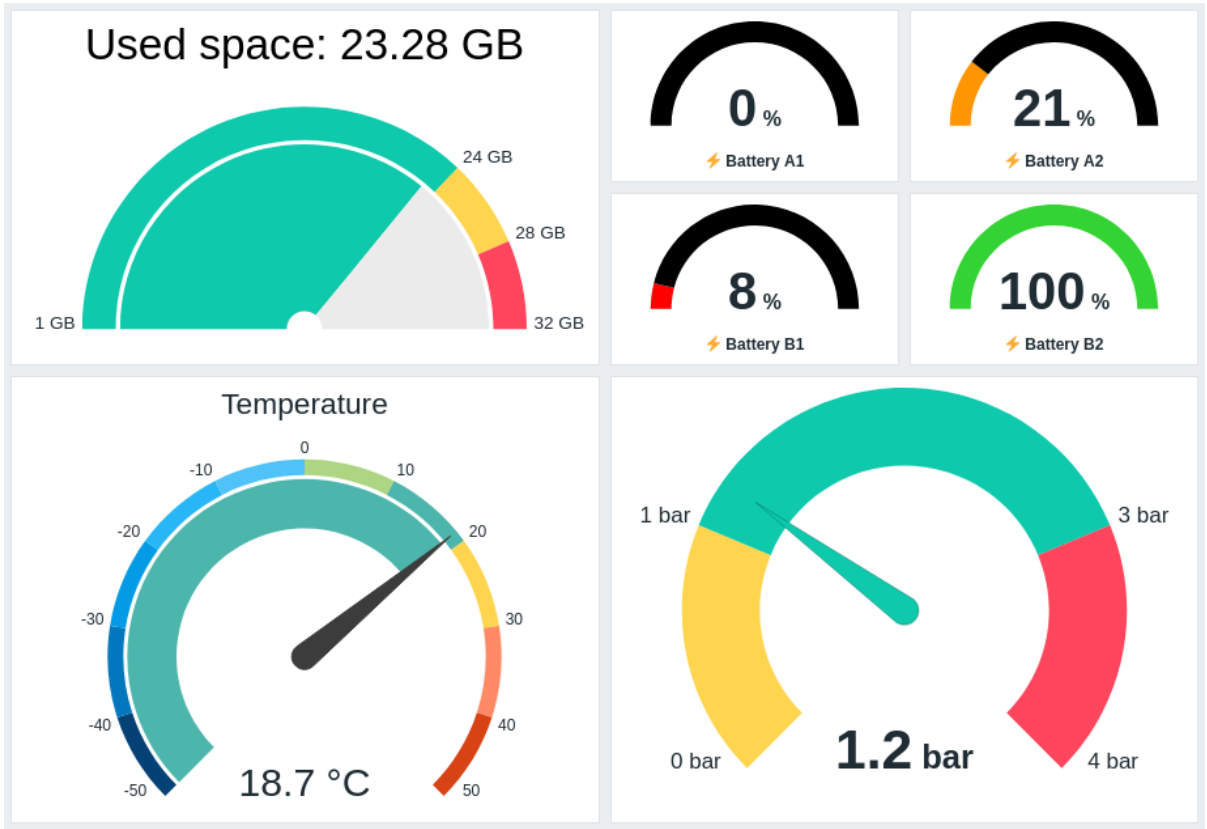
Widżet Wykres kołowy wyświetla numeryczne dane pozycji jako wektorowy wykres kołowy lub pierścieniowy. Ten widżet może pomóc zwizualizować, w jaki sposób pozycje lub hosty wpływają na cały zbiór danych.



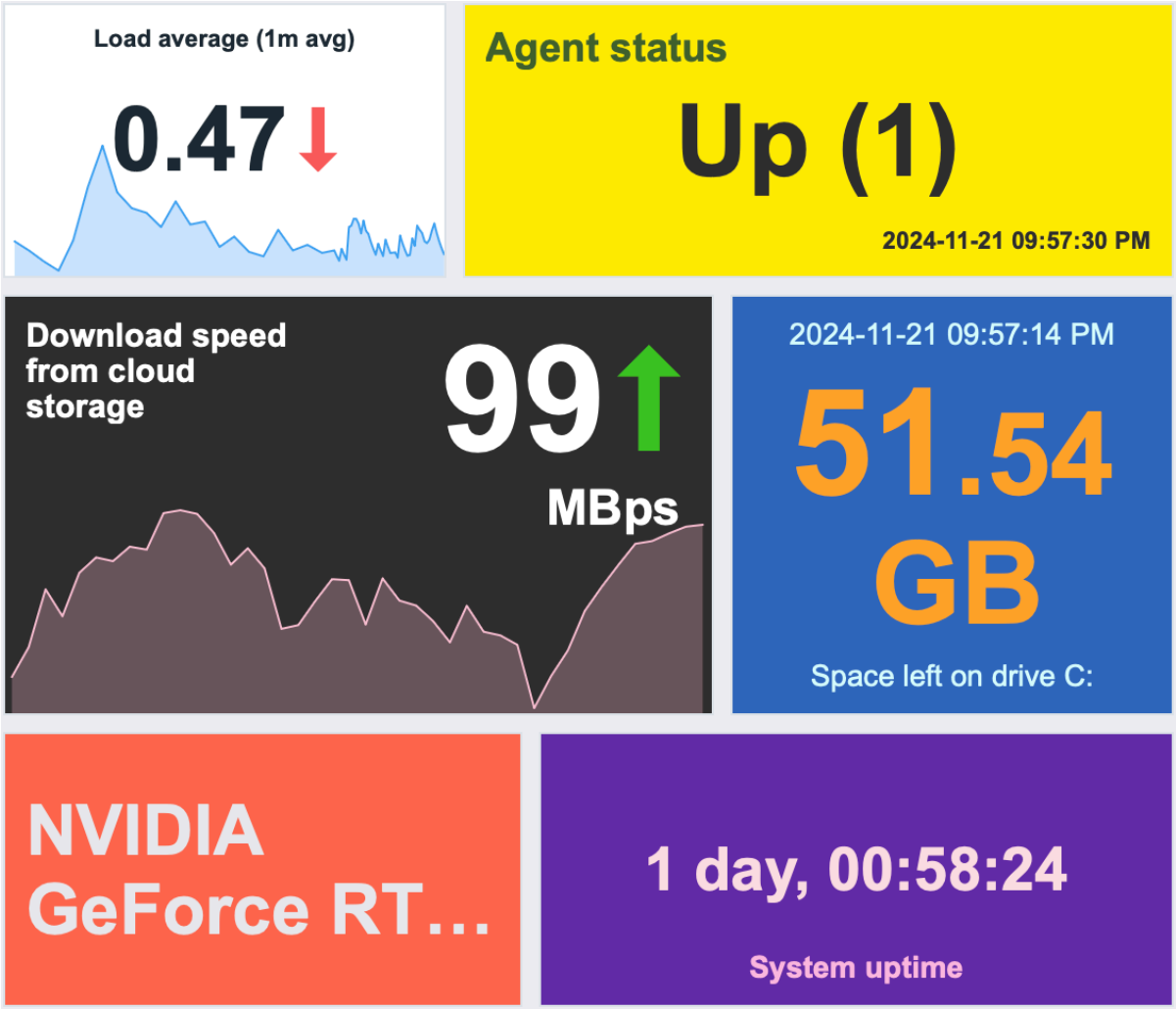
Wskaźnik/Wartość pozycji

Widżety Wskaźnik/Wartość pozycji wyświetlają wartość pojedynczej pozycji, co jest przydatne do śledzenia ważnych metryk, wizualizacji progów oraz wykrywania nagłych zmian w danych.

Widżet Wskaźnik:



Widżet Wartość pozycji:



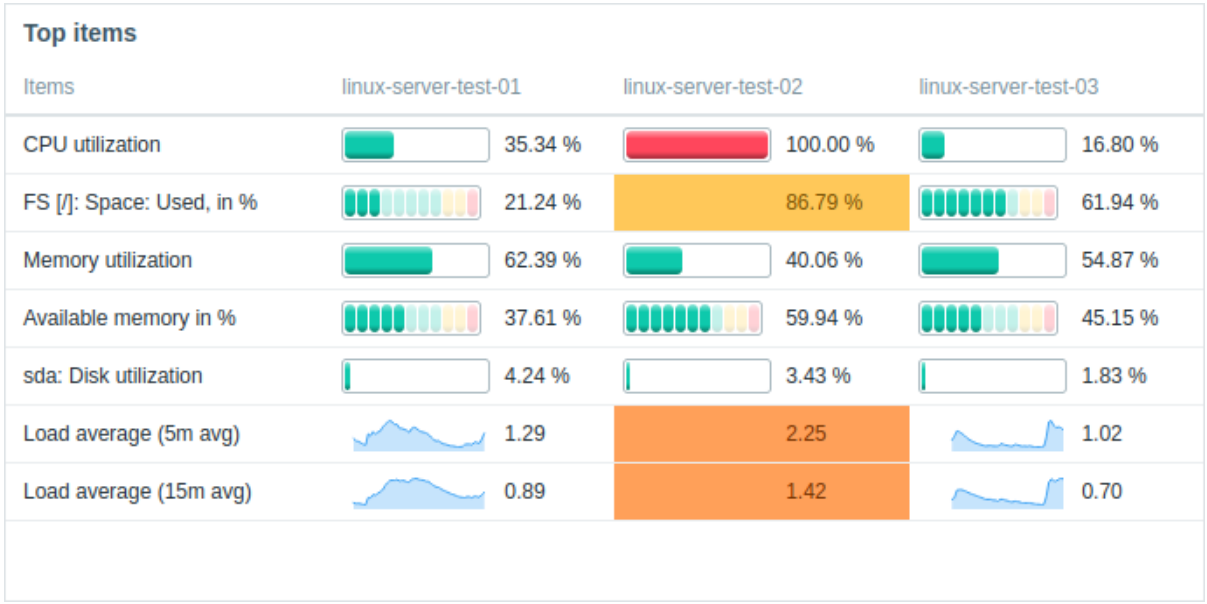
Historia pozycji

Widżet Historia pozycji wyświetla najnowsze dane dla wszystkich typów pozycji (numerycznych, tekstowych itp.) w formacie tabeli. Może wyświetlać paski postępu i obrazy (przydatne w przypadku pozycji przeglądarki) oraz wyróżniać wartości (przydatne przy monitorowaniu plików dziennika).



Najlepsze pozycje

Widżet Top items wyświetla najwyższe/najniższe wartości dla wybranych pozycji, zapewniając szybki przegląd ich wydajności.

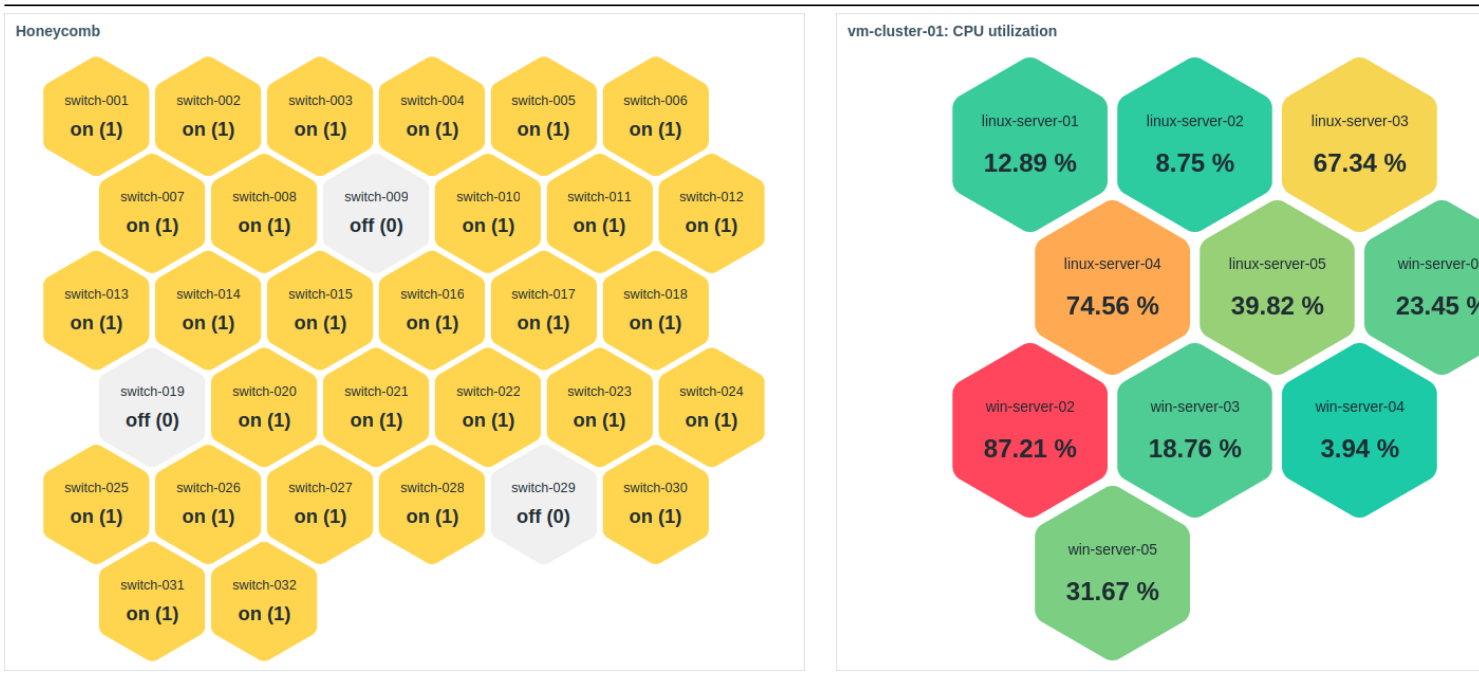


Zobacz także:

- Top hosts — wyświetla najwyższe/najniższe wartości dla wybranych pozycji z wielu hostów.
- Top triggers — wyświetla wyzwalacze z największą liczbą problemów.

Honeycomb

Widżet Honeycomb wyświetla hosty lub pozycje jako sześciokątne komórki w siatce. Ten układ ułatwia wykrywanie hostów/pozycji z problemami, dostrzeganie skupisk problemów, porównywanie grup na pierwszy rzut oka i nie tylko.

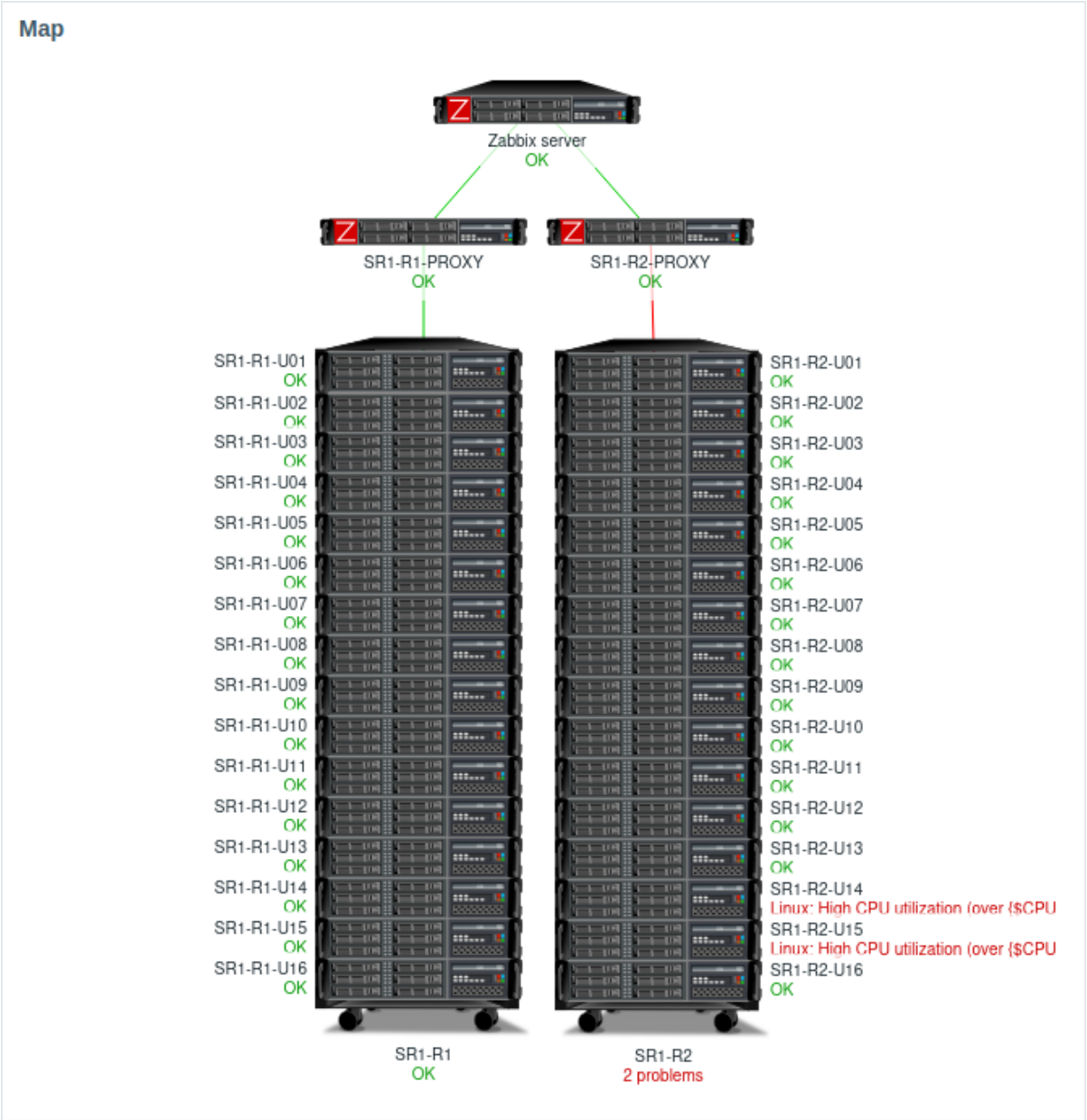


Mapy

Widżety map wizualizują topologię sieci lub lokalizacje hostów, pomagając ocenić ogólny stan oraz stan w poszczególnych lokalizacjach.

Mapa

Widżet Mapa może wyświetlać mapę sieci lub podobną wizualizację, zapewniając dynamiczny przegląd sieci.

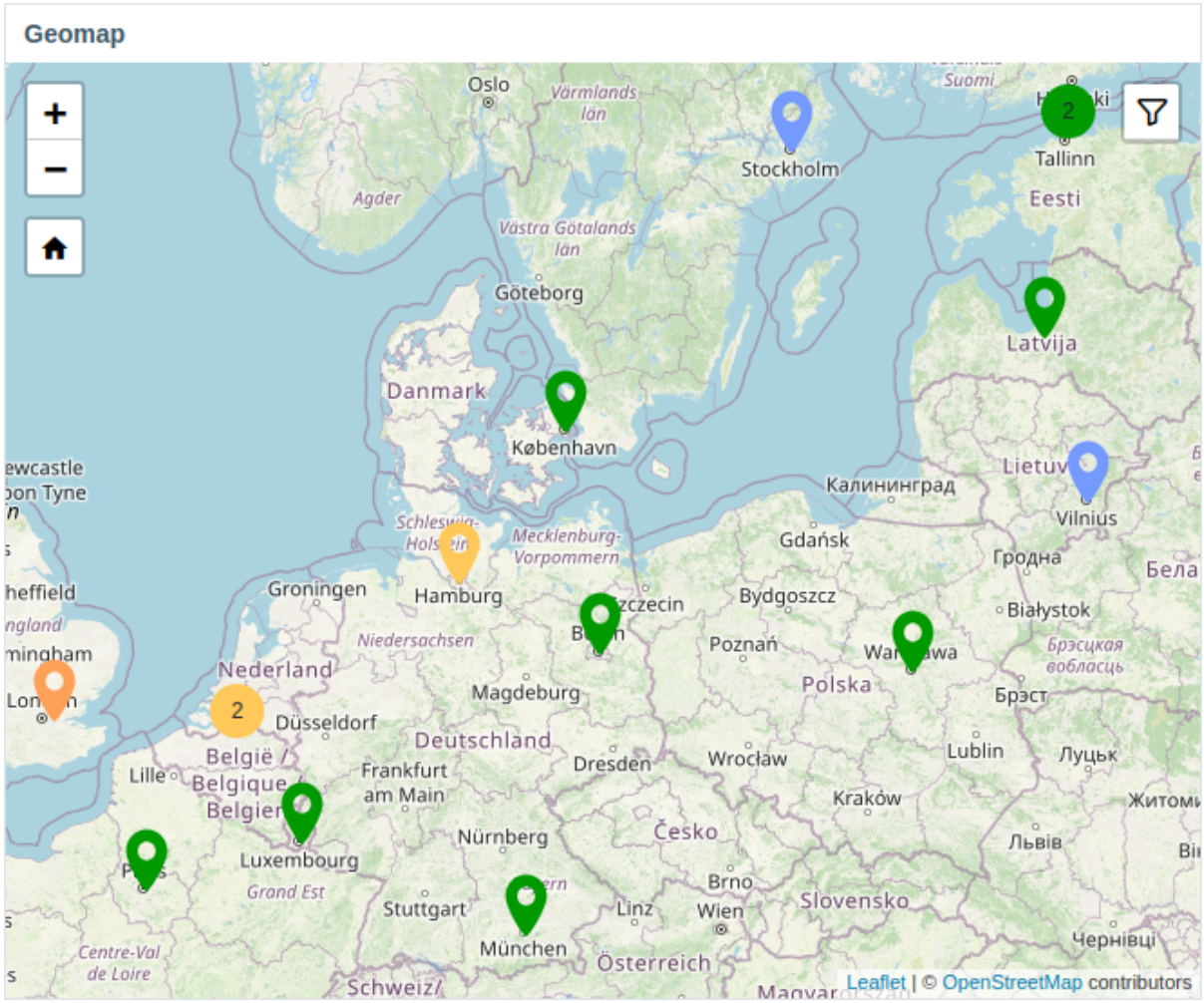


Zobacz także:

- Drzewo nawigacji map — wyświetla hierarchię istniejących map oraz liczbę problemów dla każdej mapy i grupy map.
- Ulubione mapy — wyświetla listę skrótów do map oznaczonych przez bieżącego użytkownika jako ulubione, posortowaną alfabetycznie.

Geomap

Widżet Geomap wyświetla hosty jako znaczniki na interaktywnej mapie opartej na Leaflet, przy czym kolory znaczników wskazują najpoważniejszy problem każdego hosta.

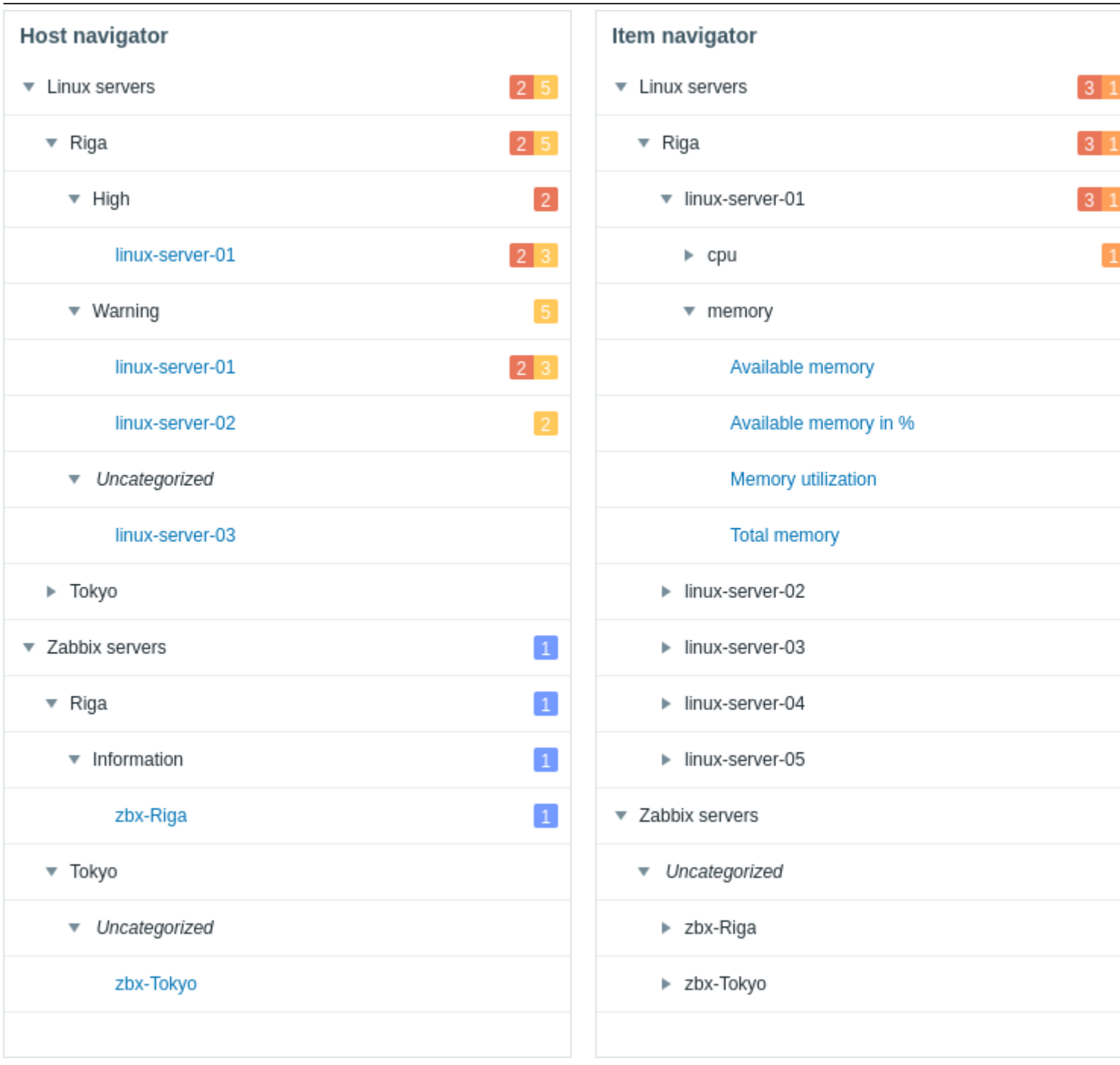


Szczegóły hosta/pozycji

Te widgety udostępniają listy oraz szczegółowe widoki hostów lub pozycji.

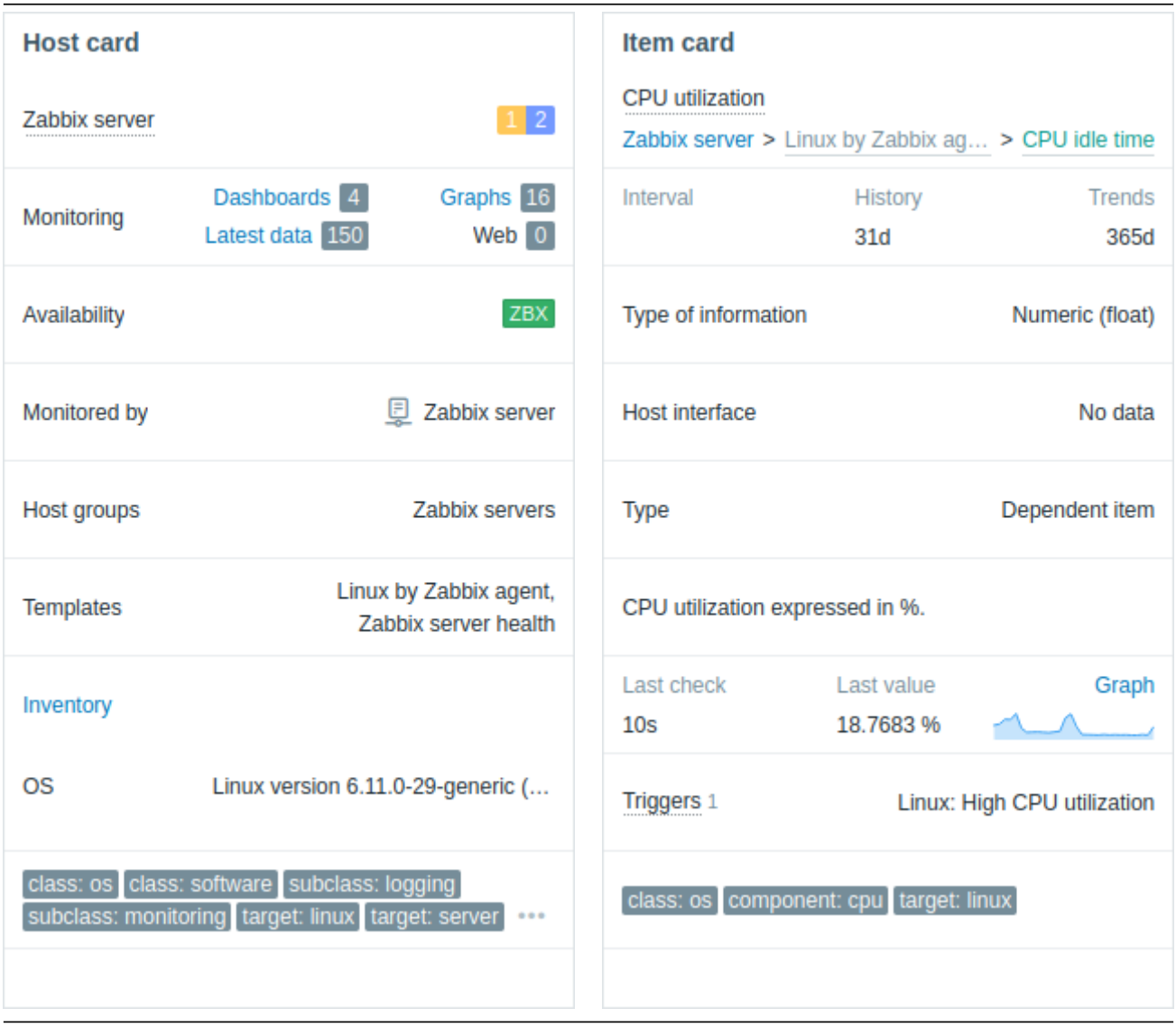
Nawigator hostów/pozycji

Widżety Nawigator hostów/Nawigator pozycji wyświetlają listę hostów/pozycji na podstawie różnych opcji filtrowania i grupowania. Te widżety są najbardziej przydatne do sterowania tym, co wyświetlają inne widżety, na podstawie wybranego hosta/pozycji.



Karta hosta/pozycji

Widżety Karta hosta/Karta pozycji wyświetlają szczegóły pojedynczego hosta/pozycji, umożliwiając szybkie sprawdzenie stanu i konfiguracji hosta lub pozycji (dostępność hosta, problemy, inwentarz, najnowsze dane pozycji, błędy, opis itp.).

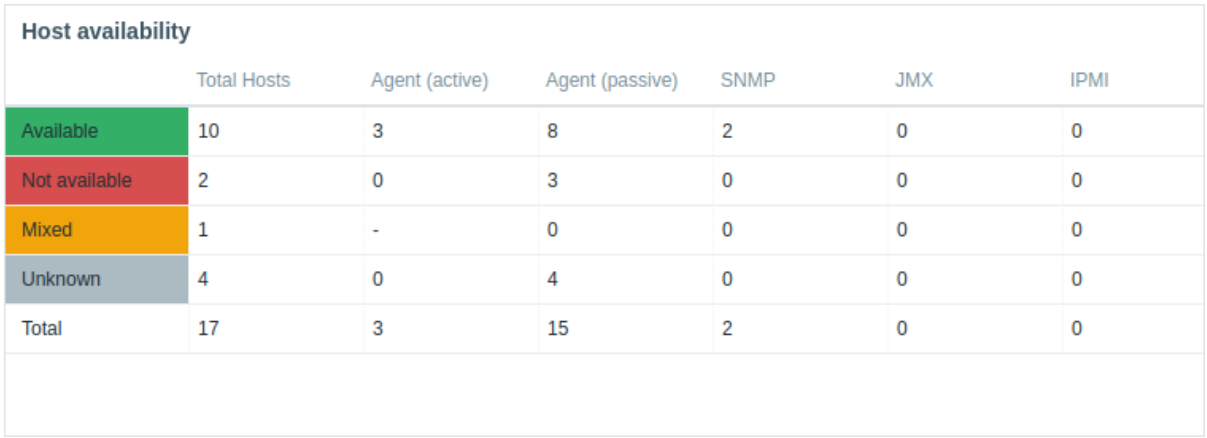


Status i raporty

Te widgety wyświetlają dane o stanie (np. dostępność, wyzwalacze, problemy), a także raporty.

Dostępność hostów

Widżet Dostępność hostów wyświetla dostępność hostów w wybranych grupach hostów, umożliwiając monitorowanie liczby hostów, które są dostępne lub niedostępne.

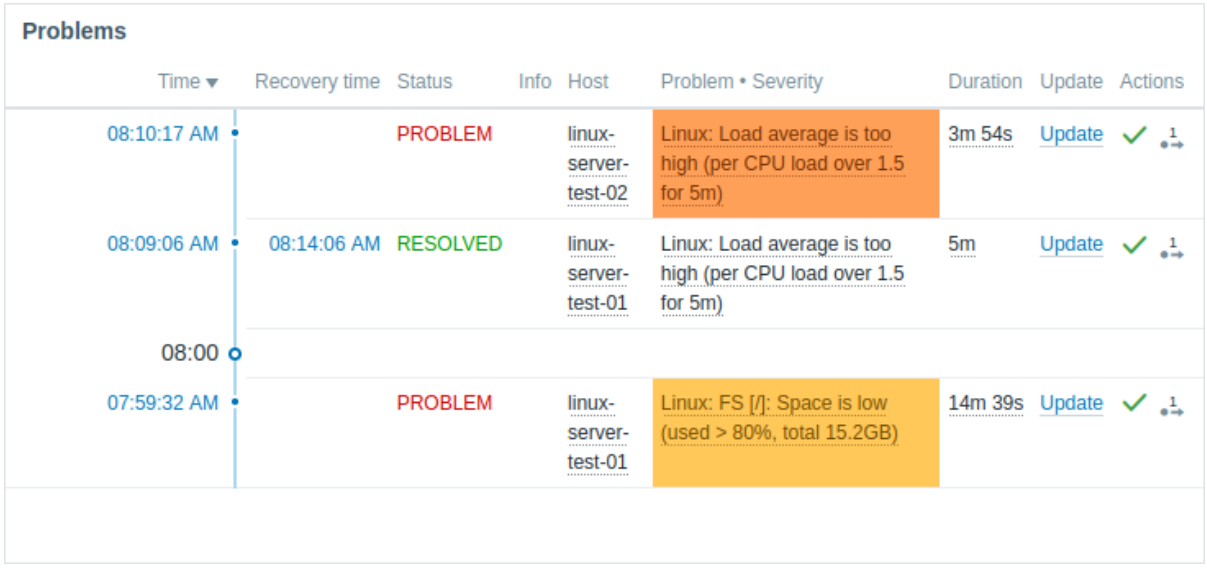


Host availability

	Total Hosts	Agent (active)	Agent (passive)	SNMP	JMX	IPMI
Available	10	3	8	2	0	0
Not available	2	0	3	0	0	0
Mixed	1	-	0	0	0	0
Unknown	4	0	4	0	0	0
Total	17	3	15	2	0	0

Problemy

Widżet Problems wyświetla bieżące problemy filtrowane według różnych parametrów (grupy hostów, hosty, nazwy problemów itp.), zapewniając przejrzysty widok tego, co wymaga uwagi.



Zobacz także:

- Problems by severity — wyświetla liczbę problemów przyczyn pogrupowanych według ważności.
- Problem hosts — wyświetla liczbę problemów przyczyn na grupę hostów i pokazuje najwyższą ważność problemu w każdej grupie.

Przegląd wyzwalaczy

Widżet Trigger overview wyświetla bieżące stany wyzwalaczy hostów w postaci tabeli z kolorowymi blokami. Zapewnia szybki wizualny podgląd kondycji i aktywności wyzwalaczy na różnych hostach.



Dziennik działań

Widżet Action log wyświetla szczegóły operacji (powiadomień, zdalnych poleceń) wykonywanych w ramach działania. Szczegółowy dziennik pomaga w audycie, rozwiązywaniu problemów i monitorowaniu wykonania każdego działania.

Action log

Time ▾	Action	Media type	Recipient	Message	Status	Info
2025-08-15 07:58:30 AM	Report problems to Zabbix administrators	Email	Admin (Zabbix Administrator) *admin@example.com*	**Resolved in 1m 59s: Linux: Load average is too high (per CPU load over 1.5 for 5m)** Problem has been resolved at 10:58:30 on 2025.08.15 Problem name: Linux: Load average is too high (per CPU load over 1.5 for 5m) Problem duration: 1m 59s Host: Linux server Severity: Average Original problem ID: 45	Sent	
2025-08-15 07:56:30 AM	Report problems to Zabbix administrators	Email	Admin (Zabbix Administrator) *admin@example.com*	**Problem: Linux: Load average is too high (per CPU load over 1.5 for 5m)** Problem started at 10:56:30 on 2025.08.15 Problem name: Linux: Load average is too high (per CPU load over 1.5 for 5m) Host: Linux server Severity: Average Operational data: Load averages(1m 5m 15m): (6.256836 4.808105 3.398438), # of CPUs: 2 Original problem ID: 45	Sent	
2025-08-15 07:42:30 AM	Report problems to Zabbix administrators		Admin (Zabbix Administrator)		Failed	i

Raport SLA

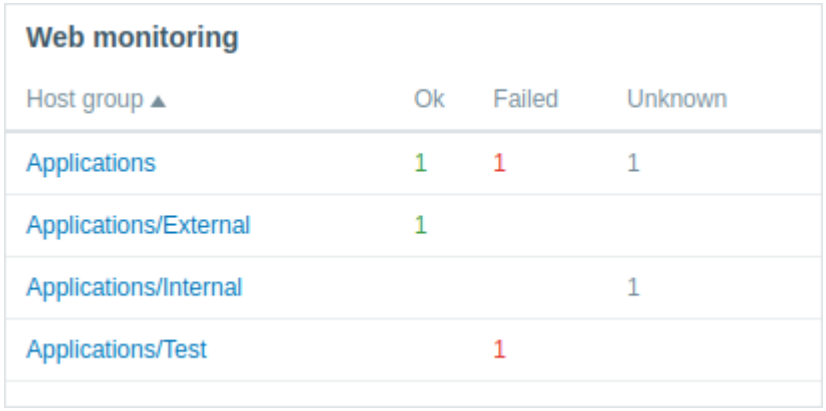
Widget Raport SLA wyświetla raporty SLA, pomagając monitorować wydajność usług względem zdefiniowanych celów.

SLA report

Day	SLO	SLI	Uptime	Downtime	Error budget	Excluded downtimes
2025-09-04	99.9%	99.8437	5h 40m 50s	28s	-8s	
2025-09-03	99.9%	99.9479	23h 59m 15s	45s	41s	
2025-09-02	99.9%	99.9190	23h 58m 50s	1m 10s	16s	
2025-09-01	99.9%	99.9251	22h 58m 58s	1h 1m 2s	21s	2025-09-01 01:00 AM Maintenance: 1h
2025-08-31	99.9%	99.6863	23h 55m 29s	4m 31s	-3m 5s	
2025-08-30	99.9%	99.9190	23h 58m 50s	1m 10s	16s	
2025-08-29	99.9%	99.7095	23h 55m 49s	4m 11s	-2m 45s	
2025-08-28	99.9%	99.9421	23h 59m 10s	50s	36s	
2025-08-27	99.9%	99.7188	23h 55m 57s	3m 15s	-2m 37s	
2025-08-26	99.9%	99.7755	23h 56m 46s	3m 14s	-1m 48s	
2025-08-25	99.9%	99.9094	22h 58m 45s	1h 1m 15s	8s	2025-08-25 01:00 AM Maintenance: 1h

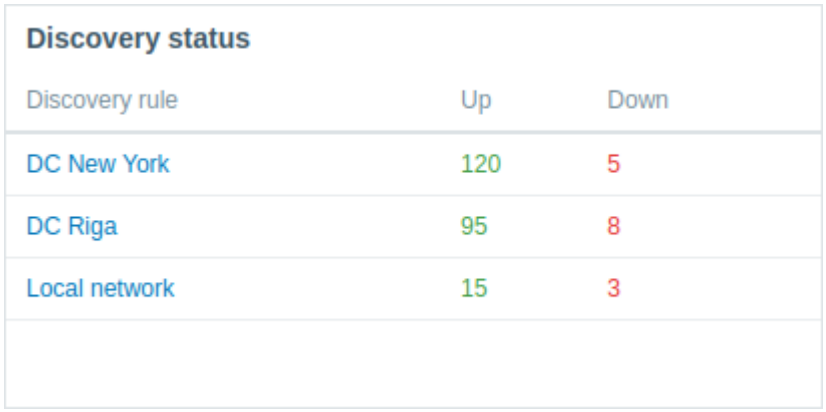
Monitorowanie WWW

Widżet Monitorowanie WWW wyświetla status aktywnych scenariuszy WWW.



Status wykrywania

Widget Discovery status wyświetla status urządzeń wykrytych przez włączone reguły wykrywania sieci. Pomaga monitorować, czy wykrywanie sieci działa prawidłowo, oraz liczbę urządzeń, które są dostępne lub niedostępne.



Narzędzia pulpitu i informacje o systemie

Te widżety dostarczają dodatkowych informacji i narzędzi, które wzbogacają pulpity.

Informacje o systemie

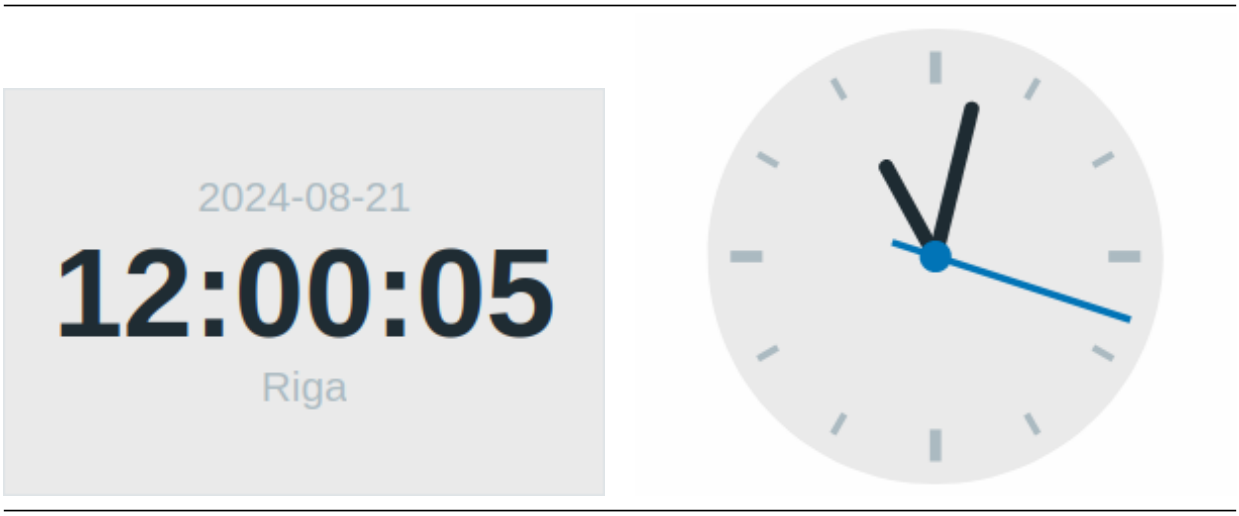
Widget Informacje o systemie wyświetla podsumowanie kluczowych danych serwera Zabbix i systemu lub szczegóły węzłów wysokiej dostępności.

System information

Parameter	Value	Details
Zabbix server is running	Yes	localhost:10051
Zabbix server version	8.0.0	Up to date
Zabbix frontend version	8.0.0	Up to date
Software update last checked	2025-08-30	
Latest release	8.0.0	Release notes
Number of hosts (enabled/disabled)	2	2 / 0
Number of templates	312	
Number of items (enabled/disabled/not supported)	176	165 / 0 / 11
Number of triggers (enabled/disabled [problem/ok])	89	89 / 0 [4 / 85]
Number of users (online)	2	1
Required server performance, new values per second	2.68	
Global scripts on Zabbix server	Disabled	
High availability cluster	Disabled	

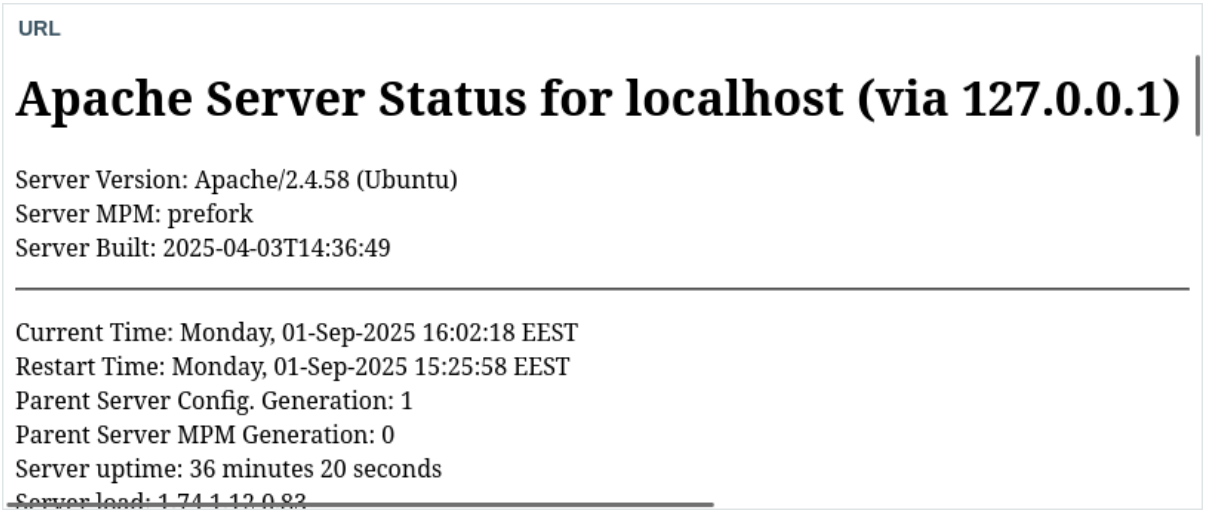
Zegar

Widget Clock wyświetla czas lokalny, czas serwera lub hosta w formacie analogowym lub cyfrowym.



URL

Widżet URL wyświetla zawartość pobraną z adresu URL.



2 Parametry widżetu pulpitu nawigacyjnego

Przegląd

Ta strona opisuje parametry wspólne dla wszystkich widgetów pulpitu, a także parametry dynamiczne, które umożliwiają wielu widgetom wymianę danych konfiguracyjnych między sobą lub z pulpitem.

Aby zobaczyć parametry specyficzne dla każdego widgetu, skorzystaj z panelu bocznego, aby przejść do odpowiedniej strony widgetu.

Wspólne parametry

Następujące parametry są wspólne dla każdego widgetu:

Nazwa	Wprowadź nazwę widgetu.
Interwał odświeżania	Skonfiguruj domyślny interwał odświeżania. Domyślne interwały odświeżania dla widgetów mieszczą się w zakresie od *Brak odświeżania* do *15 minut* w zależności od typu widgetu. Na przykład: - *Brak odświeżania* dla widgetu *URL*; - *1 minuta* dla widgetu *Dziennik działań*; - *15 minut* dla widgetu *Zegar*. Interwały odświeżania można ustawić na wartość domyślną dla wszystkich użytkowników. Przełącz pulpit na tryb edycji, kliknij przycisk edytuj widget i wybierz żądany interwał odświeżania z listy rozwijanej. Każdy użytkownik może również ustawić własny interwał odświeżania widgetu. W trybie widoku pulpitu kliknij przycisk z trzema kropkami na widżecie i wybierz żądany interwał odświeżania z listy rozwijanej. Pamiętaj, że indywidualny interwał odświeżania użytkownika ma pierwszeństwo przed ustawieniem widgetu i jest zachowywany nawet po zmianie ustawienia widgetu.
Pokaż nagłówek	Zaznacz pole wyboru, aby stale wyświetlać nagłówek widgetu. Gdy pole nie jest zaznaczone, nagłówek jest ukryty, aby zaoszczędzić miejsce, i staje się widoczny tylko po najechaniu kursorem na widget (zarówno w trybie widoku, jak i edycji). Nagłówek jest również częściowo widoczny podczas przeciągania widgetu w nowe miejsce.

Parametry dynamiczne

Wiele parametrów widżetów (np. *Hosty*, *Nadpisz hosta*, *Okres czasu*) obsługuje dynamiczne źródła danych. Zamiast konfigurować wartości statyczne, możesz powiązać te parametry z innymi widżetami lub samym pulpitem. Widżety są wtedy automatycznie aktualizowane na podstawie wyborów lub rozgłoszeń z innych części pulpitu.

Zgodność widgetów

Niektóre widgety mogą rozgłaszać dane konfiguracyjne do innych widgetów, niektóre mogą nasłuchiwać danych, a niektóre mogą robić jedno i drugie. Na przykład:

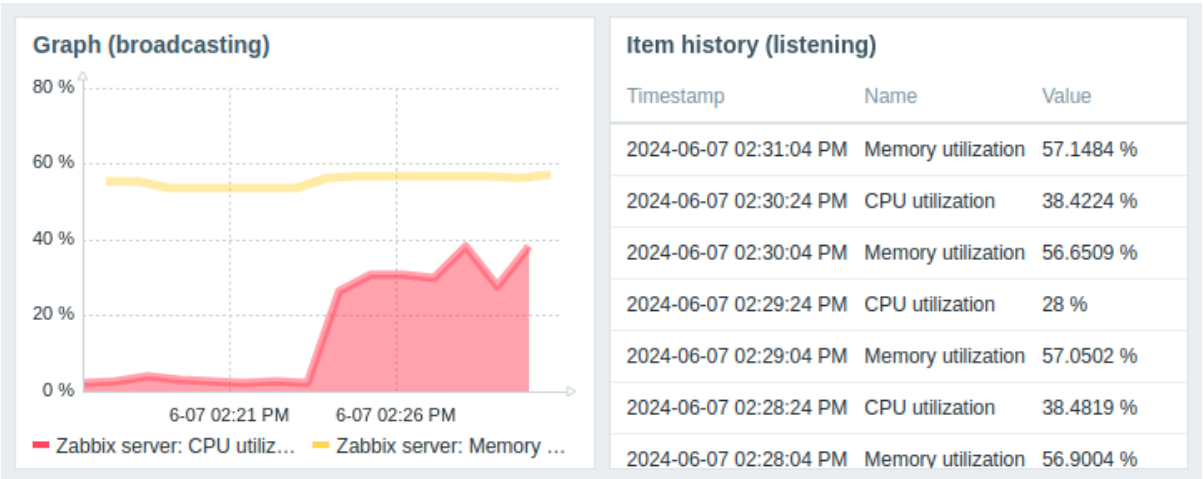
- Widget *Action log* może pobierać dane okresu tylko z widgetów *Graph*, *Graph (classic)* i *Graph prototype*.
- Widget *Geomap* może rozgłaszać dane hostów do widgetów, które ich nasłuchują (*Honeycomb*, *Top items* itd.), a także nasłuchiwać danych grup hostów i hostów z widgetów, które je rozgłaszają (*Honeycomb*, *Problem hosts* itd.).
- Widget *Clock* nie może rozgłaszać ani nasłuchiwać żadnych danych.

Poniższa tabela przedstawia możliwości rozgłaszania i nasłuchiwania dla każdego widgetu.

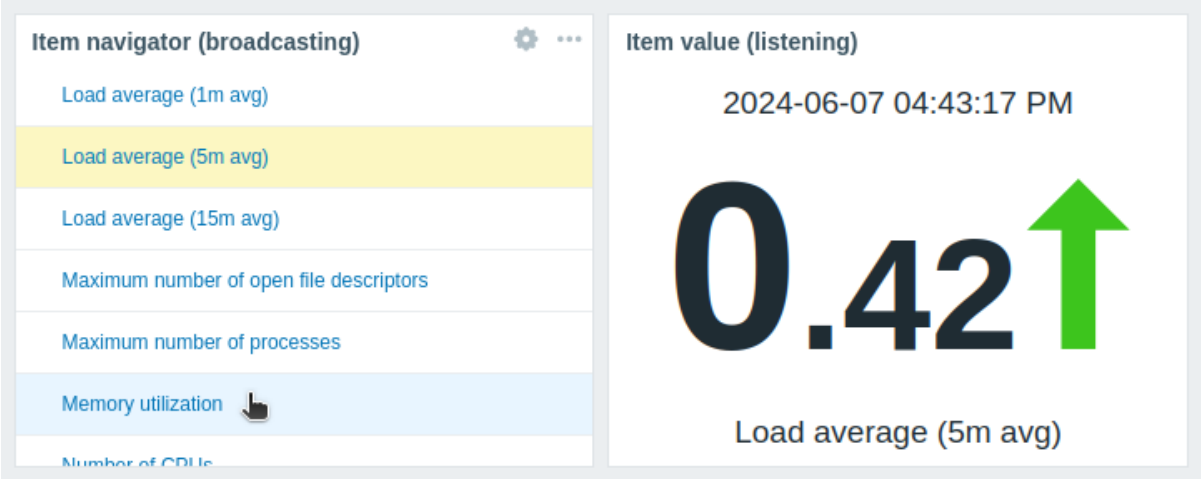
Widget	Rozgłasza	Nasłuchuje
Action log	-	Okres
Clock	-	-
Discovery status	-	-
Favorite graphs	-	-
Favorite maps	-	-
Gauge	-	Hosty, Pozycje
Geomap	Hosty	Grupy hostów, Hosty
Graph	Okres, Pozycje	Hosty, Pozycje, Okres
Graph (classic)	Okres	Hosty, Pozycje, Wykresy, Okres
Graph prototype	Okres	Hosty, Okres
Honeycomb	Hosty, Pozycje	Grupy hostów, Hosty
Host availability	-	Grupy hostów
Host card	-	Hosty
Host navigator	Hosty	Grupy hostów
Item card	-	Hosty, Pozycje, Okres
Item history	Pozycje	Hosty, Okres
Item navigator	Pozycje	Grupy hostów, Hosty
Item value	-	Hosty, Pozycje, Okres
Map	Grupy hostów, Hosty	Mapy
Map navigation tree	Mapy	-
Pie chart	-	Pozycje, Okres
Problem hosts	Grupy hostów	Grupy hostów, Hosty
Problems	Zdarzenia	Grupy hostów, Hosty
Problems by severity	Grupy hostów	Grupy hostów, Hosty
Scatter plot	Okres, Pozycje	Hosty, Pozycje, Okres
SLA report	-	-
System information	-	-
Top hosts	Hosty	Grupy hostów, Hosty
Top items	-	Grupy hostów, Hosty
Top triggers	-	Okres
Trigger overview	-	Grupy hostów, Hosty
URL	-	Hosty
Web monitoring	Grupy hostów	Grupy hostów, Hosty

Widżety różnią się sposobem, w jaki **rozgłaszają** dane do innych widżetów.

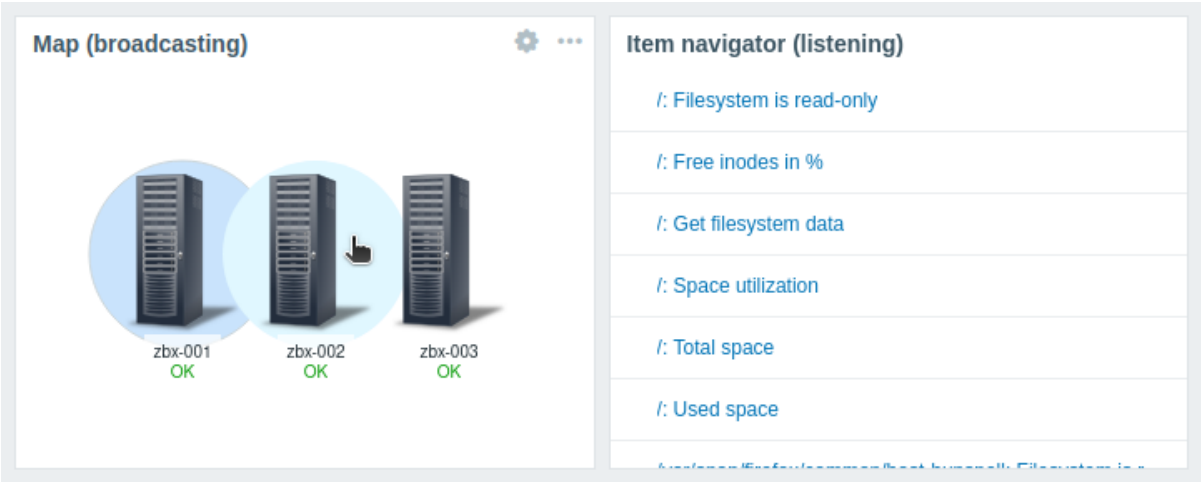
Widżety obsługujące rozgłaszanie zaczynają robić to automatycznie po utworzeniu. Na przykład widżet *Wykres* natychmiast rozgłasza dane okresu czasu do nasłuchujących widżetów.



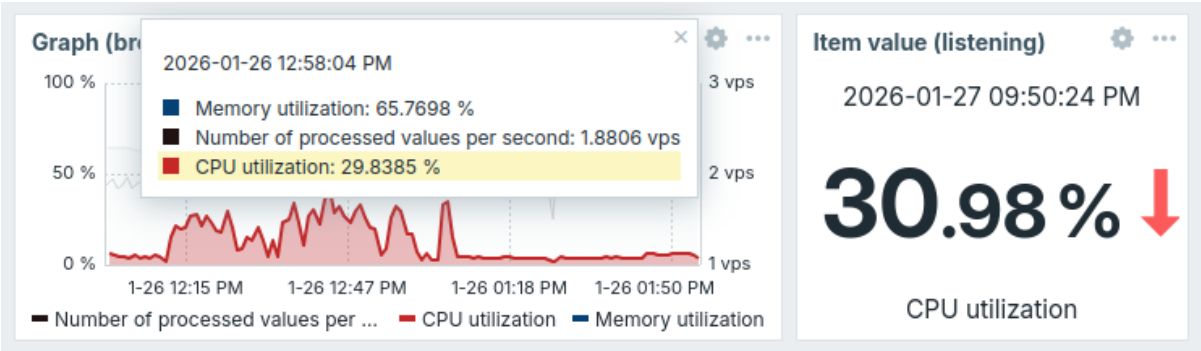
Widżety obsługujące wybór encji automatycznie rozgłaszają dane dla pierwszej dostępnej encji. Na przykład widżet *Nawigator pozycji* rozgłasza dane dla pierwszej pozycji na swojej liście pozycji. Po wybraniu innej pozycji rozgłasza dane dla tej pozycji. Po najechaniu kursorem pozycja jest podświetlana na jasnoniebiesko; po wybraniu jest podświetlana na żółto.



Widżet *Mapa* zachowuje się podobnie, rozgłaszając dane dla pierwszego elementu znajdującego się najbliżej lewego górnego rogu widocznego obszaru widżetu (w przypadku widżetu *Geomapa* — najbliżej środka). Po wybraniu innego elementu rozgłasza dane dla tego elementu. Po najechaniu kursorem element jest podświetlany na jasnoniebiesko; po wybraniu jest podświetlany na ciemnoniebiesko.

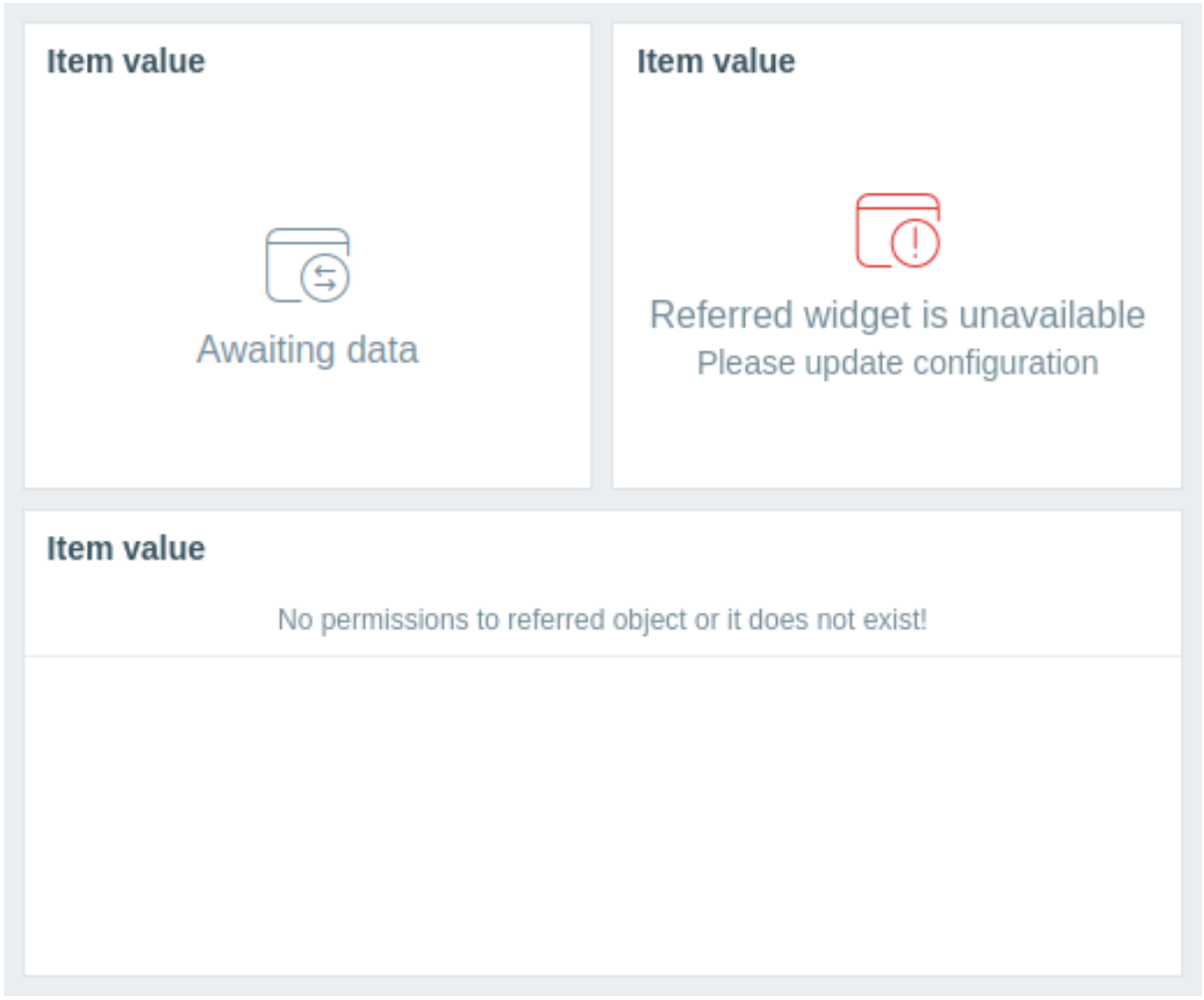


Widżety takie jak *Wykres* i *Wykres rozrzutu* mogą rozgłaszać dane pozycji po wybraniu pozycji w ich podpowiedziach:



Widżety mają również określone zachowania podczas **nasłuchiwania** danych z innych widżetów:

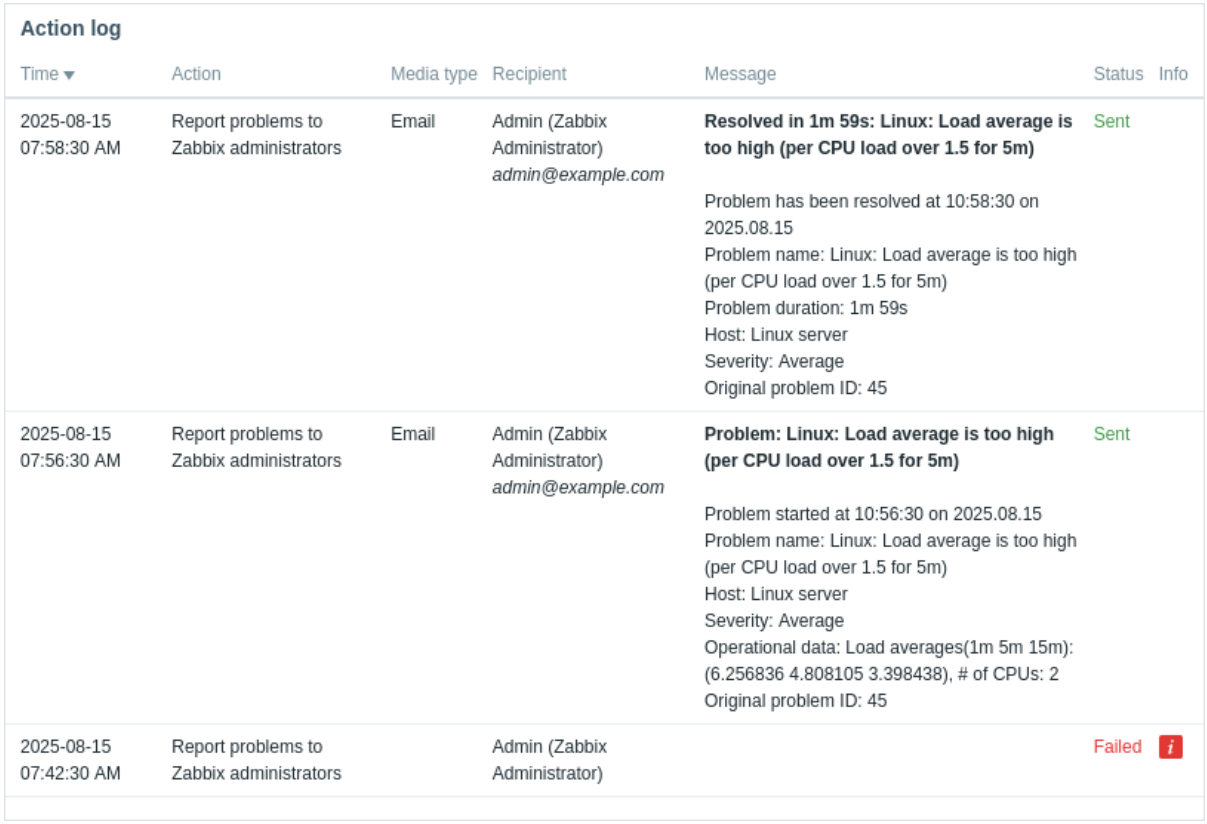
- Jeśli widżet będący źródłem danych nie rozgłasza danych, nasłuchujący widżet przechodzi w stan *Oczekiwanie na dane*.
- Jeśli widżet będący źródłem danych został usunięty, zastąpiony niekompatybilnym widżetem lub przeniesiony na inną stronę pulpitu, nasłuchujący widżet przechodzi w stan *Wskazany widżet jest niedostępny*.
- Jeśli określony host w źródle danych (widżecie lub pulpicie) nie ma encji skonfigurowanej w nasłuchującym widżecie (pozycji, wykresu, mapy itp.) lub jeśli użytkownik nie ma uprawnień dostępu do hosta, nasłuchujący widżet wyświetla następujący komunikat: *„Brak uprawnień do wskazanego obiektu lub obiekt nie istnieje!”*



1 Dziennik akcji

Przegląd

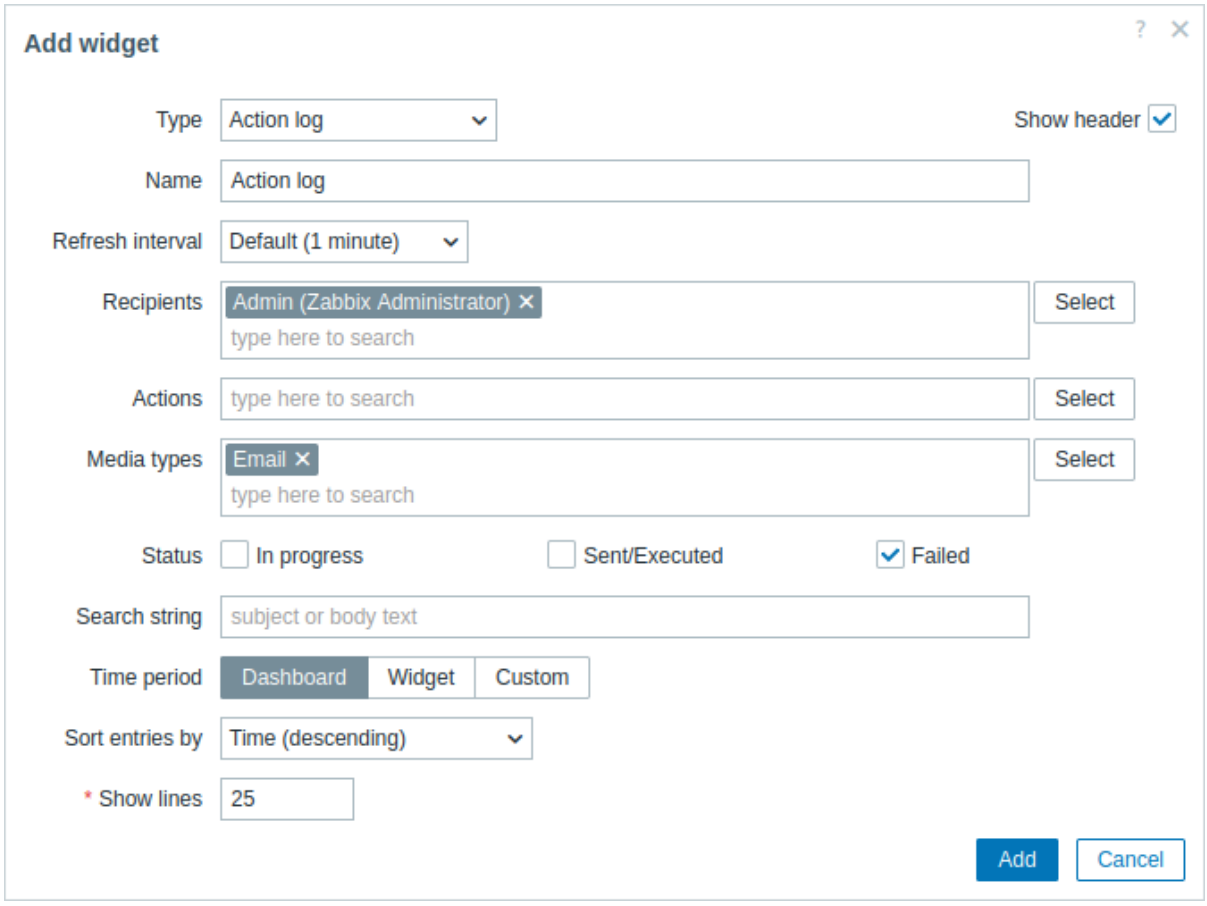
Widżet *Dziennik akcji* wyświetla szczegóły operacji (powiadomień, zdalnych poleceń) wykonanych w ramach akcji. Szczegółowy dziennik pomaga w audycie, rozwiązywaniu problemów i monitorowaniu wykonania każdej akcji.



Wyświetla te same dane co *Raporty* > *Dziennik akcji* i może wyświetlać do 1000 rekordów.

Konfiguracja

Aby skonfigurować widżet, wybierz *Action log* jako typ:



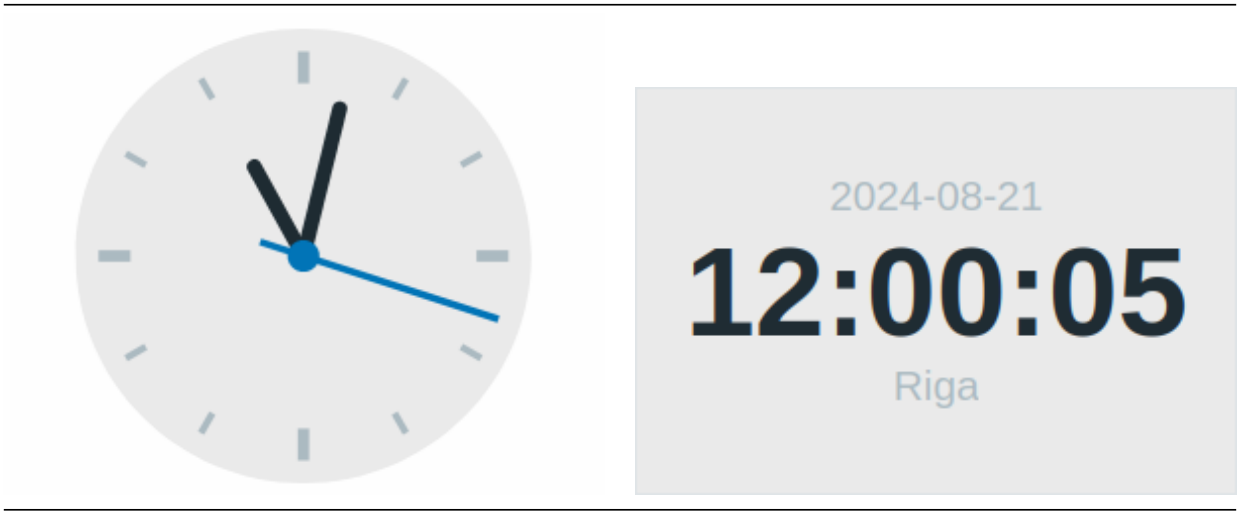
Oprócz parametrów wspólnych dla wszystkich widżetów, możesz ustawić następujące opcje specyficzne:

Recipients	Filtruj wpisy według odbiorców. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy odbiorcy zostanie wyświetlona rozwijana lista pasujących odbiorców. Jeśli nie wybrano żadnych odbiorców, zostaną wyświetlone szczegóły operacji akcji dla wszystkich odbiorców.
Actions	Filtruj wpisy według akcji. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy akcji zostanie wyświetlona rozwijana lista pasujących akcji. Jeśli nie wybrano żadnych akcji, zostaną wyświetlone szczegóły operacji akcji dla wszystkich akcji.
Media types	Filtruj wpisy według typów mediów. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy typu mediów zostanie wyświetlona rozwijana lista pasujących typów mediów. Jeśli nie wybrano żadnych typów mediów, zostaną wyświetlone szczegóły operacji akcji dla wszystkich typów mediów.
Status	Zaznacz pole wyboru, aby filtrować wpisy według odpowiedniego statusu: **In progress** - wyświetlane są operacje akcji będące w toku; **Sent/Executed** - wyświetlane są operacje akcji, które wysłały powiadomienie lub zostały wykonane; **Failed** - wyświetlane są operacje akcji, które zakończyły się niepowodzeniem.
Search string	Filtruj wpisy według treści wiadomości/zdalnego polecenia. Jeśli wpiszesz tutaj ciąg znaków, wyświetlane będą tylko te operacje akcji, których wiadomość/zdalne polecenie zawiera podany ciąg. Makra nie są rozwijane.
Time period	Filtruj wpisy według okresu czasu. Wybierz źródło danych dla okresu czasu: **Dashboard** - użyj selektora okresu czasu pulpitu; **Widget** - użyj zgodnego widżetu (ustawionego w parametrze *Widget*); **Custom** - użyj niestandardowego okresu czasu ustawionego w parametrach *From* i *To*; jeśli zostanie ustawiony, w prawym górnym rogu widżetu zostanie wyświetlona ikona zegara, wskazująca ustawiony czas po najechaniu kursorem. Zwróć uwagę, że niezależnie od konfiguracji *Time period* widżetu, zgodne widżety nadal mogą używać go jako źródła danych dla okresu czasu.
Widget	Wprowadź lub wybierz zgodny widżet jako źródło danych dla okresu czasu. Ten parametr jest dostępny, jeśli *Time period* jest ustawiony na "Widget".
From	Wprowadź lub wybierz początek okresu czasu. Obsługiwana jest składnia czasu względnego (`now`, `now/d`, `now/w-1w` itd.). Ten parametr jest dostępny, jeśli *Time period* jest ustawiony na "Custom".
To	Wprowadź lub wybierz koniec okresu czasu. Obsługiwana jest składnia czasu względnego (`now`, `now/d`, `now/w-1w` itd.). Ten parametr jest dostępny, jeśli *Time period* jest ustawiony na "Custom".
Sort entries by	Sortuj wpisy według: **Time** (malejąco lub rosnąco); **Type** (malejąco lub rosnąco); **Status** (malejąco lub rosnąco); **Recipient** (malejąco lub rosnąco).
Show lines	Ustaw, ile wierszy dziennika akcji będzie wyświetlanych w widżecie.

2 Zegar

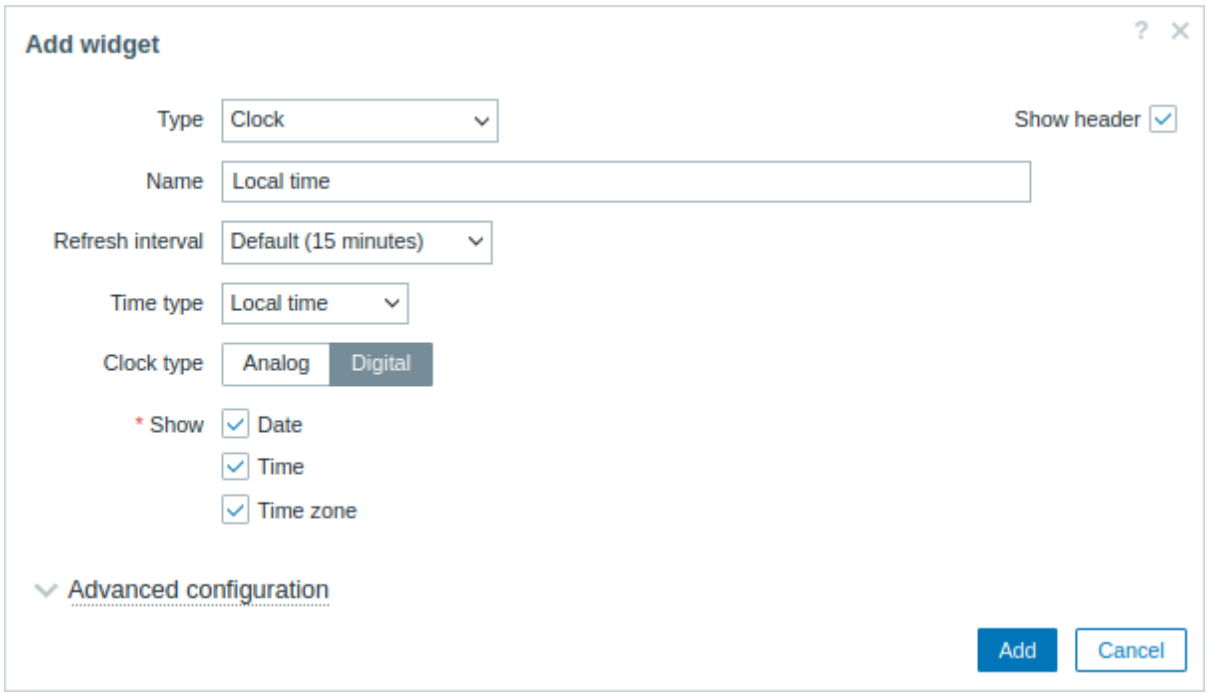
Przegląd

Widżet *Zegar* wyświetla czas lokalny, czas serwera lub hosta w formacie analogowym albo cyfrowym.



Konfiguracja

Aby skonfigurować widżet, wybierz *Clock* jako typ:



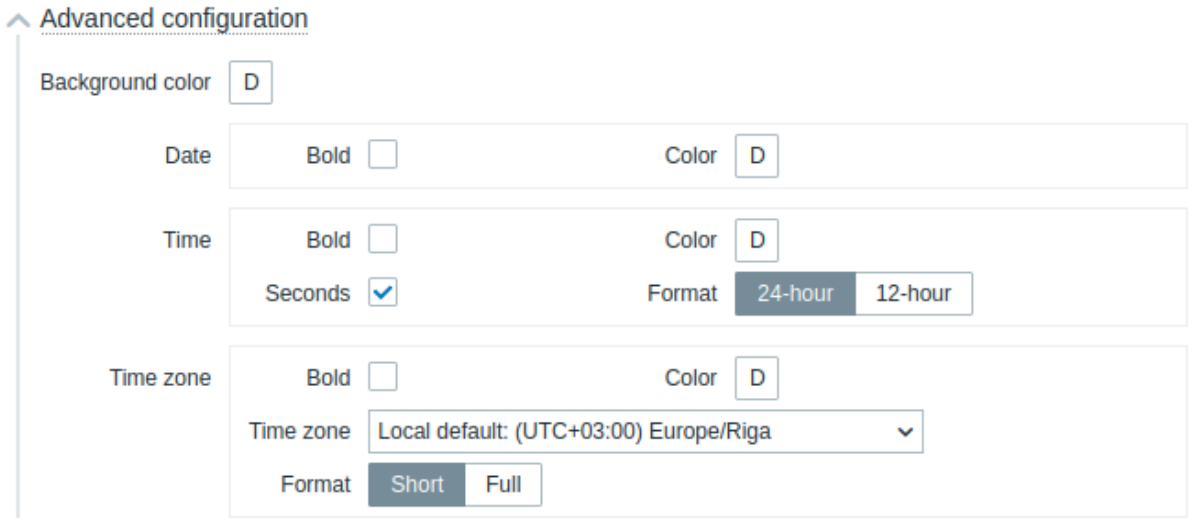
Oprócz parametrów wspólnych dla wszystkich widżetów możesz ustawić następujące opcje specyficzne:

Time type	Wybierz źródło czasu: **Local** - czas systemowy urządzenia, na którym uruchomiona jest przeglądarka; **Server** - strefa czasowa ustawiona globalnie lub dla użytkownika Zabbix; **Host** - czas pobrany z pozycji hosta.
Item	Wybierz pozycję dla czasu hosta (użyj pozycji system.localtime[local]). Ten parametr jest dostępny, jeśli *Time type* jest ustawiony na „Host time”.
Clock type	Wybierz typ zegara (analogowy lub cyfrowy).
Show	Wybierz jedną lub więcej jednostek informacji (data, godzina, strefa czasowa), które mają być wyświetlane w zegarze cyfrowym. Rozmiar jednostek automatycznie dostosowuje się do wyświetlanych jednostek, rozmiaru widżetu i skali wyświetlania. Ten parametr jest dostępny, jeśli *Clock type* jest ustawiony na „Digital”.
Advanced configuration	Kliknij etykietę *Advanced configuration*, aby wyświetlić opcje konfiguracji zaawansowanej dla zegara cyfrowego. Ta sekcja jest dostępna, jeśli *Clock type* jest ustawiony na „Digital”.

Konfiguracja zaawansowana

Zaawansowane opcje konfiguracji są dostępne w zwijanej sekcji *Konfiguracja zaawansowana* i tylko dla tych elementów, które są wybrane w polu *Pokaż* (zobacz wyżej).

Dodatkowo konfiguracja zaawansowana umożliwia zmianę koloru tła dla całego widżetu.

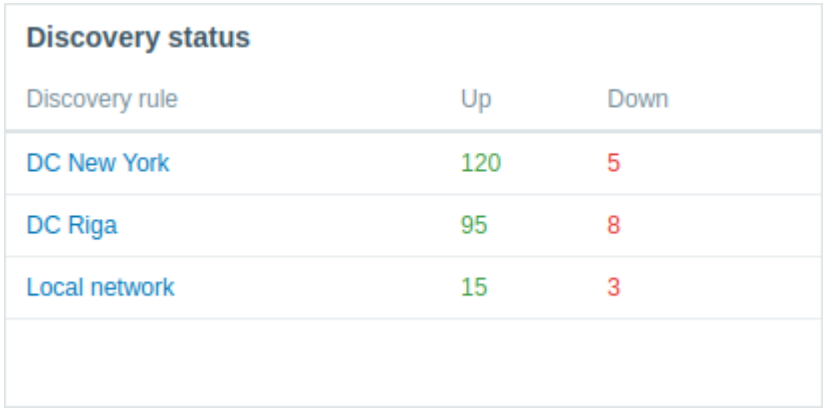


Kolor tła	Wybierz kolor tła z próbnika kolorów. D oznacza kolor domyślny (zależy od motywu frontend). Aby przywrócić wartość domyślną, kliknij przycisk *Użyj domyślnego* w próbniku kolorów.
Data	
Pogrubienie	Zaznacz pole wyboru, aby wyświetlać datę pogrubioną czcionką.
Kolor	Wybierz kolor daty z próbnika kolorów. D oznacza kolor domyślny (zależy od motywu frontend). Aby przywrócić wartość domyślną, kliknij przycisk *Użyj domyślnego* w próbniku kolorów.
Czas	
Pogrubienie	Zaznacz pole wyboru, aby wyświetlać czas pogrubioną czcionką.
Kolor	Wybierz kolor czasu z próbnika kolorów. D oznacza kolor domyślny (zależy od motywu frontend). Aby przywrócić wartość domyślną, kliknij przycisk *Użyj domyślnego* w próbniku kolorów.
Sekundy	Zaznacz pole wyboru, aby wyświetlać sekundy. W przeciwnym razie będą wyświetlane tylko godziny i minuty.
Format	Wybierz wyświetlanie czasu w formacie 24-godzinnym lub 12-godzinnym.
Strefa czasowa	
Pogrubienie	Zaznacz pole wyboru, aby wyświetlać strefę czasową pogrubioną czcionką.
Kolor	Wybierz kolor strefy czasowej z próbnika kolorów. D oznacza kolor domyślny (zależy od motywu frontend). Aby przywrócić wartość domyślną, kliknij przycisk *Użyj domyślnego* w próbniku kolorów.
Strefa czasowa	Wybierz strefę czasową.
Format	Wybierz wyświetlanie strefy czasowej w formacie skróconym (np. `New York`) lub pełnym (np. `(UTC-04:00) America/New York`).

3 Status wykrywania

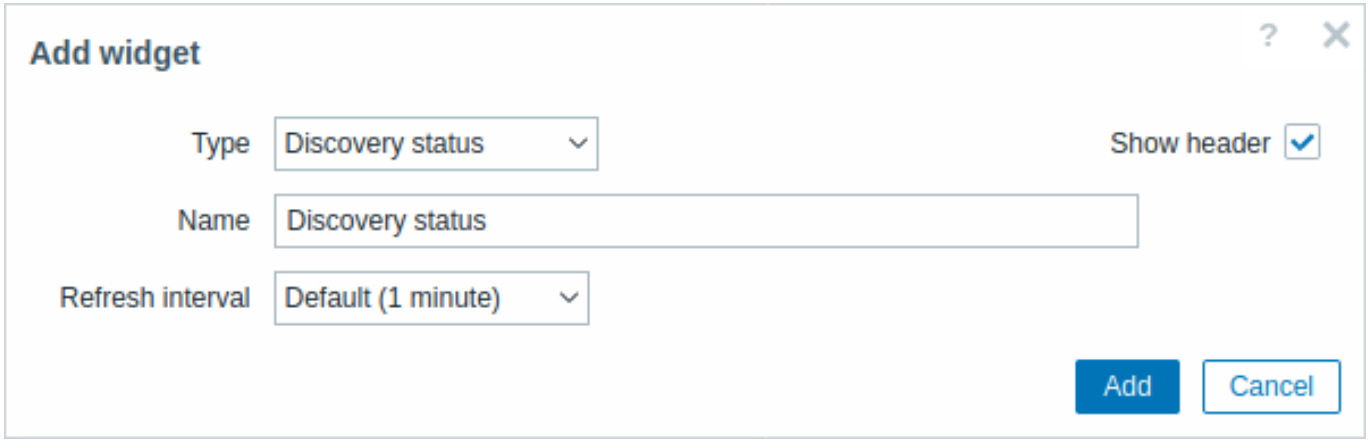
Przegląd

Widżet *Status wykrywania* wyświetla status urządzeń wykrytych przez włączone reguły wykrywania sieci. Pomaga monitorować, czy wykrywanie sieci działa prawidłowo, oraz liczbę urządzeń, które są dostępne lub niedostępne.



Konfiguracja

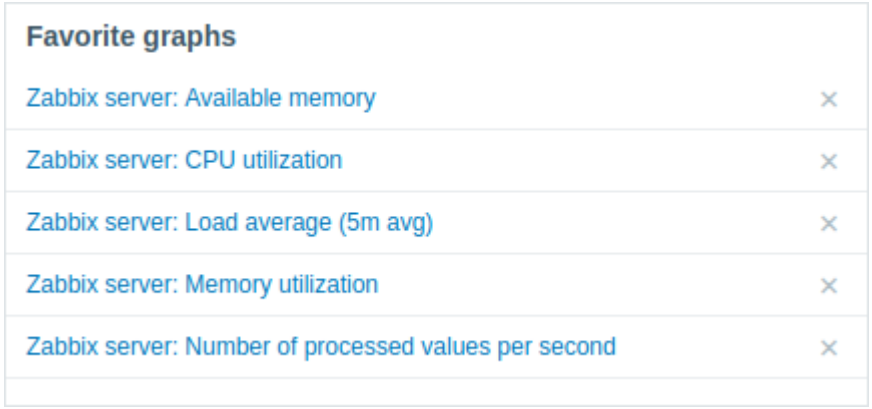
Wszystkie parametry konfiguracji dla tego widżetu są wspólne dla wszystkich widżetów.



4 Ulubione wykresy

Przegląd

Widżet *Ulubione wykresy* wyświetla alfabetyczną listę skrótów do wykresów oznaczonych jako ulubione przez bieżącego użytkownika.



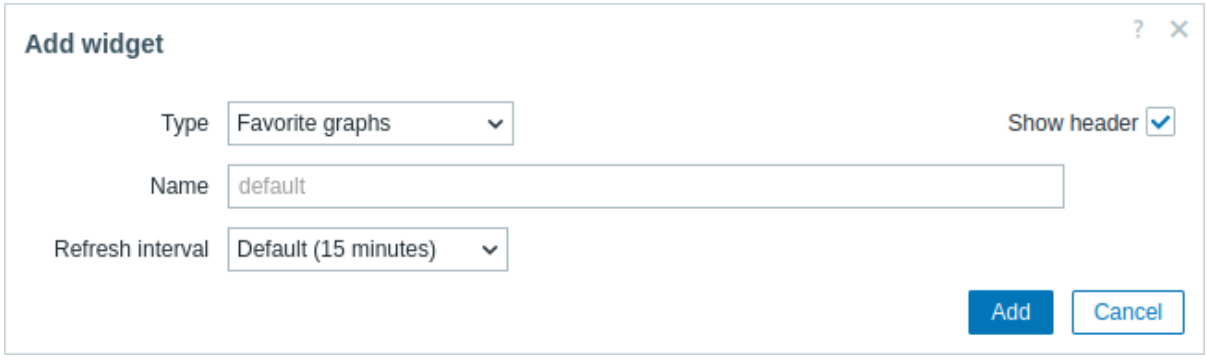
Kliknięcie x usuwa wykres z listy oraz z ulubionych.

Wykresy są oznaczane jako ulubione po kliknięciu przycisku  *Dodaj do ulubionych* podczas przeglądania wykresów pozycji w *Monitoring* > *Najnowsze dane*.



Konfiguracja

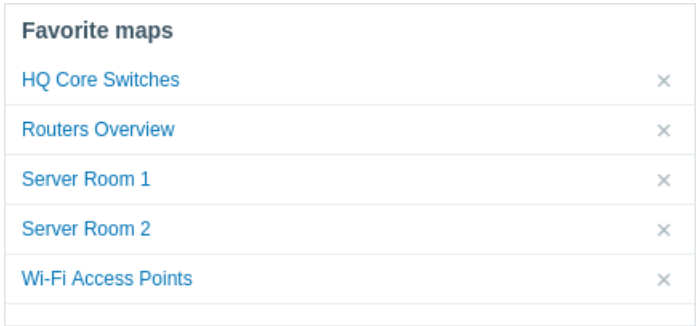
Wszystkie parametry konfiguracji tego widżetu są wspólne dla wszystkich widżetów.



5 Ulubione mapy

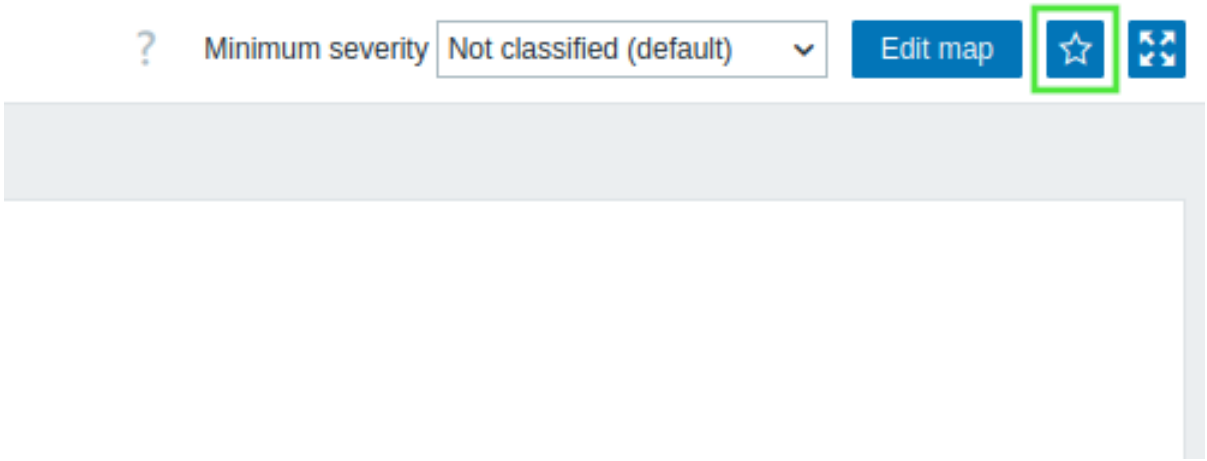
Przegląd

Widżet *Ulubione mapy* wyświetla listę skrótów do map oznaczonych przez bieżącego użytkownika jako ulubione, posortowaną alfabetycznie.



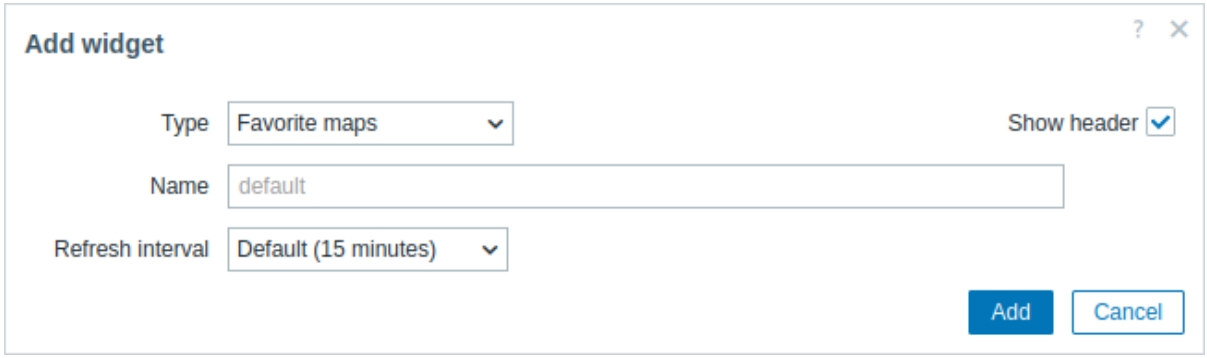
Kliknięcie x usuwa mapę z ulubionych.

Mapy są oznaczane jako ulubione po kliknięciu przycisku  *Dodaj do ulubionych* podczas przeglądania map w *Monitoring* > *Mapy*.



Konfiguracja

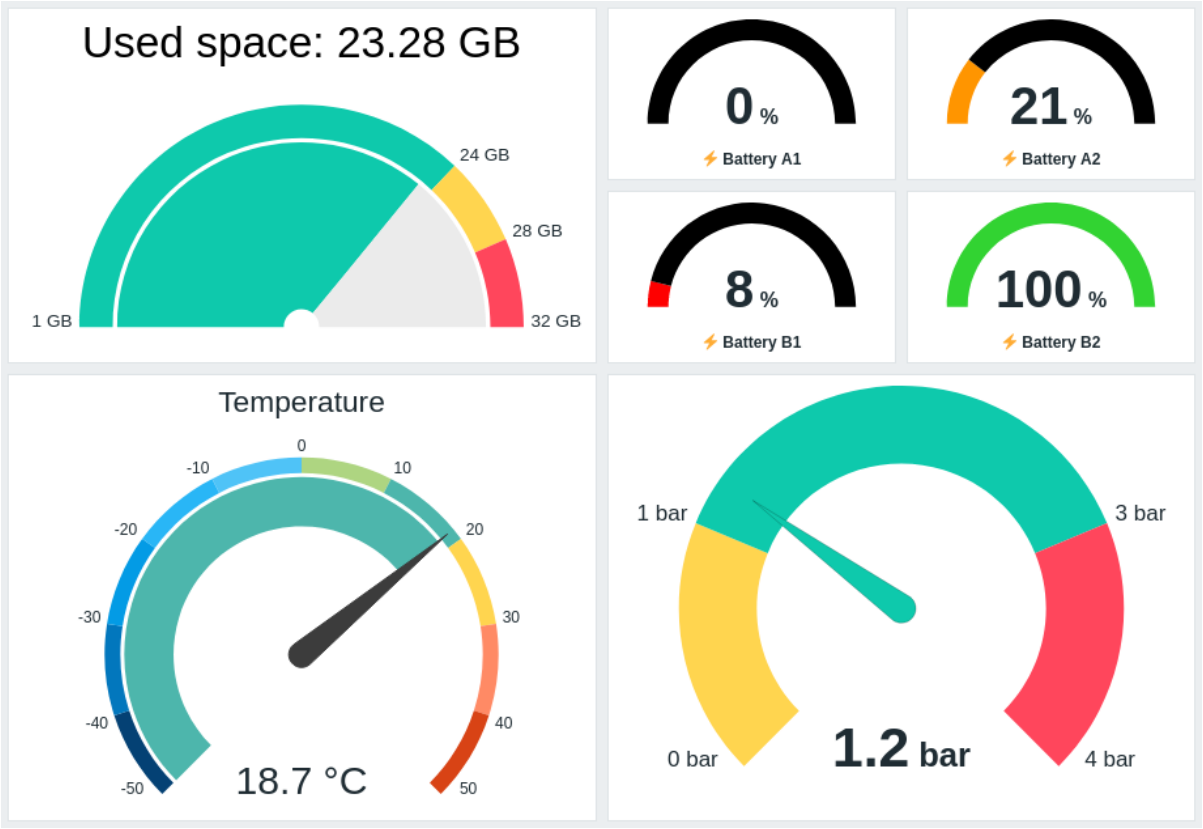
Wszystkie parametry konfiguracji tego widżetu są wspólne dla wszystkich widżetów.



6 Wskaźnik

Przegląd

Widżet *Gauge* wyświetla wartość pojedynczej numerycznej pozycji w formie wskaźnika. Jest przydatny do monitorowania ważnych metryk, wizualizacji progów oraz wykrywania nagłych zmian.



Możesz skonfigurować widżet tak, aby wyświetlał następujące elementy:

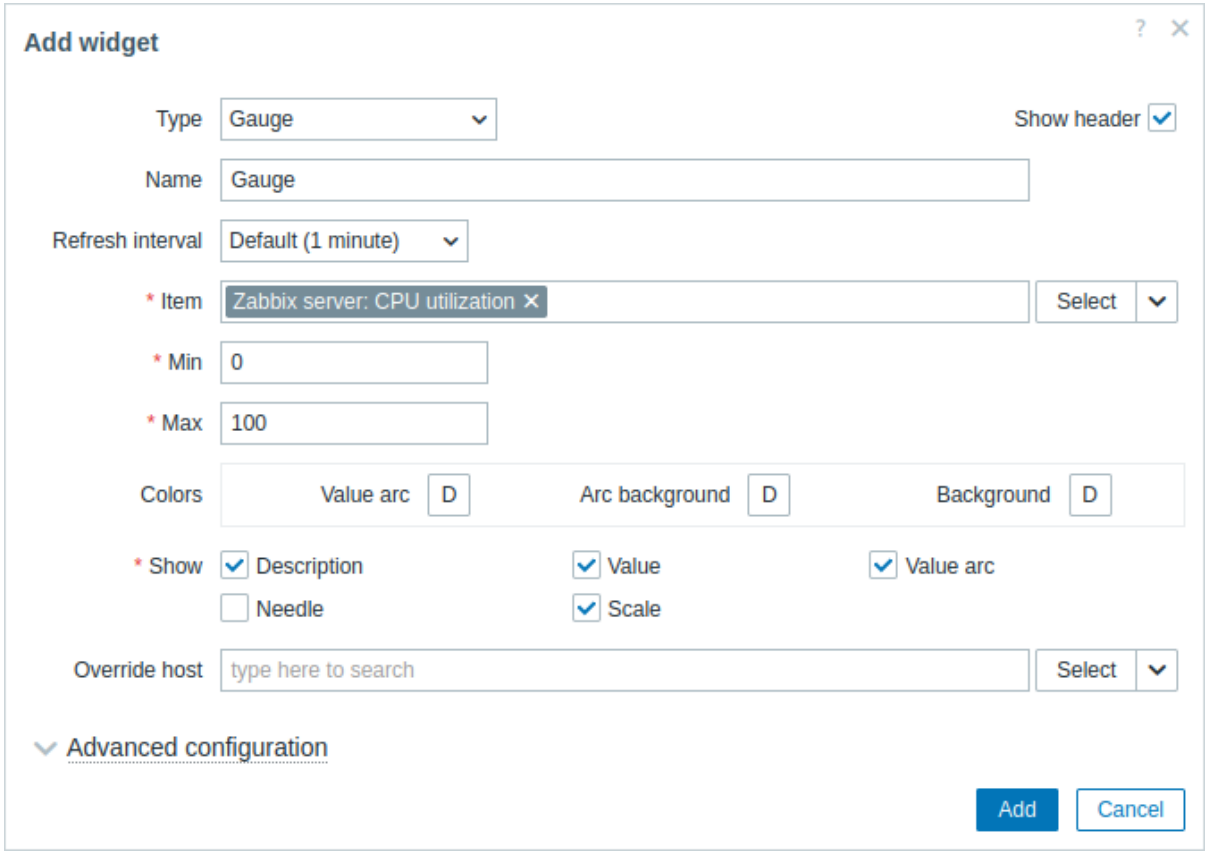
- Opis pozycji (Used space: {ITEM.LASTVALUE}, Temperature)
- Wartość pozycji i jednostki (21 %, 18.7 °C, 1.2 bar)
- Skalę wskaźnika (1GB/24GB/28GB/32GB, -50/-40/-30/etc.)
- Łuk wskaźnika (łuk wartości wskaźnika i łuk progów wskaźnika)
- Wskazówkę wskaźnika

Kliknięcie widżetu otwiera prosty wykres dla tej pozycji.

Informacje wyświetlane w widżecie *Gauge* można pobrać jako obraz PNG, wybierając opcję *Download image* w menu widżetu.

Konfiguracja

Aby skonfigurować widget, wybierz *Gauge* jako typ:

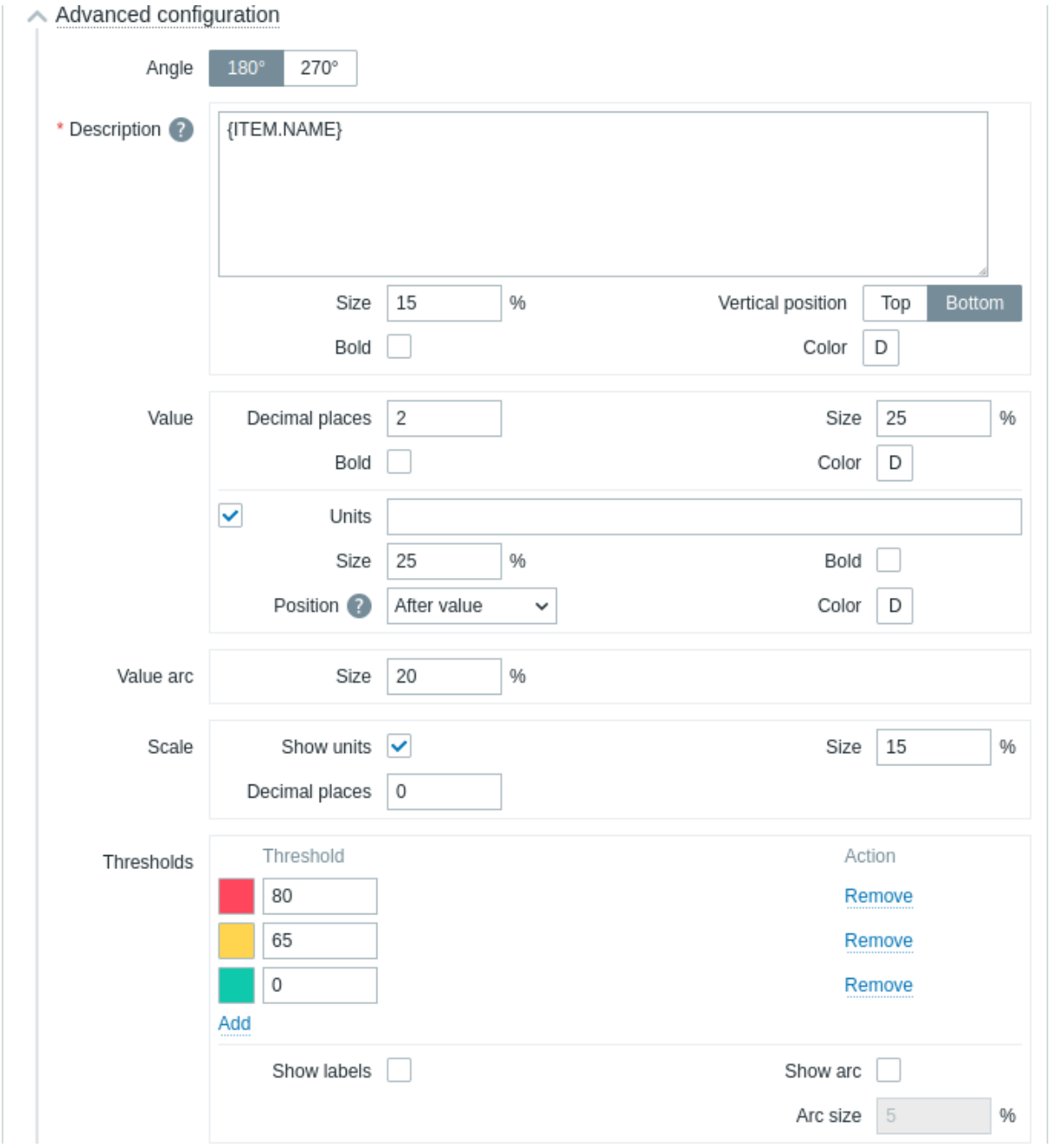


Oprócz parametrów wspólnych dla wszystkich widgetów możesz ustawić następujące opcje specyficzne:

Item	Wybierz pozycję. Alternatywnie wybierz zgodny widget jako źródło danych dla pozycji. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy pozycji zostanie wyświetlona rozwijana lista pasujących pozycji. Pamiętaj, że możesz wybierać tylko pozycje zwracające dane numeryczne (z wyjątkiem danych binarnych).
Min	Wprowadź minimalną wartość wskaźnika. Obsługiwane są sufiksy (na przykład „1d”, „2w”, „4K”, „8G”). Obsługiwane są mapowania wartości.
Max	Wprowadź maksymalną wartość wskaźnika. Obsługiwane są sufiksy (na przykład „1d”, „2w”, „4K”, „8G”). Obsługiwane są mapowania wartości.
Colors	Wybierz kolor z próbnika kolorów: **Value arc** - wybierz kolor łuku wartości wskaźnika; **Arc background** - wybierz kolor tła łuku wartości wskaźnika i łuku progów wskaźnika; **Background** - wybierz kolor tła widgetu. „D” oznacza kolor domyślny, który zależy od motywu frontend. Jeśli ustawiono *Thresholds*, domyślny kolor dla **Value arc** zależy od koloru progu. Aby powrócić do koloru domyślnego, kliknij przycisk *Use default* w próbniku kolorów.
Show	Zaznacz pole wyboru, aby wyświetlić odpowiedni element wskaźnika — opis, wartość, łuk wartości, wskazówkę, skalę (minimalną i maksymalną wartość wskaźnika na początku i końcu łuku wskaźnika). Usuń zaznaczenie, aby ukryć element. Musi być wybrany co najmniej jeden element. Pamiętaj, że wskazówka i skala wskaźnika mogą być wyświetlane, jeśli wyświetlany jest łuk wartości wskaźnika lub łuk progów wskaźnika (zobacz opcje konfiguracji zaawansowanej). Zwróć też uwagę, że jeśli wskazówka wskaźnika jest wyświetlana, wartość jest umieszczana pod wskazówką; jeśli wskazówka jest ukryta, wartość jest wyrównana do dolnej części łuku wskaźnika.
Override host	Wybierz zgodny widget lub selektor hosta pulpitu jako źródło danych dla hostów. Ten parametr nie jest dostępny podczas konfigurowania widgetu na pulpicie szablonu.
Advanced configuration	Kliknij etykietę *Advanced configuration*, aby wyświetlić opcje konfiguracji zaawansowanej. Tutaj możesz także dostosować elementy wskaźnika wybrane w polu *Show*.

Konfiguracja zaawansowana

Opcje konfiguracji zaawansowanej są dostępne w zwijanej sekcji *Konfiguracja zaawansowana*:



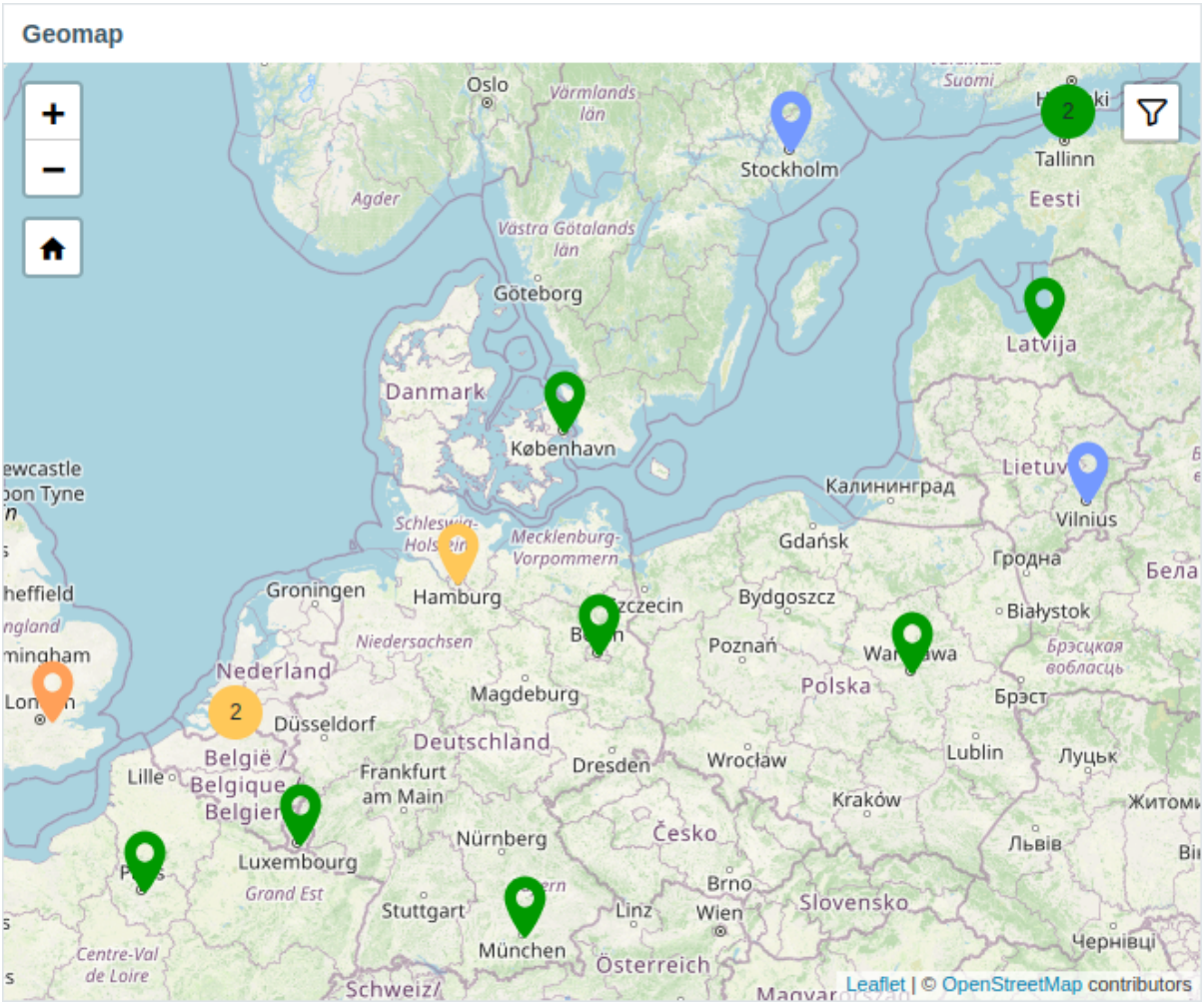
Kąt	Wybierz kąt wskaźnika (180° lub 270°).
Opis	
Opis	Wprowadź opis pozycji. Ten opis może zastąpić domyślną nazwę pozycji. Obsługiwane są opisy wielowierszowe. Możliwe jest połączenie tekstu i obsługiwanych makr. Obsługiwane są {HOST.*}, {ITEM.*}, {INVENTORY.*} oraz makra użytkownika.
Rozmiar	Wprowadź wysokość rozmiaru czcionki dla opisu pozycji (w procentach, względem całkowitej wysokości widżetu).
Pozycja pionowa	Wybierz pionowe położenie opisu pozycji (u góry lub u dołu, względem łuku wskaźnika).
Pogrubienie	Zaznacz pole wyboru, aby wyświetlać opis pozycji pogrubioną czcionką.
Kolor	Wybierz kolor opisu pozycji z próbnika kolorów. ”D” oznacza kolor domyślny, który zależy od motywu frontend. Aby przywrócić kolor domyślny, kliknij przycisk *Użyj domyślnego* w próbniku kolorów.
Wartość	
Miejsca dziesiętne	Wprowadź liczbę miejsc dziesiętnych wyświetlanych przy wartości. Ta opcja ma wpływ tylko na pozycje zwracające dane numeryczne (float).
Rozmiar	Wprowadź wysokość rozmiaru czcionki dla wartości (w procentach, względem wysokości łuku wskaźnika).
Pogrubienie	Zaznacz pole wyboru, aby wyświetlać wartość pogrubioną czcionką.

Kolor	Wybierz kolor wartości z próbnika kolorów. ”D” oznacza kolor domyślny, który zależy od motywu frontend. Aby przywrócić kolor domyślny, kliknij przycisk *Użyj domyślnego* w próbniku kolorów.
Jednostki	
Jednostki	Zaznacz pole wyboru, aby wyświetlać jednostki wraz z wartością pozycji. Jeśli wprowadzisz nazwę jednostki, zastąpi ona jednostki ustawione w konfiguracji pozycji.
Rozmiar	Wprowadź wysokość rozmiaru czcionki dla jednostek pozycji (w procentach, względem wysokości łuku wskaźnika).
Pogrubienie	Zaznacz pole wyboru, aby wyświetlać jednostki pozycji pogrubioną czcionką.
Pozycja	Wybierz położenie jednostek pozycji (nad, pod, przed lub za, względem wartości pozycji). Ta opcja jest ignorowana dla następujących jednostek związanych z czasem: unixtime, uptime, s.
Kolor	Wybierz kolor jednostek pozycji z próbnika kolorów. ”D” oznacza kolor domyślny, który zależy od motywu frontend. Aby przywrócić kolor domyślny, kliknij przycisk *Użyj domyślnego* w próbniku kolorów.
Łuk wartości	
Rozmiar łuku	Wprowadź wysokość rozmiaru łuku wartości wskaźnika (w procentach, względem promienia łuku wskaźnika).
Wskazówka	
Kolor	Wybierz kolor wskazówki wskaźnika z próbnika kolorów. ”D” oznacza kolor domyślny, który zależy od motywu frontend. Jeśli ustawiono *Progi*, domyślny kolor wskazówki zależy od koloru progu. Aby przywrócić kolor domyślny, kliknij przycisk *Użyj domyślnego* w próbniku kolorów.
Skala	
Pokaż jednostki	Zaznacz pole wyboru, aby wyświetlać jednostki przy minimalnej i maksymalnej wartości wskaźnika.
Rozmiar	Wprowadź wysokość rozmiaru czcionki dla minimalnej i maksymalnej wartości wskaźnika (w procentach, względem wysokości łuku wskaźnika).
Miejsca dziesiętne	Wprowadź liczbę miejsc dziesiętnych wyświetlanych przy minimalnej i maksymalnej wartości wskaźnika. Ta opcja ma wpływ tylko na pozycje zwracające dane numeryczne (float).
Progi	
Progi	Kliknij *Dodaj*, aby dodać próg, wybierz kolor progu z próbnika kolorów i określ wartość numeryczną. Lista progów zostanie posortowana rosnąco podczas zapisywania. Należy pamiętać, że kolory skonfigurowane jako progi będą wyświetlane poprawnie tylko dla pozycji numerycznych. Obsługiwane są sufiksy (na przykład „1d”, „2w”, „4K”, „8G”). Obsługiwane są mapowania wartości.
Pokaż etykiety	Zaznacz pole wyboru, aby wyświetlać wartości progów jako etykiety na skali wskaźnika.
Pokaż łuk	Zaznacz pole wyboru, aby wyświetlać łuk progów wskaźnika.
Rozmiar łuku	Wprowadź wysokość rozmiaru łuku progów wskaźnika (w procentach, względem promienia łuku wskaźnika).

7 Geomap

Przegląd

Widżet *Geomap* wyświetla hosty jako znaczniki na interaktywnej mapie opartej na Leaflet, a kolory znaczników wskazują najpoważniejszy problem każdego hosta.

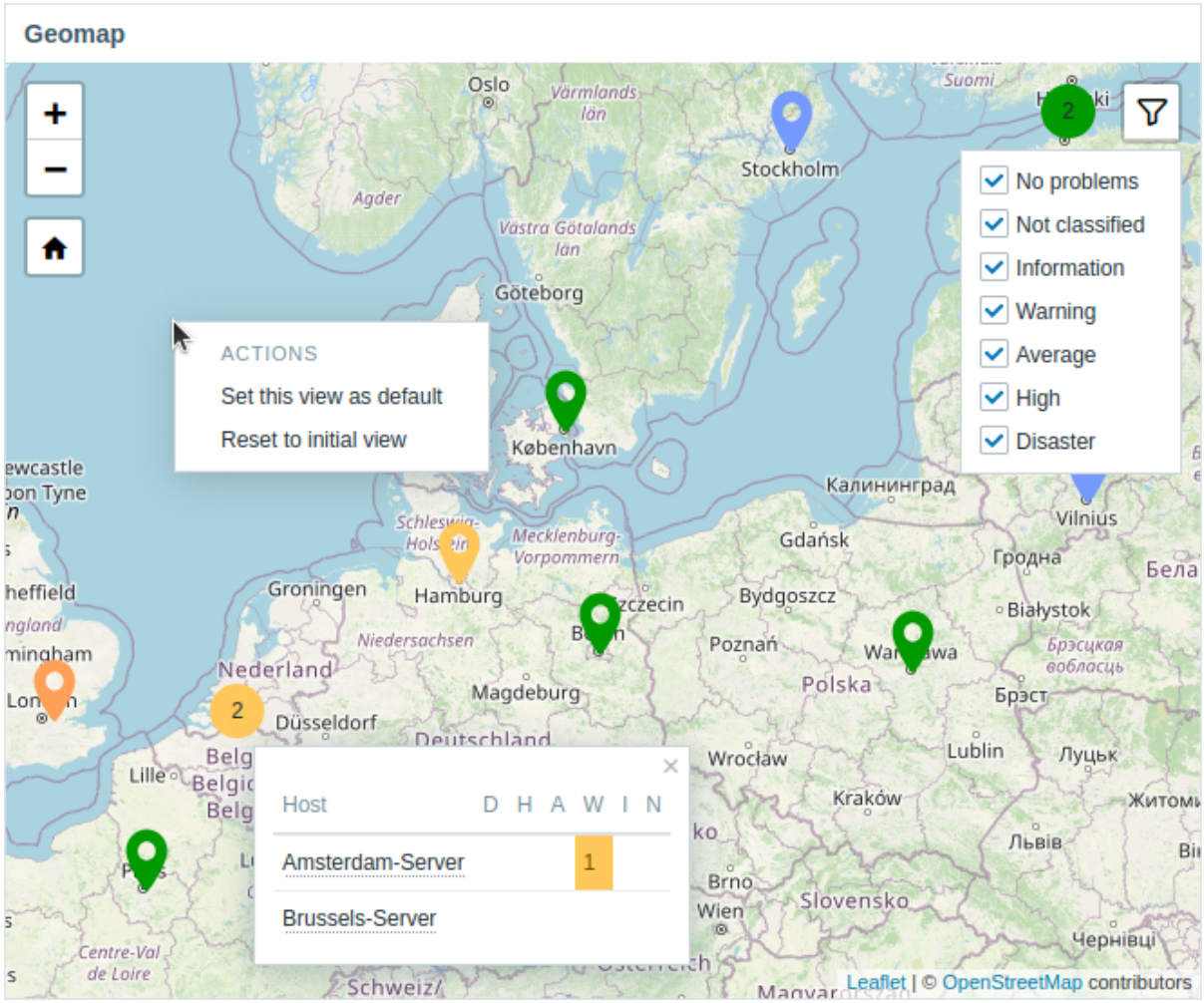


Note:
Zabbix oferuje wiele predefiniowanych dostawców kafelków mapy i umożliwia dodawanie własnych w *Administracja* > *Ogólne* > *Mapy geograficzne*.

Domyślnie widżet wyświetla wszystkie włączone hosty, które mają prawidłowe współrzędne (szerokość geograficzna od -90 do 90, długość geograficzna od -180 do 180) w swoim inwentarzu.

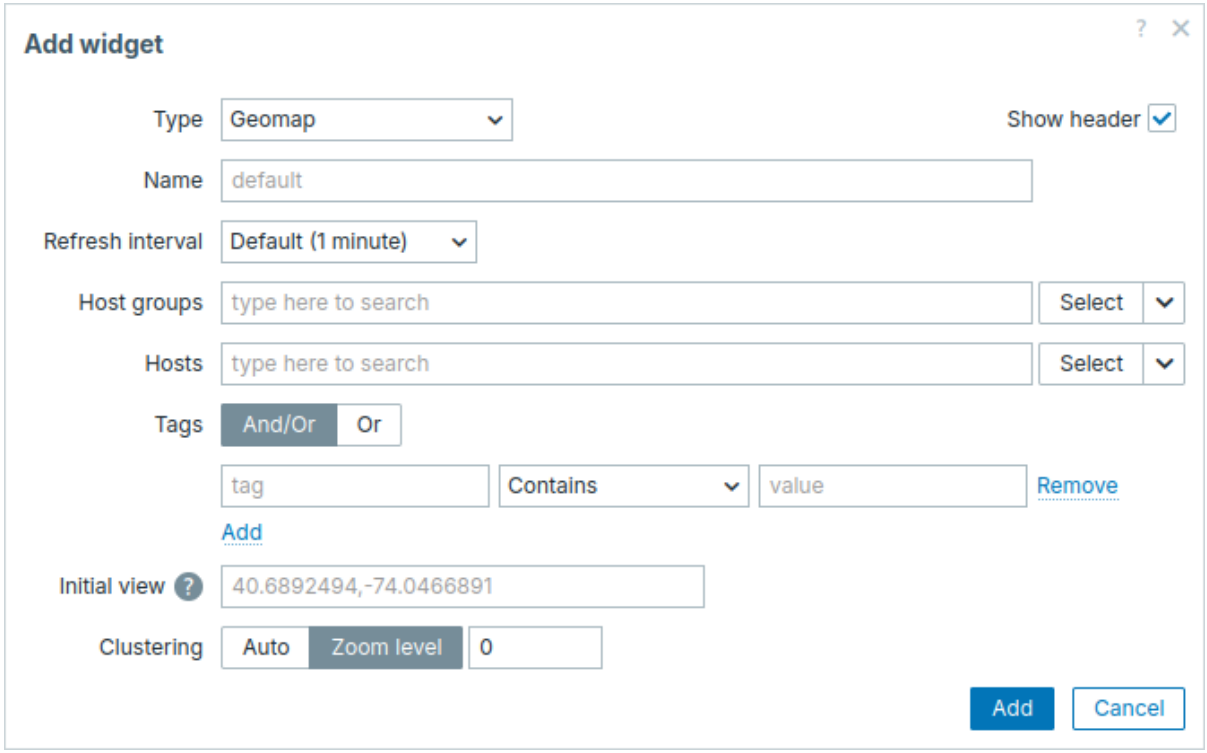
Użyj następujących opcji, aby korzystać z widżetu:

- Kliknięcie znacznika powoduje wyświetlenie nazwy hosta i nierozwiązanych problemów; kliknięcie nazwy hosta otwiera menu hosta.
- Filtruj hosty według ważności problemu za pomocą ikony filtra w prawym górnym rogu.
- Kliknij mapę prawym przyciskiem myszy, aby ustawić lub zresetować widok domyślny; użyj ikony domu, aby wrócić do widoku domyślnego.



Konfiguracja

Aby dodać widget, wybierz *Geomap* jako typ.



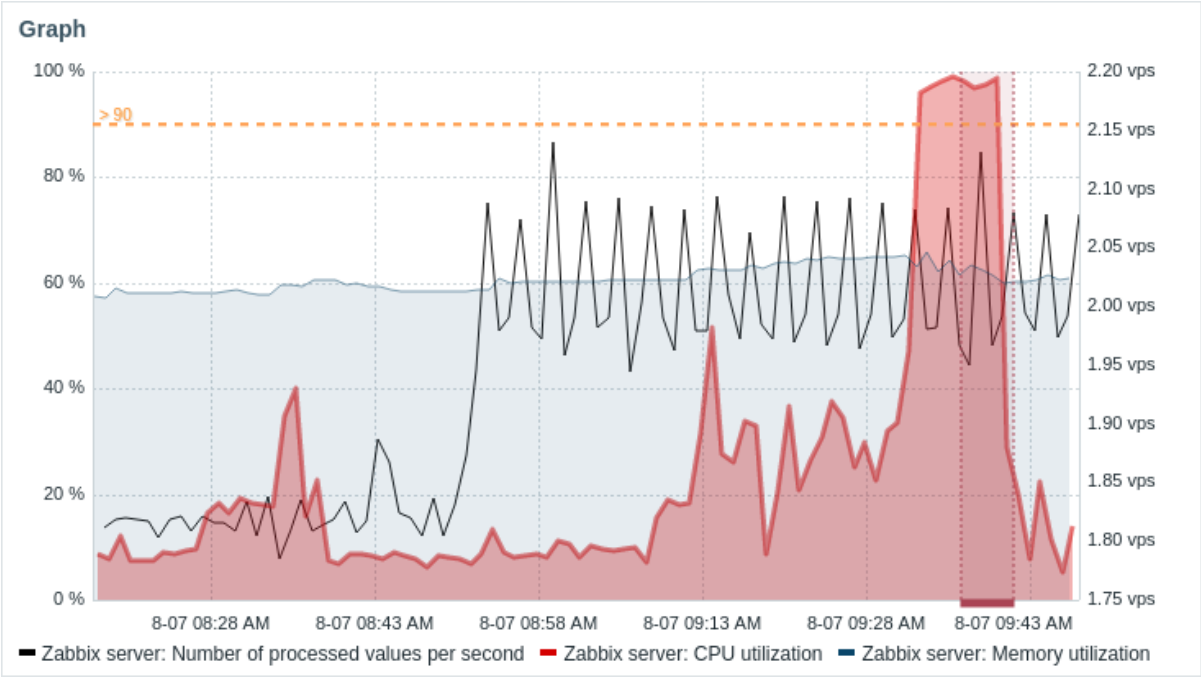
Oprócz parametrów wspólnych dla wszystkich widgetów można ustawić następujące opcje specyficzne:

Grupy hostów	Wybierz grupy hostów, które mają być wyświetlane na mapie. Alternatywnie wybierz zgodny widget jako źródło danych dla grup hostów. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy grupy zostanie wyświetlona rozwijana lista pasujących grup. Jeśli w polach *Grupy hostów* i *Hosty* nic nie zostanie wybrane, zostaną wyświetlone wszystkie hosty z prawidłowymi współrzędnymi. Ten parametr nie jest dostępny podczas konfigurowania widgetu na pulpicie szablonu.
Hosty	Wybierz hosty, które mają być wyświetlane na mapie. Alternatywnie wybierz zgodny widget lub pulpit jako źródło danych dla hostów. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy hosta zostanie wyświetlona rozwijana lista pasujących hostów. Jeśli w polach *Grupy hostów* i *Hosty* nic nie zostanie wybrane, zostaną wyświetlone wszystkie hosty z prawidłowymi współrzędnymi. Ten parametr nie jest dostępny podczas konfigurowania widgetu na pulpicie szablonu.
Tagi	Określ tagi, aby ograniczyć liczbę hostów wyświetlanych w widżecie. Można zarówno uwzględniać, jak i wykluczać określone tagi oraz wartości tagów. Można ustawić kilka warunków. Dopasowanie nazw tagów zawsze uwzględnia wielkość liter. Dla każdego warunku dostępnych jest kilka operatorów: **Istnieje** - uwzględnij określone nazwy tagów; **Równa się** - uwzględnij określone nazwy i wartości tagów (z uwzględnieniem wielkości liter); **Zawiera** - uwzględnij określone nazwy tagów, których wartości zawierają wprowadzony ciąg znaków (dopasowanie podciągu, bez uwzględniania wielkości liter); **Nie istnieje** - wyklucz określone nazwy tagów; **Nie równa się** - wyklucz określone nazwy i wartości tagów (z uwzględnieniem wielkości liter); **Nie zawiera** - wyklucz określone nazwy tagów, których wartości zawierają wprowadzony ciąg znaków (dopasowanie podciągu, bez uwzględniania wielkości liter). Dostępne są dwa typy obliczania warunków: **And/Or** - wszystkie warunki muszą być spełnione, a warunki mające tę samą nazwę tagu będą grupowane przez warunek *Or*; **Or** - wystarczy spełnienie jednego warunku. Ten parametr nie jest dostępny podczas konfigurowania widgetu na pulpicie szablonu.
Widok początkowy	Oddzielone przecinkami współrzędne środka oraz opcjonalny poziom powiększenia wyświetlany przy początkowym załadowaniu widgetu, w formacie `<latitude>,<longitude>,<zoom>` Jeśli określono początkowy poziom powiększenia, widget Geomap zostanie załadowany z podanym poziomem powiększenia. W przeciwnym razie początkowy poziom powiększenia jest obliczany jako połowa maksymalnego poziomu powiększenia dla danego dostawcy kafelków. Widok początkowy jest ignorowany, jeśli ustawiono widok domyślny (patrz poniżej). Przykłady: 40.6892494,-74.0466891 40.6892494,-122.0466891
Klastrowanie	Określ, w jaki sposób znaczniki pobliskich hostów są łączone w jeden znacznik z licznikiem: **Auto** - znaczniki są łączone automatycznie; **Poziom powiększenia** - znaczniki są łączone na podstawie określonego poziomu powiększenia (0 - maksymalne oddalenie, 30 - maksymalne przybliżenie). Na przykład, jeśli parametr jest ustawiony na 0, znaczniki nie są łączone przy żadnym poziomie powiększenia; jeśli ustawiono 15, znaczniki są łączone od maksymalnego oddalenia do poziomu powiększenia 15; jeśli ustawiono 30, znaczniki są łączone przy wszystkich poziomach powiększenia. Należy pamiętać, że maksymalny poziom przybliżenia jest określany przez dostawcę kafelków mapy.

8 Graph

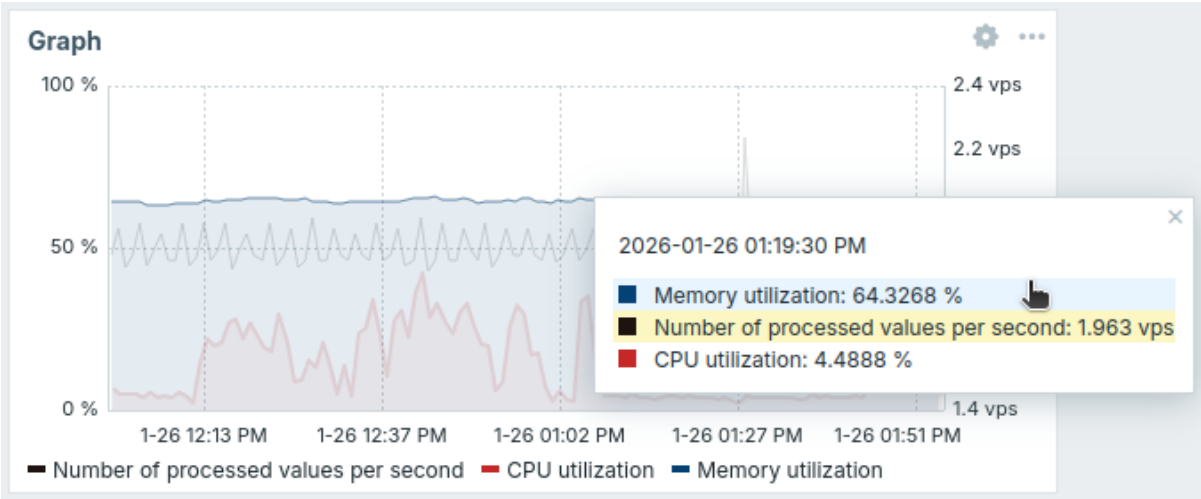
Przegląd

Widżet *Graph* wyświetla numeryczne dane pozycji w postaci grafu wektorowego. Może pomóc w śledzeniu trendów, wykrywaniu problemów oraz porównywaniu wartości w czasie i między hostami.

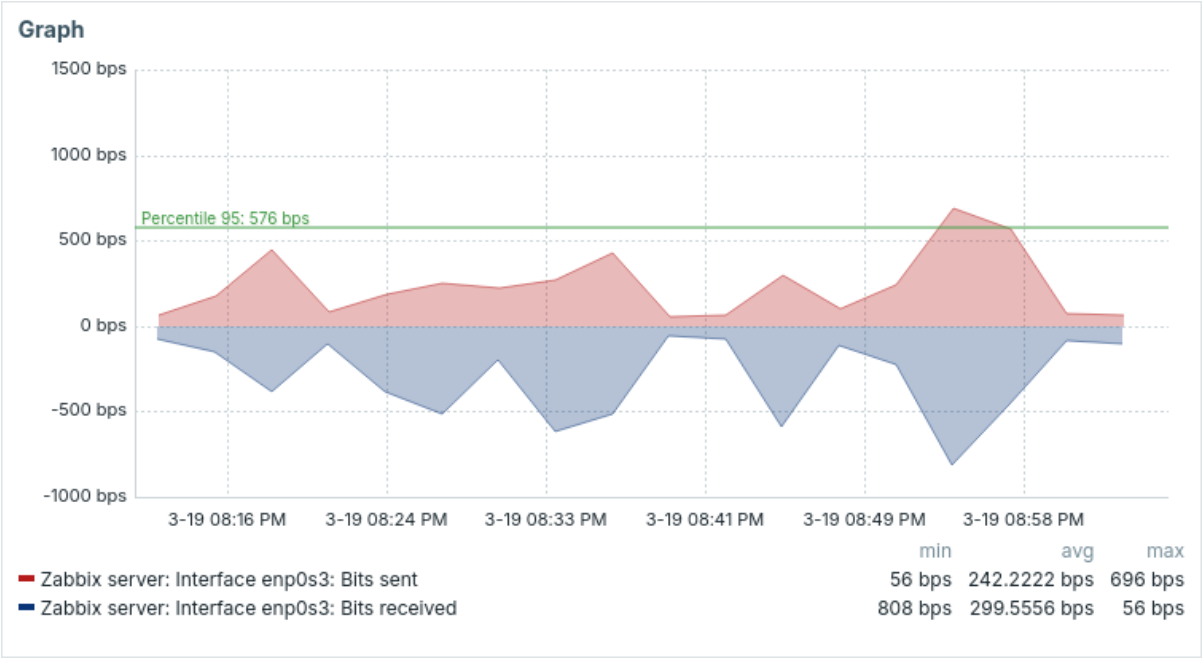


Najechanie kursorem na graf powoduje wyświetlenie podpowiedzi z listą pozycji posortowanych według wartości malejąco.

Najechanie kursorem na pozycję w podpowiedzi podświetla jej graf (pozostałe są przyciemnione); wybranie pozycji przekazuje jej dane do innych widżetów.



Graf może być wyświetlany z odwróconymi wartościami osi Y; wpływa to jedynie na reprezentację wizualną i nie zmienia oryginalnych wartości.

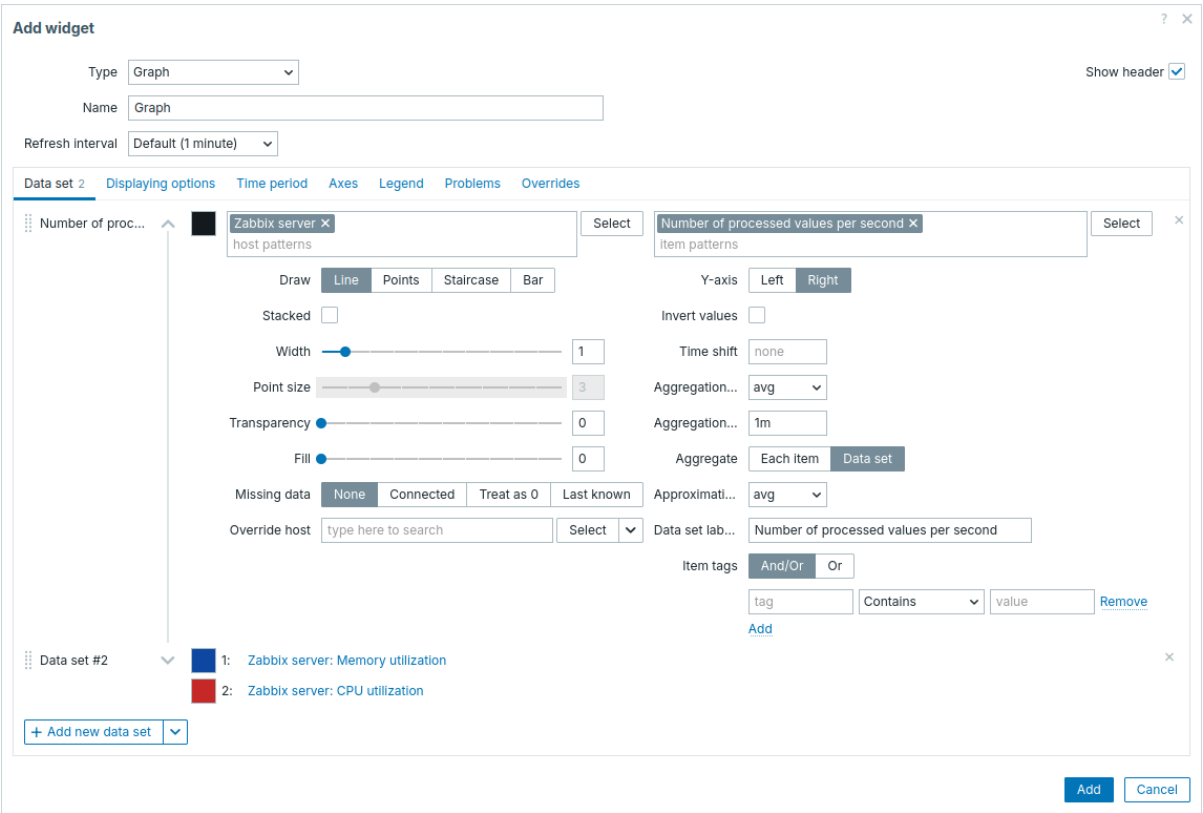


Dostępny jest również starszy widżet Graph (classic).

Informacje wyświetlane w widżecie *Graph* można pobrać jako obraz PNG, wybierając opcję *Download image* w menu widżetu.

Konfiguracja

Aby skonfigurować, wybierz *Graph* jako typ:



Zestaw danych

Zakładka **Zestaw danych** umożliwia wybór danych do wykresu przez dodawanie zestawów danych. Można dodać dwa typy zestawów danych:

- *Wzorce pozycji* - wyświetlane są dane z pasujących pozycji. Możesz wybrać jeden kolor bazowy lub wybrać wiersz palety, aby przypisać odrębne kolory do każdej dopasowanej pozycji.
- *Lista pozycji* - wyświetlane są dane z wybranych pozycji. Możesz wybrać kolor każdej pozycji indywidualnie za pomocą próbnika.

Domyślnie dodawany jest zestaw danych typu *Wzorce pozycji*.

Zestaw danych	Dla zestawu danych **Wzorce pozycji**: Wybierz lub wprowadź wzorce hosta i pozycji; dane pozycji pasujących do tych wzorców będą wyświetlane na wykresie; można wyświetlić maksymalnie 50 pozycji. Do wyboru można używać wzorców wieloznacznych (na przykład ∗ zwróci wyniki pasujące do zera lub większej liczby znaków). Aby określić wzorzec wieloznaczny, wprowadź ciąg ręcznie i naciśnij *Enter*. Symbol wieloznaczny jest zawsze interpretowany, dlatego nie można na przykład dodać indywidualnie pozycji o nazwie *item**, jeśli istnieją inne pasujące pozycje (na przykład *item2*, *item3*). Określenie wzorców hosta i pozycji jest obowiązkowe dla zestawów danych „Wzorce pozycji”. Zobacz także: Szczegóły konfiguracji zestawu danych. Dla zestawu danych **Lista pozycji**: Wybierz pozycje dla wykresu, klikając przycisk *Dodaj pozycję*. Możesz także wybrać zgodne widgety jako źródło danych dla pozycji, klikając przycisk *Dodaj widget*. Określenie pozycji lub widgetów jest obowiązkowe dla zestawów danych „Lista pozycji”. Zobacz także: Szczegóły konfiguracji zestawu danych. Pamiętaj, że dozwolone są tylko numeryczne typy pozycji. Podczas konfigurowania widgetu na pulpicie szablonu parametr do określania wzorców hosta nie jest dostępny, a parametr do określania listy pozycji pozwala wybrać tylko pozycje skonfigurowane w szablonie.
Rysowanie	Wybierz typ rysowania metryki. Dostępne typy rysowania: *Linia* (ustawiona domyślnie), *Punkty*, *Schodkowy* i *Słupkowy*. Pamiętaj, że jeśli na wykresie liniowym/schodkowym istnieje tylko jeden punkt danych, zostanie on narysowany jako punkt niezależnie od typu rysowania. Rozmiar punktu jest obliczany na podstawie szerokości linii, ale nie może być mniejszy niż 3 piksele, nawet jeśli szerokość linii jest mniejsza.
Skumulowany	Zaznacz pole wyboru, aby wyświetlać dane jako skumulowane (wyświetlane są wypełnione obszary). Ta opcja jest wyłączona, gdy wybrany jest typ rysowania *Punkty*.
Szerokość	Ustaw szerokość linii. Ta opcja jest dostępna, gdy wybrany jest typ rysowania *Linia* lub *Schodkowy*.
Rozmiar punktu	Ustaw rozmiar punktu. Ta opcja jest dostępna, gdy wybrany jest typ rysowania *Punkty*.
Przezroczystość	Ustaw poziom przezroczystości.
Wypełnienie	Ustaw poziom wypełnienia. Ta opcja jest dostępna, gdy wybrany jest typ rysowania *Linia* lub *Schodkowy*.
Brakujące dane	Wybierz opcję wyświetlania brakujących danych: **Brak** - przerwa pozostaje pusta; **Połączone** - dwie wartości graniczne są łączone; **Traktuj jako 0** - brakujące dane są wyświetlane jako wartości 0; **Ostatnia znana** - brakujące dane są wyświetlane z taką samą wartością jak ostatnia znana wartość; nie dotyczy typu rysowania *Punkty* i *Słupkowy*.
Nadpisz hosta	Wybierz zgodny widget lub selektor hosta pulpitu jako źródło danych dla hostów. Ten parametr nie jest dostępny podczas konfigurowania widgetu na pulpicie szablonu.
Oś Y	Wybierz stronę wykresu, po której będzie wyświetlana oś Y.
Odwróć wartości	Zaznacz pole wyboru, aby przed wyświetleniem na wykresie pomnożyć wszystkie wartości osi Y przez -1. Wpływa to tylko na reprezentację wizualną; oryginalne dane pozostają bez zmian. Ta opcja nie wpływa na podpowiedź, legendę ani linię percentyla. Jeśli dla osi wybrano opcję *Proste wyzwalacze*, progi wyzwalaczy będą wyświetlane jako odwrócone.
Przesunięcie czasu	W razie potrzeby określ przesunięcie czasu. W tym polu można używać sufiksów czasu. Dozwolone są wartości ujemne.

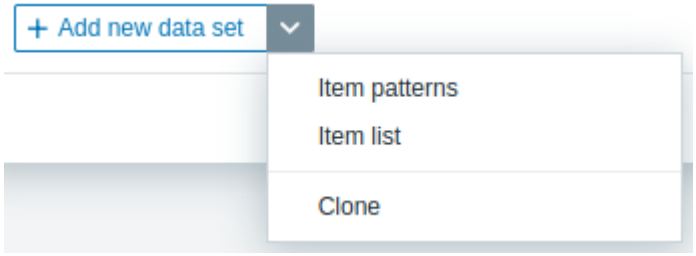
Funkcja agregacji	Określ, której funkcji agregacji użyć: **min** - wyświetl najmniejszą wartość; **max** - wyświetl największą wartość; **avg** - wyświetl wartość średnią; **sum** - wyświetl sumę wartości; **count** - wyświetl liczbę wartości; **first** - wyświetl pierwszą wartość; **last** - wyświetl ostatnią wartość; **none** - wyświetl wszystkie wartości (bez agregacji). Agregacja umożliwia wyświetlenie zagregowanej wartości dla wybranego przedziału (5 minut, godzina, dzień) zamiast wszystkich wartości. Zobacz także: Agregacja na wykresach.
Interwał agregacji	Określ przedział agregowania wartości. W tym polu można używać sufiksów czasu. Wartość liczbowa bez sufiksu będzie traktowana jako sekundy. Pamiętaj, że jeśli widget jest skonfigurowany do wyświetlania danych historycznych na podstawie trendów (*Wybór danych historycznych* jest ustawiony na *Trendy* lub *Auto*), zaleca się użycie interwału agregacji będącego wielokrotnością 1 godziny (np. 3600, 60m, 1h, 3h itd.). Trendy przechowują godzinowe wartości zagregowane, więc użycie interwału agregacji, który nie jest wielokrotnością 1 godziny (np. 100s, 7min, 15min, 90min itd.), może prowadzić do wyników trudnych do interpretacji.
Agreguj	Określ, czy agregować: **Każdą pozycję** - każda pozycja w zestawie danych będzie agregowana i wyświetlana osobno; **Zestaw danych** - wszystkie pozycje zestawu danych będą agregowane i wyświetlane jako jedna wartość.
Przybliżenie	Określ, jaką wartość wyświetlić, gdy na jeden pionowy piksel wykresu przypada więcej niż jedna wartość: **all** - wyświetl najmniejszą, największą i średnią wartość; **min** - wyświetl najmniejszą wartość; **max** - wyświetl największą wartość; **avg** - wyświetl wartość średnią. To ustawienie jest przydatne podczas wyświetlania wykresu dla długiego okresu czasu z częstym interwałem aktualizacji (na przykład jednego roku wartości zbieranych co 10 minut).
Etykieta zestawu danych	Określ etykietę zestawu danych wyświetlaną w konfiguracji wykresu *Zestaw danych* oraz w *Legendzie* wykresu (dla zagregowanych zestawów danych). Wszystkie zestawy danych są numerowane, także te z określoną *Etykietą zestawu danych*. Jeśli etykieta nie zostanie określona, zestaw danych zostanie oznaczony automatycznie zgodnie ze swoim numerem (np. „Zestaw danych #2”, „Zestaw danych #3” itd.). Numeracja zestawów danych jest przeliczana po zmianie kolejności/przeciągnięciu zestawów danych. Zbyt długie etykiety zestawów danych zostaną skrócone, aby zmieściły się w miejscu wyświetlania (np. „Liczba proc...”).

Tagi pozycji	Określ tagi do filtrowania pozycji wyświetlanych w widżecie. Możliwe jest zarówno uwzględnianie, jak i wykluczanie określonych tagów oraz wartości tagów. Można ustawić kilka warunków. Dopasowanie nazw tagów zawsze uwzględnia wielkość liter. Dla każdego warunku dostępnych jest kilka operatorów: **Istnieje** - uwzględnij określone nazwy tagów; **Równa się** - uwzględnij określone nazwy tagów i wartości (z uwzględnieniem wielkości liter); **Zawiera** - uwzględnij określone nazwy tagów, w których wartości tagów zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter); **Nie istnieje** - wyklucz określone nazwy tagów; **Nie równa się** - wyklucz określone nazwy tagów i wartości (z uwzględnieniem wielkości liter); **Nie zawiera** - wyklucz określone nazwy tagów, w których wartości tagów zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter). Dostępne są dwa typy obliczania warunków: **And/Or** - wszystkie warunki muszą być spełnione, a warunki mające tę samą nazwę tagu będą grupowane operatorem Or; **Or** - wystarczy spełnienie jednego warunku.

Szczegóły konfiguracji zestawu danych

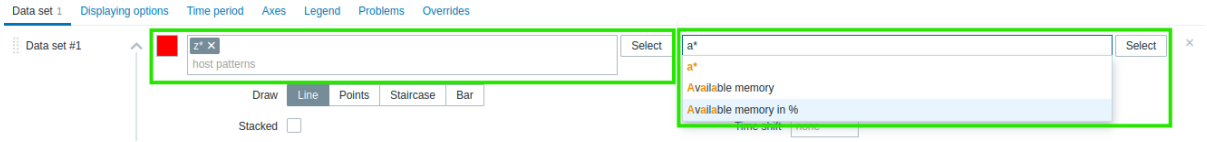
Istniejące zestawy danych są wyświetlane na liście. Możesz:

- Kliknąć ikonę przenoszenia i przeciągnąć zestaw danych w nowe miejsce na liście.
- Kliknąć ikonę rozwijania , aby rozwinąć szczegóły zestawu danych. Po rozwinięciu ikona ta zmienia się w ikonę zwijania .
- Kliknąć ikonę koloru , aby otworzyć selektor. Możesz wprowadzić kod szesnastkowy, wybrać jednolity kolor próbki albo przełączyć się na kartę *Palette* i wybrać wiersz predefiniowanych kolorów. Wybrany kolor jest stosowany bezpośrednio do zestawów danych *Item list* lub jako baza dla generowanych odcieni w *Item patterns*. Użyj klawisza Tab, aby przechodzić między elementami sterującymi okna dialogowego, klawiszy strzałek do poruszania się po próbkach lub wierszach palety, klawisza Enter, aby wybrać, oraz Esc, aby anulować.
- Kliknąć przycisk *Add new data set*, aby dodać pusty zestaw danych umożliwiający wybór wzorców hosta i pozycji. Jeśli klikniesz ikonę skierowaną w dół obok przycisku *Add new data set*, pojawi się menu rozwijane, umożliwiające dodanie nowego zestawu danych *Item patterns* lub *Item list* albo *Clone* aktualnie otwartego zestawu danych. Jeśli wszystkie zestawy danych są zwinięte, opcja *Clone* nie jest dostępna.

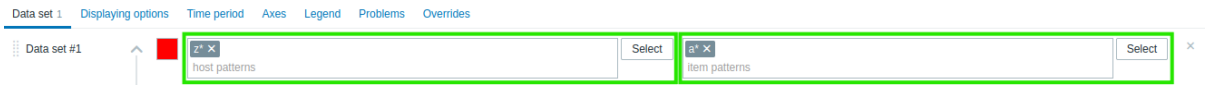


Zestaw danych **Wzorce pozycji** zawiera pola *Wzorce hostów* i *Wzorce pozycji*, które rozpoznają zarówno pełne nazwy, jak i wzorce zawierające symbol wieloznaczny (*). Ta funkcjonalność pozwala wybrać wszystkie nazwy hostów i nazwy pozycji zawierające wybrany wzorzec. Podczas wpisywania nazwy pozycji lub wzorca pozycji w polu *Wzorce pozycji* na liście rozwijanej wyświetlane są tylko pozycje należące do wybranych nazw hostów.

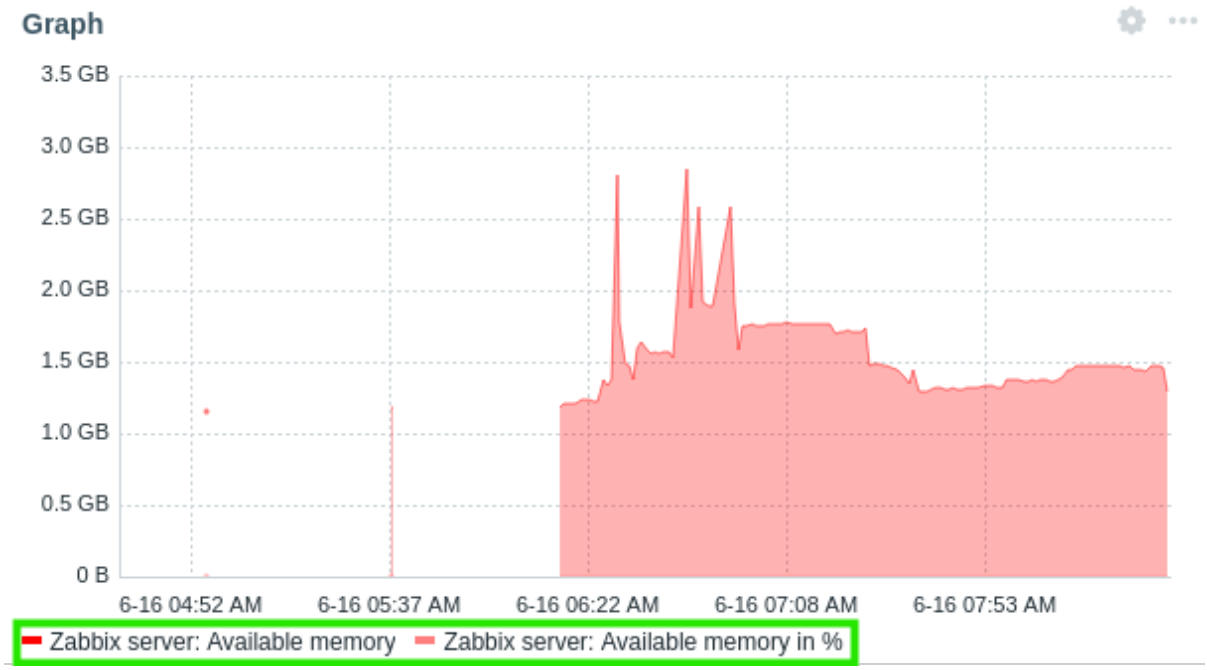
Na przykład po wpisaniu wzorca **z*** w polu *Wzorce hostów* lista rozwijana wyświetla wszystkie nazwy hostów zawierające ten wzorzec: **z*, Zabbix server, Zabbix proxy**. Po naciśnięciu *Enter* wzorzec zostaje zaakceptowany i jest wyświetlany jako **z***. Podobnie po wpisaniu wzorca **a*** w polu *Wzorce pozycji* lista rozwijana wyświetla wszystkie nazwy pozycji zawierające ten wzorzec: **a*, Available memory, Available memory in %**.



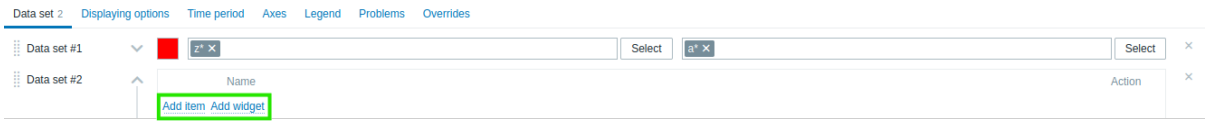
Po naciśnięciu *Enter* wzorzec zostaje zaakceptowany i wyświetlony jako **a***.



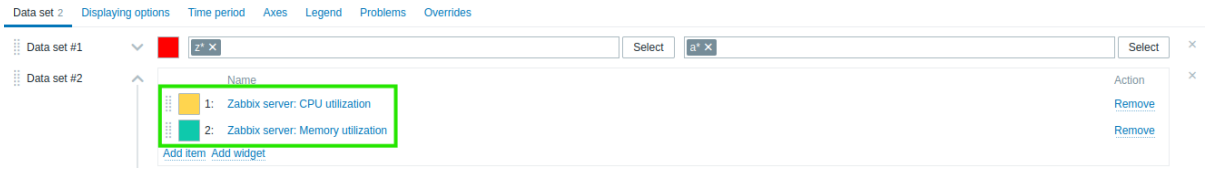
Wykres wyświetla następnie wszystkie pozycje należące do wybranych nazw hostów.



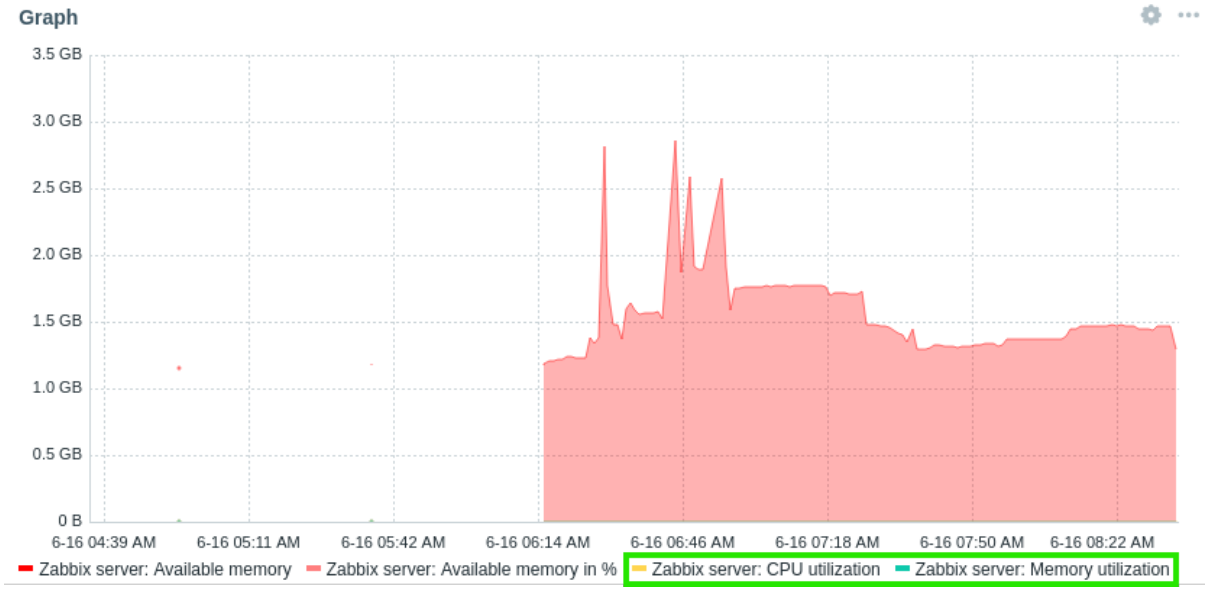
Zestaw danych **Lista pozycji** zawiera przycisk *Dodaj pozycję*, który umożliwia dodanie pozycji wyświetlanych na wykresie. Możesz także dodać zgodne widgety jako źródło danych dla pozycji, klikając przycisk *Dodaj widget*.



Na przykład kliknięcie przycisku *Dodaj pozycję* otwiera wyskakujące okno zawierające parametr *Host*. Po wybraniu hosta na liście wyświetlane są wszystkie jego pozycje dostępne do wyboru.

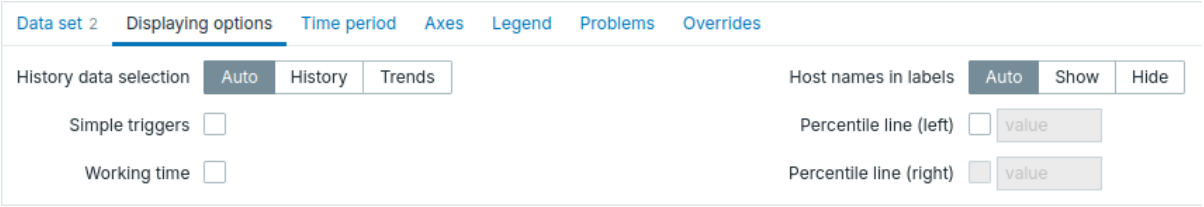


Po wybraniu jednej lub większej liczby pozycji zostaną one wyświetlone na liście pozycji zestawu danych oraz na wykresie.



Opcje wyświetlania

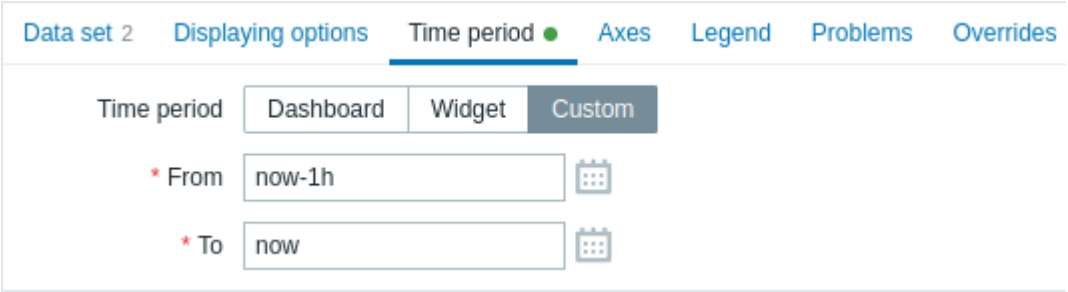
Zakładka **Opcje wyświetlania** umożliwia zdefiniowanie wyboru danych historii:



Wybór danych historii	Ustaw źródło danych wykresu: **Auto** - dane są pobierane zgodnie z klasycznym algorytmem wykresu (domyślnie); **Historia** - dane z historii; **Trendy** - dane z trendów.
Proste wyzwalacze	Zaznacz pole wyboru, aby wyświetlić progi wyzwalaczy dla prostych wyzwalaczy. Progi zostaną narysowane jako linie przerywane z użyciem koloru ważności wyzwalacza. Prosty wyzwalacz to wyzwalacz z jedną funkcją (tylko `last`, `max`, `min`, `avg`) dla jednej pozycji w wyrażeniu. Maksymalnie można narysować trzy wyzwalacze. Pamiętaj, że wyzwalacz musi znajdować się w rysowanym zakresie, aby był widoczny.
Czas pracy	Zaznacz pole wyboru, aby wyświetlić czas pracy na wykresie. Czas pracy (dni robocze) jest wyświetlany na wykresach jako białe tło, natomiast czas wolny od pracy jest wyświetlany na szaro (w domyślnym motywie frontend *Original blue*).
Nazwy hostów w etykietach	Wybierz, czy wyświetlać nazwy hostów w legendzie wykresu oraz w podpowiedzi pojawiającej się po najechaniu kursorem na dane wykresu: **Auto** - nazwy hostów są wyświetlane tylko wtedy, gdy w zestawach danych występuje więcej niż jeden host (domyślnie). **Pokaż** - nazwy hostów są wyświetlane. **Ukryj** - nazwy hostów są ukryte. Ten parametr nie jest dostępny podczas konfigurowania widżetu na pulpicie szablonu.
Linia percentyla (lewa)	Zaznacz pole wyboru i wprowadź wartość percentyla, aby wyświetlić określony percentyl jako linię na lewej osi Y wykresu. Jeśli na przykład ustawiono percentyl 95%, linia percentyla będzie znajdować się na poziomie, poniżej którego mieści się 95 procent wartości.
Linia percentyla (prawa)	Zaznacz pole wyboru i wprowadź wartość percentyla, aby wyświetlić określony percentyl jako linię na prawej osi Y wykresu. Jeśli na przykład ustawiono percentyl 95%, linia percentyla będzie znajdować się na poziomie, poniżej którego mieści się 95 procent wartości.

Okres czasu

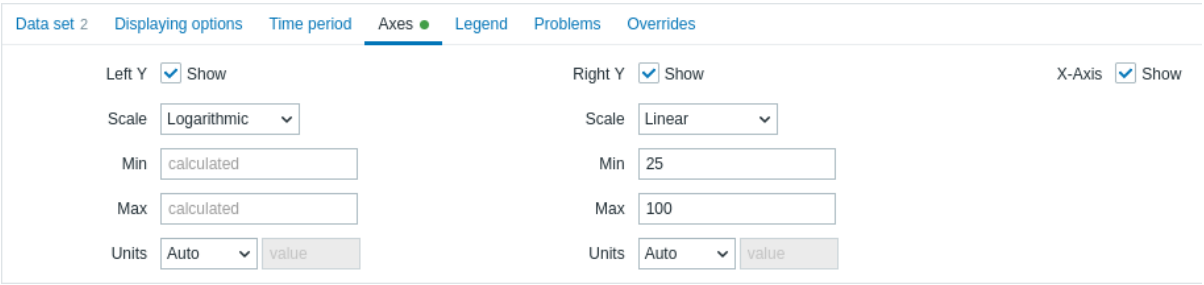
Zakładka **Okres czasu** umożliwia ustawienie okresu czasu, dla którego mają być wyświetlane dane na wykresie:



Okres czasu	Wybierz źródło danych dla okresu czasu: **Pulpit** — użyj selektora okresu czasu pulpitu; **Widget** — użyj kompatybilnego widgetu (ustawionego w parametrze *Widget*); **Niestandardowy** — użyj niestandardowego okresu czasu ustawionego w parametrach *Od* i *Do*; jeśli zostanie ustawiony, w prawym górnym rogu widgetu będzie wyświetlana ikona zegara, wskazująca ustawiony czas po najechaniu kursorem. Zwróć uwagę, że niezależnie od konfiguracji *Okres czasu* widgetu, kompatybilne widgety nadal mogą używać go jako źródła danych dla okresu czasu.
Widget	Wprowadź lub wybierz kompatybilny widget jako źródło danych dla okresu czasu. Ten parametr jest dostępny, jeśli *Okres czasu* jest ustawiony na „Widget”.
Od	Wprowadź lub wybierz początek okresu czasu. Obsługiwana jest składnia czasu względnego (`now`, `now/d`, `now/w-1w` itd.). Ten parametr jest dostępny, jeśli *Okres czasu* jest ustawiony na „Niestandardowy”.
Do	Wprowadź lub wybierz koniec okresu czasu. Obsługiwana jest składnia czasu względnego (`now`, `now/d`, `now/w-1w` itd.). Ten parametr jest dostępny, jeśli *Okres czasu* jest ustawiony na „Niestandardowy”.

Osie

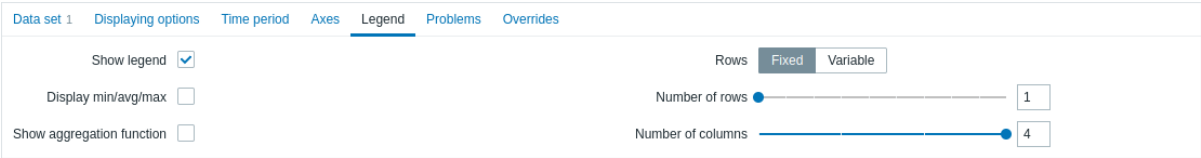
Zakładka **Osie** umożliwia dostosowanie sposobu wyświetlania osi:



Lewa Y	Zaznacz to pole wyboru, aby lewa oś Y była widoczna. Pole wyboru może być nieaktywne, jeśli opcja nie została zaznaczona ani w zakładce *Zbiór danych*, ani w zakładce *Nadpisania*.
Prawa Y	Zaznacz to pole wyboru, aby prawa oś Y była widoczna. Pole wyboru może być nieaktywne, jeśli opcja nie została zaznaczona ani w zakładce *Zbiór danych*, ani w zakładce *Nadpisania*.
Oś X	Odznacz to pole wyboru, aby ukryć oś X (domyślnie zaznaczone).
Skala	Wybierz skalę wartości osi wykresu z listy rozwijanej: **Liniowa** - wartości osi rosną o stałą wartość (np. 10, 20, 30), odpowiednia dla danych, które zmieniają się stopniowo lub obejmują mały albo średni zakres; **Logarytmiczna** - wartości osi rosną wykładniczo (np. 10, 100, 1000), odpowiednia dla danych, które zmieniają się szybko lub obejmują duży zakres.
Min	Ustaw minimalną wartość odpowiedniej osi. Określana jest minimalna wartość widocznego zakresu osi Y.
Max	Ustaw maksymalną wartość odpowiedniej osi. Określana jest maksymalna wartość widocznego zakresu osi Y.
Jednostki	Wybierz jednostkę dla wartości osi wykresu z listy rozwijanej: **Auto** - wartości osi są wyświetlane z użyciem jednostki pierwszej pozycji w zbiorze danych; **Statyczne** - wartości osi są wyświetlane z użyciem jednostki określonej w polu wejściowym *value*; jeśli pole pozostanie puste, wyświetlane będą tylko wartości liczbowe.

Legenda

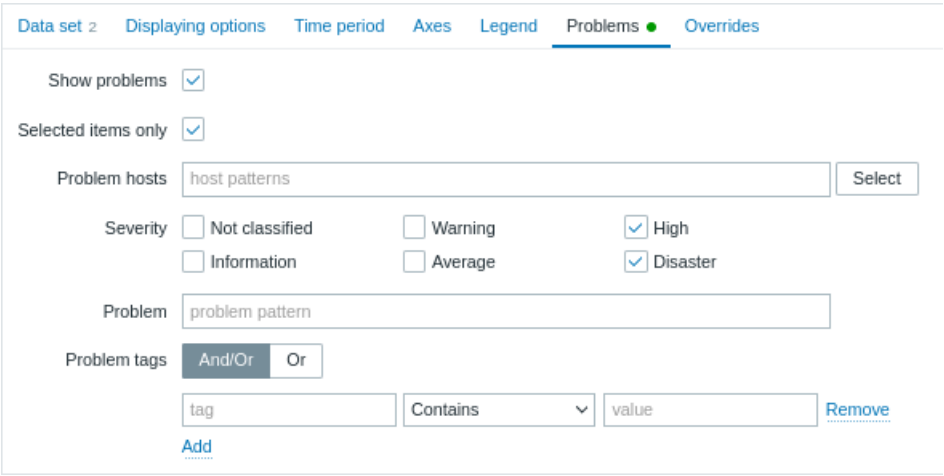
Zakładka **Legenda** umożliwia dostosowanie legendy wykresu:



Pokaż legendę	Odznacz to pole wyboru, aby ukryć legendę na wykresie (domyślnie zaznaczone).
Wyświetl min/śr./maks.	Zaznacz to pole wyboru, aby wyświetlić w legendzie minimalne, średnie i maksymalne wartości pozycji.
Pokaż funkcję agregacji	Zaznacz to pole wyboru, aby wyświetlić w legendzie funkcję agregacji.
Wiersze	Wybierz tryb wyświetlania wierszy legendy: **Stałe** — liczba wyświetlanych wierszy jest określana przez wartość parametru *Liczba wierszy*; **Zmienne** — liczba wyświetlanych wierszy jest określana przez liczbę skonfigurowanych pozycji, bez przekraczania wartości parametru *Maksymalna liczba wierszy*.
Liczba wierszy/ Maksymalna liczba wierszy	Jeśli dla parametru *Wiersze* ustawiono wartość „Stałe”, ustaw liczbę wyświetlanych wierszy legendy (1-10). Jeśli dla parametru *Wiersze* ustawiono wartość „Zmienne”, ustaw maksymalną liczbę wyświetlanych wierszy legendy (1-10).
Liczba kolumn	Ustaw liczbę wyświetlanych kolumn legendy (1-4). Ten parametr jest dostępny, jeśli opcja *Wyświetl min/śr./maks.* jest odznaczona.

Problemy

Zakładka **Problemy** umożliwia dostosowanie wyświetlania problemów:

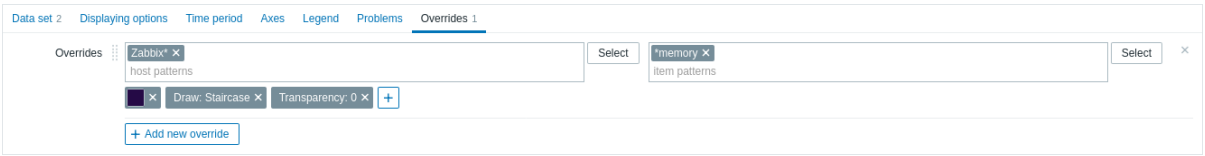


Pokaż problemy	Zaznacz to pole wyboru, aby włączyć wyświetlanie problemów na wykresie (domyślnie pole nie jest zaznaczone, tj. opcja jest wyłączona).
Tylko wybrane pozycje	Zaznacz to pole wyboru, aby na wykresie były wyświetlane tylko problemy dla wybranych pozycji.
Hosty problemów	Wybierz hosty problemów, które mają być wyświetlane na wykresie. Można używać wzorców wieloznacznych (na przykład ∗ zwróci wyniki pasujące do zera lub większej liczby znaków). Aby określić wzorzec wieloznaczny, po prostu wpisz ciąg ręcznie i naciśnij *Enter*. Podczas wpisywania zwróć uwagę, że wszystkie pasujące hosty są wyświetlane na liście rozwijanej. Ten parametr nie jest dostępny podczas konfigurowania widżetu na pulpicie szablonu.
Ważność	Zaznacz poziomy ważności problemów, aby filtrować problemy wyświetlane na wykresie. Jeśli nie zaznaczono żadnych poziomów ważności, zostaną wyświetlone wszystkie problemy.
Problem	Określ nazwę problemu, która ma być wyświetlana na wykresie.

Tagi problemu	Określ tagi problemu, aby ograniczyć liczbę problemów wyświetlanych w widżecie. Możliwe jest zarówno uwzględnianie, jak i wykluczanie określonych tagów oraz wartości tagów. Można ustawić kilka warunków. Dopasowanie nazw tagów zawsze uwzględnia wielkość liter. Dla każdego warunku dostępnych jest kilka operatorów: **Istnieje** - uwzględnij określone nazwy tagów; **Równa się** - uwzględnij określone nazwy tagów i wartości (z uwzględnieniem wielkości liter); **Zawiera** - uwzględnij określone nazwy tagów, dla których wartości tagów zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter); **Nie istnieje** - wyklucz określone nazwy tagów; **Nie równa się** - wyklucz określone nazwy tagów i wartości (z uwzględnieniem wielkości liter); **Nie zawiera** - wyklucz określone nazwy tagów, dla których wartości tagów zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter). Dostępne są dwa typy obliczeń dla warunków: **And/Or** - wszystkie warunki muszą być spełnione, warunki mające tę samą nazwę tagu będą grupowane warunkiem *Or*; **Or** - wystarczy, że jeden warunek zostanie spełniony.

Nadpisania

Zakładka **Nadpisania** umożliwia dodawanie niestandardowych nadpisań dla zestawów danych:



Nadpisania są przydatne, gdy dla zestawu danych wybrano kilka pozycji przy użyciu symbolu wieloznacznego ∗ i chcesz zmienić sposób domyślnego wyświetlania pozycji (np. domyślny kolor bazowy lub dowolną inną właściwość).

Istniejące nadpisania (jeśli są) są wyświetlane na liście. Aby dodać nowe nadpisanie:

- Kliknij przycisk 

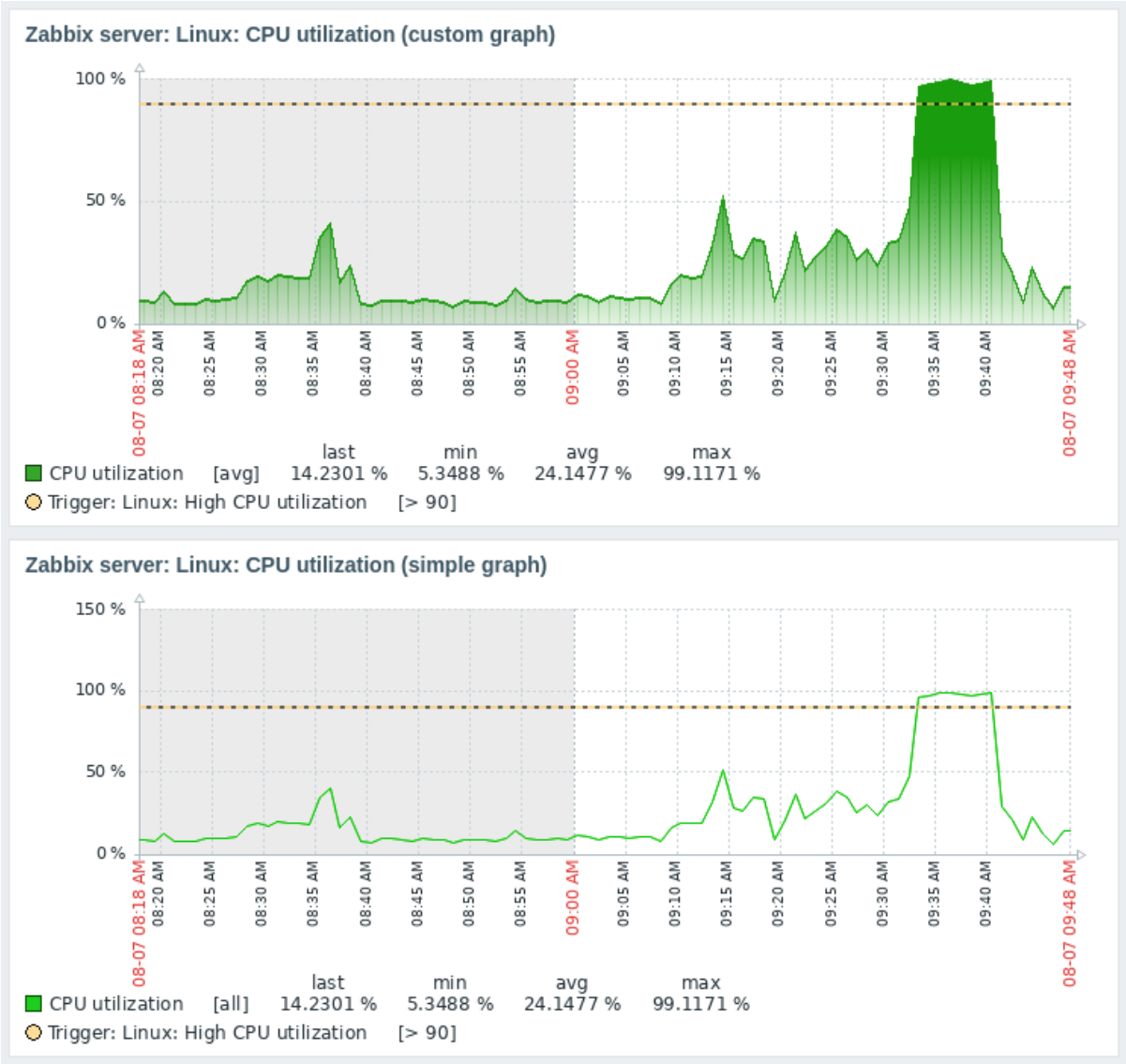
- Wybierz hosty i pozycje dla nadpisania. Alternatywnie możesz wprowadzić wzorce hostów i pozycji. Można używać wzorców wieloznacznych (na przykład ∗ zwróci wyniki pasujące do zera lub większej liczby znaków). Aby określić wzorzec wieloznaczny, po prostu wpisz ciąg ręcznie i naciśnij *Enter*. Podczas wpisywania zwróć uwagę, że wszystkie pasujące hosty są wyświetlane na liście rozwijanej. Symbol wieloznaczny jest zawsze interpretowany, dlatego nie można na przykład dodać pojedynczo pozycji o nazwie ”item*”, jeśli istnieją inne pasujące pozycje (np. item2, item3). Parametry wzorca hosta i wzorca pozycji są obowiązkowe. Parametr służący do określania wzorców hostów nie jest dostępny podczas konfigurowania widżetu na pulpicie szablonu. Parametr służący do określania listy pozycji pozwala wybrać tylko pozycje skonfigurowane w szablonie podczas konfigurowania widżetu na pulpicie szablonu.
- Kliknij 

, aby wybrać parametry nadpisania. Należy wybrać co najmniej jeden parametr nadpisania. Opisy parametrów znajdują się powyżej, w zakładce *Zestaw danych*.

9 Graph (classic)

Przegląd

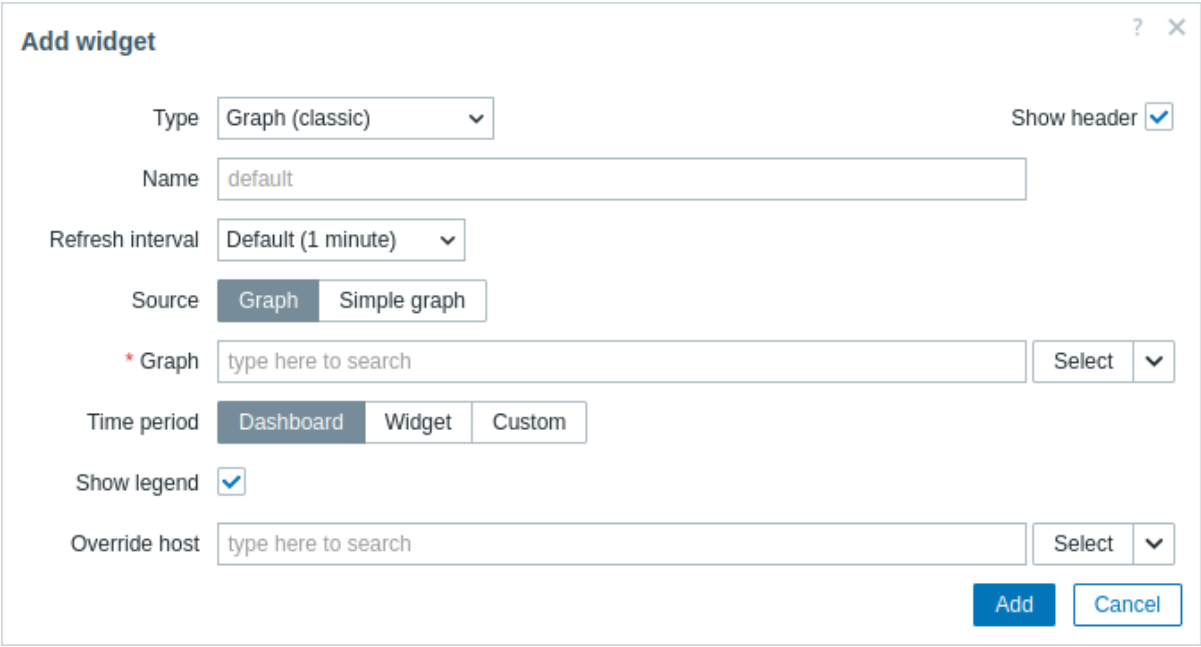
Widżet *Graph (classic)* wyświetla numeryczne dane pozycji jako obraz oparty na wykresie niestandardowym lub wykresie prostym. Obsługuje wybór przedziału czasu, linie wyzwalaczy oraz opcjonalne wyświetlanie legendy.



Informacje wyświetlane w widżecie *Graph (classic)* można pobrać jako obraz PNG, wybierając opcję *Download image* w menu widżetu.

Konfiguracja

Aby skonfigurować widget, wybierz *Graph (classic)* jako typ:



Oprócz parametrów wspólnych dla wszystkich widgetów, możesz ustawić następujące opcje specyficzne:

Source	Wybierz typ wykresu: **Graph** - wykres niestandardowy; **Simple graph** - wykres prosty.
Graph	Wybierz wykres niestandardowy do wyświetlenia. Alternatywnie wybierz kompatybilny widget jako źródło danych dla wykresów. Ten parametr jest dostępny, jeśli *Source* jest ustawione na ”Graph”.
Item	Wybierz pozycja do wyświetlenia na wykresie prostym. Alternatywnie wybierz kompatybilny widget jako źródło danych dla pozycji. Ten parametr jest dostępny, jeśli *Source* jest ustawione na ”Simple graph”.
Time period	Ustaw przedział czasu, dla którego mają być wyświetlane dane na wykresie. Wybierz źródło danych dla przedziału czasu: **Dashboard** - użyj selektora przedziału czasu pulpitu; **Widget** - użyj kompatybilnego widgetu (ustawionego w parametrze *Widget*); **Custom** - użyj niestandardowego przedziału czasu ustawionego w parametrach *From* i *To*; jeśli jest ustawiony, w prawym górnym rogu widgetu zostanie wyświetlona ikona zegara, wskazująca ustawiony czas po najechaniu kursorem. Zwróć uwagę, że niezależnie od konfiguracji *Time period* widgetu, kompatybilne widgety nadal mogą używać go jako źródła danych dla przedziału czasu.
Widget	Wprowadź lub wybierz kompatybilny widget jako źródło danych dla przedziału czasu. Ten parametr jest dostępny, jeśli *Time period* jest ustawione na ”Widget”.
From	Wprowadź lub wybierz początek przedziału czasu. Obsługiwana jest składnia czasu względnego (`now`, `now/d`, `now/w-1w` itd.). Ten parametr jest dostępny, jeśli *Time period* jest ustawione na ”Custom”.
To	Wprowadź lub wybierz koniec przedziału czasu. Obsługiwana jest składnia czasu względnego (`now`, `now/d`, `now/w-1w` itd.). Ten parametr jest dostępny, jeśli *Time period* jest ustawione na ”Custom”.
Show legend	Odznacz to pole wyboru, aby ukryć legendę na wykresie (domyślnie zaznaczone).
Override host	Wybierz kompatybilny widget lub selektor hostów pulpitu jako źródło danych dla hostów. Ten parametr nie jest dostępny podczas konfigurowania widgetu na pulpicie szablonu.

Legenda wykresu składa się z trzech sekcji:

- Pozycje i ich wartości zagregowane
- Percentyle (jeśli są skonfigurowane)
- Wyzwalacze (jeśli są powiązane z wyświetlanymi pozycjami)

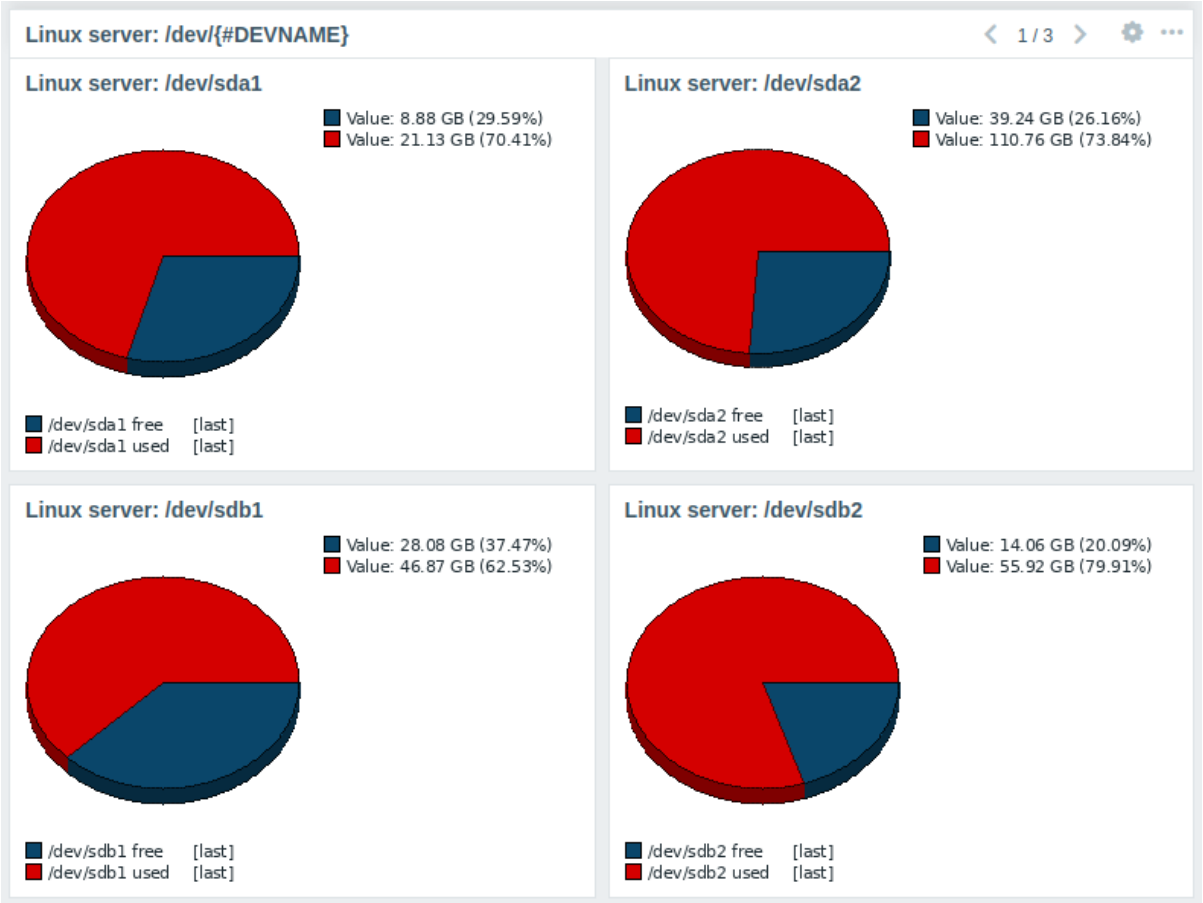
Jeśli wysokość wykresu w obrębie widgetu jest niewystarczająca, legenda może nie być wyświetlana lub może być wyświetlana tylko częściowo. Najpierw ukrywane są wyzwalacze i percentyle, a następnie legenda pozycji. Aby wyświetlić pełną legendę, zwiększ pionowy rozmiar widgetu.

Note:
Można wyświetlić nie więcej niż 3 linie wyzwalaczy. Jeśli wyzwalaczy jest więcej, priorytet wyświetlania mają wyzwalacze o niższym poziomie ważności.

10 Graph prototype

Przegląd

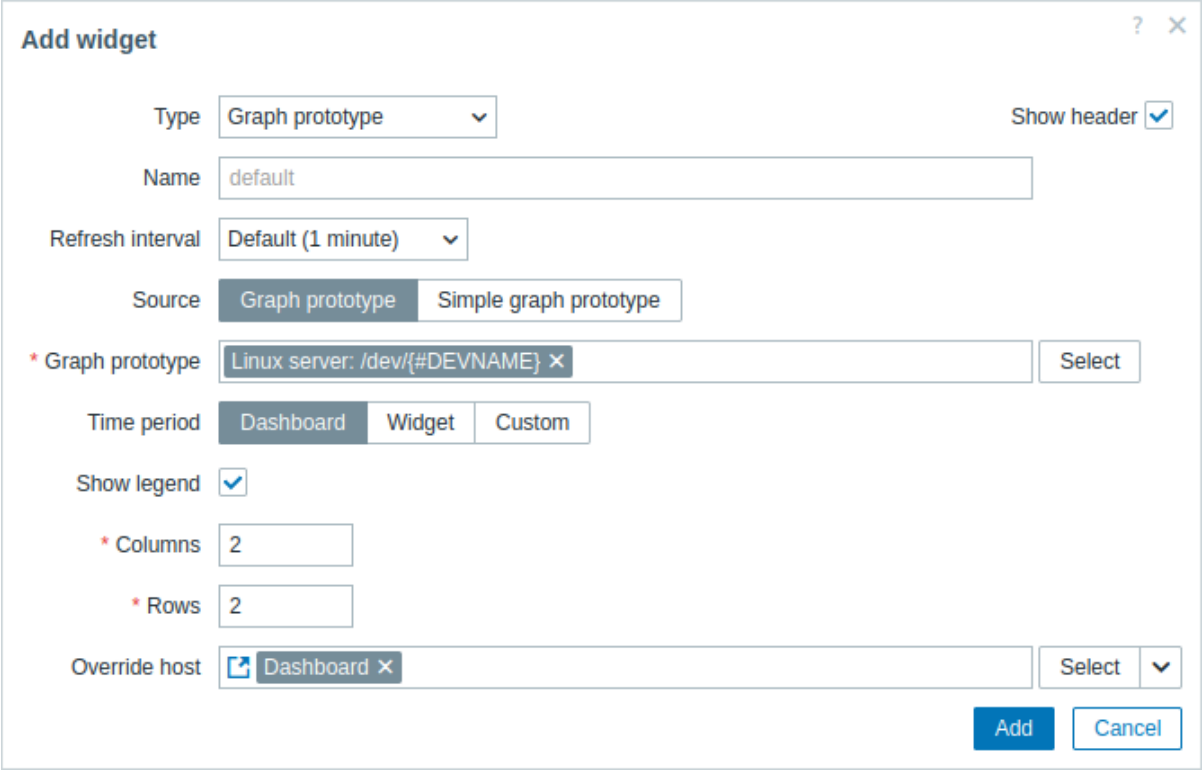
Widżet *Prototyp wykresu* wyświetla siatkę automatycznie tworzonych wykresów niestandardowych na podstawie prototypów wykresów lub prototypów pozycji reguły wykrywania niskiego poziomu.



Wykresy są rozmieszczane w konfigurowalnym układzie siatki; jeśli liczba wykresów przekracza pojemność układu, w widżecie włączane jest stronicowanie.

Konfiguracja

Aby skonfigurować widget, wybierz *Graph prototype* jako typ widgetu:



Oprócz parametrów wspólnych dla wszystkich widgetów, możesz ustawić następujące opcje specyficzne:

Source	Wybierz źródło wykresów: **Graph prototype** lub **Simple graph prototype**.

Graph prototype	Wybierz prototyp wykresu, aby wyświetlić wykresy wykryte przez prototyp wykresu. Ten parametr jest dostępny, jeśli dla *Source* ustawiono wartość „Graph prototype”.
Item prototype	Wybierz prototyp pozycji, aby wyświetlić proste wykresy dla pozycji wykrytych przez prototyp pozycji. Ten parametr jest dostępny, jeśli dla *Source* ustawiono wartość „Simple graph prototype”.
Time period	Ustaw przedział czasu, dla którego mają być wyświetlane dane na wykresach. Wybierz źródło danych dla przedziału czasu: **Dashboard** — użyj selektora przedziału czasu pulpitu; **Widget** — użyj kompatybilnego widgetu (ustawionego w parametrze *Widget*); **Custom** — użyj niestandardowego przedziału czasu ustawionego w parametrach *From* i *To*; jeśli zostanie ustawiony, w prawym górnym rogu widgetu będzie wyświetlana ikona zegara, wskazująca ustawiony czas po najechaniu kursorem. Zwróć uwagę, że niezależnie od konfiguracji *Time period* widgetu, kompatybilne widgety nadal mogą używać go jako źródła danych dla przedziału czasu.
Widget	Wprowadź lub wybierz kompatybilny widget jako źródło danych dla przedziału czasu. Ten parametr jest dostępny, jeśli dla *Time period* ustawiono wartość „Widget”.
From	Wprowadź lub wybierz początek przedziału czasu. Obsługiwana jest składnia czasu względnego (`now`, `now/d`, `now/w-1w` itd.). Ten parametr jest dostępny, jeśli dla *Time period* ustawiono wartość „Custom”.
To	Wprowadź lub wybierz koniec przedziału czasu. Obsługiwana jest składnia czasu względnego (`now`, `now/d`, `now/w-1w` itd.). Ten parametr jest dostępny, jeśli dla *Time period* ustawiono wartość „Custom”.
Show legend	Odznacz to pole wyboru, aby ukryć legendę na wykresach (domyślnie zaznaczone).
Override host	Wybierz kompatybilny widget lub selektor hosta pulpitu jako źródło danych dla hostów. Ten parametr nie jest dostępny podczas konfigurowania widgetu na pulpicie szablonu.
Columns	Wprowadź liczbę kolumn wykresów do wyświetlenia w widżecie prototypu wykresu.
Rows	Wprowadź liczbę wierszy wykresów do wyświetlenia w widżecie prototypu wykresu.

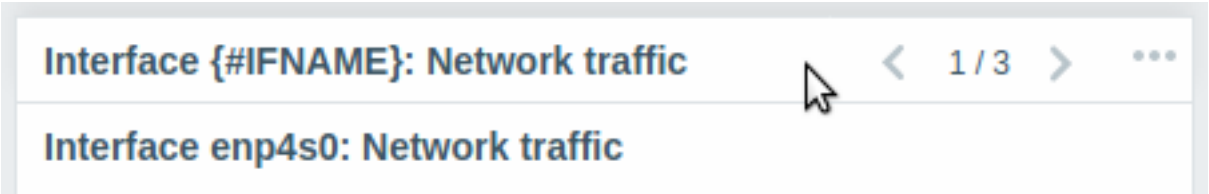
Legenda wykresu składa się z trzech sekcji:

- Pozycje i ich wartości zagregowane
- Percentyle (jeśli skonfigurowano)
- Wyzwalacze (jeśli są powiązane z wyświetlanymi pozycjami)

Jeśli wysokość wykresu w widżecie jest niewystarczająca, legenda może nie być wyświetlana lub może być wyświetlana tylko częściowo. Najpierw ukrywane są wyzwalacze i percentyle, a następnie legenda pozycji. Aby wyświetlić pełną legendę, zwiększ pionowy rozmiar widgetu.

Note:
Można wyświetlić nie więcej niż 3 linie wyzwalaczy. Jeśli wyzwalaczy jest więcej, do wyświetlenia priorytetowo wybierane są wyzwalacze o niższym poziomie ważności.

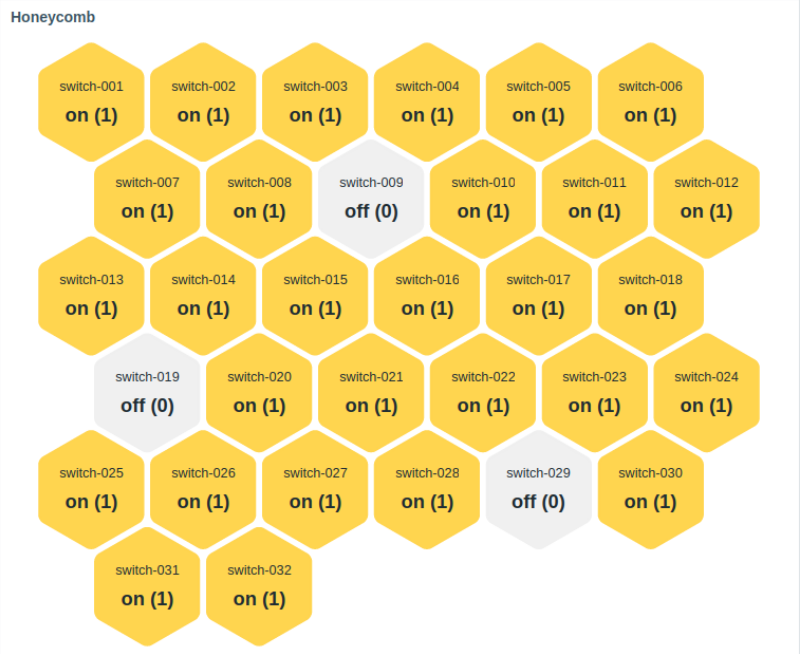
Chociaż parametry *Columns* i *Rows* pozwalają zmieścić w widżecie więcej niż jeden wykres, nadal może istnieć więcej wykrytych wykresów niż liczba kolumn/wierszy w widżecie. W takim przypadku w widżecie dostępne jest stronicowanie, a wysuwany nagłówek umożliwia przełączanie między stronami za pomocą lewej i prawej strzałki:

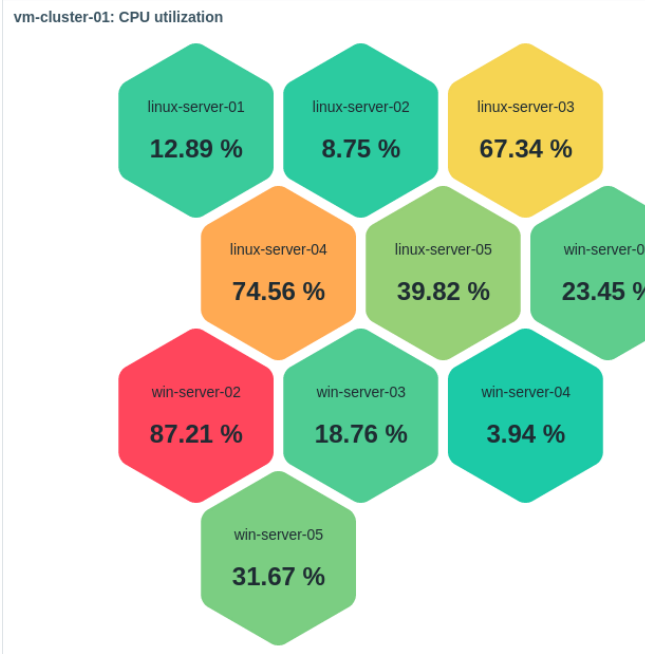


11 Honeycomb

Przegląd

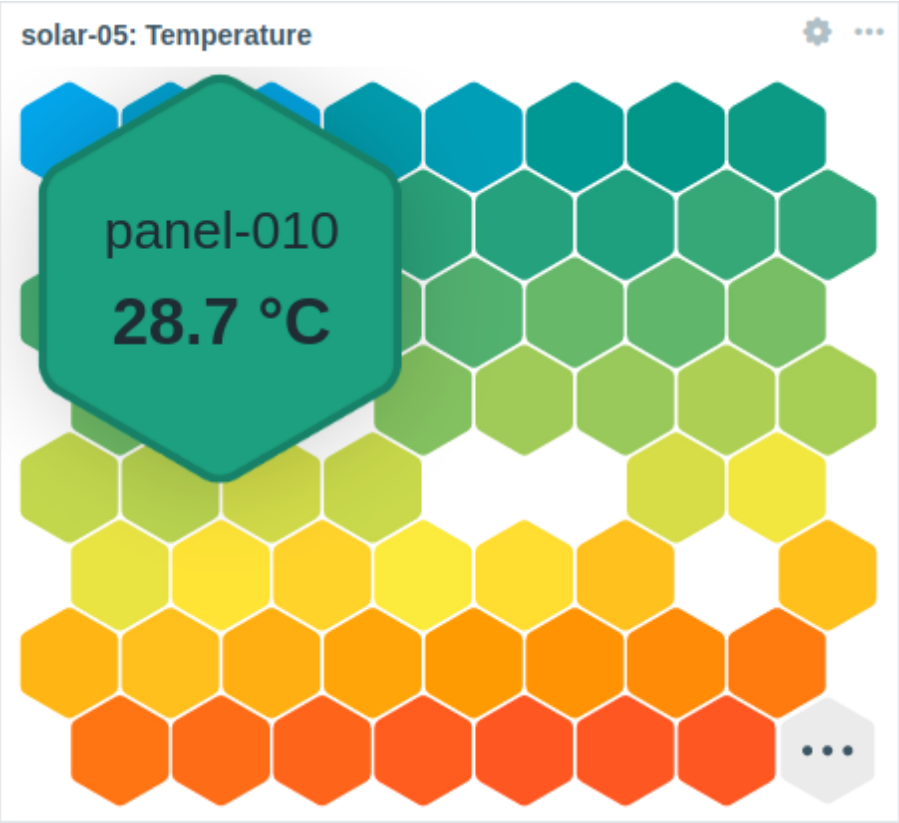
Widżet *Honeycomb* wyświetla hosty lub pozycje jako sześciokątne komórki w siatce. Taki układ ułatwia wykrywanie hostów/pozycji z problemami, identyfikowanie skupisk problemów, porównywanie grup na pierwszy rzut oka i nie tylko.





Liczba wyświetlanych komórek jest ograniczona przez rozmiar widżetu i minimalny rozmiar komórki (32px). Jeśli wszystkie komórki się nie mieszczą, ostatnia komórka wyświetla wielokropek. Rozmiar widżetu można zmieniać, a liczba komórek, ich rozmiar i położenie są dostosowywane dynamicznie.

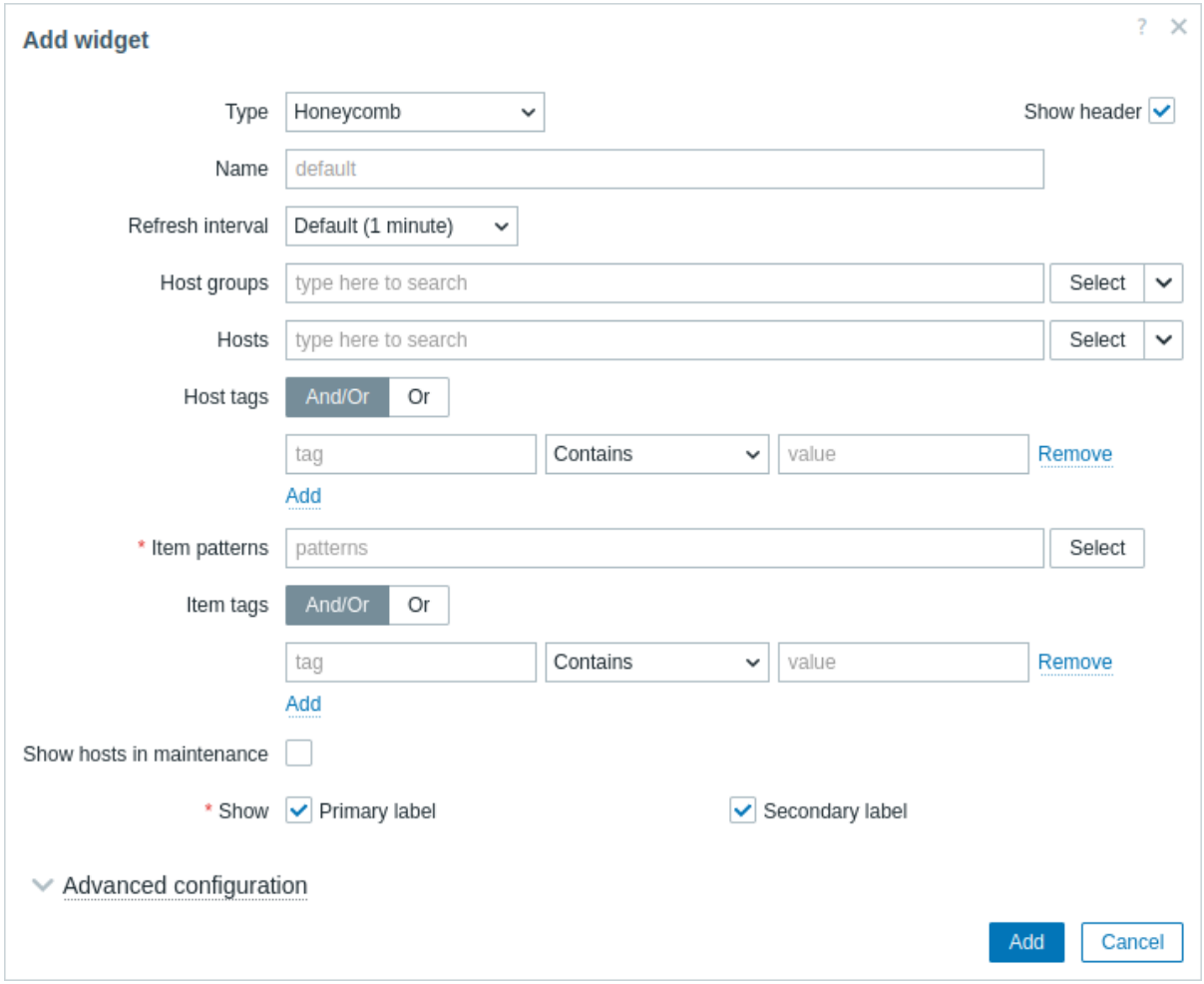
Po najechaniu kursorem wyróżniona komórka powiększa się, aby poprawić widoczność. Kliknięcie komórki powoduje podświetlenie jej obramowania do momentu wybrania innej komórki.



Informacje wyświetlane w widżecie *Honeycomb* można pobrać jako obraz PNG, wybierając opcję *Download image* w menu widżetu.

Konfiguracja

Aby skonfigurować widget, wybierz *Honeycomb* jako typ:



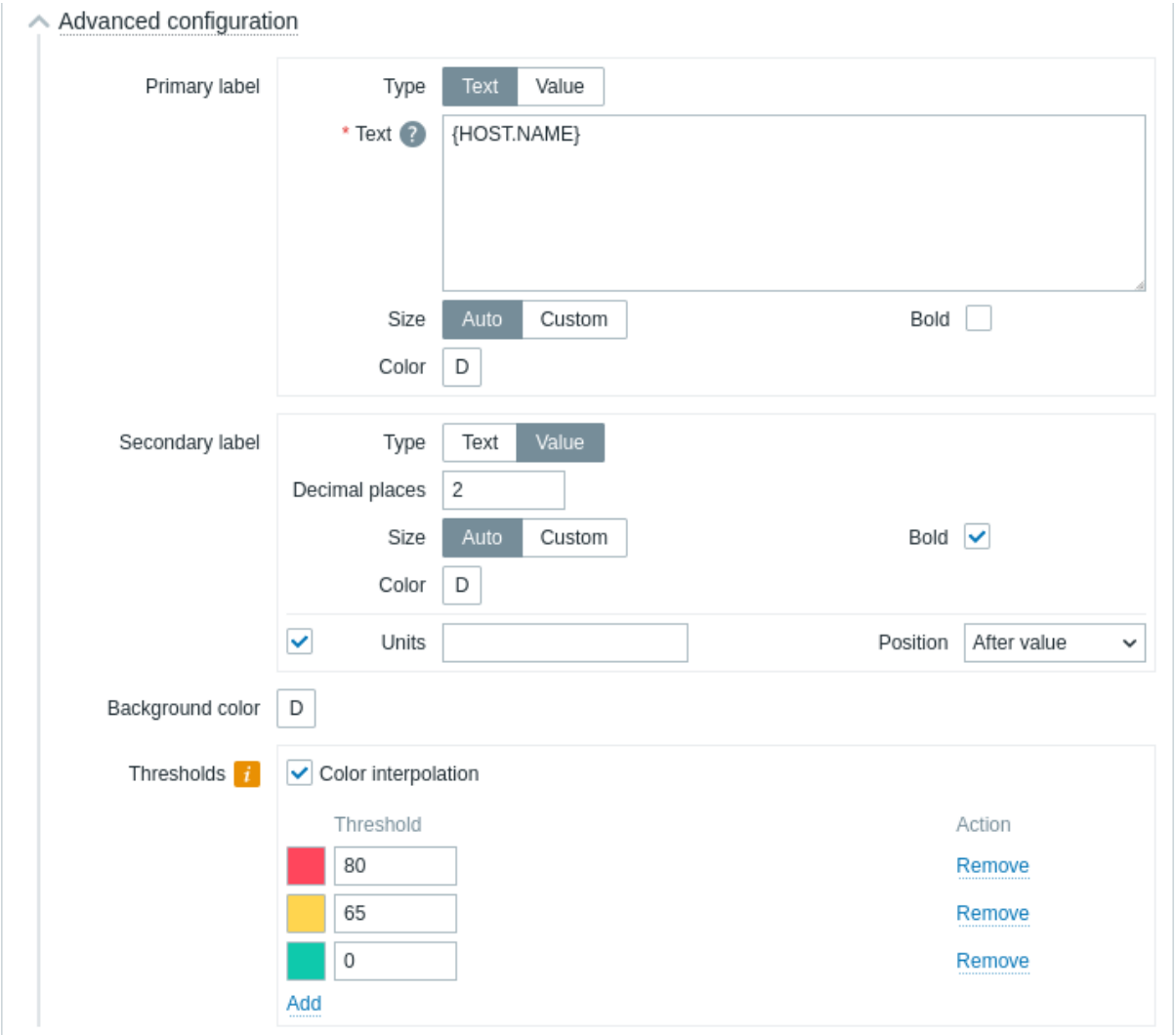
Oprócz parametrów wspólnych dla wszystkich widgetów, można ustawić następujące opcje specyficzne:

Grupy hostów	Wybierz grupy hostów. Alternatywnie wybierz zgodny widget jako źródło danych dla grup hostów. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy grupy zostanie wyświetlona rozwijana lista pasujących grup. Wybranie nadrzędnej grupy hostów powoduje automatyczne wybranie wszystkich zagnieżdżonych grup hostów; jeśli nie wybrano żadnych grup hostów, widget wyświetli wszystkie grupy hostów zawierające hosty z pozycjami pasującymi do wybranego *Wzorca pozycji* (patrz poniżej). Ten parametr nie jest dostępny podczas konfigurowania widgetu na pulpicie szablonu.
Hosty	Wybierz hosty. Alternatywnie wybierz zgodny widget lub pulpit jako źródło danych dla hostów. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy hosta zostanie wyświetlona rozwijana lista pasujących hostów. Jeśli nie wybrano żadnych hostów, widget wyświetli wszystkie hosty z pozycjami pasującymi do wybranego *Wzorca pozycji* (patrz poniżej). Ten parametr nie jest dostępny podczas konfigurowania widgetu na pulpicie szablonu.

Tagi hosta	Określ tagi, aby ograniczyć liczbę hostów wyświetlanych w widżecie. Możliwe jest zarówno uwzględnianie, jak i wykluczanie określonych tagów oraz wartości tagów. Można ustawić kilka warunków. Dopasowanie nazw tagów zawsze uwzględnia wielkość liter. Dla każdego warunku dostępnych jest kilka operatorów: **Exists** - uwzględnij określone nazwy tagów; **Equals** - uwzględnij określone nazwy tagów i wartości (z uwzględnieniem wielkości liter); **Contains** - uwzględnij określone nazwy tagów, których wartości zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter); **Does not exist** - wyklucz określone nazwy tagów; **Does not equal** - wyklucz określone nazwy tagów i wartości (z uwzględnieniem wielkości liter); **Does not contain** - wyklucz określone nazwy tagów, których wartości zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter). Dostępne są dwa typy obliczania warunków: **And/Or** - wszystkie warunki muszą być spełnione, a warunki mające tę samą nazwę tagu będą grupowane operatorem Or; **Or** - wystarczy spełnienie jednego warunku. Ten parametr nie jest dostępny podczas konfigurowania widgetu na pulpicie szablonu.
Wzorce pozycji	Wprowadź wzorce pozycji lub wybierz istniejące pozycje jako wzorce pozycji. Dane pozycji pasujących do wprowadzonych lub wybranych wzorców będą wyświetlane w widoku honeycomb. Parametr *Wzorce pozycji* jest obowiązkowy. Do wyboru można używać wzorców wieloznacznych (na przykład ∗ zwróci pozycje pasujące do zera lub większej liczby znaków; `Zabbix*` zwróci pozycje zaczynające się od „Zabbix”). Aby określić wzorzec wieloznaczny, wprowadź ciąg ręcznie i naciśnij *Enter*. Po rozpoczęciu wpisywania rozwijana lista pokaże pasujące pozycje ograniczone do tych należących do wybranych *Hostów* lub hostów w wybranych *Grupach hostów*, jeśli zostały wskazane. Symbol wieloznaczny jest zawsze interpretowany, dlatego nie można na przykład dodać pojedynczo pozycji o nazwie *item**, jeśli istnieją inne pasujące pozycje (np. item2, item3). Podczas konfigurowania widgetu na pulpicie szablonu ten parametr pozwala wybrać tylko pozycje skonfigurowane w szablonie.
Tagi pozycji	Określ tagi, aby ograniczyć liczbę pozycji wyświetlanych w widżecie. Więcej informacji znajduje się powyżej w sekcji *Tagi hosta*.
Pokaż hosty w konserwacji	Zaznacz to pole wyboru, aby wyświetlać hosty w konserwacji (w takim przypadku obok nazwy hosta będzie wyświetlana ikona konserwacji). Ten parametr ma etykietę *Pokaż dane w konserwacji* podczas konfigurowania widgetu na pulpicie szablonu.
Pokaż	Zaznacz to pole wyboru, aby wyświetlić odpowiedni element komórki honeycomb — etykietę główną, etykietę dodatkową. Musi być wybrany co najmniej jeden element.
Konfiguracja zaawansowana	Kliknij etykietę *Konfiguracja zaawansowana*, aby wyświetlić opcje konfiguracji zaawansowanej.

Konfiguracja zaawansowana

Opcje konfiguracji zaawansowanej są dostępne w zwijanej sekcji *Konfiguracja zaawansowana* i tylko dla elementów wybranych w polu *Pokaż* (zobacz wyżej), a także dla koloru tła lub progów komórek plastra miodu.



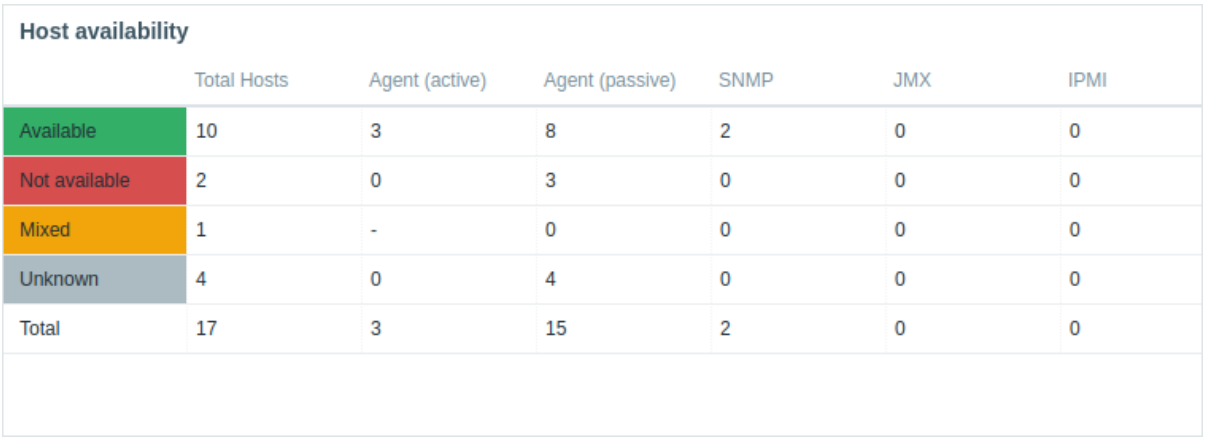
Etykieta podsta-wowa/drugorzędna	
Typ	Wybierz typ etykiety: **Tekst** — etykieta będzie wyświetlać tekst określony w parametrze *Tekst*; **Wartość** — etykieta będzie wyświetlać wartość pozycji z liczbą miejsc po przecinku określoną w parametrze *Miejsca po przecinku*.
Tekst	Wprowadź tekst etykiety. Ten tekst może zastąpić domyślną nazwę pozycji. Obsługiwany jest tekst wielowierszowy. Możliwe jest połączenie tekstu i obsługiwanych makr. Obsługiwane są {HOST.*}, {ITEM.*}, {INVENTORY.*} oraz makra użytkownika. Komórki plastra miodu są porządkowane alfabetycznie według nazwy hosta, a w obrębie każdego hosta — według nazwy pozycji. Ten parametr jest dostępny, jeśli *Typ* jest ustawiony na „Tekst”.
Miejsca po przecinku	Wprowadź liczbę miejsc po przecinku wyświetlanych wraz z wartością. Ten parametr jest dostępny, jeśli *Typ* jest ustawiony na „Wartość”, i ma wpływ tylko na pozycje zwracające dane numeryczne (float).
Rozmiar	Wybierz rozmiar etykiety: **Auto** — użyj automatycznie dopasowanego rozmiaru etykiety; **Niestandardowy** — wprowadź niestandardowy rozmiar etykiety (w procentach, względem rozmiaru komórki plastra miodu). Zwróć uwagę, że etykiety, które nie mieszczą się w rozmiarze komórki plastra miodu, są obcinane.
Pogrubienie	Zaznacz pole wyboru, aby wyświetlać jednostki pozycji pogrubioną czcionką.
Kolor	Wybierz kolor jednostek pozycji z próbnika kolorów. „D” oznacza kolor domyślny, który zależy od motywu frontend. Aby powrócić do koloru domyślnego, kliknij przycisk *Użyj domyślnego* w próbniku kolorów.
Jednostki	
Jednostki	Zaznacz pole wyboru, aby wyświetlać jednostki wraz z wartością pozycji. Jeśli wprowadzisz nazwę jednostki, zastąpi ona jednostki ustawione w konfiguracji pozycji. Ten parametr jest dostępny, jeśli *Typ* jest ustawiony na „Tekst”.

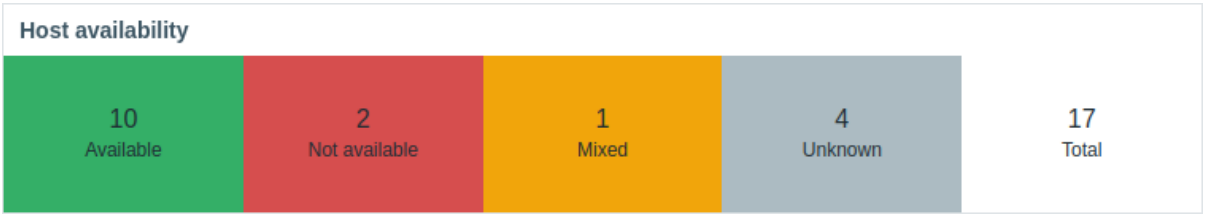
Pozycja	Wybierz położenie jednostek pozycji (przed lub po wartości pozycji). Ten parametr jest ignorowany dla następujących jednostek związanych z czasem: unixtime, uptime, s. Ten parametr jest dostępny, jeśli *Typ* jest ustawiony na „Tekst”.
Kolor tła	
Kolor tła	Wybierz kolor tła komórek plastra miodu z próbnika kolorów. „D” oznacza kolor domyślny, który zależy od motywu frontend. Aby powrócić do koloru domyślnego, kliknij przycisk *Użyj domyślnego* w próbniku kolorów.
Progi	
Interpolacja kolorów	Zaznacz pole wyboru, aby włączyć płynne przejścia między kolorami progów dla komórek plastra miodu. Ten parametr jest dostępny, jeśli ustawiono co najmniej dwa progi.
Próg	Kliknij *Dodaj*, aby dodać próg, wybierz kolor progu z próbnika kolorów i określ wartość liczbową. Lista progów zostanie posortowana rosnąco podczas zapisywania. Zwróć uwagę, że kolory skonfigurowane jako progi będą wyświetlane poprawnie tylko dla pozycji numerycznych. Obsługiwane są sufiksy (na przykład „1d”, „2w”, „4K”, „8G”). Obsługiwane są mapowania wartości.

12 Dostępność hosta

Przegląd

Widżet *Dostępność hostów* wyświetla dostępność hostów w wybranych grupach hostów, umożliwiając monitorowanie liczby hostów, które są dostępne lub niedostępne.



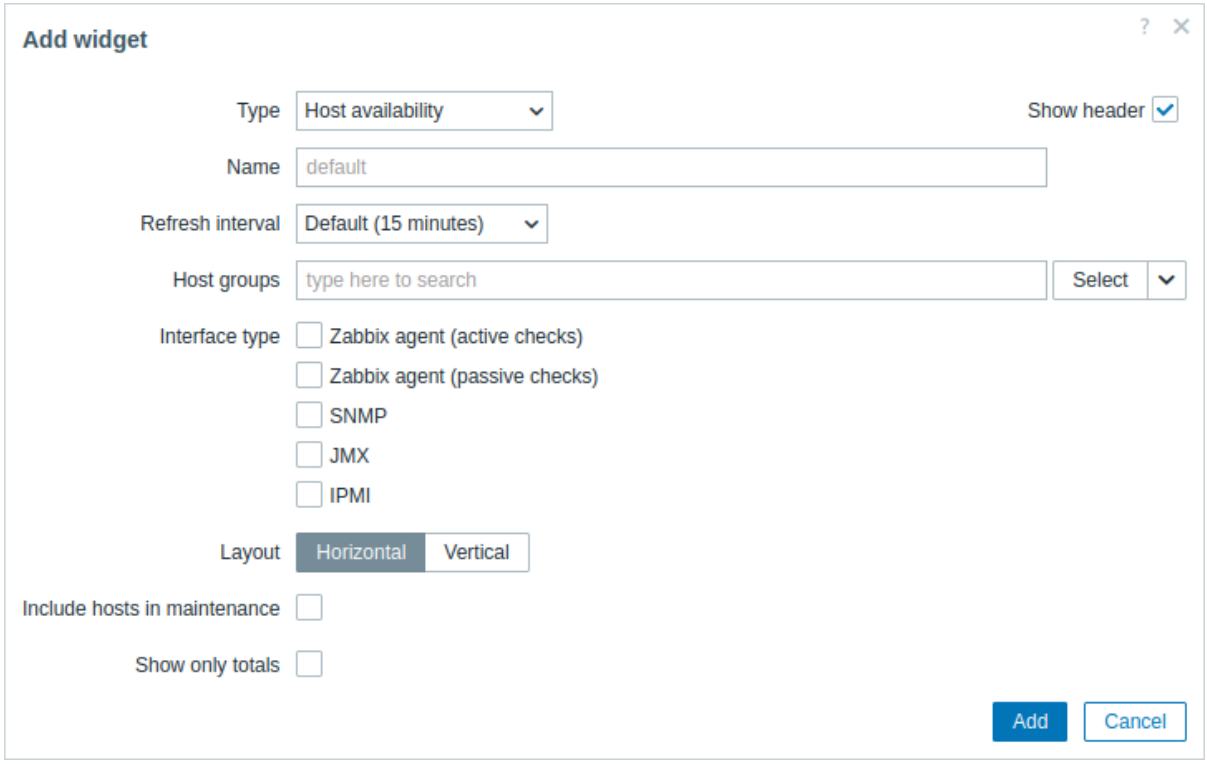


Dostępność hostów jest liczona w następujący sposób:

- *Dostępne* - hosty ze wszystkimi interfejsami dostępnymi
- *Niedostępne* - hosty ze wszystkimi interfejsami niedostępnymi
- *Mieszane* - hosty z co najmniej jednym interfejsem niedostępnym oraz co najmniej jednym dostępnym lub o nieznanym stanie
- *Nieznane* - hosty z co najmniej jednym interfejsem o nieznanym stanie, ale bez żadnego niedostępnego
- *Łącznie* - łączna liczba wszystkich hostów

Konfiguracja

Aby skonfigurować, wybierz *Dostępność hosta* jako typ:



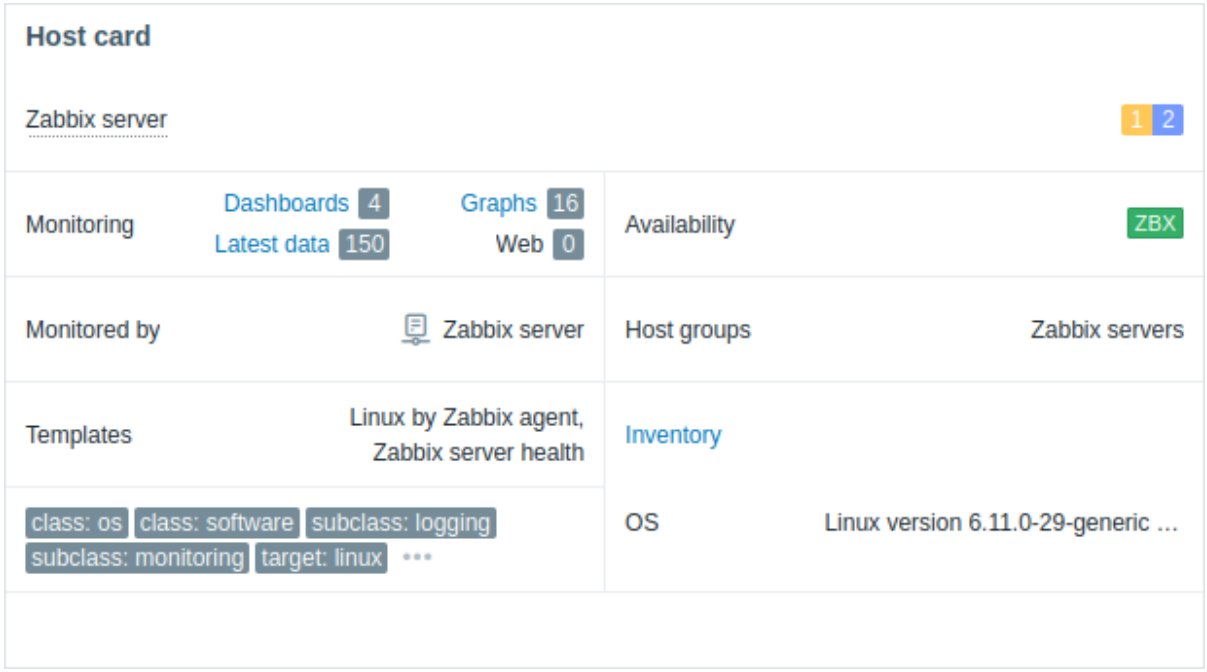
Oprócz parametrów wspólnych dla wszystkich widgetów, możesz ustawić następujące opcje specyficzne:

Grupy hostów	Wybierz grupy hostów. Alternatywnie wybierz zgodny widget jako źródło danych dla grup hostów. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy grupy zostanie wyświetlona rozwijana lista pasujących grup. Ten parametr nie jest dostępny podczas konfigurowania widgetu na pulpicie szablonu.
Typ interfejsu	Wybierz, dla których interfejsów hosta chcesz wyświetlić dane dostępności — *agent Zabbix (sprawdzenia aktywne)*, *agent Zabbix (sprawdzenia pasywne)*, *SNMP*, *JMX*, *IPMI*. W przypadku *agenta Zabbix (sprawdzenia aktywne)* komórka *Mieszane* będzie zawsze pusta, ponieważ pozycje tego typu nie mogą mieć wielu interfejsów. Jeśli nic nie zostanie wybrane, domyślnie wyświetlana jest dostępność wszystkich interfejsów.
Układ	Wybierz wyświetlanie poziome (kolumny) lub pionowe (wiersze).
Uwzględnij hosty w konserwacji	Uwzględnij w statystykach hosty będące w konserwacji. Ten parametr ma etykietę *Pokaż dane w konserwacji* podczas konfigurowania widgetu na pulpicie szablonu.
Pokaż tylko sumy	Jeśli zaznaczone, wyświetlana jest łączna liczba hostów bez podziału na interfejsy. Ta opcja jest wyłączona, jeśli wybrano tylko jeden interfejs.

13 Karta hosta

Przegląd

Widżet *Karta hosta* wyświetla szczegóły pojedynczego hosta, umożliwiając szybkie ocenienie stanu i konfiguracji hosta (dostępność, problemy, inwentarz itp.).

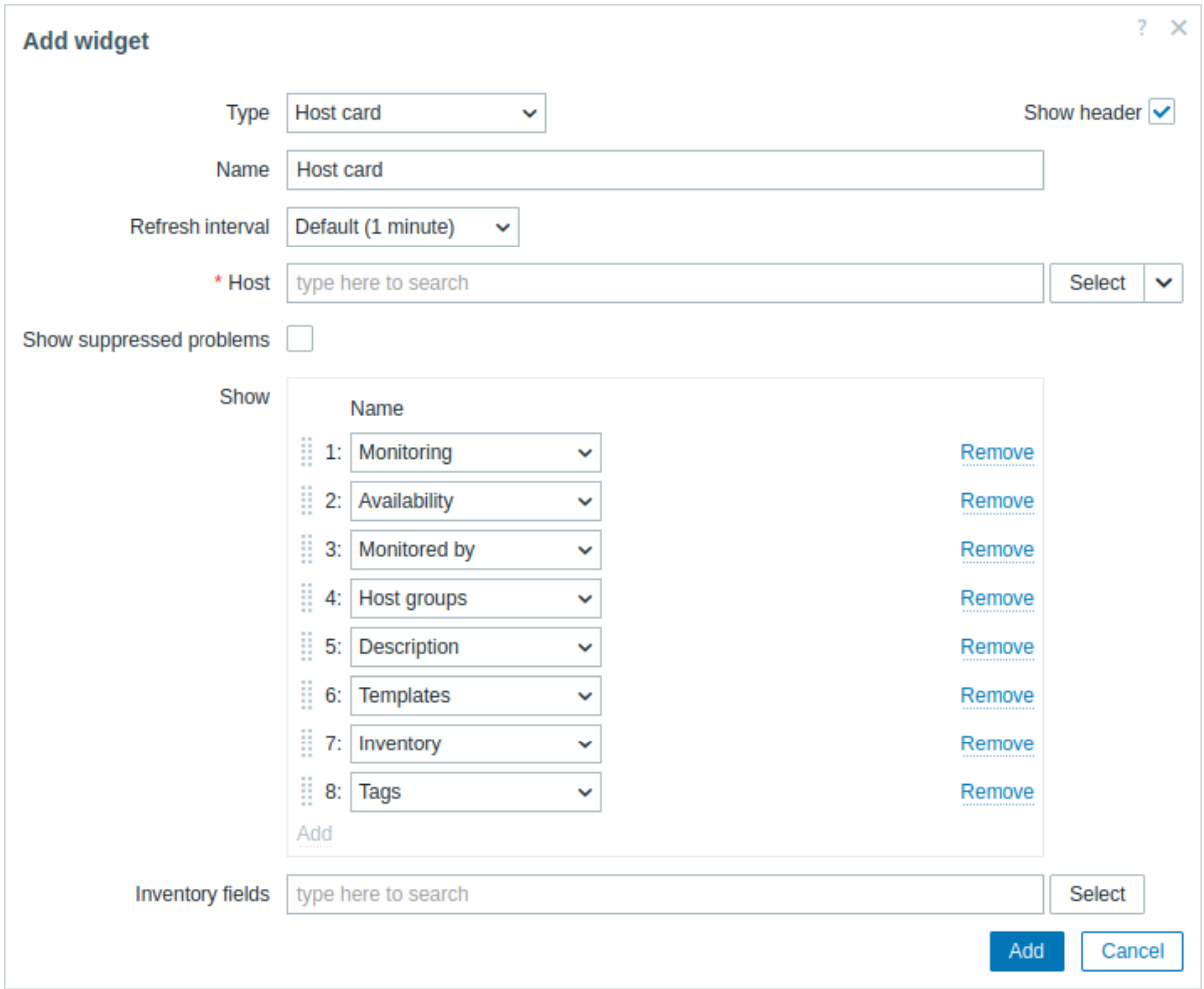


Host może zostać ustawiony bezpośrednio w konfiguracji widżetu lub wybrany z kompatybilnego widżetu albo za pomocą selektora hosta na pulpicie.

Widżet może wyświetlać wiele sekcji, z których każda pokazuje inne informacje. Układ sekcji jest dostosowywany automatycznie na podstawie szerokości widżetu; po rozszerzeniu w poziomie sekcje są automatycznie rozmieszczane w wielu kolumnach.

Konfiguracja

Aby skonfigurować, wybierz *Host card* jako typ:



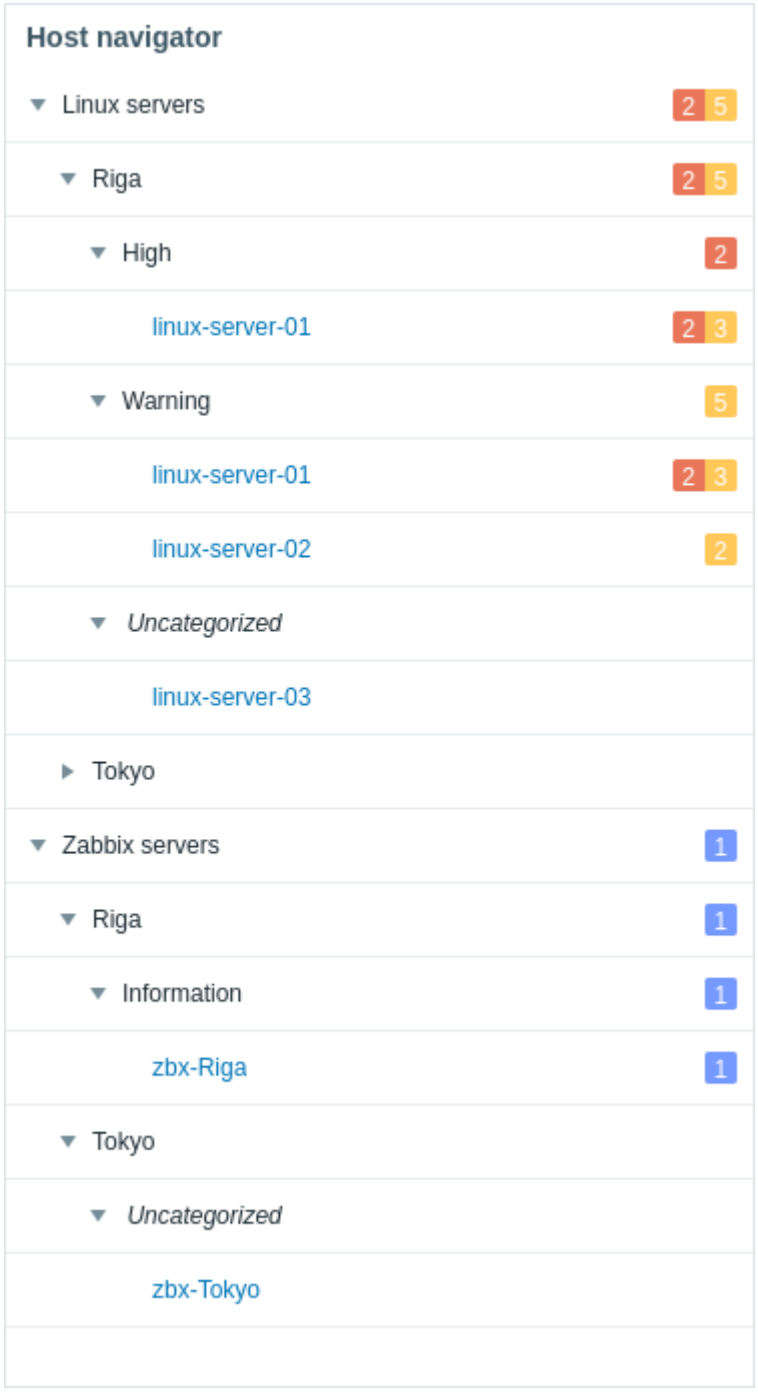
Oprócz parametrów wspólnych dla wszystkich widżetów możesz ustawić następujące parametry specyficzne:

Host	Wybierz host. Alternatywnie wybierz zgodny widżet lub pulpit jako źródło danych dla hostów. Podczas wpisywania będą wyświetlane pasujące podpowiedzi. Górna sekcja widżetu zawsze wyświetla **nazwę hosta** (kliknięcie otwiera menu hosta): - Jeśli host jest wyłączony, obok nazwy hosta wyświetlana jest czerwona etykieta *Disabled*. - Jeśli host jest w trybie konserwacji, obok nazwy hosta wyświetlana jest ikona konserwacji. Górna sekcja widżetu wyświetla również liczbę **problemów hosta** pogrupowanych według ważności (kliknięcie otwiera problemy hosta). Ten parametr nie jest dostępny podczas konfigurowania widżetu na pulpicie szablonu.
Show suppressed problems	Zaznacz to pole wyboru, aby uwzględnić ukryte problemy w obliczaniu problemów.
Show	Dodaj sekcje do wyświetlenia w widżecie. Sekcje można przestawiać metodą przeciągnij i upuść.
Host groups	Wyświetla grupy hostów, do których należy host.
Description	Wyświetla opis hosta.
Monitoring	Wyświetla szybkie odnośniki do przechodzenia do Pulpitów, Najnowszych danych, Wykresów i Scenariuszy WWW hosta. Liczba obok każdego odnośnika wskazuje liczbę odpowiednich encji.
Availability	Wyświetla dostępność hosta według interfejsu.
Monitored by	Wyświetla, czy host jest monitorowany przez serwer Zabbix, czy przez określony proxy lub grupę proxy.
Templates	Wyświetla szablony podłączone do hosta.
Inventory	Wyświetla pola inwentarza hosta.
Tags	Wyświetla tagi hosta.
Inventory fields	Wybierz pola inwentarza do wyświetlenia. Podczas wpisywania będą wyświetlane pasujące podpowiedzi. Jeśli nie określono żadnych pól inwentarza, zostaną wyświetlone wszystkie wypełnione pola inwentarza. Ten parametr jest dostępny, jeśli *Show* zawiera *Inventory*.

14 Nawigator hostów

Przegląd

Widżet *Host navigator* wyświetla listę hostów na podstawie różnych opcji filtrowania i grupowania.



Grupy, według których hosty są uporządkowane, można rozwijać lub zwijać.

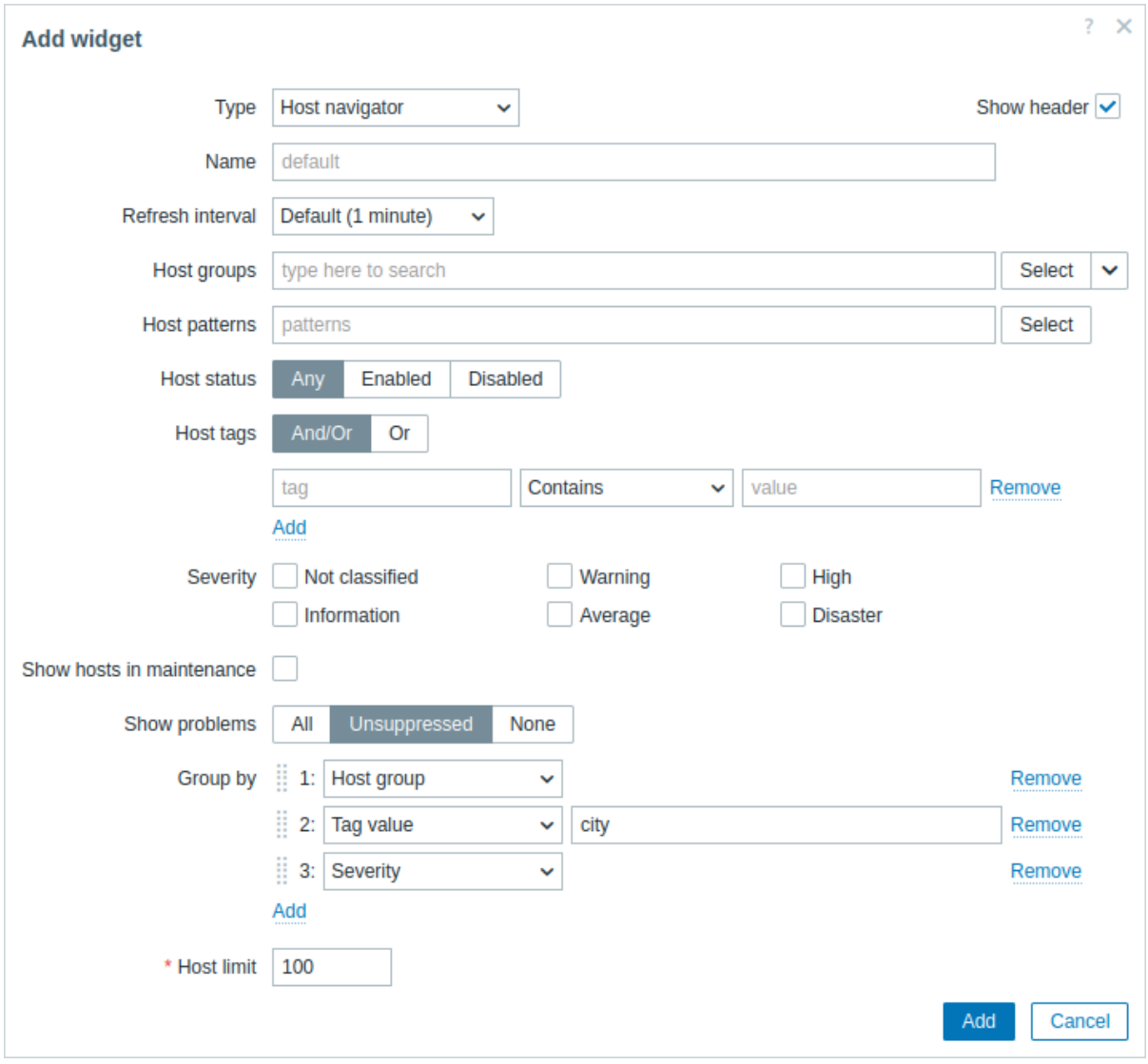
W przypadku grup, problemów oraz hostów w trybie konserwacji dodatkowe szczegóły są dostępne po najechaniu kursorem.

Widżet jest najbardziej przydatny do sterowania tym, co wyświetlają inne widżety, na podstawie wybranego hosta.



Konfiguracja

Aby skonfigurować, wybierz *Host navigator* jako typ:



Oprócz parametrów wspólnych dla wszystkich widżetów, możesz ustawić następujące opcje specyficzne:

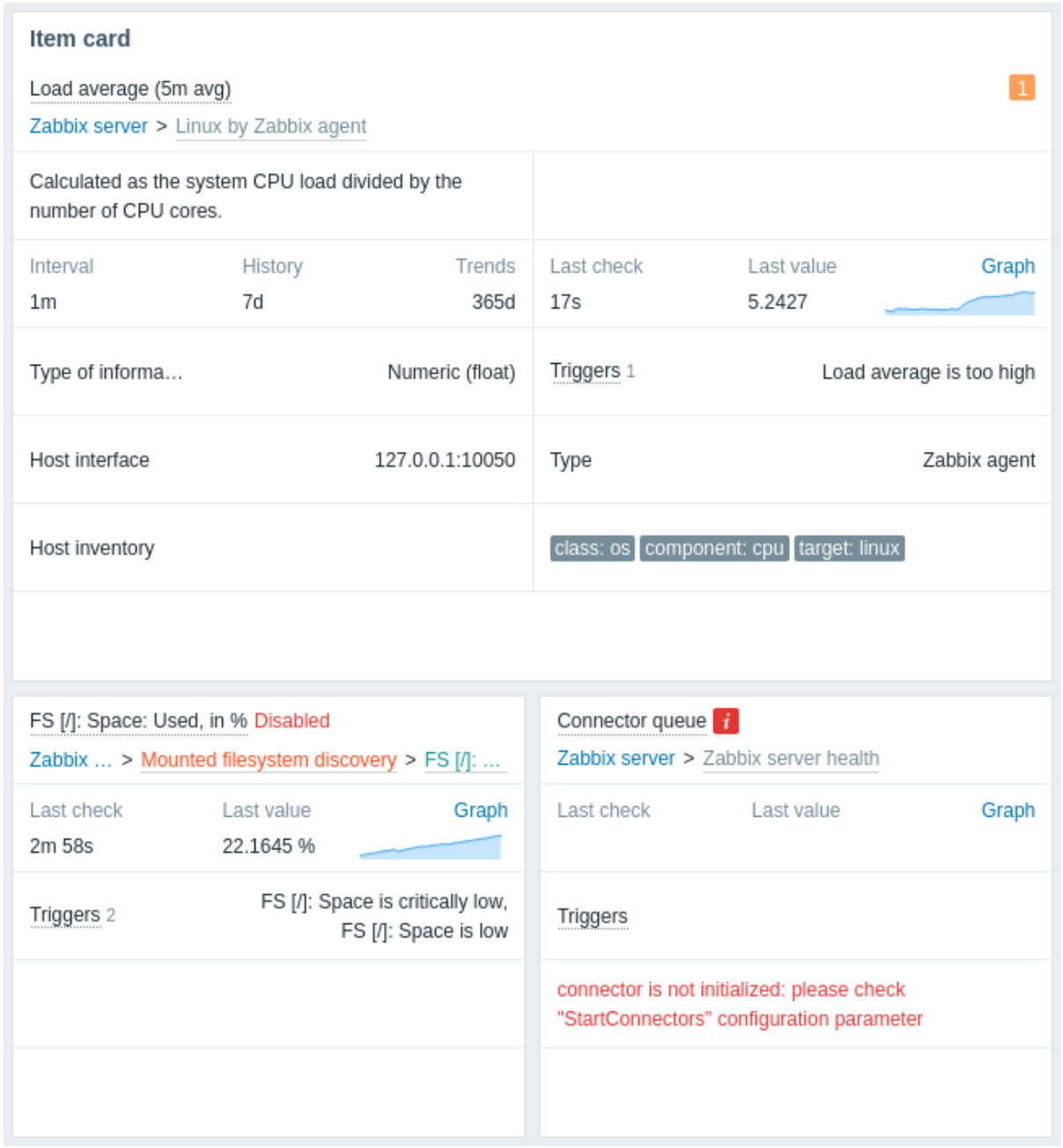
Host groups	Wybierz grupy hostów. Alternatywnie wybierz zgodny widżet jako źródło danych dla grup hostów. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy grupy zostanie wyświetlona rozwijana lista pasujących grup. Wybranie nadrzędnej grupy hostów domyślnie wybiera wszystkie zagnieżdżone grupy hostów; jeśli nie wybrano żadnych grup hostów, widżet wyświetli wszystkie hosty ze wszystkich grup hostów. Ten parametr nie jest dostępny podczas konfigurowania widżetu na pulpicie szablonu.
Host patterns	Wprowadź wzorce hostów lub wybierz istniejące hosty jako wzorce hostów. Hosty pasujące do określonych wzorców będą wyświetlane w nawigatorze hostów. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy hosta zostanie wyświetlona rozwijana lista pasujących hostów. Jeśli nie wybrano żadnych hostów, widżet wyświetli wszystkie hosty. Do wyboru można używać wzorców wieloznacznych (na przykład ∗ zwróci hosty pasujące do zera lub większej liczby znaków; `Zabbix∗` zwróci hosty, których nazwa zaczyna się od „Zabbix”). Aby określić wzorzec wieloznaczny, wprowadź ciąg ręcznie i naciśnij *Enter*. Po rozpoczęciu wpisywania rozwijana lista pokaże pasujące hosty ograniczone do tych należących do hostów w wybranych *Host groups*, jeśli takie wybrano. Ten parametr nie jest dostępny podczas konfigurowania widżetu na pulpicie szablonu.
Host status	Filtruj, które hosty mają być wyświetlane na podstawie ich stanu (dowolny, włączony, wyłączony). Ten parametr nie jest dostępny podczas konfigurowania widżetu na pulpicie szablonu.
Host tags	Określ tagi do filtrowania hostów wyświetlanych w widżecie. Możliwe jest zarówno uwzględnianie, jak i wykluczanie określonych tagów oraz wartości tagów. Można ustawić kilka warunków. Dopasowanie nazw tagów zawsze uwzględnia wielkość liter. Dla każdego warunku dostępnych jest kilka operatorów: **Exists** - uwzględnij określone nazwy tagów; **Equals** - uwzględnij określone nazwy tagów i wartości (z uwzględnieniem wielkości liter); **Contains** - uwzględnij określone nazwy tagów, których wartości zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter); **Does not exist** - wyklucz określone nazwy tagów; **Does not equal** - wyklucz określone nazwy tagów i wartości (z uwzględnieniem wielkości liter); **Does not contain** - wyklucz określone nazwy tagów, których wartości zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter). Dla warunków dostępne są dwa typy obliczeń: **And/Or** - wszystkie warunki muszą być spełnione, a warunki mające tę samą nazwę tagu będą grupowane operatorem Or; **Or** - wystarczy spełnienie jednego warunku. Ten parametr nie jest dostępny podczas konfigurowania widżetu na pulpicie szablonu.
Severity	Zaznacz poziomy ważności problemów, aby filtrować hosty z problemami wyświetlane w widżecie. Jeśli nie zaznaczono żadnych poziomów ważności, zostaną wyświetlone wszystkie hosty ze wszystkimi problemami.
Show hosts in maintenance	Zaznacz to pole wyboru, aby wyświetlać hosty w konserwacji (w takim przypadku obok nazwy hosta zostanie pokazana ikona konserwacji). Ten parametr ma etykietę *Show data in maintenance* podczas konfigurowania widżetu na pulpicie szablonu.
Show problems	

Group by	Dodaj atrybut grupowania, według którego wybrane hosty będą grupowane: **Host group** - grupuj hosty według ich grupy hostów; **Tag value** - wprowadź nazwę tagu, aby grupować hosty według wartości tego tagu (na przykład wpisz „city”, aby grupować hosty według wartości „Riga”, „Tokyo” itd.); **Severity** - grupuj hosty według poziomów ważności ich problemów. Jeśli parametr *Show problems* jest skonfigurowany do wyświetlania problemów, będą one wyświetlane następująco: - dla każdej grupy ważności wyświetlana jest tylko odpowiadająca jej liczba problemów; - dla każdego hosta wyświetlane są wszystkie liczby jego problemów. Zwróć uwagę, że hosty będą grupowane tylko według tych poziomów ważności, które zaznaczono w parametrze *Severity*; jeśli nie zaznaczono żadnych poziomów ważności, wszystkie hosty będą grupowane według wszystkich poziomów ważności. Atrybuty grupowania można zmieniać kolejnością, przeciągając je w górę lub w dół za uchwyt przed nazwą grupy. Zwróć uwagę, że kolejność atrybutów grupowania określa kolejność zagnieżdżania grup. Na przykład określenie wielu nazw tagów (1: color, 2: city) spowoduje, że hosty będą grupowane według koloru (red, blue itd.), a następnie według miasta (Riga, Tokyo itd.). Host może być wyświetlany w wielu grupach w zależności od skonfigurowanych atrybutów grupowania (na przykład podczas grupowania według grupy hostów, gdy host należy do wielu grup hostów). Kliknięcie takiego hosta wybiera go i podświetla we wszystkich grupach. Hosty, które nie pasują do skonfigurowanych atrybutów grupowania, są wyświetlane w grupie *Uncategorized*. Można określić maksymalnie 10 atrybutów grupowania i wszystkie muszą być unikalne. Jeśli nie określono żadnych atrybutów grupowania, hosty nie będą grupowane.
Host limit	Wprowadź maksymalną liczbę hostów do wyświetlenia. Możliwe wartości mieszczą się w zakresie 1-9999. Gdy do wyświetlenia dostępnych jest więcej hostów niż ustawiony limit, poniżej wyświetlonych hostów pokazywany jest odpowiedni komunikat (na przykład „100 of 100+ hosts are shown”). Zwróć uwagę, że skonfigurowany limit hostów wpływa również na wyświetlanie skonfigurowanych grup; na przykład jeśli limit hostów jest ustawiony na 100, a hosty są grupowane według wartości tagów (ponad 200), w widżecie zostanie wyświetlonych tylko pierwszych 100 wartości tagów wraz z odpowiadającymi im hostami. Na ten parametr nie wpływa parametr *Limit for search and filter results* w *Administration* → *General* → *GUI*. Ten parametr nie jest dostępny podczas konfigurowania widżetu na pulpicie szablonu.

15 Karta pozycji

Przegląd

Widżet *Karta pozycji* wyświetla szczegóły pojedynczej pozycji, umożliwiając szybkie sprawdzenie stanu i konfiguracji pozycji (najnowsze dane, błędy, opis itp.).

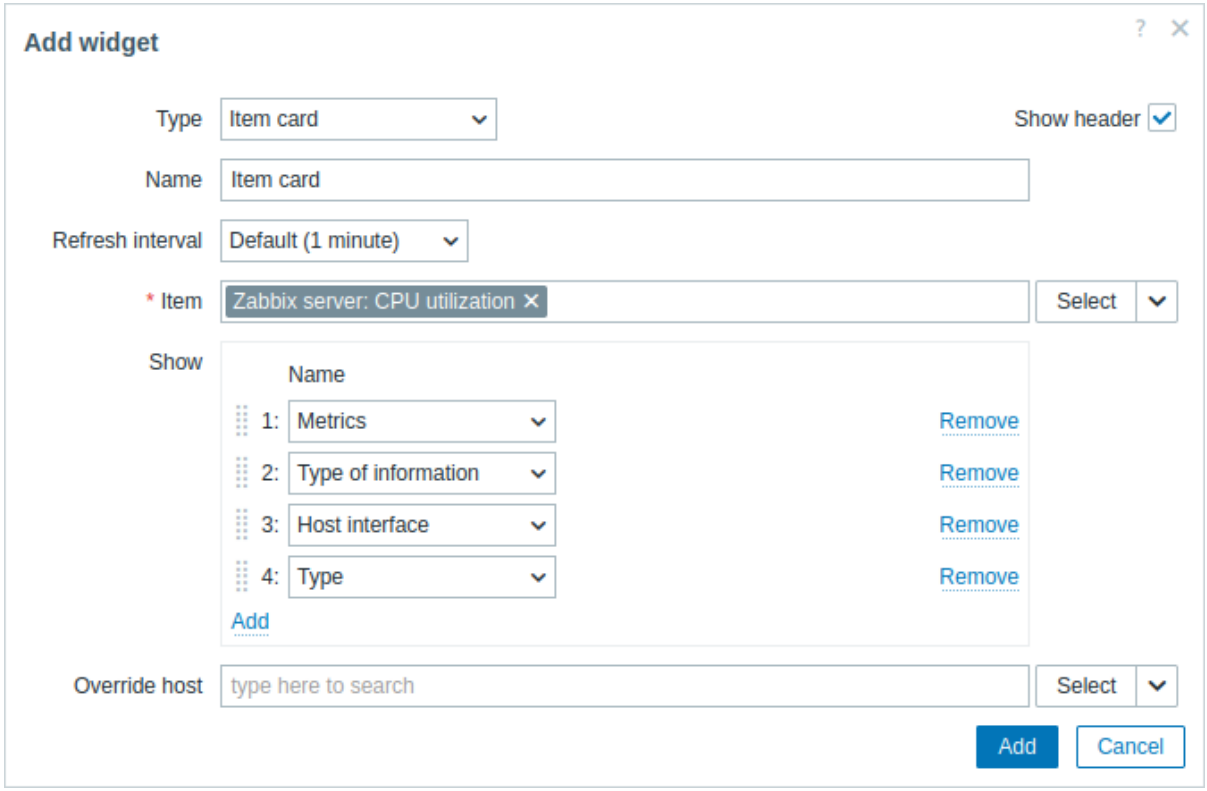


Pozycja może zostać ustawiona bezpośrednio w konfiguracji widżetu lub wybrana z kompatybilnego widżetu na pulpicie.

Widżet może wyświetlać wiele sekcji, z których każda pokazuje inne informacje. Układ sekcji jest dostosowywany automatycznie w zależności od szerokości widżetu; po rozszerzeniu w poziomie sekcje są automatycznie rozmieszczane w wielu kolumnach.

Konfiguracja

Aby skonfigurować widget, wybierz *Item card* jako typ:



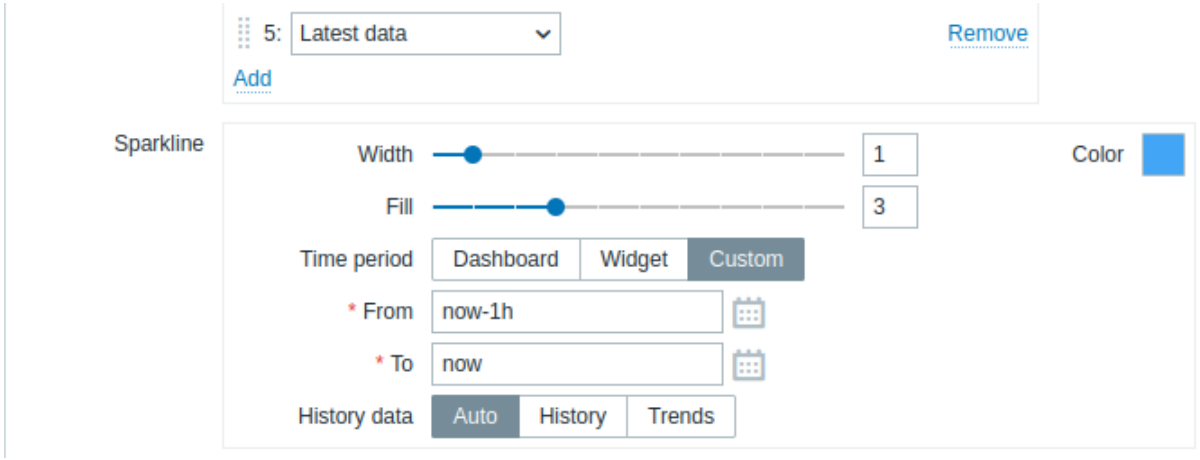
Oprócz parametrów wspólnych dla wszystkich widgetów możesz ustawić następujące opcje specyficzne:

Item	Wybierz pozycję. Alternatywnie wybierz zgodny widget jako źródło danych dla pozycji. Podczas wpisywania wyświetlane są pasujące podpowiedzi. Górna sekcja widgetu zawsze wyświetla **nazwę pozycji** (kliknięcie otwiera menu pozycji): - Jeśli pozycja jest wyłączona, obok nazwy pozycji wyświetlana jest czerwona etykieta *Disabled*. - W przypadku błędów wyświetlana jest kwadratowa ikona z literą „i”. W przypadku problemów dla każdego poziomu ważności problemu wyświetlana jest kwadratowa ikona z liczbą problemów. Najechanie kursorem na ikonę otwiera wyskakujące okno ze szczegółami. - Na pulpicie szablonu wyświetlana jest techniczna nazwa pozycji (zamiast nazwy widocznej). Górna sekcja widgetu wyświetla również **ścieżkę pozycji** — jej host oraz, jeśli dotyczy, szablon, regułę wykrywania niskopoziomowego (LLD) lub pozycję nadrzędną (kliknięcie encji otwiera jej konfigurację). Ścieżka pozycji jest wyświetlana tylko użytkownikom mającym uprawnienia do odpowiednich encji.
Show	Dodaj sekcje do wyświetlenia w widżecie. Sekcje można przestawiać metodą przeciągnij i upuść.
Description	Wyświetla opis pozycji. Makra są rozwijane.
Error text	Wyświetla błąd pozycji (jeśli występuje).
Metrics	Wyświetla następujące informacje: - Interwał aktualizacji pozycji (z wyjątkiem pozycji trapper); - Konfigurację historii pozycji (jeśli istnieje); - Konfigurację trendów pozycji (jeśli istnieje). Makra są rozwijane. Jeśli pozycja używa niestandardowych interwałów, obok interwału aktualizacji pozycji wyświetlana jest ikona pomocy. Najechanie kursorem na ikonę otwiera wyskakujące okno ze szczegółami niestandardowego interwału.

Latest data	Wyświetla następujące informacje: - Czas od ostatniego sprawdzenia pozycji; - Ostatnią wartość pozycji; - Łącze do prostego wykresu/historii wartości pozycji (jeśli historia lub trendy są przechowywane); - Konfigurowalny wykres sparkline (jeśli pozycja jest numeryczna). Dla pozycji typu binarnego zamiast ostatniej wartości wyświetlana jest miniatura lub opcja *Show*. Najechanie kursorem na miniaturę otwiera wyskakujące okno z obrazem. Najechanie kursorem na *Show* otwiera wyskakujące okno z wartością pozycji (ciąg Base64). Na pulpicie szablonu zamiast ostatniej wartości pozycji wyświetlane jest *No data*.
Type of information	Wyświetla typ informacji pozycji.
Triggers	Wyświetla następujące informacje: - Etykietę *Triggers* z liczbą wyzwalaczy (najechanie kursorem na *Triggers* otwiera wyskakujące okno ze szczegółami wyzwalaczy); - Listę nazw wyzwalaczy (makra są rozwijane).
Host interface	Wyświetla interfejs hosta używany przez pozycję albo *No data*, jeśli pozycja nie ma interfejsu hosta (np. pozycje zależne, proste testy). Na pulpicie szablonu wyświetlane jest *No data*.
Type	Wyświetla typ pozycji.
Host inventory	Wyświetla pole inwentarza hosta, które jest wypełniane wartością pozycji.
Tags	Wyświetla tagi pozycji.
Override host	Wybierz zgodny widget lub selektor hosta pulpitu jako źródło danych dla hostów. Ten parametr nie jest dostępny podczas konfigurowania widgetu na pulpicie szablonu.

Wykres sparkline

Opcje konfiguracji wykresu sparkline są dostępne tylko wtedy, gdy sekcja *Najnowsze dane* została dodana do widgetu.



Szerokość	Ustaw grubość linii wykresu za pomocą suwaka lub ręcznie, wprowadzając wartość z zakresu od 0 do 10.
Kolor	Wybierz kolor linii i wypełnienia.
Wypełnienie	Ustaw poziom przezroczystości koloru wypełnienia za pomocą suwaka lub ręcznie, wprowadzając wartość z zakresu od 0 do 10.
Okres czasu	Wybierz źródło danych dla okresu czasu: **Pulpit** - użyj selektora okresu czasu pulpitu; **Widget** - użyj zgodnego widgetu (ustawionego w parametrze *Widget*); **Niestandardowy** - użyj niestandardowego okresu czasu ustawionego w parametrach *Od* i *Do*; jeśli jest ustawiony, w prawym górnym rogu widgetu będzie wyświetlana ikona zegara, wskazująca ustawiony czas po najechaniu kursorem. Zwróć uwagę, że niezależnie od konfiguracji *Okresu czasu* widgetu, zgodne widgety nadal mogą używać go jako źródła danych dla okresu czasu.
Widget	Wprowadź lub wybierz zgodny widget jako źródło danych dla okresu czasu. Ten parametr jest dostępny, jeśli *Okres czasu* jest ustawiony na „Widget”.

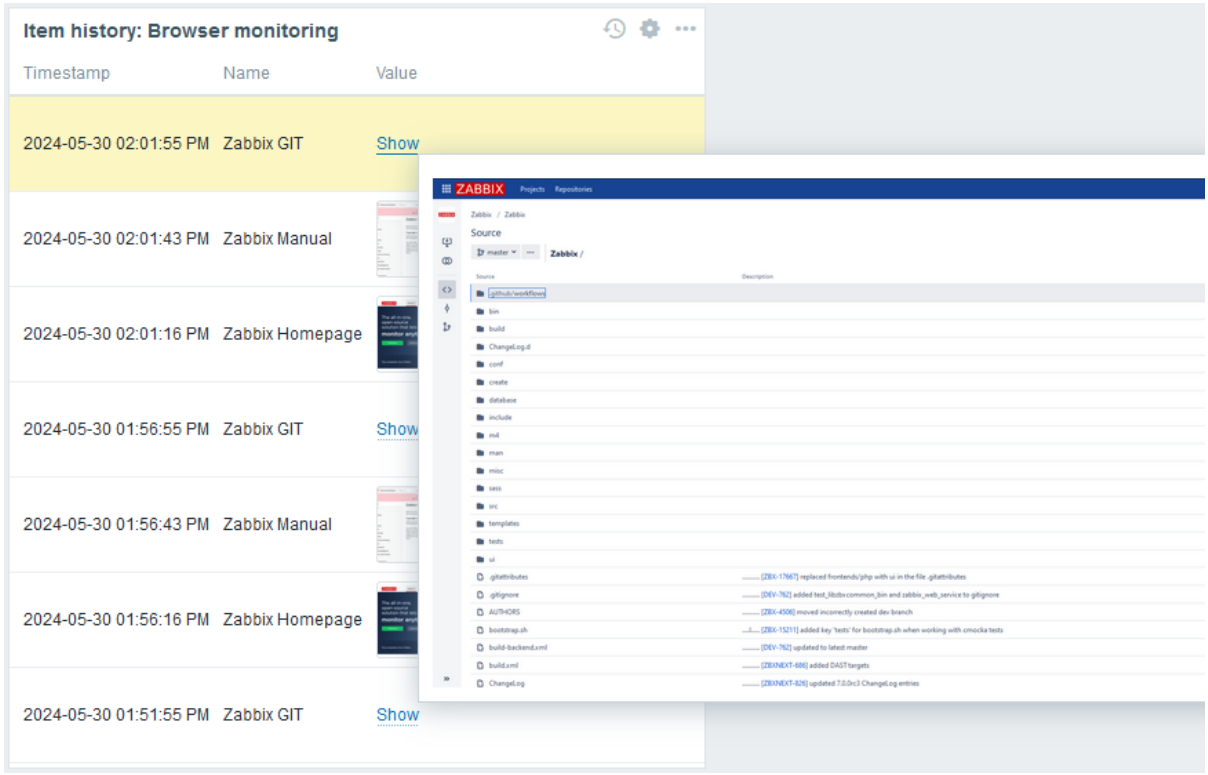
Od	Wprowadź lub wybierz początek okresu czasu. Obsługiwana jest składnia czasu względnego (`now`, `now/d`, `now/w-1w` itd.). Ten parametr jest dostępny, jeśli *Okres czasu* jest ustawiony na „Niestandardowy”.
Do	Wprowadź lub wybierz koniec okresu czasu. Obsługiwana jest składnia czasu względnego (`now`, `now/d`, `now/w-1w` itd.). Ten parametr jest dostępny, jeśli *Okres czasu* jest ustawiony na „Niestandardowy”.
Dane historyczne	Pobierz dane z historii lub trendów: **Auto** - wybór automatyczny; **Historia** - pobierz dane historyczne; **Trendy** - pobierz dane trendów. Ten parametr ma zastosowanie tylko do danych numerycznych. Dane nienumeryczne będą zawsze pobierane z historii.

16 Historia pozycji

Przegląd

Widżet *Historia pozycji* wyświetla najnowsze dane dla wszystkich typów pozycji (numerycznych, tekstowych itp.) w formacie tabeli. Może wyświetlać paski postępu i obrazy (przydatne w przypadku pozycji przeglądarki) oraz wyróżniać wartości (przydatne w przypadku monitorowania plików dziennika).

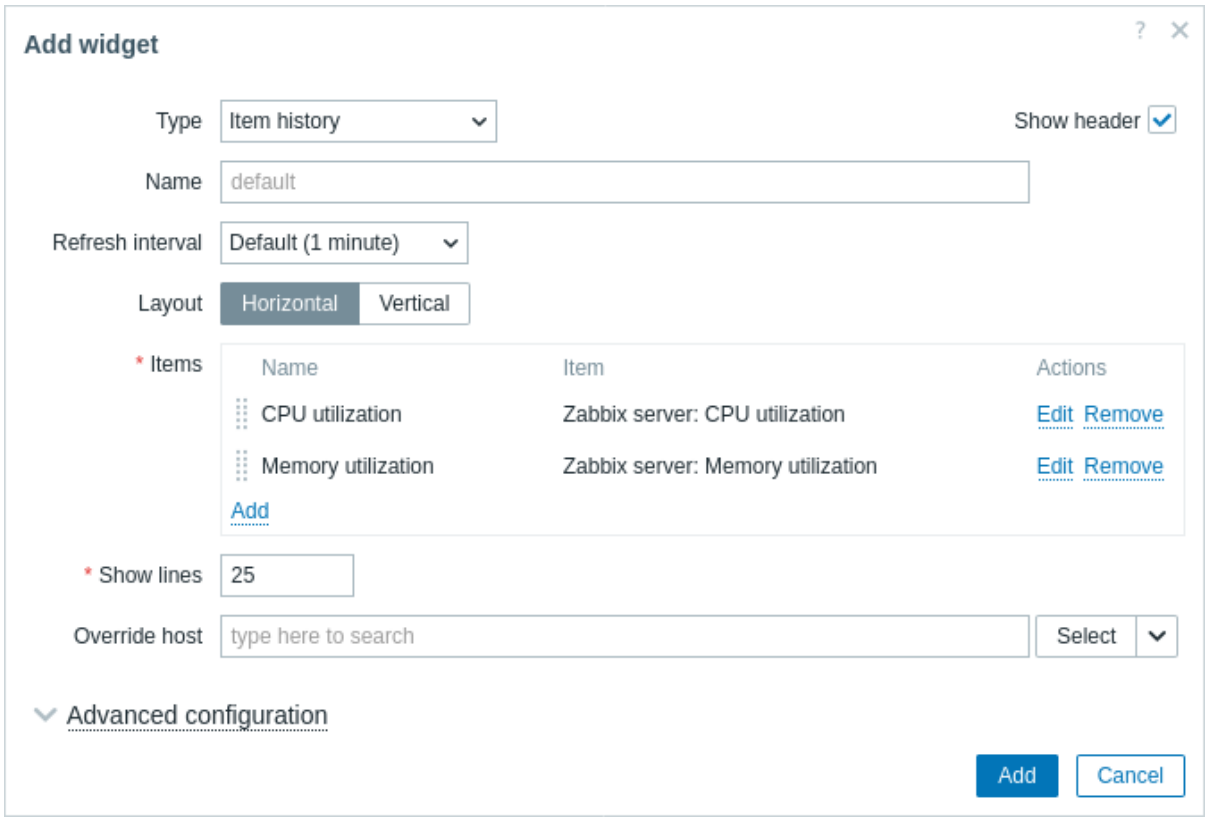




Można wyświetlić do 1000 rekordów.

Konfiguracja

Aby skonfigurować widget, wybierz *Item history* jako typ:



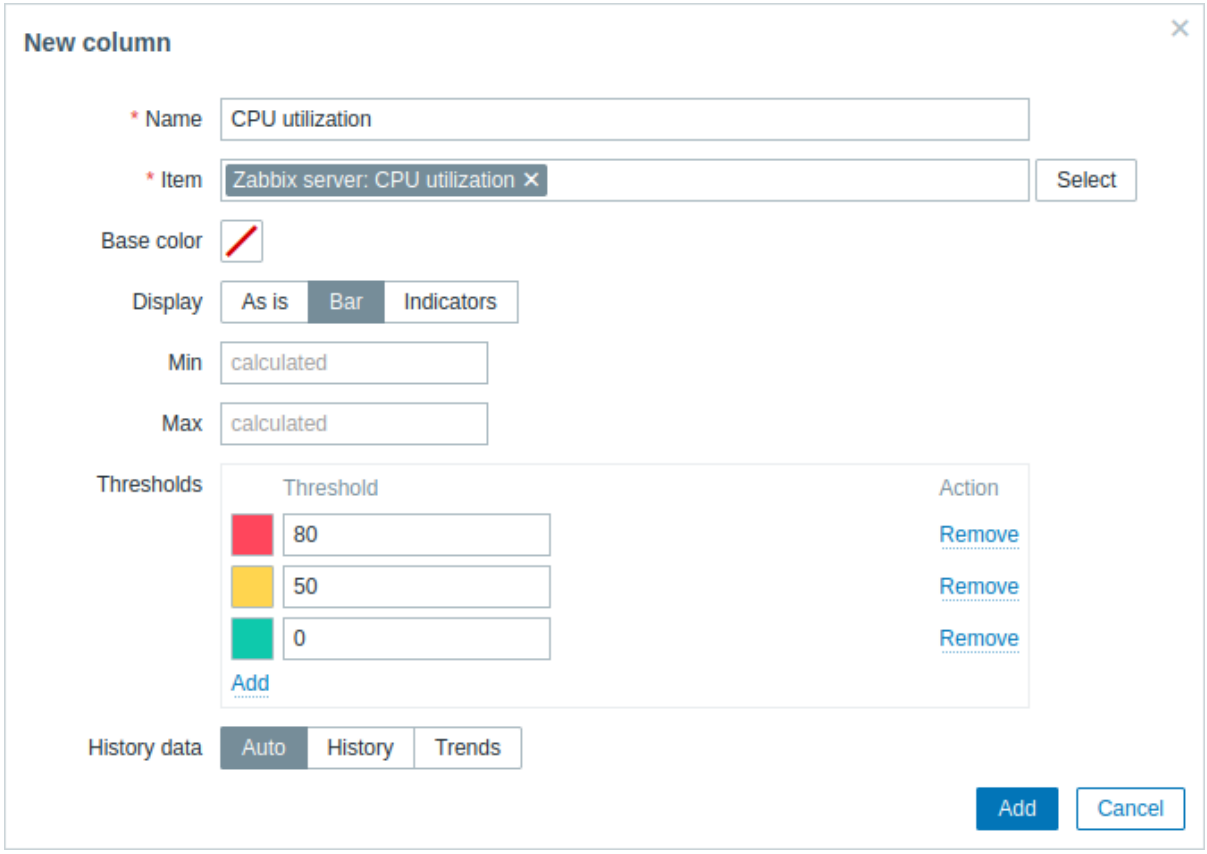
Oprócz parametrów wspólnych dla wszystkich widgetów, możesz ustawić następujące opcje specyficzne:

Layout	Wybierz układ kolumn pozycji: **Horizontal** — pozycje będą wyświetlane poziomo, wartości pionowo; **Vertical** — pozycje będą wyświetlane pionowo, wartości poziomo.

Items	Dodaj kolumny pozycji do wyświetlenia. Kolejność pozycji określa kolejność ich wyświetlania. Pozycje można zmieniać miejscami, przeciągając je w górę lub w dół za uchwyt znajdujący się przed nazwą pozycji.
Show lines	Określ liczbę wyświetlanych wierszy wartości pozycji.
Override host	Wybierz kompatybilny widget lub selektor hosta pulpitu jako źródło danych dla hostów. Ten parametr nie jest dostępny podczas konfigurowania widgetu na pulpicie szablonu.
Advanced configuration	Kliknij etykietę *Advanced configuration*, aby wyświetlić opcje konfiguracji zaawansowanej.

Konfiguracja kolumn

Aby skonfigurować kolumny pozycji, kliknij *Dodaj* w parametrze *Pozycje*:



Wspólne parametry kolumn:

Nazwa	Wprowadź nazwę kolumny. Jeśli pozostawisz puste, zostanie użyta nazwa pozycji z parametru *Pozycja*.
Pozycja	Wybierz pozycję. Zwróć uwagę, że parametry konfiguracji kolumny różnią się w zależności od typu informacji wybranej pozycji; więcej informacji znajdziesz w opisach poszczególnych parametrów poniżej. Podczas konfigurowania widżetu na pulpicie szablonu można wybrać tylko pozycje skonfigurowane w szablonie.
Kolor bazowy	Wybierz kolor tła kolumny lub kolor wypełnienia, jeśli *Wyświetlanie* jest ustawione na „Słupek” lub „Wskaźniki”. Zwróć uwagę, że kolor bazowy może zostać nadpisany przez kolory progów lub wyróżnienia.

Parametry kolumny specyficzne dla pozycji typu numerycznego:

Wyświetlanie	Wybierz sposób wyświetlania wartości pozycji: **As is** - jako zwykły tekst; **Bar** - jako jednolity pasek wypełniony kolorem; **Indicators** - jako segmentowany pasek wypełniony kolorem.

Min	Wprowadź wartość minimalną dla paska/wskaźników. Jeśli pole pozostanie puste, widget użyje minimalnej wartości pozycji. Ten parametr jest dostępny tylko wtedy, gdy opcja *Wyświetlanie* jest ustawiona na „Bar” lub „Indicators”.
Max	Wprowadź wartość maksymalną dla paska/wskaźników. Jeśli pole pozostanie puste, widget użyje maksymalnej wartości pozycji. Ten parametr jest dostępny tylko wtedy, gdy opcja *Wyświetlanie* jest ustawiona na „Bar” lub „Indicators”.
Progi	Kliknij *Dodaj*, aby dodać próg, wybierz kolor progu z próbnika kolorów i określ wartość numeryczną. Lista progów zostanie posortowana rosnąco podczas zapisywania. Obsługiwane są sufiksy (na przykład „1d”, „2w”, „4K”, „8G”). Obsługiwane są mapowania wartości.
Dane historyczne	Wybierz, czy pobierać dane z historii, czy z trendów: **Auto** - wybór automatyczny; **History** - pobierz dane historyczne; **Trends** - pobierz dane trendów.

Parametry kolumn specyficzne dla pozycji typu znakowego, tekstowego, log i JSON:

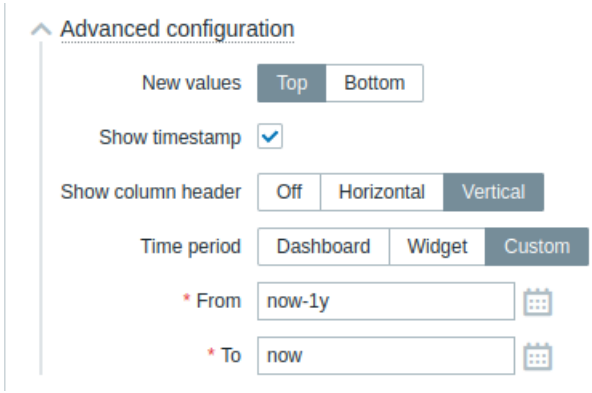
Wyróżnienia	Kliknij *Dodaj*, aby dodać wyróżnienie, wybierz kolor wyróżnienia z próbnika kolorów i określ wyrażenie regularne. Wybrany kolor zostanie użyty jako kolor tła dla wartości pozycji, w których określone wyrażenie regularne pasuje do tekstu.
Wyświetlanie	Wybierz sposób wyświetlania wartości pozycji: **Bez zmian** - dokładnie tak, jak została odebrana. Podziały wierszy są zachowywane, jeśli wartość zawiera znaki końca linii. Zawijanie wyrazów jest stosowane, jeśli *Układ* jest ustawiony na „Pionowy” i skonfigurowano więcej niż jedną kolumnę; **HTML** - jako tekst sformatowany w HTML; **Pojedynczy wiersz** - jako pojedynczy wiersz, obcięty do określonej długości (1-500 znaków). Najechanie kursorem lub kliknięcie obciętej wartości otwiera wyskakujące okno z pełną wartością.
Użyj czcionki o stałej szerokości	Zaznacz to pole wyboru, aby wyświetlać wartość pozycji czcionką o stałej szerokości (domyślnie niezaznaczone).
Wyświetlaj czas lokalny	Zaznacz to pole wyboru, aby wyświetlać czas lokalny zamiast znacznika czasu w kolumnie znacznika czasu. Zwróć uwagę, że pole wyboru *Pokaż znacznik czasu* w konfiguracji zaawansowanej również musi być zaznaczone. Ten parametr jest dostępny tylko dla pozycji typu log.

Parametry kolumny specyficzne dla pozycji typu binarnego:

Pokaż miniaturę	Zaznacz to pole wyboru, aby wyświetlać miniaturę dla binariów obrazów lub opcję „Pokaż” dla binariów niebędących obrazami. Odznacz to pole wyboru, aby wyświetlać opcję „Pokaż” dla wszystkich wartości binarnych pozycji. Najechanie kursorem na opcję „Pokaż” lub kliknięcie jej otwiera wyskakujące okno z wartością pozycji (obrazem lub ciągiem Base64). Jeśli wartość pozycji jest pustym ciągiem, wyświetlana jest opcja „Pokaż”; najechanie kursorem na nią lub kliknięcie jej otwiera wyskakujące okno zawierające „Pusty ciąg”.

Konfiguracja zaawansowana

Zaawansowane opcje konfiguracji są dostępne w zwijanej sekcji *Konfiguracja zaawansowana*:

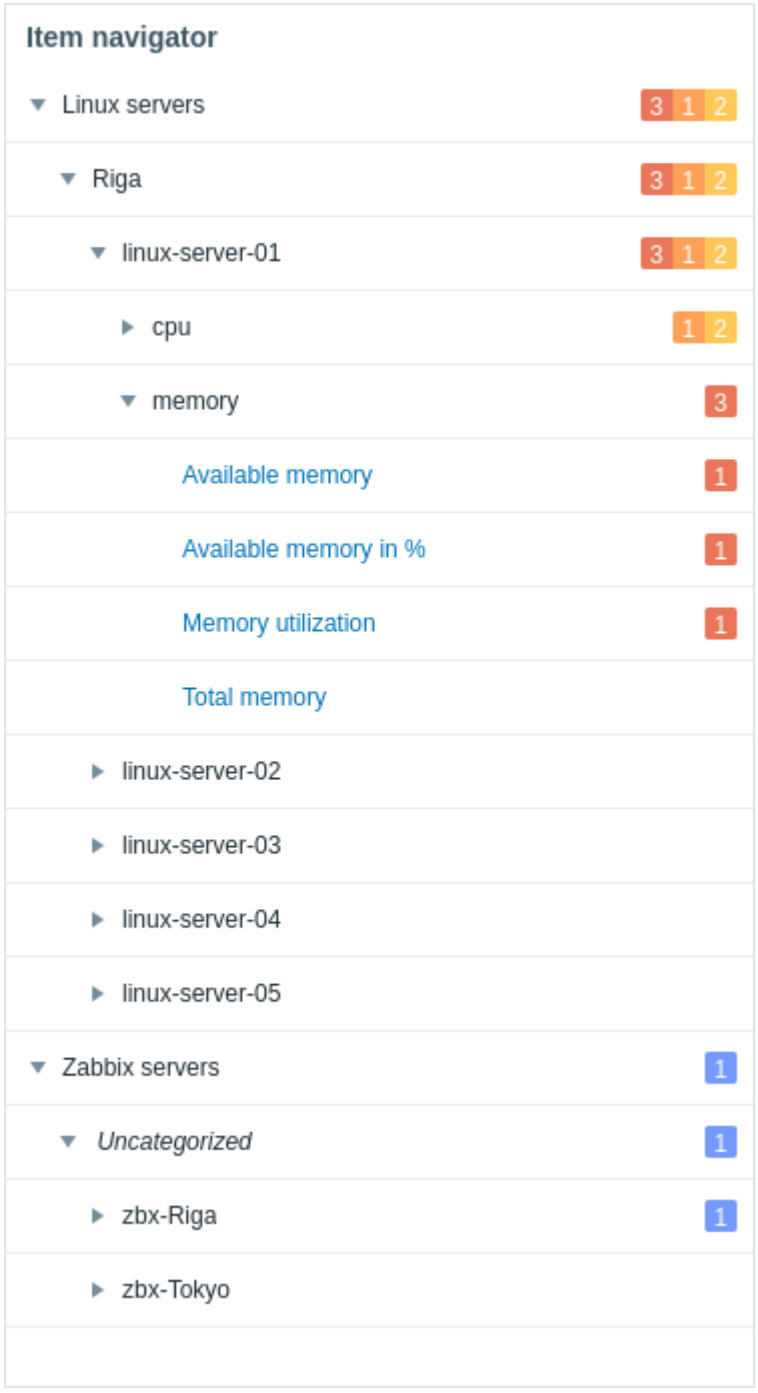


Nowe wartości	Wybierz, gdzie mają być dodawane nowe wartości pozycji: **U góry** - na górze kolumn; **Na dole** - na dole kolumn.
Pokaż znacznik czasu	Zaznacz to pole wyboru, aby wyświetlić kolumnę znacznika czasu (domyślnie niezaznaczone).
Pokaż nagłówek kolumny	Wybierz orientację nagłówka kolumny: **Wyłączone** - ukryj nagłówek; **Poziomo** - wyświetl nagłówek poziomo; **Pionowo** - wyświetl nagłówek pionowo.
Okres czasu	Wybierz źródło danych dla okresu czasu: **Pulpit** - użyj selektora okresu czasu pulpitu; **Widżet** - użyj zgodnego widżetu (ustawionego w parametrze *Widżet*); **Niestandardowy** - użyj niestandardowego okresu czasu ustawionego w parametrach *Od* i *Do*; jeśli jest ustawiony, w prawym górnym rogu widżetu zostanie wyświetlona ikona zegara, wskazująca ustawiony czas po najechaniu kursorem. Zwróć uwagę, że niezależnie od konfiguracji *Okresu czasu* widżetu, zgodne widżety nadal mogą używać go jako źródła danych dla okresu czasu.
Widżet	Wprowadź lub wybierz zgodny widżet (*Graph*, *Graph (classic)*, *Graph prototype*) jako źródło danych dla okresu czasu. Ten parametr jest dostępny, jeśli *Okres czasu* jest ustawiony na „Widżet”.
Od	Wprowadź lub wybierz początek okresu czasu. Obsługiwana jest składnia czasu względnego (`now`, `now/d`, `now/w-1w` itd.). Ten parametr jest dostępny, jeśli *Okres czasu* jest ustawiony na „Niestandardowy”.
Do	Wprowadź lub wybierz koniec okresu czasu. Obsługiwana jest składnia czasu względnego (`now`, `now/d`, `now/w-1w` itd.). Ten parametr jest dostępny, jeśli *Okres czasu* jest ustawiony na „Niestandardowy”.

17 Nawigator pozycji

Przegląd

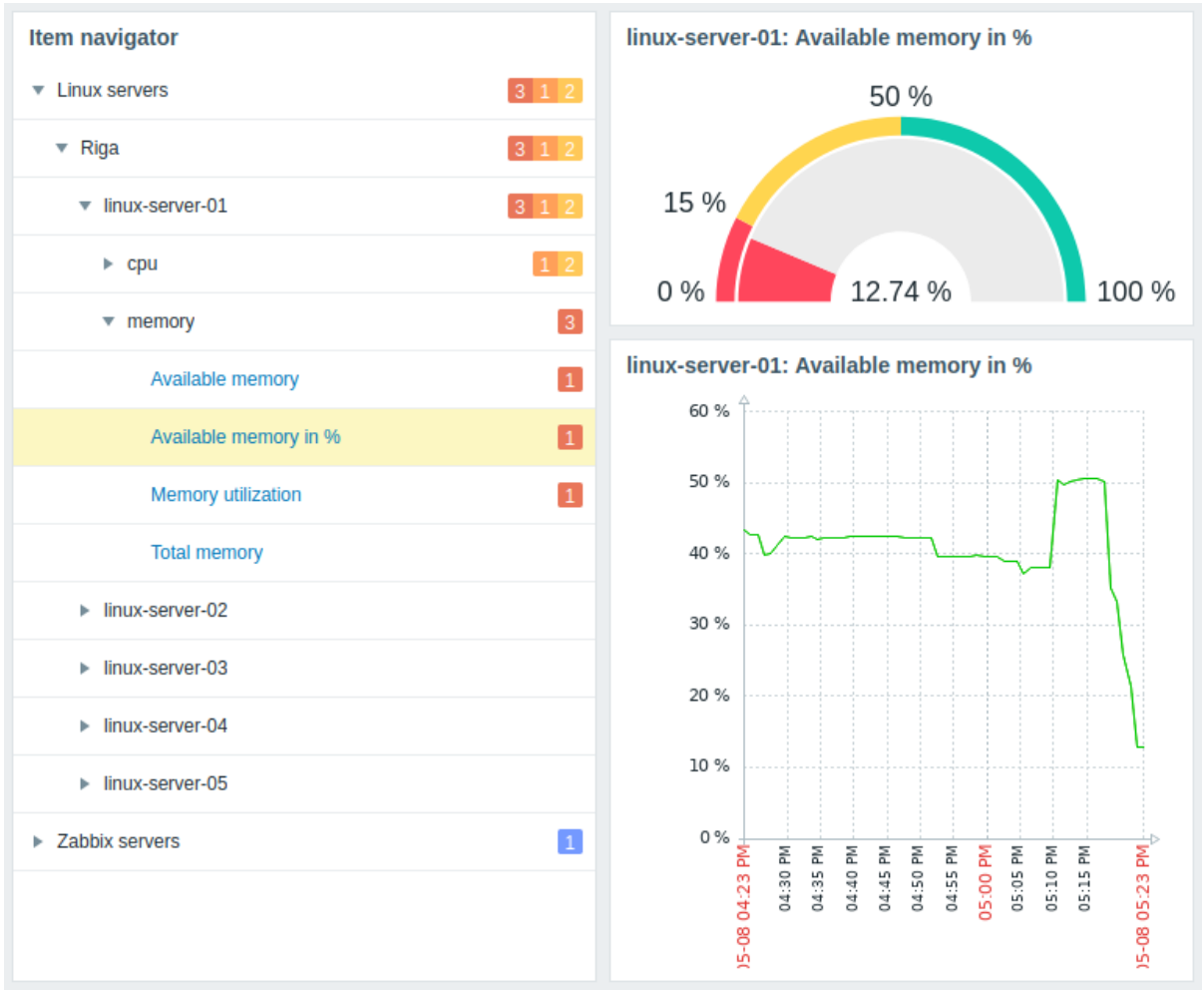
Widżet *Nawigator pozycji* wyświetla listę pozycji na podstawie różnych opcji filtrowania i grupowania.



Grupy, według których pozycje są uporządkowane, można rozwijać lub zwijać.

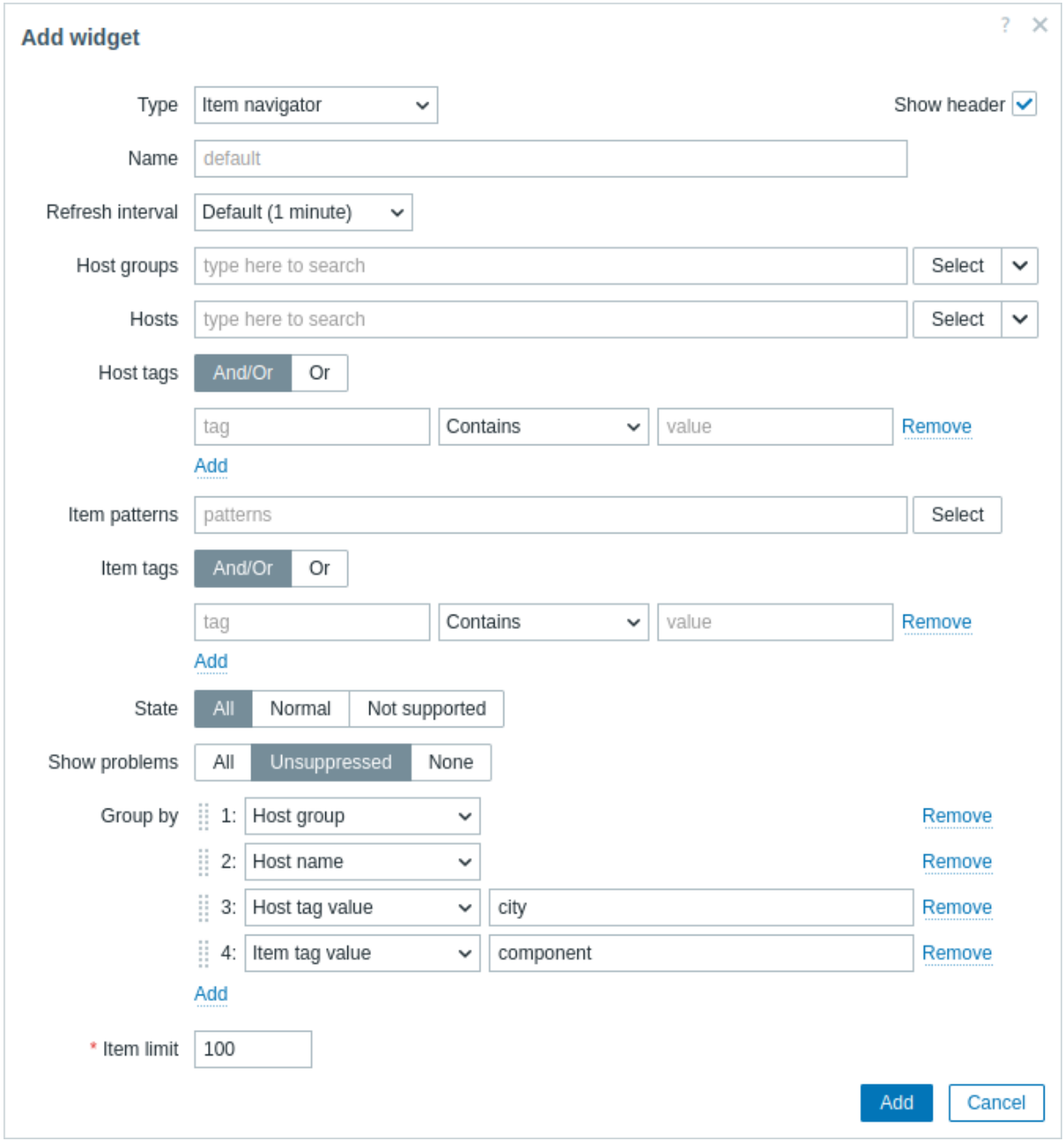
W przypadku grup i problemów dodatkowe szczegóły są dostępne po najechaniu kursorem.

Widżet jest najbardziej przydatny do sterowania tym, co wyświetlają inne widżety, na podstawie wybranej pozycji.



Konfiguracja

Aby skonfigurować, wybierz *Nawigator pozycji* jako typ:



Oprócz parametrów wspólnych dla wszystkich widżetów można ustawić następujące opcje specyficzne:

Grupy hostów	Wybierz grupy hostów. Alternatywnie wybierz zgodny widżet jako źródło danych dla grup hostów. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy grupy zostanie wyświetlona rozwijana lista pasujących grup. Wybranie nadrzędnej grupy hostów powoduje automatyczne wybranie wszystkich zagnieżdżonych grup hostów; jeśli nie wybrano żadnych grup hostów, widżet wyświetli pozycje należące do wszystkich hostów ze wszystkich grup hostów. Ten parametr nie jest dostępny podczas konfigurowania widżetu na pulpicie szablonu.
Hosty	Wybierz hosty. Alternatywnie wybierz zgodny widżet lub pulpit jako źródło danych dla hostów. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy hosta zostanie wyświetlona rozwijana lista pasujących hostów. Jeśli nie wybrano żadnych hostów, widżet wyświetli pozycje należące do wszystkich hostów. Ten parametr nie jest dostępny podczas konfigurowania widżetu na pulpicie szablonu.

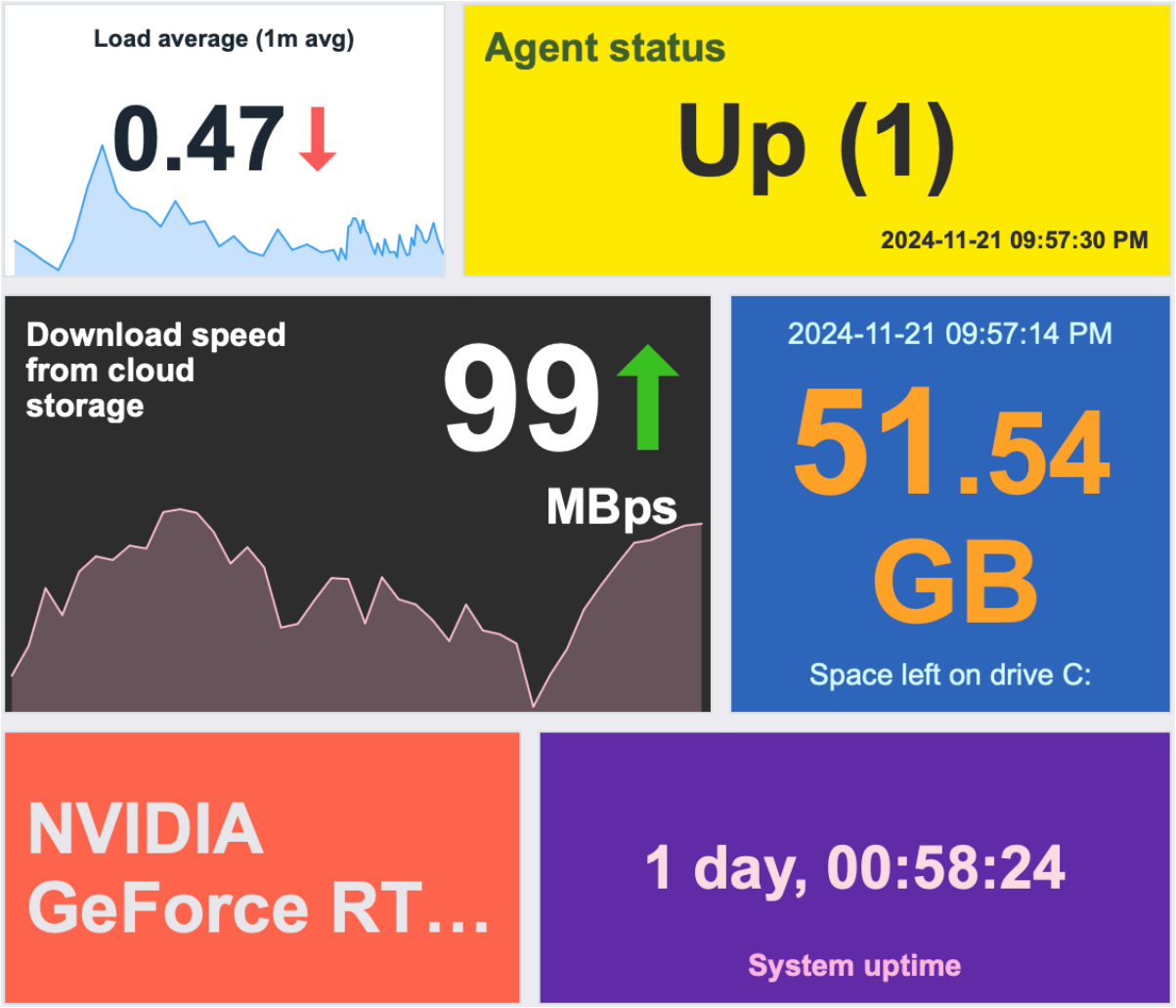
Tagi hosta	Określ tagi do filtrowania pozycji wyświetlanych w widżecie. Można zarówno uwzględniać, jak i wykluczać określone tagi oraz wartości tagów. Można ustawić kilka warunków. Dopasowanie nazw tagów zawsze uwzględnia wielkość liter. Dla każdego warunku dostępnych jest kilka operatorów: **Istnieje** - uwzględnij określone nazwy tagów; **Równa się** - uwzględnij określone nazwy tagów i wartości (z uwzględnieniem wielkości liter); **Zawiera** - uwzględnij określone nazwy tagów, dla których wartości tagów zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter); **Nie istnieje** - wyklucz określone nazwy tagów; **Nie równa się** - wyklucz określone nazwy tagów i wartości (z uwzględnieniem wielkości liter); **Nie zawiera** - wyklucz określone nazwy tagów, dla których wartości tagów zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter). Dostępne są dwa typy obliczania warunków: **I/Lub** - wszystkie warunki muszą być spełnione, a warunki mające tę samą nazwę tagu będą grupowane operatorem Lub; **Lub** - wystarczy spełnienie jednego warunku. Ten parametr nie jest dostępny podczas konfigurowania widżetu na pulpicie szablonu.
Wzorce pozycji	Wprowadź wzorce pozycji lub wybierz istniejące pozycje jako wzorce pozycji. Pozycje pasujące do określonych wzorców będą wyświetlane w nawigatorze pozycji. Do wyboru można używać wzorców wieloznacznych (na przykład ∗ zwróci pozycje pasujące do zera lub większej liczby znaków; `Zabbix*` zwróci pozycje zaczynające się od „Zabbix”). Aby określić wzorzec wieloznaczny, wprowadź ciąg ręcznie i naciśnij *Enter*. Po rozpoczęciu wpisywania zostanie wyświetlona rozwijana lista pasujących pozycji ograniczona do tych należących do wybranych *Hostów* lub hostów w wybranych *Grupach hostów*, jeśli takie wybrano. Symbol wieloznaczny jest zawsze interpretowany, dlatego nie można na przykład dodać indywidualnie pozycji o nazwie *item** , jeśli istnieją inne pasujące pozycje (np. item2, item3). Podczas konfigurowania widżetu na pulpicie szablonu ten parametr pozwala wybierać tylko pozycje skonfigurowane w szablonie.
Tagi pozycji	Określ tagi do filtrowania pozycji wyświetlanych w widżecie. Można zarówno uwzględniać, jak i wykluczać określone tagi oraz wartości tagów. Można ustawić kilka warunków. Dopasowanie nazw tagów zawsze uwzględnia wielkość liter. Dla każdego warunku dostępnych jest kilka operatorów: **Istnieje** - uwzględnij określone nazwy tagów; **Równa się** - uwzględnij określone nazwy tagów i wartości (z uwzględnieniem wielkości liter); **Zawiera** - uwzględnij określone nazwy tagów, dla których wartości tagów zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter); **Nie istnieje** - wyklucz określone nazwy tagów; **Nie równa się** - wyklucz określone nazwy tagów i wartości (z uwzględnieniem wielkości liter); **Nie zawiera** - wyklucz określone nazwy tagów, dla których wartości tagów zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter). Dostępne są dwa typy obliczania warunków: **I/Lub** - wszystkie warunki muszą być spełnione, a warunki mające tę samą nazwę tagu będą grupowane operatorem Lub; **Lub** - wystarczy spełnienie jednego warunku.
Stan	Filtruj, które pozycje mają być wyświetlane na podstawie ich stanu (wszystkie, normalne, nieobsługiwane).
Pokaż problemy	Filtruj, które problemy mają być wyświetlane na podstawie ich statusu (wszystkie, niewyciszone, brak). Problemy są oznaczane kolorowymi blokami na końcu wiersza pozycji. Kolory zależą od ważności problemu, którą można dostosować w *Administracja* > *Ogólne* > *Opcje wyświetlania wyzwalaczy*. Poziomy ważności problemów można zmieniać podczas aktualizowania problemów.

Grupuj według	Dodaj atrybut grupowania, według którego pozycje będą grupowane: **Grupa hostów** - grupuj pozycje według grup hostów ich hostów; **Nazwa hosta** - grupuj pozycje według ich hostów; **Wartość tagu hosta** - wprowadź nazwę tagu, aby grupować pozycje według wartości tego tagu hosta (na przykład wpisz „city”, aby grupować pozycje według wartości „Riga”, „Tokyo” itd.); **Wartość tagu pozycji** - wprowadź nazwę tagu, aby grupować pozycje według wartości tego tagu pozycji (na przykład wpisz „component”, aby grupować pozycje według wartości „cpu”, „memory” itd.). Atrybuty grupowania można zmieniać kolejnością, przeciągając je w górę lub w dół za uchwyt przed nazwą grupy. Należy pamiętać, że kolejność atrybutów grupowania określa kolejność zagnieżdżania grup. Na przykład określenie wielu nazw tagów hosta (1: color, 2: city) spowoduje pogrupowanie pozycji najpierw według koloru (red, blue itd.), a następnie według miasta (Riga, Tokyo itd.). Pozycja może być wyświetlana w wielu grupach w zależności od skonfigurowanych atrybutów grupowania (na przykład podczas grupowania według grupy hostów, gdy host danej pozycji należy do wielu grup hostów). Kliknięcie takiej pozycji powoduje jej zaznaczenie i podświetlenie we wszystkich grupach. Pozycje, które nie pasują do skonfigurowanych atrybutów grupowania, są wyświetlane w grupie *Bez kategorii*. Jeśli opcja *Pokaż problemy* jest skonfigurowana do wyświetlania problemów, są one wyświetlane w następujący sposób: - dla każdej grupy wyświetlana jest łączna liczba problemów wszystkich podrzędnych pozycji; - dla każdej pozycji wyświetlana jest tylko liczba jej problemów. Można określić maksymalnie 10 atrybutów grupowania i wszystkie muszą być unikalne. Jeśli nie określono żadnych atrybutów grupowania, pozycje nie będą grupowane.
Limit pozycji	Wprowadź maksymalną liczbę pozycji do wyświetlenia. Możliwe wartości mieszczą się w zakresie 1-9999. Gdy do wyświetlenia dostępnych jest więcej pozycji niż ustawiony limit, pod wyświetlonymi pozycjami zostanie pokazany odpowiedni komunikat (na przykład „Wyświetlono 100 ze 100+ pozycji”). Zwróć uwagę, że skonfigurowany limit pozycji wpływa również na wyświetlanie skonfigurowanych grup; na przykład jeśli limit pozycji ustawiono na 100, a pozycje są grupowane według hostów (z których każdy zawiera 200 pozycji), w widżecie zostanie wyświetlony tylko pierwszy host wraz ze swoimi 100 pozycjami. Na ten parametr nie wpływa parametr *Limit for search and filter results* w *Administracja* → *Ogólne* → *GUI*.

18 Wartość pozycji

Przegląd

Widżet *Wartość pozycji* wyświetla wartość pojedynczej numerycznej lub tekstowej pozycji. Jest przydatny do monitorowania ważnych metryk, wizualizacji progów oraz wykrywania nagłych zmian w danych.



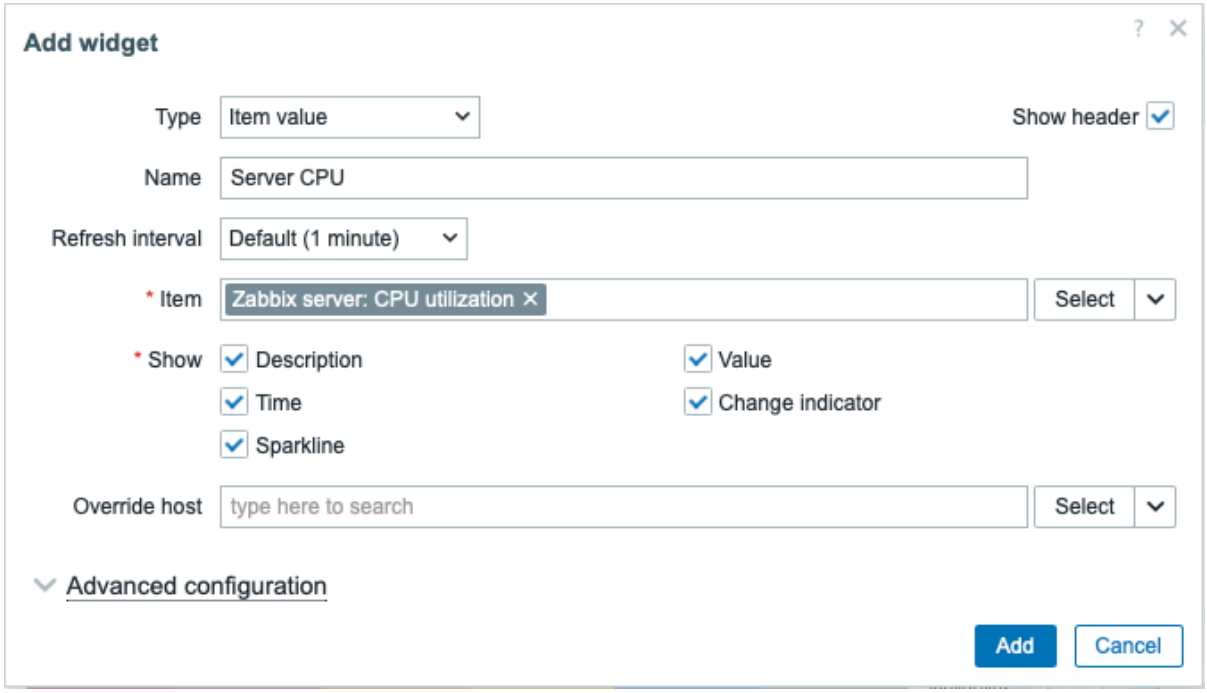
Możesz skonfigurować widżet tak, aby wyświetlał następujące elementy:

- Znacznik czasu metryki (2024-11-21 09:57:30)
- Opis pozycji (Load average (1m), Agent status)
- Wartość pozycji, wskaźnik zmiany oraz jednostki (0.47 ↓, 99 ↑ Mbps)
- Kolor tła
- Wykres sparkline dla wartości z określonego przedziału czasu

Kliknięcie widżetu otwiera wykres ad hoc dla pozycji numerycznych lub najnowsze dane dla pozycji tekstowych.

Konfiguracja

Aby skonfigurować widget, wybierz *Item value* jako typ widgetu:



Oprócz parametrów wspólnych dla wszystkich widgetów, możesz ustawić następujące opcje specyficzne:

Item	Wybierz pozycję. Alternatywnie wybierz zgodny widget jako źródło danych dla pozycji. Pozycje zwracające dane binarne nie są obsługiwane.
Show	Zaznacz pole wyboru, aby wyświetlić odpowiedni element: opis, wartość, czas, wskaźnik zmiany, wykres przebiegu. Usuń zaznaczenie, aby ukryć. Musi być wybrany co najmniej jeden element.
Override host	Wybierz zgodny widget lub selektor hosta pulpitu jako źródło danych dla hostów. Ten parametr nie jest dostępny podczas konfigurowania widgetu na pulpicie szablonu.
Advanced configuration	Kliknij etykietę *Advanced configuration*, aby wyświetlić opcje konfiguracji zaawansowanej.

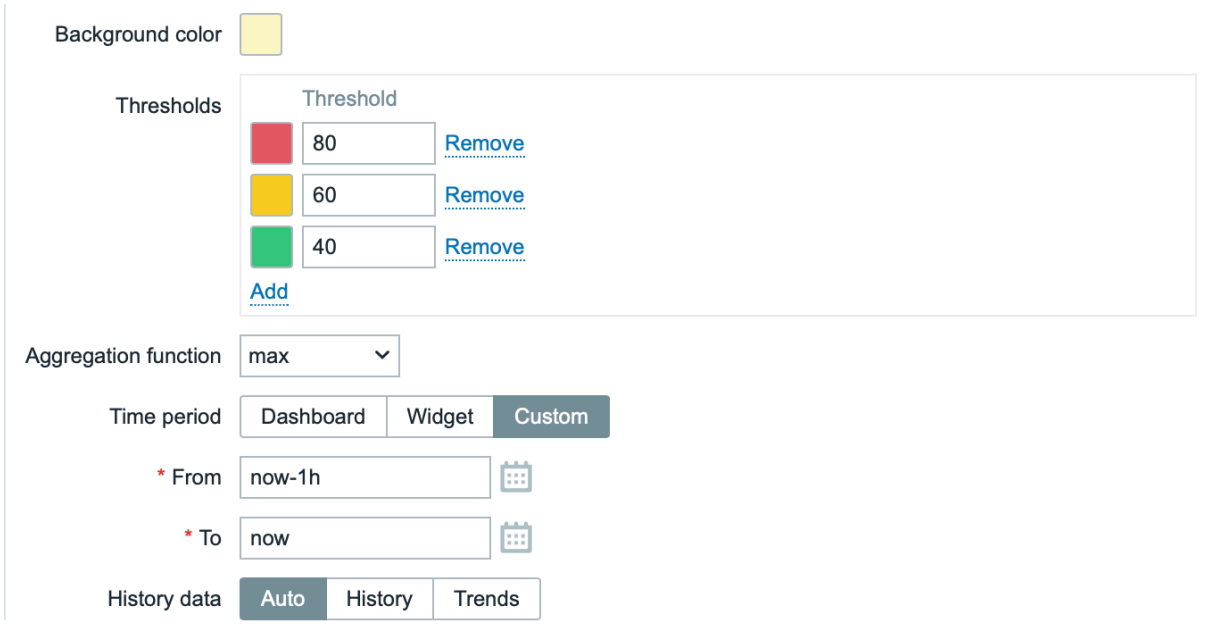
Konfiguracja zaawansowana

Opcje konfiguracji zaawansowanej są dostępne w zwijanej sekcji *Konfiguracja zaawansowana*, i tylko dla tych elementów, które są wybrane w polu *Pokaż* (zobacz powyżej).

Należy pamiętać, że wiele elementów nie może zajmować tej samej przestrzeni; jeśli zostaną umieszczone w tej samej przestrzeni, zostanie wyświetlony komunikat o błędzie.

Ogólne parametry widżetu

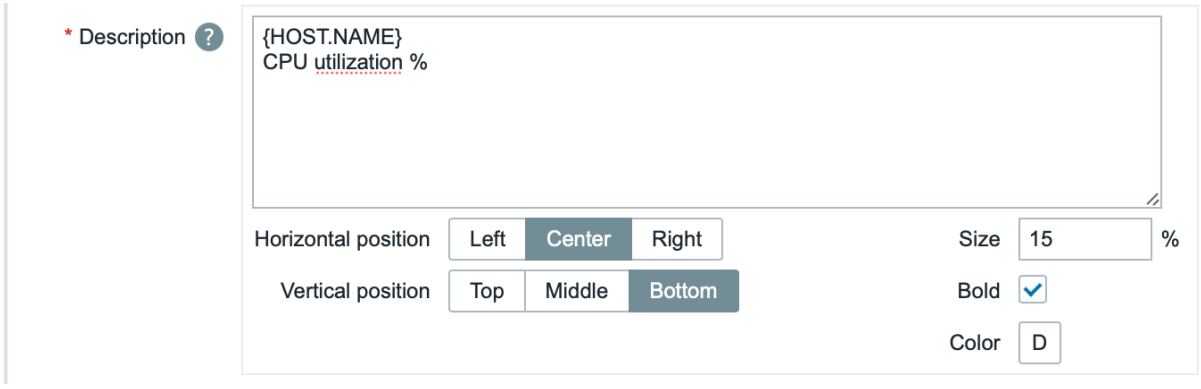
Te parametry określają kolor tła (statyczny lub dynamiczny) dla całego widżetu oraz funkcję agregacji do wyświetlania wartości.



Kolor tła	Wybierz kolor tła dla całego widżetu za pomocą próbnika kolorów. D oznacza kolor domyślny (zależy od motywu frontend). Aby przywrócić wartość domyślną, kliknij przycisk *Użyj domyślnego* w próbniku kolorów.
Progi	Skonfiguruj dynamiczny kolor tła dla całego widżetu. Kliknij *Dodaj*, aby dodać próg, wybierz kolor tła z próbnika kolorów i określ wartość liczbową. Gdy wartość pozycji będzie równa wartości progu lub większa od niej, kolor tła zmieni się. Lista zostanie posortowana rosnąco po zapisaniu. Pamiętaj, że dynamiczny kolor tła będzie wyświetlany poprawnie tylko dla pozycji numerycznych.
Funkcja agregacji	Określ, której funkcji agregacji użyć: **min** - wyświetl najmniejszą wartość; **max** - wyświetl największą wartość; **avg** - wyświetl wartość średnią; **count** - wyświetl liczbę wartości; **sum** - wyświetl sumę wartości; **first** - wyświetl pierwszą wartość; **last** - wyświetl ostatnią wartość; **not used** - wyświetl najnowszą wartość (bez agregacji). Agregacja umożliwia wyświetlenie zagregowanej wartości dla wybranego przedziału czasu (5 minut, godzina, dzień) zamiast najnowszej wartości. Tylko dane numeryczne mogą być wyświetlane dla *min*, *max*, *avg* i *sum*. W przypadku *count* dane nienumeryczne zostaną zamienione na numeryczne.
Okres czasu	Okres czasu używany do agregacji wartości. Wybierz źródło danych dla okresu czasu: **Dashboard** - użyj selektora okresu czasu dashboardu; **Widget** - użyj zgodnego widżetu (ustawionego w parametrze *Widget*); **Custom** - użyj niestandardowego okresu czasu ustawionego w parametrach *Od* i *Do*; jeśli jest ustawiony, w prawym górnym rogu widżetu zostanie wyświetlona ikona zegara, wskazująca ustawiony czas po najechaniu kursorem. Pamiętaj, że niezależnie od konfiguracji *Okresu czasu* widżetu, zgodne widżety nadal mogą używać go jako źródła danych dla okresu czasu. Ten parametr nie jest dostępny, jeśli *Funkcja agregacji* jest ustawiona na ”not used”.
Widget	Wprowadź lub wybierz zgodny widżet jako źródło danych dla okresu czasu. Ten parametr jest dostępny, jeśli *Okres czasu* jest ustawiony na ”Widget”.
Od	Wprowadź lub wybierz początek okresu czasu. Obsługiwana jest składnia czasu względnego (`now`, `now/d`, `now/w-1w` itd.). Ten parametr jest dostępny, jeśli *Okres czasu* jest ustawiony na ”Custom”.
Do	Wprowadź lub wybierz koniec okresu czasu. Obsługiwana jest składnia czasu względnego (`now`, `now/d`, `now/w-1w` itd.). Ten parametr jest dostępny, jeśli *Okres czasu* jest ustawiony na ”Custom”.
Dane historyczne	Pobieraj dane z historii lub trendów: **Auto** - wybór automatyczny; **History** - pobierz dane historyczne; **Trends** - pobierz dane trendów. To ustawienie ma zastosowanie tylko do danych numerycznych. Dane nienumeryczne będą zawsze pobierane z historii.

Opis

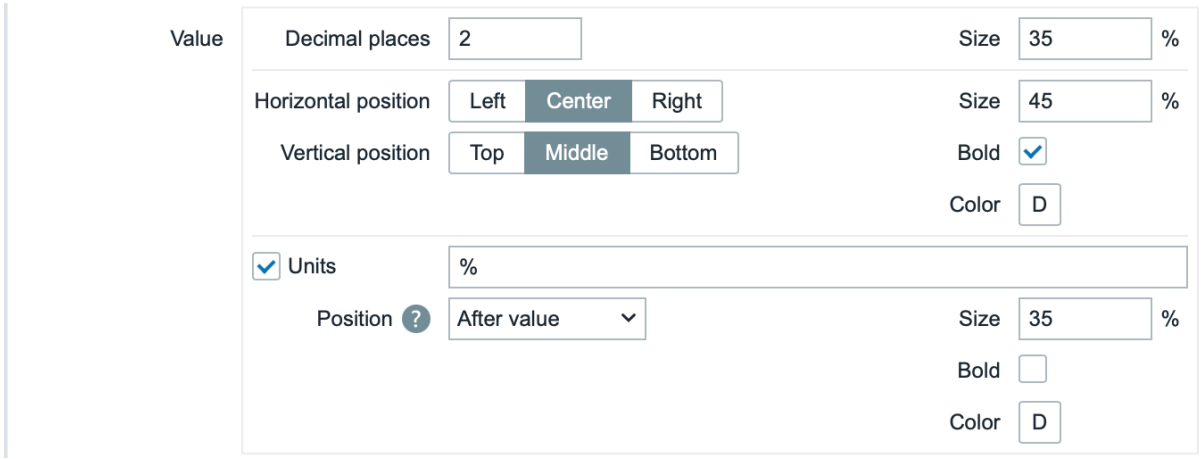
Te parametry określają, w jaki sposób ma być wyświetlany opis pozycji.



Opis	Wprowadź opis pozycji. Ten opis może zastąpić domyślną nazwę pozycji. Obsługiwane są opisy wielowierszowe. Możliwe jest połączenie tekstu i obsługiwanych makr. Obsługiwane są {HOST.*}, {ITEM.*}, {INVENTORY.*} oraz makra użytkownika.
Pozycja pozioma	Wybierz poziome położenie opisu pozycji — z lewej, z prawej lub na środku.
Pozycja pionowa	Wybierz pionowe położenie opisu pozycji — u góry, u dołu lub pośrodku.
Rozmiar	Wprowadź wysokość rozmiaru czcionki dla opisu pozycji (w procentach względem całkowitej wysokości widżetu).
Pogrubienie	Zaznacz pole wyboru, aby wyświetlać opis pozycji pogrubioną czcionką.
Kolor	Wybierz kolor opisu pozycji z próbnika kolorów. D oznacza kolor domyślny (zależy od motywu frontend). Aby przywrócić wartość domyślną, kliknij przycisk *Użyj domyślnego* w próbniku kolorów.

Wartość

Te parametry określają, jak powinna być wyświetlana wartość pozycji.

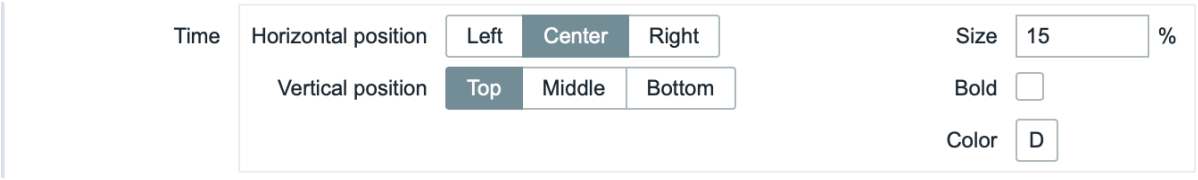


Miejsca dziesiętne	Wybierz, ile miejsc dziesiętnych ma być wyświetlanych wraz z wartością. Ta wartość wpływa tylko na pozycje typu float. Dla pozycji z jednostkami ustawionymi na „s”, jeśli ta wartość jest większa od 0 (domyślnie 2), widżet zaokrągla najbardziej znaczącą jednostkę czasu i wyświetla wartość liczbową (np. „10.43m”) zamiast konwertować wartość na pełny ciąg czasu. Po ustawieniu na 0 sekundy są konwertowane na czytelny dla człowieka ciąg czasu (na przykład „4h 56m 30s”).
Rozmiar	Wprowadź wysokość rozmiaru czcionki dla miejsc dziesiętnych (w procentach względem całkowitej wysokości widżetu).
Pozycja pozioma	Wybierz poziome położenie wartości pozycji — z lewej, z prawej lub na środku.
Pozycja pionowa	Wybierz pionowe położenie wartości pozycji — u góry, na dole lub pośrodku.
Rozmiar	Wprowadź wysokość rozmiaru czcionki dla wartości pozycji (w procentach względem całkowitej wysokości widżetu). Zwróć uwagę, że rozmiar wartości pozycji ma priorytet; pozostałe elementy muszą ustąpić jej miejsca. Jednak w przypadku wskaźnika zmiany, jeśli wartość jest zbyt duża, zostanie przycięta, aby pokazać wskaźnik zmiany.
Pogrubienie	Zaznacz pole wyboru, aby wyświetlać wartość pozycji pogrubioną czcionką.
Kolor	Wybierz kolor wartości pozycji z próbnika kolorów. D oznacza kolor domyślny (zależy od motywu frontend). Aby przywrócić wartość domyślną, kliknij przycisk *Użyj domyślnego* w próbniku kolorów.

Jednostki	
Jednostki	Zaznacz pole wyboru, aby wyświetlać jednostki wraz z wartością pozycji. Jeśli wprowadzisz nazwę jednostki, zastąpi ona jednostkę z konfiguracji pozycji.
Pozycja	Wybierz położenie jednostki pozycji — nad, pod, przed lub za wartością.
Rozmiar	Wprowadź wysokość rozmiaru czcionki dla jednostki pozycji (w procentach względem całkowitej wysokości widżetu).
Pogrubienie	Zaznacz pole wyboru, aby wyświetlać jednostkę pozycji pogrubioną czcionką.
Kolor	Wybierz kolor jednostki pozycji z próbnika kolorów. D oznacza kolor domyślny (zależy od motywu frontend). Aby przywrócić wartość domyślną, kliknij przycisk *Użyj domyślnego* w próbniku kolorów.

Czas

Te parametry określają, w jaki sposób ma być wyświetlany czas (wartość zegara z historii pozycji).



Pozycja pozioma	Wybierz poziome położenie czasu — po lewej, po prawej lub na środku.
Pozycja pionowa	Wybierz pionowe położenie czasu — u góry, na dole lub pośrodku.
Rozmiar	Wprowadź wysokość rozmiaru czcionki dla czasu (w procentach względem całkowitej wysokości widżetu).
Pogrubienie	Zaznacz pole wyboru, aby wyświetlać czas pogrubioną czcionką.
Kolor	Wybierz kolor czasu z próbnika kolorów. D oznacza kolor domyślny (zależny od motywu frontend). Aby przywrócić wartość domyślną, kliknij przycisk *Użyj domyślnego* w próbniku kolorów.

Wskaźnik zmiany

Ta sekcja umożliwia wybór koloru wskaźników zmiany za pomocą selektora kolorów.



Wskaźniki zmiany są następujące:

- ↑ - wartość pozycji wzrasta (dla pozycji numerycznych)
- ↓ - wartość pozycji spada (dla pozycji numerycznych)
- ↕ - wartość pozycji uległa zmianie (dla pozycji tekstowych oraz pozycji z mapowaniem wartości)

Uwaga:

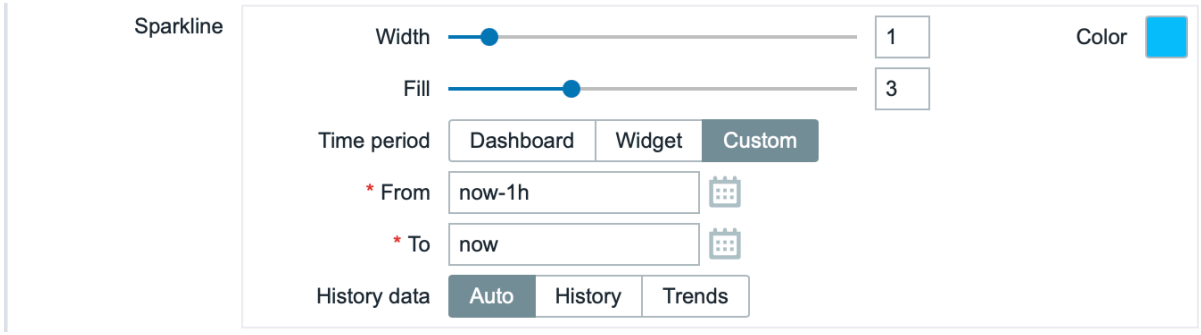
- Wskaźniki wzrostu (↑) i spadku (↓) nie są wyświetlane, jeśli istnieje tylko jedna wartość.
- Wartości są zawsze porównywane w ramach tego samego zakresu; na przykład:
  - Najnowsza wartość jest porównywana z poprzednią wartością.
  - Wartość miesięczna jest porównywana z poprzednim miesiącem.
  - W przypadku agregacji poprzedni okres ma taki sam czas trwania jak wybrany okres i kończy się bezpośrednio przed rozpoczęciem wybranego okresu.

D oznacza kolor domyślny (zależy od motywu frontend). Aby przywrócić wartość domyślną, kliknij przycisk *Use default* w selektorze kolorów.

Pionowy rozmiar wskaźnika zmiany jest równy rozmiarowi wartości (części całkowitej wartości dla pozycji numerycznych).

Sparkline

Te parametry określają sposób wyświetlania wykresu sparkline.

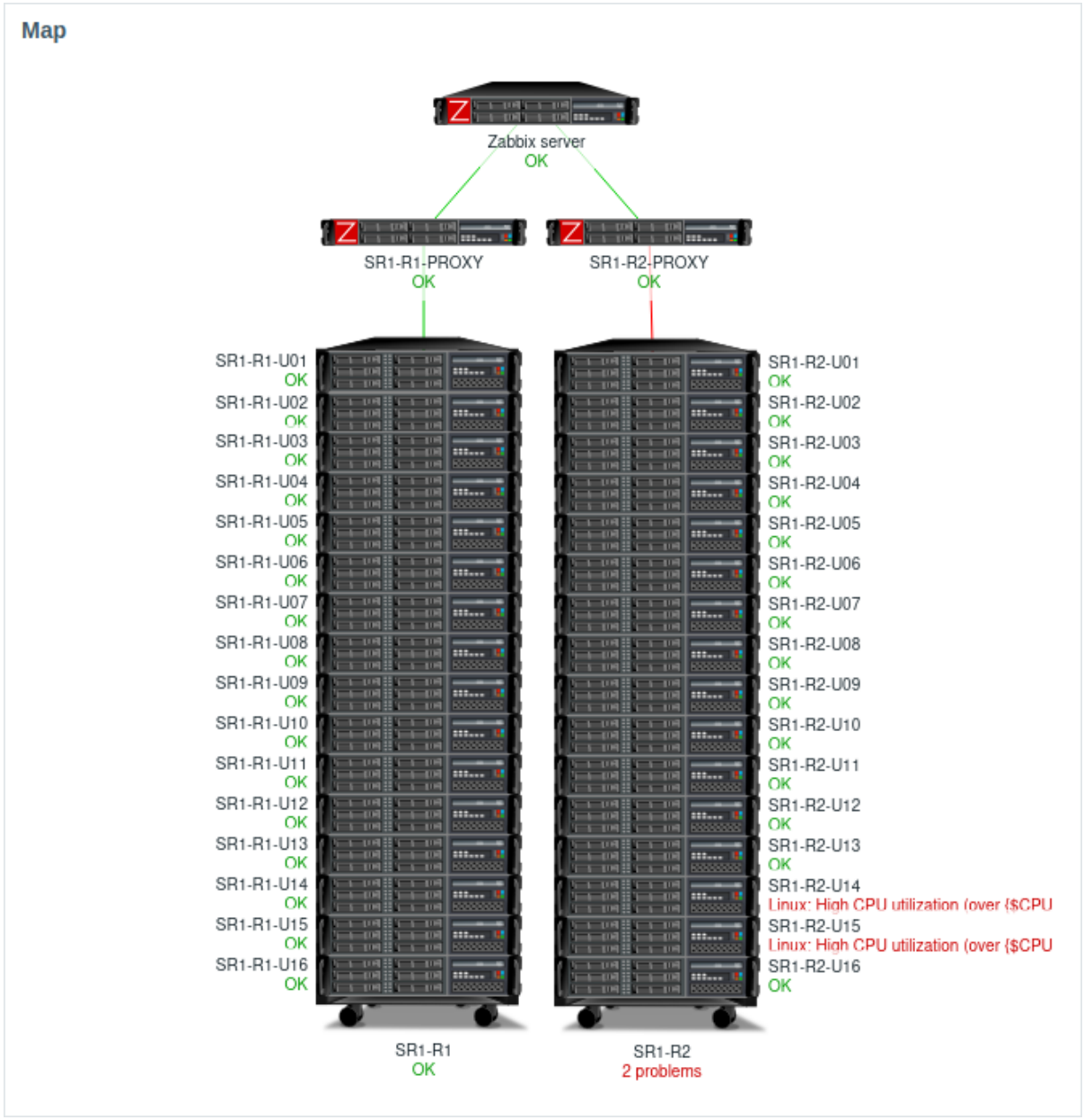


Width	Ustaw grubość linii wykresu za pomocą suwaka lub ręcznie, wprowadzając wartość z zakresu od 0 do 10.
Color	Wybierz kolor linii i wypełnienia.
Fill	Ustaw poziom przezroczystości koloru wypełnienia za pomocą suwaka lub ręcznie, wprowadzając wartość z zakresu od 0 do 10.
Time period	Określ przedział czasu dla wartości, które mają zostać uwzględnione na wykresie sparkline. Wybierz źródło danych dla przedziału czasu: **Dashboard** - użyj selektora przedziału czasu pulpitu; **Widget** - użyj kompatybilnego widżetu (ustawionego w parametrze *Widget*); **Custom** - użyj niestandardowego przedziału czasu ustawionego w parametrach *From* i *To*; jeśli jest ustawiony, w prawym górnym rogu widżetu zostanie wyświetlona ikona zegara, wskazująca ustawiony czas po najechaniu kursorem. Zwróć uwagę, że niezależnie od konfiguracji *Time period* widżetu, kompatybilne widżety nadal mogą używać go jako źródła danych dla przedziału czasu. Ten parametr nie jest dostępny, jeśli *Aggregation function* jest ustawiona na „not used”.
Widget	Wprowadź lub wybierz kompatybilny widżet jako źródło danych dla przedziału czasu. Ten parametr jest dostępny, jeśli *Time period* jest ustawiony na „Widget”.
From	Wprowadź lub wybierz początek przedziału czasu. Obsługiwana jest składnia czasu względnego (`now`, `now/d`, `now/w-1w` itd.). Ten parametr jest dostępny, jeśli *Time period* jest ustawiony na „Custom”.
To	Wprowadź lub wybierz koniec przedziału czasu. Obsługiwana jest składnia czasu względnego (`now`, `now/d`, `now/w-1w` itd.). Ten parametr jest dostępny, jeśli *Time period* jest ustawiony na „Custom”.
History data	Pobieraj dane z historii lub trendów: **Auto** - wybór automatyczny; **History** - pobieraj dane historyczne; **Trends** - pobieraj dane trendów.

19 Mapa

Przegląd

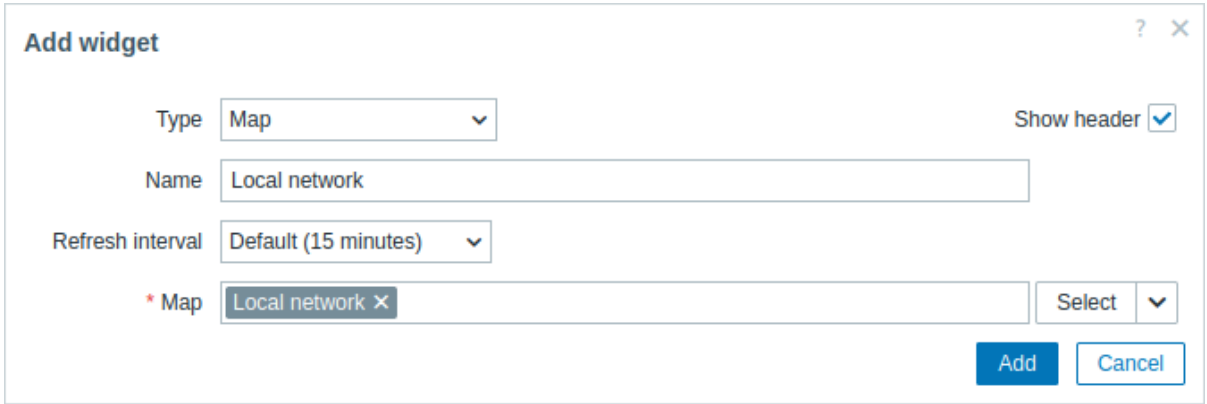
Widżet *Mapa* może wyświetlać mapę sieci lub podobną wizualizację, zapewniając dynamiczny przegląd sieci.



Można go połączyć z widżetem Drzewo nawigacji map, aby dynamicznie wyświetlać mapę wybraną w drzewie.

Konfiguracja

Aby skonfigurować, wybierz *Mapa* jako typ:



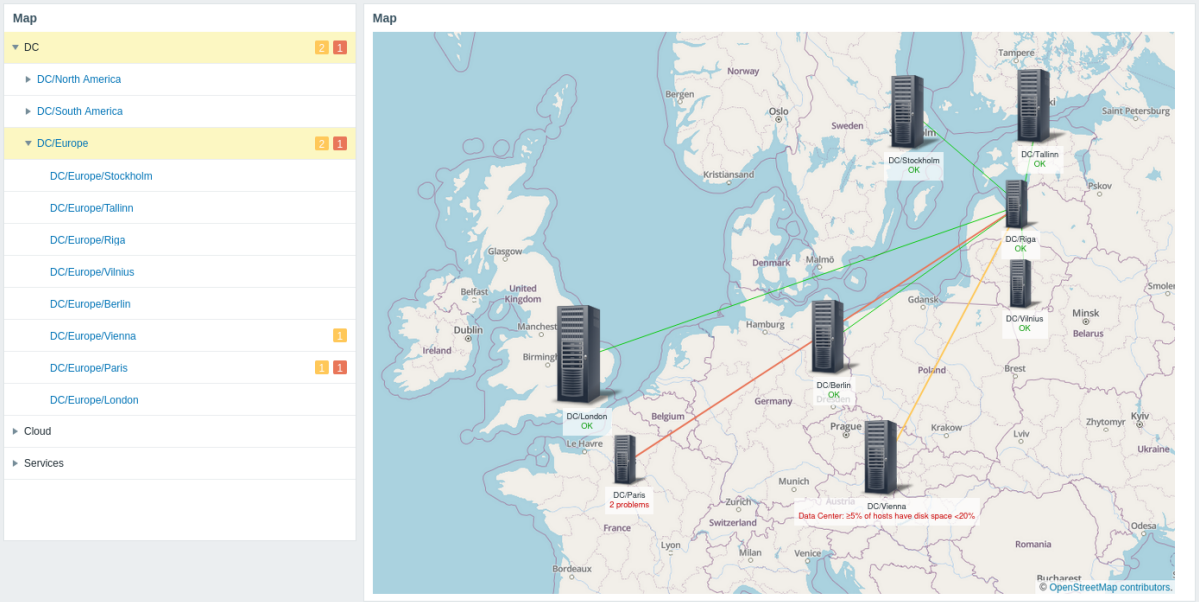
Oprócz parametrów wspólnych dla wszystkich widgetów możesz ustawić następujące opcje specyficzne:

Mapa	Ustaw mapę do wyświetlenia. Alternatywnie wybierz zgodny widget jako źródło danych dla wyświetlanej mapy. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy mapy lub widgetu zostanie wyświetlona rozwijana lista pasujących map lub widgetów.

20 Drzewo nawigacji mapy

Przegląd

Widżet *Drzewo nawigacji map* wyświetla hierarchię istniejących map oraz liczbę problemów dla każdej mapy i grupy map.

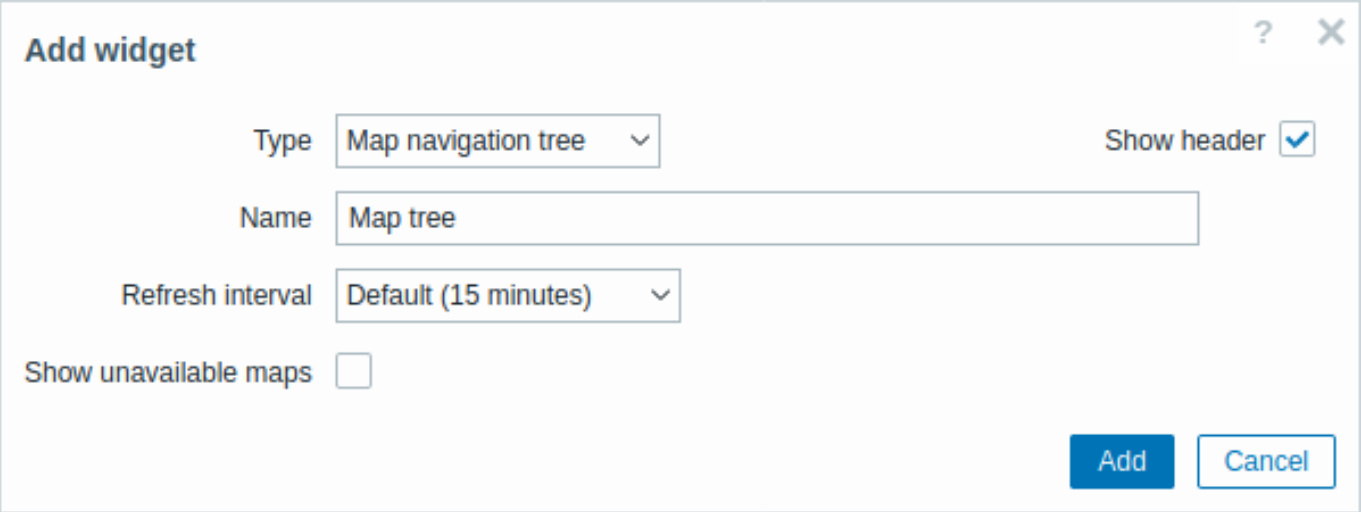


Można go połączyć z widżetem Mapa, aby dynamicznie wyświetlać mapę wybraną w drzewie.

Liczba problemów dla mapy najwyższego poziomu w hierarchii obejmuje wszystkie problemy podmap oraz problemy tej mapy.

Konfiguracja

Aby skonfigurować widżet, wybierz *Map navigation tree* jako typ:

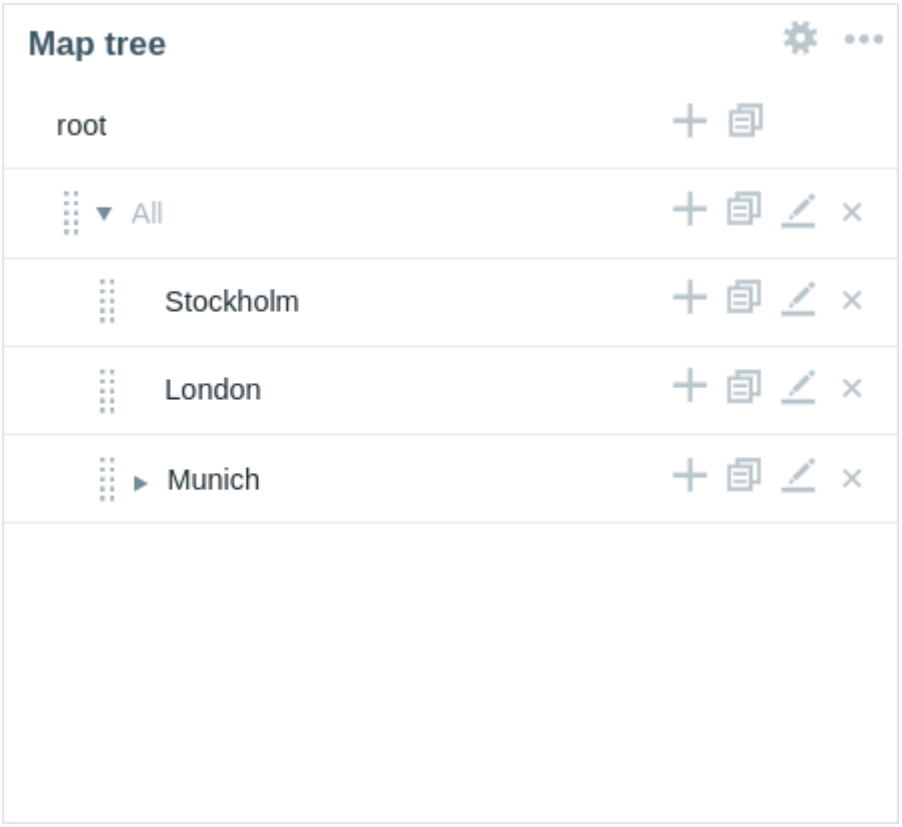


Oprócz parametrów wspólnych dla wszystkich widżetów możesz ustawić następujące opcje specyficzne:

Pokaż niedostępne mapy	Zaznacz to pole wyboru, aby wyświetlać mapy, do których użytkownik nie ma uprawnień odczytu. Niedostępne mapy w drzewie nawigacji będą wyświetlane z wyszarzoną ikoną. Zwróć uwagę, że jeśli to pole wyboru jest zaznaczone, dostępne submaps są wyświetlane nawet wtedy, gdy mapa poziomu nadrzędnego jest niedostępna. Jeśli pole nie jest zaznaczone, dostępne submaps niedostępnej mapy nadrzędnej nie będą wyświetlane w ogóle. Liczba problemów jest obliczana na podstawie dostępnych map i dostępnych elementów mapy.

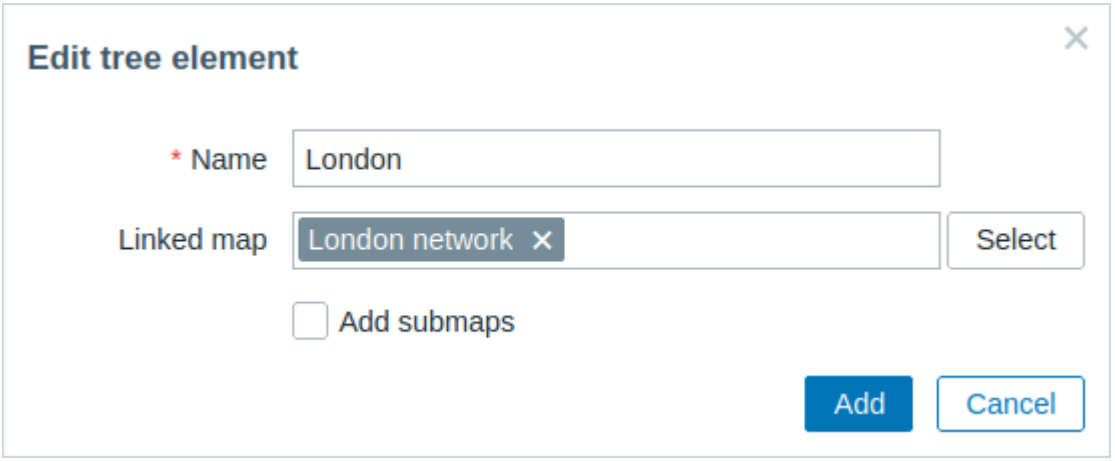
Elementy drzewa nawigacji są wyświetlane na liście. Możesz:

- przeciągnąć element (wraz z jego elementami podrzędnymi) w nowe miejsce na liście;
- rozwinąć lub zwinąć element, aby wyświetlić lub ukryć jego elementy podrzędne;
- dodać element podrzędny (z podlinkowaną mapą lub bez niej) do elementu;
- dodać wiele elementów podrzędnych (z podlinkowanymi mapami) do elementu;
- edytować element;
- usunąć element (wraz z jego elementami podrzędnymi).



Konfiguracja elementu

Aby skonfigurować element drzewa nawigacji, dodaj nowy element lub edytuj istniejący element.



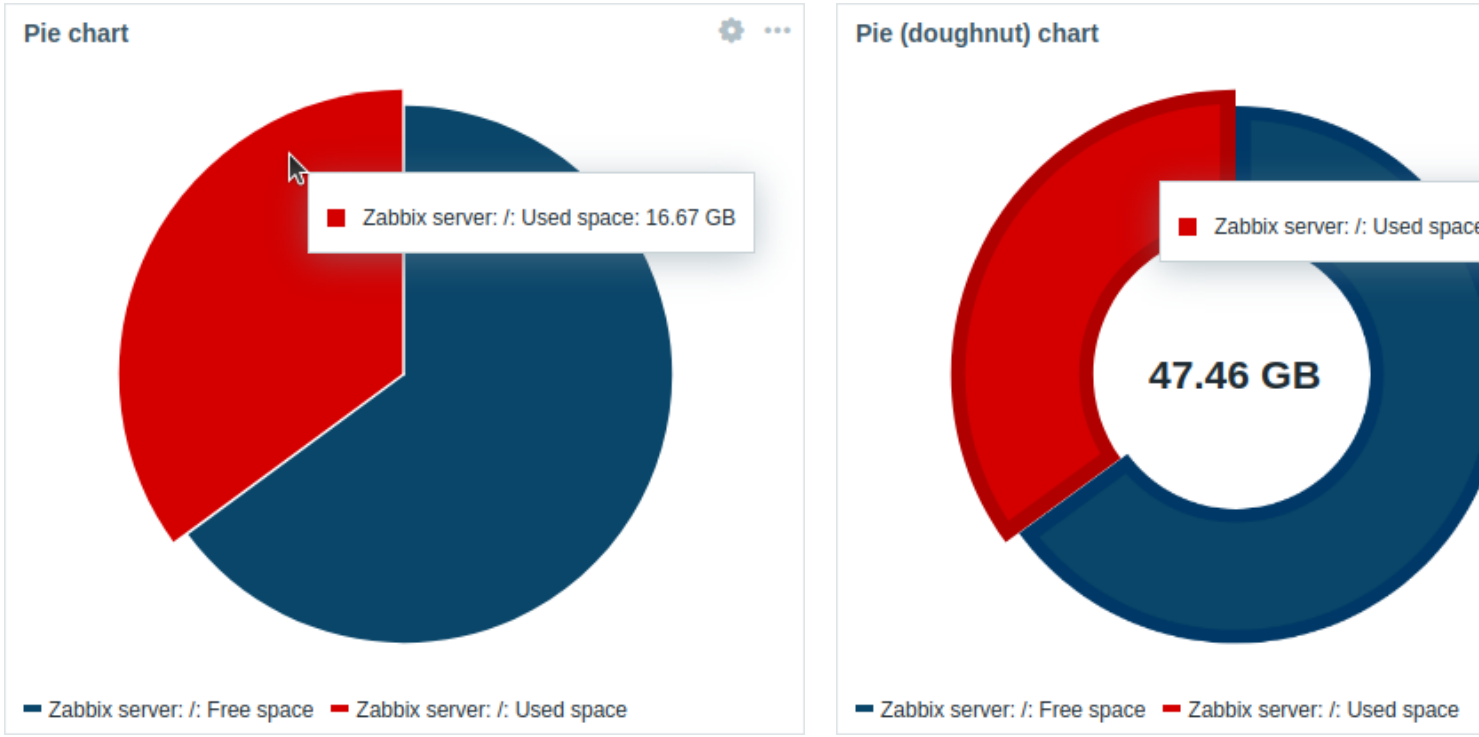
Dostępne są następujące parametry konfiguracji elementu drzewa nawigacji:

Nazwa	Wprowadź nazwę elementu drzewa nawigacji.
Powiązana mapa	Wybierz mapę, którą chcesz powiązać z elementem drzewa nawigacji. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy mapy zostanie wyświetlona rozwijana lista pasujących map.
Dodaj podmapy	Zaznacz to pole wyboru, aby dodać podmapy powiązanej mapy jako elementy podrzędne elementu drzewa nawigacji.

21 Wykres kołowy

Przegląd

Widżet *Wykres kołowy* wyświetla numeryczne dane pozycji w postaci wektorowego wykresu kołowego lub pierścieniowego. Ten widżet może pomóc w wizualizacji, w jaki sposób pozycje lub hosty wpływają na cały zbiór danych.

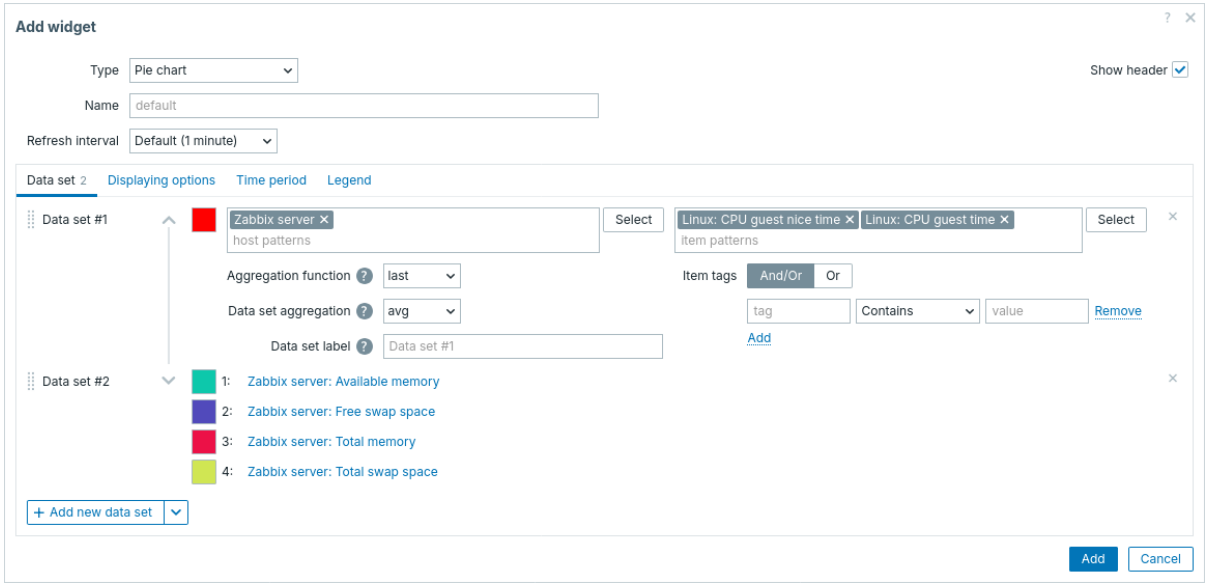


Po najechaniu kursorem wskazany sektor rozszerza się i wyświetla swoją legendę; kliknięcie sektora powoduje, że pozostaje on rozszerzony, a jego legenda widoczna do momentu zamknięcia.

Informacje wyświetlane w widżecie *Wykres kołowy* można pobrać jako obraz PNG, wybierając opcję *Pobierz obraz* w menu widżetu.

Konfiguracja

Aby skonfigurować, wybierz *Pie chart* jako typ:



Zestaw danych

Zakładka **Zestaw danych** umożliwia wybór danych dla wykresu kołowego poprzez dodawanie zestawów danych. Można dodać dwa typy zestawów danych:

- *Wzorce pozycji* - wyświetlane są dane z pasujących pozycji. Możesz wybrać pojedynczy kolor bazowy lub wybrać wiersz palety, aby przypisać odrębne kolory do każdej dopasowanej pozycji.
- *Lista pozycji* - wyświetlane są dane z wybranych pozycji. Możesz wybrać kolor każdej pozycji indywidualnie za pomocą selektora.

Domyślnie dodawany jest zestaw danych *Wzorce pozycji*.

Zestaw danych	Dla zestawu danych **Wzorce pozycji**: Wybierz lub wprowadź wzorce hosta i pozycji; dane pozycji pasujących do wprowadzonych wzorców będą wyświetlane na wykresie kołowym; można wyświetlić maksymalnie 50 pozycji. Do wyboru można używać wzorców wieloznacznych (na przykład ∗ zwróci wyniki pasujące do zera lub większej liczby znaków). Aby określić wzorzec wieloznaczny, wprowadź ciąg ręcznie i naciśnij *Enter*. Symbol wieloznaczny jest zawsze interpretowany, dlatego nie można na przykład dodać indywidualnie pozycji o nazwie *item**, jeśli istnieją inne pasujące pozycje (na przykład *item2*, *item3*). Określenie wzorców hosta i pozycji jest obowiązkowe dla zestawów danych „Wzorce pozycji”. Zobacz także: Szczegóły konfiguracji zestawu danych. Dla zestawu danych **Lista pozycji**: Wybierz pozycje dla wykresu kołowego, klikając przycisk *Dodaj pozycję*. Lista rozwijana *Typ* po nazwie pozycji umożliwia wybór typu wyświetlania dla każdej pozycji: **Normalny** - wartość pozycji jest przedstawiana proporcjonalnie na wykresie kołowym (domyślnie); **Łącznie** - wartość pozycji zajmuje cały wykres kołowy. Pamiętaj, że na jeden wykres kołowy może przypadać tylko jedna pozycja typu „Łącznie” i zostanie ona umieszczona jako pierwsza w legendzie wykresu kołowego. Jeśli pozycja jest ustawiona jako „Łącznie”, parametr *Agregacja zestawu danych* (patrz poniżej) zostanie wyłączony i ustawiony na „nieużywane”. Możesz także wybrać zgodne widgety jako źródło danych dla pozycji, klikając przycisk *Dodaj widget*. Do widgetów mają zastosowanie te same opcje, co do pojedynczych pozycji. Określenie pozycji lub widgetów jest obowiązkowe dla zestawów danych „Lista pozycji”. Zobacz także: Szczegóły konfiguracji zestawu danych. Pamiętaj, że dozwolone są tylko numeryczne typy pozycji. Podczas konfigurowania widgetu na pulpicie szablonu parametr do określania wzorców hosta nie jest dostępny, a parametr do określania listy pozycji pozwala wybrać tylko pozycje skonfigurowane w szablonie.

Funkcja agregacji	Określ, której funkcji agregacji użyć dla każdej pozycji w zestawie danych: **min** - wyświetl najmniejszą wartość; **max** - wyświetl największą wartość; **avg** - wyświetl wartość średnią; **sum** - wyświetl sumę wartości; **count** - wyświetl liczbę wartości; **first** - wyświetl pierwszą wartość; **last** - wyświetl ostatnią wartość (domyślnie). Agregacja umożliwia wyświetlenie zagregowanej wartości dla przedziału (5 minut, godzina, dzień) wybranego w zakładce *Okres czasu* lub używanego dla całego pulpitu.
Agregacja zestawu danych	Określ, której funkcji agregacji użyć dla całego zestawu danych: **not used** - bez agregacji, pozycje są wyświetlane oddzielnie (domyślnie); **min** - wyświetl najmniejszą wartość; **max** - wyświetl największą wartość; **avg** - wyświetl wartość średnią; **sum** - wyświetl sumę wartości; **count** - wyświetl liczbę wartości. Agregacja umożliwia wyświetlenie zagregowanej wartości dla przedziału (5 minut, godzina, dzień) wybranego w zakładce *Okres czasu* lub używanego dla całego pulpitu.
Etykieta zestawu danych	Określ niestandardową etykietę dla zestawu danych. Etykieta jest wyświetlana w konfiguracji zestawu danych oraz w legendzie wykresu kołowego (dla zagregowanych zestawów danych). Wszystkie zestawy danych są numerowane, także te z określoną *Etykietą zestawu danych*. Jeśli etykieta nie zostanie określona, zestaw danych zostanie oznaczony automatycznie zgodnie ze swoim numerem (np. „Zestaw danych #2”, „Zestaw danych #3” itd.). Numeracja zestawów danych jest przeliczana po zmianie kolejności/przeciągnięciu zestawów danych. Etykiety zestawów danych, które są zbyt długie, zostaną skrócone, aby zmieściły się w miejscu wyświetlania (np. „Liczba proc...”).
Tagi pozycji	Określ tagi, aby filtrować pozycje wyświetlane w widżecie. Możliwe jest zarówno uwzględnianie, jak i wykluczanie określonych tagów oraz wartości tagów. Można ustawić kilka warunków. Dopasowanie nazw tagów zawsze uwzględnia wielkość liter. Dla każdego warunku dostępnych jest kilka operatorów: **Exists** - uwzględnij określone nazwy tagów; **Equals** - uwzględnij określone nazwy i wartości tagów (z uwzględnieniem wielkości liter); **Contains** - uwzględnij określone nazwy tagów, których wartości zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter); **Does not exist** - wyklucz określone nazwy tagów; **Does not equal** - wyklucz określone nazwy i wartości tagów (z uwzględnieniem wielkości liter); **Does not contain** - wyklucz określone nazwy tagów, których wartości zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter). Dostępne są dwa typy obliczania warunków: **And/Or** - wszystkie warunki muszą być spełnione, a warunki mające tę samą nazwę tagu będą grupowane warunkiem Or; **Or** - wystarczy spełnienie jednego warunku.

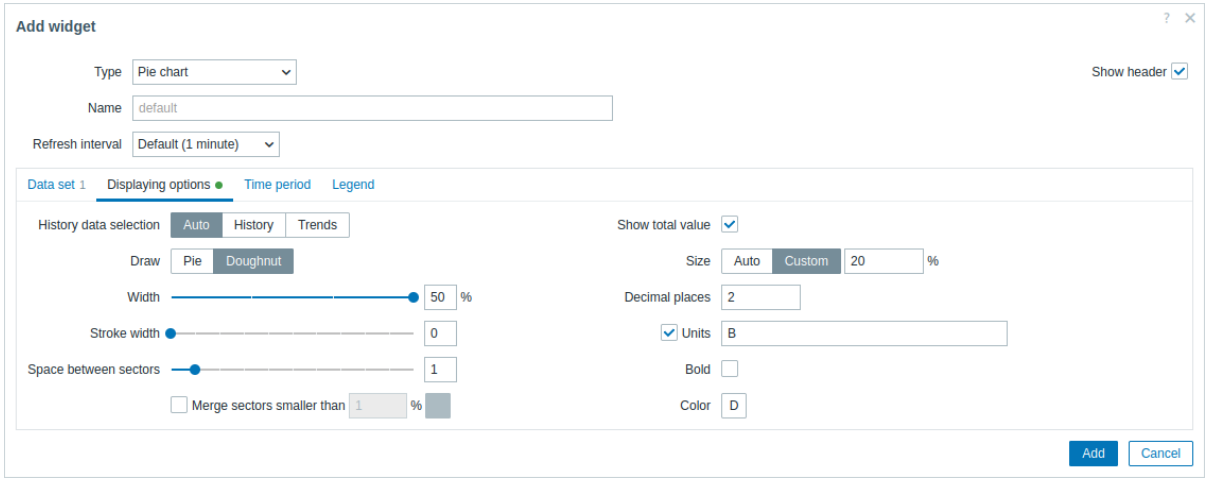
Szczegóły konfiguracji zestawu danych

Istniejące zestawy danych są wyświetlane na liście. Możesz zmieniać ich kolejność, rozwijać/zwijać, zmieniać kolory oraz klonować te zestawy danych.

Więcej informacji można znaleźć w sekcji dotyczącej szczegółów konfiguracji zestawu danych widżetu *Graph*. Te szczegóły mają również zastosowanie do widżetu *Pie chart*.

Opcje wyświetlania

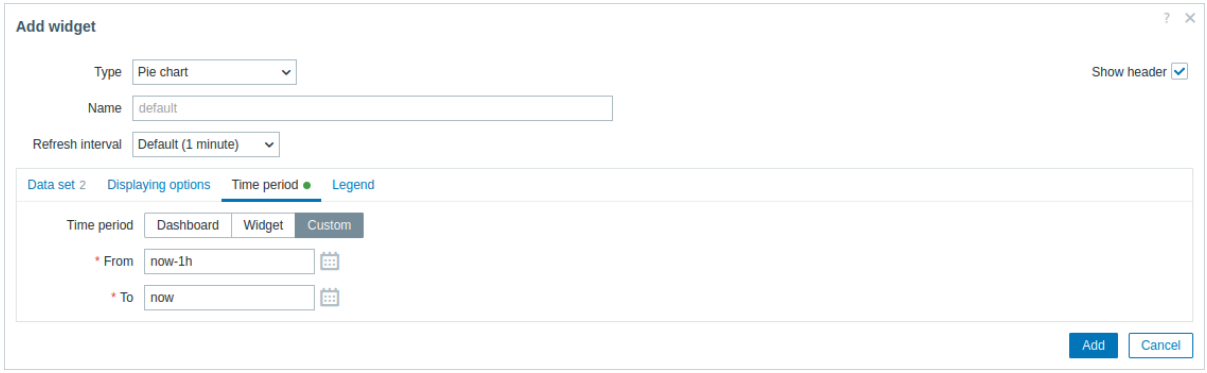
Zakładka **Opcje wyświetlania** umożliwia zdefiniowanie opcji wyboru danych historycznych i wizualizacji dla wykresu kołowego:



Wybór danych historycznych	Wybierz źródło danych: **Auto** - dane są pobierane zgodnie z klasycznym algorytmem (domyślnie); **Historia** - dane z historii; **Trendy** - dane z trendów.
Rysuj	Wybierz styl wizualizacji wykresu kołowego: **Kołowy** - pełny wykres kołowy (sektory zajmują 100% promienia); **Pierścieniowy** - wykres kołowy z pustym okręgiem pośrodku (sektory zajmują do 50% promienia).
Odstęp między sektorami	Wybierz rozmiar odstępu (w jednostkach od 0 do 10) między sektorami (domyślnie „1”).
Scal sektory mniejsze niż N%	Zaznacz pole wyboru, aby scalić sektory mniejsze niż N%. Po włączeniu wybierz kolor dla scalonych sektorów oraz próg procentowy (N) dla scalania małych sektorów.
Styl rysowania: ***Pierścieniowy***	
Szerokość	Wybierz szerokość wykresu pierścieniowego: 20, 30, 40 lub 50% (domyślnie) promienia.
Szerokość obramowania	Wybierz szerokość obramowania sektora wykresu pierścieniowego (0-10).
Pokaż wartość całkowitą	Zaznacz pole wyboru, aby wyświetlić wartość całkowitą pośrodku wykresu pierścieniowego.
Rozmiar	Wybierz opcję rozmiaru dla wartości całkowitej: **Auto** - rozmiar tekstu jest dobierany automatycznie, aby czytelnie mieścił się w środku wykresu pierścieniowego; **Własny** - określ rozmiar tekstu jako procent wysokości całego widżetu.
Miejsca po przecinku	Określ liczbę miejsc po przecinku dla wartości całkowitej (0-6).
Jednostki	Określ jednostki dla wartości całkowitej.
Pogrubienie	Zaznacz pole wyboru, aby wyświetlić wartość całkowitą pogrubioną czcionką.
Kolor	Wybierz kolor dla wartości całkowitej.

Okres czasu

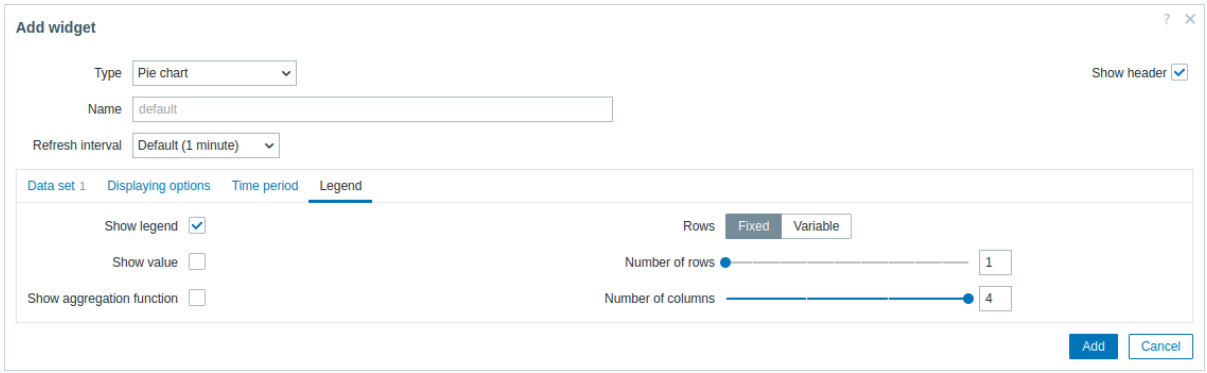
Zakładka **Okres czasu** umożliwia ustawienie niestandardowego okresu czasu dla ustawień agregacji wykresu kołowego:



Okres czasu	Wybierz źródło danych dla okresu czasu: **Pulpit** - użyj selektora okresu czasu pulpitu; **Widget** - użyj kompatybilnego widgetu (ustawionego w parametrze *Widget*); **Niestandardowy** - użyj niestandardowego okresu czasu określonego w parametrach *Od* i *Do*; jeśli jest ustawiony, w prawym górnym rogu widgetu będzie wyświetlana ikona zegara, wskazująca ustawiony czas po najechaniu kursorem. Zwróć uwagę, że niezależnie od konfiguracji *Okres czasu* widgetu, kompatybilne widgety nadal mogą używać go jako źródła danych dla okresu czasu.
Widget	Wprowadź lub wybierz kompatybilny widget (*Wykres*, *Wykres (klasyczny)*, *Prototyp wykresu*) jako źródło danych dla okresu czasu. Ten parametr jest dostępny, jeśli *Okres czasu* jest ustawiony na „Widget”.
Od	Wprowadź lub wybierz początek okresu czasu. Obsługiwana jest składnia czasu względnego (`now`, `now/d`, `now/w-1w` itd.). Ten parametr jest dostępny, jeśli *Okres czasu* jest ustawiony na „Niestandardowy”.
Do	Wprowadź lub wybierz koniec okresu czasu. Obsługiwana jest składnia czasu względnego (`now`, `now/d`, `now/w-1w` itd.). Ten parametr jest dostępny, jeśli *Okres czasu* jest ustawiony na „Niestandardowy”.

Legenda

Zakładka **Legenda** umożliwia dostosowanie legendy wykresu kołowego:

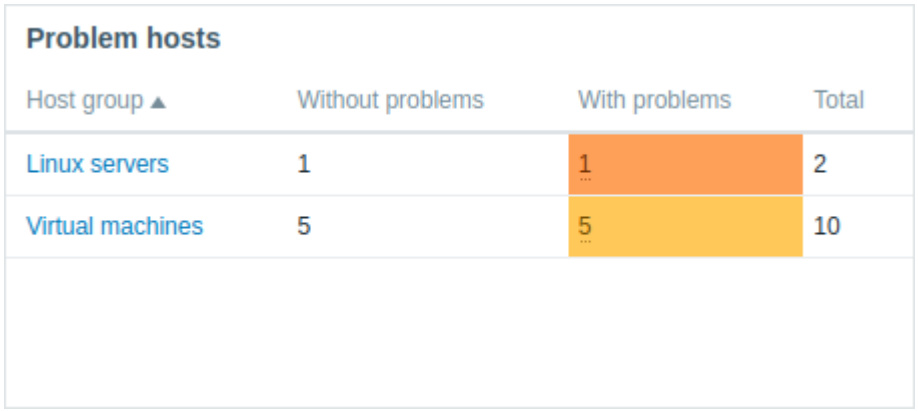


Pokaż legendę	Odznacz to pole wyboru, aby ukryć legendę na wykresie kołowym (domyślnie zaznaczone).
Pokaż wartość	Zaznacz to pole wyboru, aby wyświetlić wartość pozycji w legendzie.
Pokaż funkcję agregacji	Zaznacz to pole wyboru, aby wyświetlić funkcję agregacji w legendzie.
Wiersze	Wybierz tryb wyświetlania wierszy legendy: **Stałe** — liczba wyświetlanych wierszy jest określana przez wartość parametru *Liczba wierszy*; **Zmienne** — liczba wyświetlanych wierszy jest określana przez liczbę skonfigurowanych pozycji, bez przekraczania wartości parametru *Maksymalna liczba wierszy*.
Liczba wierszy/ Maksymalna liczba wierszy	Jeśli dla parametru *Wiersze* ustawiono wartość „Stałe”, określ liczbę wyświetlanych wierszy legendy (1-10). Jeśli dla parametru *Wiersze* ustawiono wartość „Zmienne”, określ maksymalną liczbę wyświetlanych wierszy legendy (1-10).
Liczba kolumn	Określ liczbę wyświetlanych kolumn legendy (1-4). Ten parametr jest dostępny, jeśli opcja *Pokaż wartość* jest odznaczona.

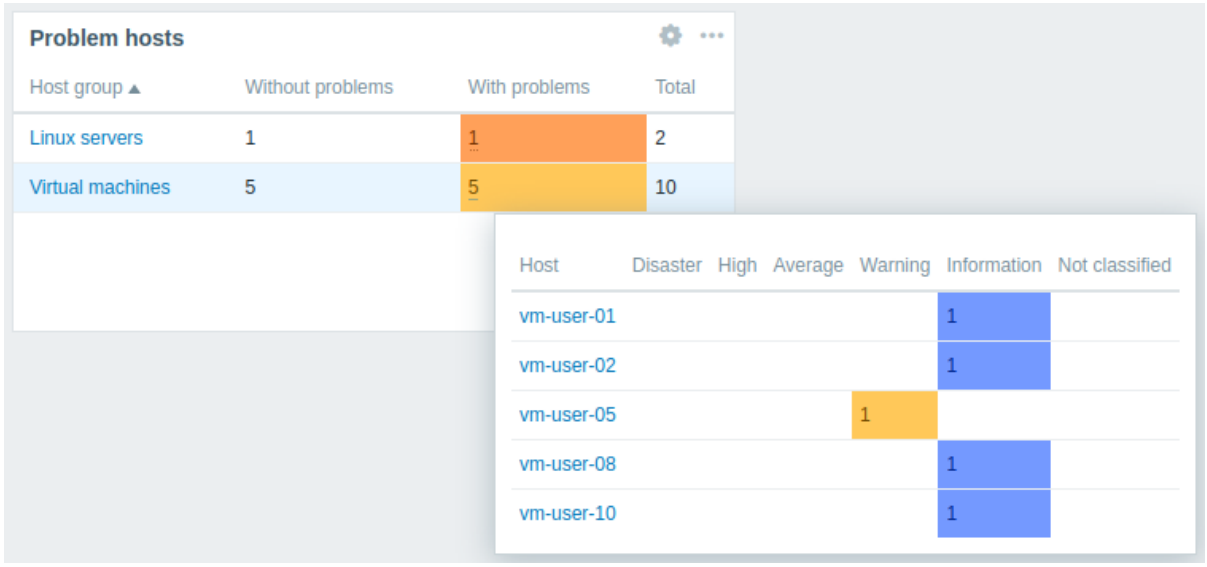
22 Problematyczne hosty

Przegląd

Widżet *Hosty z problemami* wyświetla liczbę problemów przyczynowych dla każdej grupy hostów oraz pokazuje najwyższy poziom ważności problemu w każdej grupie. Umożliwia filtrowanie problemów według różnych parametrów (grupy hostów, hosty, nazwy problemów itp.).

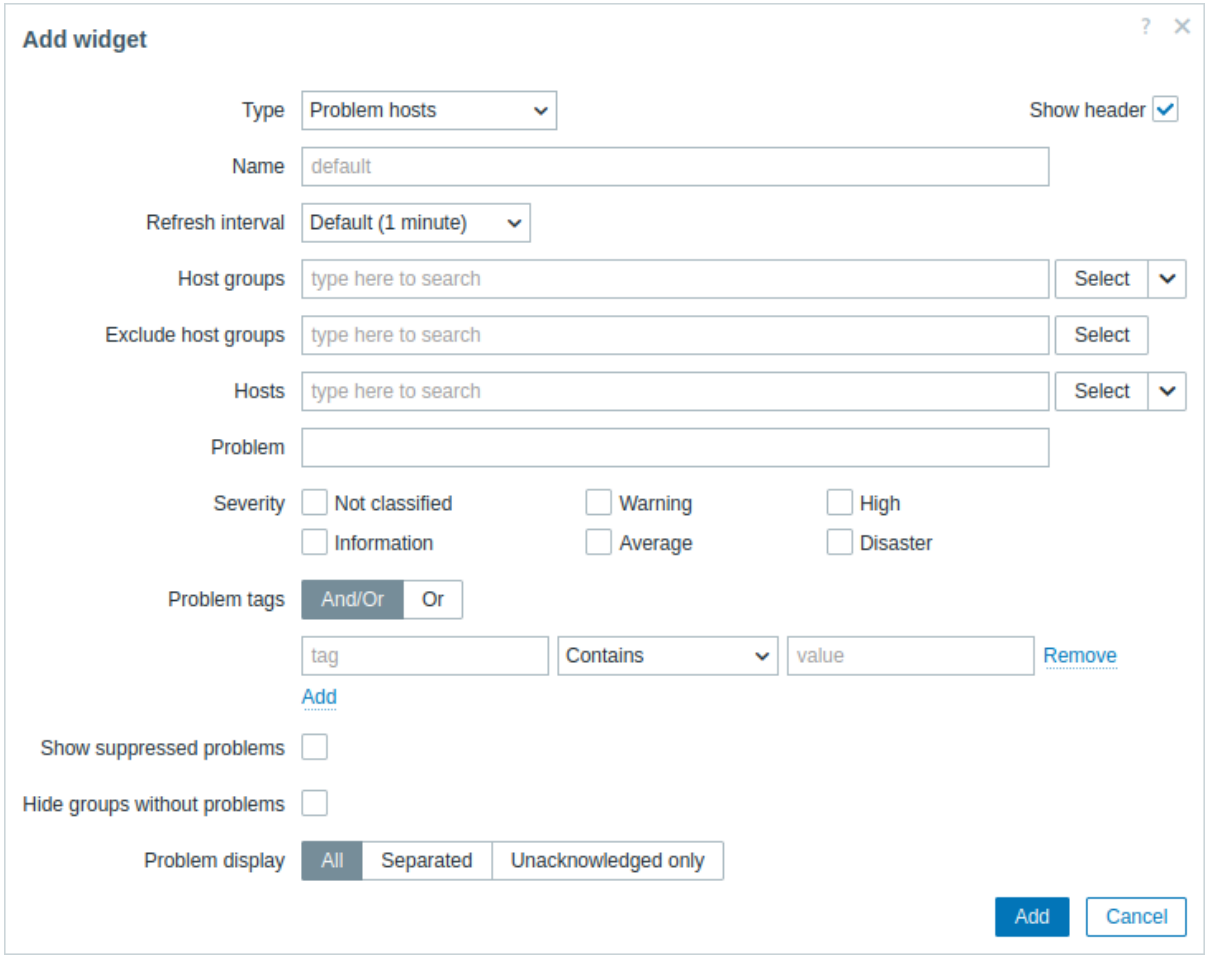


Po najechaniu kursorem na liczbę problemów wyświetlana jest lista hostów z problemami:



Konfiguracja

Aby skonfigurować, wybierz *Problem hosts* jako typ:



Oprócz parametrów wspólnych dla wszystkich widżetów, możesz ustawić następujące opcje specyficzne:

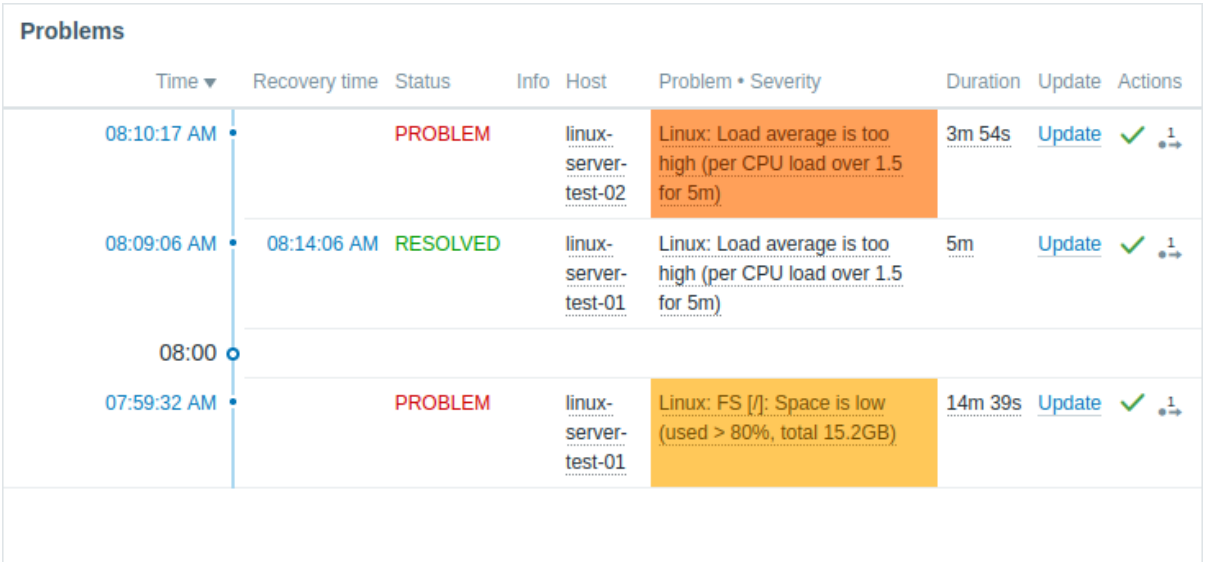
Host groups	Wybierz grupy hostów, które mają być wyświetlane w widżecie. Alternatywnie wybierz zgodny widżet jako źródło danych dla grup hostów. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy grupy zostanie wyświetlona rozwijana lista pasujących grup. Określenie nadrzędnej grupy hostów powoduje automatyczne wybranie wszystkich zagnieżdżonych grup hostów. Dane hostów z tych grup hostów będą wyświetlane w widżecie; jeśli nie zostaną wprowadzone żadne grupy hostów, wyświetlone zostaną wszystkie grupy hostów. Ten parametr nie jest dostępny podczas konfigurowania widżetu na pulpicie szablonu.
Exclude host groups	Wybierz grupy hostów, które mają zostać ukryte w widżecie. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy grupy zostanie wyświetlona rozwijana lista pasujących grup. Określenie nadrzędnej grupy hostów powoduje automatyczne wybranie wszystkich zagnieżdżonych grup hostów. Dane hostów z tych grup hostów nie będą wyświetlane w widżecie. Na przykład hosty 001, 002, 003 mogą należeć do Grupy A, a hosty 002, 003 również do Grupy B. Jeśli jednocześnie wybierzemy *show* dla Grupy A i *exclude* dla Grupy B, na pulpicie zostaną wyświetlone tylko dane hosta 001. Ten parametr nie jest dostępny podczas konfigurowania widżetu na pulpicie szablonu.
Hosts	Wybierz hosty, które mają być wyświetlane w widżecie. Alternatywnie wybierz zgodny widżet lub pulpit jako źródło danych dla hostów. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy hosta zostanie wyświetlona rozwijana lista pasujących hostów. Jeśli nie zostaną wprowadzone żadne hosty, wyświetlone zostaną wszystkie hosty. Ten parametr nie jest dostępny podczas konfigurowania widżetu na pulpicie szablonu.
Problem	Możesz ograniczyć liczbę hostów z problemami wyświetlanych według nazwy problemu. Jeśli wpiszesz tutaj ciąg znaków, wyświetlone zostaną tylko te hosty, które mają problemy, których nazwa zawiera podany ciąg. Makra nie są rozwijane.

Severity	Zaznacz poziomy ważności problemów, aby filtrować problemy wyświetlane w widżecie. Jeśli nie zostanie zaznaczony żaden poziom ważności, wyświetlone zostaną wszystkie problemy.
Problem tags	Określ tagi problemów, aby ograniczyć liczbę problemów wyświetlanych w widżecie. Możliwe jest zarówno uwzględnianie, jak i wykluczanie określonych tagów oraz wartości tagów. Można ustawić kilka warunków. Dopasowanie nazw tagów zawsze uwzględnia wielkość liter. Dla każdego warunku dostępnych jest kilka operatorów: **Exists** - uwzględnij określone nazwy tagów; **Equals** - uwzględnij określone nazwy tagów i wartości (z uwzględnieniem wielkości liter); **Contains** - uwzględnij określone nazwy tagów, których wartości zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter); **Does not exist** - wyklucz określone nazwy tagów; **Does not equal** - wyklucz określone nazwy tagów i wartości (z uwzględnieniem wielkości liter); **Does not contain** - wyklucz określone nazwy tagów, których wartości zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter). Dla warunków dostępne są dwa typy obliczeń: **And/Or** - wszystkie warunki muszą być spełnione, a warunki mające tę samą nazwę tagu będą grupowane przez warunek *Or*; **Or** - wystarczy spełnienie jednego warunku.
Show suppressed problems	Zaznacz pole wyboru, aby wyświetlać problemy, które w przeciwnym razie byłyby tłumione (niewyświetlane) z powodu konserwacji hosta.
Hide groups without problems	Zaznacz opcję *Hide groups without problems*, aby ukryć w widżecie dane z grup hostów bez problemów. Ten parametr nie jest dostępny podczas konfigurowania widżetu na pulpicie szablonu.
Problem display	Wyświetl liczbę problemów jako: **All** - zostanie wyświetlona pełna liczba problemów; **Separated** - liczba niepotwierdzonych problemów zostanie wyświetlona oddzielnie jako część całkowitej liczby problemów; **Unacknowledged only** - zostanie wyświetlona tylko liczba niepotwierdzonych problemów.

23 Problemy

Przegląd

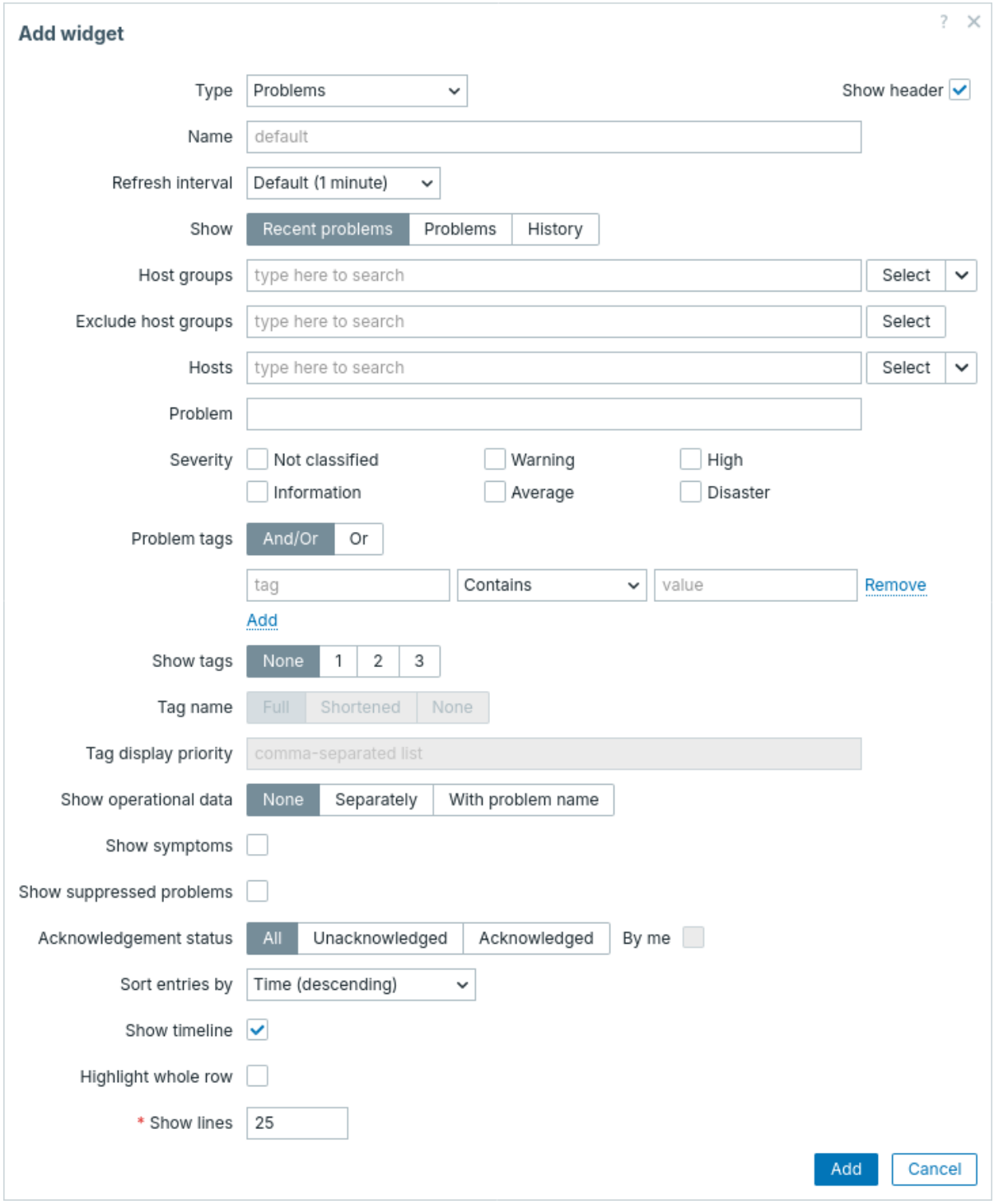
Widżet *Problemy* wyświetla bieżące problemy filtrowane według różnych parametrów (grupy hostów, hosty, nazwy problemów itp.), zapewniając przejrzysty widok tego, co wymaga uwagi.



Wyświetla te same dane co *Monitoring* > *Problemy* i może wyświetlić do 1000 rekordów.

Konfiguracja

Aby skonfigurować, wybierz *Problemy* jako typ:



Możesz ograniczyć liczbę problemów wyświetlanych w widżecie na różne sposoby — według statusu problemu, nazwy problemu, ważności, grupy hostów, hosta, tagu zdarzenia, statusu potwierdzenia itd.

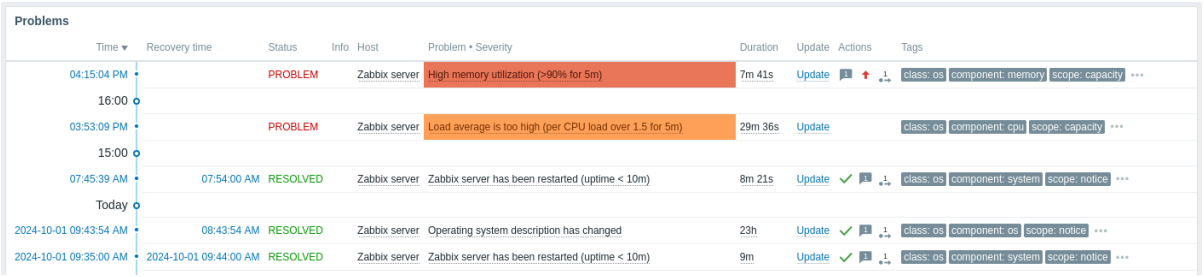
Oprócz parametrów wspólnych dla wszystkich widżetów możesz ustawić następujące opcje specyficzne:

Pokaż	Filtruj według statusu problemu: **Ostatnie problemy** — wyświetlane są nierozwiązane i ostatnio rozwiązane problemy (domyślnie); **Problemy** — wyświetlane są nierozwiązane problemy; **Historia** — wyświetlana jest historia wszystkich zdarzeń.

Grupy hostów	Wybierz grupy hostów, których problemy mają być wyświetlane w widżecie. Alternatywnie wybierz zgodny widżet jako źródło danych dla grup hostów. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy grupy zostanie wyświetlona rozwijana lista pasujących grup. Wskazanie nadrzędnej grupy hostów domyślnie wybiera wszystkie zagnieżdżone grupy hostów. Problemy z tych grup hostów będą wyświetlane w widżecie; jeśli nie zostaną wprowadzone żadne grupy hostów, wyświetlane będą problemy ze wszystkich grup hostów. Ten parametr nie jest dostępny podczas konfigurowania widżetu na pulpicie szablonu.
Wyklucz grupy hostów	Wybierz grupy hostów, których problemy mają być ukryte w widżecie. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy grupy zostanie wyświetlona rozwijana lista pasujących grup. Wskazanie nadrzędnej grupy hostów domyślnie wybiera wszystkie zagnieżdżone grupy hostów. Problemy z tych grup hostów nie będą wyświetlane w widżecie. Na przykład hosty 001, 002, 003 mogą należeć do Grupy A, a hosty 002, 003 również do Grupy B. Jeśli jednocześnie wybierzemy *pokaż* Grupę A i *wyklucz* Grupę B, w widżecie będą wyświetlane tylko problemy hosta 001. Ten parametr nie jest dostępny podczas konfigurowania widżetu na pulpicie szablonu.
Hosty	Wybierz hosty, których problemy mają być wyświetlane w widżecie. Alternatywnie wybierz zgodny widżet lub pulpit jako źródło danych dla hostów. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy hosta zostanie wyświetlona rozwijana lista pasujących hostów. Jeśli nie zostaną wprowadzone żadne hosty, wyświetlane będą problemy wszystkich hostów. Ten parametr nie jest dostępny podczas konfigurowania widżetu na pulpicie szablonu.
Problem	Możesz ograniczyć liczbę wyświetlanych problemów według ich nazwy. Jeśli wpiszesz tutaj ciąg znaków, wyświetlane będą tylko te problemy, których nazwa zawiera podany ciąg. Makra nie są rozwijane.
Ważność	Zaznacz poziomy ważności problemów, aby filtrować problemy wyświetlane w widżecie. Jeśli nie zostanie zaznaczona żadna ważność, wyświetlane będą wszystkie problemy.
Tagi problemu	Określ tagi problemu, aby ograniczyć liczbę problemów wyświetlanych w widżecie. Możliwe jest zarówno uwzględnianie, jak i wykluczanie określonych tagów oraz wartości tagów. Można ustawić kilka warunków. Dopasowanie nazw tagów zawsze uwzględnia wielkość liter. Dla każdego warunku dostępnych jest kilka operatorów: **Istnieje** — uwzględnij określone nazwy tagów; **Równa się** — uwzględnij określone nazwy i wartości tagów (z uwzględnieniem wielkości liter); **Zawiera** — uwzględnij określone nazwy tagów, których wartości zawierają podany ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter); **Nie istnieje** — wyklucz określone nazwy tagów; **Nie równa się** — wyklucz określone nazwy i wartości tagów (z uwzględnieniem wielkości liter); **Nie zawiera** — wyklucz określone nazwy tagów, których wartości zawierają podany ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter). Dla warunków dostępne są dwa typy obliczeń: **I/Lub** — wszystkie warunki muszą być spełnione, a warunki mające tę samą nazwę tagu będą grupowane warunkiem *Lub*; **Lub** — wystarczy spełnienie jednego warunku. Po zastosowaniu filtrowania określone tutaj tagi będą wyświetlane przy problemie jako pierwsze, chyba że zostanie to nadpisane przez listę *Priorytet wyświetlania tagów* (patrz poniżej).
Pokaż tagi	Wybierz liczbę wyświetlanych tagów: **Brak** — brak kolumny *Tagi*; **1** — kolumna *Tagi* zawiera jeden tag; **2** — kolumna *Tagi* zawiera dwa tagi; **3** — kolumna *Tagi* zawiera trzy tagi. Aby zobaczyć wszystkie tagi problemu, najedź kursorem myszy na ikonę trzech kropek.
Nazwa tagu	Wybierz tryb wyświetlania nazwy tagu: **Pełna** — nazwy i wartości tagów są wyświetlane w całości; **Skrócona** — nazwy tagów są skracane do 3 znaków, ale wartości tagów są wyświetlane w całości; **Brak** — wyświetlane są tylko wartości tagów; bez nazw.

Priorytet wyświetlania tagów	Wprowadź priorytet wyświetlania tagów dla problemu jako listę tagów oddzielonych przecinkami. Należy używać tylko nazw tagów, bez wartości. Przykład: `Services,Applications,Application` Tagi z tej listy będą zawsze wyświetlane jako pierwsze, zastępując naturalną kolejność alfabetyczną.
Pokaż dane operacyjne	Wybierz tryb wyświetlania danych operacyjnych: **Brak** — dane operacyjne nie są wyświetlane; **Oddzielnie** — dane operacyjne są wyświetlane w osobnej kolumnie; **Z nazwą problemu** — dołącz dane operacyjne do nazwy problemu, używając nawiasów dla danych operacyjnych.
Pokaż symptomy	Zaznacz pole wyboru, aby wyświetlać w osobnym wierszu problemy sklasyfikowane jako symptomy.
Pokaż wyciszone problemy	Zaznacz pole wyboru, aby wyświetlać problemy, które w przeciwnym razie byłyby wyciszone (niewyświetlane) z powodu konserwacji hosta lub pojedynczego wyciszenia problemu.
Status potwierdzenia	Filtruj, aby wyświetlać wszystkie problemy, tylko niepotwierdzone problemy albo tylko potwierdzone problemy. Zaznacz dodatkowe pole wyboru, aby odfiltrować te problemy, które kiedykolwiek zostały przez Ciebie potwierdzone.
Sortuj wpisy według	Sortuj wpisy według: **Czasu** (malejąco lub rosnąco); **Ważności** (malejąco lub rosnąco); **Nazwy problemu** (malejąco lub rosnąco); **Hosta** (malejąco lub rosnąco). Sortowanie wpisów według **Hosta** (malejąco lub rosnąco) nie jest dostępne podczas konfigurowania widżetu na pulpicie szablonu.
Pokaż oś czasu	Zaznacz pole wyboru, aby wyświetlać wizualną oś czasu.
Podświetl cały wiersz	Zaznacz pole wyboru, aby podświetlić cały wiersz dla nierozwiązanych problemów. Do podświetlenia używany jest kolor ważności problemu. *Podświetl cały wiersz* nie jest dostępne w motywach o wysokim kontraście.
Pokaż wiersze	Określ liczbę wierszy problemów do wyświetlenia.

Korzystanie z widżetu

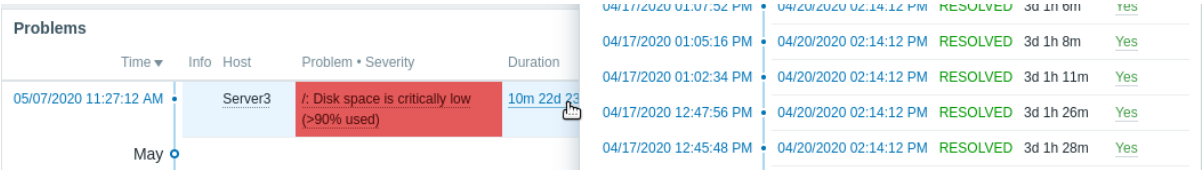


Widżet Problemów oferuje szybki dostęp do dodatkowych informacji:

- Kliknij datę problemu (w kolumnie Czas) lub datę odzyskania (w kolumnie Czas odzyskania), aby wyświetlić szczegóły zdarzenia.
- Jeśli pole Informacje nie jest puste, najedź kursorem na wyświetlaną ikonę, aby zobaczyć dodatkowe szczegóły.
- Kliknij nazwę hosta, aby otworzyć menu hosta.
- Kliknij nazwę problemu, aby otworzyć menu zdarzenia.
- Najedź kursorem na czas trwania problemu lub kliknij go, aby wyświetlić wyskakujące okno zdarzenia problemu.
- Naciśnięcie przycisku Aktualizuj otwiera okno Aktualizacja problemu.
- Najedź kursorem na szarą ikonę strzałki w kolumnie Akcje lub kliknij ją, aby wyświetlić listę wykonanych akcji.

Wyskakujące okno zdarzenia problemu

Wyskakujące okno zdarzenia problemu zawiera listę zdarzeń problemu dla tego wyzwalacza oraz, jeśli zostały zdefiniowane, opis wyzwalacza i klikalny adres URL.



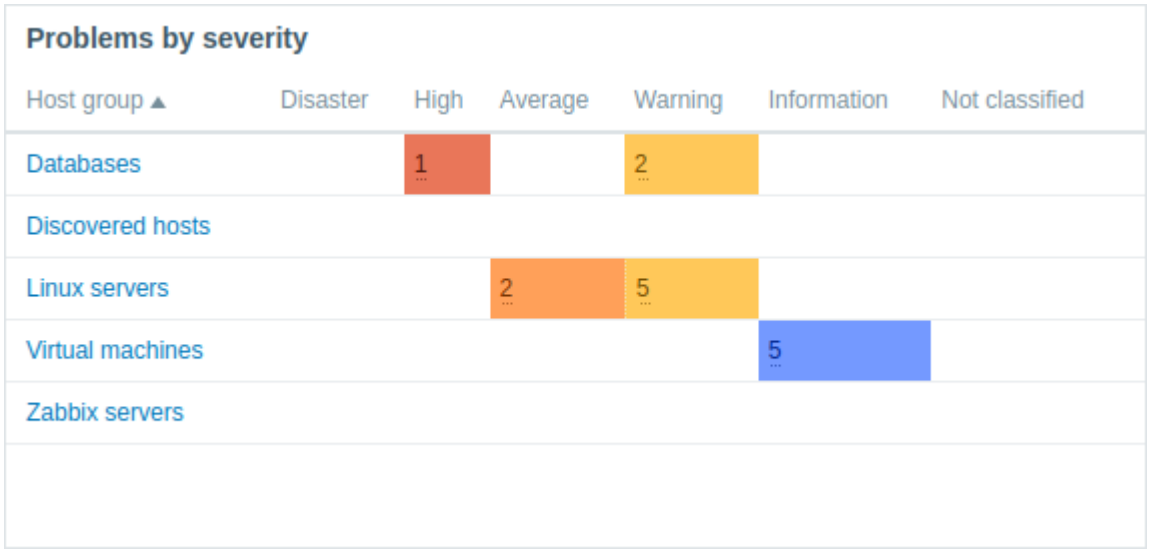
Aby wyświetlić wyskakujące okno zdarzenia problemu:

- Najedź kursorem myszy na czas trwania problemu w kolumnie *Czas trwania* widżetu *Problemy*. Okno zniknie po odsunięciu kursora od czasu trwania.
- Kliknij czas trwania w kolumnie *Czas trwania* widżetu *Problemy*. Okno zniknie dopiero po ponownym kliknięciu czasu trwania.

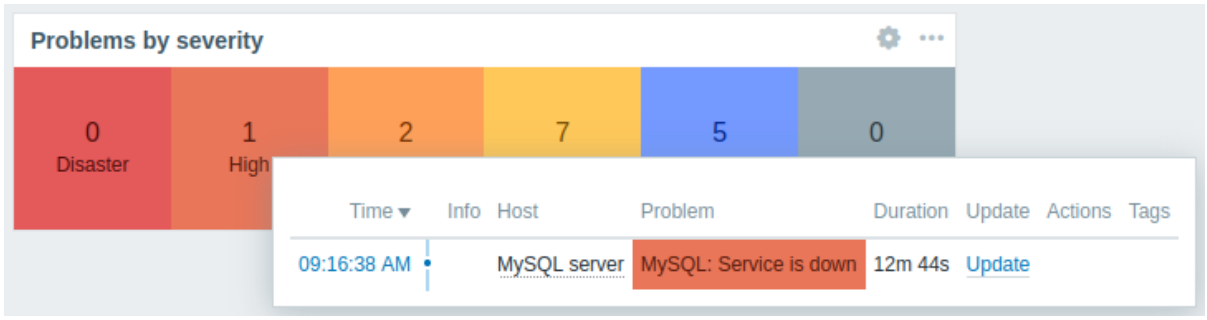
24 Problemy według ważności

Przegląd

Widżet *Problemy według ważności* wyświetla liczbę problemów przyczynowych pogrupowanych według ważności. Umożliwia filtrowanie problemów według różnych parametrów (grupy hostów, hosty, nazwy problemów itp.).

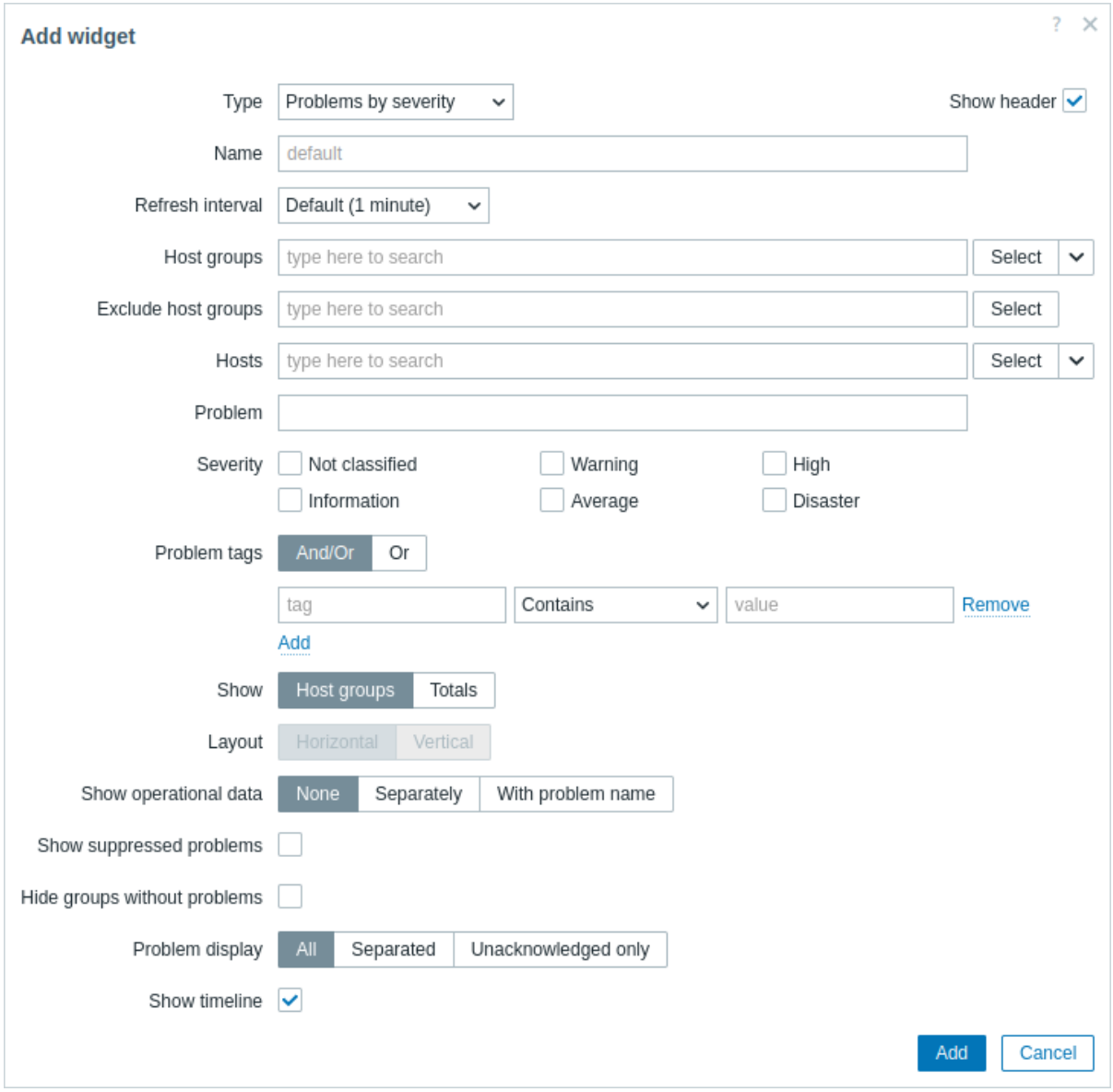


Po najechaniu kursorem na liczbę problemów wyświetlana jest lista powiązanych problemów:



Konfiguracja

Aby skonfigurować widget, wybierz *Problems by severity* jako typ:



Oprócz parametrów wspólnych dla wszystkich widgetów, możesz ustawić następujące opcje specyficzne:

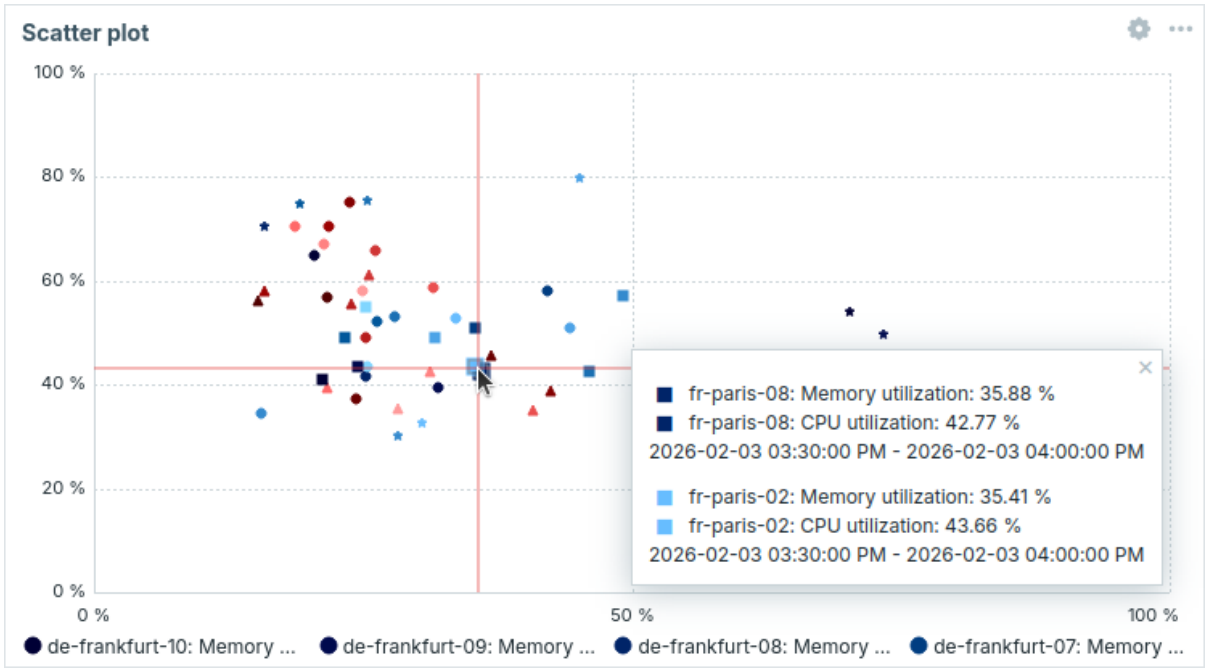
Grupy hostów	Wybierz grupy hostów, które mają być wyświetlane w widżecie. Alternatywnie wybierz zgodny widget jako źródło danych dla grup hostów. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy grupy zostanie wyświetlona rozwijana lista pasujących grup. Określenie nadrzędnej grupy hostów powoduje automatyczne wybranie wszystkich zagnieżdżonych grup hostów. Dane hostów z tych grup hostów będą wyświetlane w widżecie; jeśli nie zostaną wprowadzone żadne grupy hostów, wyświetlone zostaną wszystkie grupy hostów. Ten parametr nie jest dostępny podczas konfigurowania widgetu na pulpicie szablonu.
Wyklucz grupy hostów	Wybierz grupy hostów, które mają zostać ukryte w widżecie. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy grupy zostanie wyświetlona rozwijana lista pasujących grup. Określenie nadrzędnej grupy hostów powoduje automatyczne wybranie wszystkich zagnieżdżonych grup hostów. Dane hostów z tych grup hostów nie będą wyświetlane w widżecie. Na przykład hosty 001, 002, 003 mogą należeć do Grupy A, a hosty 002, 003 również do Grupy B. Jeśli jednocześnie wybierzemy *pokazywanie* Grupy A i *wykluczenie* Grupy B, na pulpicie zostaną wyświetlone tylko dane hosta 001. Ten parametr nie jest dostępny podczas konfigurowania widgetu na pulpicie szablonu.

Hosty	Wybierz hosty, które mają być wyświetlane w widżecie. Alternatywnie wybierz zgodny widget lub pulpit jako źródło danych dla hostów. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy hosta zostanie wyświetlona rozwijana lista pasujących hostów. Jeśli nie zostaną wprowadzone żadne hosty, wyświetlone zostaną wszystkie hosty. Ten parametr nie jest dostępny podczas konfigurowania widgetu na pulpicie szablonu.
Problem	Możesz ograniczyć liczbę hostów z problemami wyświetlanych na podstawie nazwy problemu. Jeśli wpiszesz tutaj ciąg znaków, wyświetlane będą tylko te hosty, których problemy mają w nazwie podany ciąg. Makra nie są rozwijane.
Ważność	Zaznacz poziomy ważności problemów, aby filtrować problemy wyświetlane w widżecie. Jeśli nie zostanie zaznaczony żaden poziom ważności, wyświetlane będą wszystkie problemy.
Tagi problemów	Określ tagi problemów, aby ograniczyć liczbę problemów wyświetlanych w widżecie. Można zarówno uwzględniać, jak i wykluczać określone tagi oraz wartości tagów. Można ustawić kilka warunków. Dopasowanie nazw tagów zawsze uwzględnia wielkość liter. Dla każdego warunku dostępnych jest kilka operatorów: **Exists** - uwzględnij określone nazwy tagów; **Equals** - uwzględnij określone nazwy i wartości tagów (z uwzględnieniem wielkości liter); **Contains** - uwzględnij określone nazwy tagów, których wartości zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter); **Does not exist** - wyklucz określone nazwy tagów; **Does not equal** - wyklucz określone nazwy i wartości tagów (z uwzględnieniem wielkości liter); **Does not contain** - wyklucz określone nazwy tagów, których wartości zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter). Dostępne są dwa typy obliczania warunków: **And/Or** - wszystkie warunki muszą być spełnione, a warunki mające tę samą nazwę tagu będą grupowane operatorem *Or*; **Or** - wystarczy spełnienie jednego warunku.
Pokaż	Wybierz opcję wyświetlania: **Host groups** - wyświetl problemy według grup hostów; **Totals** - wyświetl łączną liczbę problemów dla wszystkich wybranych grup hostów w kolorowych blokach odpowiadających ważności problemu. Ten parametr nie jest dostępny podczas konfigurowania widgetu na pulpicie szablonu, a wyświetlana będzie tylko łączna liczba problemów.
Układ	Wybierz opcję układu: **Horizontal** - kolorowe bloki z sumami będą wyświetlane poziomo; **Vertical** - kolorowe bloki z sumami będą wyświetlane pionowo. Ten parametr jest dostępny, jeśli *Pokaż* jest ustawione na ”Totals”.
Pokaż dane operacyjne	Wyświetl dane operacyjne (zobacz opis *Operational data* w *Monitoring* > *Problems*) jako: **None** - dane operacyjne nie będą wyświetlane **Separately** - dane operacyjne będą wyświetlane w osobnym wierszu **With problem name** - dane operacyjne będą wyświetlane razem z nazwą problemu.
Pokaż wyciszone problemy	Zaznacz pole wyboru, aby wyświetlać problemy, które w przeciwnym razie byłyby wyciszone (niepokazywane) z powodu konserwacji hosta.
Ukryj grupy bez problemów	Zaznacz opcję *Ukryj grupy bez problemów*, aby ukryć w widżecie dane z grup hostów bez problemów. Ten parametr nie jest dostępny podczas konfigurowania widgetu na pulpicie szablonu.
Wyświetlanie problemów	Wyświetl liczbę problemów jako: **All** - zostanie wyświetlona pełna liczba problemów; **Separated** - liczba niepotwierdzonych problemów będzie wyświetlana oddzielnie jako część całkowitej liczby problemów; **Unacknowledged only** - wyświetlana będzie tylko liczba niepotwierdzonych problemów.
Pokaż oś czasu	Zaznacz pole wyboru, aby wyświetlić wizualną oś czasu.

25 Wykres punktowy

Przegląd

Widżet *Scatter plot* wyświetla zależność między dwiema metrykami, nanosząc pojedyncze punkty danych wzdłuż osi X i Y. Pomaga to ujawnić wzorce, skupiska, korelacje i wartości odstające w zbiorze danych.



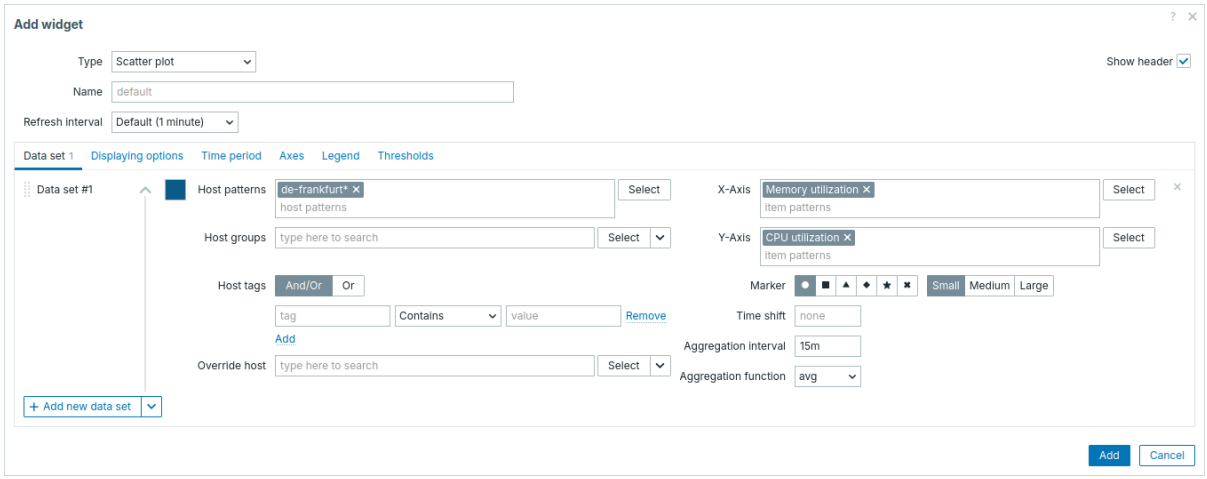
Po najechaniu kursorem na punkt danych wyświetlany jest podpowiedź z listą pozycji z tego punktu danych oraz innych punktów w promieniu 6 px; posortowaną najpierw według wartości osi X wykresu punktowego rosnąco, a następnie według wartości osi Y malejąco.

Wybranie pozycji w podpowiedzi rozgłasza jej dane do innych widżetów.

Informacje wyświetlane w widżecie *Scatter plot* można pobrać jako obraz PNG, wybierając opcję *Download image* w menu widżetu.

Konfiguracja

Aby skonfigurować, wybierz *Scatter plot* jako typ:



Zestaw danych

Zakładka **Zestaw danych** umożliwia wybór danych dla wykresu rozrzutu przez dodawanie zestawów danych. Można dodać dwa typy zestawów danych:

- *Wzorce pozycji* - hosty z pasującymi pozycjami są wyświetlane jako punkty danych. Możesz wybrać jeden kolor bazowy lub wybrać wiersz palety, aby przypisać odrębne kolory każdemu hostowi z dopasowanymi pozycjami.
- *Lista pozycji* - wybrane pozycje są wyświetlane jako punkty danych, gdzie każdy punkt reprezentuje parę pozycji (X i Y). Możesz wybrać kolor każdego zestawu danych indywidualnie z próbnika.

Punkty danych są tworzone tylko dla tych par host/pozycja, które mają co najmniej jedną wartość na obu osiach.

Domyślnie dodawany jest zestaw danych *Wzorce pozycji*.

Zestaw danych	Dla zestawu danych **Wzorce pozycji**: Wybierz lub wprowadź wzorce hostów i pozycji; dane pozycji pasujących do tych wzorców będą wyświetlane na wykresie rozrzutu; może zostać wyświetlonych maksymalnie 100 pozycji (po 50 na każdej osi dla łącznie 50 hostów). Do wyboru można używać wzorców wieloznacznych (na przykład ∗ zwróci wyniki pasujące do zera lub większej liczby znaków). Aby określić wzorzec wieloznaczny, wprowadź ciąg ręcznie i naciśnij *Enter*. Symbol wieloznaczny jest zawsze interpretowany, więc nie jest możliwe dodanie na przykład pozycji o nazwie *item** pojedynczo, jeśli istnieją inne pasujące pozycje (na przykład *item2*, *item3*). Określenie wzorców hostów i pozycji jest obowiązkowe dla zestawów danych „Wzorce pozycji". Zobacz także: Szczegóły konfiguracji zestawu danych. Dla zestawu danych **Lista pozycji**: Wybierz pozycje dla wykresu rozrzutu, klikając przycisk *Dodaj pozycję*. Możesz także wybrać kompatybilne widgety jako źródło danych dla pozycji, klikając przycisk *Dodaj widget*. Określenie pozycji lub widgetów jest obowiązkowe dla zestawów danych „Lista pozycji". Zobacz także: Szczegóły konfiguracji zestawu danych. Należy pamiętać, że dozwolone są tylko numeryczne typy pozycji. Podczas konfigurowania widgetu na pulpicie szablonu parametr do określania wzorców hostów nie jest dostępny, a parametr do określania listy pozycji pozwala wybrać tylko pozycje skonfigurowane w szablonie.
Grupy hostów	Wybierz grupy hostów. Alternatywnie wybierz kompatybilny widget jako źródło danych dla grup hostów. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy grupy zostanie wyświetlona rozwijana lista pasujących grup. Określenie nadrzędnej grupy hostów niejawnie wybiera wszystkie zagnieżdżone grupy hostów. Dane hostów z tych grup hostów będą wyświetlane w widżecie; jeśli nie zostaną wprowadzone żadne grupy hostów, wyświetlane będą wszystkie grupy hostów. Ten parametr jest dostępny tylko dla zestawów danych *Wzorce pozycji* i nie jest dostępny podczas konfigurowania widgetu na pulpicie szablonu.
Tagi hostów	Określ tagi, aby filtrować hosty wyświetlane w widżecie. Możliwe jest zarówno uwzględnianie, jak i wykluczanie określonych tagów oraz wartości tagów. Można ustawić kilka warunków. Dopasowanie nazw tagów zawsze uwzględnia wielkość liter. Dla każdego warunku dostępnych jest kilka operatorów: **Istnieje** - uwzględnij określone nazwy tagów; **Równa się** - uwzględnij określone nazwy tagów i wartości (z uwzględnieniem wielkości liter); **Zawiera** - uwzględnij określone nazwy tagów, w których wartości tagów zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter); **Nie istnieje** - wyklucz określone nazwy tagów; **Nie równa się** - wyklucz określone nazwy tagów i wartości (z uwzględnieniem wielkości liter); **Nie zawiera** - wyklucz określone nazwy tagów, w których wartości tagów zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter). Dostępne są dwa typy obliczeń dla warunków: **And/Or** - wszystkie warunki muszą zostać spełnione, warunki mające tę samą nazwę tagu będą grupowane warunkiem Or; **Or** - wystarczy spełnienie jednego warunku. Ten parametr jest dostępny tylko dla zestawów danych *Wzorce pozycji* i nie jest dostępny podczas konfigurowania widgetu na pulpicie szablonu.
Nadpisz host	Wybierz kompatybilny widget lub selektor hosta pulpitu jako źródło danych dla hostów. Ten parametr nie jest dostępny podczas konfigurowania widgetu na pulpicie szablonu.
Znacznik	Wybierz typ i rozmiar znacznika dla punktów danych hosta w zestawie danych.

Przesunięcie czasu	W razie potrzeby określ przesunięcie czasu. W tym polu możesz używać sufiksów czasu. Dozwolone są wartości ujemne.
Funkcja agregacji	Określ, której funkcji agregacji użyć: **min** - wyświetl najmniejszą wartość; **max** - wyświetl największą wartość; **avg** - wyświetl wartość średnią; **sum** - wyświetl sumę wartości; **count** - wyświetl liczbę wartości (jeśli na obu osiach istnieje co najmniej jedna wartość); **first** - wyświetl pierwszą wartość; **last** - wyświetl ostatnią wartość; **none** - wyświetl wszystkie wartości (bez agregacji). Agregacja umożliwia wyświetlenie zagregowanej wartości dla wybranego przedziału (5 minut, godzina, dzień) zamiast wszystkich wartości. Zobacz także: Agregacja na wykresach.
Interwał agregacji	Określ interwał agregacji wartości. W tym polu możesz używać sufiksów czasu. Wartość liczbowa bez sufiksu będzie traktowana jako liczba sekund. Zwróć uwagę, że jeśli widget jest skonfigurowany do wyświetlania danych historycznych na podstawie trendów (*Wybór danych historycznych* jest ustawiony na *Trendy* lub *Auto*), zaleca się użycie interwału agregacji będącego wielokrotnością 1 godziny (np. 3600, 60m, 1h, 3h itd.). Trendy przechowują zagregowane wartości godzinowe, więc użycie interwału agregacji, który nie jest wielokrotnością 1 godziny (np. 100s, 7min, 15min, 90min itd.), może prowadzić do wyników trudnych do interpretacji. Określenie interwału agregacji jest obowiązkowe. Interwał agregacji określa przedział czasu i współrzędne punktu danych; na przykład, jeśli pozycje osi X mają 4 wartości, a pozycje osi Y mają 1 wartość, współrzędne odzwierciedlają agregację 4 wartości na osi X i 1 wartości na osi Y w określonym interwale.

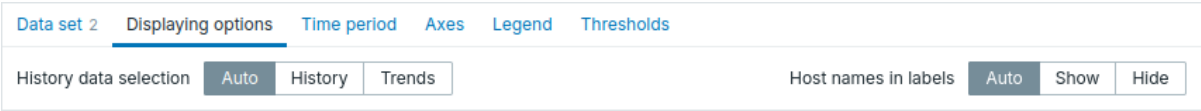
Szczegóły konfiguracji zestawu danych

Istniejące zestawy danych są wyświetlane na liście. Możesz zmieniać ich kolejność, rozwijać/zwijać, zmieniać kolory oraz klonować te zestawy danych.

Więcej informacji można znaleźć w opisie szczegółów konfiguracji zestawu danych w widżecie *Graph*. Te szczegóły mają również zastosowanie do widżetu *Scatter plot*.

Opcje wyświetlania

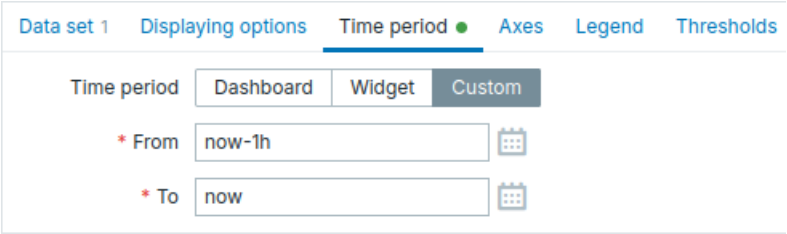
Zakładka **Opcje wyświetlania** pozwala zdefiniować wybór danych historii:



Wybór danych historii	Ustaw źródło danych wykresu rozrzutu: **Auto** - dane są pobierane zgodnie z klasycznym algorytmem wykresu (domyślnie). **Historia** - dane z historii. **Trendy** - dane z trendów.
Nazwy hostów w etykietach	Wybierz, czy wyświetlać nazwy hostów w legendzie wykresu oraz w podpowiedzi pojawiającej się po najechaniu kursorem na dane wykresu: **Auto** - nazwy hostów są wyświetlane tylko wtedy, gdy w zestawach danych występuje więcej niż jeden host (domyślnie). **Pokaż** - nazwy hostów są wyświetlane. **Ukryj** - nazwy hostów są ukryte. Ten parametr nie jest dostępny podczas konfigurowania widżetu na pulpicie szablonu.

Okres czasu

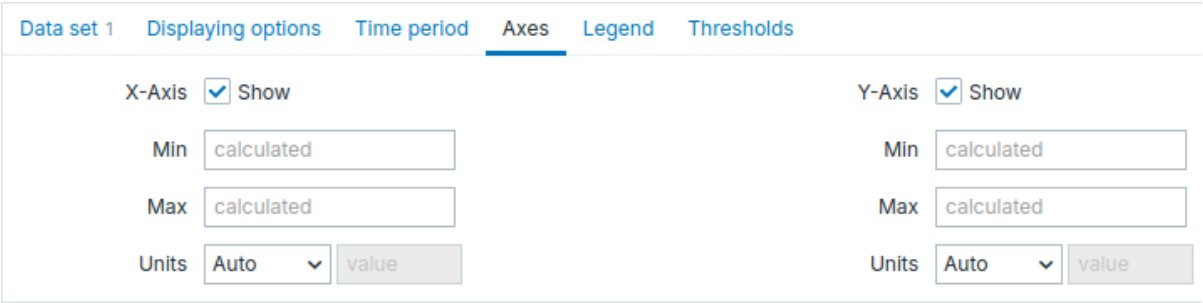
Zakładka **Okres czasu** umożliwia ustawienie okresu czasu, dla którego mają być wyświetlane dane na wykresie punktowym:



Okres czasu	Wybierz źródło danych dla okresu czasu: **Pulpit** - użyj selektora okresu czasu pulpitu; **Widżet** - użyj zgodnego widżetu (ustawionego w parametrze *Widżet*); **Niestandardowy** - użyj niestandardowego okresu czasu ustawionego w parametrach *Od* i *Do*; jeśli jest ustawiony, w prawym górnym rogu widżetu będzie wyświetlana ikona zegara, wskazująca ustawiony czas po najechaniu kursorem. Zwróć uwagę, że niezależnie od konfiguracji *Okresu czasu* widżetu, zgodne widżety nadal mogą używać go jako źródła danych dla okresu czasu.
Widżet	Wprowadź lub wybierz zgodny widżet jako źródło danych dla okresu czasu. Ten parametr jest dostępny, jeśli *Okres czasu* jest ustawiony na „Widżet”.
Od	Wprowadź lub wybierz początek okresu czasu. Obsługiwana jest składnia czasu względnego (`now`, `now/d`, `now/w-1w` itd.). Ten parametr jest dostępny, jeśli *Okres czasu* jest ustawiony na „Niestandardowy”.
Do	Wprowadź lub wybierz koniec okresu czasu. Obsługiwana jest składnia czasu względnego (`now`, `now/d`, `now/w-1w` itd.). Ten parametr jest dostępny, jeśli *Okres czasu* jest ustawiony na „Niestandardowy”.

Osie

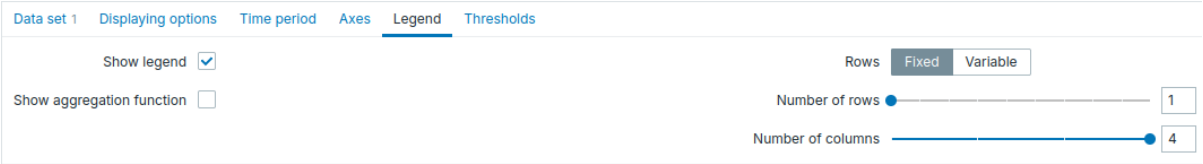
Zakładka **Osie** umożliwia dostosowanie sposobu wyświetlania osi:



Oś X/Oś Y	Odznacz to pole wyboru, aby ukryć oś X/oś Y (domyślnie zaznaczone).
Min	Ustaw minimalną wartość odpowiedniej osi.
Max	Ustaw maksymalną wartość odpowiedniej osi.
Jednostki	Wybierz jednostkę dla wartości osi wykresu punktowego z listy rozwijanej: **Auto** — wartości osi są wyświetlane z użyciem jednostki pierwszej pozycji w zbiorze danych; **Static** — wartości osi są wyświetlane z użyciem jednostki określonej w polu wejściowym *value*; jeśli pole pozostanie puste, wyświetlane będą tylko wartości liczbowe.

Legenda

Zakładka **Legenda** umożliwia dostosowanie legendy wykresu punktowego:

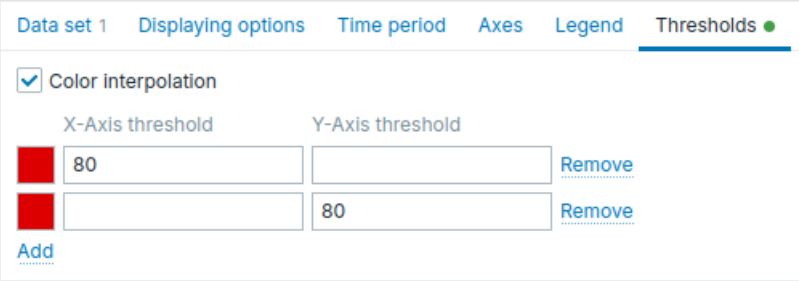


Pokaż legendę	Odznacz to pole wyboru, aby ukryć legendę na wykresie punktowym (domyślnie zaznaczone).
Pokaż funkcję agregacji	Zaznacz to pole wyboru, aby wyświetlać funkcję agregacji w legendzie.

Wiersze	Wybierz tryb wyświetlania wierszy legendy: **Stałe** — liczba wyświetlanych wierszy jest określana przez wartość parametru *Liczba wierszy*; **Zmienne** — liczba wyświetlanych wierszy jest określana przez liczbę skonfigurowanych pozycji, bez przekraczania wartości parametru *Maksymalna liczba wierszy*.
Liczba wierszy/ Maksymalna liczba wierszy	Jeśli dla parametru *Wiersze* ustawiono wartość „Stałe”, ustaw liczbę wyświetlanych wierszy legendy (1-10). Jeśli dla parametru *Wiersze* ustawiono wartość „Zmienne”, ustaw maksymalną liczbę wyświetlanych wierszy legendy (1-10).
Liczba kolumn	Ustaw liczbę wyświetlanych kolumn legendy (1-4). Ten parametr jest dostępny, jeśli opcja *Wyświetl min/avg/max* jest odznaczona.

Progi

Zakładka **Progi** umożliwia skonfigurowanie progów określających kolory znaczników hostów:

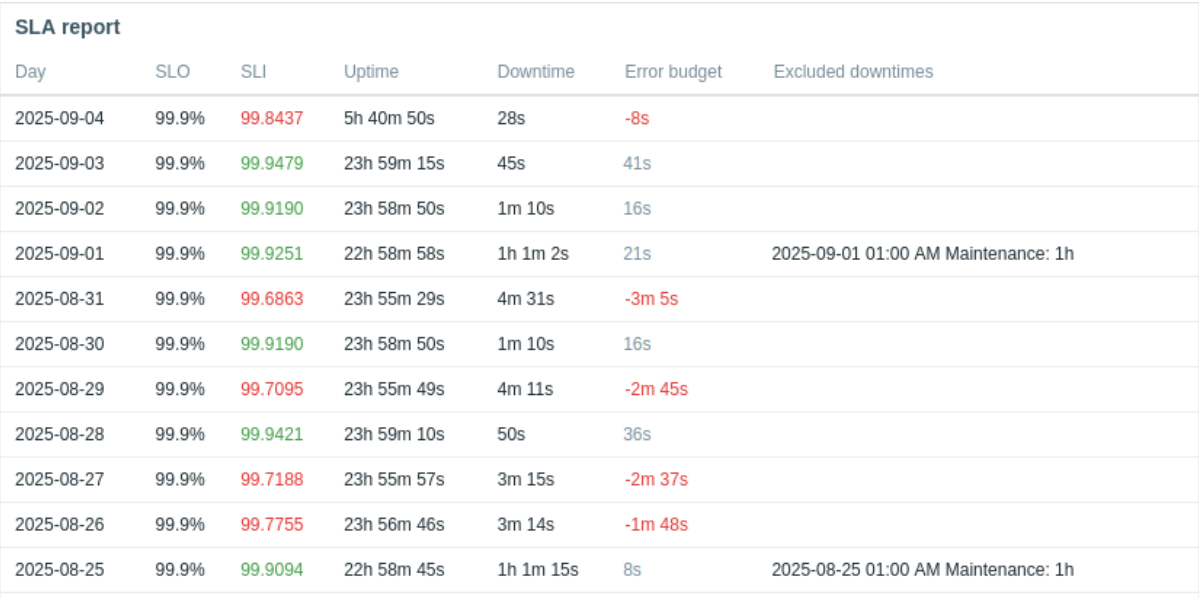


Interpolacja kolorów	Zaznacz pole wyboru, aby włączyć płynne przejścia między kolorami progów dla znaczników hostów. Ten parametr ma zastosowanie, jeśli ustawiono co najmniej dwa progi dla osi X, osi Y lub obu osi jednocześnie.
Próg osi X/osi Y	Kliknij *Dodaj*, aby dodać próg, wybierz kolor progu z próbnika kolorów i określ wartość liczbową. Progi można stosować do jednej osi, obu osi osobno lub obu osi jednocześnie. Na przykład pojedynczy próg z X=80 i Y=80 pokoloruje znaczniki, gdy oba warunki są spełnione. Lista progów zostanie posortowana rosnąco podczas zapisywania. Obsługiwane są sufiksy (na przykład „1d”, „2w”, „4K”, „8G”). Obsługiwane są mapowania wartości.

26 Raport SLA

Przegląd

Widżet *Raport SLA* wyświetla raporty SLA, pomagając monitorować wydajność usług względem zdefiniowanych celów.

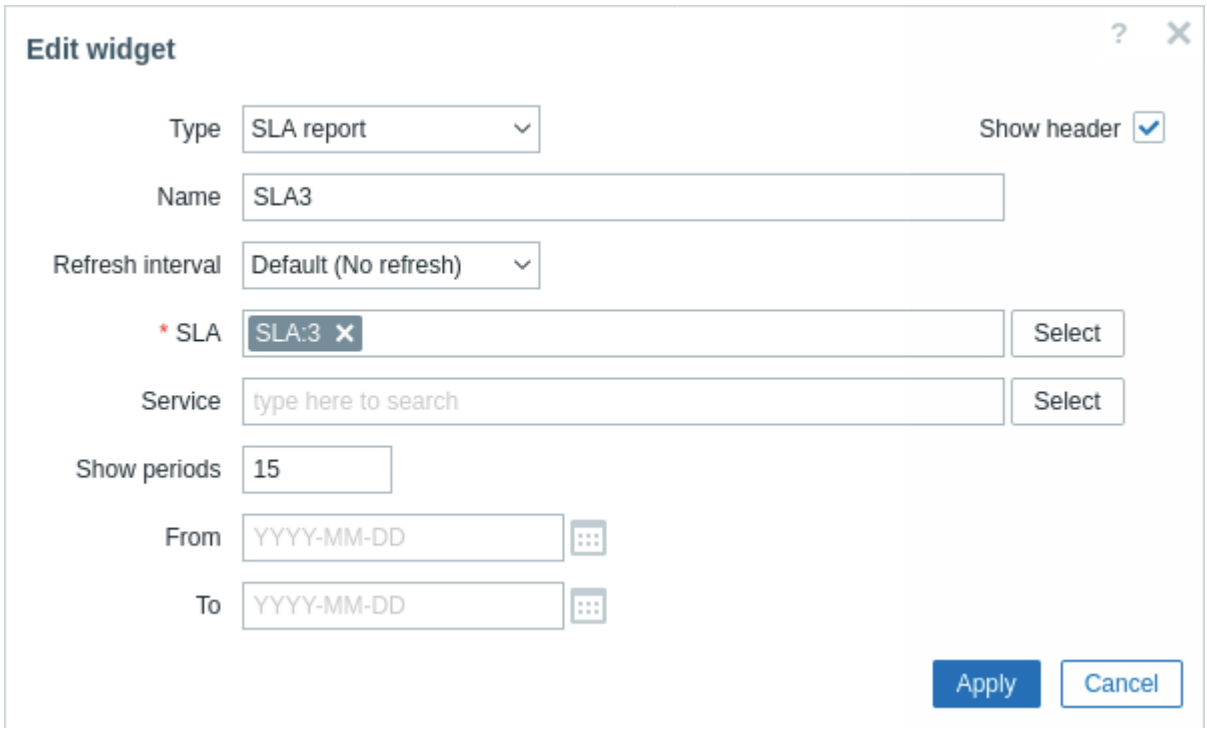

SLA report

Day	SLO	SLI	Uptime	Downtime	Error budget	Excluded downtimes
2025-09-04	99.9%	99.8437	5h 40m 50s	28s	-8s	
2025-09-03	99.9%	99.9479	23h 59m 15s	45s	41s	
2025-09-02	99.9%	99.9190	23h 58m 50s	1m 10s	16s	
2025-09-01	99.9%	99.9251	22h 58m 58s	1h 1m 2s	21s	2025-09-01 01:00 AM Maintenance: 1h
2025-08-31	99.9%	99.6863	23h 55m 29s	4m 31s	-3m 5s	
2025-08-30	99.9%	99.9190	23h 58m 50s	1m 10s	16s	
2025-08-29	99.9%	99.7095	23h 55m 49s	4m 11s	-2m 45s	
2025-08-28	99.9%	99.9421	23h 59m 10s	50s	36s	
2025-08-27	99.9%	99.7188	23h 55m 57s	3m 15s	-2m 37s	
2025-08-26	99.9%	99.7755	23h 56m 46s	3m 14s	-1m 48s	
2025-08-25	99.9%	99.9094	22h 58m 45s	1h 1m 15s	8s	2025-08-25 01:00 AM Maintenance: 1h

Wyświetla te same dane co *Usługi* > *Raport SLA*.

Konfiguracja

Aby skonfigurować widget, wybierz *SLA report* jako typ:



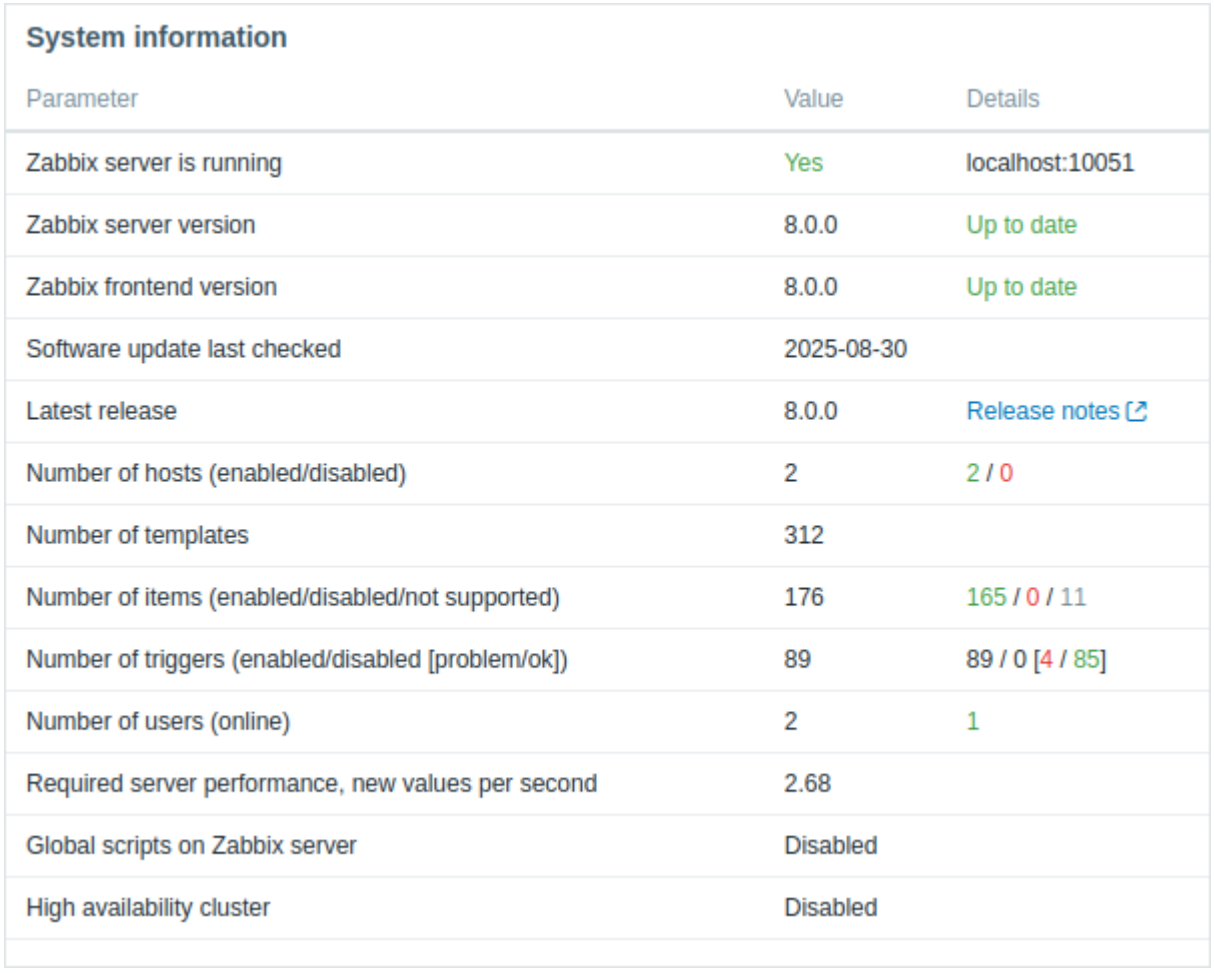
Oprócz parametrów wspólnych dla wszystkich widgetów można ustawić następujące opcje specyficzne:

SLA	Wybierz SLA dla raportu.
Service	Wybierz usługę dla raportu.
Show periods	Ustaw, ile okresów będzie wyświetlanych w widżecie (domyślnie 20, maksymalnie 100).
From	Wybierz datę początkową raportu. Obsługiwane są daty względne: `now`, `now/d`, `now/w-1w` itd.; obsługiwane modyfikatory daty: `d`, `w`, `M`, `y`.
To	Wybierz datę końcową raportu. Obsługiwane są daty względne: `now`, `now/d`, `now/w-1w` itd.; obsługiwane modyfikatory daty: `d`, `w`, `M`, `y`.

27 Informacje o systemie

Przegląd

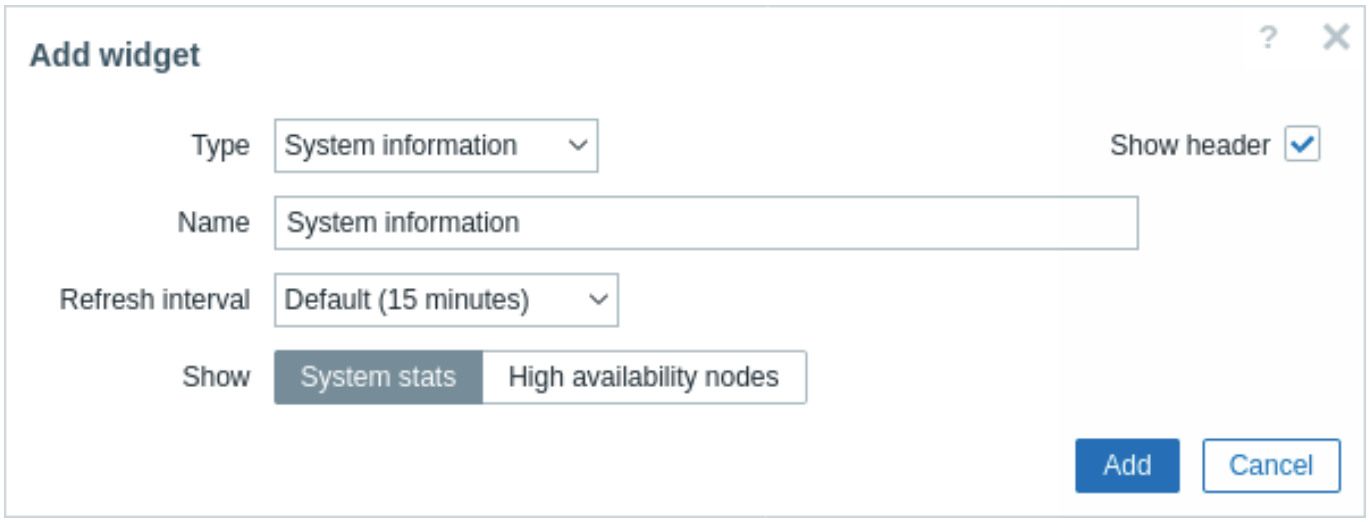
Widżet *Informacje o systemie* wyświetla podsumowanie kluczowych danych serwera Zabbix i systemu lub szczegóły węzłów wysokiej dostępności.



Wyświetla te same dane co *Raporty* > *Informacje o systemie*.

Konfiguracja

Aby skonfigurować, wybierz *Informacje o systemie* jako typ:



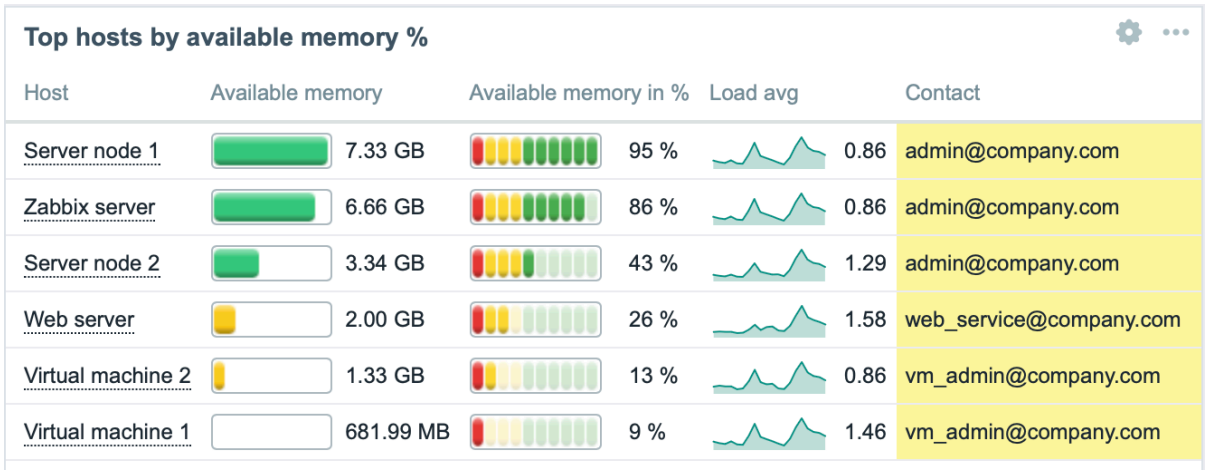
Oprócz parametrów wspólnych dla wszystkich widgetów, możesz ustawić następujące opcje specyficzne:

Pokaż	Wybierz, co wyświetlać: **Statystyki systemu** — wyświetla podsumowanie kluczowych danych serwera Zabbix i systemu; **Węzły wysokiej dostępności** — wyświetla status węzłów wysokiej dostępności (jeśli klaster wysokiej dostępności jest włączony).
Pokaż szczegóły sprawdzania aktualizacji oprogramowania	Zaznacz pole wyboru, aby wyświetlać szczegóły sprawdzania aktualizacji oprogramowania Zabbix. Ta opcja jest dostępna tylko wtedy, gdy sprawdzanie aktualizacji oprogramowania jest włączone w konfiguracji serwera Zabbix i w polu *Pokaż* wybrano opcję „Statystyki systemu”.

28 Najważniejsze hosty

Przegląd

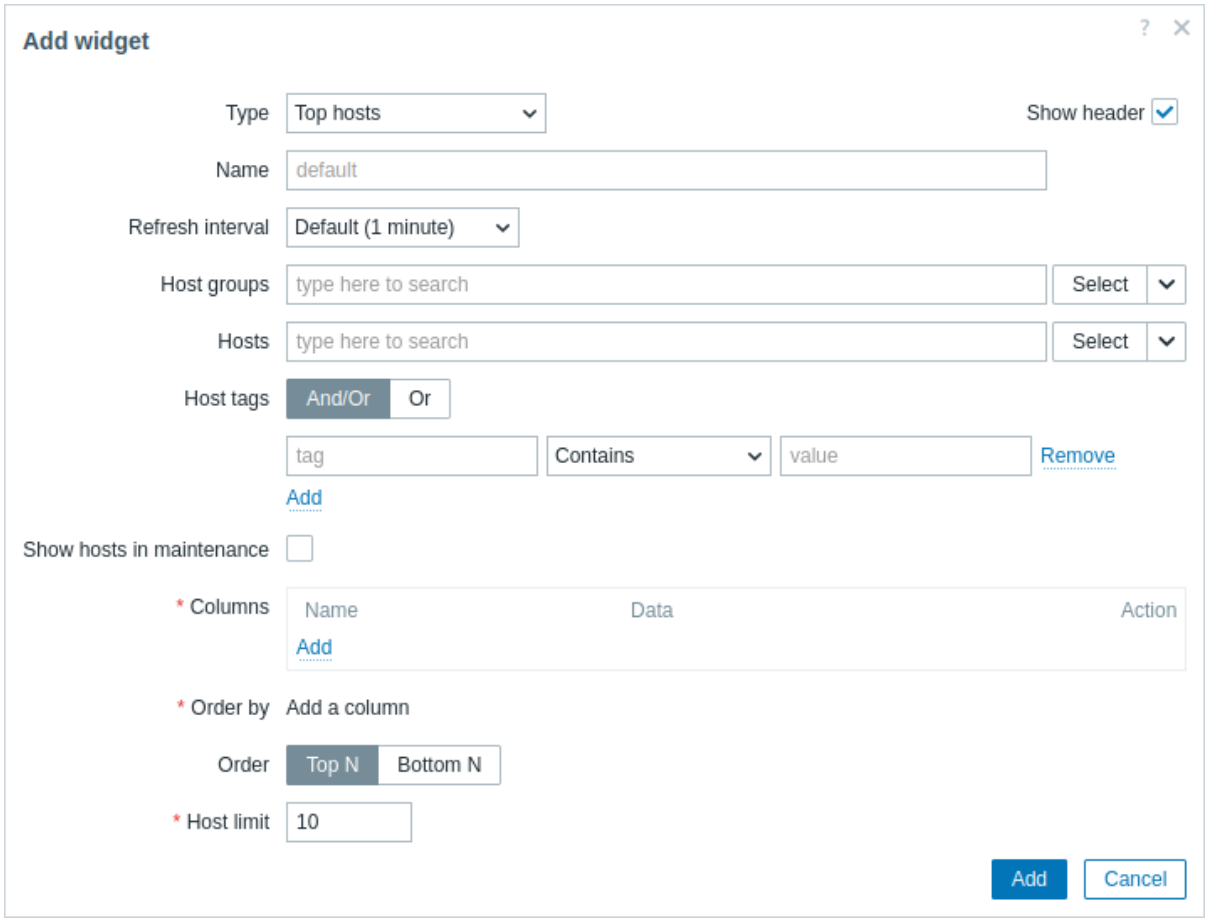
Widżet *Top hosts* wyświetla najwyższe/najniższe wartości dla wybranych pozycji z wielu hostów.



Widżet obsługuje jednoczesne wyświetlanie do 1000 hostów.

Konfiguracja

Aby skonfigurować, wybierz *Top hosts* jako typ:



Oprócz parametrów wspólnych dla wszystkich widgetów można ustawić następujące opcje specyficzne:

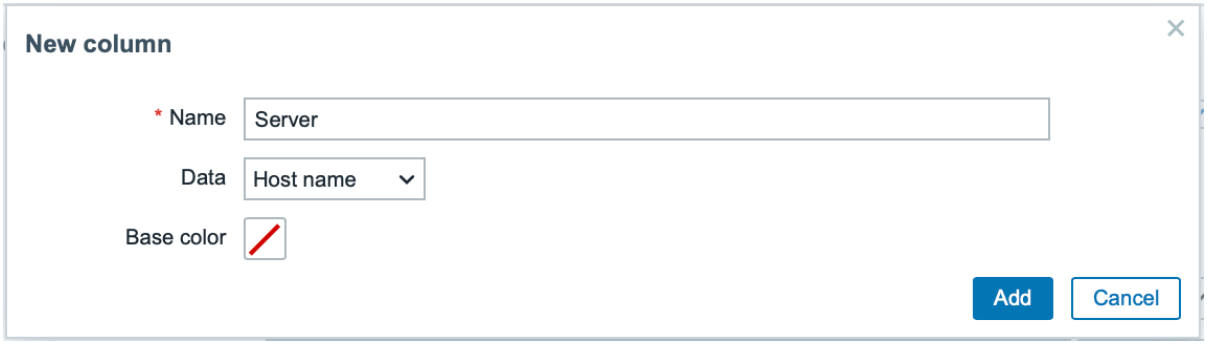
Host groups	Wybierz grupy hostów, które mają być wyświetlane w widżecie. Alternatywnie wybierz zgodny widget jako źródło danych dla grup hostów. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy grupy zostanie wyświetlona rozwijana lista pasujących grup. Ten parametr nie jest dostępny podczas konfigurowania widżetu na pulpicie szablonu.
Hosts	Wybierz hosty, które mają być wyświetlane w widżecie. Alternatywnie wybierz zgodny widget lub pulpit jako źródło danych dla hostów. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy hosta zostanie wyświetlona rozwijana lista pasujących hostów. Ten parametr nie jest dostępny podczas konfigurowania widżetu na pulpicie szablonu.
Host tags	Określ tagi, aby ograniczyć liczbę hostów wyświetlanych w widżecie. Można zarówno uwzględniać, jak i wykluczać określone tagi oraz wartości tagów. Można ustawić kilka warunków. Dopasowanie nazw tagów zawsze uwzględnia wielkość liter. Dla każdego warunku dostępnych jest kilka operatorów: **Exists** - uwzględnij określone nazwy tagów; **Equals** - uwzględnij określone nazwy tagów i wartości (z uwzględnieniem wielkości liter); **Contains** - uwzględnij określone nazwy tagów, dla których wartości tagów zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter); **Does not exist** - wyklucz określone nazwy tagów; **Does not equal** - wyklucz określone nazwy tagów i wartości (z uwzględnieniem wielkości liter); **Does not contain** - wyklucz określone nazwy tagów, dla których wartości tagów zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter). Dostępne są dwa typy obliczania warunków: **And/Or** - wszystkie warunki muszą być spełnione, a warunki mające tę samą nazwę tagu będą grupowane operatorem Or; **Or** - wystarczy spełnienie jednego warunku. Ten parametr nie jest dostępny podczas konfigurowania widżetu na pulpicie szablonu.
Show hosts in maintenance	Zaznacz to pole wyboru, aby wyświetlać również hosty w utrzymaniu (w takim przypadku obok nazwy hosta zostanie pokazana ikona utrzymania). Domyślnie niezaznaczone.
Columns	Dodaj kolumny danych do wyświetlenia. Kolejność kolumn określa ich wyświetlanie od lewej do prawej. Kolumny można zmieniać miejscami, przeciągając je w górę i w dół za uchwyt znajdujący się przed nazwą kolumny.
Order by	Określ kolumnę ze zdefiniowanej listy *Columns*, która ma być używana do sortowania *Top N* lub *Bottom N*.
Order	Określ kolejność wierszy: **Top N** - malejąco zgodnie z zagregowaną wartością *Order by*; **Bottom N** - rosnąco zgodnie z zagregowaną wartością *Order by*.
Host limit	Liczba wierszy hostów do wyświetlenia (1-1000). Ten parametr nie jest dostępny podczas konfigurowania widżetu na pulpicie szablonu.

Konfiguracja kolumn

Możliwe jest dodanie kolumn trzech typów danych: nazwa hosta, wartość pozycji lub tekst. Lista dostępnych parametrów kolumny zależy od typu danych kolumny, a w przypadku typu wartość pozycji — od formatu wartości.

Kolumna Nazwa hosta

Kolumna Nazwa hosta służy do wyświetlania nazwy hosta.

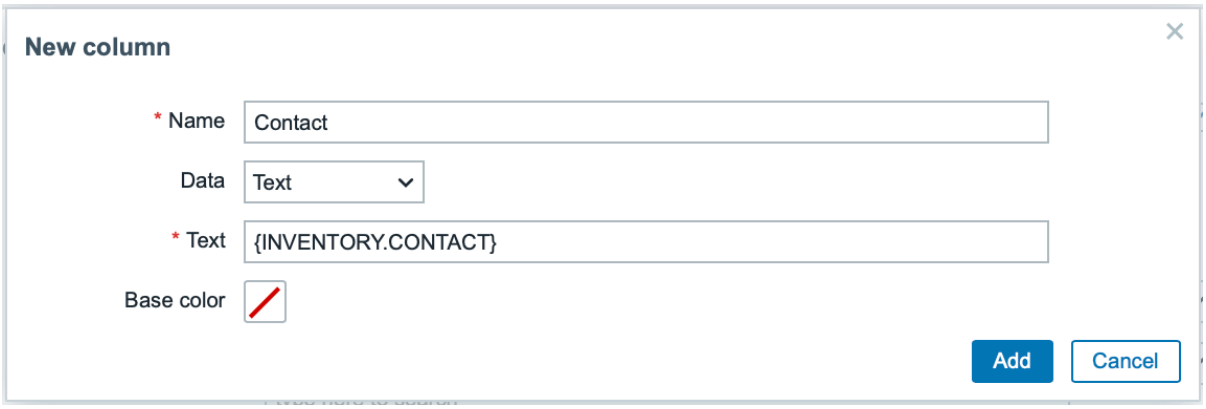


Obsługiwane parametry:

Name	Nazwa kolumny.
Data	Typ danych wyświetlanych w kolumnie; wybierz **Nazwa hosta**.
Base color	Kolor tła kolumny.

Kolumna tekstowa

Kolumna tekstowa służy do wyświetlania dowolnego określonego ciągu tekstowego.

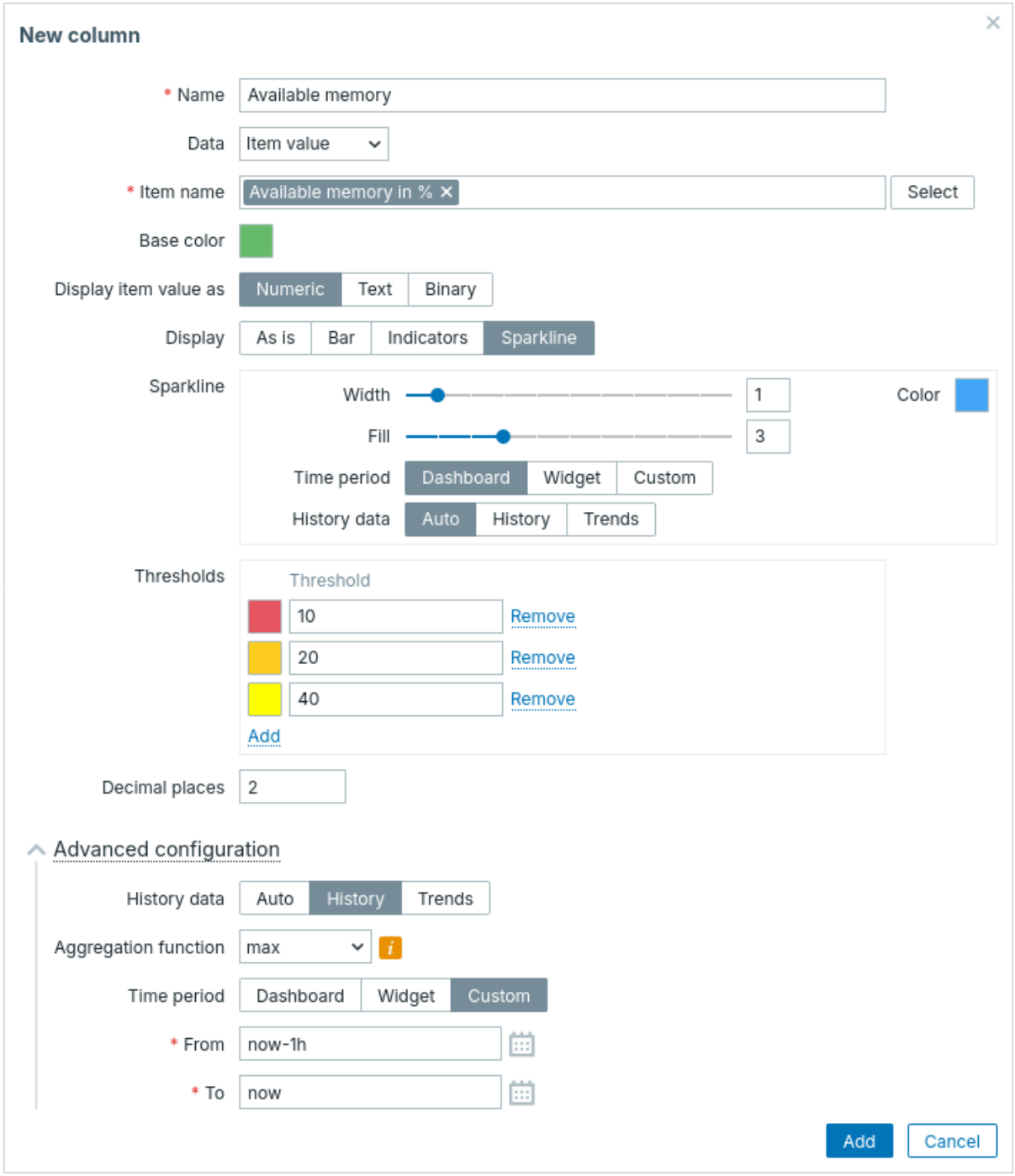


Obsługiwane parametry:

Nazwa	Nazwa kolumny.
Dane	Typ danych wyświetlany w kolumnie, wybierz **Tekst**.
Kolor bazowy	Kolor tła kolumny.
Tekst	Wprowadź ciąg do wyświetlenia. Może zawierać makra hosta i inwentarza.

Kolumna wartości pozycji

Kolumna wartości pozycji służy do wyświetlania wartości określonej pozycji; obsługuje wiele formatów i opcji wyświetlania wartości.



Obsługiwane parametry:

Name	Nazwa kolumny.
Data	Typ danych wyświetlanych w kolumnie; wybierz **Item value**.
Item name	Wybierz pozycję; jej nazwa jest używana do dopasowania i wyświetlania pozycji o tej samej nazwie na wszystkich wybranych hostach. Jeśli host ma wiele takich pozycji, widget wyświetli pozycję, której klucz jest pierwszy w kolejności alfabetycznej (np. *CPU utilization* z kluczem `proc.cpu.util` zamiast `system.cpu.util`). Podczas konfigurowania widgetu na pulpicie szablonu można wybrać tylko pozycje skonfigurowane w szablonie.
Base color	Kolor tła kolumny; kolor wypełnienia, jeśli dane *Item value* są wyświetlane jako pasek/wskaźniki. Domyślny kolor może zostać zastąpiony kolorem niestandardowym, jeśli wartość pozycji przekroczy jeden z określonych progów.
Display item value as	Format wyświetlania wartości pozycji: **Numeric**, **Text** lub **Binary**. Wybrana opcja określa, które dodatkowe parametry będą dostępne. Zobacz listę parametrów dla każdego formatu poniżej.
Advanced configuration	

History data	Pobieranie danych z historii lub trendów: **Auto** - wybór automatyczny; **History** - pobierz dane historyczne; **Trends** - pobierz dane trendów. Ten parametr jest dostępny tylko dla numerycznych wartości pozycji. W przypadku wartości tekstowych i binarnych dane będą zawsze pobierane z historii.
Aggregation function	Określ, której funkcji agregującej użyć: **min** - wyświetl najmniejszą wartość; **max** - wyświetl największą wartość; **avg** - wyświetl wartość średnią; **count** - wyświetl liczbę wartości; **sum** - wyświetl sumę wartości; **first** - wyświetl pierwszą wartość; **last** - wyświetl ostatnią wartość; **not used** - wyświetl najnowszą wartość (bez agregacji). Agregacja umożliwia wyświetlenie zagregowanej wartości dla wybranego przedziału (5 minut, godzina, dzień) zamiast najnowszej wartości. Tylko dane numeryczne mogą być wyświetlane dla *min*, *max*, *avg* i *sum*. Dla *count* dane nienumeryczne zostaną przekształcone na numeryczne.
Time period	Określ okres czasu używany do agregacji wartości. Wybierz źródło danych dla okresu czasu: **Dashboard** - użyj selektora okresu czasu pulpitu; **Widget** - użyj zgodnego widgetu (ustawionego w parametrze *Widget*); **Custom** - użyj niestandardowego okresu czasu ustawionego w parametrach *From* i *To*; jeśli zostanie ustawiony, w prawym górnym rogu widgetu zostanie wyświetlona ikona zegara wskazująca ustawiony czas po najechaniu kursorem. Zwróć uwagę, że niezależnie od konfiguracji *Time period* widgetu, zgodne widgety nadal mogą używać go jako źródła danych dla okresu czasu. Ten parametr nie jest dostępny, jeśli *Aggregation function* jest ustawione na "not used".
Widget	Wprowadź lub wybierz zgodny widget jako źródło danych dla okresu czasu. Ten parametr jest dostępny, jeśli *Time period* jest ustawione na "Widget".
From	Wprowadź lub wybierz początek okresu czasu. Obsługiwana jest składnia czasu względnego (`now`, `now/d`, `now/w-1w` itd.). Ten parametr jest dostępny, jeśli *Time period* jest ustawione na "Custom".
To	Wprowadź lub wybierz koniec okresu czasu. Obsługiwana jest składnia czasu względnego (`now`, `now/d`, `now/w-1w` itd.). Ten parametr jest dostępny, jeśli *Time period* jest ustawione na "Custom".

Parametry numerycznej wartości pozycji:

Display	Określ, jak wartość ma być wyświetlana: **As is** - jako zwykły tekst; **Bar** - jako jednolity pasek wypełniony kolorem; **Indicators** - jako segmentowany pasek wypełniony kolorem; **Sparkline** - miniaturowy wykres liniowy.
Thresholds	Określ wartości progowe, przy których kolor tła/wypełnienia ma się zmienić. Lista zostanie posortowana rosnąco podczas zapisywania. W przypadku sparkline progi są stosowane tylko do ostatniej wartości pozycji.
Decimal places	Określ, ile miejsc po przecinku ma być wyświetlanych przy wartości.
Bar/Indicators	
Min	Wartość minimalna.
Max	Wartość maksymalna.
Sparkline	
Width	Ustaw grubość linii wykresu za pomocą suwaka lub ręcznie, wprowadzając wartość z zakresu od 0 do 10.
Color	Wybierz kolor linii i wypełnienia.
Fill	Ustaw poziom przezroczystości koloru wypełnienia za pomocą suwaka lub ręcznie, wprowadzając wartość z zakresu od 0 do 10.

Time period	Określ okres czasu dla wartości, które mają zostać uwzględnione na wykresie sparkline. Wybierz źródło danych dla okresu czasu: **Dashboard** - użyj selektora okresu czasu pulpitu **Widget** - użyj zgodnego widgetu (ustawionego w parametrze *Widget*); **Custom** - użyj niestandardowego okresu czasu ustawionego w parametrach *From* i *To*; jeśli zostanie ustawiony, w prawym górnym rogu widgetu zostanie wyświetlona ikona zegara wskazująca ustawiony czas po najechaniu kursorem. Zwróć uwagę, że niezależnie od konfiguracji *Time period* widgetu, zgodne widgety nadal mogą używać go jako źródła danych dla okresu czasu.
Widget	Wprowadź lub wybierz zgodny widget jako źródło danych dla okresu czasu. Ten parametr jest dostępny, jeśli *Time period* jest ustawione na "Widget".
From	Wprowadź lub wybierz początek okresu czasu. Obsługiwana jest składnia czasu względnego (`now`, `now/d`, `now/w-1w` itd.). Ten parametr jest dostępny, jeśli *Time period* jest ustawione na "Custom".
To	Wprowadź lub wybierz koniec okresu czasu. Obsługiwana jest składnia czasu względnego (`now`, `now/d`, `now/w-1w` itd.). Ten parametr jest dostępny, jeśli *Time period* jest ustawione na "Custom".
History data	Pobieranie danych z historii lub trendów: **Auto** - wybór automatyczny; **History** - pobierz dane historyczne; **Trends** - pobierz dane trendów.

Parametry tekstowej wartości pozycji:

Highlights	Określ wyrażenia regularne, po dopasowaniu których kolor tła/wypełnienia ma się zmienić.

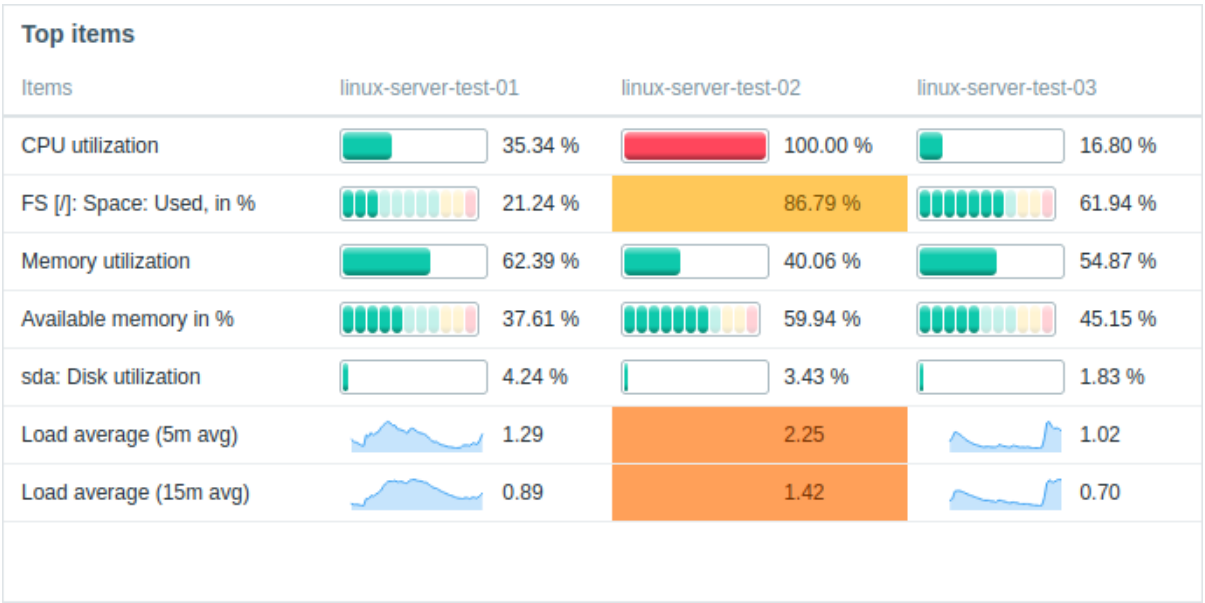
Parametry binarnej wartości pozycji:

Show thumbnail	Określ, czy utworzyć i wyświetlić miniaturę obrazu zawierającego dane binarne, czy wyświetlić hiperłącze *Show* prowadzące do obrazu w pełnym rozmiarze w kolumnie wartości.

29 Najważniejsze pozycje

Przegląd

Widżet *Top items* wyświetla najwyższe/najniższe wartości dla wybranych pozycji, zapewniając szybki przegląd ich wydajności.

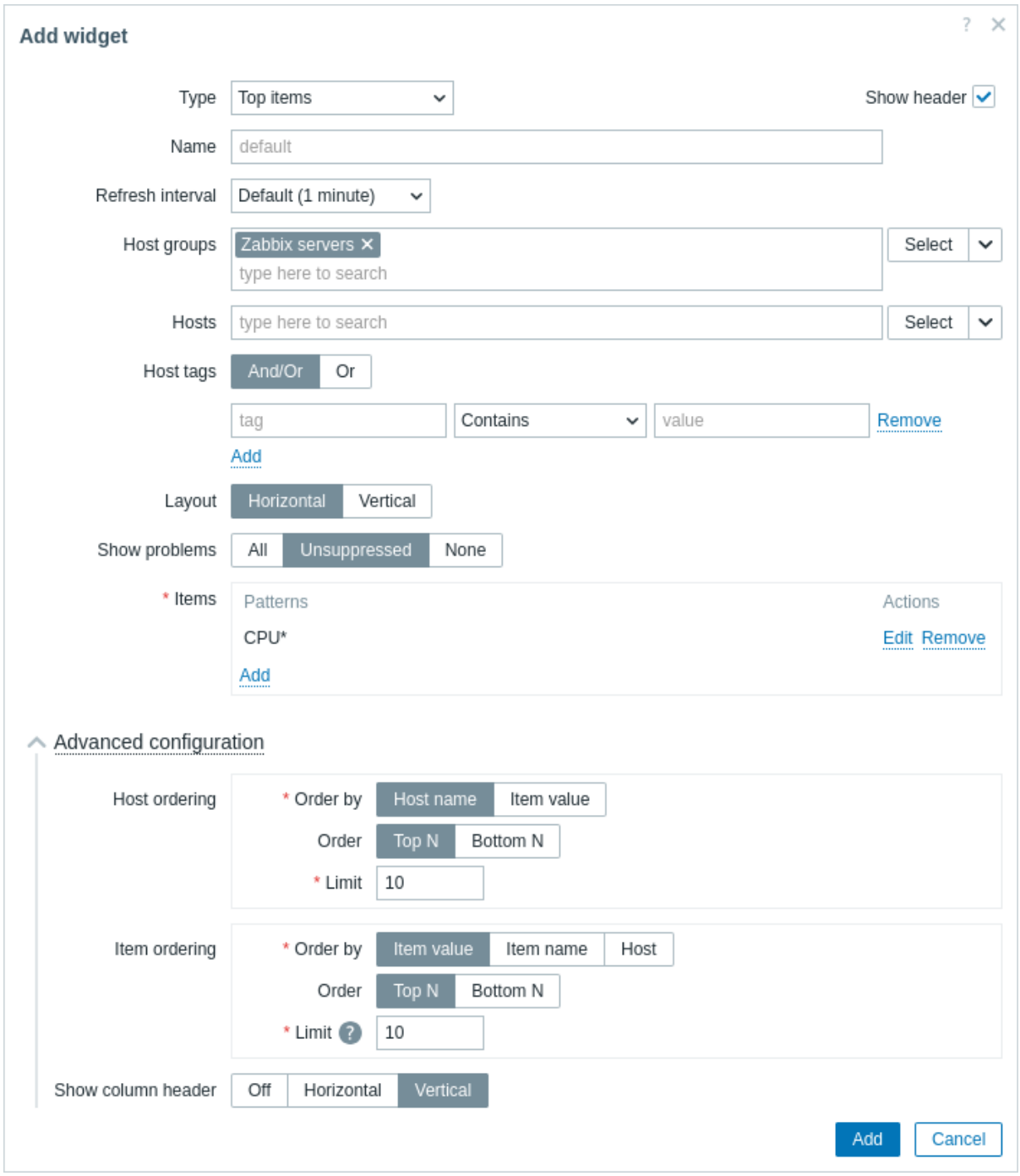


Domyślnie widżet wyświetla wartości z ostatnich 24 godzin. Ten okres można zmienić w *Administracja* > *Ogólne* > *GUI* (*Maksymalny okres wyświetlania historii*).

Kliknięcie wartości pozycji otwiera menu pozycji.

Konfiguracja

Aby skonfigurować widżet, wybierz *Top items* jako typ:



Oprócz parametrów wspólnych dla wszystkich widżetów, możesz ustawić następujące opcje specyficzne:

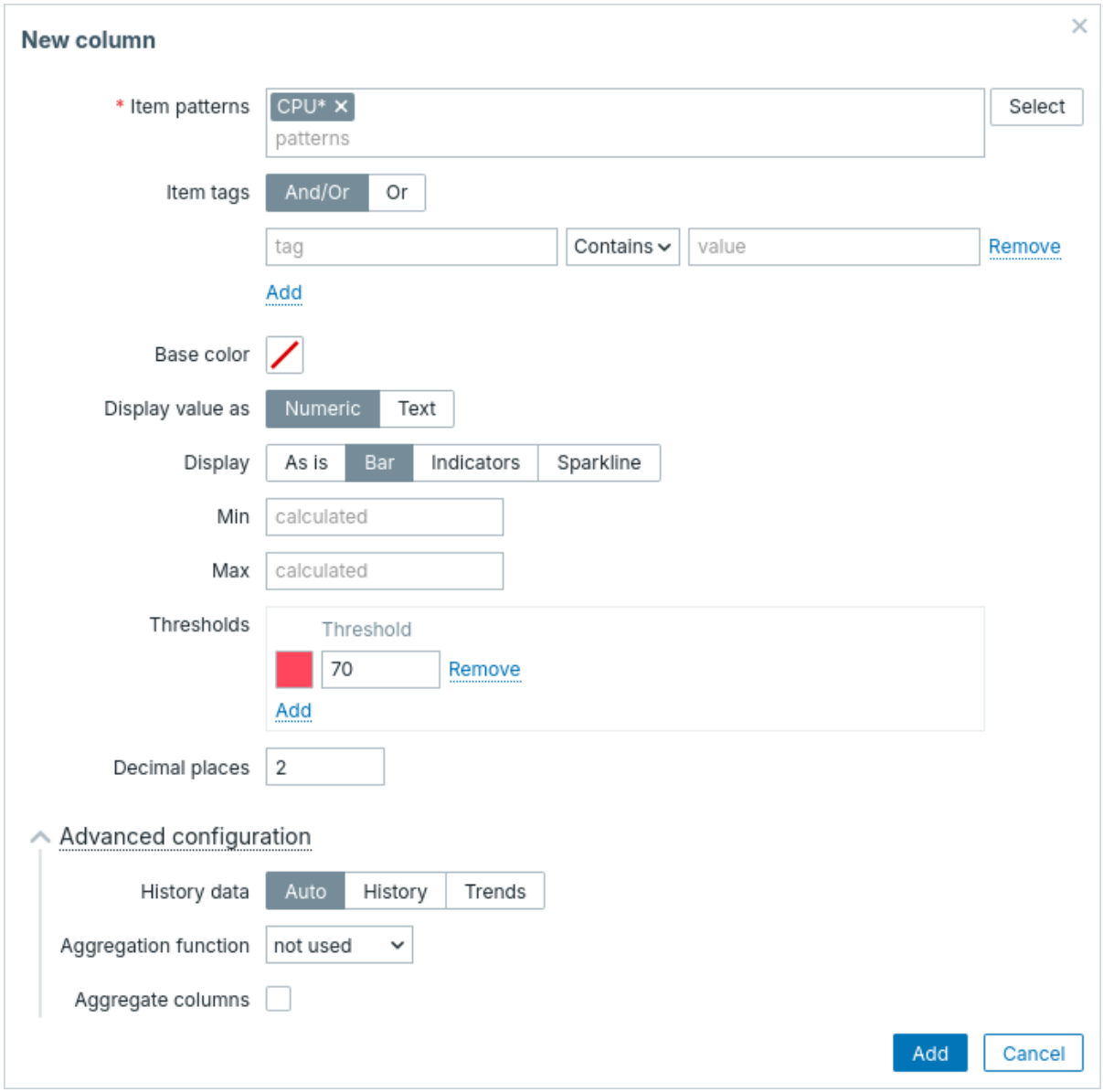
Host groups	Wybierz grupy hostów. Alternatywnie wybierz zgodny widżet jako źródło danych dla grup hostów. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy grupy zostanie wyświetlona rozwijana lista pasujących grup. Ten parametr nie jest dostępny podczas konfigurowania widżetu na pulpicie szablonu.
Hosts	Wybierz hosty. Alternatywnie wybierz zgodny widżet lub pulpit jako źródło danych dla hostów. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy hosta zostanie wyświetlona rozwijana lista pasujących hostów. Ten parametr nie jest dostępny podczas konfigurowania widżetu na pulpicie szablonu.

Host tags		Określ tagi, aby ograniczyć liczbę danych hostów wyświetlanych w widżecie. Można zarówno uwzględniać, jak i wykluczać określone tagi oraz wartości tagów. Można ustawić kilka warunków. Dopasowanie nazw tagów zawsze uwzględnia wielkość liter. Dla każdego warunku dostępnych jest kilka operatorów: **Exists** - uwzględnij określone nazwy tagów; **Equals** - uwzględnij określone nazwy tagów i wartości (z uwzględnieniem wielkości liter); **Contains** - uwzględnij określone nazwy tagów, których wartości zawierają wprowadzony ciąg znaków (dopasowanie podciągu, bez uwzględniania wielkości liter); **Does not exist** - wyklucz określone nazwy tagów; **Does not equal** - wyklucz określone nazwy tagów i wartości (z uwzględnieniem wielkości liter); **Does not contain** - wyklucz określone nazwy tagów, których wartości zawierają wprowadzony ciąg znaków (dopasowanie podciągu, bez uwzględniania wielkości liter). Dla warunków dostępne są dwa typy obliczeń: **And/Or** - wszystkie warunki muszą być spełnione, a warunki mające tę samą nazwę tagu będą grupowane warunkiem *Or*; **Or** - wystarczy spełnienie jednego warunku.
Layout		Wybierz opcję układu: **Horizontal** - nazwy hostów będą wyświetlane po lewej stronie; **Vertical** - nazwy hostów będą wyświetlane u góry.
Show problems		Filtruj, które problemy mają być wyświetlane na podstawie ich stanu (wszystkie, niewyciszone, brak). Problemy są oznaczane kolorowymi wartościami pozycji, zastępując ustawienia wyświetlania kolumn pozycji. Kolory są oparte na ważności problemu, którą można dostosować w *Administration* > *General* > *Trigger displaying options*. Ważności problemów można zmieniać podczas aktualizowania problemów.
Items		Dodaj wzorce pozycji lub konkretne pozycje do wyświetlenia (zobacz Konfiguracja kolumn).
Advanced configuration		
Host ordering		Wybierz opcje sortowania dla kolumny/wiersza hostów.
	Order by	Sortuj hosty według: **Host name** - hosty będą sortowane według nazwy hosta; **Item value** - hosty będą sortowane według wartości wybranych pozycji.
	Order	Wybierz, czy mają być wyświetlane najwyższe czy najniższe wartości: **TopN** - N najwyższych wartości; **BottomN** - N najniższych wartości. Wartość N jest wybierana w polu *Limit*.
	Limit	Wprowadź limit wyświetlanych hostów (zakres 1-1000; domyślnie 10). Ta wartość stanie się wartością N w polu *Order*.
Item ordering		Wybierz opcje sortowania dla kolumny/wiersza pozycji.
	Order by	Sortuj pozycje według: **Item value** - pozycje będą sortowane według wartości pozycji; **Item name** - pozycje będą sortowane według nazwy pozycji; **Host** - pozycje będą sortowane według wybranego wzorca hosta.
	Order	Wybierz, czy mają być wyświetlane najwyższe czy najniższe wartości: **TopN** - N najwyższych wartości; **BottomN** - N najniższych wartości. Wartość N jest wybierana w polu *Limit*.
	Limit	Wprowadź limit wyświetlanych pozycji (zakres 1-1000; domyślnie 10). Ta wartość stanie się wartością N w polu *Order*.

Show column header	Wybierz opcje wyświetlania nagłówka kolumny: **Off** - nie wyświetlaj nagłówka kolumny; **Horizontal** - wyświetlaj tekst poziomo w nagłówku; **Vertical** - wyświetlaj tekst pionowo w nagłówku.

Konfiguracja kolumn

Aby skonfigurować kolumny pozycji, kliknij *Dodaj* w parametrze *Pozycje*:



Wspólne parametry kolumn:

Wzorce pozycji	Określ jeden lub kilka wzorców pozycji, używając znaku wieloznacznego. Alternatywnie wybierz pozycje. Podczas konfigurowania widżetu na pulpicie szablonu można wybrać tylko pozycje skonfigurowane w szablonie.

Tagi pozycji	Określ tagi, aby ograniczyć liczbę danych pozycji wyświetlanych w widżecie. Możliwe jest zarówno uwzględnianie, jak i wykluczanie określonych tagów oraz wartości tagów. Można ustawić kilka warunków. Dopasowanie nazw tagów zawsze rozróżnia wielkość liter. Dla każdego warunku dostępnych jest kilka operatorów: **Istnieje** - uwzględnij określone nazwy tagów; **Równa się** - uwzględnij określone nazwy tagów i wartości (z rozróżnianiem wielkości liter); **Zawiera** - uwzględnij określone nazwy tagów, w których wartości tagów zawierają wprowadzony ciąg (dopasowanie podciągu, bez rozróżniania wielkości liter); **Nie istnieje** - wyklucz określone nazwy tagów; **Nie równa się** - wyklucz określone nazwy tagów i wartości (z rozróżnianiem wielkości liter); **Nie zawiera** - wyklucz określone nazwy tagów, w których wartości tagów zawierają wprowadzony ciąg (dopasowanie podciągu, bez rozróżniania wielkości liter). Dostępne są dwa typy obliczania warunków: **And/Or** - wszystkie warunki muszą być spełnione, warunki mające tę samą nazwę tagu będą grupowane przez warunek *Or*; **Or** - wystarczy spełnienie jednego warunku.
Kolor bazowy	Wybierz kolor tła kolumny lub kolor wypełnienia, jeśli dla parametru *Wyświetlanie* ustawiono wartość „Słupek” lub „Wskaźniki”. Zwróć uwagę, że kolor bazowy może zostać zastąpiony przez kolory progów lub wyróżnienia.
Wyświetlaj wartość jako	Format wyświetlania wartości pozycji: **Liczbowy** lub **Tekst**. Wybrana opcja określa, które dodatkowe parametry będą dostępne. Szczegóły znajdują się na poniższej liście parametrów dla każdego formatu.

Parametry kolumny dla wartości numerycznych:

Wyświetlanie	Określ, jak wartość ma być wyświetlana: **As is** - jako zwykły tekst; **Bar** - jako jednolity pasek wypełniony kolorem; **Indicators** - jako segmentowany pasek wypełniony kolorem; **Sparkline** - miniwykres liniowy.
Min	Wartość minimalna dla wyświetlania jako pasek/wskaźniki.
Max	Wartość maksymalna dla wyświetlania jako pasek/wskaźniki.
Width	Ustaw grubość linii wykresu za pomocą suwaka lub ręcznie, wprowadzając wartość z zakresu od 0 do 10. Ten parametr dotyczy tylko wyświetlania sparkline.
Fill	Ustaw poziom przezroczystości koloru wypełnienia za pomocą suwaka lub ręcznie, wprowadzając wartość z zakresu od 0 do 10. Ten parametr dotyczy tylko wyświetlania sparkline.
Color	Wybierz kolor linii i wypełnienia. Ten parametr dotyczy tylko wyświetlania sparkline.
Opis pól związanych z okresem czasu i wyborem danych historycznych znajduje się w sekcji *Konfiguracja zaawansowana*.	
Thresholds	Określ wartości progowe, przy których kolor tła/wypełnienia ma się zmienić. Lista zostanie posortowana rosnąco po zapisaniu. Dla sparkline wartości progowe są stosowane tylko do ostatniej wartości pozycji.
Decimal places	Określ, ile miejsc po przecinku ma być wyświetlanych przy wartości.
Konfiguracja zaawansowana	
History data	Pobieraj dane z historii lub trendów: **Auto** - wybór automatyczny; **History** - pobierz dane historyczne; **Trends** - pobierz dane trendów. Ten parametr jest dostępny tylko dla wartości numerycznych pozycji. W przypadku wartości tekstowych dane będą zawsze pobierane z historii.

Aggregation function	Określ, której funkcji agregującej użyć: **min** - wyświetl najmniejszą wartość; **max** - wyświetl największą wartość; **avg** - wyświetl wartość średnią; **count** - wyświetl liczbę wartości; **sum** - wyświetl sumę wartości; **first** - wyświetl pierwszą wartość; **last** - wyświetl ostatnią wartość; **not used** - wyświetl najnowszą wartość (bez agregacji). Agregacja umożliwia wyświetlenie wartości zagregowanej dla wybranego przedziału (5 minut, godzina, dzień) zamiast najnowszej wartości. Tylko dane numeryczne mogą być wyświetlane dla *min*, *max*, *avg* i *sum*. W przypadku *count* dane nienumeryczne zostaną zamienione na numeryczne.
Time period	Określ okres czasu używany do agregacji wartości. Wybierz źródło danych dla okresu czasu: **Dashboard** - użyj selektora okresu czasu pulpitu; **Widget** - użyj zgodnego widżetu (ustawionego w parametrze *Widget*); **Custom** - użyj niestandardowego okresu czasu ustawionego w parametrach *From* i *To*; jeśli zostanie ustawiony, w prawym górnym rogu widżetu zostanie wyświetlona ikona zegara wskazująca ustawiony czas po najechaniu kursorem. Zwróć uwagę, że niezależnie od konfiguracji *Time period* widżetu, zgodne widżety nadal mogą używać go jako źródła danych dla okresu czasu. Ten parametr nie jest dostępny, jeśli *Aggregation function* jest ustawiona na ”not used”.
Widget	Wprowadź lub wybierz zgodny widżet jako źródło danych dla okresu czasu. Ten parametr jest dostępny, jeśli *Time period* jest ustawiony na ”Widget”.
From	Wprowadź lub wybierz początek okresu czasu. Obsługiwana jest składnia czasu względnego (`now`, `now/d`, `now/w-1w` itd.). Ten parametr jest dostępny, jeśli *Time period* jest ustawiony na ”Custom”.
To	Wprowadź lub wybierz koniec okresu czasu. Obsługiwana jest składnia czasu względnego (`now`, `now/d`, `now/w-1w` itd.). Ten parametr jest dostępny, jeśli *Time period* jest ustawiony na ”Custom”.
Aggregate columns	Po zaznaczeniu wszystkie pozycje pasujące do wzorców pozycji kolumny zostaną zgrupowane w jedną wspólną kolumnę/wiersz. Wartości z pasujących pozycji zostaną zagregowane przy użyciu wybranej *Column aggregation function* i wyświetlone pod nazwą *Combined column name*. Wartość domyślna: wyłączone (niezaznaczone). Ten parametr jest wyświetlany tylko wtedy, gdy *Display value as* ma wartość **Numeric**.
Column aggregation function	Wybierz sposób łączenia wartości z pogrupowanych wzorców pozycji. Dostępne opcje: **min**, **max**, **avg**, **count**, **sum** (domyślnie). Ten parametr jest wyświetlany tylko wtedy, gdy *Aggregate columns* jest zaznaczone.
Combined column name	Wprowadź nazwę wyświetlaną dla zagregowanej kolumny. To pole jest wymagane, gdy *Aggregate columns* jest zaznaczone, i staje się nagłówkiem kolumny dla połączonych wartości.

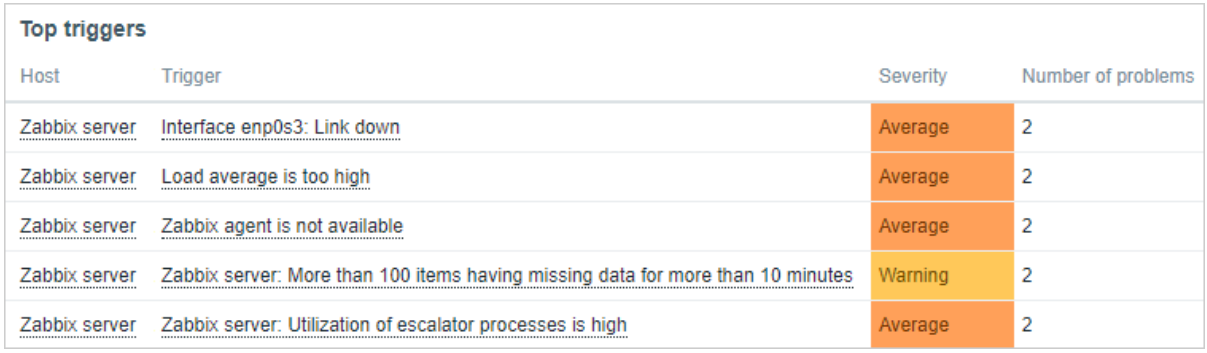
Parametry kolumny dla wartości tekstowych:

Highlights	Określ wyrażenia regularne, po dopasowaniu których kolor tła/wypełnienia ma się zmienić.

30 najważniejszych wyzwalaczy

Przegląd

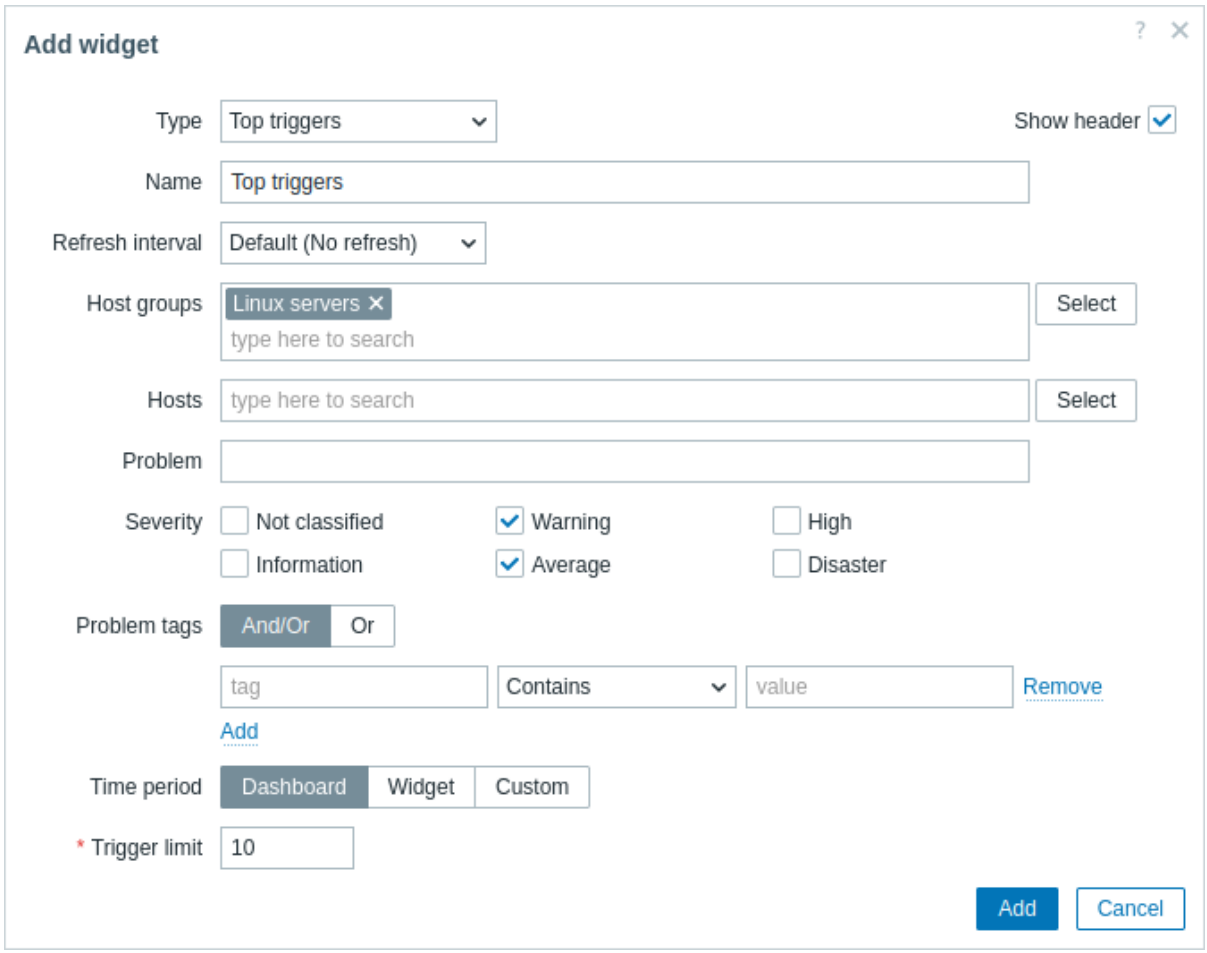
Widżet *Top triggers* wyświetla wyzwalacze z największą liczbą problemów.



Wyświetla te same dane co *Raporty > Top 100 triggers* i może wyświetlić do 1000 rekordów.

Konfiguracja

Aby skonfigurować widget, wybierz *Top triggers* jako typ widgetu:



Oprócz parametrów wspólnych dla wszystkich widgetów, możesz ustawić następujące opcje specyficzne:

Host groups	Wybierz grupy hostów, których problemy mają być wyświetlane w widżecie. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy grupy zostanie wyświetlona rozwijana lista pasujących grup. Określenie nadrzędnej grupy hostów powoduje automatyczne wybranie wszystkich zagnieżdżonych grup hostów. Problemy z tych grup hostów będą wyświetlane w widżecie; jeśli nie zostaną wprowadzone żadne grupy hostów, wyświetlane będą problemy ze wszystkich grup hostów. Ten parametr nie jest dostępny podczas konfigurowania widgetu na dashboardzie szablonu.
Hosts	Wybierz hosty, których problemy mają być wyświetlane w widżecie. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy hosta zostanie wyświetlona rozwijana lista pasujących hostów. Jeśli nie zostaną wprowadzone żadne hosty, wyświetlane będą problemy wszystkich hostów. Ten parametr nie jest dostępny podczas konfigurowania widgetu na dashboardzie szablonu.

Problem	Możesz wyświetlać wyzwalacze tylko dla określonych problemów. W tym celu wprowadź ciąg znaków, który ma zostać dopasowany w nazwie problemu. Makra nie są rozwijane.
Severity	Zaznacz poziomy ważności wyzwalaczy, aby filtrować wyzwalacze wyświetlane w widżecie. Jeśli nie zostanie zaznaczony żaden poziom ważności, wyświetlane będą wszystkie wyzwalacze.
Problem tags	Określ tagi problemów, które mają być wyświetlane w widżecie. Możliwe jest zarówno uwzględnianie, jak i wykluczanie określonych tagów oraz wartości tagów. Można ustawić kilka warunków. Dopasowanie nazw tagów zawsze uwzględnia wielkość liter. Dla każdego warunku dostępnych jest kilka operatorów: **Exists** - uwzględnij określone nazwy tagów; **Equals** - uwzględnij określone nazwy i wartości tagów (z uwzględnieniem wielkości liter); **Contains** - uwzględnij określone nazwy tagów, których wartości zawierają wprowadzony ciąg znaków (dopasowanie podciągu, bez uwzględniania wielkości liter); **Does not exist** - wyklucz określone nazwy tagów; **Does not equal** - wyklucz określone nazwy i wartości tagów (z uwzględnieniem wielkości liter); **Does not contain** - wyklucz określone nazwy tagów, których wartości zawierają wprowadzony ciąg znaków (dopasowanie podciągu, bez uwzględniania wielkości liter). Dostępne są dwa typy obliczania warunków: **And/Or** - wszystkie warunki muszą być spełnione, a warunki mające tę samą nazwę tagu będą grupowane warunkiem *Or*; **Or** - wystarczy spełnienie jednego warunku.
Time period	Wybierz źródło danych dla okresu czasu: **Dashboard** - użyj selektora okresu czasu dashboardu; **Widget** - użyj kompatybilnego widgetu (ustawionego w parametrze *Widget*); **Custom** - użyj niestandardowego okresu czasu ustawionego w parametrach *From* i *To*; jeśli zostanie ustawiony, w prawym górnym rogu widgetu będzie wyświetlana ikona zegara, wskazująca ustawiony czas po najechaniu kursorem. Zwróć uwagę, że niezależnie od konfiguracji *Time period* widgetu, kompatybilne widgety nadal mogą używać go jako źródła danych dla okresu czasu.
Widget	Wprowadź lub wybierz kompatybilny widget jako źródło danych dla okresu czasu. Ten parametr jest dostępny, jeśli *Time period* jest ustawiony na ”Widget”.
From	Wprowadź lub wybierz początek okresu czasu. Obsługiwana jest składnia czasu względnego (`now`, `now/d`, `now/w-1w` itd.). Ten parametr jest dostępny, jeśli *Time period* jest ustawiony na ”Custom”.
To	Wprowadź lub wybierz koniec okresu czasu. Obsługiwana jest składnia czasu względnego (`now`, `now/d`, `now/w-1w` itd.). Ten parametr jest dostępny, jeśli *Time period* jest ustawiony na ”Custom”.
Trigger limit	Ustaw liczbę wyzwalaczy do wyświetlenia. Możliwy zakres wartości: 1-1000.

31 Przegląd wyzwalaczy

Przegląd

Widżet *Przegląd wyzwalaczy* wyświetla bieżące stany wyzwalaczy hostów w postaci tabeli kolorowych bloków. Zapewnia szybki wizualny podgląd kondycji i aktywności wyzwalaczy na różnych hostach.



Widżet wykorzystuje wiele elementów wizualnych do przedstawienia szczegółów wyzwalaczy:

- Kolory bloków dla wyzwalaczy w stanie PROBLEM odpowiadają poziomom ważności problemów.
- Migające bloki wskazują niedawne zmiany stanu wyzwalacza (w ciągu ostatnich 2 minut).
- Szare strzałki wskazują wyzwalacze z zależnościami (najedź na nie kursorem, aby zobaczyć szczegóły).
- Ikony pól wyboru wskazują potwierdzone problemy; aby ta ikona się pojawiła, wszystkie aktywne lub rozwiązane problemy dla wyzwalacza muszą być potwierdzone.

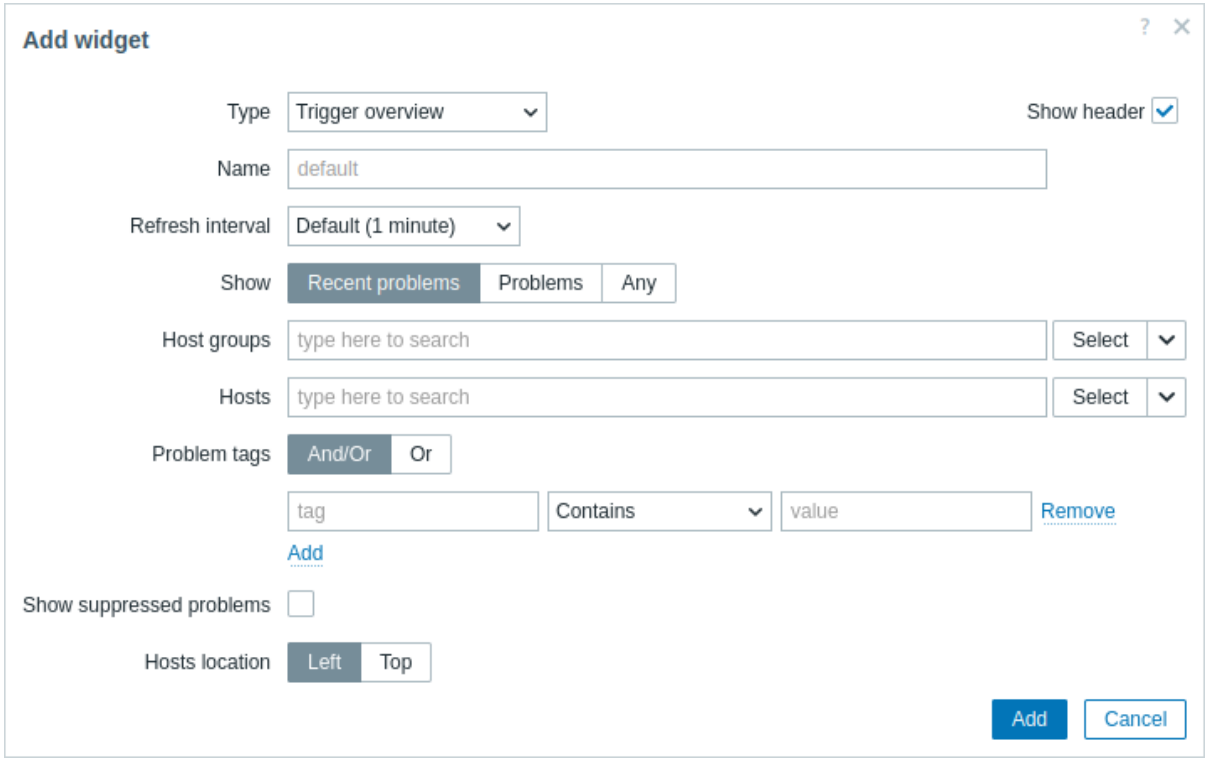
Note:
Kolory ważności wyzwalaczy można dostosować w *Administracja* > *Ogólne*. Poziomy ważności wyzwalaczy można zmieniać podczas aktualizacji problemów.

Kliknięcie bloku udostępnia odnośniki do informacji związanych z wyzwalaczem (problemy, konfiguracja wyzwalacza itp.).

Domyślnie wyświetlanych jest maksymalnie 50 rekordów (wartość konfigurowalna w *Administracja* > *Ogólne* > *GUI* w opcji *Maksymalna liczba kolumn i wierszy w tabelach przeglądu*). Jeśli istnieje więcej wyzwalaczy, zostanie wyświetlony komunikat z prośbą o doprecyzowanie kryteriów filtrowania. Ten limit jest stosowany przed zastosowaniem dodatkowego filtrowania (na przykład według tagów).

Konfiguracja

Aby skonfigurować widget, wybierz *Przegląd wyzwalaczy* jako typ:



Oprócz parametrów wspólnych dla wszystkich widgetów, możesz ustawić następujące opcje specyficzne:

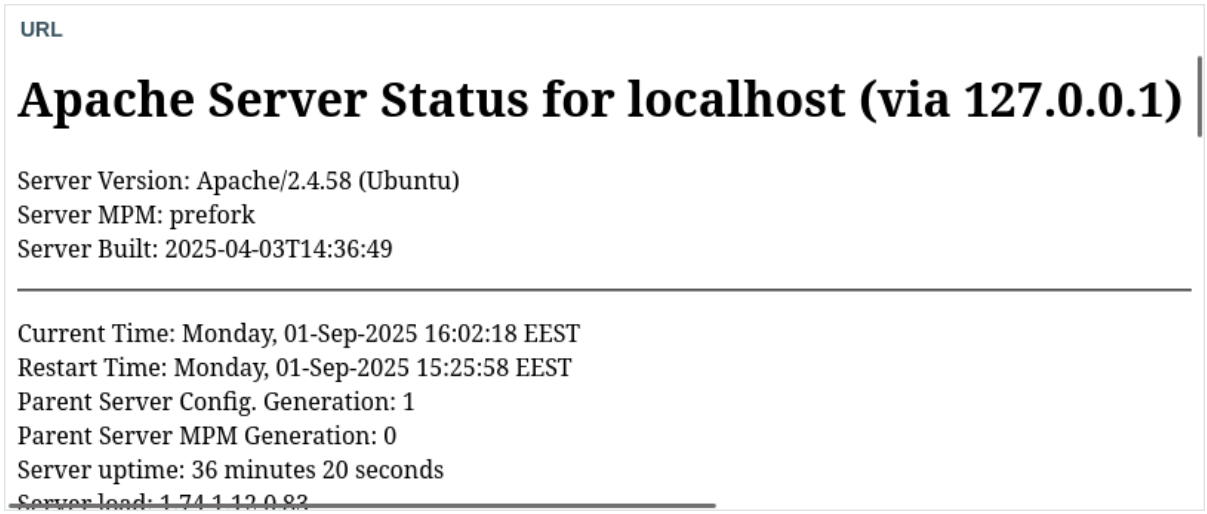
Pokaż	Filtruj wyzwalacze według stanu wyzwalacza: **Ostatnie problemy** - *(domyślnie)* pokazuj wyzwalacze, które niedawno były lub nadal są w stanie PROBLEM (rozwiązane i nierozwiązane); **Problemy** - pokazuj wyzwalacze, które są w stanie PROBLEM (nierozwiązane); **Dowolne** - pokazuj wszystkie wyzwalacze.
Grupy hostów	Wybierz grupy hostów. Alternatywnie wybierz zgodny widget jako źródło danych dla grup hostów. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy grupy zostanie wyświetlona rozwijana lista pasujących grup. Ten parametr nie jest dostępny podczas konfigurowania widgetu na pulpicie szablonu.
Hosty	Wybierz hosty. Alternatywnie wybierz zgodny widget lub pulpit jako źródło danych dla hostów. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy hosta zostanie wyświetlona rozwijana lista pasujących hostów. Ten parametr nie jest dostępny podczas konfigurowania widgetu na pulpicie szablonu.

Tagi problemów	Określ tagi do filtrowania wyzwalaczy wyświetlanych w widżecie. Można zarówno uwzględniać, jak i wykluczać określone tagi oraz wartości tagów. Można ustawić kilka warunków. Dopasowanie nazw tagów zawsze uwzględnia wielkość liter. **Uwaga:** Jeśli parametr *Pokaż* jest ustawiony na „Dowolne”, zostaną wyświetlone wszystkie wyzwalacze, nawet jeśli określono tagi. Jednak chociaż ostatnie zmiany stanu wyzwalacza (wyświetlane jako migające bloki) będą aktualizowane dla wszystkich wyzwalaczy, szczegóły stanu wyzwalacza (kolor ważności problemu oraz informacja, czy problem został potwierdzony) będą aktualizowane tylko dla wyzwalaczy pasujących do określonych tagów. Dla każdego warunku dostępnych jest kilka operatorów: **Istnieje** - uwzględnij określone nazwy tagów; **Równa się** - uwzględnij określone nazwy i wartości tagów (z uwzględnieniem wielkości liter); **Zawiera** - uwzględnij określone nazwy tagów, dla których wartości tagów zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter); **Nie istnieje** - wyklucz określone nazwy tagów; **Nie równa się** - wyklucz określone nazwy i wartości tagów (z uwzględnieniem wielkości liter); **Nie zawiera** - wyklucz określone nazwy tagów, dla których wartości tagów zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter). Dostępne są dwa typy obliczania warunków: **And/Or** - wszystkie warunki muszą być spełnione, a warunki mające tę samą nazwę tagu będą grupowane przez warunek *Or*; **Or** - wystarczy spełnienie jednego warunku.
Pokaż ukryte problemy	Zaznacz pole wyboru, aby wyświetlać problemy, które w przeciwnym razie byłyby ukryte (niepokazywane) z powodu konserwacji hosta.
Układ	Wybierz opcję układu: **Poziomy** - nazwy hostów będą wyświetlane po lewej stronie; **Pionowy** - nazwy hostów będą wyświetlane u góry.

32 URL

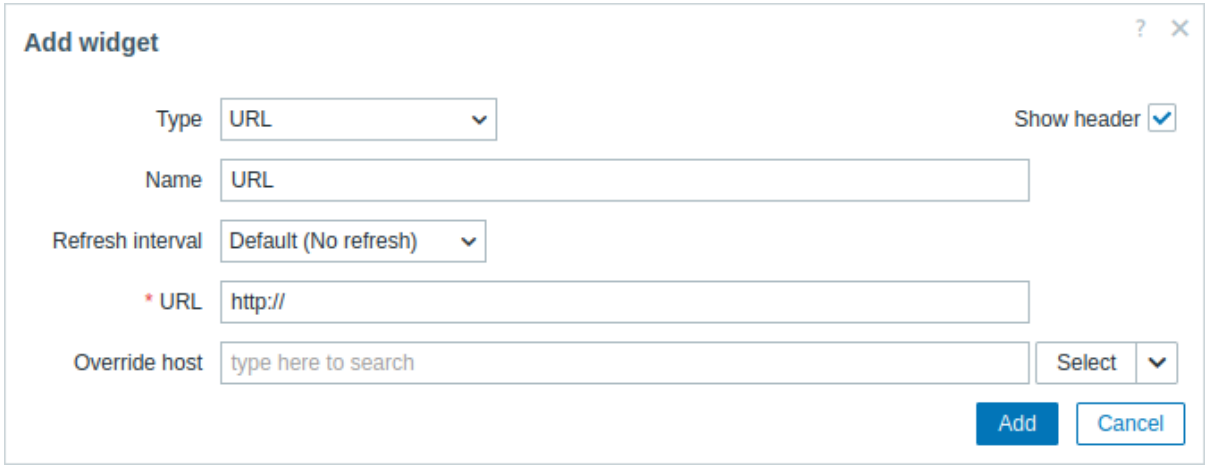
Przegląd

Widżet *URL* wyświetla zawartość pobraną z adresu URL.



Konfiguracja

Aby skonfigurować, wybierz *URL* jako typ:



Oprócz parametrów wspólnych dla wszystkich widżetów, możesz ustawić następujące opcje specyficzne:

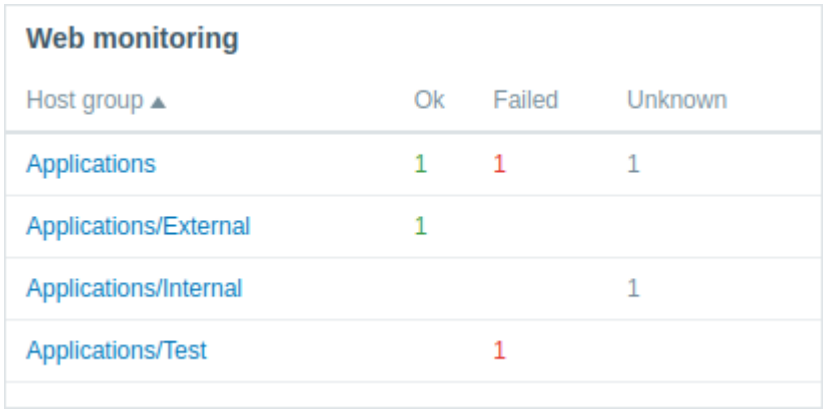
URL	Wprowadź adres URL do wyświetlenia (do 2048 znaków). Zewnętrzne adresy URL muszą zaczynać się od `http://` lub `https://`. Wewnętrzne adresy URL obsługują ścieżki względne (na przykład `zabbix.php?action=report.status`). Makra {HOST.*} są obsługiwane.
Override host	Wybierz zgodny widżet lub selektor hosta pulpitu jako źródło danych dla hostów. Ten parametr nie jest dostępny podczas konfigurowania widżetu na pulpicie szablonu.

Attention:
Przeglądarki mogą nie załadować strony HTTP skonfigurowanej w widżecie, jeśli do frontend Zabbix uzyskuje się dostęp przez HTTPS. Ponadto może być konieczna modyfikacja nagłówka odpowiedzi HTTP X-Frame-Options, aby wyświetlać treść zewnętrzną względem frontend Zabbix.

33 Monitorowanie WWW

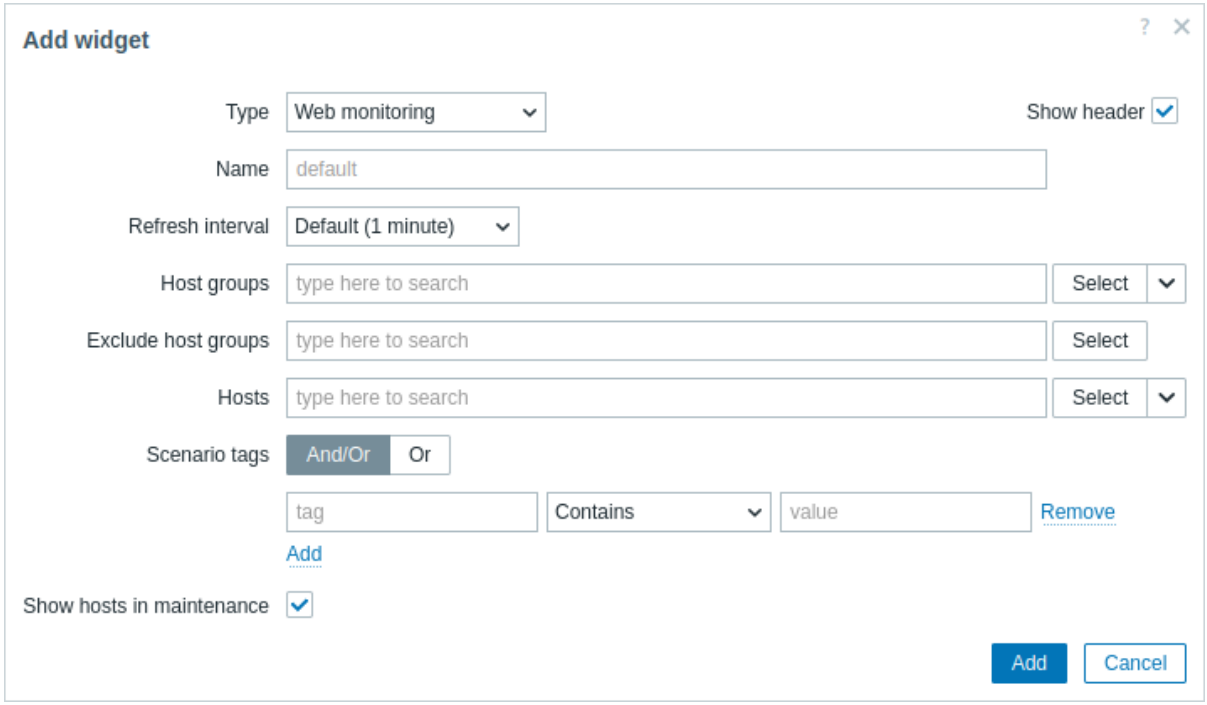
Przegląd

Widżet *Monitorowanie WWW* wyświetla stan aktywnych scenariuszy WWW.



Kliknięcie nazwy grupy hostów otwiera *Monitorowanie* > *Hosty* > *Scenariusze WWW*, gdzie można wyświetlić szczegóły scenariusza.

Konfiguracja



Oprócz parametrów wspólnych dla wszystkich widżetów można ustawić następujące opcje specyficzne:

Grupy hostów	Wybierz grupy hostów do wyświetlenia w widżecie. Alternatywnie wybierz zgodny widżet jako źródło danych dla grup hostów. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy grupy zostanie wyświetlona rozwijana lista pasujących grup. Określenie nadrzędnej grupy hostów powoduje automatyczne wybranie wszystkich zagnieżdżonych grup hostów. Dane hostów z tych grup hostów będą wyświetlane w widżecie; jeśli nie zostaną wprowadzone żadne grupy hostów, wyświetlone zostaną wszystkie grupy hostów. Ten parametr nie jest dostępny podczas konfigurowania widżetu na pulpicie szablonu.
Wyklucz grupy hostów	Wybierz grupy hostów, które mają zostać ukryte w widżecie. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy grupy zostanie wyświetlona rozwijana lista pasujących grup. Określenie nadrzędnej grupy hostów powoduje automatyczne wybranie wszystkich zagnieżdżonych grup hostów. Dane hostów z tych grup hostów nie będą wyświetlane w widżecie. Na przykład hosty 001, 002, 003 mogą należeć do Grupy A, a hosty 002, 003 również do Grupy B. Jeśli jednocześnie wybierzemy *pokazywanie* Grupy A i *wykluczenie* Grupy B, na pulpicie zostaną wyświetlone tylko dane hosta 001. Ten parametr nie jest dostępny podczas konfigurowania widżetu na pulpicie szablonu.
Hosty	Wybierz hosty do wyświetlenia w widżecie. Alternatywnie wybierz zgodny widżet lub pulpit jako źródło danych dla hostów. To pole obsługuje autouzupełnianie, więc po rozpoczęciu wpisywania nazwy hosta zostanie wyświetlona rozwijana lista pasujących hostów. Jeśli nie zostaną wprowadzone żadne hosty, wyświetlone zostaną wszystkie hosty. Ten parametr nie jest dostępny podczas konfigurowania widżetu na pulpicie szablonu.

Tagi scenariuszy	Określ tagi, aby ograniczyć liczbę scenariuszy WWW wyświetlanych w widżecie. Możliwe jest zarówno uwzględnianie, jak i wykluczanie określonych tagów oraz wartości tagów. Można ustawić kilka warunków. Dopasowanie nazw tagów zawsze uwzględnia wielkość liter. Dla każdego warunku dostępnych jest kilka operatorów: **Istnieje** - uwzględnij określone nazwy tagów; **Równa się** - uwzględnij określone nazwy tagów i wartości (z uwzględnieniem wielkości liter); **Zawiera** - uwzględnij określone nazwy tagów, których wartości zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter); **Nie istnieje** - wyklucz określone nazwy tagów; **Nie równa się** - wyklucz określone nazwy tagów i wartości (z uwzględnieniem wielkości liter); **Nie zawiera** - wyklucz określone nazwy tagów, których wartości zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter). Dla warunków dostępne są dwa typy obliczeń: **And/Or** - wszystkie warunki muszą być spełnione, warunki mające tę samą nazwę tagu będą grupowane warunkiem *Or*; **Or** - wystarczy, że jeden warunek zostanie spełniony.
Pokaż hosty w konserwacji	Uwzględnij w statystykach hosty będące w konserwacji. Ten parametr ma etykietę *Pokaż dane w konserwacji* podczas konfigurowania widżetu na pulpicie szablonu.

2 Monitorowanie

Przegląd

Menu Monitoring służy do wyświetlania danych. Niezależnie od tego, jakie informacje Zabbix jest skonfigurowany do zbierania, wizualizacji i reagowania na nie, będą one wyświetlane w różnych sekcjach menu Monitoring.

Przyciski trybu widoku

Następujące przyciski znajdujące się w prawym górnym rogu są wspólne dla każdej sekcji:

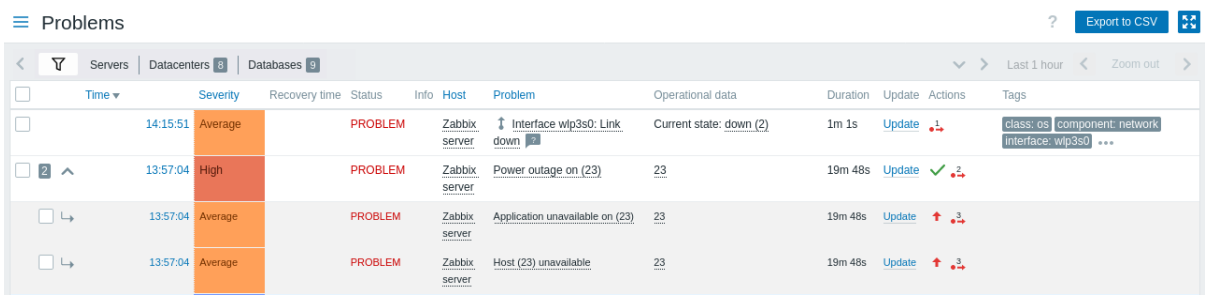
	Wyświetl stronę w trybie kiosku. W tym trybie wyświetlana jest tylko zawartość strony. Aby opuścić tryb kiosku, przesuń kursor myszy, aż pojawi się przycisk wyjścia  , a następnie kliknij go. Zostaniesz przeniesiony z powrotem do trybu normalnego.

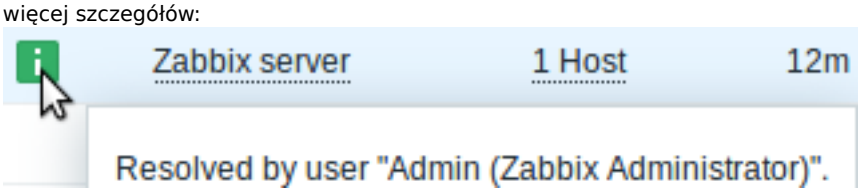
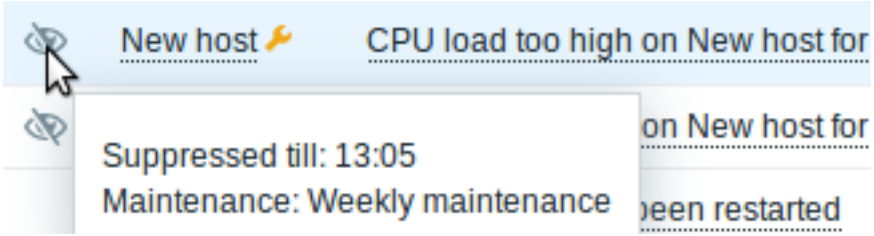
1 Problemy

Przegląd

W *Monitoring* > *Problemy* możesz zobaczyć, jakie problemy aktualnie występują. Problemy to te wyzwalacze, które znajdują się w stanie „Problem”.

Domyślnie wszystkie nowe problemy są klasyfikowane jako problemy przyczynowe. Można ręcznie przeklasyfikować określone problemy jako problemy objawowe problemu przyczynowego. Więcej szczegółów znajduje się w sekcji zdarzenia przyczynowe i objawowe.



Kolumna	Opis
Pole wyboru	Wyświetlane są pola wyboru do zaznaczania problemów. Ikony obok pól wyboru mają następujące znaczenie:  - liczba zdarzeń objawowych dla problemu przyczynowego;  - rozwiń, aby wyświetlić zdarzenia objawowe;  - zwiń, aby ukryć zdarzenia objawowe;  - to jest zdarzenie objawowe.
Czas	Wyświetlany jest czas rozpoczęcia problemu.
Ważność	Wyświetlana jest ważność problemu. Ważność problemu jest początkowo oparta na ważności bazowego wyzwalacza problemu, jednak po wystąpieniu zdarzenia może zostać zaktualizowana za pomocą ekranu *Aktualizacja problemu*. Kolor ważności problemu jest używany jako tło komórki przez czas trwania problemu.
Czas rozwiązania	Wyświetlany jest czas rozwiązania problemu.
Status	Wyświetlany jest status problemu: **Problem** - nierozwiązany problem **Rozwiązany** - niedawno rozwiązany problem. Możesz ukryć niedawno rozwiązane problemy za pomocą filtra. Nowe i niedawno rozwiązane problemy migają przez 2 minuty. Rozwiązane problemy są wyświetlane łącznie przez 5 minut. Obie te wartości można skonfigurować w *Administracja* > *Ogólne* > *Opcje wyświetlania wyzwalaczy*.
Informacje	Wyświetlana jest zielona ikona informacyjna, jeśli problem został zamknięty przez globalną korelację lub ręcznie podczas aktualizacji problemu. Najechanie kursorem na ikonę wyświetli więcej szczegółów:  Następująca ikona jest wyświetlana, jeśli pokazywany jest stłumiony problem (zobacz opcję *Pokaż stłumione problemy* w filtrze). Najechanie kursorem na ikonę wyświetli więcej szczegółów: 
Host	Wyświetlany jest host problemu. Kliknięcie nazwy hosta otwiera menu hosta.
Problem	Wyświetlana jest nazwa problemu. Nazwa problemu jest oparta na nazwie bazowego wyzwalacza problemu. Makra w nazwie wyzwalacza są rozwijane w momencie wystąpienia problemu i rozwinięte wartości nie są już później aktualizowane. *Uwaga*: możliwe jest dołączenie do nazwy problemu danych operacyjnych pokazujących niektóre najnowsze wartości pozycji. Kliknięcie nazwy problemu otwiera menu zdarzenia. Najechanie kursorem na ikonę  po nazwie problemu spowoduje wyświetlenie opisu wyzwalacza (dla tych problemów, które go mają).
Dane operacyjne	Wyświetlane są dane operacyjne zawierające najnowsze wartości pozycji. Dane operacyjne mogą być kombinacją tekstu i makr wartości pozycji, jeśli zostały skonfigurowane na poziomie wyzwalacza. Jeśli na poziomie wyzwalacza nie skonfigurowano danych operacyjnych, wyświetlane są najnowsze wartości wszystkich pozycji z wyrażenia. Ta kolumna jest wyświetlana tylko wtedy, gdy dla opcji *Pokaż dane operacyjne* w filtrze wybrano *Oddzielnie*.
Czas trwania	Wyświetlany jest czas trwania problemu. Zobacz także: Ujemny czas trwania problemu
Aktualizacja	Kliknij łącze *Aktualizacja*, aby przejść do ekranu aktualizacji problemu, gdzie można wykonać różne działania dotyczące problemu, w tym dodać komentarz i potwierdzić problem.

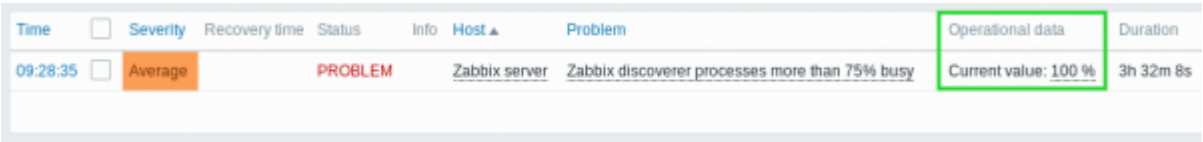
Kolumna	Opis
Działania	Historia aktywności dotyczących problemu jest wyświetlana za pomocą symbolicznych ikon:  - problem został potwierdzony. Ta ikona jest zawsze wyświetlana jako pierwsza.  - dodano komentarze. Wyświetlana jest również liczba komentarzy.  - ważność problemu została zwiększona (np. Informacja > Ostrzeżenie).  - ważność problemu została zmniejszona (np. Ostrzeżenie > Informacja).  - ważność problemu została zmieniona, ale wróciła do pierwotnego poziomu (np. Ostrzeżenie > Informacja > Ostrzeżenie).  - problem został stłumiony.  - problem przestał być stłumiony.  - wykonano działania. Wyświetlana jest również liczba działań.  - wykonano działania, co najmniej jedno jest w toku. Wyświetlana jest również liczba działań.  - wykonano działania, co najmniej jedno zakończyło się niepowodzeniem. Wyświetlana jest również liczba działań. Po najechaniu kursorem na ikony wyświetlane są wyskakujące okna ze szczegółami aktywności. Zobacz wyświetlanie szczegółów, aby dowiedzieć się więcej o ikonach używanych w wyskakującym oknie dla wykonanych działań.
Tagi	Wyświetlane są tagi (jeśli istnieją). Dodatkowo mogą być również wyświetlane tagi z zewnętrznego systemu zgłoszeń (zobacz opcję *Process tags* podczas konfigurowania webhooków).

Dane operacyjne problemów

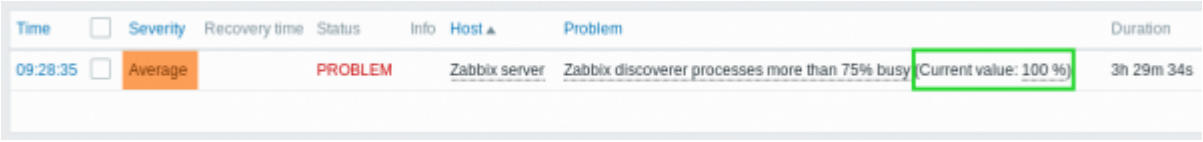
Możliwe jest wyświetlanie danych operacyjnych dla bieżących problemów, tj. najnowszych wartości pozycji, w przeciwieństwie do wartości pozycji z momentu wystąpienia problemu.

Wyświetlanie danych operacyjnych można skonfigurować w filtrze *Monitoring* > *Problems* lub w konfiguracji odpowiedniego widgetu pulpitu, wybierając jedną z trzech opcji:

- *Brak* - dane operacyjne nie są wyświetlane
- *Oddzielnie* - dane operacyjne są wyświetlane w osobnej kolumnie



- *Z nazwą problemu* - dane operacyjne są dołączane do nazwy problemu i umieszczane w nawiasach. Dane operacyjne są dołączane do nazwy problemu tylko wtedy, gdy pole *Operational data* w konfiguracji wyzwalacza nie jest puste.



Zawartość danych operacyjnych można skonfigurować dla każdego wyzwalacza w polu *Operational data*. To pole akceptuje dowolny ciąg znaków zawierający makra, a najważniejszym z nich jest makro `{ITEM.LASTVALUE<1-9>}`.

`{ITEM.LASTVALUE<1-9>}` w tym polu będzie zawsze rozwijane do najnowszych wartości pozycji w wyrażeniu wyzwalacza. `{ITEM.VALUE<1-9>}` w tym polu będzie rozwijane do wartości pozycji z momentu zmiany stanu wyzwalacza (tj. przejścia do stanu `**Problem**`, przejścia do stanu `**OK**`, ręcznego zamknięcia przez użytkownika lub zamknięcia przez korelację).

Należy pamiętać, że ręczne zamknięcie problemu nie powoduje utworzenia nowej wartości, więc rozwinięta wartość `{ITEM.LASTVALUE<1-9>}` lub `{ITEM.VALUE<1-9>}` nadal będzie pokazywać wartość z czasu wystąpienia problemu.

`{ITEM.LASTVALUE<1-9>}` lub `{ITEM.VALUE<1-9>}` zostanie rozwinięte do *UNKNOWN*, jeśli najnowsza wartość historii została zebrana wcześniej niż wynosi czas *Max history display period* (zobacz *Administration > General*).

Ujemny czas trwania problemu

W niektórych typowych sytuacjach rzeczywiście możliwe jest wystąpienie ujemnego czasu trwania problemu, tj. gdy czas rozwiązania problemu jest wcześniejszy niż czas utworzenia problemu, np.:

- Jeśli jakiś host jest monitorowany przez proxy i wystąpi błąd sieci, w wyniku którego przez pewien czas nie są odbierane dane z proxy, wyzwalacz nodata(/host/key) zostanie uruchomiony przez serwer. Po przywróceniu połączenia serwer otrzyma dane pozycji z proxy z czasem z przeszłości. Następnie problem nodata(/host/key) zostanie rozwiązany i będzie miał ujemny czas trwania problemu;
- Gdy dane pozycji rozwiązujące zdarzenie problemu są wysyłane przez Zabbix sender i zawierają znacznik czasu wcześniejszy niż czas utworzenia problemu, również zostanie wyświetlony ujemny czas trwania problemu.

Note:
Ujemny czas trwania problemu nie wpływa w żaden sposób na obliczanie SLA ani raport dostępności dla danego wyzwalacza; nie skraca ani nie wydłuża czasu trwania problemu.

Opcje masowej edycji

Przyciski poniżej listy oferują kilka opcji masowej edycji:

- *Masowa aktualizacja* — aktualizacja wybranych problemów poprzez przejście do ekranu aktualizacji problemu

Aby użyć tej opcji, zaznacz pola wyboru przy odpowiednich problemach, a następnie kliknij przycisk *Masowa aktualizacja*.

Przyciski

Przycisk po prawej stronie oferuje następującą opcję:

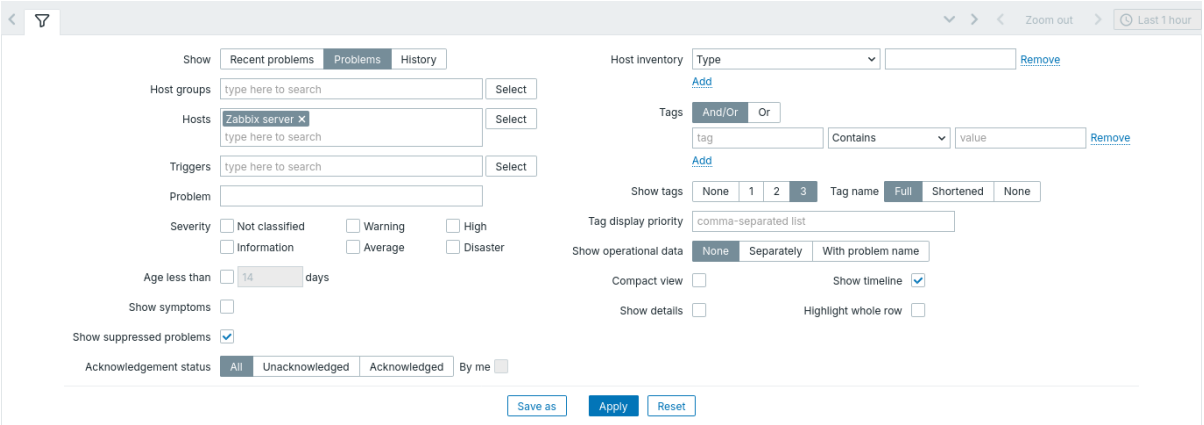
Export to CSV	Eksportuj zawartość ze wszystkich stron do pliku CSV.

Przyciski trybu widoku, wspólne dla wszystkich sekcji, zostały opisane na stronie Monitoring.

Używanie filtra

Możesz użyć filtra, aby wyświetlać tylko te problemy, które Cię interesują. Dla lepszej wydajności wyszukiwania dane są przeszukiwane z nierozwiniętymi makrami.

Filtr znajduje się nad tabelą. Ulubione ustawienia filtra można zapisać jako karty, a następnie szybko uzyskać do nich dostęp, klikając karty nad filtrem.



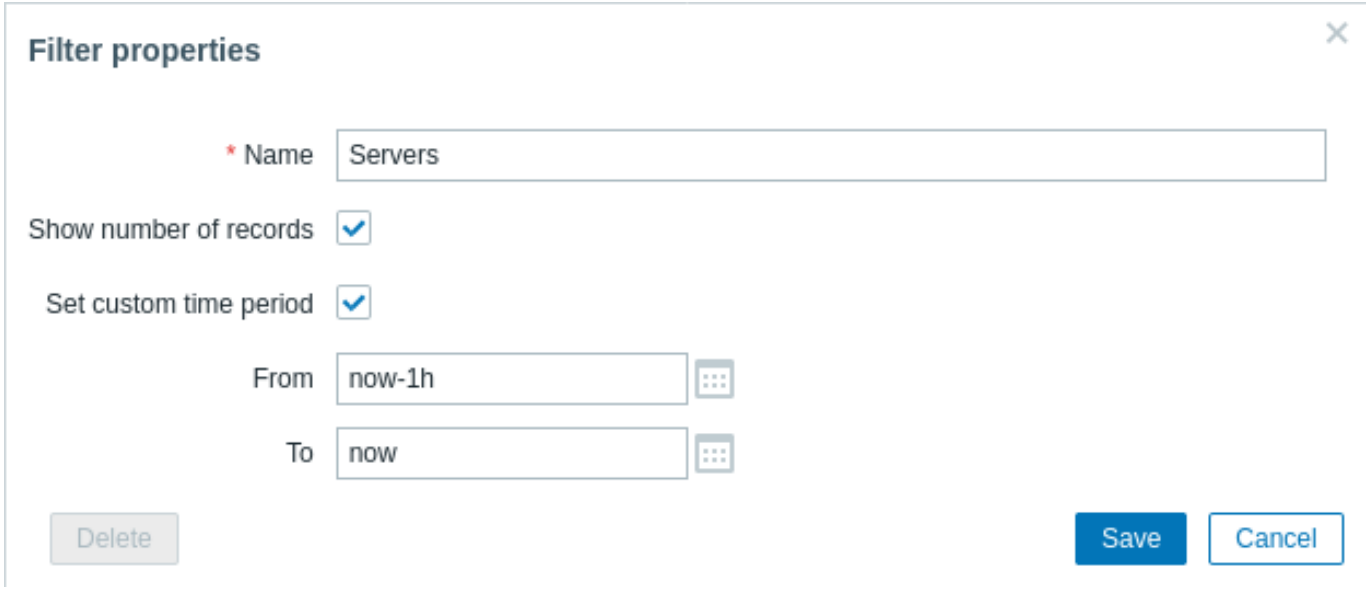
Parametr	Opis
Pokaż	Filtruj według statusu problemu: **Ostatnie problemy** - wyświetlane są nierozwiązane i ostatnio rozwiązane problemy (domyślnie) **Problemy** - wyświetlane są nierozwiązane problemy **Historia** - wyświetlana jest historia wszystkich zdarzeń
Grupy hostów	Filtruj według jednej lub większej liczby grup hostów. Określenie nadrzędnej grupy hostów powoduje automatyczne wybranie wszystkich zagnieżdżonych grup hostów.

Parametr	Opis
Hosty	Filtruj według jednego lub większej liczby hostów.
Wyzwalacze	Filtruj według jednego lub większej liczby wyzwalaczy.
Problem	Filtruj według nazwy problemu.
Istotność	Filtruj według istotności wyzwalacza (problemu).
Wiek mniejszy niż	Filtruj według wieku problemu.
Pokaż symptomy	Zaznacz pole wyboru, aby wyświetlać problemy sklasyfikowane jako symptomy w osobnym wierszu.
Pokaż ukryte problemy	Zaznacz pole wyboru, aby wyświetlać problemy, które w przeciwnym razie byłyby ukryte (niewyświetlane) z powodu konserwacji hosta lub pojedynczego tłumienia problemów.
Status potwierdzenia	Filtruj, aby wyświetlać wszystkie problemy, tylko niepotwierdzone problemy albo tylko potwierdzone problemy. Zaznacz dodatkowe pole wyboru, aby odfiltrować problemy kiedykolwiek potwierdzone przez Ciebie.
Inwentaryzacja hosta	Filtruj według typu i wartości inwentaryzacji.
Tagi	Filtruj według nazwy i wartości tagu zdarzenia. Możliwe jest zarówno uwzględnianie, jak i wykluczanie określonych tagów i wartości tagów. Można ustawić kilka warunków. Dopasowanie nazwy tagu zawsze uwzględnia wielkość liter. Dla każdego warunku dostępnych jest kilka operatorów: **Istnieje** - uwzględnij określone nazwy tagów **Równa się** - uwzględnij określone nazwy i wartości tagów (z uwzględnieniem wielkości liter) **Zawiera** - uwzględnij określone nazwy tagów, których wartości zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter) **Nie istnieje** - wyklucz określone nazwy tagów **Nie równa się** - wyklucz określone nazwy i wartości tagów (z uwzględnieniem wielkości liter) **Nie zawiera** - wyklucz określone nazwy tagów, których wartości zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter) Dostępne są dwa typy obliczania warunków: **And/Or** - wszystkie warunki muszą być spełnione, a warunki mające tę samą nazwę tagu będą grupowane operatorem Or **Or** - wystarczy spełnienie jednego warunku Po przefiltrowaniu tagi określone tutaj będą wyświetlane przy problemie jako pierwsze, chyba że zostanie to nadpisane przez listę *Priorytet wyświetlania tagów* (patrz poniżej).
Pokaż tagi	Wybierz liczbę wyświetlanych tagów: **Brak** - brak kolumny *Tagi* w *Monitoring* > *Problemy* **1** - kolumna *Tagi* zawiera jeden tag **2** - kolumna *Tagi* zawiera dwa tagi **3** - kolumna *Tagi* zawiera trzy tagi Aby zobaczyć wszystkie tagi problemu, najedź kursorem myszy na ikonę trzech kropek.
Nazwa tagu	Wybierz tryb wyświetlania nazwy tagu: **Pełna** - nazwy i wartości tagów są wyświetlane w całości **Skrócona** - nazwy tagów są skracane do 3 znaków; wartości tagów są wyświetlane w całości **Brak** - wyświetlane są tylko wartości tagów; bez nazw
Priorytet wyświetlania tagów	Wprowadź priorytet wyświetlania tagów dla problemu jako listę tagów oddzielonych przecinkami (na przykład: `customer,scope,component`). Należy używać tylko nazw tagów, bez wartości. Tagi z tej listy będą zawsze wyświetlane jako pierwsze, nadpisując naturalną kolejność alfabetyczną.
Pokaż dane operacyjne	Wybierz tryb wyświetlania danych operacyjnych: **Brak** - dane operacyjne nie są wyświetlane **Oddzielnie** - dane operacyjne są wyświetlane w osobnej kolumnie **Z nazwą problemu** - dołącz dane operacyjne do nazwy problemu, używając nawiasów dla danych operacyjnych
Widok kompaktowy	Zaznacz pole wyboru, aby włączyć widok kompaktowy.
Pokaż szczegóły	Zaznacz pole wyboru, aby wyświetlać bazowe wyrażenia wyzwalaczy problemów. Opcja niedostępna, jeśli zaznaczone jest pole wyboru *Widok kompaktowy*.
Pokaż oś czasu	Zaznacz pole wyboru, aby wyświetlać wizualną oś czasu i grupowanie. Opcja niedostępna, jeśli zaznaczone jest pole wyboru *Widok kompaktowy*.
Podświetl cały wiersz	Zaznacz pole wyboru, aby podświetlać cały wiersz dla nierozwiązanych problemów. Do podświetlenia używany jest kolor istotności problemu. *Podświetl cały wiersz* nie jest dostępne w motywach o wysokim kontraście.

Karty ulubionych filtrów

Często używane zestawy parametrów filtra można zapisać w kartach.

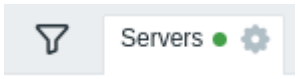
Aby zapisać nowy zestaw parametrów filtra, otwórz główną kartę i skonfiguruj ustawienia filtra, a następnie naciśnij przycisk *Zapisz jako*. W nowym wyskakującym oknie zdefiniuj *Właściwości filtra*.



Parametr	Opis
Nazwa	Nazwa filtra wyświetlana na liście kart.
Pokaż liczbę rekordów	Zaznacz, jeśli chcesz, aby liczba problemów była wyświetlana obok nazwy karty.
Zastąp selektor przedziału czasu	Zaznacz, aby ustawić określony domyślny przedział czasu dla tego zestawu filtrów. Jeśli ustawione, zmianę przedziału czasu dla tej karty będzie można wykonać tylko przez aktualizację ustawień filtra. Dla kart bez niestandardowego przedziału czasu zakres czasu można zmienić, naciskając przycisk selektora czasu w prawym górnym rogu (nazwa przycisku zależy od wybranego przedziału czasu: Ten tydzień, Ostatnie 30 minut, Wczoraj itd.). Ta opcja jest dostępna tylko dla filtrów w *Monitoring* > *Problemy*.
Od/Do	Początek i koniec przedziału czasu w składni czasu bezwzględnego (`Y-m-d H:i:s`) lub względnego (`now-1d`). Dostępne, jeśli zaznaczono *Ustaw niestandardowy przedział czasu*.

Po zapisaniu filtr zostanie utworzony jako nazwana karta filtra i natychmiast aktywowany.

Aby edytować właściwości filtra istniejącego filtra, naciśnij symbol koła zębatego obok nazwy aktywnej karty.



Uwagi:

- Aby ukryć obszar filtra, kliknij nazwę bieżącej karty. Kliknij ponownie nazwę aktywnej karty, aby ponownie otworzyć obszar filtra.
- Obsługiwana jest nawigacja za pomocą klawiatury: użyj strzałek, aby przełączać się między kartami, naciśnij *Enter*, aby otworzyć.
- Przyciski w lewo/w prawo nad filtrem mogą być używane do przełączania między zapisanymi filtrami. Alternatywnie przycisk skierowany w dół otwiera menu rozwijane ze wszystkimi zapisanymi filtrami i można kliknąć ten, którego potrzebujesz.
- Karty filtrów można przestawiać metodą przeciągnij i upuść.
- Jeśli ustawienia zapisanego filtra zostały zmienione (ale nie zapisane), po nazwie filtra wyświetlana jest zielona kropka. Aby zaktualizować filtr zgodnie z nowymi ustawieniami, kliknij przycisk *Aktualizuj*, który jest wyświetlany zamiast przycisku *Zapisz jako*.
- Bieżące ustawienia filtra są zapamiętywane w profilu użytkownika. Gdy użytkownik ponownie otworzy stronę, ustawienia filtra pozostaną takie same.

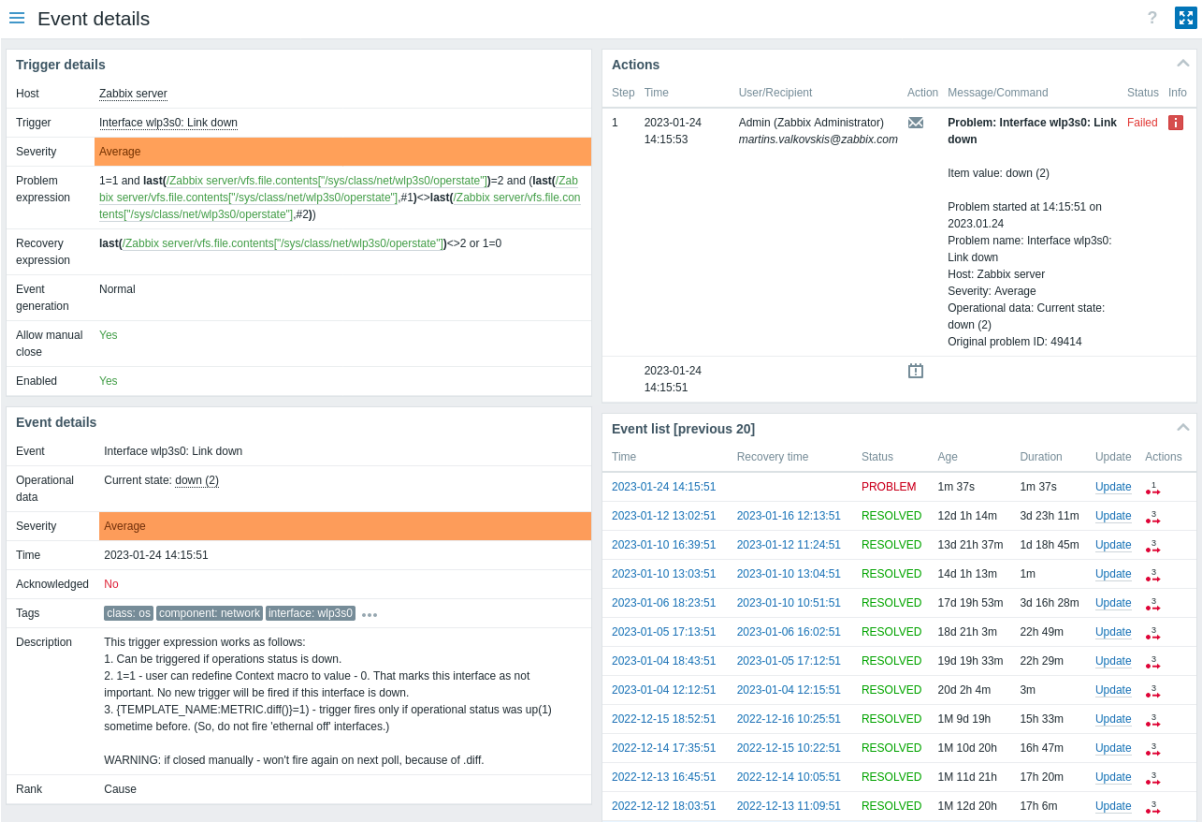
Note:
Aby udostępnić filtry, skopiuj adres URL aktywnego filtra i wyślij go innym. Po otwarciu tego adresu URL inni użytkownicy będą mogli zapisać ten zestaw parametrów jako trwały filtr na swoim koncie Zabbix.
Zobacz także: Parametry strony.

Przyciski filtra

Apply	Zastosuj określone kryteria filtrowania (bez zapisywania).
Reset	Zresetuj bieżący filtr i przywróć zapisane parametry bieżącej karty. Na karcie głównej spowoduje to wyczyszczenie filtra.
Save as	Zapisz bieżące parametry filtra na nowej karcie. Dostępne tylko na karcie głównej.
Update	Zastąp parametry karty aktualnie określonymi parametrami. Niedostępne na karcie głównej.

Wyświetlanie szczegółów

Czasy rozpoczęcia problemu i powrotu do normy w *Monitoring* > *Problems* są linkami. Kliknięcie ich otwiera bardziej szczegółowe informacje o zdarzeniu.



Należy pamiętać, że ważność problemu może różnić się dla wyzwalacza i zdarzenia problemu — jeśli została zaktualizowana dla zdarzenia problemu przy użyciu ekranu *Update problem*.

Na liście działań używane są następujące ikony do oznaczania typu aktywności:

-  - wygenerowano zdarzenie problemu.
-  - wiadomość została wysłana.
-  - zdarzenie problemu zostało potwierdzone.
-  - cofnięto potwierdzenie zdarzenia problemu.
-  - dodano komentarz.
-  - ważność problemu została zwiększona (np. Informacja > Ostrzeżenie).
-  - ważność problemu została zmniejszona (np. Ostrzeżenie > Informacja).
-  - ważność problemu została zmieniona, ale wróciła do pierwotnego poziomu (np. Ostrzeżenie > Informacja > Ostrzeżenie).

-  - wykonano zdalne polecenie.
-  - zdarzenie problemu wróciło do normy.
-  - problem został zamknięty ręcznie.
-  - problem został wyciszony.
-  - wyłączono wyciszenie problemu.
-  - problem został przekształcony w problem będący symptomem.
-  - problem został przekształcony w problem będący przyczyną.

1 Problemy przyczyn i objawów

Przegląd

Domyślnie wszystkie nowe problemy są klasyfikowane jako problemy przyczynowe. Możliwe jest ręczne przeklasyfikowanie określonych problemów na problemy objawowe problemu przyczynowego.

Na przykład awaria zasilania może być rzeczywistą przyczyną źródłową, przez którą jakiś host jest nieosiągalny lub jakaś usługa nie działa. W takim przypadku problemy „host jest nieosiągalny” i „usługa nie działa” muszą zostać sklasyfikowane jako problemy objawowe problemu „awaria zasilania” — problemu przyczynowego.

Hierarchia przyczyna-objaw obsługuje tylko dwa poziomy. Problemu, który jest już objawem, nie można przypisać „podrzędnych” problemów objawowych; wszelkie problemy przypisane jako objawy do problemu objawowego staną się objawami tego samego problemu przyczynowego.

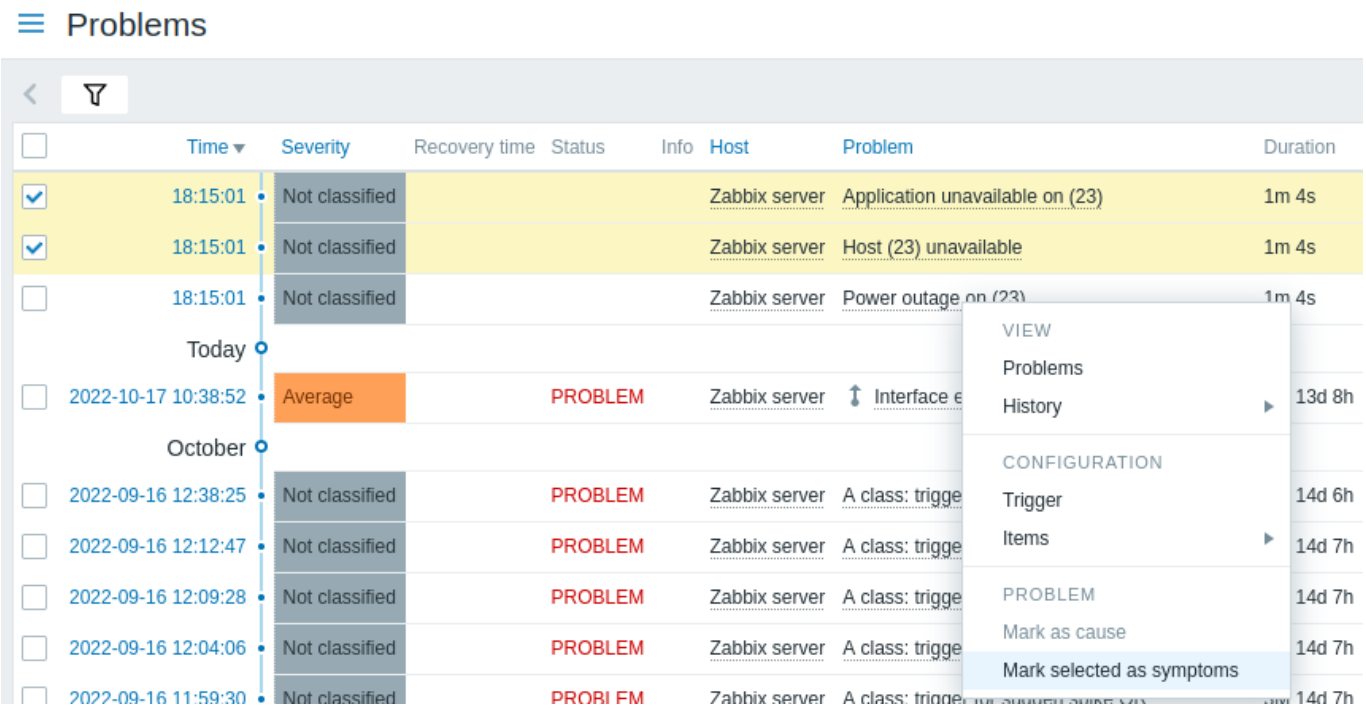
W sumach problemów na mapach, w widżetach pulpitu, takich jak *Problemy według ważności* lub *Hosty problemowe* itd., uwzględniane są tylko problemy przyczynowe. Jednak klasyfikacja problemów nie wpływa na usługi.

Problem objawowy może być powiązany tylko z jednym problemem przyczynowym. Problemy objawowe nie są rozwiązywane automatycznie, jeśli problem przyczynowy zostanie rozwiązany lub zamknięty.

Konfiguracja

Aby przeklasyfikować problem na problem będący symptomem, najpierw wybierz go na liście problemów. Można wybrać jeden lub kilka problemów.

Następnie przejdź do problemu-przyczyny i w jego menu kontekstowym kliknij opcję *Oznacz wybrane jako symptomy*.



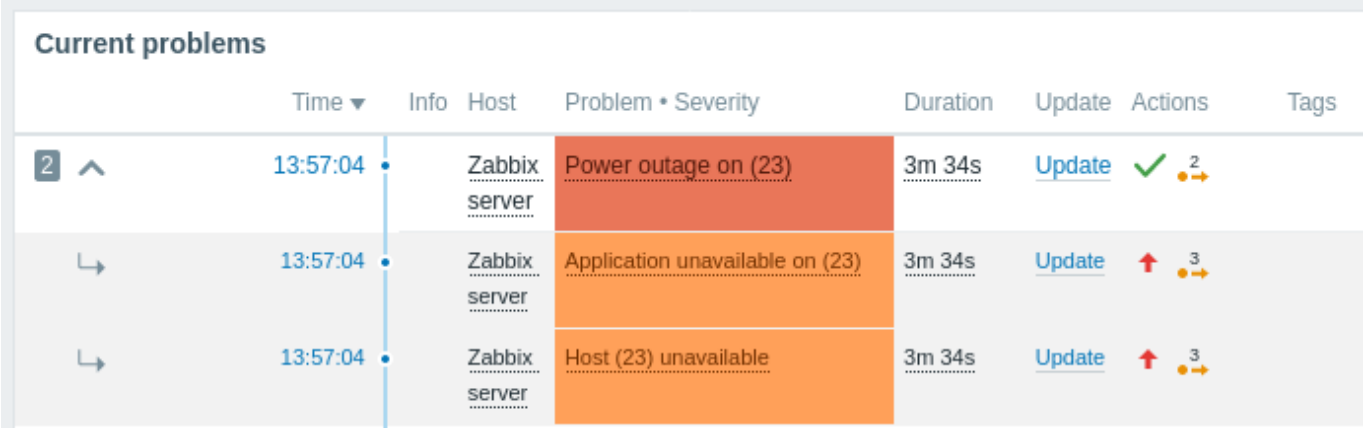
Po tym wybrane problemy zostaną zaktualizowane przez serwer i staną się problemami będącymi symptomami problemu-przyczyny.

Podczas aktualizacji statusu problemu jest on wyświetlany na jeden z dwóch sposobów:

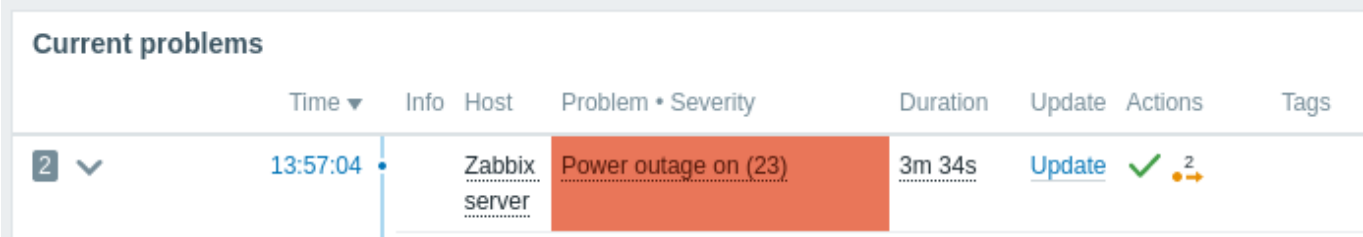
- W kolumnie Status wyświetlany jest migający status „UPDATING”;
- Migająca ikona lub w kolumnie Info (ma to zastosowanie, jeśli w filtrze wybrano tylko *Problemy*, a zatem kolumna Status nie jest wyświetlana).

Wyświetlanie

Problemy symptomów są wyświetlane poniżej problemu przyczyny i odpowiednio oznaczone w *Monitoring -> Problems* (oraz w widżecie pulpitu *Problems*) — za pomocą ikony, mniejszej czcionki i innego tła.



W widoku zwiniętym widoczny jest tylko problem przyczyny; istnienie problemów symptomów jest wskazywane przez liczbę na początku wiersza oraz ikonę rozwijania widoku.



Możliwe jest również dodatkowe wyświetlanie problemów symptomów normalną czcionką i w osobnym wierszu. W tym celu wybierz *Show symptoms* w ustawieniach filtra lub konfiguracji widżetu.

Przywracanie do problemu przyczyny

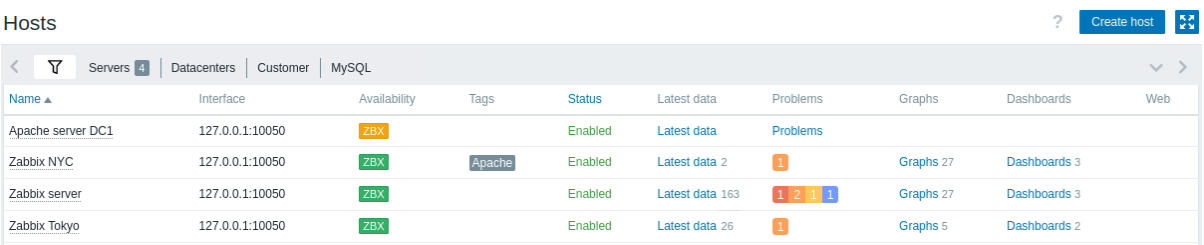
Problem objawu można przywrócić do problemu przyczyny. Aby to zrobić, należy:

- kliknąć opcję *Oznacz jako przyczynę* w menu kontekstowym problemu objawu;
- zaznaczyć opcję *Przekształć w przyczynę* na ekranie aktualizacji problemu i kliknąć *Aktualizuj* (ta opcja zadziała również, jeśli wybrano kilka problemów).

2 Hosty

Przegląd

Sekcja *Monitoring → Hosty* wyświetla pełną listę monitorowanych hostów ze szczegółowymi informacjami o interfejsie hosta, dostępności, tagach, bieżących problemach, statusie (włączony/wyłączony) oraz odnośnikami umożliwiającymi łatwe przejście do najnowszych danych hosta, historii problemów, wykresów, pulpitów i scenariuszy WWW.



Kolumna	Opis
Nazwa	Widoczna nazwa hosta. Kliknięcie nazwy otwiera menu hosta. Pomarańczowa ikona klucza po nazwie wskazuje, że ten host jest w okresie konserwacji. Kliknij nagłówek kolumny, aby sortować hosty według nazwy rosnąco lub malejąco.
Interfejs	Wyświetlany jest główny interfejs hosta.
Dostępność	Wyświetlana jest dostępność hosta dla każdego skonfigurowanego interfejsu. Ikony dostępności przedstawiają bieżący status interfejsu hosta na serwerze Zabbix. Dlatego jeśli wyłączysz host w frontend, jego dostępność zostanie zaktualizowana po zsynchronizowaniu zmian konfiguracji przez serwer Zabbix. Podobnie, jeśli włączysz host, jego dostępność zostanie zaktualizowana po zsynchronizowaniu zmian konfiguracji przez serwer Zabbix i odpytaniu hosta. Ikony dostępności przedstawiają tylko te typy interfejsów (Agent, SNMP, IPMI, JMX), które są skonfigurowane. Najechanie kursorem na ikonę wyświetla wyskakujące okno z listą wszystkich interfejsów tego samego typu wraz ze szczegółami, statusem i błędami. Dla interfejsu Agent wyskakujące okno wyświetla interfejsy (pasywne) oraz aktywne testy. Jeśli host ma tylko aktywne testy, ikona interfejsu Agent jest wyświetlana nawet wtedy, gdy host nie ma skonfigurowanego interfejsu Agent. Kolumna jest pusta dla hostów bez interfejsów. Status pojedynczego interfejsu hosta jest określany przez połączenie między włączoną pozycją używającą tego interfejsu a hostem. Status może być następujący: **Dostępny** - połączenie z hostem zakończyło się powodzeniem; **Niedostępny** - połączenie z hostem nie powiodło się (przekroczenie czasu, problemy z zaporą sieciową itp.); **Nieznany** - nie podjęto próby połączenia z hostem lub wynik jest nieznany. Aby uzyskać dodatkowe informacje o tym, jak serwer Zabbix określa status interfejsu, zobacz Nieznany status interfejsu oraz Ustawienia nieosiągalnego/niedostępnego interfejsu hosta. Status wszystkich interfejsów hosta jednego typu (Agent, SNMP, IPMI, JMX) jest określany przez te interfejsy, które są używane przez co najmniej jedną włączoną pozycję. Status jest wskazywany kolorem ikony: **Zielony** - wszystkie interfejsy są dostępne; **Żółty** - co najmniej jeden interfejs jest niedostępny, a co najmniej jeden jest dostępny lub nieznany; **Czerwony** - wszystkie interfejsy są niedostępne; **Szary** - co najmniej jeden interfejs jest nieznany, ale żaden nie jest niedostępny. **Dostępność aktywnych testów.** Jeśli na hoście włączony jest co najmniej jeden aktywny test, aktywne testy również wpływają na całkowitą dostępność interfejsu Agent, jak opisano powyżej. Aby określić dostępność aktywnych testów, w wątku aktywnych testów agenta wysyłane są komunikaty heartbeat. Częstotliwość komunikatów heartbeat jest kontrolowana przez parametr `HeartbeatFrequency` w konfiguracji Zabbix agent lub agent 2 (domyślnie 60 sekund, zakres 0-3600). Aktywne testy są uznawane za niedostępne, gdy heartbeat aktywnych testów jest starszy niż 2 x HeartbeatFrequency sekund. **Uwaga:** Agenty Zabbix starsze niż wersja 6.2.x nie wysyłają heartbeatów aktywnych testów, dlatego dostępność ich hostów pozostaje nieznana.
Tagi	Tagi hosta i wszystkich podłączonych szablonów, z nierozwiniętymi makrami.
Status	Status hosta - *Włączony* lub *Wyłączony*. Kliknij nagłówek kolumny, aby sortować hosty według statusu rosnąco lub malejąco.
Najnowsze dane	Kliknięcie odnośnika otworzy stronę *Monitoring* - *Najnowsze dane* ze wszystkimi najnowszymi danymi zebranymi z hosta. Liczba pozycji z najnowszymi danymi jest wyświetlana na szaro.
Problemy	Liczba otwartych problemów hosta posortowanych według ważności. Kolor kwadratu wskazuje ważność problemu. Liczba na kwadracie oznacza liczbę problemów dla danej ważności. Kliknięcie ikony otworzy stronę *Monitoring* - *Problemy* dla bieżącego hosta. Jeśli host nie ma problemów, odnośnik do sekcji *Problemy* dla tego hosta jest wyświetlany jako tekst. Użyj filtra, aby wybrać, czy wyciszone problemy mają być uwzględniane (domyślnie nie są uwzględniane).

Kolumna	Opis
Wykresy	Kliknięcie odnośnika spowoduje wyświetlenie wykresów skonfigurowanych dla hosta. Liczba wykresów jest wyświetlana na szaro. Jeśli host nie ma wykresów, odnośnik nie jest wyświetlany.
Pulpity	Kliknięcie odnośnika spowoduje wyświetlenie pulpitów skonfigurowanych dla hosta. Liczba pulpitów jest wyświetlana na szaro. Jeśli host nie ma pulpitów, odnośnik nie jest wyświetlany.
WWW	Kliknięcie odnośnika spowoduje wyświetlenie scenariuszy WWW skonfigurowanych dla hosta. Liczba scenariuszy WWW jest wyświetlana na szaro. Jeśli host nie ma scenariuszy WWW, odnośnik nie jest wyświetlany.

Przyciski

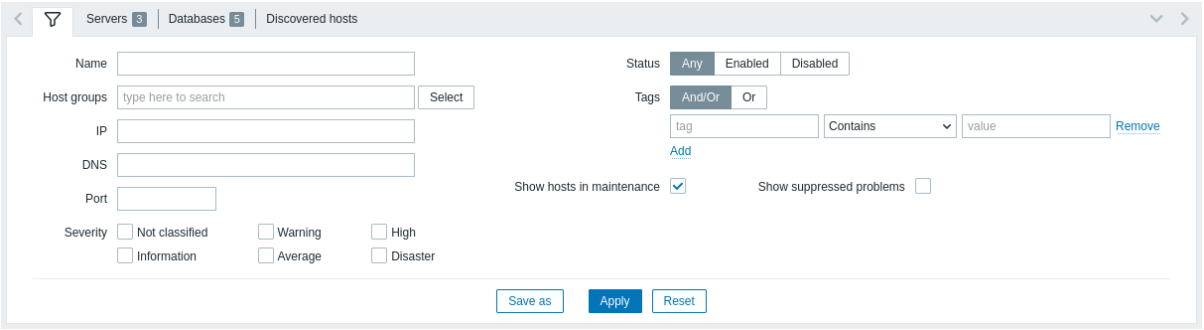
Utwórz host umożliwia utworzenie nowego hosta. Ten przycisk jest dostępny tylko dla użytkowników typu Admin i Super Admin.

Przyciski trybu widoku, wspólne dla wszystkich sekcji, zostały opisane na stronie Monitoring.

Używanie filtra

Możesz użyć filtra, aby wyświetlić tylko te hosty, którymi jesteś zainteresowany. Dla lepszej wydajności wyszukiwania dane są przeszukiwane z nierozwiniętymi makrami.

Filtr znajduje się nad tabelą. Możliwe jest filtrowanie hostów według nazwy, grupy hostów, IP lub DNS, portu interfejsu, tagów, ważności problemu, statusu (włączony/wyłączony/dowolny); możesz także wybrać, czy wyświetlać stłumione problemy oraz hosty, które są obecnie w konserwacji.



Parametr	Opis
Name	Filtruj według widocznej nazwy hosta.
Host groups	Filtruj według jednej lub większej liczby grup hostów. Określenie nadrzędnej grupy hostów powoduje automatyczne wybranie wszystkich zagnieżdżonych grup hostów.
IP	Filtruj według adresu IP.
DNS	Filtruj według nazwy DNS.
Port	Filtruj według numeru portu.
Severity	Filtruj według ważności problemu. Domyślnie wyświetlane są problemy o wszystkich poziomach ważności. Problemy są wyświetlane, jeśli nie są stłumione.
Status	Filtruj według statusu hosta.

Parametr	Opis
Tags	Filtruj według nazwy i wartości tagu hosta. Hosty mogą być filtrowane zarówno według tagów na poziomie hosta, jak i tagów ze wszystkich podłączonych szablonów, w tym szablonów zagnieżdżonych. Możliwe jest zarówno uwzględnianie, jak i wykluczanie określonych tagów oraz wartości tagów. Można ustawić kilka warunków. Dopasowanie nazwy tagu zawsze uwzględnia wielkość liter. Dla każdego warunku dostępnych jest kilka operatorów: **Exists** - uwzględnij określone nazwy tagów **Equals** - uwzględnij określone nazwy i wartości tagów (z uwzględnieniem wielkości liter) **Contains** - uwzględnij określone nazwy tagów, których wartości zawierają wprowadzony ciąg znaków (dopasowanie podciągu, bez uwzględniania wielkości liter) **Does not exist** - wyklucz określone nazwy tagów **Does not equal** - wyklucz określone nazwy i wartości tagów (z uwzględnieniem wielkości liter) **Does not contain** - wyklucz określone nazwy tagów, których wartości zawierają wprowadzony ciąg znaków (dopasowanie podciągu, bez uwzględniania wielkości liter) Istnieją dwa typy obliczania warunków: **And/Or** - wszystkie warunki muszą być spełnione, warunki mające tę samą nazwę tagu będą grupowane operatorem Or **Or** - wystarczy, że jeden warunek zostanie spełniony
Show hosts in maintenance	Zaznacz pole wyboru, aby wyświetlić hosty będące w konserwacji (domyślnie wyświetlane).
Show suppressed problems	Zaznacz pole wyboru, aby wyświetlić problemy, które w przeciwnym razie byłyby stłumione (niewyświetlane) z powodu konserwacji hosta lub pojedynczego problem suppression.

Zapisywanie filtra

Ulubione ustawienia filtra można zapisać jako karty, a następnie szybko uzyskać do nich dostęp, klikając odpowiednią kartę nad filtrem.

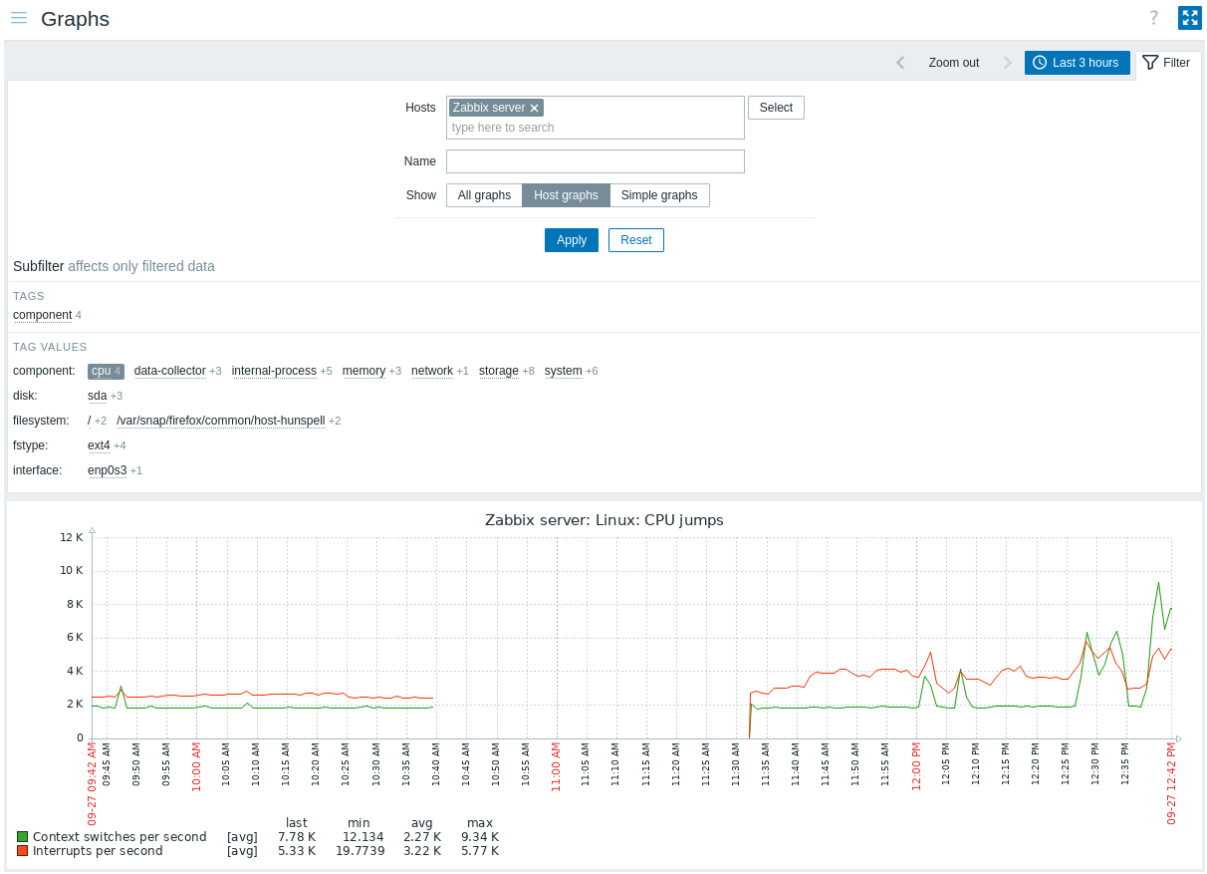
Zobacz więcej szczegółów o zapisywaniu filtrów.

1 Wykresy

Przegląd

Wykresy hosta są dostępne w *Monitoring* → *Hosts* po kliknięciu Wykresy dla odpowiedniego hosta.

Można wyświetlić dowolny wykres niestandardowy, który został skonfigurowany dla hosta, a także dowolny wykres prosty.



Wykresy są sortowane według:

- nazwy wykresu (wykresy niestandardowe)
- nazwy pozycji (wykresy proste)

Wykresy dla wyłączonych hostów są również dostępne.

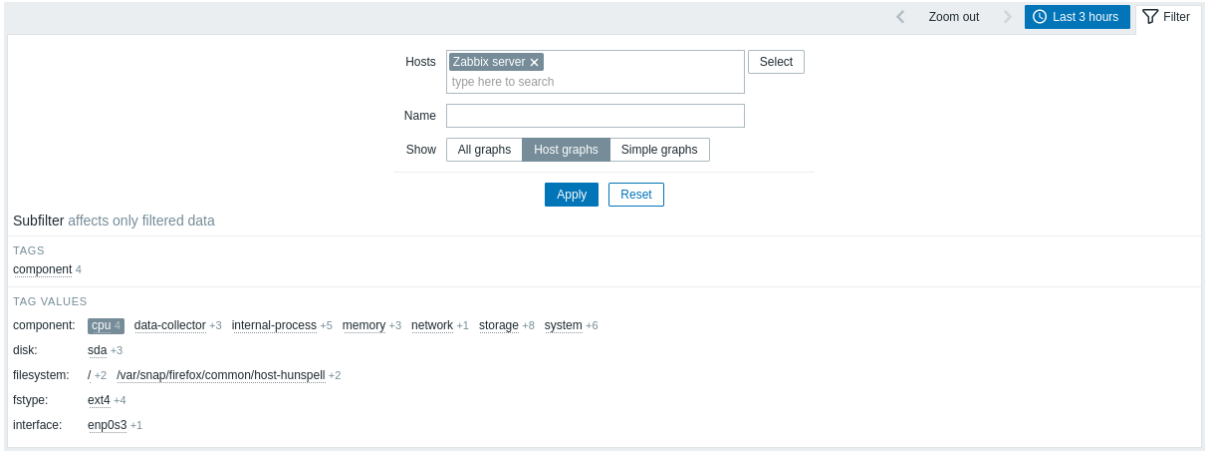
Selektor przedziału czasu

Zwróć uwagę na selektor przedziału czasu nad wykresem. Umożliwia on wybór często wymaganych przedziałów jednym kliknięciem myszy.

Zobacz także: *Selektor przedziału czasu*

Używanie filtra

Aby wyświetlić określony wykres, wybierz go w filtrze. Filtr umożliwia określenie hosta, nazwy wykresu oraz opcji *Pokaż* (wszystkie/wykresy hosta/proste wykresy).



Jeśli w filtrze nie wybrano hosta, żadne wykresy nie są wyświetlane.

Używanie podfiltra

Podfiltr umożliwia dalszą modyfikację filtrowania z filtra głównego.

Zawiera klikalne odnośniki zapewniające szybki dostęp do powiązanych wykresów. Wykresy są powiązane wspólną jednostką — nazwą tagu lub jego wartością. Po kliknięciu nazwy/wartości tagu zostaje ona podświetlona szarym tłem, a wykresy są natychmiast filtrowane (bez potrzeby klikania *Apply* w filtrze głównym). Kliknięcie innej nazwy/wartości tagu dodaje ją do przefiltrowanych wyników. Ponowne kliknięcie nazwy/wartości tagu usuwa filtrowanie.

Podfiltry są generowane na podstawie przefiltrowanych danych, których liczba jest ograniczona do 1000 rekordów. Jeśli chcesz zobaczyć więcej rekordów w podfiltrze, musisz zwiększyć wartość parametru *Limit for search and filter results* (w *Administration -> General -> GUI*).

W przeciwieństwie do filtra głównego podfiltr jest aktualizowany przy każdym żądaniu odświeżenia tabeli, aby zawsze zapewnić aktualne informacje o dostępnych opcjach filtrowania i licznikach ich wystąpień.

Liczba wyświetlanych jednostek jest ograniczona poziomo do 100. Jeśli jest ich więcej, na końcu wyświetlana jest ikona trzech kropek; nie jest ona klikalna. Listy pionowe (takie jak tagi i ich wartości) są ograniczone do 20 wpisów. Jeśli jest ich więcej, wyświetlana jest ikona trzech kropek; nie jest ona klikalna.

Liczba obok każdej klikalnej jednostki wskazuje liczbę wykresów, które znajdują się w wynikach filtra głównego.

Po wybraniu jednej jednostki liczby przy pozostałych dostępnych jednostkach są wyświetlane ze znakiem plus, wskazującym, ile wykresów można dodać do bieżącego wyboru.

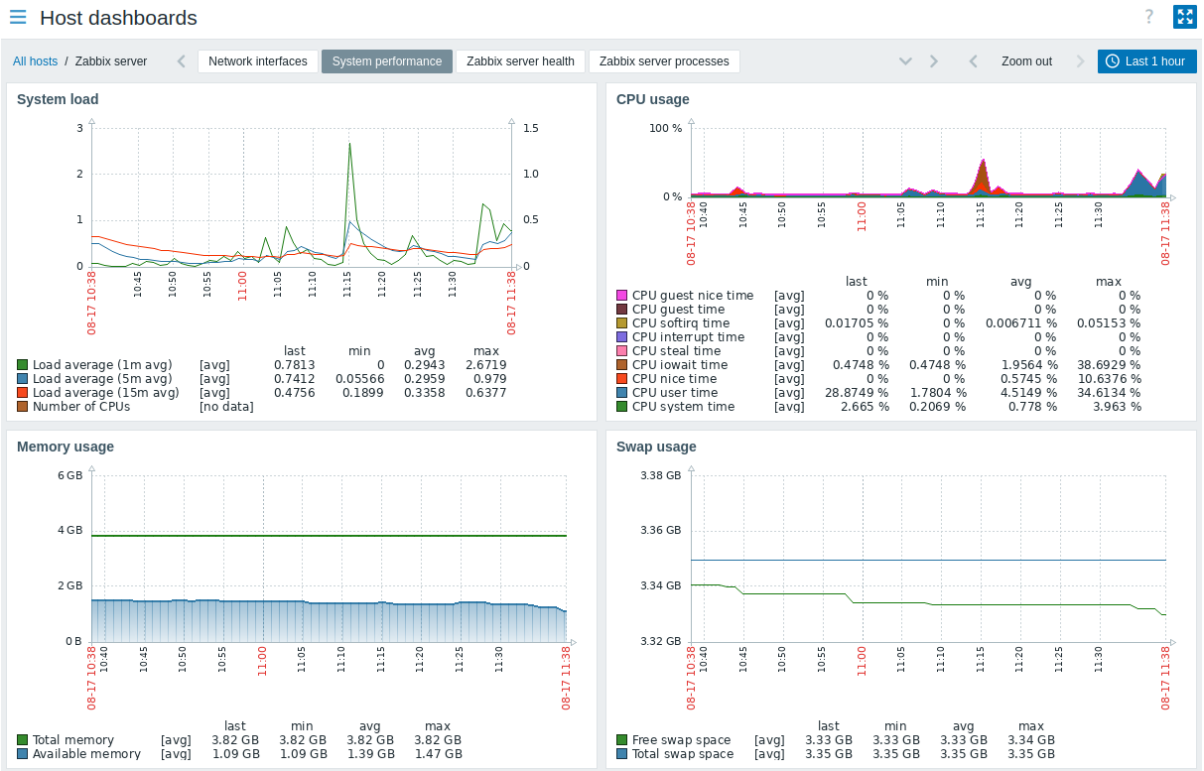
Przyciski

Przyciski trybu widoku, wspólne dla wszystkich sekcji, zostały opisane na stronie Monitoring.

2 Pulpity hosta

Przegląd

Dashboardy hostów wyglądają podobnie do dashboardów globalnych; jednak dashboardy hostów nie mają właściciela i wyświetlają dane tylko dla wybranego hosta.



Podczas przeglądania dashboardów hostów można przełączać się między skonfigurowanymi dashboardami, klikając:

- karty dashboardów;
- przyciski strzałek pod nagłówkiem;
- przycisk strzałki pod nagłówkiem, który wyświetli pełną listę dostępnych dashboardów hostów.

Aby przejść do sekcji *Monitoring* → *Hosts*, kliknij łącze nawigacyjne *All hosts* pod nagłówkiem w lewym górnym rogu.

Konfiguracja

Pulpity hostów są konfigurowane na poziomie szablonu. Po podłączeniu szablonu do hosta dla tego hosta generowane są pulpity hosta. Należy pamiętać, że pulpitów hosta *nie można* konfigurować w sekcji *Pulpity*, która jest zarezerwowana dla pulpitów globalnych.

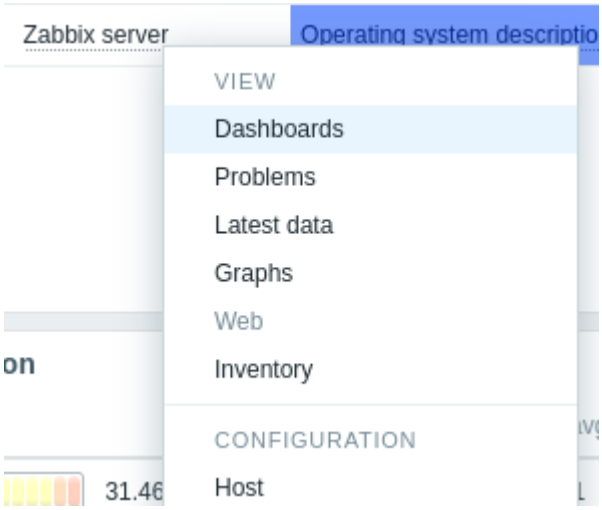
Widżety pulpitów hosta również można konfigurować wyłącznie na poziomie szablonu, z wyjątkiem zmiany interwału odświeżania. Ponadto widżety pulpitów hosta można kopiować wyłącznie do innych pulpitów hosta w obrębie tego samego szablonu. Należy pamiętać, że widżetów z pulpitów globalnych *nie można* kopiować do pulpitów hosta.

Note:
Pulpity hosta przed Zabbix 5.2 były ekranami hosta. Podczas importowania starszego szablonu zawierającego ekrany import ekranów zostanie zignorowany.

Dostęp

Do dashboardów hosta można uzyskać dostęp:

- po wyszukaniu nazwy hosta w wyszukiwaniu globalnym (kliknij link *Dashboards* widoczny w wynikach wyszukiwania);
- po kliknięciu nazwy hosta w *Inwentaryzacja* → *Hosty* (kliknij link *Dashboards* dostępny w podglądzie hosta);
- z menu hosta, klikając *Dashboards*.



Należy pamiętać, że dashboardy hosta *nie mogą* być dostępne bezpośrednio w sekcji *Dashboards*, która jest przeznaczona dla dashboardów globalnych.

3 Scenariusze WWW

Przegląd

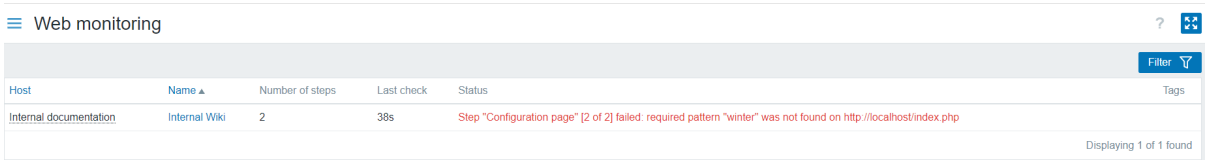
Informacje o scenariuszu WWW hosta są dostępne z poziomu *Monitoring* → *Hosts* po kliknięciu Web dla odpowiedniego hosta.



Kliknięcie nazwy hosta otwiera menu hosta. Dane wyłączonych hostów są również dostępne. Nazwa wyłączonego hosta jest wyświetlana na czerwono.

Status scenariusza WWW może być następujący:

- OK (zielony) — wszystkie kroki zakończyły się powodzeniem i Zabbix zebrał dane dla scenariusza.
- Błąd (czerwony) — co najmniej jeden krok zakończył się niepowodzeniem (zobacz komunikat o błędzie, aby uzyskać wskazówki, które parametry mogą wymagać poprawy).
- Nieznany (szary) — status żadnego kroku nie jest jeszcze dostępny lub nie zebrano żadnych danych.



Maksymalna liczba scenariuszy wyświetlanych na stronie zależy od ustawienia profilu użytkownika *Rows per page* setting.

Domyślnie wyświetlane są tylko wartości z ostatnich 24 godzin. To ograniczenie zostało wprowadzone w celu poprawy początkowego czasu ładowania dużych stron z najnowszymi danymi. Możesz wydłużyć ten okres, zmieniając wartość parametru *Max history display period* w sekcji menu *Administration → General → GUI*.

Nazwa scenariusza jest odnośnikiem do bardziej szczegółowych statystyk:



Używanie filtra

Strona wyświetla listę wszystkich scenariuszy WWW wybranego hosta. Aby wyświetlić scenariusze WWW dla innego hosta lub grupy hostów bez powrotu do strony *Monitoring → Hosts*, wybierz tego hosta lub grupę w filtrze. Możesz również filtrować scenariusze na podstawie tagów.

Przyciski

Przyciski trybu widoku, wspólne dla wszystkich sekcji, zostały opisane na stronie Monitoring.

3 Najnowsze dane

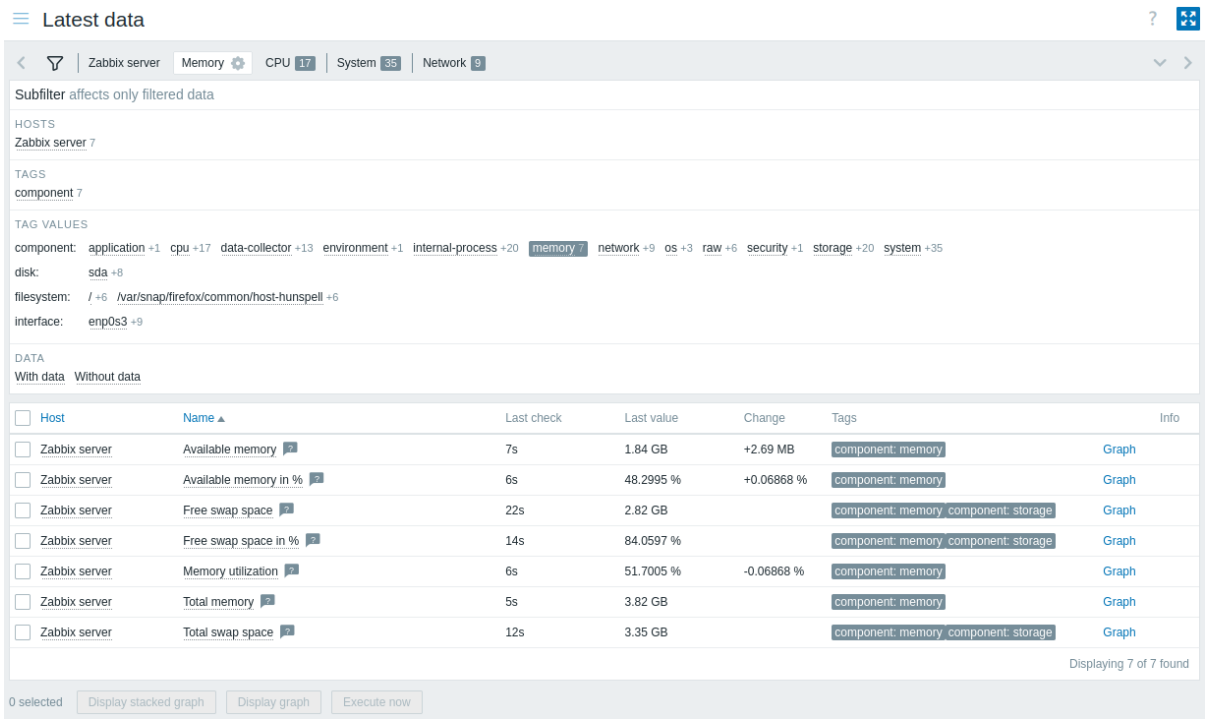
Przegląd

Sekcja *Monitoring* → *Najnowsze dane* wyświetla najnowsze wartości zebrane przez pozycje.

Ta sekcja zawiera następujące elementy:

- Filtr
- Podfiltr
- Lista pozycji

Note:
Podfiltr i lista pozycji są wyświetlane tylko wtedy, gdy filtr jest ustawiony i są wyniki do wyświetlenia.



Kolumna	Opis
Host	Nazwa hosta, do którego należy pozycja. Kliknięcie nazwy otwiera menu kontekstowe hosta. Jeśli host jest w okresie konserwacji, po nazwie hosta wyświetlana jest pomarańczowa ikona klucza . Jeśli host jest wyłączony, jego nazwa jest wyświetlana na czerwono. Należy pamiętać, że dane wyłączonych hostów (w tym wykresy i listy wartości pozycji) są dostępne w sekcji *Najnowsze dane*.
Name	Nazwa pozycji. Kliknięcie nazwy otwiera menu pozycji. Obok nazwy pozycji dla wszystkich pozycji, które mają opis, wyświetlana jest ikona znaku zapytania . Najedź kursorem na ikonę, aby wyświetlić podpowiedź z opisem pozycji.
Last check	Czas od ostatniego sprawdzenia pozycji.
Last value	Najnowsza wartość pozycji. Wartości są wyświetlane z zastosowaniem konwersji jednostek i mapowania wartości. Najedź kursorem na wartość, aby wyświetlić surowe dane (obcięte do 8192 znaków). Wartości binarne są wyświetlane jako symbol zastępczy (*binary value*) zamiast rzeczywistej wartości. Domyślnie wyświetlane są tylko wartości odebrane w ciągu ostatnich 24 godzin. To ograniczenie poprawia początkowy czas ładowania dużych stron z najnowszymi danymi; aby je rozszerzyć, zaktualizuj wartość parametru *Max history display period* w *Administration* → *General* → *GUI*.

Kolumna	Opis
Change	Różnica między poprzednią wartością a najnowszą wartością. Dla pozycji z częstotliwością aktualizacji wynoszącą 1 dzień lub więcej wartość zmiany nigdy nie będzie wyświetlana (przy ustawieniu domyślnym). W takim przypadku ostatnia wartość również nie będzie wyświetlana, jeśli została odebrana ponad 24 godziny temu.
Tags	Tagi powiązane z pozycją. Tagi na liście pozycji są klikalne. Kliknięcie tagu włącza go w podfiltrze, przez co lista pozycji wyświetla tylko pozycje zawierające ten tag (oraz wszelkie inne tagi wcześniej wybrane w podfiltrze). Należy pamiętać, że po przefiltrowaniu pozycji w ten sposób tagi na liście pozycji nie są już klikalne. Dalsze modyfikacje oparte na tagach (na przykład usuwanie tagów lub określanie innych filtrów) należy wykonywać w podfiltrze.
Graph/History	Łącze do prostego wykresu/historii wartości pozycji.
Info	Dodatkowe informacje o pozycji. Jeśli pozycja ma błędy (na przykład stała się nieobsługiwana), wyświetlana jest ikona informacji . Najedź kursorem na ikonę, aby zobaczyć szczegóły.

Przyciski

Przyciski trybu widoku, wspólne dla wszystkich sekcji, zostały opisane na stronie Monitoring.

Działania masowe

Przyciski pod listą oferują działania masowe dla jednej lub kilku wybranych pozycji:

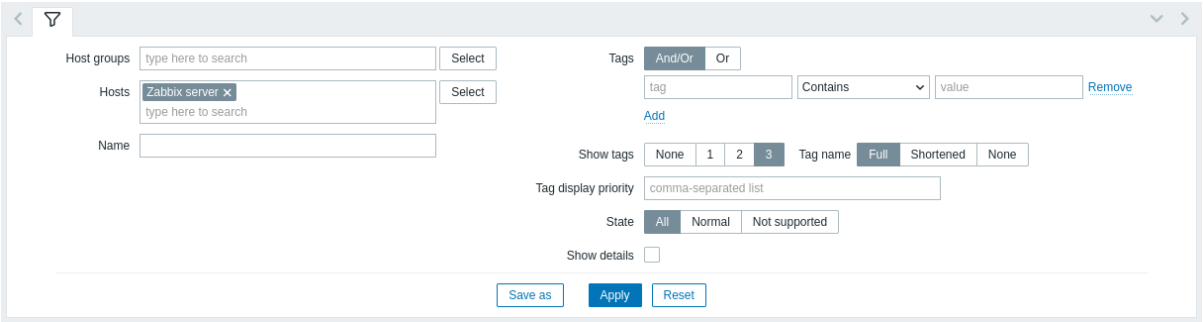
- *Wyświetl skumulowany wykres* - wyświetl skumulowany wykres ad hoc.
- *Wyświetl wykres* - wyświetl prosty wykres ad hoc.
- *Wykonaj teraz* - natychmiast wykonaj sprawdzenie nowych wartości pozycji. Obsługiwane tylko dla sprawdzeń **pasywnych** (zobacz więcej szczegółów). Ta opcja jest dostępna tylko dla hostów z dostępem do odczytu i zapisu. Dostęp do tej opcji dla hostów z uprawnieniami tylko do odczytu zależy od opcji roli użytkownika o nazwie *Wywołaj "Wykonaj teraz" na hostach tylko do odczytu*.

Aby użyć tych opcji, zaznacz pola wyboru przy odpowiednich pozycjach, a następnie kliknij wymagany przycisk.

Używanie filtra

Możesz użyć filtra, aby wyświetlić tylko te pozycje, które Cię interesują. Dla lepszej wydajności wyszukiwania dane są przeszukiwane z nierozwiniętymi makrami.

Ikona filtra znajduje się nad listą pozycji i podfiltrem. Kliknij ją, aby rozwinąć filtr.



Filtr umożliwia zawężenie listy pozycji według grupy hostów, hosta, nazwy pozycji, tagu, stanu i innych ustawień. Określenie nadrzędnej grupy hostów w filtrze powoduje niejawne wybranie wszystkich zagnieżdżonych grup hostów. Szczegółowe informacje o filtrowaniu według tagów można znaleźć w *Monitoring* → *Problems*.

Opcja filtra *Show details* pozwala rozszerzyć informacje wyświetlane dla pozycji. Zaznacz ją, aby wyświetlić takie szczegóły, jak interwał odświeżania pozycji, ustawienia historii i trendów, typ pozycji oraz błędy pozycji (fine/unsupported).

Zapisywanie filtra

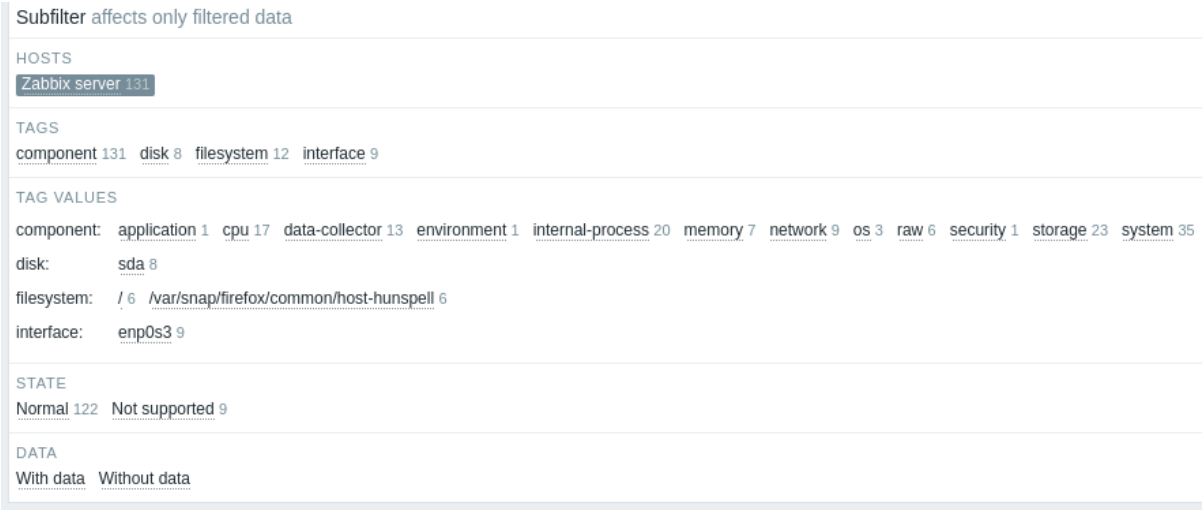
Ulubione ustawienia filtra można zapisać jako karty, a następnie szybko uzyskać do nich dostęp, klikając odpowiednią kartę nad filtrem.

Więcej szczegółów na temat zapisywania filtrów.

Używanie podfiltra

Podfiltr umożliwia dalszą modyfikację filtrowania z filtra głównego.

Zawiera klikalne odnośniki zapewniające szybki dostęp do powiązanych pozycji. Pozycje są powiązane wspólną jednostką — hostem, nazwą lub wartością tagu, stanem pozycji albo statusem danych. Po kliknięciu jednostki zostaje ona wyróżniona szarym tłem, a pozycje są natychmiast filtrowane (bez konieczności kliknięcia *Apply* w filtrze głównym). Kliknięcie innej jednostki dodaje ją do filtrowanych wyników. Ponowne kliknięcie jednostki usuwa filtrowanie.



Podfiltry są generowane na podstawie przefiltrowanych danych, których liczba jest ograniczona do 1000 rekordów. Jeśli jest 20 hostów, z których każdy ma 100 pozycji (czyli łącznie 2000 rekordów), w podfiltrze będzie widoczna tylko połowa hostów. Jeśli chcesz zobaczyć więcej rekordów w podfiltrze, musisz zwiększyć wartość parametru *Limit for search and filter results* (w *Administration -> General -> GUI*).

W przeciwieństwie do filtra głównego, podfiltr jest aktualizowany przy każdym żądaniu odświeżenia tabeli, aby zawsze zawierał aktualne informacje o dostępnych opcjach filtrowania i licznikach.

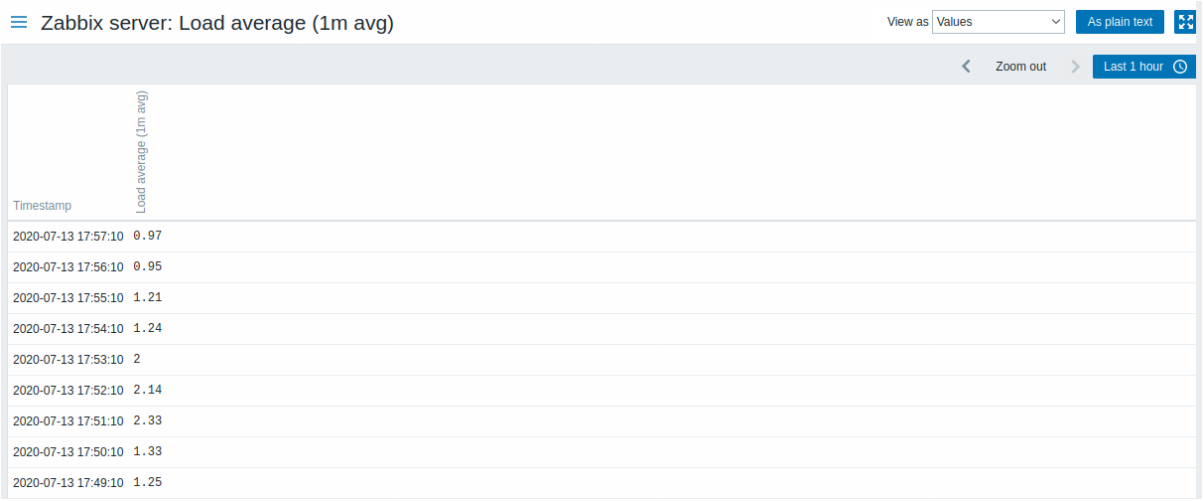
Dla każdej grupy jednostek (hosty, tagi, wartości tagów itd.) wyświetlanych jest maksymalnie 10 wierszy jednostek. Jeśli jednostek jest więcej, tę listę można rozwinąć, aby wyświetlić maksymalnie 1000 wpisów (wartość SUBFILTER_VALUES_PER_GROUP w frontend definitions), klikając ikonę trzech kropek ••• na końcu listy. W przypadku *Tag values* listę można rozwinąć, aby wyświetlić maksymalnie 200 nazw tagów wraz z odpowiadającymi im wartościami. Pamiętaj, że po pełnym rozwinięciu listy nie można jej zwinąć.

Liczba obok każdej klikalnej jednostki wskazuje liczbę pozycji w niej zgrupowanych (na podstawie wyników filtra głównego). Po kliknięciu jednostki liczby przy innych dostępnych jednostkach są wyświetlane ze znakiem plus, wskazującym, ile pozycji można dodać do bieżącego wyboru. Jednostki bez pozycji nie są wyświetlane, chyba że zostały wcześniej wybrane w podfiltrze.

Wykresy i historia

Kolumna *Graph/History* na liście pozycji oferuje następujące odnośniki:

- **History** — dla wszystkich tekstowych pozycji, prowadzi do list (*Values/500 latest values*) wyświetlających historię poprzednich wartości pozycji.
- **Graph** — dla wszystkich numerycznych pozycji, prowadzi do prostego wykresu. Zwróć uwagę, że po wyświetleniu wykresu lista rozwijana w prawym górnym rogu umożliwia również przełączenie do *Values/500 latest values*.



Wartości wyświetlane na tej liście są surowe, tzn. nie jest stosowane żadne przetwarzanie końcowe.

Note:
Łączna liczba wyświetlanych wartości jest określana przez parametr *Limit for search and filter results*, ustawiany w *Administration → General → GUI*.

4 Mapy

Przegląd

W sekcji *Monitoring → Mapy* można konfigurować, zarządzać i wyświetlać mapy sieci.

Po otwarciu tej sekcji zobaczysz albo ostatnią mapę, do której uzyskano dostęp, albo listę wszystkich map, do których masz dostęp.

Wszystkie mapy mogą być publiczne lub prywatne. Mapy publiczne są dostępne dla wszystkich użytkowników, natomiast mapy prywatne są dostępne tylko dla ich właściciela oraz użytkowników, którym mapa została udostępniona.

Lista map



Wyświetlane dane:

Kolumna	Opis
Nazwa	Nazwa mapy. Kliknij nazwę, aby wyświetlić mapę.
Szerokość	Wyświetlana jest szerokość mapy.
Wysokość	Wyświetlana jest wysokość mapy.
Działania	Dostępne są dwa działania: **Właściwości** - ustaw ogólne właściwości mapy **Edytuj** - przejdź do siatki, aby dodawać elementy mapy

Aby skonfigurować nową mapę, kliknij przycisk *Utwórz mapę* w prawym górnym rogu. Aby zaimportować mapę z pliku YAML, XML lub JSON, kliknij przycisk *Importuj* w prawym górnym rogu. Użytkownik, który importuje mapę, zostanie ustawiony jako jej właściciel.

Dwa przyciski pod listą oferują opcje edycji zbiorczej:

- *Eksportuj* - eksportuj mapy do pliku YAML, XML lub JSON
- *Usuń* - usuń mapy

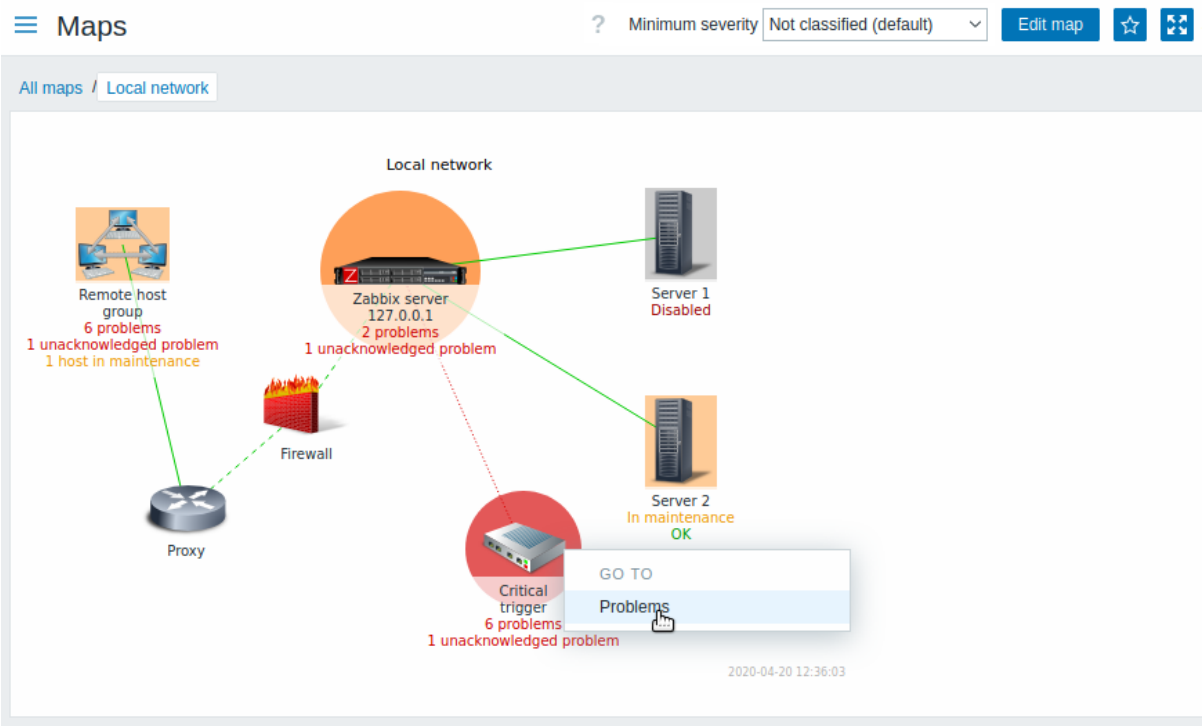
Aby użyć tych opcji, zaznacz pola wyboru przy odpowiednich mapach, a następnie kliknij wymagany przycisk.

Używanie filtra

Możesz użyć filtra, aby wyświetlić tylko mapy, którymi jesteś zainteresowany. Dla lepszej wydajności wyszukiwania dane są przeszukiwane z nierozwiązanymi makrami.

Wyświetlanie map

Aby wyświetlić mapę, kliknij jej nazwę na liście wszystkich map.



Możesz użyć listy rozwijanej na pasku tytułu mapy, aby wybrać najniższy poziom ważności problemów wyzwalaczy, które mają być wyświetlane. Poziom ważności oznaczony jako *domyślny* to poziom ustawiony w konfiguracji mapy. Jeśli mapa zawiera podmapę, przejście do podmapy zachowa poziom ważności mapy wyższego poziomu (z wyjątkiem sytuacji, gdy jest to *Niesklasyfikowane*; w takim przypadku nie zostanie on przekazany do podmapy).

Podświetlanie ikon

Jeśli element mapy jest w stanie problemu, jest podświetlany okrągłym kółkiem. Kolor wypełnienia kółka odpowiada kolorowi ważności problemu. Przy elemencie będą wyświetlane tylko problemy o wybranym poziomie ważności lub wyższym. Jeśli wszystkie problemy są potwierdzone, wokół kółka wyświetlana jest gruba zielona obwódka.

Dodatkowo:

- host w maintenance jest podświetlany pomarańczowym, wypełnionym kwadratem. Należy pamiętać, że podświetlanie maintenance ma priorytet nad podświetlaniem ważności problemu, jeśli elementem mapy jest host.
- wyłączony (niemonitorowany) host jest podświetlany szarym, wypełnionym kwadratem.

Podświetlanie jest wyświetlane, jeśli pole wyboru *Icon highlighting* jest zaznaczone w konfiguracji mapy.

Wskaźniki ostatnich zmian

Czerwone trójkąty skierowane do wewnątrz wokół elementu wskazują na niedawną zmianę stanu wyzwalacza — taką, która nastąpiła w ciągu ostatnich 30 minut. Trójkąty te są wyświetlane, jeśli pole wyboru *Oznacz elementy przy zmianie stanu wyzwalacza* jest zaznaczone w konfiguracji mapy.

Linki

Kliknięcie elementu mapy otwiera menu z dostępnymi linkami. Kliknięcie nazwy hosta powoduje wyświetlenie menu hosta.

Przyciski

Przyciski po prawej stronie oferują następujące opcje:

Edit map	Przejdź do edycji zawartości mapy.
	Dodaj mapę do widżetu ulubionych w Dashboardach.
	Mapa znajduje się w widżecie ulubionych w Dashboardach. Kliknij, aby usunąć mapę z widżetu ulubionych.

Przyciski trybu widoku, wspólne dla wszystkich sekcji, zostały opisane na stronie Monitoring.

Czytelne podsumowanie na mapach

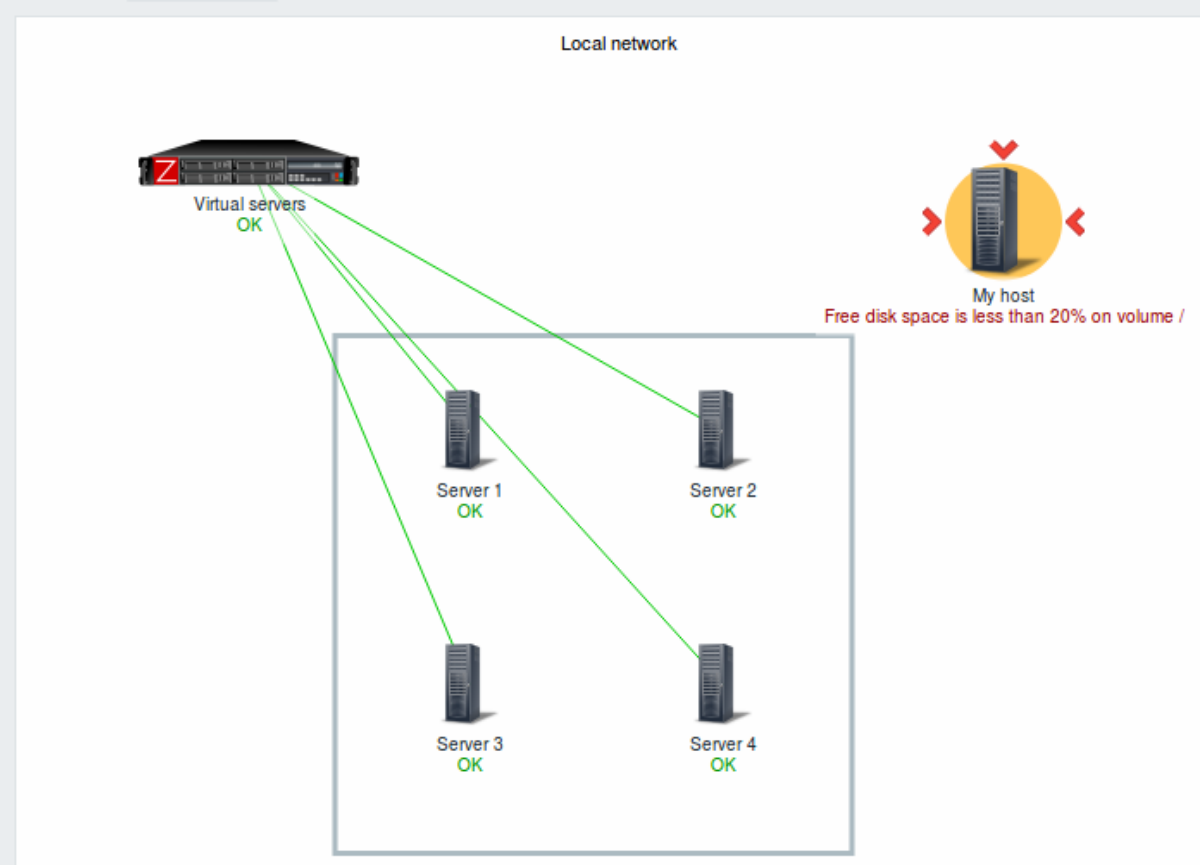
Dostępna jest ukryta właściwość „aria-label”, która umożliwia odczytywanie informacji o mapie za pomocą czytnika ekranu. Dostępny jest zarówno ogólny opis mapy, jak i opis poszczególnych elementów, w następującym formacie:

- dla opisu mapy: `<Nazwa mapy>, <* z * elementów w stanie problemu>, <* problemów łącznie>.`
- dla opisu jednego elementu z jednym problemem: `<Typ elementu>, Status <Status elementu>, <Nazwa elementu>, <Opis problemu>.`
- dla opisu jednego elementu z wieloma problemami: `<Typ elementu>, Status <Status elementu>, <Nazwa elementu>, <* problemów>.`
- dla opisu jednego elementu bez problemów: `<Typ elementu>, Status <Status elementu>, <Nazwa elementu>.`

Na przykład dostępny jest następujący opis:

```
'Sieć lokalna, 1 z 6 elementów w stanie problemu, 1 problem łącznie. Host, Status problem, Mój host, Wolne
```

dla następującej mapy:



Odwoływanie się do mapy sieciowej

Do map sieciowych można odwoływać się za pomocą parametrów GET `sysmapid` i `mapname`. Na przykład,

```
http://zabbix/zabbix/zabbix.php?action=map.view&mapname=Local%20network
```

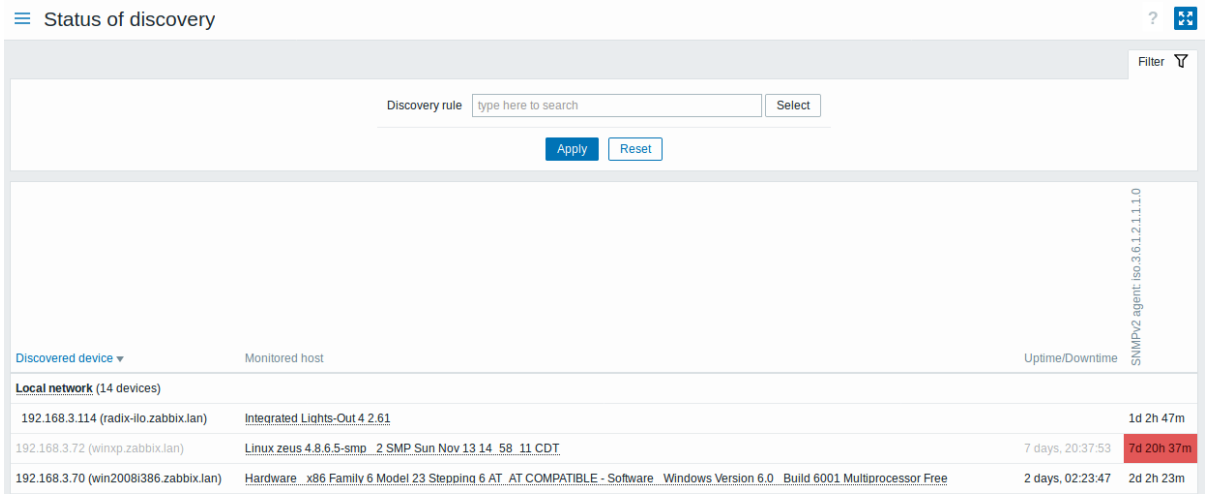
otworzy mapę o tej nazwie (Local network).

Jeśli określono zarówno `sysmapid` (ID mapy), jak i `mapname` (nazwę mapy), `mapname` ma wyższy priorytet.

5 Wykrywanie

Przegląd

W sekcji *Monitoring* → *Discovery* wyświetlane są wyniki odkrywania sieci. Odkryte urządzenia są sortowane według reguły odkrywania.



Wyświetlane dane:

Kolumna	Opis
Odkryte urządzenie	Odkryte urządzenia są wyświetlane na liście, pogrupowane według reguły odkrywania. Kliknięcie reguły odkrywania otwiera menu reguły zawierające odnośnik do formularza konfiguracji reguły odkrywania.
Monitorowany host	Jeśli urządzenie jest już monitorowane, w tej kolumnie zostanie wyświetlona nazwa hosta. Kliknięcie nazwy hosta otwiera menu hosta.
Czas działania/Czas niedostępności	W tej kolumnie wyświetlany jest czas, przez jaki urządzenie pozostaje wykryte, lub czas od jego utraty po wcześniejszym odkryciu.
Sprawdzenie odkrywania	Wyświetlany jest stan poszczególnej usługi (sprawdzenia odkrywania) dla każdego odkrytego urządzenia. Czerwona komórka oznacza, że usługa jest niedostępna. Czas działania lub czas niedostępności usługi jest podany w komórce. Ta kolumna jest wyświetlana tylko wtedy, gdy usługa została znaleziona na co najmniej jednym odkrytym urządzeniu.

Przyciski

Przyciski trybu widoku, wspólne dla wszystkich sekcji, zostały opisane na stronie Monitoring.

Używanie filtra

Możesz użyć filtra, aby wyświetlić tylko te reguły wykrywania, które Cię interesują. Aby zapewnić lepszą wydajność wyszukiwania, dane są przeszukiwane z nierozwiniętymi makrami.

Jeśli w filtrze nic nie wybrano, wyświetlane są wszystkie włączone reguły wykrywania. Aby wybrać do wyświetlenia konkretną regułę wykrywania, zacznij wpisywać jej nazwę w filtrze. Wszystkie pasujące włączone reguły wykrywania zostaną wyświetlone na liście do wyboru. Można wybrać więcej niż jedną regułę wykrywania.

3 Usługi

Przegląd

Menu Usługi służy do funkcji monitorowania usług w Zabbix.

1 Usługi

Przegląd

W tej sekcji można zobaczyć ogólny stan wszystkich usług, które zostały skonfigurowane w Zabbix, na podstawie infrastruktury.

Usługa może stanowić hierarchię składającą się z kilku poziomów innych usług, nazywanych usługami „podrzędnymi”, które wpływają na ogólny stan usługi (zobacz także przegląd funkcji monitorowania usług.)

Główne kategorie stanu usługi to *OK* lub *Problem*, przy czym stan *Problem* jest wyrażany odpowiednią nazwą i kolorem ważności problemu.

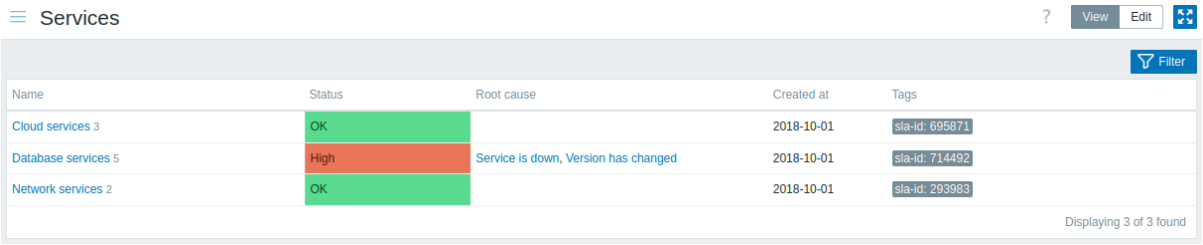
Tryb widoku umożliwia monitorowanie usług wraz z ich stanem i innymi szczegółami, ale w tej sekcji można również skonfigurować hierarchię usług (dodawać/edytować usługi i usługi podrzędne), przełączając się do trybu edycji.

Aby przełączyć się z trybu widoku do trybu edycji (i z powrotem), kliknij odpowiedni przycisk w prawym górnym rogu:

- View - wyświetl usługi
- Edit - dodawaj/edytuj usługi i usługi podrzędne

Pamiętaj, że dostęp do edycji zależy od ustawień roli użytkownika.

Wyświetlanie usług



Wyświetlana jest lista istniejących usług.

Wyświetlane dane:

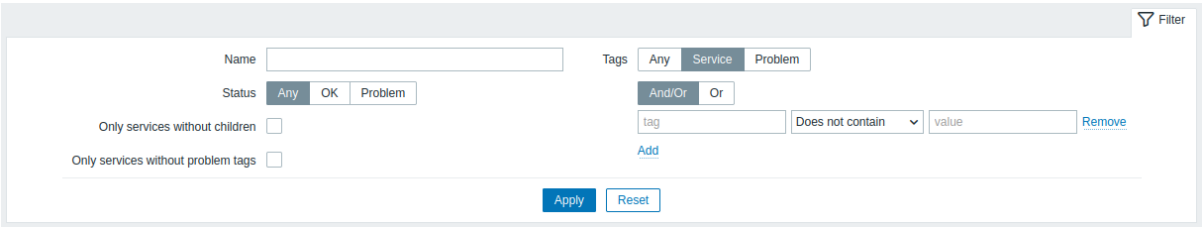
Parametr	Opis
Nazwa	Nazwa usługi. Nazwa usługi jest linkiem do szczegółów usługi. Liczba po nazwie wskazuje, ile usług podrzędnych ma dana usługa.
Status	Stan usługi: **OK** - brak problemów **<kolor problemu i ważność>** - wskazuje problem i jego ważność. W przypadku wielu problemów wyświetlane są kolor i ważność problemu o najwyższym poziomie krytyczności.
Przyczyna źródłowa	Wyświetlana jest lista problemów źródłowych, które bezpośrednio lub pośrednio wpływają na stan usługi. Te same problemy są wymienione jako zwracane przez makro {SERVICE.ROOTCAUSE}. Kliknij nazwę problemu, aby zobaczyć więcej szczegółów w *Monitoring* → *Problemy*. Problemy, które nie wpływają na stan usługi, nie są uwzględniane na liście.
Utworzono	Wyświetlany jest czas utworzenia usługi.
Tagi	Wyświetlane są tagi usługi. Tagi służą do identyfikacji usługi w akcjach usług i SLA.

Przyciski

Przyciski trybu widoku, wspólne dla wszystkich sekcji, zostały opisane na stronie Monitoring.

Używanie filtra

Możesz użyć filtra, aby wyświetlić tylko te usługi, które Cię interesują.



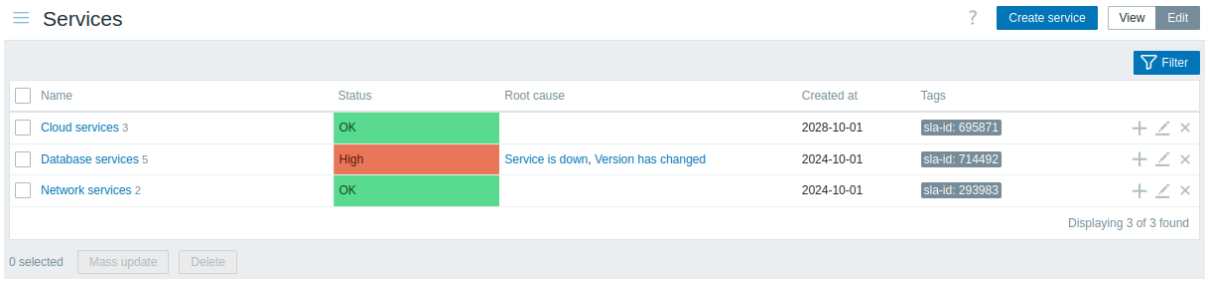
Parametr	Opis
Nazwa	Filtruj według nazwy usługi.
Status	Filtruj według stanu usługi.
Tylko usługi bez usług podrzędnych	Zaznacz pole wyboru, aby wyświetlić tylko usługi bez usług podrzędnych. Ten parametr jest dostępny tylko w trybie edycji usługi.
Tylko usługi bez tagów problemów	Zaznacz pole wyboru, aby wyświetlić tylko usługi bez tagów problemów. Ten parametr jest dostępny tylko w trybie edycji usługi.

Parametr	Opis
Tagi	Filtruj według nazwy i wartości tagu usługi albo nazwy i wartości tagu problemu usługi (w trybie edycji usługi). Możliwe jest zarówno uwzględnianie, jak i wykluczanie określonych tagów i wartości tagów. Można ustawić kilka warunków. Dopasowanie nazw tagów zawsze uwzględnia wielkość liter. Dla każdego warunku dostępnych jest kilka operatorów: **Istnieje** - uwzględnij określone nazwy tagów; **Równa się** - uwzględnij określone nazwy i wartości tagów (z uwzględnieniem wielkości liter); **Zawiera** - uwzględnij określone nazwy tagów, których wartości zawierają wprowadzony ciąg znaków (dopasowanie podciągu, bez uwzględniania wielkości liter); **Nie istnieje** - wyklucz określone nazwy tagów; **Nie równa się** - wyklucz określone nazwy i wartości tagów (z uwzględnieniem wielkości liter); **Nie zawiera** - wyklucz określone nazwy tagów, których wartości zawierają wprowadzony ciąg znaków (dopasowanie podciągu, bez uwzględniania wielkości liter). Dostępne są dwa typy obliczania warunków: **And/Or** - wszystkie warunki muszą być spełnione, warunki mające tę samą nazwę tagu będą grupowane operatorem Or; **Or** - wystarczy, że jeden warunek zostanie spełniony.

Edycja usług

Kliknij przycisk *Edytuj*, aby przejść do trybu edycji. W trybie edycji lista jest uzupełniona o pola wyboru przed wpisami, a także o następujące dodatkowe opcje:

-  - dodaj usługę podrzędną do tej usługi
-  - edytuj tę usługę
-  - usuń tę usługę

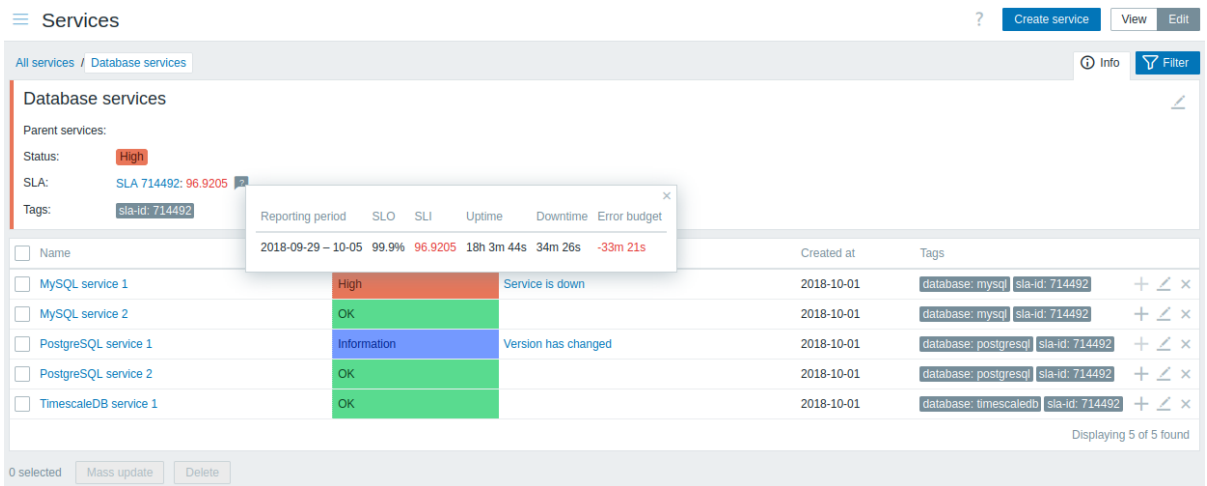


Aby skonfigurować nową usługę, kliknij przycisk *Utwórz usługę* w prawym górnym rogu.

Szczegóły usługi

Aby uzyskać dostęp do szczegółów usługi, kliknij nazwę usługi. Aby wrócić do listy wszystkich usług, kliknij *Wszystkie usługi*.

Szczegóły usługi obejmują pole informacyjne oraz listę usług podrzędnych.



Aby uzyskać dostęp do pola informacyjnego, kliknij kartę *Info*. Pole informacyjne zawiera następujące wpisy:

- Nazwy usług nadrzędnych (jeśli istnieją)
- Bieżący status tej usługi
- Bieżące SLA tej usługi w formacie `nazwa SLA:wskaźnik poziomu usługi`. „Nazwa SLA" jest również łączem do raportu SLA dla tej usługi. Jeśli umieścisz kursor myszy nad polem informacyjnym obok wskaźnika poziomu usługi (SLI), zostanie wyświetlona wyskakująca lista informacyjna ze szczegółami SLI. Wskaźnik poziomu usługi wyświetla bieżący poziom usługi w procentach.
- Tagi usługi

Pole informacyjne zawiera również łącze do konfiguracji usługi.

Aby użyć filtra dla usług podrzędnych, kliknij kartę *Filtr*.

W trybie edycji lista usług podrzędnych jest uzupełniona o dodatkowe opcje edycji:

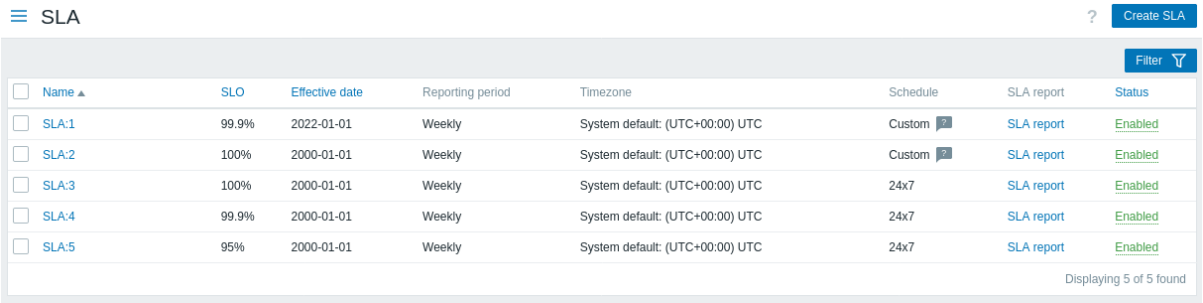
-  - dodaj usługę podrzędną do tej usługi
-  - edytuj tę usługę
-  - usuń tę usługę

2 SLA

Przegląd

Ta sekcja umożliwia przeglądanie i konfigurowanie SLA.

SLA



Wyświetlana jest lista skonfigurowanych SLA. *Uwaga*: wyświetlane będą tylko SLA powiązane z usługami dostępnymi dla użytkownika (tylko do odczytu, chyba że dla roli użytkownika włączono opcję *Manage SLA*).

Wyświetlane dane:

Parametr	Opis
Name	Wyświetlana jest nazwa SLA. Nazwa jest linkiem do konfiguracji SLA.
SLO	Wyświetlany jest cel poziomu usługi (SLO).
Effective date	Wyświetlana jest data rozpoczęcia obliczania SLA.
Reporting period	Wyświetlany jest okres używany w raporcie SLA — *dzienny*, *tygodniowy*, *miesięczny*, *kwartalny* lub *roczny*.
Time zone	Wyświetlana jest strefa czasowa SLA.
Schedule	Wyświetlany jest harmonogram SLA — 24x7 lub niestandardowy.
SLA report	Kliknij link, aby zobaczyć raport SLA dla tego SLA.
Status	Wyświetlany jest status SLA — włączone lub wyłączone.

3 Raport SLA

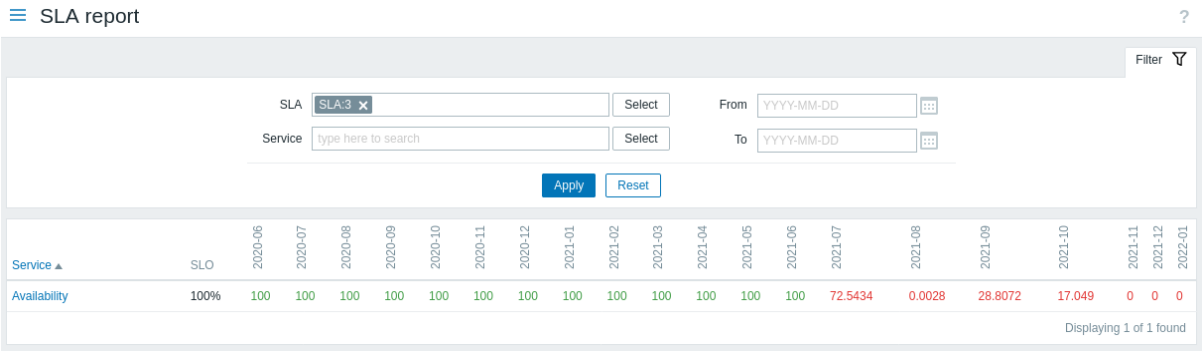
Przegląd

Ta sekcja umożliwia przeglądanie raportów SLA na podstawie kryteriów wybranych w filtrze.

Raporty SLA mogą być również wyświetlane jako widget pulpitu.

Raport

Filtr umożliwia wybór raportu na podstawie nazwy SLA, a także nazwy usługi. Możliwe jest również ograniczenie wyświetlanego okresu.

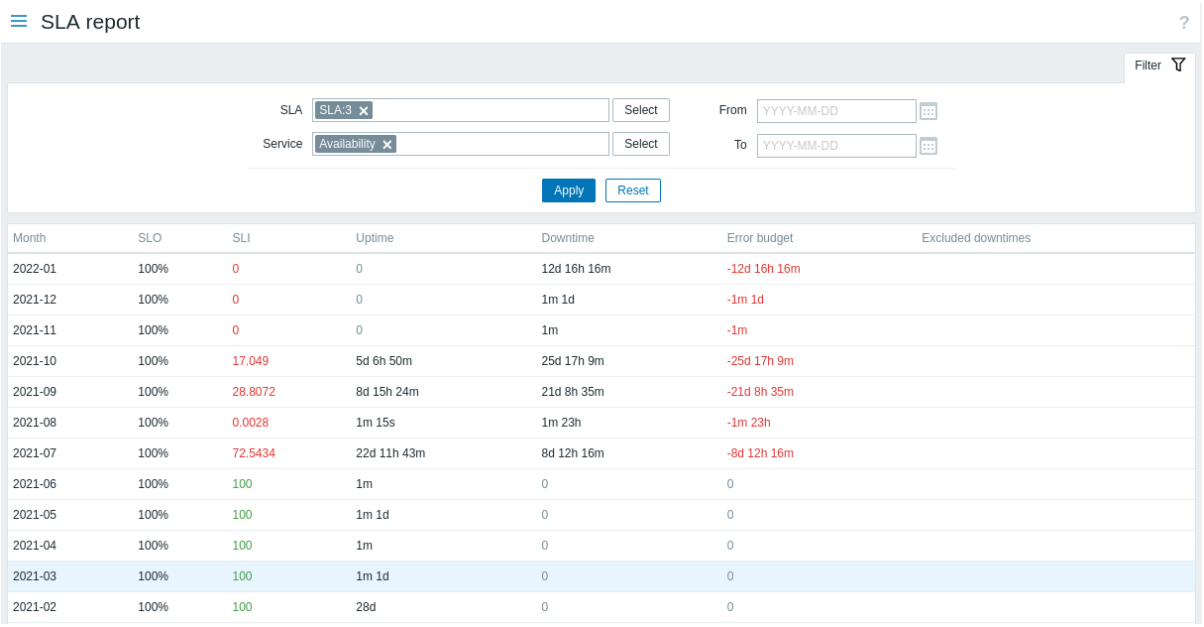


Każda kolumna (okres) wyświetla SLI dla tego okresu. Wartości SLI, które naruszają ustawiony SLO, są wyróżnione na czerwono.

W raporcie wyświetlanych jest 20 okresów. Maksymalnie można wyświetlić 100 okresów, jeśli określono zarówno datę *Od*, jak i datę *Do*.

Szczegóły raportu

Jeśli klikniesz nazwę usługi w raporcie, możesz przejść do innego raportu, który wyświetla bardziej szczegółowy widok.



Pamiętaj, że ujemny czas trwania problemu nie wpływa na obliczanie ani raportowanie SLA.

4 Inwentaryzacja

Przegląd

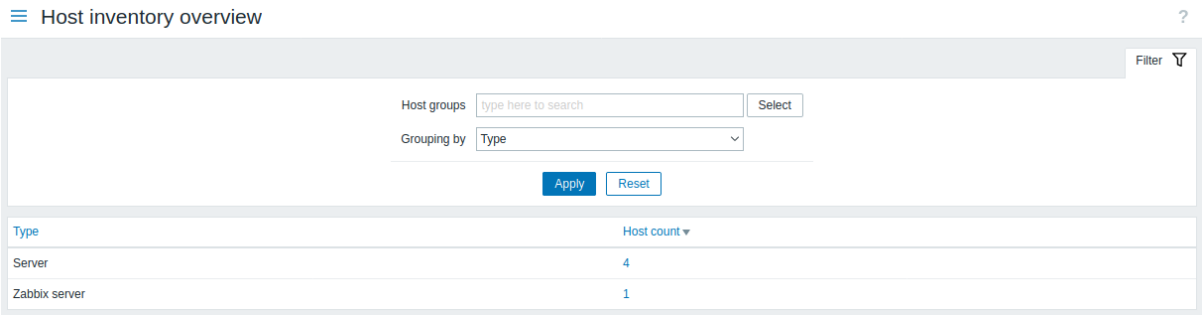
Menu Inwentaryzacja zawiera sekcje zapewniające przegląd danych inwentaryzacyjnych hostów według wybranego parametru, a także możliwość wyświetlania szczegółów inwentaryzacyjnych hosta.

1 Przegląd

Przegląd

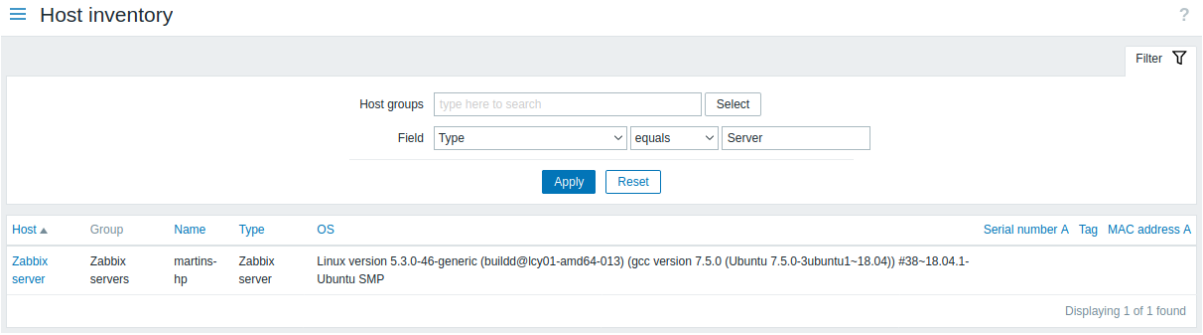
Sekcja *Inwentaryzacja* → *Przegląd* udostępnia sposoby uzyskania przeglądu danych inwentaryzacji hostów.

Aby wyświetlić przegląd, wybierz grupy hostów (lub żadną) oraz pole inwentaryzacji, według którego mają być wyświetlane dane. Zostanie wyświetlona liczba hostów odpowiadających każdej wartości wybranego pola.



Kompletność przeglądu zależy od tego, jak dużo informacji inwentaryzacyjnych jest utrzymywanych dla hostów.

Liczby w kolumnie *Liczba hostów* są odnośnikami; prowadzą do przefiltrowania tych hostów w tabeli *Inwentaryzacja hostów*.

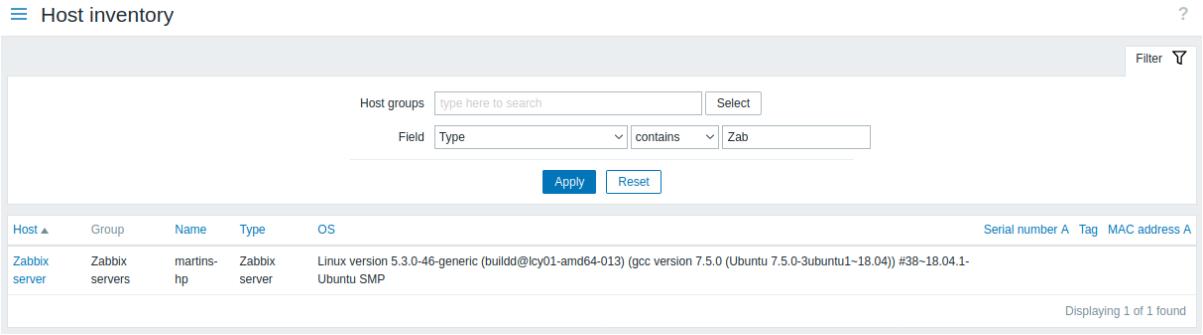


2 Hosty

Przegląd

W sekcji *Inwentaryzacja* → *Hosty* wyświetlane są dane inwentaryzacyjne hostów.

Możesz filtrować hosty według grup(y) hostów oraz według dowolnego pola inwentaryzacji, aby wyświetlić tylko te hosty, które Cię interesują.

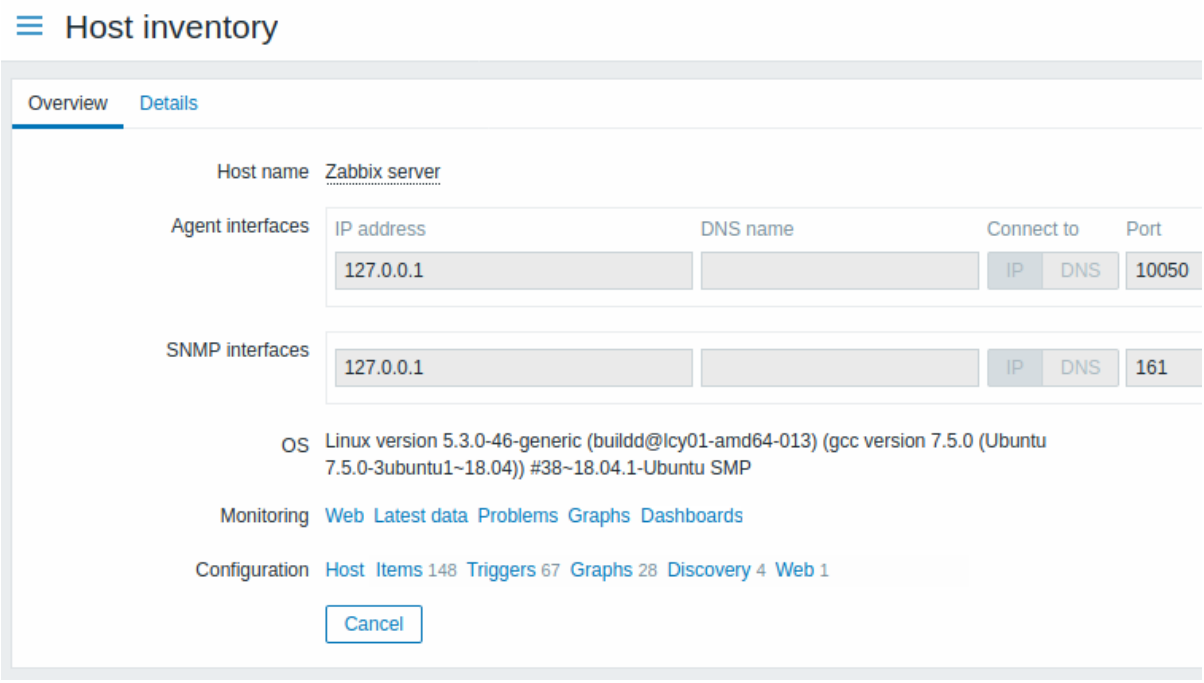


Aby wyświetlić pełną inwentaryzację wszystkich hostów, naciśnij przycisk „Reset".

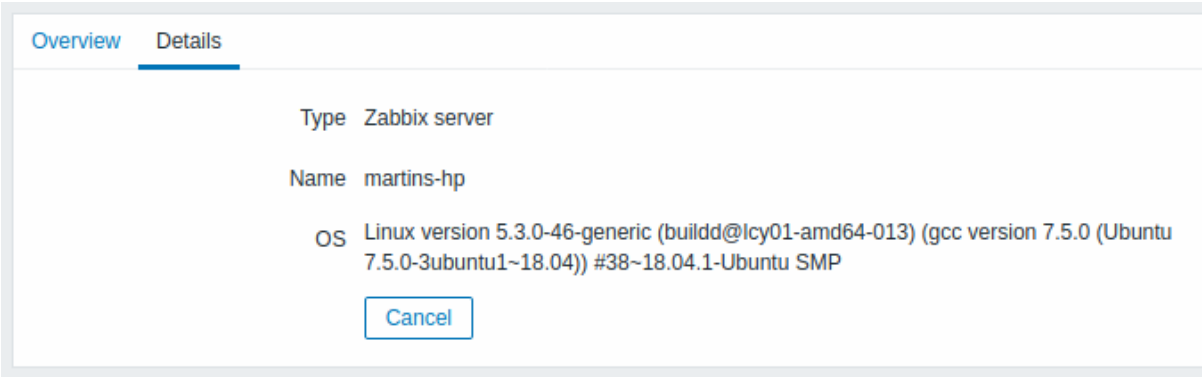
Chociaż w tabeli wyświetlane są tylko niektóre kluczowe pola inwentaryzacji, możesz również zobaczyć wszystkie dostępne informacje inwentaryzacyjne dla danego hosta. Aby to zrobić, kliknij nazwę hosta w pierwszej kolumnie.

Szczegóły inwentarza

Zakładka **Przegląd** zawiera ogólne informacje o hoście, najnowsze dane monitoringu oraz opcje konfiguracji hosta:



Zakładka **Szczegóły** zawiera wszystkie dostępne szczegóły inwentarza dla hosta:



Kompletność danych inwentarza zależy od tego, ile informacji inwentarzowych jest utrzymywanych dla hosta. Jeśli żadne informacje nie są utrzymywane, zakładka *Szczegóły* jest wyłączona.

5 Raporty

Przegląd

Menu Raporty zawiera kilka sekcji z różnorodnymi, predefiniowanymi i dostosowywanymi przez użytkownika raportami, które koncentrują się na wyświetlaniu przeglądu takich parametrów jak informacje o systemie, wyzwalacze i zebrane dane.

1 Informacje o systemie

Przegląd

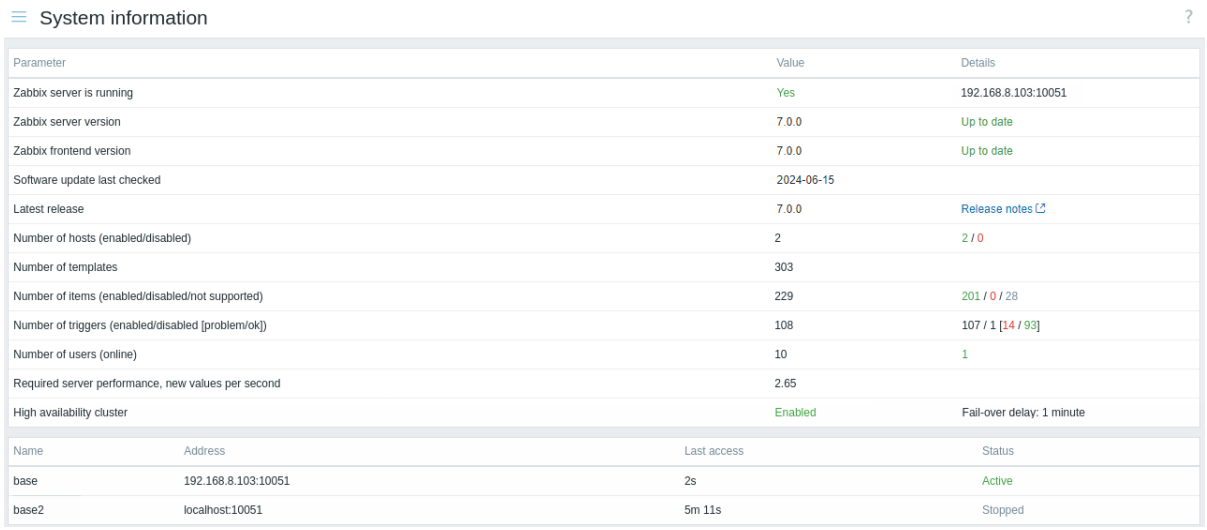
W *Raporty* → *Informacje o systemie* wyświetlane jest podsumowanie kluczowych danych serwera Zabbix i systemu. Dane systemowe są zbierane przy użyciu pozycji wewnętrznych.

Należy pamiętać, że w konfiguracji wysokiej dostępności możliwe jest przekierowanie źródła informacji o systemie (instancji serwera). Aby to zrobić, edytuj plik *zabbix.conf.php* — odkomentuj i ustaw `$ZBX_SERVER` lub jednocześnie `$ZBX_SERVER` i `$ZBX_SERVER_PORT` na serwer inny niż ten aktualnie pokazany jako aktywny. Pamiętaj, że przy ustawieniu tylko `$ZBX_SERVER` zostanie użyta domyślna wartość (10051) dla `$ZBX_SERVER_PORT`.

Po włączeniu konfiguracji wysokiej dostępności poniżej statystyk systemowych wyświetlany jest osobny blok ze szczegółami węzłów wysokiej dostępności. Ten blok jest widoczny tylko dla użytkowników Zabbix *Super Admin*.

Informacje o systemie są również dostępne jako widget pulpitu.

Statystyki systemu



Wyświetlane dane:

Parametr	Wartość	Szczegóły
Serwer Zabbix jest uruchomiony	Status serwera Zabbix: **Tak** - serwer jest uruchomiony **Nie** - serwer nie jest uruchomiony *Uwaga:* Aby wyświetlić pozostałe informacje, frontend wymaga uruchomionego serwera i co najmniej jednego uruchomionego procesu trapper na serwerze (parametr StartTrappers w pliku zabbix_server.conf > 0).	Lokalizacja i port serwera Zabbix.
Wersja serwera Zabbix	Wyświetlany jest numer bieżącej wersji serwera. *Uwaga:* Jest wyświetlany tylko wtedy, gdy serwer Zabbix jest uruchomiony.	Wyświetlany jest status wersji serwera: **Aktualna** - używana jest najnowsza wersja; **Dostępna nowa aktualizacja** - dostępna jest nowsza wersja; **Nieaktualna** - okres pełnego wsparcia dla tej wersji wygasł. Ta informacja jest dostępna tylko wtedy, gdy sprawdzanie aktualizacji oprogramowania jest włączone w konfiguracji serwera Zabbix. Nic nie jest wyświetlane, jeśli ostatnie sprawdzenie aktualizacji oprogramowania zostało wykonane ponad tydzień temu lub brak danych o bieżącej wersji.
Wersja frontendu Zabbix	Wyświetlany jest numer wersji frontendu Zabbix.	Wyświetlany jest status wersji frontendu Zabbix: **Aktualna** - używana jest najnowsza wersja; **Dostępna nowa aktualizacja** - dostępna jest nowsza wersja; **Nieaktualna** - okres pełnego wsparcia dla tej wersji wygasł. Ta informacja jest dostępna tylko wtedy, gdy sprawdzanie aktualizacji oprogramowania jest włączone w konfiguracji serwera Zabbix. Nic nie jest wyświetlane, jeśli ostatnie sprawdzenie aktualizacji oprogramowania zostało wykonane ponad tydzień temu lub brak danych o bieżącej wersji.
Ostatnie sprawdzenie aktualizacji oprogramowania	Wyświetlana jest data ostatniego sprawdzenia aktualizacji oprogramowania Zabbix. Ta informacja jest dostępna tylko wtedy, gdy sprawdzanie aktualizacji oprogramowania jest włączone w konfiguracji serwera Zabbix.	

Parametr	Wartość	Szczegóły
Najnowsze wydanie	Wyświetlany jest numer nowszego wydania (jeśli jest dostępne) dla bieżącej wersji Zabbix. Ta informacja jest dostępna tylko wtedy, gdy sprawdzanie aktualizacji oprogramowania jest włączone w konfiguracji serwera Zabbix. Nic nie jest wyświetlane, jeśli ostatnie sprawdzenie aktualizacji oprogramowania zostało wykonane ponad tydzień temu lub brak danych o bieżącej wersji.	Wyświetlany jest link do informacji o wydaniu najnowszego dostępnego wydania Zabbix.
Liczba hostów	Wyświetlana jest łączna liczba skonfigurowanych hostów.	Liczba monitorowanych/niemonitorowanych hostów.
Liczba szablonów	Wyświetlana jest łączna liczba szablonów.	
Liczba pozycji	Wyświetlana jest łączna liczba pozycji.	Liczba monitorowanych/wyłączonych/nieobsługiwanych pozycji na poziomie hosta. Pozycje na wyłączonych hostach są liczone jako wyłączone.
Liczba wyzwalaczy	Wyświetlana jest łączna liczba wyzwalaczy.	Liczba włączonych/wyłączonych wyzwalaczy na poziomie hosta; podział włączonych wyzwalaczy według stanów „Problem”/„OK”. Wyzwalacze wymienione w stanie „OK” obejmują wyzwalacze ze statusem „Nieznany”. Wyzwalacze zależne od wyłączonych pozycji lub przypisane do wyłączonych hostów są liczone jako wyłączone.
Liczba użytkowników	Wyświetlana jest łączna liczba skonfigurowanych użytkowników.	Liczba użytkowników online.
Wymagana wydajność serwera, nowe wartości na sekundę	Wyświetlana jest oczekiwana liczba nowych wartości przetwarzanych przez serwer Zabbix na sekundę.	*Wymagana wydajność serwera* jest wartością szacunkową i może być użyteczna jako wskazówka. Aby uzyskać dokładne liczby przetwarzanych wartości, użyj wewnętrznej pozycji `zabbix[wcache,values,all]`. W obliczeniach uwzględniane są włączone pozycje z monitorowanych hostów. Pozycje logów są liczone jako jedna wartość na interwał aktualizacji pozycji. Liczone są wartości z regularnych interwałów; wartości z interwałów elastycznych i harmonogramowanych nie są uwzględniane. Obliczenia nie są korygowane podczas okresu utrzymania „nodata”. Pozycje trapper nie są liczone.
Skrypty globalne na serwerze Zabbix	W tym polu zostanie wyświetlone **Wyłączone**, jeśli skrypty globalne są wyłączone na serwerze Zabbix przez ustawienie EnableGlobalScripts=0 w konfiguracji serwera.	
Klaster wysokiej dostępności	Status klastra wysokiej dostępności dla serwera Zabbix: **Wyłączony** - serwer samodzielny **Włączony** - istnieje co najmniej jeden węzeł wysokiej dostępności	Jeśli jest włączony, wyświetlane jest opóźnienie przełączenia awaryjnego.

Informacje o systemie wyświetlą również komunikat o błędzie w następujących przypadkach:

- Używana baza danych nie ma wymaganego zestawu znaków ani reguł porównywania (UTF-8).
- Wersja bazy danych jest niższa lub wyższa niż obsługiwany zakres (dostępne tylko dla użytkowników z typem roli *Super admin role*).
- Housekeeping dla TimescaleDB jest skonfigurowany nieprawidłowo (tabele historii lub trendów zawierają skompresowane chunki, ale opcje *Override item history period* lub *Override item trend period* są wyłączone).

Węzły wysokiej dostępności

Jeśli klaster wysokiej dostępności jest włączony, wyświetlany jest dodatkowy blok danych ze statusem każdego węzła wysokiej dostępności.



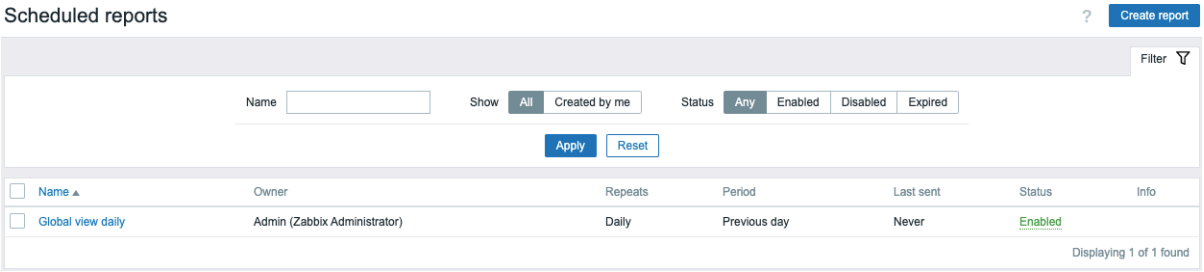
Wyświetlane dane:

Kolumna	Opis
Nazwa	Nazwa węzła, zgodnie z definicją w konfiguracji serwera.
Adres	Adres IP węzła i port.
Ostatni dostęp	Czas ostatniego dostępu do węzła. Po najechaniu kursorem na komórkę wyświetlany jest znacznik czasu ostatniego dostępu w długim formacie.
Status	Status węzła. Wiersze tabeli są sortowane według tych statusów w następującej kolejności priorytetów: **Aktywny** - węzeł działa i pracuje **Niedostępny** - węzeł nie był widziany dłużej niż wynosi opóźnienie przełączenia awaryjnego (warto ustalić przyczynę) **Zatrzymany** - węzeł został zatrzymany lub nie mógł się uruchomić (warto go uruchomić lub usunąć) **W gotowości** - węzeł działa i oczekuje

2 Zaplanowane raporty

Przegląd

W *Raporty* → *Raporty cykliczne* użytkownicy z odpowiednimi uprawnieniami mogą skonfigurować cykliczne generowanie wersji PDF pulpitów, które będą wysyłane pocztą e-mail do określonych odbiorców.



Ekran otwierający wyświetla informacje o raportach cyklicznych, które można filtrować w celu łatwiejszej nawigacji — zobacz sekcję Korzystanie z filtra poniżej.

Wyświetlane dane:

Kolumna	Opis
Nazwa	Nazwa raportu. Kliknięcie otwiera formularz konfiguracji raportu.
Właściciel	Użytkownik, który utworzył raport.
Powtarzanie	Częstotliwość generowania raportu (codziennie/co tydzień/co miesiąc/co rok).
Okres	Przedział czasu, dla którego przygotowywany jest raport (poprzedni dzień, tydzień, miesiąc lub rok).
Ostatnio wysłano	Data i godzina wysłania ostatniego raportu.

Kolumna	Opis
Status	Bieżący status raportu (włączony/wyłączony/wygasły). Użytkownicy z odpowiednimi uprawnieniami mogą zmienić status, klikając go — z „Włączony” na „Wyłączony” (i z powrotem); z „Wygasły” na „Wyłączony” (i z powrotem). Dla użytkowników z niewystarczającymi uprawnieniami status nie jest klikalny.
Informacje	Wyświetla ikony informacyjne: Czerwona ikona wskazuje, że generowanie raportu nie powiodło się; po najechaniu kursorem zostanie wyświetlona podpowiedź z informacją o błędzie. Żółta ikona wskazuje, że raport został wygenerowany, ale wysyłka do części (lub wszystkich) odbiorców nie powiodła się albo że raport wygasł; po najechaniu kursorem zostanie wyświetlona podpowiedź z dodatkowymi informacjami.

Używanie filtra

Możesz użyć filtra, aby zawęzić listę raportów. Dla lepszej wydajności wyszukiwania dane są przeszukiwane przy nierozwiniętych makrach.

Dostępne są następujące opcje filtrowania:

- *Nazwa* - dozwolone jest częściowe dopasowanie nazwy
- *Pokaż* - utworzone przez bieżącego użytkownika lub wszystkie raporty
- *Status* - wybierz spośród „Dowolny” (pokaż wszystkie raporty), „Włączony”, „Wyłączony” lub „Wygasły”

Filtr znajduje się poniżej nazwy sekcji *Raporty cykliczne*. Można go rozwinąć i zwinąć, klikając kartę *Filtr* w prawym górnym rogu.

Aktualizacja masowa

Czasami możesz chcieć usunąć lub zmienić status wielu raportów jednocześnie. Zamiast otwierać każdy raport osobno do edycji, możesz w tym celu użyć funkcji aktualizacji masowej.

Aby masowo zaktualizować raporty, wykonaj następujące czynności:

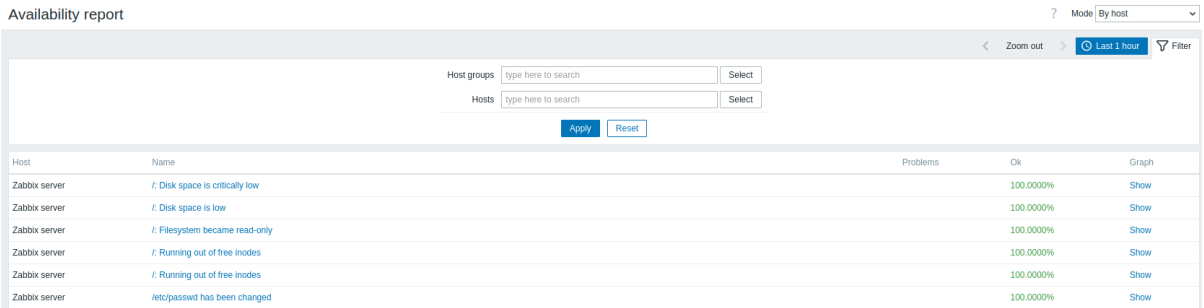
- Zaznacz pola wyboru raportów, które chcesz zaktualizować, na liście
- Kliknij odpowiedni przycisk pod listą, aby wprowadzić zmiany (*Włącz*, *Wyłącz* lub *Usuń*)

3 Raport dostępności

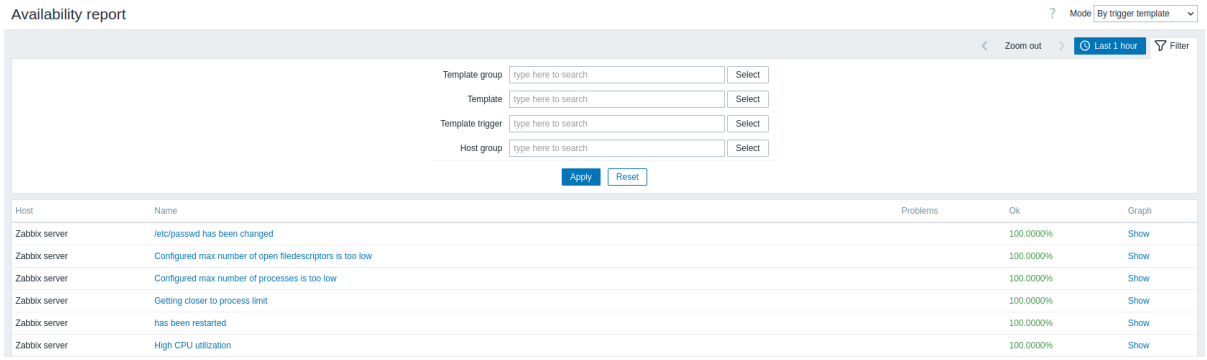
Przegląd

W *Raporty* > *Raport dostępności* możesz zobaczyć, przez jaki procent czasu każdy wyzwalacz znajdował się w stanie problem/OK.

Dla każdego stanu wyświetlany jest procent czasu, co ułatwia określenie dostępności różnych elementów w systemie.



Z listy rozwijanej w prawym górnym rogu możesz wybrać tryb wyboru — czy wyświetlać wyzwalacze według hostów, czy według wyzwalaczy należących do szablonu.



Nazwa wyzwalacza jest łączem do najnowszych zdarzeń tego wyzwalacza.

Używanie filtra

Filtr może pomóc zawęzić liczbę wyświetlanych hostów i/lub wyzwalaczy. Aby uzyskać lepszą wydajność wyszukiwania, dane są przeszukiwane z nierozwiniętymi makrami.

Filtr znajduje się poniżej nazwy sekcji *Raport dostępności*. Można go otworzyć i zwinąć, klikając kartę *Filtr* po prawej stronie.

Filtrowanie według szablonu wyzwalacza

W trybie *Według szablonu wyzwalacza* wyniki można filtrować według jednego lub kilku parametrów wymienionych poniżej.

Parametr	Opis
Grupa szablonów	Filtruj hosty według wyzwalaczy dziedziczonych z szablonów należących do wybranej grupy szablonów. Określenie nadrzędnej grupy szablonów powoduje niejawne wybranie wszystkich zagnieżdżonych grup szablonów.
Szablon	Filtruj hosty według wyzwalaczy dziedziczonych z wybranego szablonu, w tym z szablonów zagnieżdżonych. Jeśli zagnieżdżony szablon ma własne wyzwalacze, te wyzwalacze nie będą wyświetlane.
Wyzwalacz szablonu	Filtruj hosty według wybranego wyzwalacza. Inne wyzwalacze przefiltrowanych hostów nie będą wyświetlane.
Grupa hostów	Filtruj hosty należące do wybranej grupy hostów.

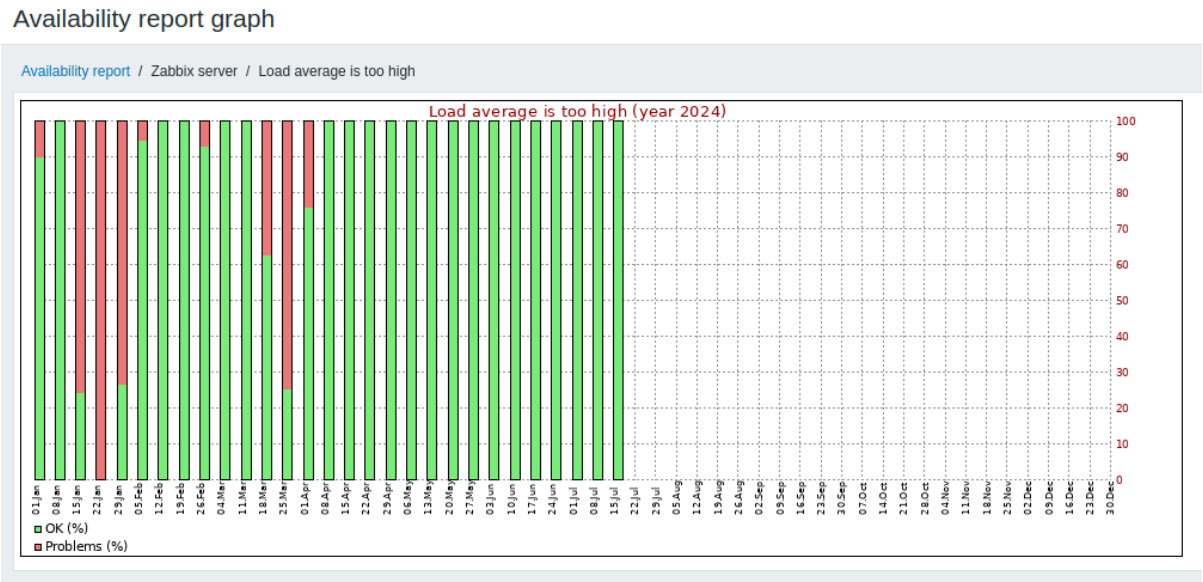
Filtrowanie według hosta

W trybie *Według hosta* wyniki mogą być filtrowane według hosta lub grupy hostów. Określenie nadrzędnej grupy hostów automatycznie wybiera wszystkie zagnieżdżone grupy hostów.

Selektor okresu czasu

Selektor okresu czasu umożliwia wybór często używanych okresów czasu jednym kliknięciem. Selektor można rozwinąć i zwinąć, klikając kartę *Okres czasu* obok filtra.

Kliknięcie *Pokaż* w kolumnie *Wykres* wyświetla informacje o dostępności na wykresie słupkowym, gdzie każdy słupek reprezentuje miniony tydzień bieżącego roku.



Zielony kolor słupka oznacza czas OK, a czerwony — czas problemu.

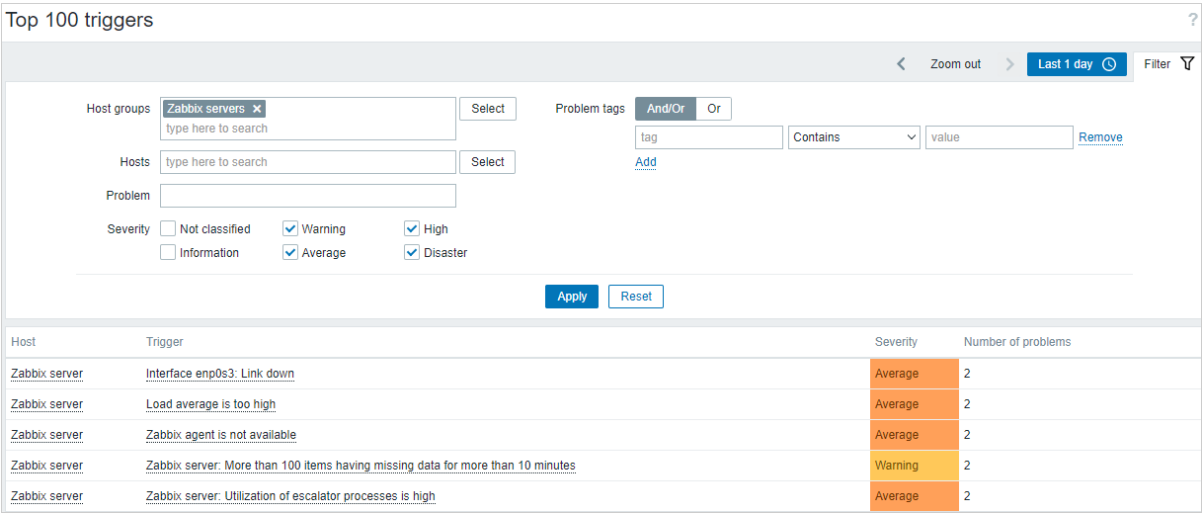
Wpływ okresów konserwacji

Konserwacja nie wyklucza automatycznie czasu z raportu dostępności. Tylko konserwacja skonfigurowana jako *Brak zbierania danych* zatrzymuje odpytywanie (więc nie są generowane żadne problemy), a zatem pozostawia procent dostępności bez zmian dla wyzwalaczy, których to dotyczy.

4 Top 100 wyzwalaczy

Przegląd

W *Raporty → 100 najczęstszych wyzwalaczy* można zobaczyć wyzwalacze z największą liczbą problemów wykrytych w wybranym okresie.



Wpisy zarówno w kolumnie hosta, jak i wyzwalacza są linkami oferującymi kilka przydatnych opcji:

- dla hosta — kliknięcie nazwy hosta otwiera menu hosta
- dla wyzwalacza — kliknięcie nazwy wyzwalacza otwiera odnośniki do najnowszych zdarzeń, prostego wykresu dla każdej pozycji wyzwalacza oraz formularzy konfiguracji samego wyzwalacza i każdej pozycji wyzwalacza

Korzystanie z filtra

Możesz użyć filtra, aby wyświetlić wyzwalacze według grupy hostów, hosta, nazwy problemu, tagów lub ważności wyzwalacza. Określenie nadrzędnej grupy hostów powoduje automatyczne wybranie wszystkich zagnieżdżonych grup hostów. Aby zapewnić lepszą wydajność wyszukiwania, dane są przeszukiwane przy nierozwiniętych makrach.

Filtr znajduje się poniżej nazwy sekcji *100 najczęstszych wyzwalaczy*. Można go rozwinąć i zwinąć, klikając kartę *Filtr* po prawej stronie.

Selektor okresu

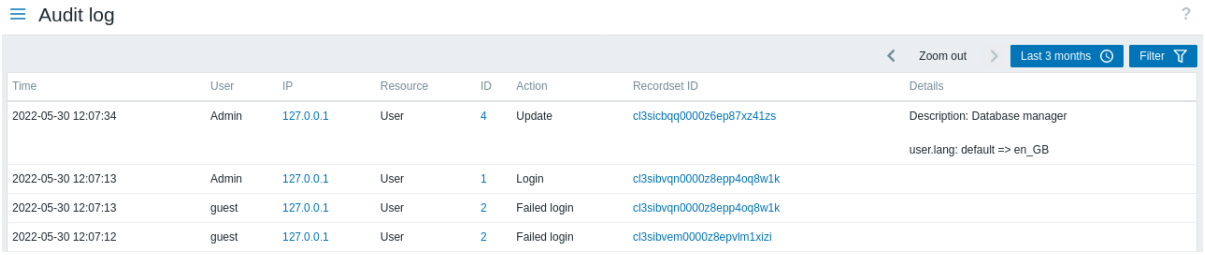
Selektor okresu obok filtra umożliwia wybranie często używanych okresów jednym kliknięciem myszy. Więcej informacji można znaleźć w sekcji Selektory okresu i hosta.

5 Dziennik audytu

Przegląd

W sekcji *Raporty* → *Dziennik audytu* można przeglądać wpisy dotyczące aktywności użytkowników i systemu.

Note:
Aby wpisy audytu były zbierane i wyświetlane, w sekcji *Administracja* → *Dziennik audytu* musi być zaznaczone pole wyboru *Włącz rejestrowanie audytu*. Jeśli to ustawienie nie jest włączone, historia aktywności nie będzie zapisywana w bazie danych i nie będzie wyświetlana w dzienniku audytu.



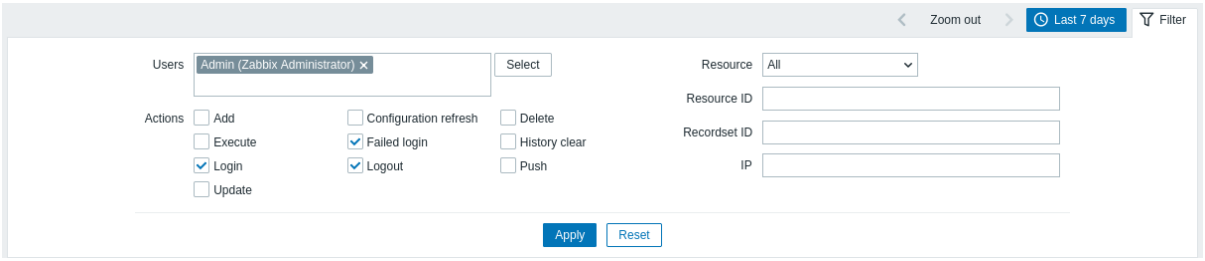
Dziennik audytu wyświetla następujące dane:

Kolumna	Opis
Czas	Znacznik czasu wpisu audytu.
Użytkownik	Użytkownik, który wykonał działanie.
IP	Adres IP, z którego zainicjowano działanie. Kliknięcie hiperłącza spowoduje filtrowanie wpisów dziennika audytu według tego adresu IP.
Zasób	Typ zasobu, którego dotyczy działanie (*Token API*, *Akcja*, *Uwierzytelnianie*, *Autorejestracja* itd.).
ID	ID zasobu, którego dotyczy działanie. Kliknięcie hiperłącza spowoduje filtrowanie wpisów dziennika audytu według ID tego zasobu.
Działanie	Typ działania (*Dodanie*, *Odświeżenie konfiguracji*, *Usunięcie*, *Wykonanie*, *Nieudane logowanie*, *Wyczyszczenie historii*, *Logowanie*, *Wylogowanie*, *Push*, *Aktualizacja*).
ID zestawu rekordów	Wspólne ID dla wszystkich wpisów dziennika audytu utworzonych w wyniku tej samej operacji. Na przykład podczas podłączania szablonu do hosta tworzony jest osobny wpis dziennika audytu dla każdej dziedziczonej encji szablonu (pozycja, wyzwalacz itd.) — wszystkie te wpisy będą miały to samo *ID zestawu rekordów*. Kliknięcie hiperłącza spowoduje filtrowanie wpisów dziennika audytu według tego *ID zestawu rekordów*.
Szczegóły	Opis zasobu oraz szczegółowe informacje o wykonanym działaniu. Jeśli wpis zawiera więcej niż dwa wiersze, zostanie wyświetlony dodatkowy odnośnik *Szczegóły*. Kliknij ten odnośnik, aby wyświetlić pełną listę zmian.

Note:
Gdy pozycja trapper lub pozycja HTTP agent (z włączonym przechwytywaniem) otrzyma dane, wpis w dzienniku audytu zostanie dodany tylko wtedy, gdy dane zostały wysłane przy użyciu metody API `history.push`, a nie narzędzia Zabbix sender.

Korzystanie z filtra

Filtr znajduje się poniżej paska *Dziennik audytu*. Można go otworzyć i zwinąć, klikając kartę *Filtr* w prawym górnym rogu.



Za pomocą filtra można zawęzić rekordy według użytkownika, zasobu, którego dotyczy operacja, identyfikatora zasobu, wykonanej operacji (*ID zestawu rekordów*) oraz adresu IP. W zależności od zasobu w filtrze można wybrać jedną lub więcej określonych akcji.

Aby zapewnić lepszą wydajność wyszukiwania, wszystkie dane są przeszukiwane z nierozwiniętymi makrami.

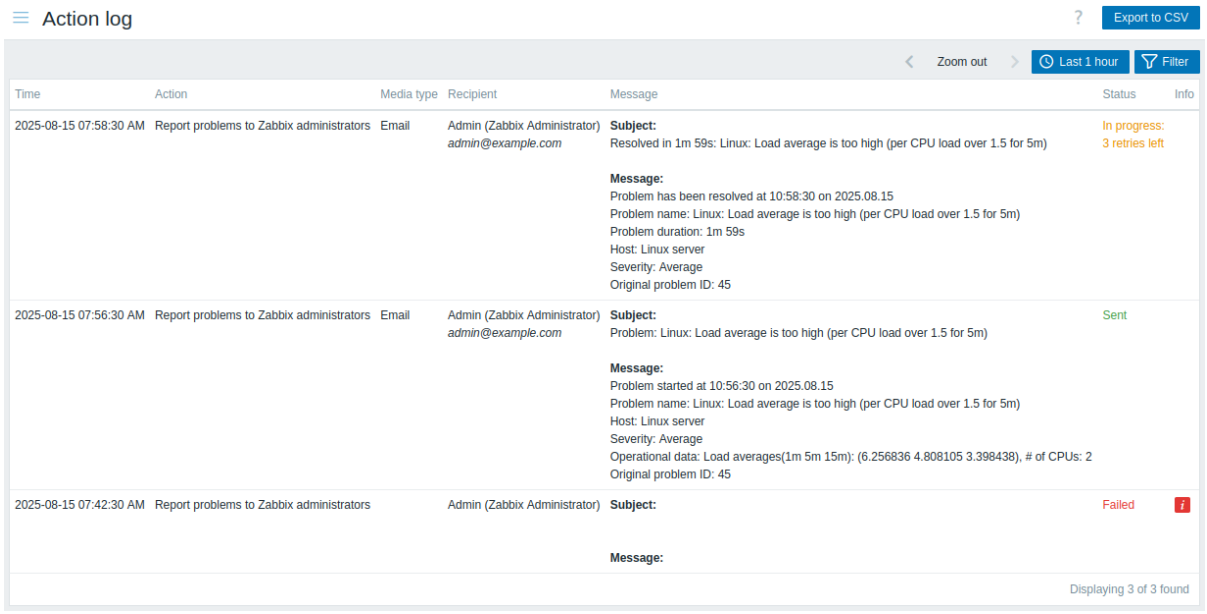
Selektor okresu czasu

Selektor okresu czasu obok filtra umożliwia wybór często wymaganych okresów jednym kliknięciem myszy. Więcej informacji można znaleźć w sekcji Selektory okresu czasu i hosta.

6 Dziennik akcji

Przegląd

W *Raporty* → *Dziennik akcji* można wyświetlić szczegóły operacji (powiadomień, zdalnych poleceń) wykonanych w ramach akcji.



Wyświetlane dane:

Kolumna	Opis
Czas	Znacznik czasu operacji.
Akcja	Nazwa akcji powodującej wykonanie operacji.
Typ nośnika	Typ nośnika (np. Email, Jira itp.) używany do wysyłania powiadomienia. W przypadku operacji wykonujących zdalne polecenia ta kolumna będzie pusta.
Odbiorca	Informacje o odbiorcy powiadomienia — nazwa użytkownika, imię i nazwisko (w nawiasach) oraz dodatkowe informacje zależne od typu nośnika (email, nazwa użytkownika itp.). W przypadku operacji wykonujących zdalne polecenia ta kolumna będzie pusta.
Wiadomość	Treść wiadomości, zdalnego polecenia lub nazwa skryptu globalnego. Zdalne polecenie jest oddzielone od docelowego hosta dwukropkiem: `<host>:<command>`. Na przykład, jeśli zdalne polecenie zostało wykonane na serwerze Zabbix, informacja będzie miała następujący format: `Zabbix server:<command>`.
Status	Status operacji: *W toku* - operacja wysyłania powiadomienia jest w toku (wyświetlana jest również pozostała liczba prób wysłania powiadomienia przez serwer) *Wysłano* - powiadomienie zostało wysłane *Wykonano* - zdalne polecenie zostało wykonane *Niepowodzenie* - operacja nie została ukończona
Informacje	Informacje o błędzie (jeśli wystąpił) dotyczące wykonania operacji.

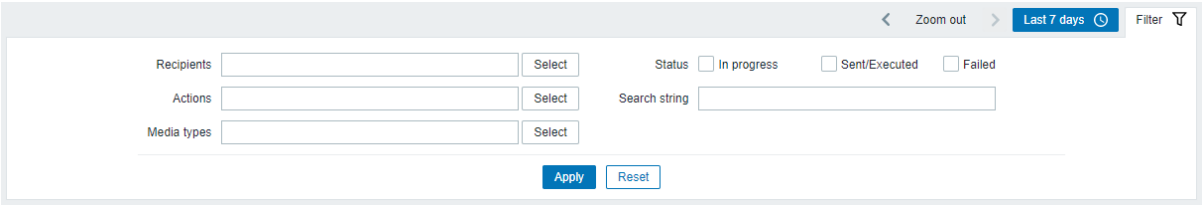
Przyciski

Przycisk w prawym górnym rogu strony oferuje następującą opcję:

Export to CSV	Eksportuj rekordy dziennika akcji z bieżącej strony do pliku CSV. Jeśli zastosowano filtr, wyeksportowane zostaną tylko przefiltrowane rekordy. W wyeksportowanym pliku CSV kolumny „Recipient" i „Message" są podzielone na kilka kolumn — „Recipient's Zabbix username", „Recipient's name", „Recipient's surname", „Recipient" oraz „Subject", „Message", „Command".

Korzystanie z filtra

Filtr znajduje się poniżej paska *Dziennik akcji*. Można go rozwinąć i zwinąć, klikając kartę *Filtr* w prawym górnym rogu strony.



Za pomocą filtra można zawęzić rekordy według odbiorców powiadomień, akcji, typów mediów, statusu lub treści wiadomości/zdalnego polecenia (*Szukany ciąg*). Aby zapewnić lepszą wydajność wyszukiwania, dane są przeszukiwane z nierozwiniętymi makrami.

Selektor okresu czasu

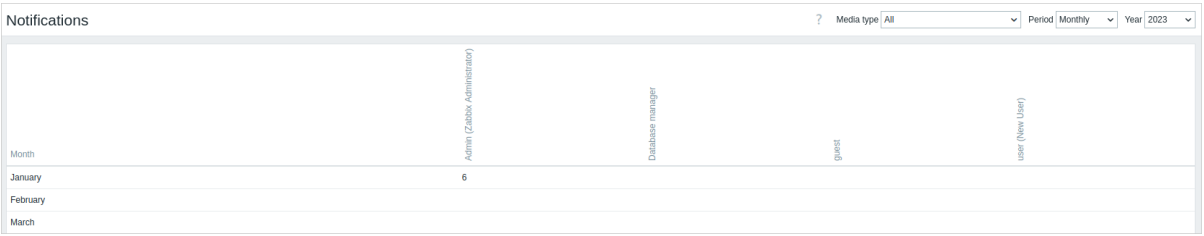
Selektor okresu czasu obok filtra umożliwia wybranie często wymaganych okresów jednym kliknięciem myszy. Więcej informacji można znaleźć w sekcji Selektory okresu czasu i hosta.

7 Powiadomienia

Przegląd

W sekcji *Raporty* → *Powiadomienia* wyświetlany jest raport dotyczący liczby powiadomień wysłanych do każdego użytkownika.

Z list rozwijanych w prawym górnym rogu można wybrać typ nośnika (lub wszystkie), okres (dane dla każdego dnia/tygodnia/miesiąca/roku) oraz rok dla wysłanych powiadomień.



Każda kolumna wyświetla sumy dla jednego użytkownika systemu.

6 Zbieranie danych

Przegląd

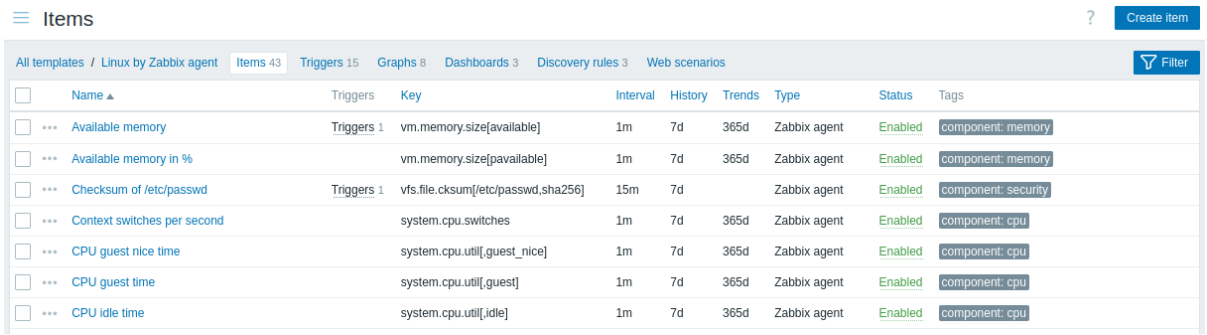
To menu zawiera sekcje związane z konfiguracją zbierania danych.

1 Pozycje

Przegląd

Lista pozycji dla szablonu jest dostępna w *Zbieranie danych* → *Szablony* po kliknięciu *Pozycje* dla odpowiedniego szablonu.

Zostanie wyświetlona lista istniejących pozycji.



Wyświetlane dane:

Kolumna	Opis
Menu pozycji	Kliknij ikonę z trzema kropkami, aby otworzyć menu pozycji.
Szablon	Szablon, do którego należy pozycja. Kliknięcie nazwy szablonu otwiera formularz konfiguracji szablonu. Ta kolumna jest wyświetlana tylko wtedy, gdy w filtrze wybrano wiele szablonów lub nie wybrano żadnego szablonu.
Nazwa	Nazwa pozycji jest wyświetlana jako niebieski link do szczegółów pozycji. Kliknięcie linku z nazwą pozycji otwiera formularz konfiguracji pozycji. Jeśli pozycja jest dziedziczona z innego szablonu, nazwa szablonu jest wyświetlana przed nazwą pozycji jako szary link. Kliknięcie linku szablonu otwiera listę pozycji na poziomie tego szablonu.
Wyzwalacze	Po najechaniu kursorem na Wyzwalacze zostanie wyświetlone okno informacyjne pokazujące wyzwalacze powiązane z pozycją. Liczba wyzwalaczy jest wyświetlana na szaro.
Klucz	Wyświetlany jest klucz pozycji.
Interwał	Wyświetlana jest częstotliwość sprawdzania.
Historia	Wyświetlana jest liczba dni, przez które będzie przechowywana historia danych pozycji.
Trendy	Wyświetlana jest liczba dni, przez które będzie przechowywana historia trendów pozycji.
Typ	Wyświetlany jest typ pozycji (agent Zabbix, agent SNMP, proste sprawdzenie itd.).
Status	Wyświetlany jest status pozycji — *Włączony* lub *Wyłączony*. Klikając status, możesz go zmienić — z Włączony na Wyłączony (i odwrotnie).
Tagi	Wyświetlane są tagi pozycji. Można wyświetlić maksymalnie trzy tagi (pary nazwa:wartość). Jeśli tagów jest więcej, wyświetlany jest link „...", który po najechaniu kursorem pozwala zobaczyć wszystkie tagi.

Aby skonfigurować nową pozycję, kliknij przycisk *Utwórz pozycję* w prawym górnym rogu.

Opcje masowej edycji

Przyciski pod listą oferują kilka opcji masowej edycji:

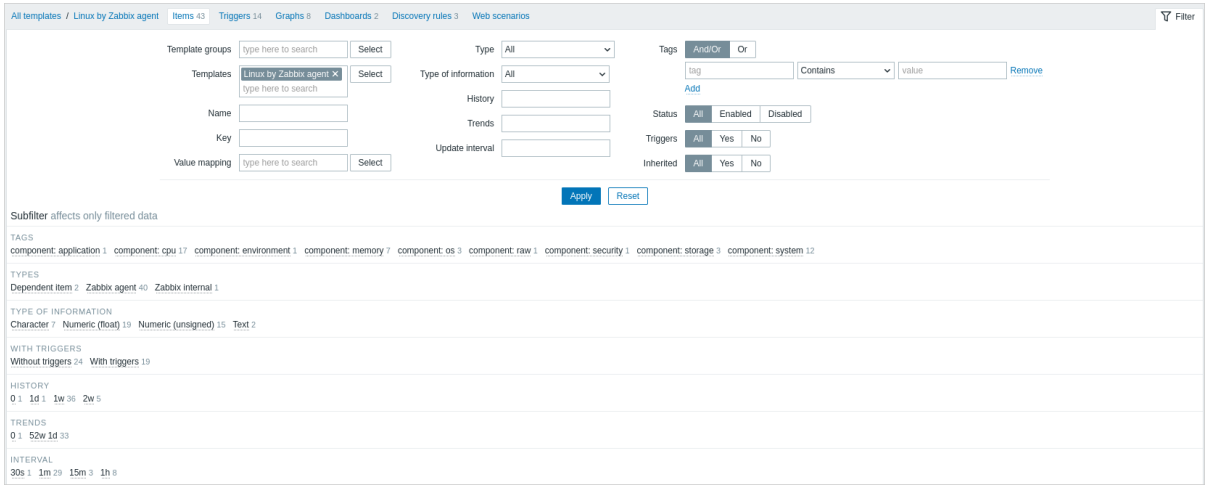
- *Włącz* — zmień status pozycji na *Włączony*.
- *Wyłącz* — zmień status pozycji na *Wyłączony*.
- *Kopiuj* — skopiuj pozycje do innych hostów lub szablonów.
- *Masowa aktualizacja* — zaktualizuj kilka właściwości dla wielu pozycji jednocześnie.
- *Usuń* — usuń pozycje.

Aby skorzystać z tych opcji, zaznacz pola wyboru przy odpowiednich pozycjach, a następnie kliknij wymagany przycisk.

Korzystanie z filtra

Lista pozycji może zawierać wiele pozycji. Korzystając z filtra, możesz odfiltrować część z nich, aby szybko znaleźć szukane pozycje. Dla lepszej wydajności wyszukiwania dane są przeszukiwane z nierozwiniętymi makrami.

Ikona *Filtr* jest dostępna w prawym górnym rogu. Kliknięcie jej otworzy filtr, w którym można określić żądane kryteria filtrowania.

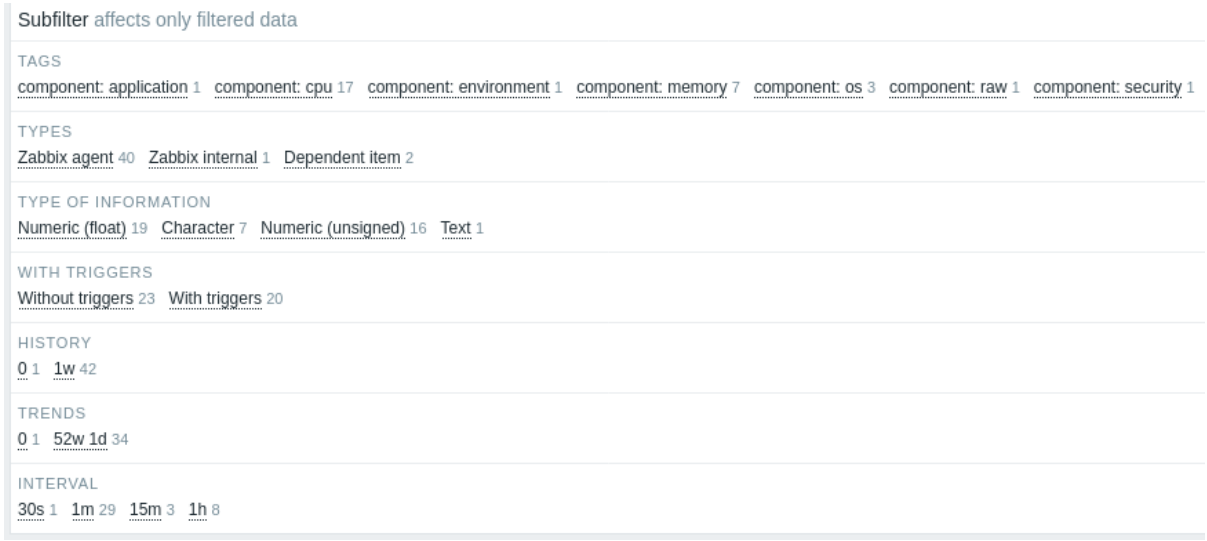


Parametr	Opis
Template groups	Filtruj według jednej lub większej liczby grup szablonów. Określenie nadrzędnej grupy szablonów powoduje domyślnie wybranie wszystkich grup zagnieżdżonych.
Templates	Filtruj według jednego lub większej liczby szablonów.
Name	Filtruj według nazwy pozycji.
Key	Filtruj według klucza pozycji.
Value mapping	Filtruj według używanej mapy wartości. Ten parametr nie jest wyświetlany, jeśli opcja *Templates* jest pusta.
Type	Filtruj według typu pozycji (agent Zabbix, agent SNMP itp.).
Type of information	Filtruj według typu informacji (bezznakowa wartość numeryczna, liczba zmiennoprzecinkowa itp.).
History	Filtruj według czasu przechowywania historii pozycji.
Trends	Filtruj według czasu przechowywania trendów pozycji.
Update interval	Filtruj według interwału aktualizacji pozycji.
Tags	Określ tagi, aby ograniczyć liczbę wyświetlanych pozycji. Możliwe jest zarówno uwzględnianie, jak i wykluczanie określonych tagów oraz wartości tagów. Można ustawić kilka warunków. Dopasowanie nazw tagów zawsze uwzględnia wielkość liter. Dla każdego warunku dostępnych jest kilka operatorów: **Exists** - uwzględnij określone nazwy tagów **Equals** - uwzględnij określone nazwy i wartości tagów (z uwzględnieniem wielkości liter) **Contains** - uwzględnij określone nazwy tagów, dla których wartości tagów zawierają wprowadzony ciąg znaków (dopasowanie podciągu, bez uwzględniania wielkości liter) **Does not exist** - wyklucz określone nazwy tagów **Does not equal** - wyklucz określone nazwy i wartości tagów (z uwzględnieniem wielkości liter) **Does not contain** - wyklucz określone nazwy tagów, dla których wartości tagów zawierają wprowadzony ciąg znaków (dopasowanie podciągu, bez uwzględniania wielkości liter) Dla warunków dostępne są dwa typy obliczeń: **And/Or** - wszystkie warunki muszą być spełnione, warunki mające tę samą nazwę tagu będą grupowane operatorem Or **Or** - wystarczy spełnienie jednego warunku
Status	Filtruj według statusu pozycji — *Enabled* lub *Disabled*.
Triggers	Filtruj pozycje z wyzwalaczami (lub bez nich).
Inherited	Filtruj pozycje dziedziczone (lub niedziedziczone) z podłączonych szablonów.

Korzystanie z podfiltra

Podfiltr pozwala dalej modyfikować filtrowanie z filtra głównego.

Zawiera klikalne odnośniki umożliwiające szybki dostęp do powiązanych pozycji. Pozycje są powiązane wspólną jednostką, taką jak tag, typ pozycji, interwał aktualizacji pozycji itp. Po kliknięciu jednostki zostaje ona wyróżniona szarym tłem, a pozycje są natychmiast filtrowane (bez potrzeby klikania przycisku *Zastosuj* w filtrze głównym). Kliknięcie innej jednostki dodaje ją do filtrowanych wyników. Ponowne kliknięcie jednostki usuwa filtrowanie.



Podfiltry są generowane na podstawie przefiltrowanych danych, których liczba jest ograniczona do 1000 rekordów. Jeśli chcesz zobaczyć więcej rekordów w podfiltrze, musisz zwiększyć wartość parametru *Limit for search and filter results* (w *Administration -> General -> GUI*).

W przeciwieństwie do filtra głównego, podfiltr jest aktualizowany przy każdym żądaniu odświeżenia tabeli, aby zawsze zawierał aktualne informacje o dostępnych opcjach filtrowania i licznikach.

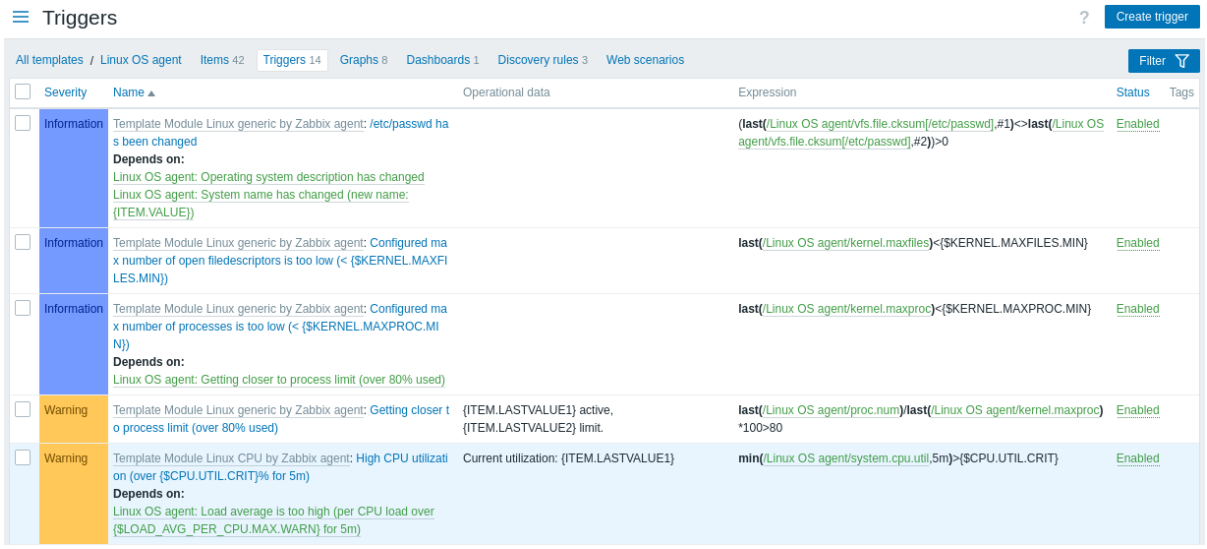
Liczba wyświetlanych jednostek jest ograniczona poziomo do 100. Jeśli jest ich więcej, na końcu wyświetlana jest ikona trzech kropek; nie można jej kliknąć.

Liczba obok każdej klikalnej jednostki wskazuje liczbę pozycji w niej zgrupowanych (na podstawie wyników filtra głównego). Po kliknięciu jednostki liczby przy innych dostępnych jednostkach są wyświetlane ze znakiem plus, wskazującym, ile pozycji można dodać do bieżącego wyboru. Jednostki bez pozycji nie są wyświetlane, chyba że zostały wcześniej wybrane w podfiltrze.

2 Wyzwalacze

Przegląd

Lista wyzwalaczy dla szablonu jest dostępna w *Zbieranie danych* → *Szablony* po kliknięciu *Wyzwalacze* dla odpowiedniego szablonu.



Wyświetlane dane:

Kolumna	Opis
Istotność	Istotność wyzwalacza jest wyświetlana zarówno nazwą, jak i kolorem tła komórki.

Kolumna	Opis
Szablon	Szablon, do którego należy wyzwalacz. Kliknięcie nazwy szablonu otwiera formularz konfiguracji szablonu. Ta kolumna jest wyświetlana tylko wtedy, gdy w filtrze wybrano wiele szablonów lub nie wybrano żadnego szablonu.
Nazwa	Nazwa wyzwalacza jest wyświetlana jako niebieski link do szczegółów wyzwalacza. Kliknięcie linku z nazwą wyzwalacza otwiera formularz konfiguracji wyzwalacza. Jeśli wyzwalacz jest dziedziczony z innego szablonu, nazwa szablonu jest wyświetlana przed nazwą wyzwalacza jako szary link. Kliknięcie linku szablonu otwiera listę wyzwalaczy na poziomie tego szablonu.
Dane operacyjne	Definicja danych operacyjnych wyzwalacza, zawierająca dowolne ciągi znaków i makra, które będą dynamicznie rozwijane w *Monitorowanie* → *Problemy*.
Wyrażenie	Wyświetlane jest wyrażenie wyzwalacza. Część wyrażenia dotycząca szablonu i pozycji jest wyświetlana jako link prowadzący do formularza konfiguracji pozycji.
Status	Wyświetlany jest status wyzwalacza — *Włączony* lub *Wyłączony*. Klikając status, można go zmienić — z Włączony na Wyłączony (i z powrotem).
Tagi	Jeśli wyzwalacz zawiera tagi, w tej kolumnie wyświetlana jest nazwa tagu i jego wartość.

Aby skonfigurować nowy wyzwalacz, kliknij przycisk *Utwórz wyzwalacz* w prawym górnym rogu.

Opcje masowej edycji

Przyciski pod listą oferują kilka opcji masowej edycji:

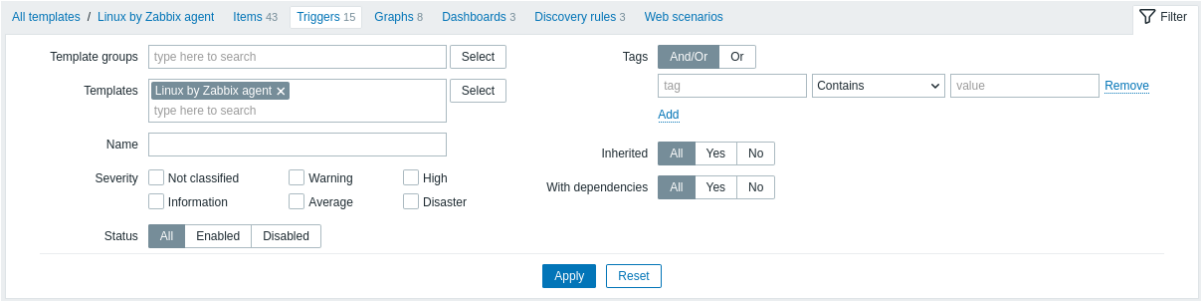
- *Włącz* - zmień status wyzwalacza na *Włączony*
- *Wyłącz* - zmień status wyzwalacza na *Wyłączony*
- *Kopiuj* - skopiuj wyzwalacze do innych hostów lub szablonów
- *Masowa aktualizacja* - zaktualizuj jednocześnie kilka właściwości dla wielu wyzwalaczy
- *Usuń* - usuń wyzwalacze

Aby użyć tych opcji, zaznacz pola wyboru przy odpowiednich wyzwalaczach, a następnie kliknij wymagany przycisk.

Korzystanie z filtra

Możesz użyć filtra, aby wyświetlić tylko te wyzwalacze, które Cię interesują. Dla lepszej wydajności wyszukiwania dane są przeszukiwane z nierozwiniętymi makrami.

Ikona *Filtr* jest dostępna w prawym górnym rogu. Kliknięcie jej otworzy filtr, w którym można określić żądane kryteria filtrowania.



Parametr	Opis
Grupy szablonów	Filtruj według jednej lub większej liczby grup szablonów. Określenie nadrzędnej grupy szablonów powoduje domyślnie wybranie wszystkich grup zagnieżdżonych.
Szablony	Filtruj według jednego lub większej liczby szablonów. Jeśli powyżej wybrano już grupy szablonów, wybór szablonów jest ograniczony do tych grup.
Nazwa	Filtruj według nazwy wyzwalacza.
Ważność	Wybierz, aby filtrować według jednego lub kilku poziomów ważności wyzwalacza.
Status	Filtruj według statusu aktywacji wyzwalacza (Włączony/Wyłączony).

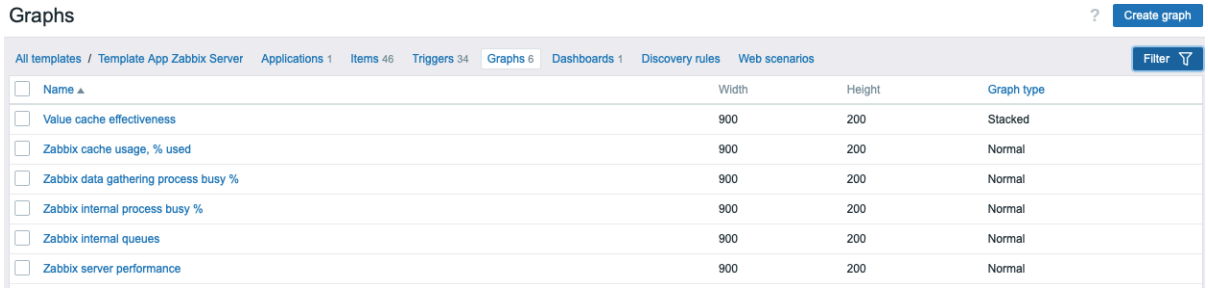
Parametr	Opis
Tagi	Filtruj według nazwy i wartości tagu wyzwalacza. Możliwe jest zarówno uwzględnianie, jak i wykluczanie określonych tagów oraz wartości tagów. Można ustawić kilka warunków. Dopasowanie nazw tagów zawsze uwzględnia wielkość liter. Dla każdego warunku dostępnych jest kilka operatorów: **Istnieje** - uwzględnij określone nazwy tagów **Równa się** - uwzględnij określone nazwy i wartości tagów (z uwzględnieniem wielkości liter) **Zawiera** - uwzględnij określone nazwy tagów, których wartości zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter) **Nie istnieje** - wyklucz określone nazwy tagów **Nie równa się** - wyklucz określone nazwy i wartości tagów (z uwzględnieniem wielkości liter) **Nie zawiera** - wyklucz określone nazwy tagów, których wartości zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter) Dostępne są dwa typy obliczania warunków: **And/Or** - wszystkie warunki muszą być spełnione, warunki mające tę samą nazwę tagu będą grupowane przez warunek Or **Or** - wystarczy, że jeden warunek zostanie spełniony Makra i funkcje makr są obsługiwane w polach nazwy i wartości tagu.
Dziedziczone	Filtruj wyzwalacze dziedziczone (lub niedziedziczone) z podłączonych szablonów.
Z zależnościami	Filtruj wyzwalacze z zależnościami (lub bez zależności).

3 Wykresy

Przegląd

Do listy wykresów niestandardowych dla szablonu można przejść z poziomu *Data collection* → *Templates*, klikając *Graphs* przy odpowiednim szablonie.

Wyświetlana jest lista istniejących wykresów.



Wyświetlane dane:

Kolumna	Opis
Template	Szablon, do którego należy wykres. Kliknięcie nazwy szablonu otwiera formularz konfiguracji szablonu. Ta kolumna jest wyświetlana tylko wtedy, gdy w filtrze wybrano wiele szablonów lub nie wybrano żadnego szablonu.
Name	Nazwa wykresu niestandardowego, wyświetlana jako niebieski link do szczegółów wykresu. Kliknięcie linku z nazwą wykresu otwiera formularz konfiguracji wykresu. Jeśli wykres jest dziedziczony z innego szablonu, przed nazwą wykresu wyświetlana jest nazwa szablonu jako szary link. Kliknięcie linku szablonu otwiera listę wykresów na poziomie tego szablonu.
Width	Wyświetlana jest szerokość wykresu.
Height	Wyświetlana jest wysokość wykresu.
Graph type	Wyświetlany jest typ wykresu — *Normal*, *Stacked*, *Pie* lub *Exploded*.

Aby skonfigurować nowy wykres, kliknij przycisk *Create graph* w prawym górnym rogu.

Opcje masowej edycji

Przyciski pod listą oferują kilka opcji masowej edycji:

- *Kopiuj* - kopiowanie wykresów do innych hostów lub szablonów
- *Usuń* - usuwanie wykresów

Aby skorzystać z tych opcji, zaznacz pola wyboru przy odpowiednich wykresach, a następnie kliknij wymagany przycisk.

Używanie filtra

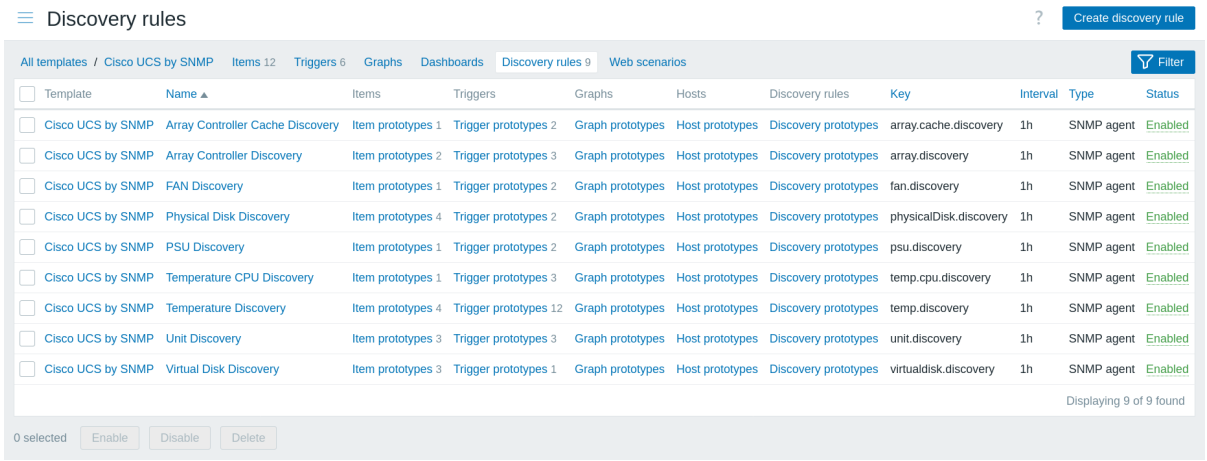
Możesz filtrować wykresy według grupy szablonów i szablonu. Aby uzyskać lepszą wydajność wyszukiwania, dane są przeszukiwane z nierozwiniętymi makrami.

4 Reguły wykrywania

Przegląd

Lista reguł wykrywania niskiego poziomu dla szablonu jest dostępna w *Zbieranie danych* → *Szablony* po kliknięciu *Wykrywanie* dla odpowiedniego szablonu.

Wyświetlana jest lista istniejących reguł wykrywania niskiego poziomu. Możliwe jest również wyświetlenie wszystkich reguł wykrywania niezależnie od szablonu lub wszystkich reguł wykrywania dla określonej grupy szablonów poprzez zmianę ustawień filtra.



Wyświetlane dane:

Kolumna	Opis
Szablon	Szablon, do którego należy reguła wykrywania. Kliknięcie nazwy szablonu otwiera formularz konfiguracji szablonu.
Nazwa	Nazwa reguły, wyświetlana jako niebieski link. Kliknięcie nazwy reguły otwiera formularz konfiguracji reguły wykrywania niskiego poziomu. Jeśli reguła wykrywania jest dziedziczona z innego szablonu, nazwa szablonu jest wyświetlana przed nazwą reguły jako szary link. Kliknięcie linku szablonu otwiera listę reguł wykrywania na poziomie tego szablonu.
Pozycje	Wyświetlany jest link do listy prototypów pozycji. Liczba istniejących prototypów pozycji jest wyświetlana na szaro.
Wyzwalacze	Wyświetlany jest link do listy prototypów wyzwalaczy. Liczba istniejących prototypów wyzwalaczy jest wyświetlana na szaro.
Wykresy	Wyświetlany jest link do listy prototypów wykresów. Liczba istniejących prototypów wykresów jest wyświetlana na szaro.
Hosty	Wyświetlany jest link do listy prototypów hostów. Liczba istniejących prototypów hostów jest wyświetlana na szaro.
Klucz	Wyświetlany jest klucz pozycji używany do wykrywania.
Interwał	Wyświetlana jest częstotliwość wykonywania wykrywania.
Typ	Wyświetlany jest typ pozycji używany do wykrywania (agent Zabbix, agent SNMP itp.).
Status	Wyświetlany jest status reguły wykrywania — *Włączona* lub *Wyłączona*. Klikając status, można go zmienić — z Włączona na Wyłączona (i odwrotnie).

Aby skonfigurować nową regułę wykrywania niskiego poziomu, kliknij przycisk *Utwórz regułę wykrywania* w prawym górnym rogu.

Opcje masowej edycji

Przyciski pod listą oferują kilka opcji masowej edycji:

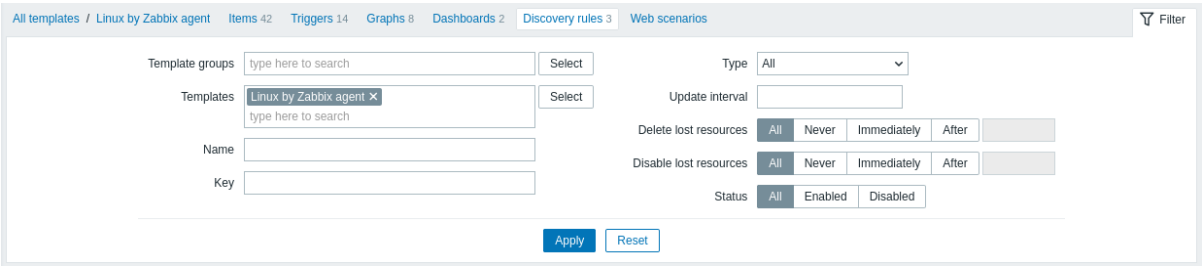
- *Włącz* - zmień status reguły wykrywania niskiego poziomu na *Włączony*
- *Wyłącz* - zmień status reguły wykrywania niskiego poziomu na *Wyłączony*
- *Usuń* - usuń reguły wykrywania niskiego poziomu

Aby użyć tych opcji, zaznacz pola wyboru przy odpowiednich regułach wykrywania, a następnie kliknij wymagany przycisk.

Używanie filtra

Możesz użyć filtra, aby wyświetlić tylko te reguły wykrywania, które Cię interesują. Aby zapewnić lepszą wydajność wyszukiwania, dane są przeszukiwane z nierozwiniętymi makrami.

Ikona *Filtr* jest dostępna w prawym górnym rogu. Kliknięcie jej otworzy filtr, w którym można określić żądane kryteria filtrowania, takie jak szablon, nazwa reguły wykrywania, klucz pozycji, typ pozycji itp.



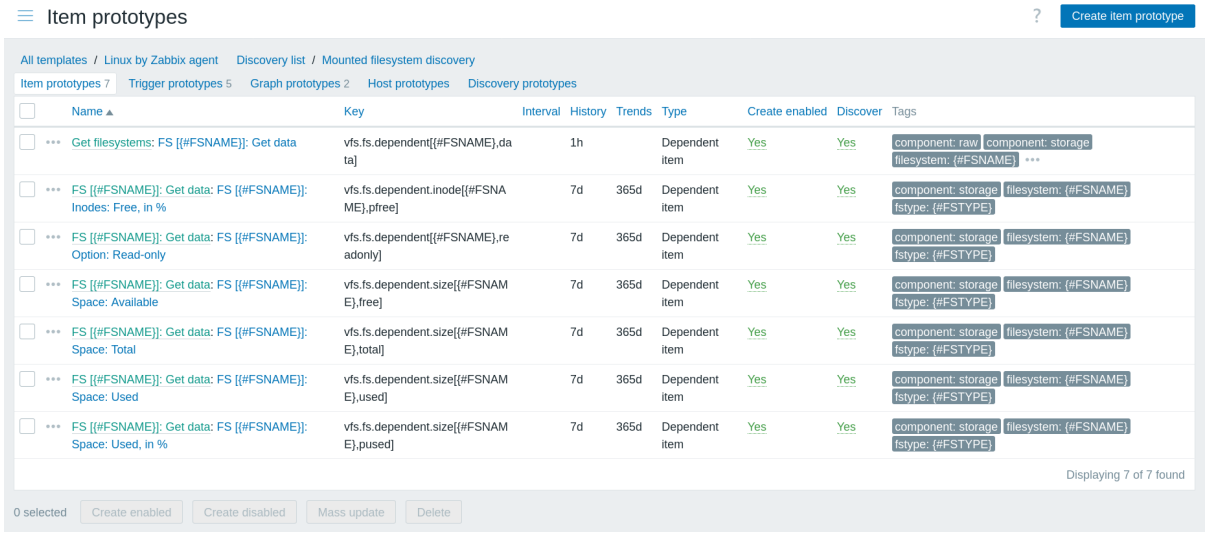
Parametr	Opis
Grupy szablonów	Filtruj według jednej lub większej liczby grup szablonów. Określenie nadrzędnej grupy szablonów powoduje domyślnie wybranie wszystkich grup zagnieżdżonych.
Szablony	Filtruj według jednego lub większej liczby szablonów.
Nazwa	Filtruj według nazwy reguły wykrywania.
Klucz	Filtruj według klucza pozycji wykrywania.
Typ	Filtruj według typu pozycji wykrywania.
Interwał aktualizacji	Filtruj według interwału aktualizacji. Niedostępne dla pozycji typu Zabbix trapper i pozycji zależnych.
Usuwanie utraconych zasobów	Filtruj według okresu *Usuwanie utraconych zasobów*.
Wyłączanie utraconych zasobów	Filtruj według okresu *Wyłączanie utraconych zasobów*.
Status	Filtruj według statusu reguły wykrywania (Wszystkie/Włączone/Wyłączone).

1 Prototypy pozycji

Przegląd

W tej sekcji wyświetlane są skonfigurowane prototypy pozycji reguły wykrywania niskiego poziomu w szablonie.

Jeśli szablon jest podłączony do hosta, prototypy pozycji staną się podstawą do tworzenia rzeczywistych pozycji hosta podczas wykrywania niskiego poziomu.



Wyświetlane dane:

Kolumna	Opis
Nazwa	Wyświetlana jest nazwa prototypu pozycji jako niebieski link. Kliknięcie nazwy otwiera formularz konfiguracji prototypu pozycji. Jeśli prototyp pozycji należy do podłączonego szablonu, nazwa szablonu jest wyświetlana przed nazwą prototypu pozycji jako szary link. Kliknięcie linku szablonu otwiera listę prototypów pozycji na poziomie podłączonego szablonu. Jeśli prototyp pozycji jest typu „Pozycja zależna”, nazwa pozycji nadrzędnej jest wyświetlana przed nazwą prototypu pozycji na zielono (tak jak w przypadku prototypów pozycji na poziomie hosta).
Klucz	Wyświetlany jest klucz prototypu pozycji.
Interwał	Wyświetlana jest częstotliwość sprawdzania.
Historia	Wyświetlana jest liczba dni przechowywania historii danych pozycji.
Trendy	Wyświetlana jest liczba dni przechowywania historii trendów pozycji.
Typ	Wyświetlany jest typ prototypu pozycji (agent Zabbix, agent SNMP, proste sprawdzenie itp.).
Utwórz włączone	Utwórz pozycję na podstawie tego prototypu jako: **Tak** - włączona **Nie** - wyłączona. Możesz przełączać między „Tak” i „Nie”, klikając je.
Odkrywaj	Odkrywaj pozycję na podstawie tego prototypu: **Tak** - odkrywaj **Nie** - nie odkrywaj. Możesz przełączać między „Tak” i „Nie”, klikając je.
Tagi	Wyświetlane są tagi prototypu pozycji.

Aby skonfigurować nowy prototyp pozycji, kliknij przycisk *Utwórz prototyp pozycji* w prawym górnym rogu.

Opcje masowej edycji

Przyciski poniżej listy oferują kilka opcji masowej edycji:

- *Utwórz włączone* - utwórz te pozycje jako *Włączone*
- *Utwórz wyłączone* - utwórz te pozycje jako *Wyłączone*
- *Masowa aktualizacja* - masowo zaktualizuj te prototypy pozycji
- *Usuń* - usuń te prototypy pozycji

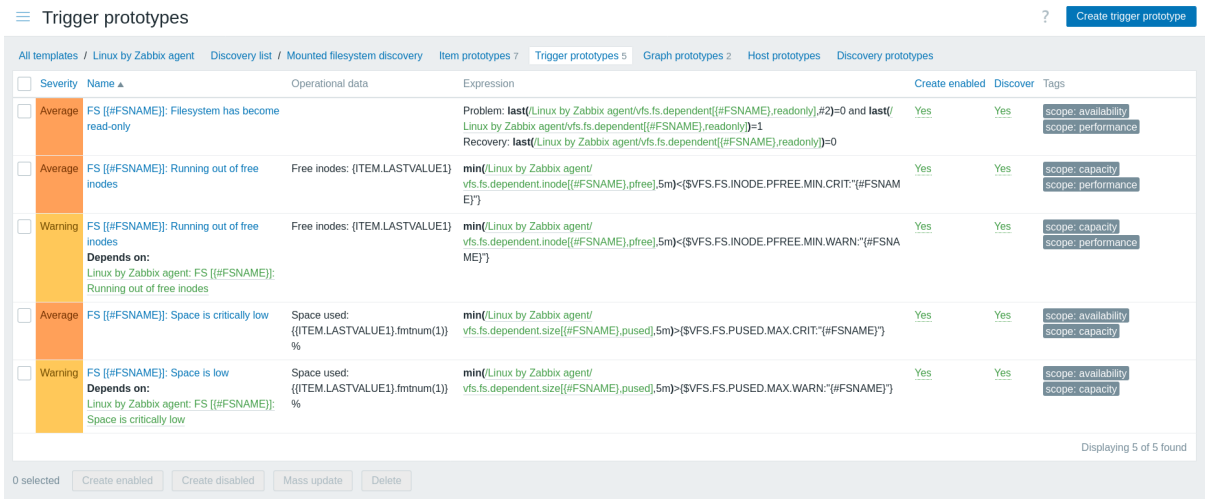
Aby użyć tych opcji, zaznacz pola wyboru przy odpowiednich prototypach pozycji, a następnie kliknij wymagany przycisk.

2 Prototypy wyzwalaczy

Przegląd

W tej sekcji wyświetlane są skonfigurowane prototypy wyzwalaczy reguły wykrywania niskiego poziomu w szablonie.

Jeśli szablon jest podłączony do hosta, prototypy wyzwalaczy staną się podstawą do tworzenia rzeczywistych wyzwalaczy hosta podczas wykrywania niskiego poziomu.



Wyświetlane dane:

Column	Description
Severity	Poziom ważności wyzwalacza jest wyświetlany zarówno nazwą, jak i kolorem tła komórki.
Name	Nazwa prototypu wyzwalacza, wyświetlana jako niebieski link. Kliknięcie nazwy otwiera formularz konfiguracji prototypu wyzwalacza. Jeśli prototyp wyzwalacza należy do podłączonego szablonu, nazwa szablonu jest wyświetlana przed nazwą wyzwalacza jako szary link. Kliknięcie linku szablonu otwiera listę prototypów wyzwalaczy na poziomie podłączonego szablonu.
Expression	Wyświetlane jest wyrażenie wyzwalacza. Część wyrażenia odnosząca się do szablonu i pozycji jest wyświetlana jako link prowadzący do formularza konfiguracji pozycji.
Operational data	Wyświetlany jest format danych operacyjnych wyzwalacza, zawierający dowolne ciągi znaków i makra, które będą dynamicznie rozwijane w *Monitoring* → *Problems*.
Create enabled	Utwórz wyzwalacz na podstawie tego prototypu jako: **Yes** - włączony **No** - wyłączony. Możesz przełączać między „Yes” i „No”, klikając je.
Discover	Wykrywaj wyzwalacz na podstawie tego prototypu: **Yes** - wykrywaj **No** - nie wykrywaj. Możesz przełączać między „Yes” i „No”, klikając je.
Tags	Wyświetlane są tagi prototypu wyzwalacza.

Aby skonfigurować nowy prototyp wyzwalacza, kliknij przycisk *Create trigger prototype* w prawym górnym rogu.

Opcje masowej edycji

Przyciski pod listą oferują kilka opcji masowej edycji:

- *Utwórz włączone* - utwórz te wyzwalacze jako *Włączone*
- *Utwórz wyłączone* - utwórz te wyzwalacze jako *Wyłączone*
- *Masowa aktualizacja* - masowo zaktualizuj te prototypy wyzwalaczy
- *Usuń* - usuń te prototypy wyzwalaczy

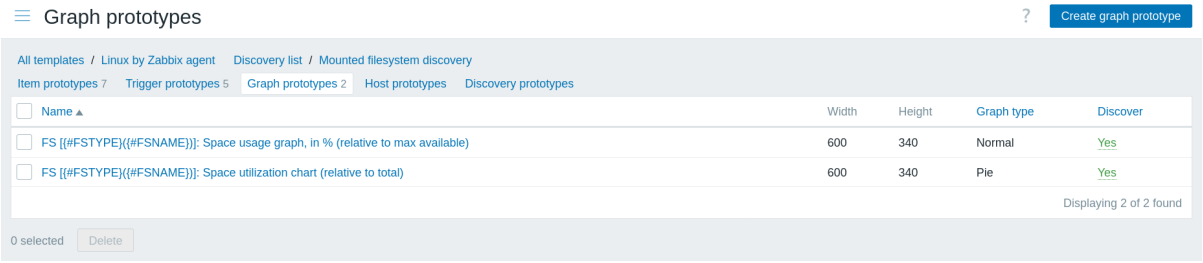
Aby użyć tych opcji, zaznacz pola wyboru przy odpowiednich prototypach wyzwalaczy, a następnie kliknij wymagany przycisk.

3 Prototypy wykresów

Przegląd

W tej sekcji wyświetlane są skonfigurowane prototypy wykresów reguły wykrywania niskiego poziomu w szablonie.

Jeśli szablon jest podłączony do hosta, prototypy wykresów staną się podstawą do tworzenia rzeczywistych wykresów hosta podczas wykrywania niskiego poziomu.



Wyświetlane dane:

Kolumna	Opis
Nazwa	Nazwa prototypu wykresu, wyświetlana jako niebieski odnośnik. Kliknięcie nazwy otwiera formularz konfiguracji prototypu wykresu. Jeśli prototyp wykresu należy do podłączonego szablonu, nazwa szablonu jest wyświetlana przed nazwą wykresu jako szary odnośnik. Kliknięcie odnośnika szablonu otwiera listę prototypów wykresów na poziomie podłączonego szablonu.
Szerokość	Wyświetlana jest szerokość prototypu wykresu.
Wysokość	Wyświetlana jest wysokość prototypu wykresu.
Typ	Wyświetlany jest typ prototypu wykresu — *Normalny*, *Skumulowany*, *Kołowy* lub *Rozsunięty*.
Odkrywaj	Odkrywanie wykresu na podstawie tego prototypu: **Tak** - odkrywaj **Nie** - nie odkrywaj. Możesz przełączać między „Tak” i „Nie”, klikając te wartości.

Aby skonfigurować nowy prototyp wykresu, kliknij przycisk *Utwórz prototyp wykresu* w prawym górnym rogu.

Opcje masowej edycji

Przyciski poniżej listy oferują kilka opcji masowej edycji:

- *Usuń* - usuń te prototypy wykresów

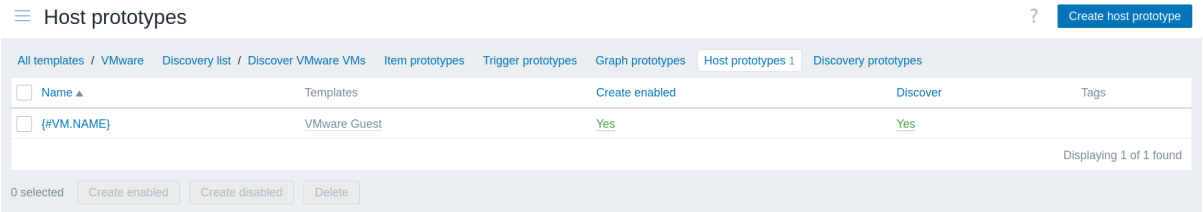
Aby skorzystać z tych opcji, zaznacz pola wyboru przy odpowiednich prototypach wykresów, a następnie kliknij wymagany przycisk.

4 Prototypy hostów

Przegląd

W tej sekcji wyświetlane są skonfigurowane prototypy hostów reguły wykrywania niskiego poziomu w szablonie.

Jeśli szablon jest podłączony do hosta, prototypy hostów staną się podstawą do tworzenia rzeczywistych hostów podczas wykrywania niskiego poziomu.



Wyświetlane dane:

Kolumna	Opis
Nazwa	Nazwa prototypu hosta, wyświetlana jako niebieski link. Kliknięcie nazwy otwiera formularz konfiguracji prototypu hosta. Jeśli prototyp hosta należy do podłączonego szablonu, nazwa szablonu jest wyświetlana przed nazwą hosta jako szary link. Kliknięcie linku szablonu otwiera listę prototypów hostów na poziomie podłączonego szablonu.
Szablony	Wyświetlane są szablony prototypu hosta.
Tworzenie włączone	Utwórz host na podstawie tego prototypu jako: **Tak** - włączone **Nie** - wyłączone. Możesz przełączać między „Tak” i „Nie”, klikając te wartości.

Kolumna	Opis
Wykrywaj	Wykrywaj host na podstawie tego prototypu: **Tak** - wykrywaj **Nie** - nie wykrywaj. Możesz przełączać między „Tak” i „Nie”, klikając te wartości.
Tagi	Wyświetlane są tagi prototypu hosta.

Aby skonfigurować nowy prototyp hosta, kliknij przycisk *Utwórz prototyp hosta* w prawym górnym rogu.

Opcje masowej edycji

Przyciski pod listą oferują kilka opcji masowej edycji:

- *Create enabled* — utwórz te hosty jako *Enabled*
- *Create disabled* — utwórz te hosty jako *Disabled*
- *Delete* — usuń te prototypy hostów

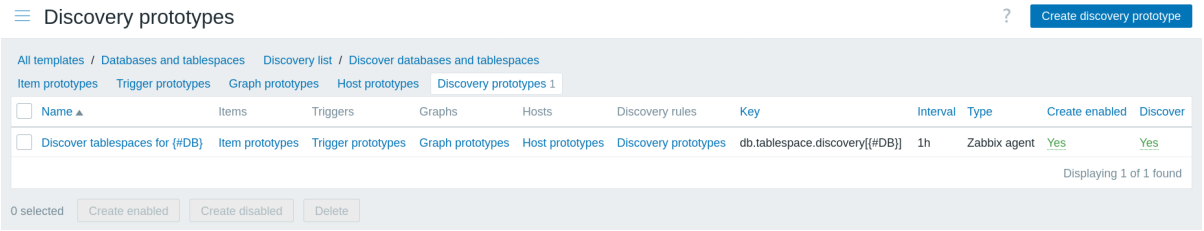
Aby skorzystać z tych opcji, zaznacz pola wyboru przy odpowiednich prototypach hostów, a następnie kliknij wymagany przycisk.

5 Prototypy wykrywania

Przegląd

W tej sekcji wyświetlane są skonfigurowane prototypy wykrywania reguły wykrywania niskiego poziomu w szablonie.

Jeśli szablon jest podłączony do hosta, prototypy wykrywania staną się podstawą do tworzenia rzeczywistych prototypów wykrywania nadrzędnej reguły wykrywania.



Wyświetlane dane:

Column	Description
Name	Nazwa prototypu wykrywania, wyświetlana jako niebieski link. Kliknięcie nazwy otwiera formularz konfiguracji prototypu wykrywania. Jeśli prototyp wykrywania należy do podłączonego szablonu, nazwa szablonu jest wyświetlana przed nazwą prototypu wykrywania jako szary link. Kliknięcie linku szablonu otwiera listę prototypów wykrywania na poziomie podłączonego szablonu.
Items	Wyświetlany jest link do listy prototypów pozycji. Liczba istniejących prototypów pozycji jest wyświetlana na szaro.
Triggers	Wyświetlany jest link do listy prototypów wyzwalaczy. Liczba istniejących prototypów wyzwalaczy jest wyświetlana na szaro.
Graphs	Wyświetlany jest link do listy prototypów wykresów. Liczba istniejących prototypów wykresów jest wyświetlana na szaro.
Hosts	Wyświetlany jest link do listy prototypów hostów. Liczba istniejących prototypów hostów jest wyświetlana na szaro.
Discovery rules	Wyświetlany jest link do listy prototypów wykrywania. Liczba istniejących prototypów wykrywania jest wyświetlana na szaro.
Key	Wyświetlany jest klucz pozycji używany do wykrywania.
Interval	Wyświetlana jest częstotliwość wykonywania wykrywania.
Type	Wyświetlany jest typ pozycji używany do wykrywania (agent Zabbix, agent SNMP itp.).
Create enabled	Wyświetlany jest status tworzenia prototypu wykrywania — tworzenie włączone (*Yes*) lub tworzenie wyłączone (*No*). Klikając status, można go zmienić — z Yes na No (i z powrotem).
Discover	Wyświetlany jest status wykrywania prototypu wykrywania — wykrywaj (*Yes*) lub nie wykrywaj (*No*). Klikając status, można go zmienić — z Yes na No (i z powrotem).

Aby skonfigurować nowy prototyp wykrywania, kliknij przycisk *Create discovery prototype* w prawym górnym rogu.

Opcje masowej edycji

Przyciski pod listą oferują kilka opcji masowej edycji:

- *Utwórz włączone* - utwórz te prototypy wykrywania jako *Włączone*
- *Utwórz wyłączone* - utwórz te prototypy wykrywania jako *Wyłączone*
- *Usuń* - usuń te prototypy wykrywania

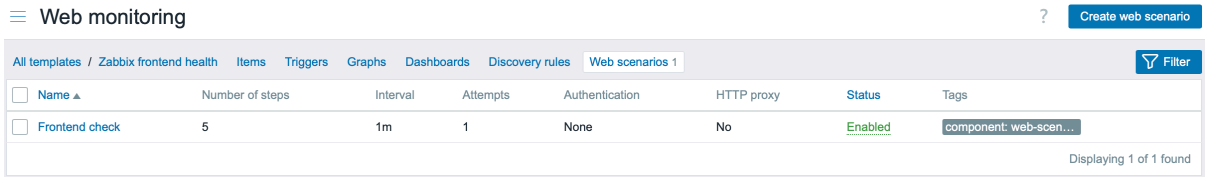
Aby użyć tych opcji, zaznacz pola wyboru przy odpowiednich prototypach wykrywania, a następnie kliknij wymagany przycisk.

5 Scenariusze WWW

Przegląd

Do listy scenariuszy WWW dla szablonu można przejść z poziomu *Data collection* → *Templates*, klikając *Web* przy odpowiednim szablonie.

Zostanie wyświetlona lista istniejących scenariuszy WWW.



Wyświetlane dane:

Kolumna	Opis
Name	Nazwa scenariusza WWW. Kliknięcie nazwy scenariusza WWW otwiera formularz konfiguracji scenariusza WWW. Jeśli scenariusz WWW jest dziedziczony z innego szablonu, nazwa szablonu jest wyświetlana przed nazwą scenariusza WWW jako szare łącze. Kliknięcie łącza szablonu otwiera listę scenariuszy WWW na poziomie tego szablonu.
Number of steps	Liczba kroków zawartych w scenariuszu.
Update interval	Jak często scenariusz jest wykonywany.
Attempts	Ile prób wykonania kroków scenariusza WWW jest podejmowanych.
Authentication	Wyświetlana jest metoda uwierzytelniania — Basic, NTLM, Kerberos, Digest lub None.
HTTP proxy	Wyświetla HTTP proxy lub „No”, jeśli nie jest używany.
Status	Wyświetlany jest status scenariusza WWW — *Enabled* lub *Disabled*. Kliknięcie statusu pozwala go zmienić.
Tags	Wyświetlane są tagi scenariusza WWW. Można wyświetlić maksymalnie trzy tagi (pary nazwa:wartość). Jeśli tagów jest więcej, wyświetlane jest łącze „...”, które po najechaniu kursorem pozwala zobaczyć wszystkie tagi.

Aby skonfigurować nowy scenariusz WWW, kliknij przycisk *Create web scenario* w prawym górnym rogu.

Opcje masowej edycji

Przyciski poniżej listy oferują kilka opcji masowej edycji:

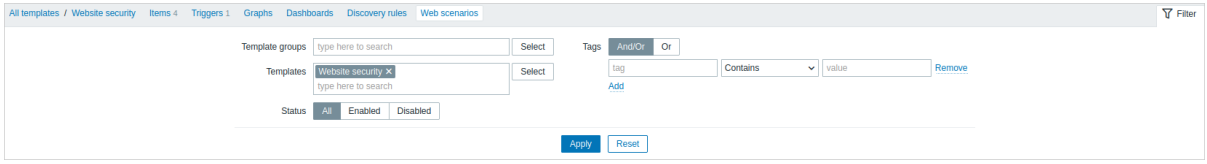
- *Włącz* - zmień status scenariusza na *Włączony*
- *Wyłącz* - zmień status scenariusza na *Wyłączony*
- *Usuń* - usuń scenariusze web

Aby użyć tych opcji, zaznacz pola wyboru przy odpowiednich scenariuszach web, a następnie kliknij wymagany przycisk.

Używanie filtra

Możesz użyć filtra, aby wyświetlić tylko scenariusze, które Cię interesują. Dla lepszej wydajności wyszukiwania dane są przeszukiwane z nierozwiniętymi makrami.

Link *Filtr* jest dostępny nad listą scenariuszy WWW. Po jego kliknięciu pojawi się filtr, za pomocą którego można filtrować scenariusze według grupy szablonów, szablonu, statusu i tagów.

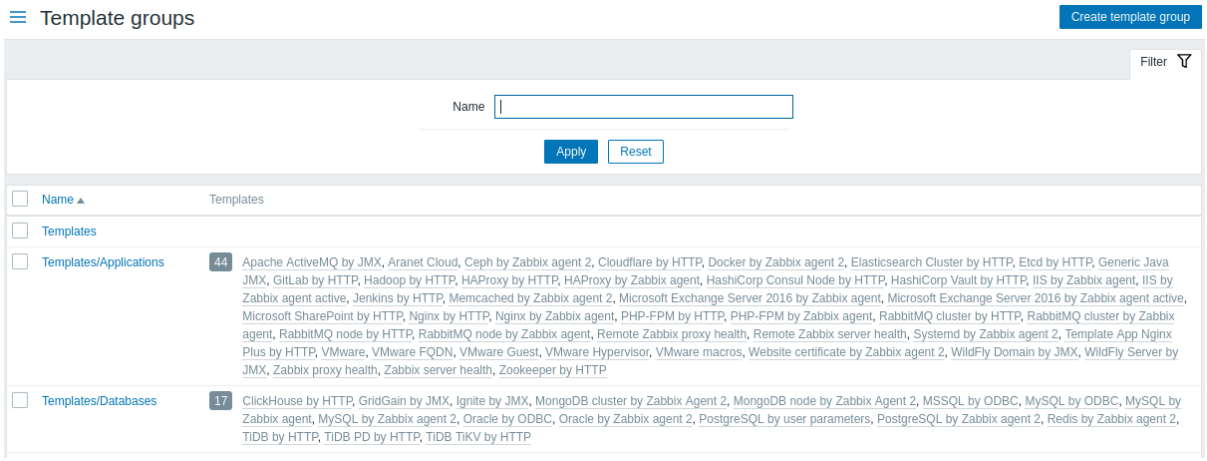


1 Grupy szablonów

Przegląd

W sekcji *Zbieranie danych* → *Grupy szablonów* użytkownicy mogą konfigurować i zarządzać grupami szablonów.

Wyświetlana jest lista istniejących grup szablonów wraz z ich szczegółami. Można wyszukiwać i filtrować grupy szablonów według nazwy.



Wyświetlane dane:

Kolumna	Opis
Nazwa	Nazwa grupy szablonów. Kliknięcie nazwy grupy otwiera formularz konfiguracji grupy.
Szablony	Liczba szablonów w grupie (wyświetlana na szaro), po której następuje lista członków grupy. Kliknięcie nazwy szablonu otwiera formularz konfiguracji szablonu. Kliknięcie liczby otwiera listę szablonów w tej grupie.

Opcje masowej edycji

Aby usunąć jednocześnie kilka grup szablonów, zaznacz pola wyboru przy odpowiednich grupach, a następnie kliknij przycisk Delete poniżej listy.

Używanie filtra

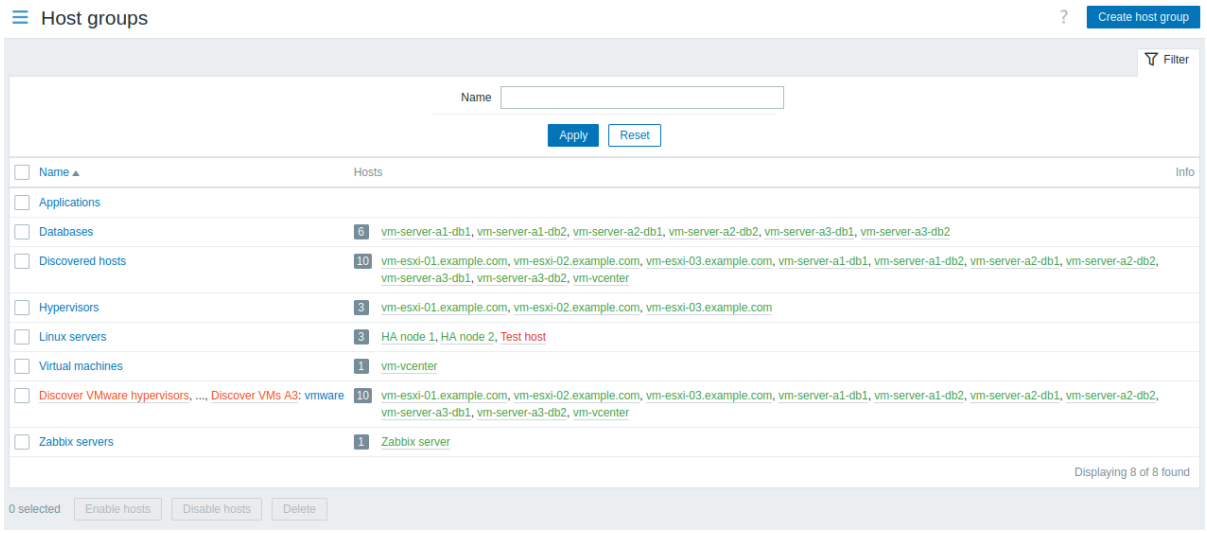
Możesz użyć filtra, aby wyświetlić tylko te grupy szablonów, którymi jesteś zainteresowany. Dla lepszej wydajności wyszukiwania dane są przeszukiwane przy nierozwiniętych makrach.

2 Grupy hostów

Przegląd

W sekcji *Zbieranie danych* → *Grupy hostów* użytkownicy mogą konfigurować i zarządzać grupami hostów.

Wyświetlana jest lista istniejących grup hostów wraz z ich szczegółami. Można wyszukiwać i filtrować grupy hostów według nazwy.



Wyświetlane dane:

Kolumna	Opis
Nazwa	Nazwa grupy hostów. Kliknięcie nazwy grupy otwiera formularz konfiguracji grupy. Wykryte grupy hostów są wyświetlane z nazwami reguł wykrywania niskiego poziomu jako prefiksem. Kliknięcie nazwy reguły LLD otwiera formularz konfiguracji prototypu hosta. Należy pamiętać, że wykryte grupy hostów są usuwane, gdy wszystkie reguły LLD, które je wykryły, zostaną usunięte.
Hosty	Liczba hostów w grupie (wyświetlana na szaro), po której następuje lista członków grupy. Kliknięcie nazwy hosta otworzy formularz konfiguracji hosta. Kliknięcie liczby spowoduje odfiltrowanie na pełnej liście hostów tych, które należą do grupy.
Informacje	Wyświetlane są informacje o błędach (jeśli występują) dotyczące grupy hostów.

Opcje masowej edycji

Przyciski pod listą oferują kilka opcji masowej edycji:

- *Włącz hosty* — zmienia status wszystkich hostów w grupie na „Monitorowany”
- *Wyłącz hosty* — zmienia status wszystkich hostów w grupie na „Niemonitorowany”
- *Usuń* — usuwa grupy hostów

Aby skorzystać z tych opcji, zaznacz pola wyboru przy odpowiednich grupach hostów, a następnie kliknij wymagany przycisk.

Używanie filtra

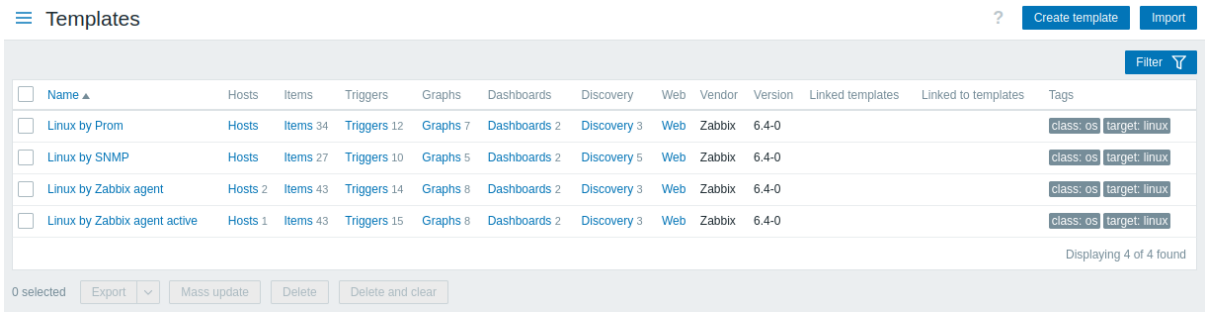
Możesz użyć filtra, aby wyświetlić tylko te grupy hostów, którymi jesteś zainteresowany. Dla lepszej wydajności wyszukiwania dane są przeszukiwane z nierozwiniętymi makrami.

3 Szablony

Przegląd

W sekcji *Data collection* → *Templates* użytkownicy mogą konfigurować i zarządzać szablonami.

Wyświetlana jest lista istniejących szablonów wraz z ich szczegółami.



Wyświetlane dane:

Kolumna	Opis
Name	Nazwa szablonu. Kliknięcie nazwy szablonu otwiera formularz konfiguracji szablonu.
Hosts	Liczba hostów z możliwością edycji, z którymi szablon jest powiązany; hosty tylko do odczytu nie są uwzględniane. Kliknięcie *Hosts* otworzy listę hostów z odfiltrowanymi tylko tymi hostami, które są powiązane z szablonem.
Entities (Items, Triggers, Graphs, Dashboards, Discovery, Web)	Liczba odpowiednich encji w szablonie (wyświetlana na szaro). Kliknięcie nazwy encji spowoduje odfiltrowanie w pełnej liście tej encji tych, które należą do szablonu.
Linked templates	Szablony, które są powiązane z tym szablonem.
Linked to templates	Szablony, z którymi ten szablon jest powiązany.
Vendor, *Version*	Dostawca i wersja szablonu; wyświetlane, jeśli konfiguracja szablonu zawiera takie informacje, i tylko dla gotowych szablonów, zaimportowanych szablonów lub szablonów zmodyfikowanych za pomocą Template API. W przypadku gotowych szablonów wersja jest wyświetlana w następujący sposób: główna wersja Zabbix, separator (”-”), numer rewizji (zwiększany z każdą nową wersją szablonu i resetowany przy każdej głównej wersji Zabbix). Na przykład 7.0-0, 7.0-3, 8.0-0, 8.0-3.
Tags	Tagi szablonu, z nierozwiniętymi makrami.

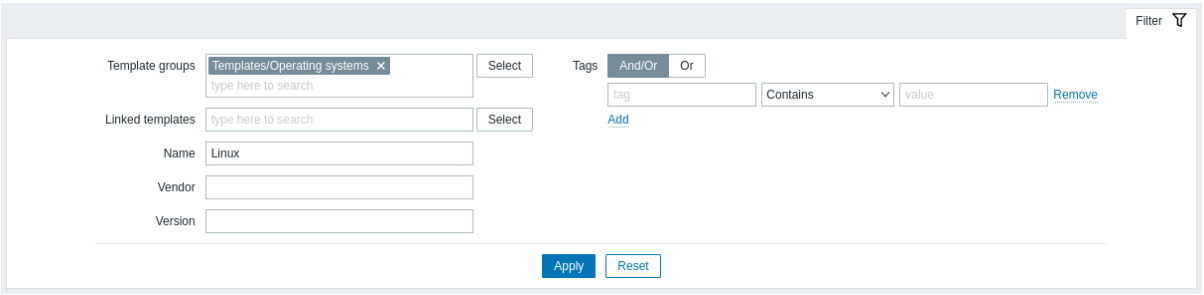
Aby skonfigurować nowy szablon, kliknij przycisk *Create template* w prawym górnym rogu.

Aby zaimportować szablon z pliku YAML, XML lub JSON, kliknij przycisk *Import* w prawym górnym rogu.

Używanie filtra

Możesz użyć filtra, aby wyświetlić tylko te szablony, które Cię interesują. Dla lepszej wydajności wyszukiwania dane są przeszukiwane z nierozwiniętymi makrami.

Łącze *Filtr* jest dostępne poniżej przycisków *Utwórz szablon* i *Importuj*. Po jego kliknięciu dostępny staje się filtr, w którym można filtrować szablony według grup szablonów, podłączonych szablonów, nazwy i tagów.



Parametr	Opis
Grupy szablonów	Filtruj według jednej lub większej liczby grup szablonów. Określenie nadrzędnej grupy szablonów powoduje domyślny wybór wszystkich grup zagnieżdżonych.
Podłączone szablony	Filtruj według bezpośrednio podłączonych szablonów.
Nazwa	Filtruj według nazwy szablonu.
Dostawca	Filtruj według dostawcy szablonu.
Wersja	Filtruj według wersji szablonu.

Parametr	Opis
Tagi	Filtruj według nazwy i wartości tagu szablonu. Filtrowanie jest możliwe tylko według tagów na poziomie szablonu (nie dziedziczonych). Można zarówno uwzględniać, jak i wykluczać określone tagi oraz wartości tagów. Można ustawić kilka warunków. Dopasowanie nazw tagów zawsze uwzględnia wielkość liter. Dla każdego warunku dostępnych jest kilka operatorów: **Istnieje** - uwzględnij określone nazwy tagów; **Równa się** - uwzględnij określone nazwy i wartości tagów (z uwzględnieniem wielkości liter); **Zawiera** - uwzględnij określone nazwy tagów, dla których wartości tagów zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter); **Nie istnieje** - wyklucz określone nazwy tagów; **Nie równa się** - wyklucz określone nazwy i wartości tagów (z uwzględnieniem wielkości liter); **Nie zawiera** - wyklucz określone nazwy tagów, dla których wartości tagów zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter). Dostępne są dwa typy obliczania warunków: **And/Or** - wszystkie warunki muszą być spełnione, warunki mające tę samą nazwę tagu będą grupowane przez warunek Or; **Or** - wystarczy, że jeden warunek zostanie spełniony.

Opcje masowej edycji

Przyciski pod listą oferują kilka opcji masowej edycji:

- *Eksport* — eksport szablonu do pliku YAML, XML lub JSON;
- *Masowa aktualizacja* — zaktualizuj kilka właściwości dla wielu szablonów jednocześnie;
- *Usuń* — usuń szablon, pozostawiając jego powiązane encje (pozycje, wyzwalacze itp.) na hostach;
- *Usuń i wyczyść* — usuń szablon i jego powiązane encje z hostów.

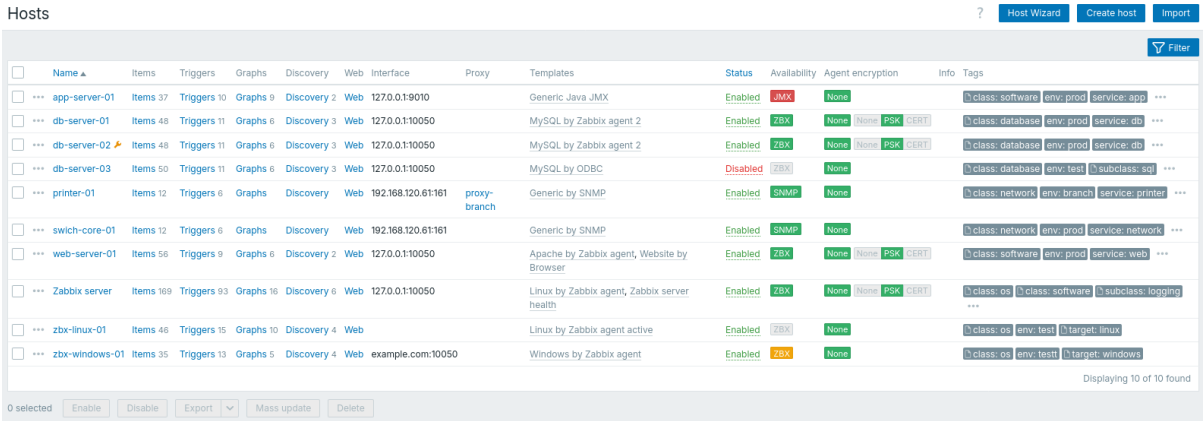
Aby skorzystać z tych opcji, zaznacz pola wyboru przy odpowiednich szablonach, a następnie kliknij wymagany przycisk.

4 Hosty

Przegląd

W sekcji *Zbieranie danych* → *Hosty* użytkownicy mogą konfigurować i utrzymywać hosty.

Wyświetlana jest lista istniejących hostów wraz z ich szczegółami.



Wyświetlane dane:

Kolumna	Opis
Menu hosta	Kliknij ikonę trzech kropek, aby otworzyć menu hosta.
Nazwa	Nazwa hosta. Kliknięcie nazwy hosta otwiera formularz konfiguracji hosta. Pomarańczowa ikona klucza po nazwie hosta wskazuje, że ten host jest w trakcie konserwacji. Szczegóły konserwacji są wyświetlane po najechaniu kursorem myszy na ikonę.

Kolumna	Opis
Encje (Pozycje, Wyzwalacze, Wykresy, Odkrywanie, WWW)	Kliknięcie nazwy encji spowoduje wyświetlenie pozycji, wyzwalaczy itd. hosta. Liczba odpowiednich encji jest wyświetlana na szaro.
Interfejs	Wyświetlany jest główny interfejs hosta.
Proxy	Przypisane proxy są wyświetlane w tej kolumnie: <Nazwa proxy> - host jest monitorowany przez samodzielny proxy (nawet jeśli proxy jest częścią grupy proxy); <Nazwa grupy proxy: nazwa proxy> - host jest monitorowany przez grupę proxy, a serwer Zabbix przypisał proxy do monitorowania hosta; <Nazwa grupy proxy> - host jest monitorowany przez grupę proxy bez żadnych proxy lub jeśli serwer Zabbix nie przypisał proxy do monitorowania hosta; Brak - host nie jest monitorowany ani przez proxy, ani przez grupę proxy. Ta kolumna jest wyświetlana tylko wtedy, gdy opcja filtra *Monitorowany przez* jest ustawiona na „Dowolny”, „Proxy” lub „Grupa proxy”.
Szablony	Wyświetlane są szablony podłączone do hosta. Jeśli podłączony szablon zawiera inne szablony, są one wyświetlane w nawiasach, oddzielone przecinkami. Kliknięcie nazwy szablonu otworzy jego formularz konfiguracji.
Status	Wyświetlany jest status hosta — *Włączony* lub *Wyłączony*. Klikając status, można go zmienić ręcznie. Odnalezione hosty, które zostały utracone, są oznaczone ikoną informacji. Tekst podpowiedzi zawiera szczegóły dotyczące ich statusu.

Kolumna	Opis
Dostępność	Wyświetlana jest dostępność hosta dla każdego skonfigurowanego interfejsu. Ikony dostępności przedstawiają bieżący status interfejsu hosta na serwerze Zabbix. Dlatego jeśli wyłączysz host w frontend, jego dostępność zostanie zaktualizowana po zsynchronizowaniu zmian konfiguracji przez serwer Zabbix. Podobnie, jeśli włączysz host, jego dostępność zostanie zaktualizowana po zsynchronizowaniu zmian konfiguracji przez serwer Zabbix i odpytaniu hosta. Ikony dostępności przedstawiają tylko te typy interfejsów (Agent, SNMP, IPMI, JMX), które są skonfigurowane. Najechanie kursorem na ikonę powoduje wyświetlenie wyskakującego okna z listą wszystkich interfejsów tego samego typu wraz ze szczegółami, statusem i błędami. Dla interfejsu Agent wyskakujące okno wyświetla interfejsy (pasywne) oraz aktywne testy. Jeśli host ma tylko aktywne testy, ikona interfejsu Agent jest wyświetlana nawet wtedy, gdy host nie ma skonfigurowanego interfejsu Agent. Kolumna jest pusta dla hostów bez interfejsów. Status pojedynczego interfejsu hosta jest określany przez połączenie między włączoną pozycją używającą tego interfejsu a hostem. Status może być następujący: **Dostępny** - połączenie z hostem zakończyło się powodzeniem; **Niedostępny** - połączenie z hostem nie powiodło się (przekroczenie czasu, problemy z firewallem itp.); **Nieznany** - nie podjęto próby połączenia z hostem lub wynik jest nieznany. Aby uzyskać dodatkowe informacje o tym, jak serwer Zabbix określa status interfejsu, zobacz Nieznany status interfejsu oraz Ustawienia nieosiągalnego/niedostępnego interfejsu hosta. Status wszystkich interfejsów hosta jednego typu (Agent, SNMP, IPMI, JMX) jest określany przez te interfejsy, które są używane przez co najmniej jedną włączoną pozycję. Status jest wskazywany kolorem ikony: **Zielony** - wszystkie interfejsy są dostępne; **Żółty** - co najmniej jeden interfejs jest niedostępny, a co najmniej jeden jest dostępny lub nieznany; **Czerwony** - wszystkie interfejsy są niedostępne; **Szary** - co najmniej jeden interfejs jest nieznany, ale żaden nie jest niedostępny. **Dostępność aktywnych testów.** Jeśli na hoście jest włączony co najmniej jeden aktywny test, aktywne testy również wpływają na całkowitą dostępność interfejsu Agent, jak opisano powyżej. Aby określić dostępność aktywnych testów, komunikaty heartbeat są wysyłane w wątku aktywnych testów agenta. Częstotliwość komunikatów heartbeat jest kontrolowana przez parametr `HeartbeatFrequency` w konfiguracji Zabbix agent lub agent 2 (domyślnie 60 sekund, zakres 0-3600). Aktywne testy są uznawane za niedostępne, gdy heartbeat aktywnych testów jest starszy niż 2 x HeartbeatFrequency sekund. **Uwaga:** Agenty Zabbix starsze niż wersja 6.2.x nie wysyłają heartbeatów aktywnych testów, więc dostępność ich hostów pozostaje nieznana.
Szyfrowanie agenta	Wyświetlany jest status szyfrowania dla połączeń do hosta i z hosta: **Brak** - brak szyfrowania; **PSK** - użycie klucza współdzielonego; **Cert** - użycie certyfikatu.
Informacje	Wyświetlane są informacje o błędach dotyczących hosta (jeśli występują).
Tagi	Tagi hosta z nierozwiniętymi makrami.

Aby skonfigurować nowy host, kliknij przycisk *Host Wizard* lub *Utwórz host* w prawym górnym rogu. Aby zaimportować host z pliku YAML, XML lub JSON, kliknij przycisk *Importuj* w prawym górnym rogu.

Opcje masowej edycji

Przyciski poniżej listy oferują kilka opcji masowej edycji:

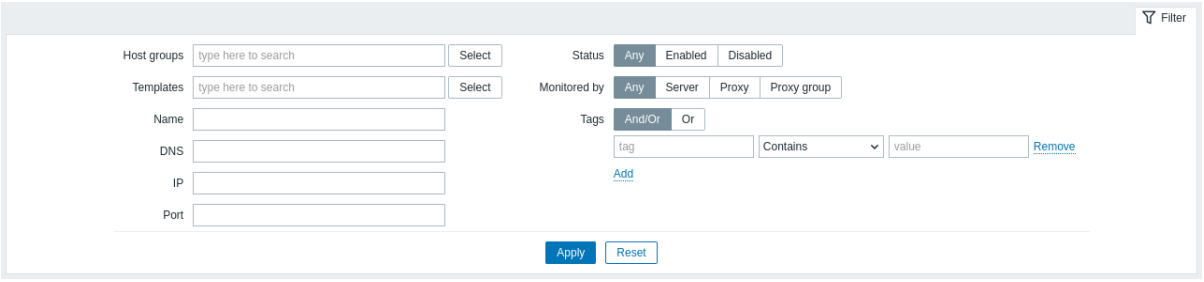
- *Włącz* — zmień status hosta na *Monitorowany*;
- *Wyłącz* — zmień status hosta na *Niemonitorowany*;
- *Eksportuj* — wyeksportuj hosty do pliku YAML, XML lub JSON;
- *Masowa aktualizacja* — zaktualizuj kilka właściwości dla wielu hostów jednocześnie;
- *Usuń* — usuń hosty.

Aby użyć tych opcji, zaznacz pola wyboru przy odpowiednich hostach, a następnie kliknij wymagany przycisk.

Używanie filtra

Możesz użyć filtra, aby wyświetlić tylko hosty, które Cię interesują. Dla lepszej wydajności wyszukiwania dane są przeszukiwane z nierozwiniętymi makrami.

Ikona *Filtr* jest dostępna w prawym górnym rogu. Kliknięcie jej otworzy filtr, w którym można określić żądane kryteria filtrowania.



Parametr	Opis
Grupy hostów	Filtruj według jednej lub większej liczby grup hostów. Określenie nadrzędnej grupy hostów powoduje domyślnie wybranie wszystkich zagnieżdżonych grup hostów.
Szablony	Filtruj według podłączonych szablonów.
Nazwa	Filtruj według widocznej nazwy hosta.
DNS	Filtruj według nazwy DNS.
IP	Filtruj według adresu IP.
Port	Filtruj według numeru portu.
Status	Filtruj według statusu hosta.
Monitorowane przez	Filtruj hosty monitorowane przez serwer Zabbix, proxy lub grupę proxy.
Proxy	Filtruj hosty monitorowane przez określone tutaj proxy. To pole jest dostępne tylko wtedy, gdy w polu *Monitorowane przez* wybrano „Proxy”.
Grupy proxy	Filtruj hosty monitorowane przez określone tutaj grupy proxy. To pole jest dostępne tylko wtedy, gdy w polu *Monitorowane przez* wybrano „Grupa proxy”.
Tagi	Filtruj według nazwy i wartości tagu hosta. Możliwe jest zarówno uwzględnianie, jak i wykluczanie określonych tagów i wartości tagów. Można ustawić kilka warunków. Dopasowanie nazwy tagu zawsze uwzględnia wielkość liter. Dla każdego warunku dostępnych jest kilka operatorów: **Istnieje** — uwzględnij określone nazwy tagów; **Równa się** — uwzględnij określone nazwy i wartości tagów (z uwzględnieniem wielkości liter); **Zawiera** — uwzględnij określone nazwy tagów, których wartości zawierają wprowadzony ciąg znaków (dopasowanie podciągu, bez uwzględniania wielkości liter); **Nie istnieje** — wyklucz określone nazwy tagów; **Nie równa się** — wyklucz określone nazwy i wartości tagów (z uwzględnieniem wielkości liter); **Nie zawiera** — wyklucz określone nazwy tagów, których wartości zawierają wprowadzony ciąg znaków (dopasowanie podciągu, bez uwzględniania wielkości liter). Dostępne są dwa typy obliczania warunków: **And/Or** — wszystkie warunki muszą być spełnione, a warunki mające tę samą nazwę tagu będą grupowane operatorem Or; **Or** — wystarczy spełnienie jednego warunku.

Nieznany status interfejsu

Serwer Zabbix wyświetla status „Unknown” dla interfejsu hosta (Agent, SNMP, IPMI, JMX) w następujących przypadkach:

- Host jest wyłączony.
- Host jest ustawiony do monitorowania przez proxy, inny proxy lub serwer, jeśli wcześniej był monitorowany przez proxy.
- Host jest monitorowany przez proxy, który wydaje się być offline (nie otrzymano żadnych aktualizacji z proxy podczas maksymalnego interwału heartbeat — 1 godzina).
- Wszystkie pozycje hosta z tym typem interfejsu są wyłączone.
- Nie skonfigurowano żadnych pollerów dla tego typu interfejsu (na przykład parametr konfiguracji serwera `StartAgentPollers` lub `StartSNMPPollers` jest ustawiony na 0).

Dostępność interfejsu jest ustawiana na „Unknown” po synchronizacji pamięci podręcznej konfiguracji serwera Zabbix.

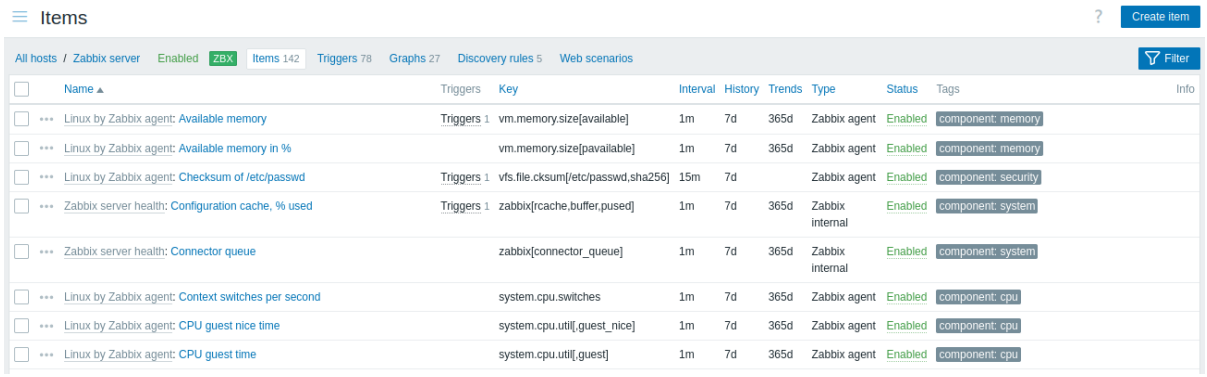
Dostępność interfejsu (Available/Not available) na hostach monitorowanych przez proxy jest przywracana po synchronizacji pamięci podręcznej konfiguracji proxy.

1 Pozycje

Przegląd

Lista pozycji dla hosta jest dostępna w *Zbieranie danych* → *Hosty* po kliknięciu *Pozycje* dla odpowiedniego hosta.

Zostanie wyświetlona lista istniejących pozycji.



Wyświetlane dane:

Kolumna	Opis
Menu pozycji	Kliknij ikonę z trzema kropkami, aby otworzyć menu pozycji.
Host	Host pozycji. Kliknięcie nazwy hosta otwiera formularz konfiguracji hosta. Ta kolumna jest wyświetlana tylko wtedy, gdy w filtrze wybrano wiele hostów lub nie wybrano żadnego hosta.
Nazwa	Nazwa pozycji jest wyświetlana jako niebieski link do szczegółów pozycji. Kliknięcie linku z nazwą pozycji otwiera formularz konfiguracji pozycji. Jeśli pozycja hosta należy do szablonu, nazwa szablonu jest wyświetlana przed nazwą pozycji jako szary link. Kliknięcie linku szablonu otworzy listę pozycji na poziomie szablonu. Jeśli pozycja została utworzona z prototypu pozycji, jej nazwa jest poprzedzona nazwą reguły wykrywania niskiego poziomu, wyświetlaną na pomarańczowo. Kliknięcie nazwy reguły wykrywania otworzy listę prototypów pozycji.
Wyzwalacze	Po najechaniu kursorem na Wyzwalacze zostanie wyświetlone okno informacyjne pokazujące wyzwalacze powiązane z pozycją. Liczba wyzwalaczy jest wyświetlana na szaro.
Klucz	Wyświetlany jest klucz pozycji.
Interwał	Wyświetlana jest częstotliwość sprawdzania. *Uwaga:* pozycje pasywne mogą być również sprawdzane natychmiast po naciśnięciu przycisku *Wykonaj teraz* button.
Historia	Wyświetlana jest liczba dni, przez które będzie przechowywana historia danych pozycji.
Trendy	Wyświetlana jest liczba dni, przez które będzie przechowywana historia trendów pozycji.
Typ	Wyświetlany jest typ pozycji (agent Zabbix, agent SNMP, proste sprawdzenie itp.).
Status	Wyświetlany jest status pozycji — *Włączona*, *Wyłączona* lub *Nieobsługiwana*. Status można zmienić ręcznie, klikając go — z Włączona na Wyłączona (i z powrotem); z Nieobsługiwana na Wyłączona (i z powrotem). Wykryte pozycje, które zostały utracone, są oznaczone ikoną informacji. Tekst podpowiedzi zawiera szczegóły dotyczące ich statusu.
Tagi	Wyświetlane są tagi pozycji. Można wyświetlić maksymalnie trzy tagi (pary nazwa:wartość). Jeśli tagów jest więcej, wyświetlany jest link „...”, który po najechaniu kursorem pozwala zobaczyć wszystkie tagi.
Informacje	Jeśli pozycja działa poprawnie, w tej kolumnie nie jest wyświetlana żadna ikona. W przypadku błędów wyświetlana jest kwadratowa ikona z literą „i”. Najedź kursorem na ikonę, aby zobaczyć podpowiedź z opisem błędu.

Aby skonfigurować nową pozycję, kliknij przycisk *Utwórz pozycję* w prawym górnym rogu.

Opcje masowej edycji

Przyciski pod listą oferują kilka opcji masowej edycji:

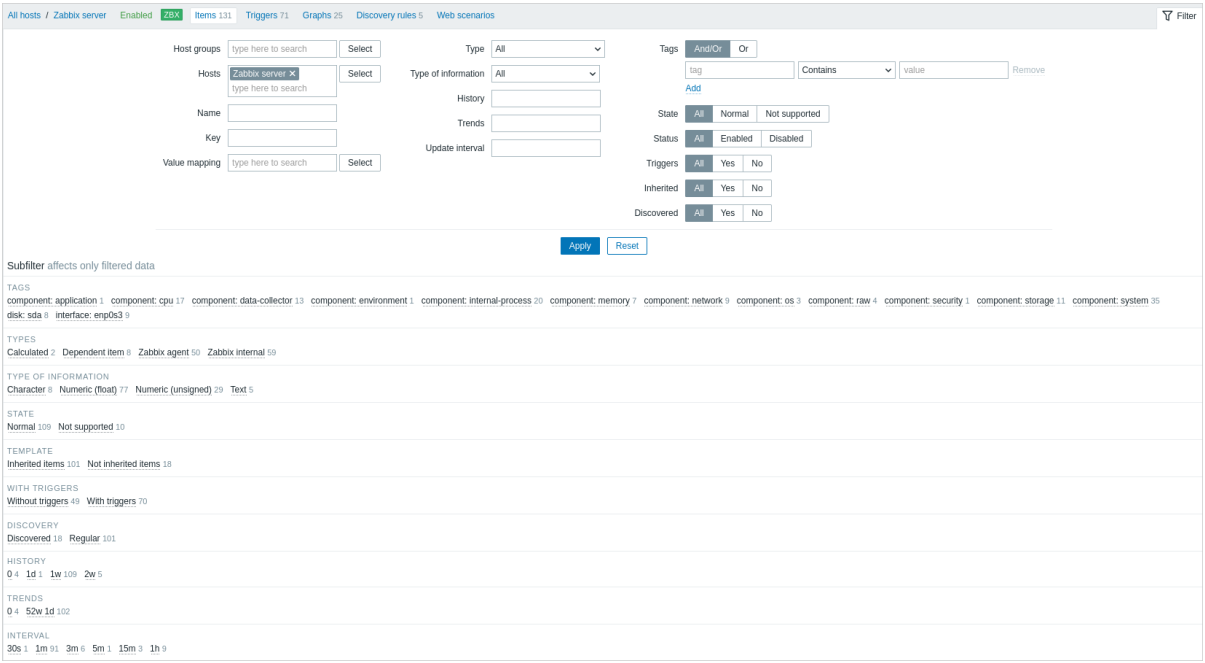
- *Włącz* - zmień status pozycji na *Włączony*
- *Wyłącz* - zmień status pozycji na *Wyłączony*
- *Wykonaj teraz* - natychmiast wykonaj sprawdzenie nowych wartości pozycji. Obsługiwane tylko dla sprawdzeń **pasywnych** (zobacz więcej szczegółów). Należy pamiętać, że podczas natychmiastowego sprawdzania wartości pamięć podręczna konfiguracji nie jest aktualizowana, dlatego wartości nie będą odzwierciedlać bardzo niedawnych zmian w konfiguracji pozycji.
- *Wyczyść historię i trendy* - usuń dane historii i trendów dla pozycji.
- *Kopiuj* - skopiuj pozycje do innych hostów lub szablonów.
- *Masowa aktualizacja* - zaktualizuj kilka właściwości dla wielu pozycji jednocześnie.
- *Usuń* - usuń pozycje.

Aby użyć tych opcji, zaznacz pola wyboru przy odpowiednich pozycjach, a następnie kliknij wymagany przycisk.

Korzystanie z filtra

Możesz użyć filtra, aby wyświetlić tylko te pozycje, które Cię interesują. Dla lepszej wydajności wyszukiwania dane są przeszukiwane z nierozwiniętymi makrami.

Ikona *Filtr* jest dostępna w prawym górnym rogu. Kliknięcie jej otworzy filtr, w którym można określić żądane kryteria filtrowania.



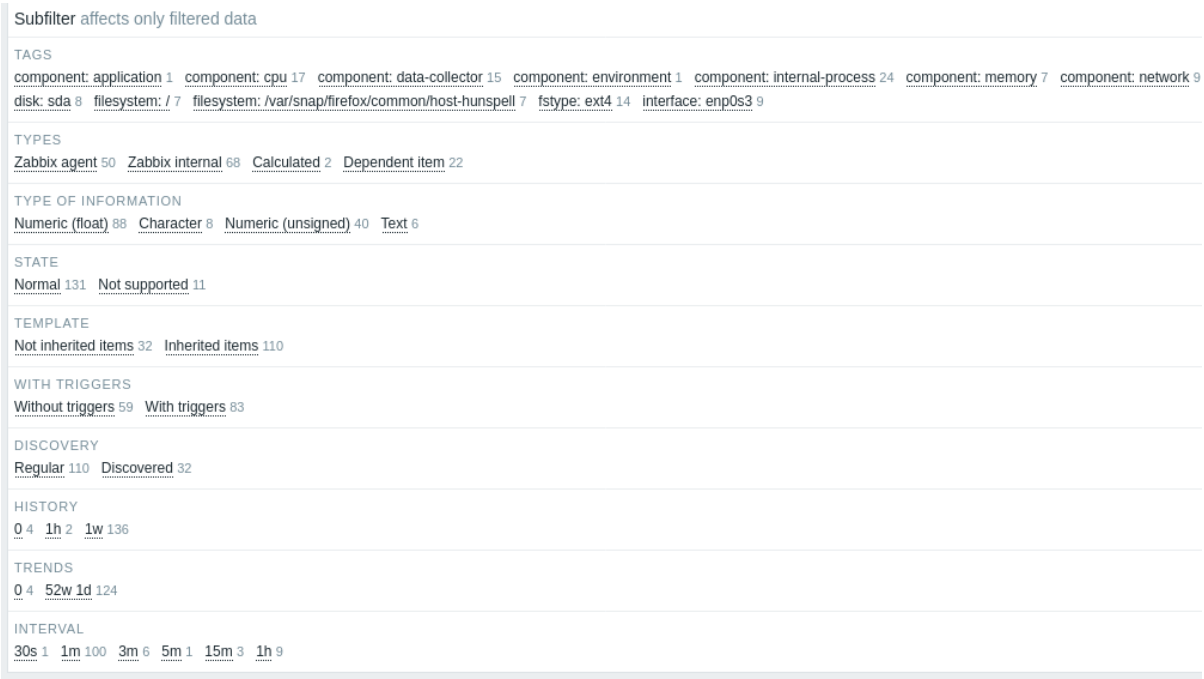
Parametr	Opis
Grupy hostów	Filtruj według jednej lub większej liczby grup hostów. Określenie nadrzędnej grupy hostów powoduje automatyczne wybranie wszystkich zagnieżdżonych grup hostów. Nie można wybrać grup hostów zawierających wyłącznie szablony.
Hosty	Filtruj według jednego lub większej liczby hostów.
Nazwa	Filtruj według nazwy pozycji.
Klucz	Filtruj według klucza pozycji.
Mapowanie wartości	Filtruj według używanej mapy wartości. Ten parametr nie jest wyświetlany, jeśli opcja *Hosty* jest pusta.
Typ	Filtruj według typu pozycji (agent Zabbix, agent SNMP itp.).
Typ informacji	Filtruj według typu informacji (bezznakowa wartość liczbowa, liczba zmiennoprzecinkowa itp.).
Historia	Filtruj według czasu przechowywania historii pozycji.
Trendy	Filtruj według czasu przechowywania trendów pozycji.
Interwał aktualizacji	Filtruj według interwału aktualizacji pozycji.

Parametr	Opis
Tagi	Określ tagi, aby ograniczyć liczbę wyświetlanych pozycji. Możliwe jest zarówno uwzględnianie, jak i wykluczanie określonych tagów oraz wartości tagów. Można ustawić kilka warunków. Dopasowanie nazw tagów zawsze uwzględnia wielkość liter. Dla każdego warunku dostępnych jest kilka operatorów: **Istnieje** - uwzględnij określone nazwy tagów **Równa się** - uwzględnij określone nazwy i wartości tagów (z uwzględnieniem wielkości liter) **Zawiera** - uwzględnij określone nazwy tagów, których wartości zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter) **Nie istnieje** - wyklucz określone nazwy tagów **Nie równa się** - wyklucz określone nazwy i wartości tagów (z uwzględnieniem wielkości liter) **Nie zawiera** - wyklucz określone nazwy tagów, których wartości zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter) Dostępne są dwa typy obliczania warunków: **And/Or** - wszystkie warunki muszą być spełnione, a warunki mające tę samą nazwę tagu będą grupowane operatorem Or **Or** - wystarczy spełnienie jednego warunku
Stan	Filtruj według stanu pozycji — *Normalny* lub *Nieobsługiwany*.
Status	Filtruj według statusu pozycji — *Włączony* lub *Wyłączony*.
Wyzwalacze	Filtruj pozycje z wyzwalaczami (lub bez nich).
Dziedziczone	Filtruj pozycje dziedziczone (lub niedziedziczone) z szablonu.
Odkrywanie	Filtruj pozycje wykryte (lub niewykryte) przez wykrywanie niskiego poziomu.

Używanie podfiltra

Podfiltr pozwala dalej modyfikować filtrowanie z filtra głównego.

Zawiera klikalne odnośniki umożliwiające szybki dostęp do powiązanych pozycji. Pozycje są powiązane wspólną jednostką, taką jak tag, typ pozycji, stan pozycji, interwał aktualizacji pozycji itp. Po kliknięciu jednostki zostaje ona wyróżniona szarym tłem, a pozycje są natychmiast filtrowane (bez potrzeby klikania *Zastosuj* w filtrze głównym). Kliknięcie innej jednostki dodaje ją do filtrowanych wyników. Ponowne kliknięcie jednostki usuwa filtrowanie.



Podfiltry są generowane na podstawie przefiltrowanych danych, których liczba jest ograniczona do 1000 rekordów. Jeśli chcesz zobaczyć więcej rekordów w podfiltrze, musisz zwiększyć wartość parametru *Limit for search and filter results* (w *Administracja -> Ogólne -> GUI*).

W przeciwieństwie do filtra głównego, podfiltr jest aktualizowany przy każdym żądaniu odświeżenia tabeli, aby zawsze zawierał aktualne informacje o dostępnych opcjach filtrowania i licznikach.

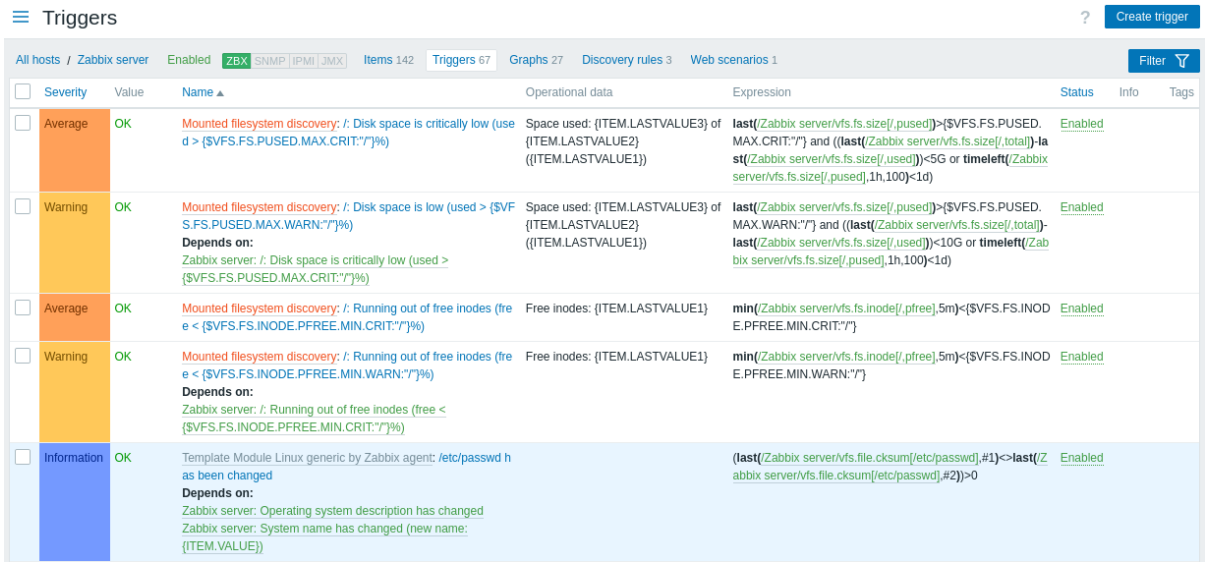
Liczba wyświetlanych jednostek jest ograniczona poziomo do 100. Jeśli jest ich więcej, na końcu wyświetlana jest ikona trzech kropek; nie można jej kliknąć.

Liczba obok każdej klikalnej jednostki wskazuje liczbę pozycji w niej zgrupowanych (na podstawie wyników filtra głównego). Po kliknięciu jednostki liczby przy innych dostępnych jednostkach są wyświetlane ze znakiem plus, wskazującym, ile pozycji można dodać do bieżącego wyboru. Jednostki bez pozycji nie są wyświetlane, chyba że zostały wcześniej wybrane w podfiltrze.

2 Wyzwalacze

Przegląd

Lista wyzwalaczy dla hosta jest dostępna z poziomu *Zbieranie danych* → *Hosty*, po kliknięciu *Wyzwalacze* dla odpowiedniego hosta.



Wyświetlane dane:

Column	Description
Severity	Poziom ważności wyzwalacza jest wyświetlany zarówno nazwą, jak i kolorem tła komórki.
Value	Stan wyzwalacza jest wyświetlany jako: **OK** - stan OK **PROBLEM** - stan problemu
Host	Host wyzwalacza. Kliknięcie nazwy hosta otwiera formularz konfiguracji hosta. Ta kolumna jest wyświetlana tylko wtedy, gdy w filtrze wybrano wiele hostów lub nie wybrano żadnego hosta.
Name	Nazwa wyzwalacza, wyświetlana jako niebieski link do szczegółów wyzwalacza. Kliknięcie linku z nazwą wyzwalacza otwiera formularz konfiguracji wyzwalacza. Jeśli wyzwalacz hosta należy do szablonu, nazwa szablonu jest wyświetlana przed nazwą wyzwalacza jako szary link. Kliknięcie linku szablonu otworzy listę wyzwalaczy na poziomie szablonu. Jeśli wyzwalacz został utworzony z prototypu wyzwalacza, jego nazwa jest poprzedzona nazwą reguły wykrywania niskiego poziomu, wyświetlaną na pomarańczowo. Kliknięcie nazwy reguły wykrywania otwiera listę prototypów wyzwalaczy.
Operational data	Definicja danych operacyjnych wyzwalacza, zawierająca dowolne ciągi znaków i makra, które będą dynamicznie rozwijane w *Monitorowanie* → *Problemy*.
Expression	Wyświetlane jest wyrażenie wyzwalacza. Część host-pozycja tego wyrażenia jest wyświetlana jako link prowadzący do formularza konfiguracji pozycji.
Status	Wyświetlany jest status wyzwalacza — *Włączony*, *Wyłączony* lub *Nieznany*. Klikając status, można go ręcznie zmienić — z Włączony na Wyłączony (i z powrotem) oraz z Nieznany na Wyłączony (i z powrotem). Problemy wyłączonego wyzwalacza nie są już wyświetlane we frontend, ale nie są usuwane. Odnalezione wyzwalacze, które zostały utracone, są oznaczone ikoną informacji. Tekst podpowiedzi zawiera szczegóły dotyczące ich statusu.
Info	Jeśli wszystko działa poprawnie, w tej kolumnie nie jest wyświetlana żadna ikona. W przypadku błędów wyświetlana jest kwadratowa ikona z literą „i”. Najedź kursorem na ikonę, aby zobaczyć podpowiedź z opisem błędu.
Tags	Jeśli wyzwalacz zawiera tagi, w tej kolumnie wyświetlane są nazwa i wartość tagu.

Aby skonfigurować nowy wyzwalacz, kliknij przycisk *Utwórz wyzwalacz* w prawym górnym rogu.

Opcje masowej edycji

Przyciski poniżej listy oferują kilka opcji masowej edycji:

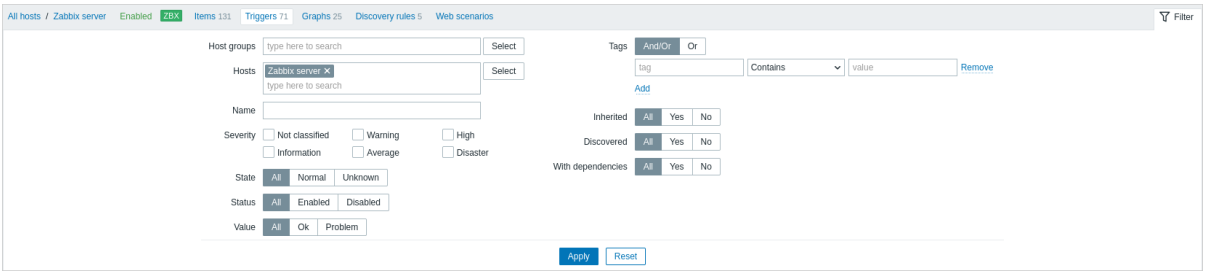
- *Włącz* - zmień status wyzwalacza na *Włączony*.
- *Wyłącz* - zmień status wyzwalacza na *Wyłączony*.
- *Kopiuj* - skopiuj wyzwalacze do innych hostów lub szablonów.
- *Masowa aktualizacja* - zaktualizuj jednocześnie kilka właściwości dla wielu wyzwalaczy.
- *Usuń* - usuń wyzwalacze.

Aby użyć tych opcji, zaznacz pola wyboru przy odpowiednich wyzwalaczach, a następnie kliknij wymagany przycisk.

Używanie filtra

Możesz użyć filtra, aby wyświetlić tylko te wyzwalacze, które Cię interesują. Dla lepszej wydajności wyszukiwania dane są przeszukiwane z nierozwiniętymi makrami.

Ikona *Filtr* jest dostępna w prawym górnym rogu. Kliknięcie jej otworzy filtr, w którym można określić żądane kryteria filtrowania.



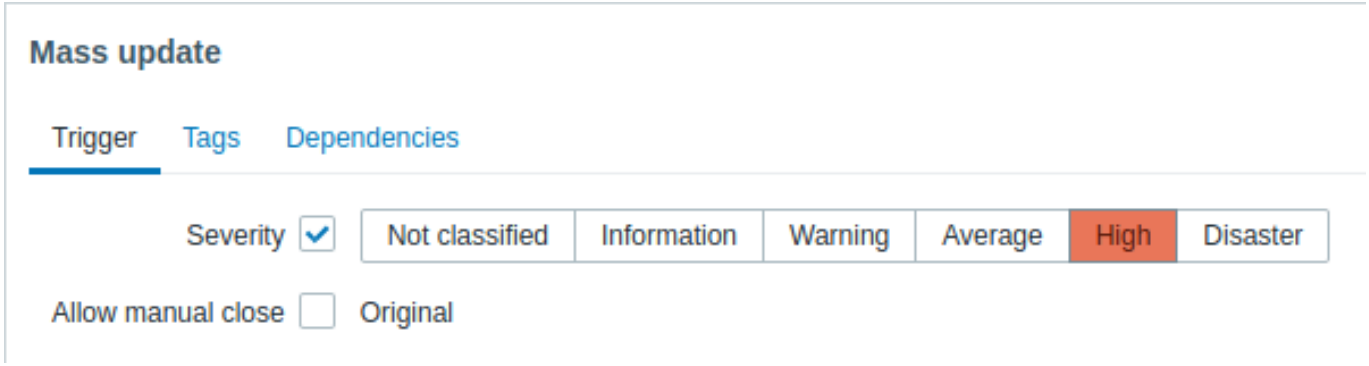
Parametr	Opis
Grupy hostów	Filtruj według jednej lub wielu grup hostów. Określenie nadrzędnej grupy hostów powoduje domyślny wybór wszystkich zagnieżdżonych grup hostów. Nie można wybrać grup hostów zawierających wyłącznie szablony.
Hosty	Filtruj według jednego lub wielu hostów. Jeśli powyżej wybrano już grupy hostów, wybór hostów jest ograniczony do tych grup.
Nazwa	Filtruj według nazwy wyzwalacza.
Ważność	Wybierz, aby filtrować według jednego lub kilku poziomów ważności wyzwalacza.
Stan	Filtruj według stanu wyrażenia wyzwalacza (Normalny/Nieznany).
Status	Filtruj według statusu aktywacji wyzwalacza (Włączony/Wyłączony).
Wartość	Filtruj według wartości wyzwalacza.
Tagi	Filtruj według nazwy i wartości tagu wyzwalacza. Możliwe jest zarówno uwzględnianie, jak i wykluczanie określonych tagów oraz wartości tagów. Można ustawić kilka warunków. Dopasowanie nazwy tagu zawsze uwzględnia wielkość liter. Dla każdego warunku dostępnych jest kilka operatorów: **Istnieje** - uwzględnij określone nazwy tagów **Równa się** - uwzględnij określone nazwy i wartości tagów (z uwzględnieniem wielkości liter) **Zawiera** - uwzględnij określone nazwy tagów, których wartości zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter) **Nie istnieje** - wyklucz określone nazwy tagów **Nie równa się** - wyklucz określone nazwy i wartości tagów (z uwzględnieniem wielkości liter) **Nie zawiera** - wyklucz określone nazwy tagów, których wartości zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter) Dostępne są dwa typy obliczania warunków: **And/Or** - wszystkie warunki muszą być spełnione, warunki mające tę samą nazwę tagu będą grupowane przez warunek Or **Or** - wystarczy, że jeden warunek zostanie spełniony Makra i funkcje makr są obsługiwane zarówno w polach nazwy tagu, jak i wartości tagu.
Dziedziczone	Filtruj wyzwalacze dziedziczone z szablonu (lub niedziedziczone).
Odkryte	Filtruj wyzwalacze odkryte przez wykrywanie niskiego poziomu (lub nieodkryte).
Z zależnościami	Filtruj wyzwalacze z zależnościami (lub bez zależności).

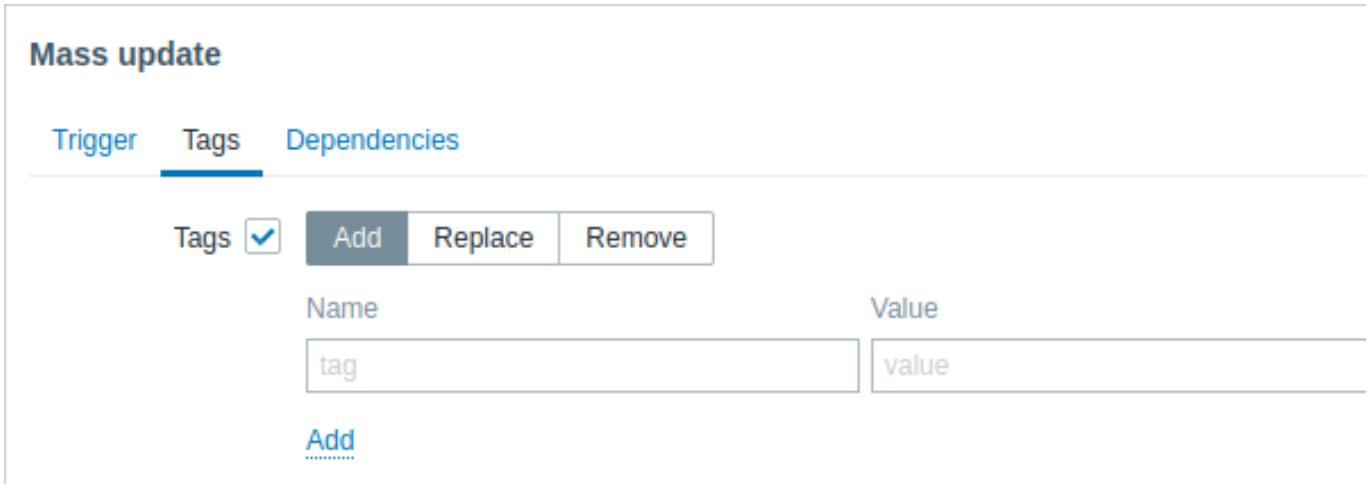
Używanie aktualizacji masowej

Za pomocą aktualizacji masowej możesz zmienić wybrany atrybut dla wielu wyzwalaczy jednocześnie, bez konieczności otwierania każdego wyzwalacza osobno do edycji.

Aby masowo zaktualizować wyzwalacze, wykonaj następujące czynności:

- Zaznacz pola wyboru wyzwalaczy, które chcesz zaktualizować na liście
- Kliknij *Mass update* pod listą
- Przejdź do karty z wymaganymi atrybutami (*Trigger*, *Tags* lub *Dependencies*)
- Zaznacz pola wyboru atrybutów, które chcesz zaktualizować

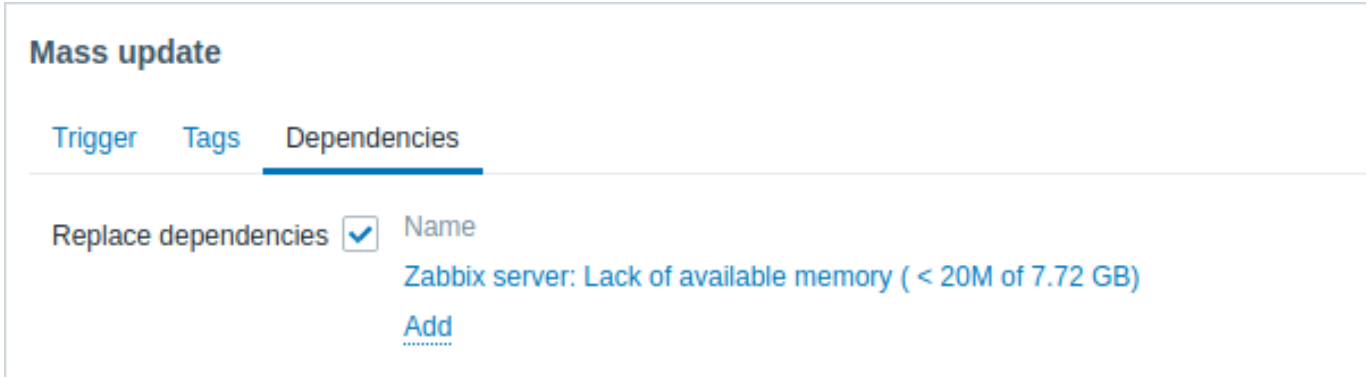




Po wybraniu odpowiedniego przycisku aktualizacji tagów dostępne są następujące opcje:

- *Add* - umożliwia dodanie nowych tagów do wyzwalaczy;
- *Replace* - usunie wszystkie istniejące tagi z wyzwalacza i zastąpi je tagiem lub tagami określonymi poniżej;
- *Remove* - usunie określone tagi z wyzwalaczy.

Pamiętaj, że tagi o tej samej nazwie, ale różnych wartościach, nie są traktowane jako „duplikaty” i mogą zostać dodane do tego samego wyzwalacza.



Replace dependencies - usunie wszystkie istniejące zależności z wyzwalacza i zastąpi je określonymi zależnościami.

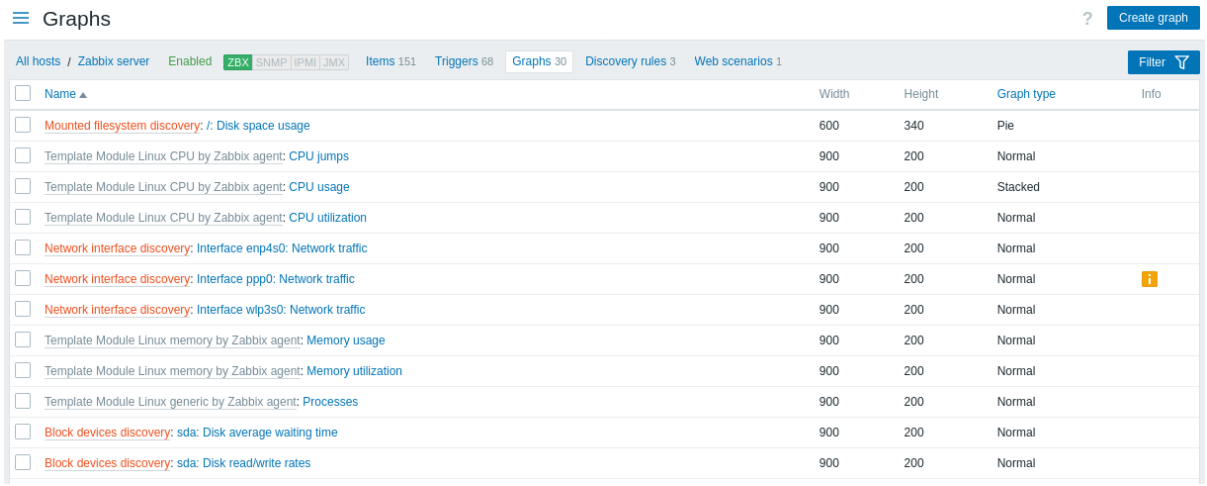
Kliknij *Update*, aby zastosować zmiany.

3 Wykresy

Przegląd

Do listy niestandardowych wykresów dla hosta można przejść z poziomu *Zbieranie danych* → *Hosts*, klikając *Graphs* przy odpowiednim hoście.

Wyświetlana jest lista istniejących wykresów.



Wyświetlane dane:

Kolumna	Opis
Host	Host wykresu. Kliknięcie nazwy hosta otwiera formularz konfiguracji hosta. Ta kolumna jest wyświetlana tylko wtedy, gdy w filtrze wybrano wiele hostów lub nie wybrano żadnego hosta.
Name	Nazwa niestandardowego wykresu, wyświetlana jako niebieski link do szczegółów wykresu. Kliknięcie linku z nazwą wykresu otwiera formularz konfiguracji wykresu. Jeśli wykres hosta należy do szablonu, nazwa szablonu jest wyświetlana przed nazwą wykresu jako szary link. Kliknięcie linku szablonu otworzy listę wykresów na poziomie szablonu. Jeśli wykres został utworzony z prototypu wykresu, jego nazwę poprzedza nazwa reguły wykrywania niskiego poziomu, wyświetlana na pomarańczowo. Kliknięcie nazwy reguły wykrywania otwiera listę prototypów wykresów.
Width	Wyświetlana jest szerokość wykresu.
Height	Wyświetlana jest wysokość wykresu.
Graph type	Wyświetlany jest typ wykresu — *Normal*, *Stacked*, *Pie* lub *Exploded*.
Info	Jeśli wykres działa poprawnie, w tej kolumnie nie jest wyświetlana żadna ikona. W przypadku błędów wyświetlana jest kwadratowa ikona z literą „i”. Najedź kursorem na ikonę, aby zobaczyć podpowiedź z opisem błędu.

Aby skonfigurować nowy wykres, kliknij przycisk *Create graph* w prawym górnym rogu.

Opcje masowej edycji

Przyciski poniżej listy oferują kilka opcji masowej edycji:

- *Kopiuj* — kopiowanie wykresów do innych hostów lub szablonów
- *Usuń* — usuwanie wykresów

Aby skorzystać z tych opcji, zaznacz pola wyboru przy odpowiednich wykresach, a następnie kliknij wymagany przycisk.

Używanie filtra

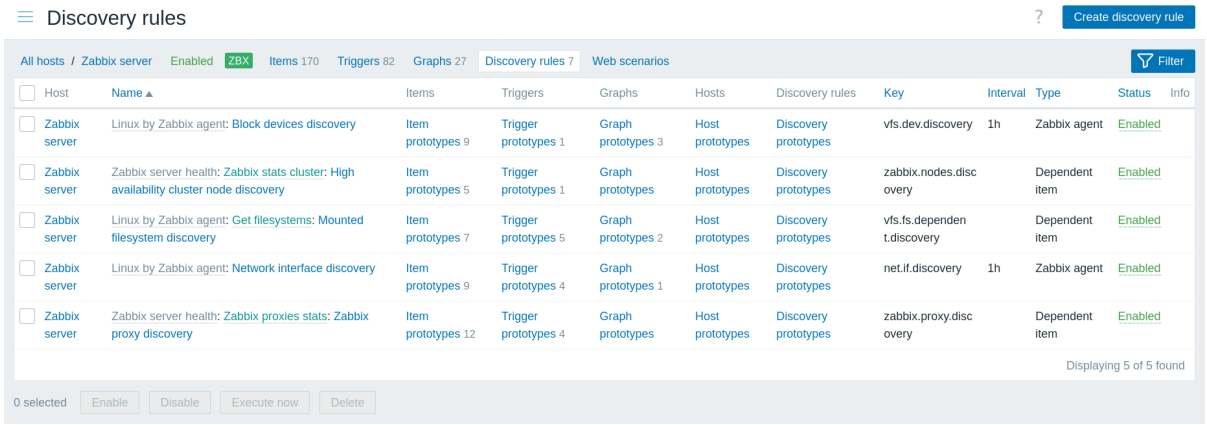
Możesz filtrować wykresy według grupy hostów i hosta. Aby uzyskać lepszą wydajność wyszukiwania, dane są przeszukiwane z nierozwiązanymi makrami.

4 Reguły wykrywania

Przegląd

Lista reguł wykrywania niskiego poziomu dla hosta jest dostępna w *Zbieranie danych* → *Hosty* po kliknięciu *Wykrywanie* dla odpowiedniego hosta.

Wyświetlana jest lista istniejących reguł wykrywania niskiego poziomu. Możliwe jest również wyświetlenie wszystkich reguł wykrywania niezależnie od hosta lub wszystkich reguł wykrywania dla określonej grupy hostów poprzez zmianę ustawień filtra.



Wyświetlane dane:

Kolumna	Opis
Host	Wyświetlana jest widoczna nazwa hosta. Kliknięcie nazwy hosta otwiera formularz konfiguracji hosta. Jeśli widoczna nazwa hosta nie jest dostępna, wyświetlana jest techniczna nazwa hosta.
Name	Wyświetlana jest nazwa reguły jako niebieski odnośnik. Kliknięcie nazwy reguły otwiera formularz konfiguracji reguły wykrywania niskiego poziomu. Jeśli reguła wykrywania należy do szablonu, nazwa szablonu jest wyświetlana przed nazwą reguły jako szary odnośnik. Kliknięcie odnośnika szablonu otwiera listę reguł na poziomie szablonu.
Items	Wyświetlany jest odnośnik do listy prototypów pozycji. Liczba istniejących prototypów pozycji jest wyświetlana na szaro.
Triggers	Wyświetlany jest odnośnik do listy prototypów wyzwalaczy. Liczba istniejących prototypów wyzwalaczy jest wyświetlana na szaro.
Graphs	Wyświetlany jest odnośnik do listy prototypów wykresów. Liczba istniejących prototypów wykresów jest wyświetlana na szaro.
Hosts	Wyświetlany jest odnośnik do listy prototypów hostów. Liczba istniejących prototypów hostów jest wyświetlana na szaro.
Key	Wyświetlany jest klucz pozycji używany do wykrywania.
Interval	Wyświetlana jest częstotliwość wykonywania wykrywania. *Uwaga*: wykrywanie można również wykonać natychmiast, naciskając przycisk *Execute now* pod listą.
Type	Wyświetlany jest typ pozycji używany do wykrywania (agent Zabbix, agent SNMP itp.).
Status	Wyświetlany jest status reguły wykrywania — *Włączona*, *Wyłączona* lub *Nieobsługiwana*. Kliknięcie statusu umożliwia jego zmianę — z Włączona na Wyłączona (i z powrotem) oraz z Nieobsługiwana na Wyłączona (i z powrotem).
Info	Jeśli wszystko działa prawidłowo, w tej kolumnie nie jest wyświetlana żadna ikona. W przypadku błędów wyświetlana jest kwadratowa ikona z literą „i”. Najedź kursorem na ikonę, aby zobaczyć podpowiedź z opisem błędu.

Aby skonfigurować nową regułę wykrywania niskiego poziomu, kliknij przycisk *Create discovery rule* w prawym górnym rogu.

Opcje masowej edycji

Przyciski pod listą oferują kilka opcji masowej edycji:

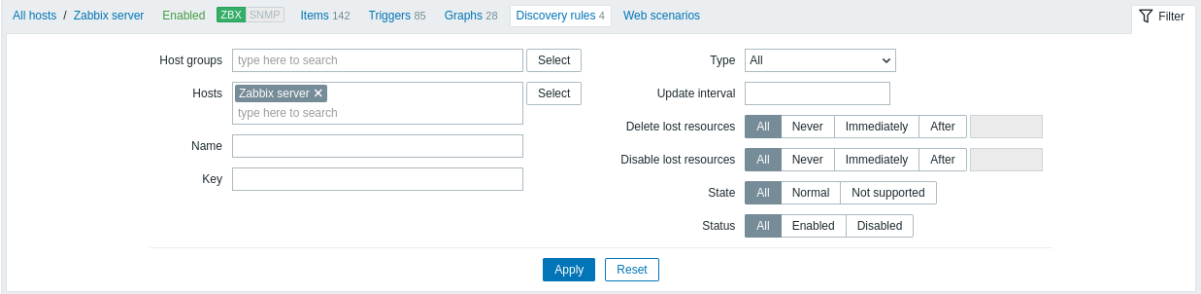
- *Włącz* - zmień status reguły wykrywania niskiego poziomu na *Włączony*.
- *Wyłącz* - zmień status reguły wykrywania niskiego poziomu na *Wyłączony*.
- *Wykonaj teraz* - wykonaj wykrywanie na podstawie reguł wykrywania natychmiast. Zobacz więcej szczegółów. Należy pamiętać, że podczas natychmiastowego wykonywania wykrywania pamięć podręczna konfiguracji nie jest aktualizowana, dlatego wynik nie będzie odzwierciedlał bardzo niedawnych zmian w konfiguracji reguł wykrywania.
- *Usuń* - usuń reguły wykrywania niskiego poziomu.

Aby użyć tych opcji, zaznacz pola wyboru przy odpowiednich regułach wykrywania, a następnie kliknij wymagany przycisk.

Używanie filtra

Możesz użyć filtra, aby wyświetlić tylko te reguły wykrywania, które Cię interesują. Aby zapewnić lepszą wydajność wyszukiwania, dane są przeszukiwane z nierozwiniętymi makrami.

Łącze *Filtr* jest dostępne nad listą reguł wykrywania. Po jego kliknięciu dostępny staje się filtr, w którym można filtrować reguły wykrywania według grup hostów, hosta, nazwy, klucza pozycji, typu pozycji i innych parametrów.

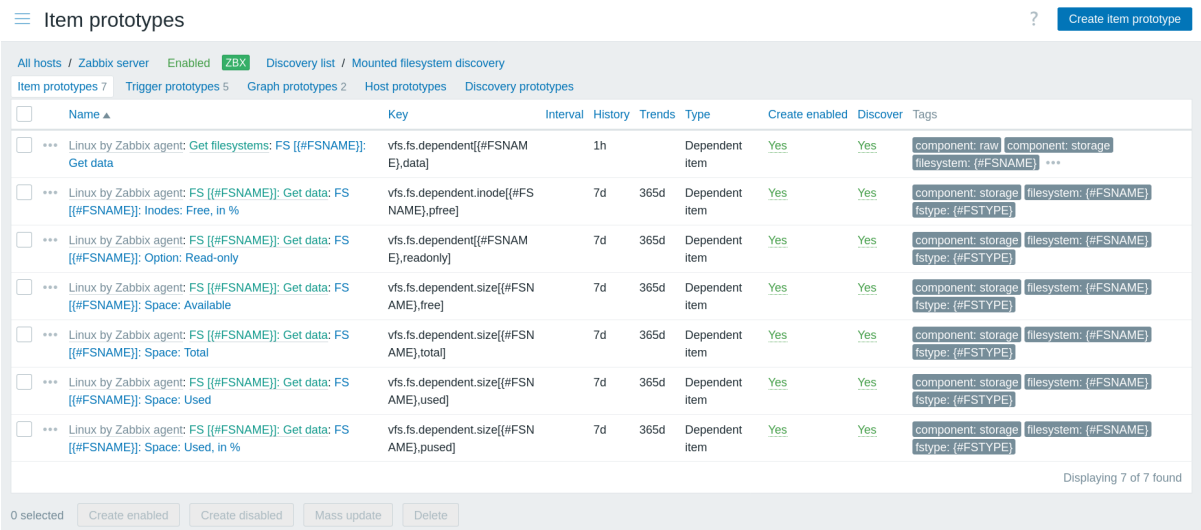


Parametr	Opis
Host groups	Filtruj według jednej lub większej liczby grup hostów. Określenie nadrzędnej grupy hostów powoduje automatyczne wybranie wszystkich zagnieżdżonych grup hostów.
Hosts	Filtruj według jednego lub większej liczby hostów.
Name	Filtruj według nazwy reguły wykrywania.
Key	Filtruj według klucza pozycji wykrywania.
Type	Filtruj według typu pozycji wykrywania.
Update interval	Filtruj według interwału aktualizacji. Niedostępne dla pozycji typu Zabbix trapper i pozycji zależnych.
Delete lost resources	Filtruj według okresu *Delete lost resources*.
Disable lost resources	Filtruj według okresu *Disable lost resources*.
SNMP OID	Filtruj według SNMP OID. Dostępne tylko wtedy, gdy jako typ wybrano *SNMP agent*.
State	Filtruj według stanu reguły wykrywania (Wszystkie/Normalny/Nieobsługiwany).
Status	Filtruj według statusu reguły wykrywania (Wszystkie/Włączone/Wyłączone).

1 Prototypy pozycji

Przegląd

W tej sekcji wyświetlane są prototypy pozycji reguły wykrywania niskiego poziomu na hoście. Prototypy pozycji stanowią podstawę rzeczywistych pozycji hosta, które są tworzone podczas wykrywania niskiego poziomu.



Wyświetlane dane:

Column	Description
Name	Nazwa prototypu pozycji, wyświetlana jako niebieski link. Kliknięcie nazwy otwiera formularz konfiguracji prototypu pozycji. Jeśli prototyp pozycji należy do szablonu, nazwa szablonu jest wyświetlana przed nazwą reguły jako szary link. Kliknięcie linku szablonu otwiera listę prototypów pozycji na poziomie szablonu. Jeśli prototyp pozycji jest typu „Pozycja zależna”, nazwa pozycji nadrzędnej jest wyświetlana przed nazwą prototypu pozycji na zielono.
Key	Wyświetlany jest klucz prototypu pozycji.
Interval	Wyświetlana jest częstotliwość sprawdzania.
History	Wyświetlana jest liczba dni przechowywania historii danych pozycji.
Trends	Wyświetlana jest liczba dni przechowywania historii trendów pozycji.
Type	Wyświetlany jest typ prototypu pozycji (agent Zabbix, agent SNMP, proste sprawdzenie itp.).
Create enabled	Utwórz pozycję na podstawie tego prototypu jako: **Yes** - włączoną **No** - wyłączoną. Możesz przełączać między „Yes” i „No”, klikając je.
Discover	Wykrywaj pozycję na podstawie tego prototypu: **Yes** - wykrywaj **No** - nie wykrywaj. Możesz przełączać między „Yes” i „No”, klikając je.
Tags	Wyświetlane są tagi prototypu pozycji.

Aby skonfigurować nowy prototyp pozycji, kliknij przycisk *Create item prototype* w prawym górnym rogu.

Opcje masowej edycji

Przyciski pod listą oferują kilka opcji masowej edycji:

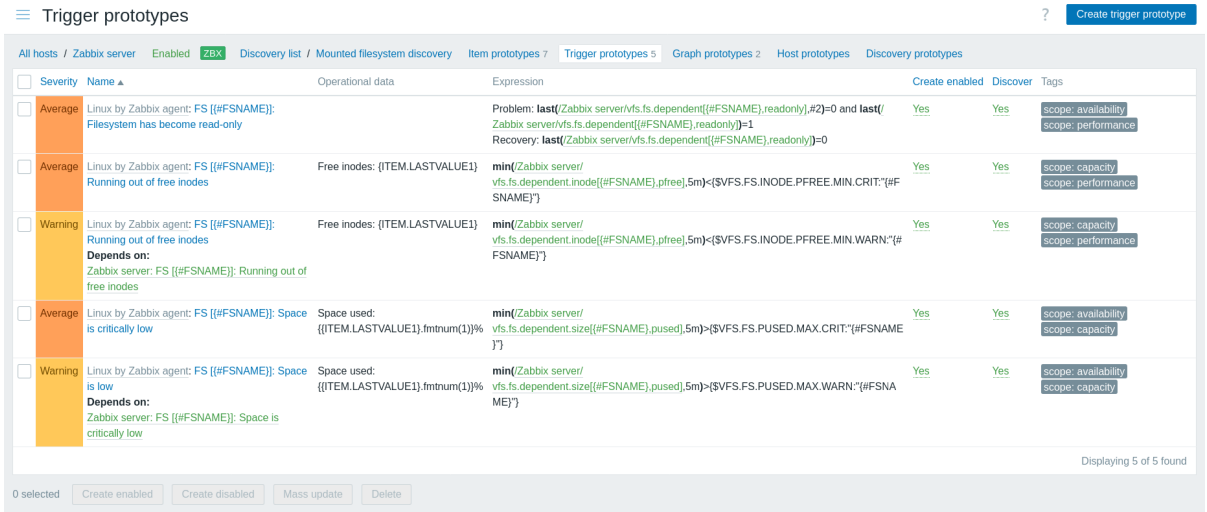
- *Utwórz włączone* - utwórz te prototypy pozycji jako *Włączone*
- *Utwórz wyłączone* - utwórz te prototypy pozycji jako *Wyłączone*
- *Masowa aktualizacja* - masowo zaktualizuj te prototypy pozycji
- *Usuń* - usuń te prototypy pozycji

Aby użyć tych opcji, zaznacz pola wyboru przy odpowiednich prototypach pozycji, a następnie kliknij wymagany przycisk.

2 Prototypy wyzwalaczy

Przegląd

W tej sekcji wyświetlane są prototypy wyzwalaczy reguły wykrywania niskiego poziomu na hoście. Prototypy wyzwalaczy stanowią podstawę rzeczywistych wyzwalaczy hosta, które są tworzone podczas wykrywania niskiego poziomu.



Wyświetlane dane:

Kolumna	Opis
Nazwa	Nazwa prototypu wyzwalacza, wyświetlana jako niebieski link. Kliknięcie nazwy otwiera formularz konfiguracji prototypu wyzwalacza. Jeśli prototyp wyzwalacza należy do podłączonego szablonu, nazwa szablonu jest wyświetlana przed nazwą wyzwalacza jako szary link. Kliknięcie linku szablonu otwiera listę prototypów wyzwalaczy na poziomie podłączonego szablonu.
Dane operacyjne	Wyświetlany jest format danych operacyjnych wyzwalacza, zawierający dowolne ciągi znaków i makra, które będą dynamicznie rozwijane w *Monitoring* → *Problemy*.
Twórz jako włączone	Utwórz wyzwalacz na podstawie tego prototypu jako: **Tak** - włączony **Nie** - wyłączony. Możesz przełączać między „Tak” i „Nie”, klikając je.
Odkrywaj	Odkrywaj wyzwalacz na podstawie tego prototypu: **Tak** - odkrywaj **Nie** - nie odkrywaj. Możesz przełączać między „Tak” i „Nie”, klikając je.
Tagi	Wyświetlane są tagi prototypu wyzwalacza.

Aby skonfigurować nowy prototyp wyzwalacza, kliknij przycisk *Utwórz prototyp wyzwalacza* w prawym górnym rogu.

Opcje masowej edycji

Przyciski poniżej listy oferują kilka opcji masowej edycji:

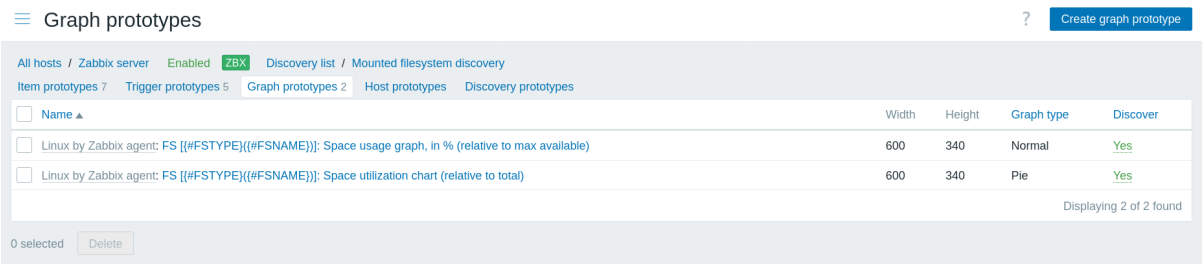
- *Create enabled* - utwórz te wyzwalacze jako *Enabled*
- *Create disabled* - utwórz te wyzwalacze jako *Disabled*
- *Mass update* - masowo zaktualizuj te prototypy wyzwalaczy
- *Delete* - usuń te prototypy wyzwalaczy

Aby użyć tych opcji, zaznacz pola wyboru przy odpowiednich prototypach wyzwalaczy, a następnie kliknij wymagany przycisk.

3 Prototypy wykresów

Przegląd

W tej sekcji wyświetlane są prototypy wykresów reguły wykrywania niskiego poziomu na hoście. Prototypy wykresów stanowią podstawę rzeczywistych wykresów hosta, które są tworzone podczas wykrywania niskiego poziomu.



Wyświetlane dane:

Kolumna	Opis
Nazwa	Nazwa prototypu wykresu, wyświetlana jako niebieski link. Kliknięcie nazwy otwiera formularz konfiguracji prototypu wykresu. Jeśli prototyp wykresu należy do podłączonego szablonu, nazwa szablonu jest wyświetlana przed nazwą wykresu jako szary link. Kliknięcie linku szablonu otwiera listę prototypów wykresów na poziomie podłączonego szablonu.
Szerokość	Wyświetlana jest szerokość prototypu wykresu.
Wysokość	Wyświetlana jest wysokość prototypu wykresu.
Typ	Wyświetlany jest typ prototypu wykresu — *Normalny*, *Skumulowany*, *Kołowy* lub *Rozsunięty*.
Odkrywaj	Odkrywaj wykres na podstawie tego prototypu: **Tak** — odkrywaj **Nie** — nie odkrywaj. Możesz przełączać między „Tak” i „Nie”, klikając je.

Aby skonfigurować nowy prototyp wykresu, kliknij przycisk *Utwórz prototyp wykresu* w prawym górnym rogu.

Opcje masowej edycji

Przyciski poniżej listy oferują kilka opcji masowej edycji:

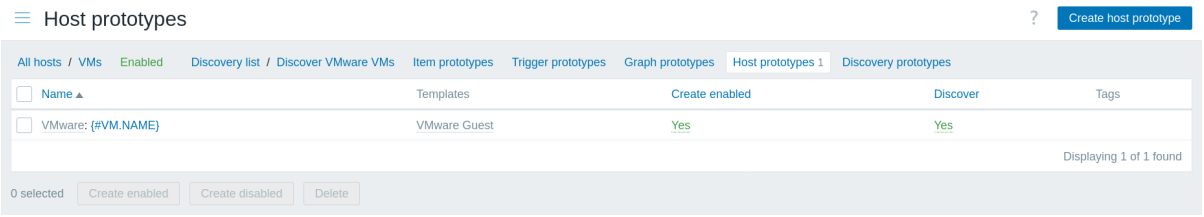
- *Usuń* - usuń te prototypy wykresów

Aby skorzystać z tych opcji, zaznacz pola wyboru przy odpowiednich prototypach wykresów, a następnie kliknij wymagany przycisk.

4 Prototypy hostów

Przegląd

W tej sekcji wyświetlane są prototypy hostów reguły wykrywania niskiego poziomu na hoście. Prototypy hostów stanowią podstawę rzeczywistych hostów, które są tworzone podczas wykrywania niskiego poziomu.



Wyświetlane dane:

Kolumna	Opis
Nazwa	Nazwa prototypu hosta, wyświetlana jako niebieski link. Kliknięcie nazwy otwiera formularz konfiguracji prototypu hosta. Jeśli prototyp hosta należy do podłączonego szablonu, nazwa szablonu jest wyświetlana przed nazwą hosta jako szary link. Kliknięcie linku szablonu otwiera listę prototypów hostów na poziomie podłączonego szablonu.
Szablony	Wyświetlane są szablony prototypu hosta.
Twórz włączone	Utwórz host na podstawie tego prototypu jako: **Tak** - włączone **Nie** - wyłączone. Możesz przełączać między „Tak” i „Nie”, klikając je.
Odkrywaj	Odkrywaj host na podstawie tego prototypu: **Tak** - odkrywaj **Nie** - nie odkrywaj. Możesz przełączać między „Tak” i „Nie”, klikając je.
Tagi	Wyświetlane są tagi prototypu hosta.

Aby skonfigurować nowy prototyp hosta, kliknij przycisk *Utwórz prototyp hosta* w prawym górnym rogu.

Opcje masowej edycji

Przyciski pod listą oferują kilka opcji masowej edycji:

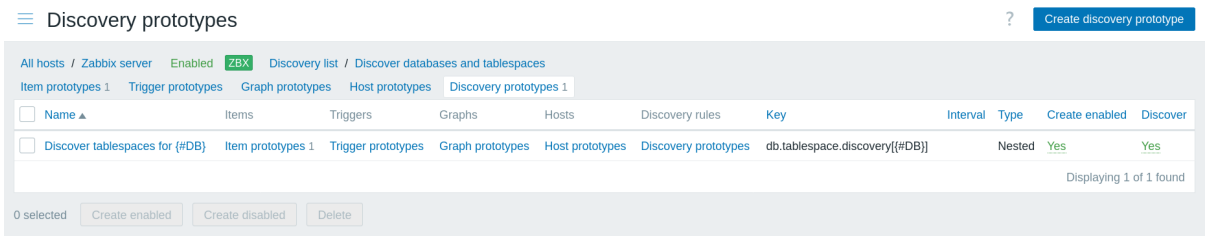
- *Utwórz włączone* - utwórz te hosty jako *Włączone*
- *Utwórz wyłączone* - utwórz te hosty jako *Wyłączone*
- *Usuń* - usuń te prototypy hostów

Aby użyć tych opcji, zaznacz pola wyboru przy odpowiednich prototypach hostów, a następnie kliknij wymagany przycisk.

5 Prototypy wykrywania

Przegląd

W tej sekcji wyświetlane są prototypy wykrywania reguły wykrywania niskiego poziomu na hoście. Prototypy wykrywania są zagnieżdżonymi regułami wykrywania nadrzędnej reguły wykrywania.



Wyświetlane dane:

Column	Description
Name	Nazwa prototypu wykrywania, wyświetlana jako niebieski link. Kliknięcie nazwy otwiera formularz konfiguracji prototypu wykrywania. Jeśli prototyp wykrywania należy do podłączonego szablonu, nazwa szablonu jest wyświetlana przed nazwą hosta jako szary link. Kliknięcie linku szablonu otwiera listę prototypów wykrywania na poziomie podłączonego szablonu.
Items	Wyświetlany jest link do listy prototypów pozycji. Liczba istniejących prototypów pozycji jest wyświetlana na szaro.
Triggers	Wyświetlany jest link do listy prototypów wyzwalaczy. Liczba istniejących prototypów wyzwalaczy jest wyświetlana na szaro.
Graphs	Wyświetlany jest link do listy prototypów wykresów. Liczba istniejących prototypów wykresów jest wyświetlana na szaro.
Hosts	Wyświetlany jest link do listy prototypów hostów. Liczba istniejących prototypów hostów jest wyświetlana na szaro.
Discovery rules	Wyświetlany jest link do listy prototypów wykrywania. Liczba istniejących prototypów wykrywania jest wyświetlana na szaro.
Key	Wyświetlany jest klucz pozycji używany do wykrywania.
Interval	Wyświetlana jest częstotliwość wykonywania wykrywania. *Uwaga*: wykrywanie można również wykonać natychmiast, naciskając przycisk *Execute now* poniżej listy.
Type	Wyświetlany jest typ pozycji używany do wykrywania (Zabbix agent, SNMP agent itp.).
Create enabled	Wyświetlany jest status tworzenia prototypu wykrywania — tworzenie włączone (*Yes*) lub tworzenie wyłączone (*No*). Klikając status, można go zmienić — z Yes na No (i z powrotem).
Discover	Wyświetlany jest status wykrywania prototypu wykrywania — wykrywaj (*Yes*) lub nie wykrywaj (*No*). Klikając status, można go zmienić — z Yes na No (i z powrotem).

Aby skonfigurować nowy prototyp wykrywania, kliknij przycisk *Create discovery prototype* w prawym górnym rogu.

Opcje masowej edycji

Przyciski poniżej listy oferują kilka opcji masowej edycji:

- *Utwórz włączone* - utwórz te prototypy wykrywania jako *Włączone*
- *Utwórz wyłączone* - utwórz te prototypy wykrywania jako *Wyłączone*
- *Usuń* - usuń te prototypy wykrywania

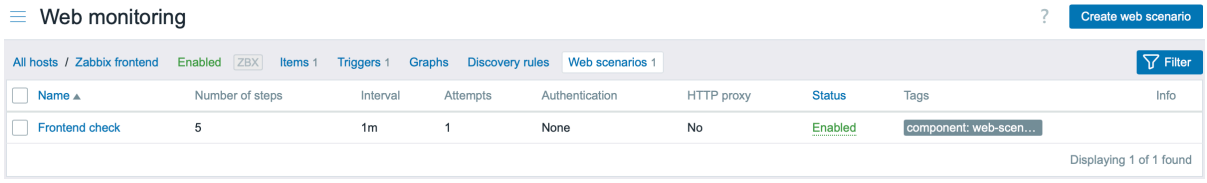
Aby użyć tych opcji, zaznacz pola wyboru przy odpowiednich prototypach wykrywania, a następnie kliknij wymagany przycisk.

5 Scenariusze webowe

Przegląd

Lista scenariuszy WWW dla hosta jest dostępna z poziomu *Zbieranie danych* → *Hosty*, po kliknięciu *WWW* dla odpowiedniego hosta.

Wyświetlana jest lista istniejących scenariuszy WWW.



Wyświetlane dane:

Kolumna	Opis
Nazwa	Nazwa scenariusza WWW. Kliknięcie nazwy scenariusza WWW otwiera formularz konfiguracji scenariusza WWW. Jeśli scenariusz WWW hosta należy do szablonu, nazwa szablonu jest wyświetlana przed nazwą scenariusza WWW jako szary odnośnik. Kliknięcie odnośnika szablonu otworzy listę scenariuszy WWW na poziomie szablonu.
Liczba kroków	Liczba kroków zawartych w scenariuszu.
Interwał aktualizacji	Jak często scenariusz jest wykonywany.
Próby	Liczba prób wykonywania kroków scenariusza WWW.
Uwierzytelnianie	Wyświetlana jest metoda uwierzytelniania — Basic, NTLM, Kerberos, Digest lub None.
HTTP proxy	Wyświetla HTTP proxy lub „Nie”, jeśli nie jest używany.
Status	Wyświetlany jest status scenariusza WWW — *Włączony* lub *Wyłączony*. Kliknięcie statusu pozwala go zmienić.
Tagi	Wyświetlane są tagi scenariusza WWW. Można wyświetlić maksymalnie trzy tagi (pary nazwa:wartość). Jeśli tagów jest więcej, wyświetlany jest odnośnik „...”, który po najechaniu kursorem pozwala zobaczyć wszystkie tagi.
Informacje	Jeśli wszystko działa poprawnie, w tej kolumnie nie jest wyświetlana żadna ikona. W przypadku błędów wyświetlana jest kwadratowa ikona z literą „i”. Najedź kursorem na ikonę, aby zobaczyć podpowiedź z opisem błędu.

Aby skonfigurować nowy scenariusz WWW, kliknij przycisk *Utwórz scenariusz WWW* w prawym górnym rogu.

Opcje masowej edycji

Przyciski pod listą oferują kilka opcji masowej edycji:

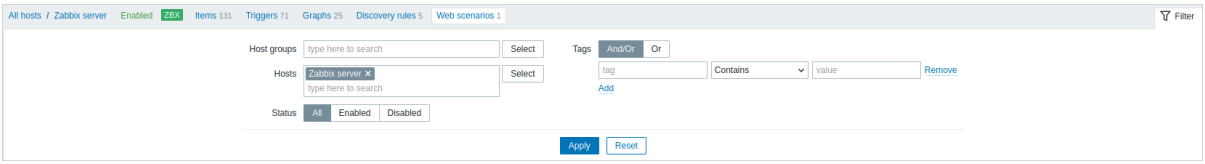
- *Włącz* - zmień status scenariusza na *Włączony*
- *Wyłącz* - zmień status scenariusza na *Wyłączony*
- *Wyczyść historię i trendy* - wyczyść dane historii i trendów dla scenariuszy
- *Usuń* - usuń scenariusze WWW

Aby użyć tych opcji, zaznacz pola wyboru przy odpowiednich scenariuszach WWW, a następnie kliknij wymagany przycisk.

Używanie filtra

Możesz użyć filtra, aby wyświetlić tylko te scenariusze, które Cię interesują. Dla lepszej wydajności wyszukiwania dane są przeszukiwane z nierozwiniętymi makrami.

Łącze *Filtr* jest dostępne nad listą scenariuszy WWW. Kliknięcie go otworzy filtr, w którym można określić żądane kryteria filtrowania.



Parametr	Opis
Grupy hostów	Filtruj według jednej lub większej liczby grup hostów. Określenie nadrzędnej grupy hostów powoduje automatyczne wybranie wszystkich zagnieżdżonych grup hostów.
Hosty	Filtruj według jednego lub większej liczby hostów. Jeśli powyżej wybrano już grupy hostów, wybór hostów jest ograniczony do tych grup.
Status	Filtruj według statusu scenariusza WWW.

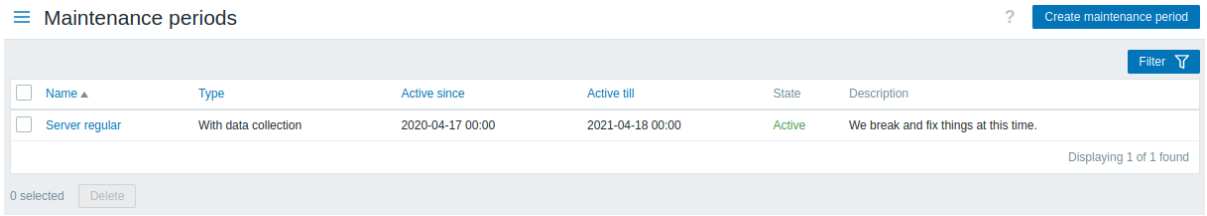
Parametr	Opis
Tagi	Filtruj według nazwy i wartości tagu scenariusza WWW. Możliwe jest zarówno uwzględnianie, jak i wykluczanie określonych tagów oraz wartości tagów. Można ustawić kilka warunków. Dopasowanie nazw tagów zawsze uwzględnia wielkość liter. Dla każdego warunku dostępnych jest kilka operatorów: **Istnieje** - uwzględnij określone nazwy tagów; **Równa się** - uwzględnij określone nazwy i wartości tagów (z uwzględnieniem wielkości liter); **Zawiera** - uwzględnij określone nazwy tagów, dla których wartości tagów zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter); **Nie istnieje** - wyklucz określone nazwy tagów; **Nie równa się** - wyklucz określone nazwy i wartości tagów (z uwzględnieniem wielkości liter); **Nie zawiera** - wyklucz określone nazwy tagów, dla których wartości tagów zawierają wprowadzony ciąg (dopasowanie podciągu, bez uwzględniania wielkości liter). Dostępne są dwa typy obliczania warunków: **And/Or** - wszystkie warunki muszą być spełnione, a warunki mające tę samą nazwę tagu będą grupowane operatorem Or; **Or** - wystarczy, że spełniony będzie jeden warunek.

5 Konserwacja

Przegląd

W sekcji *Zbieranie danych* → *Konserwacja* użytkownicy mogą konfigurować i utrzymywać okresy konserwacji dla hostów.

Wyświetlana jest lista istniejących okresów konserwacji wraz z ich szczegółami.



Wyświetlane dane:

Kolumna	Opis
Nazwa	Nazwa okresu konserwacji. Kliknięcie nazwy okresu konserwacji otwiera formularz konfiguracji okresu konserwacji.
Typ	Wyświetlany jest typ konserwacji: *Ze zbieraniem danych* lub *Bez zbierania danych*
Aktywny od	Data i godzina, od których wykonywanie okresów konserwacji staje się aktywne. Uwaga: Ten czas nie aktywuje okresu konserwacji; okresy konserwacji należy ustawić osobno.
Aktywny do	Data i godzina, o której wykonywanie okresów konserwacji przestaje być aktywne.
Stan	Stan okresu konserwacji: **Zbliża się** - wkrótce stanie się aktywny **Aktywny** - jest aktywny **Wygasły** - nie jest już aktywny
Opis	Wyświetlany jest opis okresu konserwacji.

Aby skonfigurować nowy okres konserwacji, kliknij przycisk *Utwórz okres konserwacji* w prawym górnym rogu.

Opcje masowej edycji

Przycisk poniżej listy udostępnia jedną opcję masowej edycji:

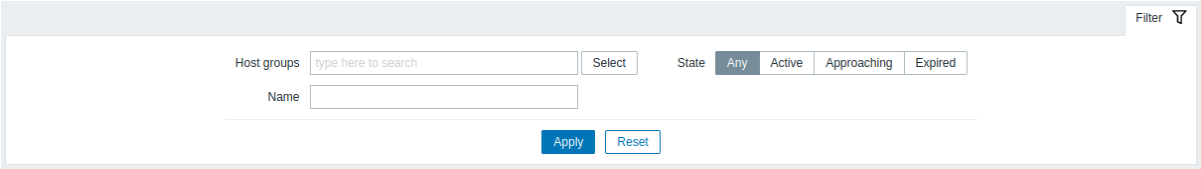
- *Usuń* — usuń okresy konserwacji

Aby użyć tej opcji, zaznacz pola wyboru przy odpowiednich okresach konserwacji i kliknij *Usuń*.

Używanie filtra

Możesz użyć filtra, aby wyświetlić tylko te okresy konserwacji, które Cię interesują. Dla lepszej wydajności wyszukiwania dane są przeszukiwane bez rozwijania makr.

Link *Filtr* jest dostępny nad listą okresów konserwacji. Po kliknięciu go dostępny staje się filtr, za pomocą którego można filtrować okresy konserwacji według grupy hostów, nazwy i stanu.



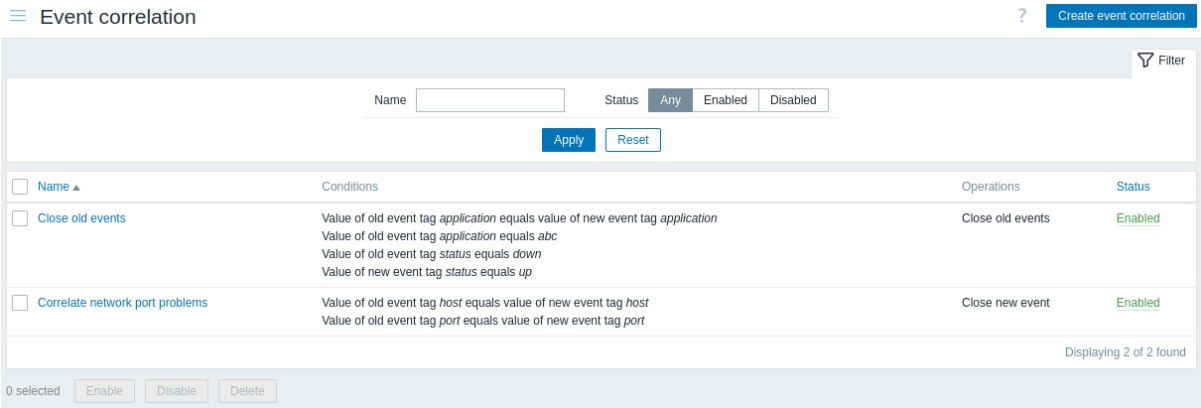
Obliczanie kolejek podczas konserwacji

Attention:
Proxy Zabbix nie jest świadomy okresów konserwacji; szczegóły znajdują się w Obliczanie kolejek podczas konserwacji.

6 Korelacja zdarzeń

Przegląd

W sekcji *Zbieranie danych* → *Korelacja zdarzeń* użytkownicy mogą konfigurować i utrzymywać reguły globalnej korelacji dla zdarzeń Zabbix.



Wyświetlane dane:

Kolumna	Opis
Nazwa	Nazwa reguły korelacji. Kliknięcie nazwy reguły korelacji otwiera formularz konfiguracji reguły.
Warunki	Wyświetlane są warunki reguły korelacji.
Operacje	Wyświetlane są operacje reguły korelacji.
Status	Wyświetlany jest status reguły korelacji — *Włączona* lub *Wyłączona*. Kliknięcie statusu umożliwia jego zmianę.

Aby skonfigurować nową regułę korelacji, kliknij przycisk *Utwórz korelację zdarzeń* w prawym górnym rogu.

Opcje masowej edycji

Przyciski poniżej listy oferują kilka opcji masowej edycji:

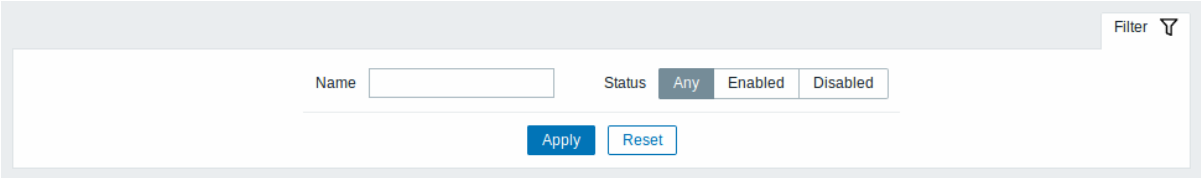
- *Włącz* - zmień stan reguły korelacji na *Włączony*
- *Wyłącz* - zmień stan reguły korelacji na *Wyłączony*
- *Usuń* - usuń reguły korelacji

Aby użyć tych opcji, zaznacz pola wyboru przy odpowiednich regułach korelacji, a następnie kliknij wymagany przycisk.

Używanie filtra

Możesz użyć filtra, aby wyświetlić tylko te reguły korelacji, które Cię interesują. Aby zapewnić lepszą wydajność wyszukiwania, dane są przeszukiwane z nierozwiniętymi makrami.

Link *Filtr* jest dostępny nad listą reguł korelacji. Po jego kliknięciu dostępny staje się filtr, za pomocą którego można filtrować reguły korelacji według nazwy i statusu.

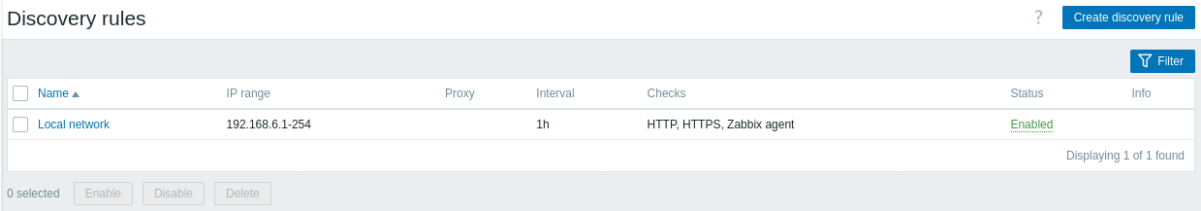


7 Wykrywanie

Przegląd

W sekcji *Zbieranie danych* → *Wykrywanie* użytkownicy mogą konfigurować i utrzymywać reguły wykrywania.

Wyświetlana jest lista istniejących reguł wykrywania wraz z ich szczegółami.



Wyświetlane dane:

Kolumna	Opis
Nazwa	Nazwa reguły wykrywania. Kliknięcie nazwy reguły wykrywania otwiera formularz konfiguracji reguły wykrywania.
Zakres IP	Wyświetlany jest zakres adresów IP używany do skanowania sieci.
Proxy	Wyświetlana jest nazwa proxy, jeśli wykrywanie jest wykonywane przez proxy.
Interwał	Wyświetlana jest częstotliwość wykonywania wykrywania.
Kontrole	Wyświetlane są typy kontroli używane do wykrywania.
Status	Wyświetlany jest status reguły wykrywania — *Włączona* lub *Wyłączona*. Kliknięcie statusu umożliwia jego zmianę.
Informacja	Jeśli wszystko działa poprawnie, w tej kolumnie nic nie jest wyświetlane. W przypadku błędów wyświetlana jest czerwona ikona informacji z literą „i”. Najedź kursorem na ikonę, aby zobaczyć podpowiedź z opisem błędu.

Aby skonfigurować nową regułę wykrywania, kliknij przycisk *Utwórz regułę wykrywania* w prawym górnym rogu.

Opcje masowej edycji

Przyciski poniżej listy oferują kilka opcji masowej edycji:

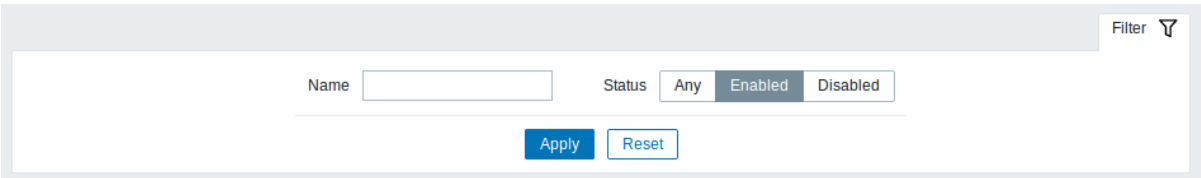
- *Włącz* - zmień status reguły wykrywania na *Włączony*
- *Wyłącz* - zmień status reguły wykrywania na *Wyłączony*
- *Usuń* - usuń reguły wykrywania

Aby użyć tych opcji, zaznacz pola wyboru przy odpowiednich regułach wykrywania, a następnie kliknij wymagany przycisk.

Używanie filtra

Możesz użyć filtra, aby wyświetlić tylko te reguły wykrywania, które Cię interesują. Dla lepszej wydajności wyszukiwania dane są przeszukiwane z nierozwiniętymi makrami.

Link *Filtr* jest dostępny nad listą reguł wykrywania. Po kliknięciu staje się dostępny filtr, za pomocą którego można filtrować reguły wykrywania według nazwy i statusu.



7 Alerty

Przegląd

To menu zawiera sekcje związane z konfiguracją alertów w Zabbix.

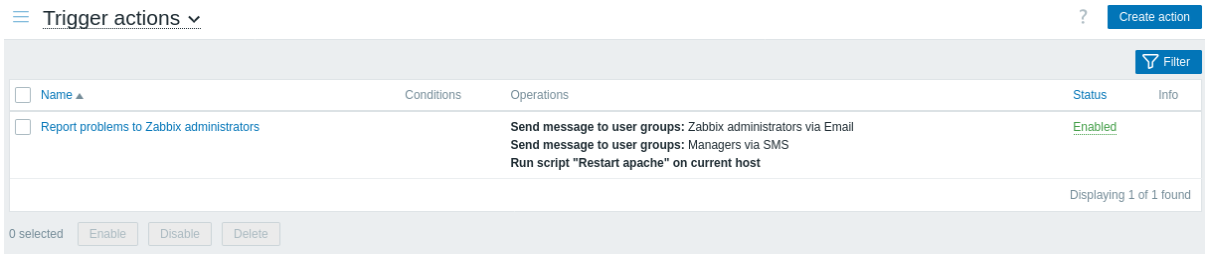
1 Akcje

Przegląd

W sekcji *Alerty* → *Akcje* użytkownicy mogą konfigurować i zarządzać akcjami.

Wyświetlane akcje to akcje przypisane do wybranego źródła zdarzeń (wyzwalacze, usługi, wykrywanie, autorejestracja, akcje wewnętrzne).

Aby przełączyć się na inne źródło zdarzeń, kliknij *Akcje* w sekcji menu *Alerty*. Możliwe jest również przełączanie się między źródłami za pomocą rozwijanej listy tytułu w lewym górnym rogu.



Wyświetlane dane:

Kolumna	Opis
Nazwa	Nazwa akcji. Kliknięcie nazwy akcji otwiera formularz konfiguracji akcji.
Warunki	Wyświetlane są warunki akcji.
Operacje	Wyświetlane są operacje akcji. Lista operacji wyświetla również typ nośnika (e-mail, SMS lub skrypt) używanego do powiadomień, a także imię i nazwisko (w nawiasach po nazwie użytkownika) odbiorcy powiadomienia. Operacja akcji może być zarówno powiadomieniem, jak i zdalnym poleceniem, w zależności od wybranego typu operacji.
Status	Wyświetlany jest status akcji — *Włączona* lub *Wyłączona*. Kliknięcie statusu umożliwia jego zmianę. Więcej informacji o tym, co się stanie, jeśli akcja zostanie wyłączona podczas trwającej eskalacji, znajduje się w sekcji Eskalacje.
Info	Jeśli wszystko działa poprawnie, w tej kolumnie nie jest wyświetlana żadna ikona. W przypadku błędów, takich jak brakujące operacje akcji lub warunki po aktualizacji/wykrywaniu niskopoziomowym, wyświetlana jest ikona ostrzeżenia. Najedź kursorem na ikonę, aby zobaczyć podpowiedź z opisem błędu.

Aby skonfigurować nową akcję, kliknij przycisk *Utwórz akcję* w prawym górnym rogu.

Dla użytkowników bez uprawnień Super admin akcje są wyświetlane zgodnie z ustawieniami uprawnień. Oznacza to, że w niektórych przypadkach użytkownik bez uprawnień Super admin nie może wyświetlić pełnej listy akcji z powodu określonych ograniczeń uprawnień. Akcja jest wyświetlana użytkownikowi bez uprawnień Super admin, jeśli spełnione są następujące warunki:

- Użytkownik ma dostęp do odczytu i zapisu do grup hostów, hostów, szablonów oraz wyzwalaczy w warunkach akcji
- Użytkownik ma dostęp do odczytu i zapisu do grup hostów, hostów i szablonów w operacjach akcji, operacjach odzyskiwania i operacjach aktualizacji
- Użytkownik ma dostęp do odczytu do grup użytkowników i użytkowników w operacjach akcji, operacjach odzyskiwania i operacjach aktualizacji

Opcje masowej edycji

Przyciski poniżej listy oferują kilka opcji masowej edycji:

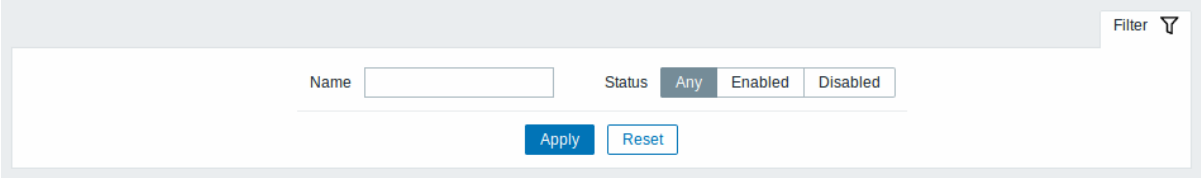
- *Włącz* - zmień status akcji na *Włączona*
- *Wyłącz* - zmień status akcji na *Wyłączona*
- *Usuń* - usuń akcje

Aby skorzystać z tych opcji, zaznacz pola wyboru przy odpowiednich akcjach, a następnie kliknij wymagany przycisk.

Używanie filtra

Możesz użyć filtra, aby wyświetlić tylko te akcje, które Cię interesują. Dla lepszej wydajności wyszukiwania dane są przeszukiwane z nierozwiązanymi makrami.

Link *Filtr* jest dostępny nad listą akcji. Po kliknięciu udostępniony zostanie filtr, w którym można filtrować akcje według nazwy i statusu.



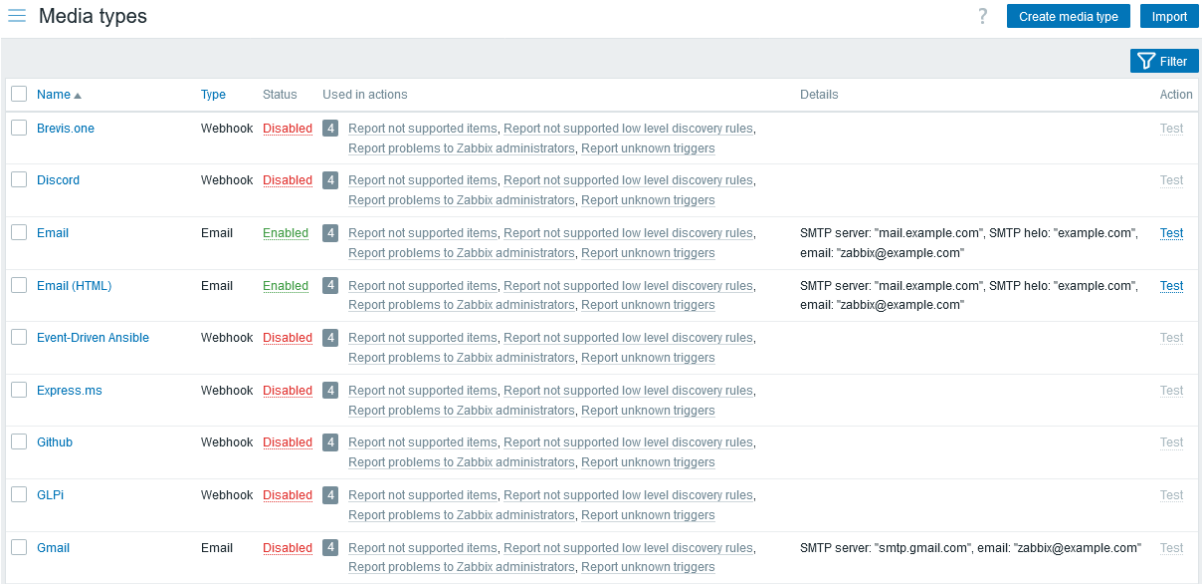
2 Typy mediów

Przegląd

W sekcji *Alerty* → *Typy mediów* użytkownicy mogą konfigurować i zarządzać informacjami o typach mediów.

Informacje o typie mediów zawierają ogólne instrukcje dotyczące używania danego medium jako kanału dostarczania powiadomień. Szczegółowe dane, takie jak indywidualne adresy e-mail, na które ma zostać wysłane powiadomienie, są przechowywane przy poszczególnych użytkownikach.

Wyświetlana jest lista istniejących typów mediów wraz z ich szczegółami.



Wyświetlane dane:

Kolumna	Opis
Nazwa	Nazwa typu mediów. Kliknięcie nazwy otwiera formularz konfiguracji typu mediów.
Typ	Wyświetlany jest typ medium (e-mail, SMS itp.).
Status	Wyświetlany jest status typu mediów — *Włączony* lub *Wyłączony*. Kliknięcie statusu pozwala go zmienić.
Używany w akcjach	Wyświetlane są akcje, w których używany jest typ mediów, poprzedzone łączną liczbą tych akcji. Kliknięcie nazwy akcji otwiera formularz konfiguracji akcji. Jeśli użytkownik nie ma uprawnień do akcji, nazwa nie jest klikalna.
Szczegóły	Wyświetlane są szczegółowe informacje o typie mediów.
Działania	Dostępne jest następujące działanie: **Test** — kliknij, aby otworzyć formularz testowy, w którym można wprowadzić parametry typu mediów (np. adres odbiorcy wraz z testowym tematem i treścią) oraz wysłać wiadomość testową w celu sprawdzenia, czy skonfigurowany typ mediów działa. Zobacz także: Testowanie typu mediów.

Aby skonfigurować nowy typ mediów, kliknij przycisk *Utwórz typ mediów* w prawym górnym rogu.

Aby zaimportować typ mediów, kliknij przycisk *Importuj* w prawym górnym rogu.

Opcje masowej edycji

Przyciski poniżej listy oferują kilka opcji masowej edycji:

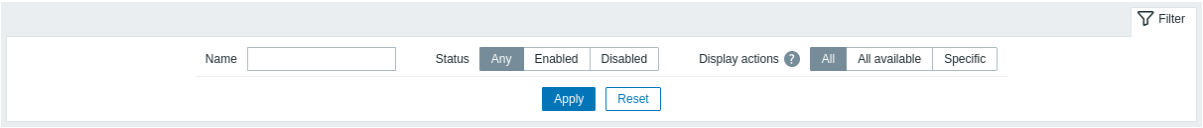
- *Włącz* - zmień status typu nośnika na *Włączony*
- *Wyłącz* - zmień status typu nośnika na *Wyłączony*
- *Eksportuj* - wyeksportuj typy nośników do pliku YAML, XML lub JSON
- *Usuń* - usuń typy nośników

Aby użyć tych opcji, zaznacz pola wyboru przy odpowiednich typach nośników, a następnie kliknij wymagany przycisk.

Używanie filtra

Możesz użyć filtra, aby wyświetlić tylko te typy mediów, które Cię interesują. Dla lepszej wydajności wyszukiwania dane są przeszukiwane z nierozwiniętymi makrami.

Link *Filtr* jest dostępny nad listą typów mediów. Po jego kliknięciu dostępny staje się filtr, za pomocą którego można filtrować typy mediów według nazwy i statusu. Dodatkowo możesz użyć filtra, aby wyświetlać akcje w kolumnie *Używane w akcjach* na podstawie zakresu użycia ich typu mediów (zdefiniowanego przez parametr *Send to media type* w szczegółach operacji akcji).



3 Skrypty

Przegląd

W sekcji *Alerty* > *Skrypty* można konfigurować i utrzymywać globalne skrypty zdefiniowane przez użytkownika.

Globalne skrypty, w zależności od skonfigurowanego zakresu oraz uprawnień użytkownika, są dostępne do uruchomienia:

- z menu hosta w różnych miejscach frontendu (*Pulpit*, *Problemy*, *Najnowsze dane*, *Mapy* itp.)
- z menu zdarzenia
- mogą być uruchamiane jako operacja akcji

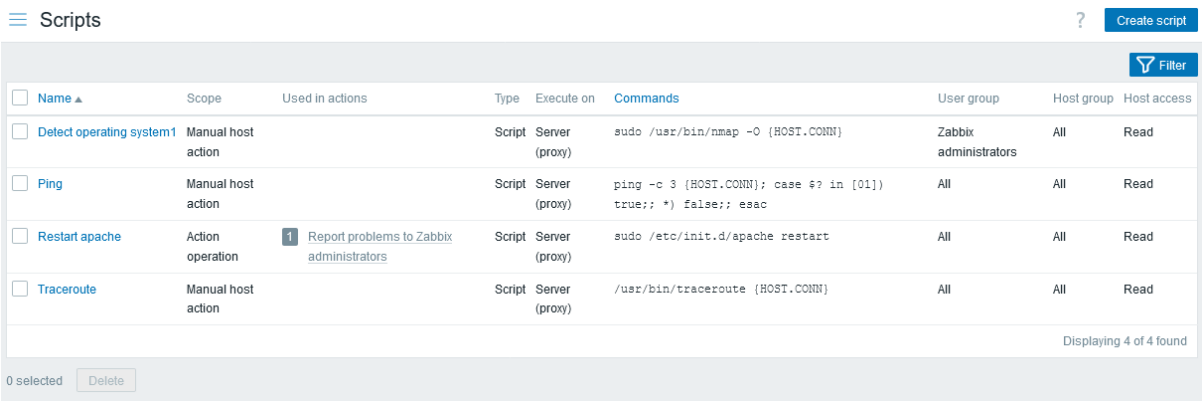
Skrypty są wykonywane na Zabbix agent, serwerze Zabbix (proxy) lub tylko na serwerze Zabbix. Zobacz także Wykonywanie poleceń.

Zarówno na Zabbix agent, jak i Zabbix proxy zdalne skrypty są domyślnie wyłączone. Można je włączyć w następujący sposób:

- Dla zdalnych poleceń wykonywanych na Zabbix agent:
  - dodając parametr AllowKey=system.run[<command>,*] dla każdego dozwolonego polecenia w konfiguracji agenta; * oznacza tryb wait i nowait;
- Dla zdalnych poleceń wykonywanych na Zabbix proxy:
  - **Ostrzeżenie: Nie jest wymagane włączanie zdalnych poleceń na Zabbix proxy, jeśli zdalne polecenia są wykonywane na Zabbix agent monitorowanym przez Zabbix proxy.** Jeśli jednak wymagane jest wykonywanie zdalnych poleceń na Zabbix proxy, ustaw parametr *EnableRemoteCommands* na '1' w konfiguracji proxy.

Wykonywanie globalnych skryptów na serwerze Zabbix można wyłączyć, ustawiając `EnableGlobalScripts=0` w konfiguracji serwera. W nowych instalacjach, począwszy od Zabbix 7.0, wykonywanie globalnych skryptów na serwerze Zabbix jest domyślnie wyłączone.

Wyświetlana jest lista istniejących skryptów wraz z ich szczegółami.



Wyświetlane dane:

Column	Description
Name	Nazwa skryptu. Kliknięcie nazwy skryptu otwiera formularz konfiguracji skryptu.
Scope	Zakres skryptu - operacja akcji, ręczna akcja hosta lub ręczna akcja zdarzenia. To ustawienie określa, gdzie skrypt jest dostępny.
Used in actions	Wyświetlane są wszystkie akcje, w których używany jest skrypt, poprzedzone łączną liczbą tych akcji. Kliknięcie nazwy akcji otwiera formularz konfiguracji akcji. Jeśli użytkownik nie ma uprawnień do akcji, nazwa nie jest klikalna.
Type	Wyświetlany jest typ skryptu - polecenie *URL*, *Webhook*, *Script*, *SSH*, *Telnet* lub *IPMI*.
Execute on	Wyświetlana jest informacja, czy skrypt będzie wykonywany na Zabbix agent, Zabbix proxy lub serwerze, czy tylko na serwerze Zabbix.
Commands	Wyświetlane są wszystkie polecenia, które mają zostać wykonane w ramach skryptu. Dla webhooków nic nie jest tutaj wyświetlane.
User group	Wyświetlana jest grupa użytkowników, dla której skrypt jest dostępny (lub *All* dla wszystkich grup użytkowników).
Host group	Wyświetlana jest grupa hostów, dla której skrypt jest dostępny (lub *All* dla wszystkich grup hostów).
Host access	Wyświetlany jest poziom uprawnień dla grupy hostów - *Read* lub *Write*. Tylko użytkownicy z wymaganym poziomem uprawnień będą mieli dostęp do wykonania skryptu.

Aby skonfigurować nowy skrypt, kliknij przycisk *Create script* w prawym górnym rogu.

Opcje masowej edycji

Przycisk pod listą oferuje jedną opcję masowej edycji:

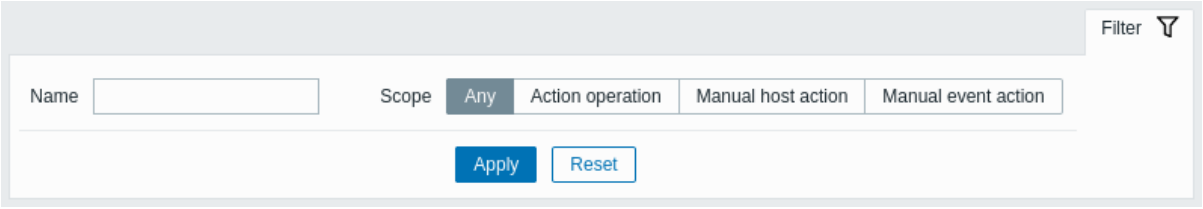
- *Usuń* - usuń skrypty

Aby użyć tej opcji, zaznacz pola wyboru przy odpowiednich skryptach i kliknij *Usuń*.

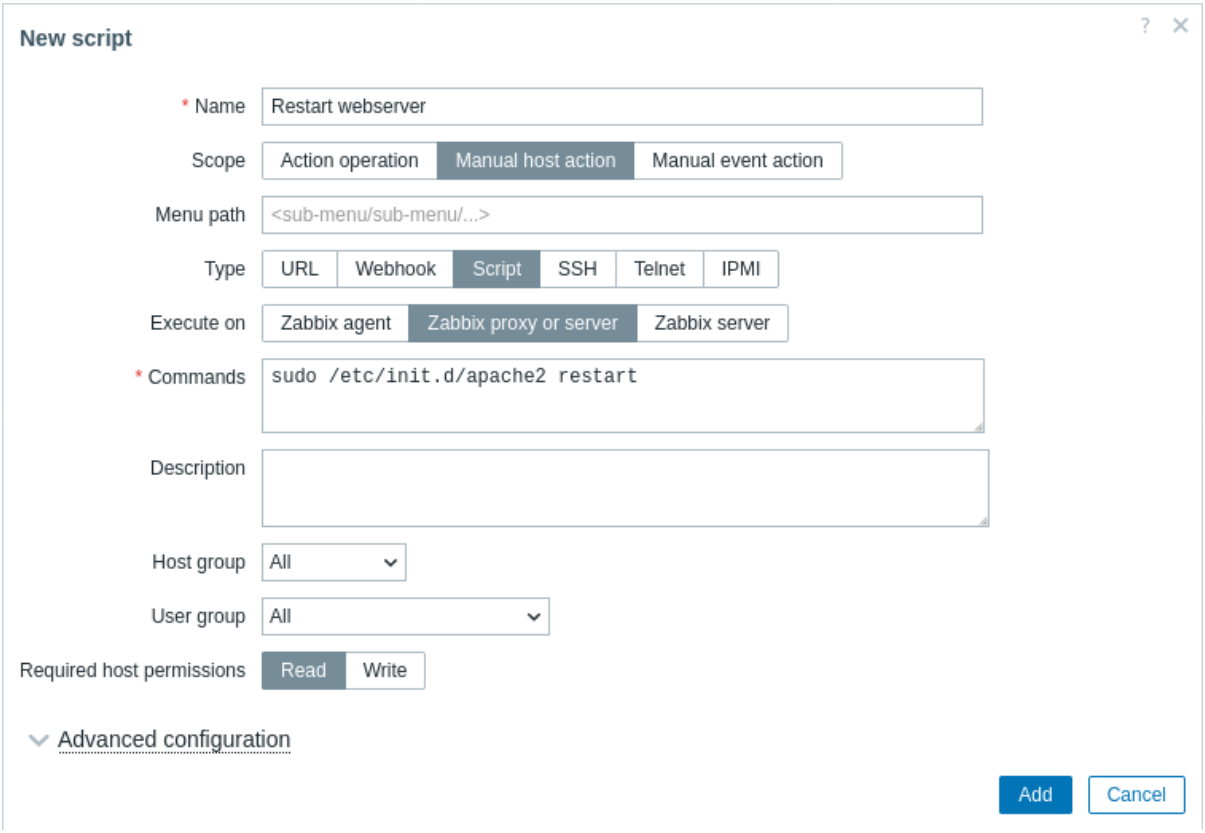
Używanie filtra

Możesz użyć filtra, aby wyświetlić tylko te skrypty, które Cię interesują. Dla lepszej wydajności wyszukiwania dane są przeszukiwane z nierozwiniętymi makrami.

Link *Filtr* jest dostępny nad listą skryptów. Po jego kliknięciu pojawi się filtr, w którym można filtrować skrypty według nazwy i zakresu.



Konfigurowanie skryptu globalnego



Note:
Zaleca się używanie funkcji makr zamiast zwykłych makr w skryptach globalnych w celu zwiększenia bezpieczeństwa, ponieważ makra nie są automatycznie poprzedzane znakami ucieczki.

Atrybuty skryptu:

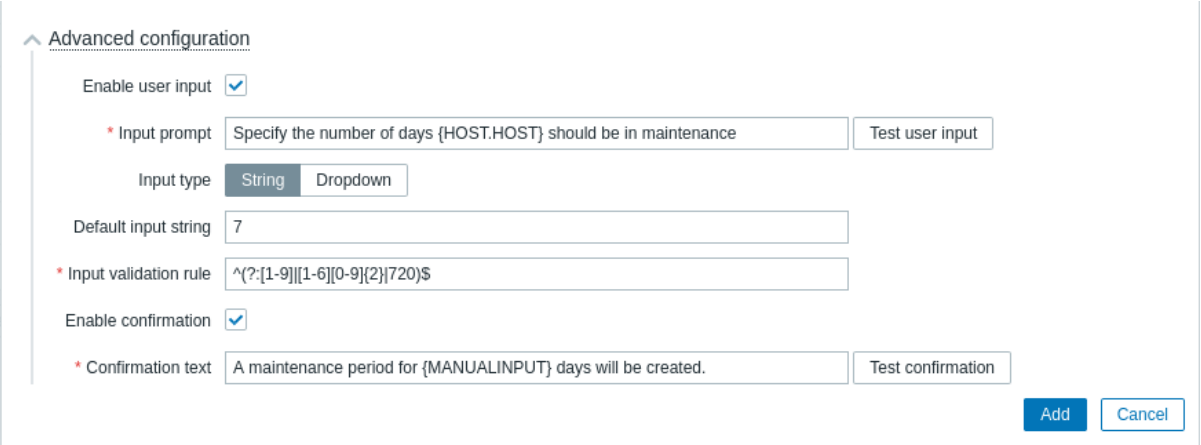
Parametr	Opis
Nazwa	Unikalna nazwa skryptu. Np. `Clear /tmp filesystem`
Zakres	Zakres skryptu — operacja akcji, ręczna akcja hosta lub ręczna akcja zdarzenia. To ustawienie określa, gdzie skrypt może być używany — odpowiednio w zdalnych poleceniach operacji akcji, z menu hosta lub z menu zdarzenia. Ustawienie zakresu na „Operacja akcji" powoduje, że skrypt jest dostępny dla wszystkich użytkowników mających dostęp do *Alerty* > *Akcje*. Jeśli skrypt jest faktycznie używany w akcji, jego zakres nie może zostać zmieniony z „operacja akcji" na inny. **Obsługa makr** Zakres wpływa na zakres dostępnych makr. Na przykład makra związane z użytkownikiem ({USER.*}) są obsługiwane w skryptach, aby umożliwić przekazywanie informacji o użytkowniku, który uruchomił skrypt. Nie są one jednak obsługiwane, jeśli zakresem skryptu jest operacja akcji, ponieważ operacje akcji są wykonywane automatycznie. Makro {MANUALINPUT} umożliwia określenie ręcznego wejścia w czasie wykonywania skryptu. Jest ono obsługiwane dla skryptów ręcznej akcji hosta i ręcznej akcji zdarzenia. Aby sprawdzić, które inne makra są obsługiwane, wyszukaj „Trigger-based notifications and commands/Trigger-based commands", „Manual host action scripts" oraz „Manual event action scripts" w tabeli obsługiwanych makr. Pamiętaj, że jeśli makro może zostać rozwinięte do wartości zawierającej spacje (na przykład nazwa hosta), należy je odpowiednio ująć w cudzysłów.
Ścieżka menu	Żądana ścieżka menu do skryptu. Na przykład `Default` lub `Default/` spowoduje wyświetlenie skryptu w odpowiednim katalogu. Menu mogą być zagnieżdżone, np. `Main menu/Sub menu1/Sub menu2`. Podczas uzyskiwania dostępu do skryptów przez menu hosta/zdarzenia w sekcjach monitorowania będą one uporządkowane zgodnie z podanymi katalogami. To pole jest wyświetlane tylko wtedy, gdy jako *Zakres* wybrano „Ręczna akcja hosta" lub „Ręczna akcja zdarzenia".

Parametr	Opis
Typ	Kliknij odpowiedni przycisk, aby wybrać typ skryptu: **URL**, **Webhook**, **Skrypt**, **SSH**, **Telnet** lub polecenie **IPMI**. Typ **URL** jest dostępny tylko wtedy, gdy jako *Zakres* wybrano „Ręczna akcja hosta” lub „Ręczna akcja zdarzenia”.
Typ skryptu: **URL**	
URL	Określ adres URL do szybkiego dostępu z menu hosta lub menu zdarzenia. Obsługiwane są makra oraz niestandardowe makra użytkownika. Obsługa makr zależy od zakresu skryptu (zobacz *Zakres* powyżej). Użyj makra {MANUALINPUT} w tym polu, aby móc określić ręczne wejście w czasie wykonywania skryptu, na przykład: `http://{MANUALINPUT}/zabbix/zabbix.php?action=dashboard.view` Wartości makr nie mogą być kodowane URL.
Otwórz w nowym oknie	Określa, czy adres URL powinien zostać otwarty w nowej karcie przeglądarki, czy w tej samej.
Typ skryptu: **Webhook**	
Parametry	Określ zmienne webhooka jako pary atrybut-wartość. Zobacz także: konfiguracja mediów Webhook. W wartościach parametrów obsługiwane są makra oraz niestandardowe makra użytkownika. Obsługa makr zależy od zakresu skryptu (zobacz *Zakres* powyżej).
Skrypt	Wprowadź kod JavaScript w modalnym edytorze, który otwiera się po kliknięciu w pole parametru lub ikonę ołówka obok niego. Obsługa makr zależy od zakresu skryptu (zobacz *Zakres* powyżej). Zobacz także: konfiguracja mediów Webhook, Dodatkowe obiekty Javascript.
Limit czasu	Limit czasu wykonania JavaScript (1-60s, domyślnie 30s). Obsługiwane są przyrostki czasu, np. 30s, 1m.
Typ skryptu: **Skrypt**	
Wykonaj na	Kliknij odpowiedni przycisk, aby wykonać skrypt powłoki na: **Zabbix agent** — skrypt zostanie wykonany przez Zabbix agent (jeśli pozycja system.run jest dozwolona) na hoście **Zabbix proxy lub serwer** — skrypt zostanie wykonany przez Zabbix proxy lub serwer — w zależności od tego, czy host jest monitorowany przez proxy czy serwer. Zostanie wykonany na proxy, jeśli jest to włączone przez EnableRemoteCommands. Zostanie wykonany na serwerze, jeśli skrypty globalne są włączone przez parametr serwera EnableGlobalScripts. **Zabbix serwer** — skrypt zostanie wykonany tylko przez Zabbix serwer. Ta opcja nie będzie dostępna, jeśli skrypty globalne są wyłączone przez parametr serwera EnableGlobalScripts.
Polecenia	Wprowadź pełną ścieżkę do poleceń, które mają zostać wykonane w ramach skryptu. Obsługa makr zależy od zakresu skryptu (zobacz *Zakres* powyżej). Obsługiwane są niestandardowe makra użytkownika.
Typ skryptu: **SSH**	
Metoda uwierzytelniania	Wybierz metodę uwierzytelniania — hasło lub klucz publiczny.
Nazwa użytkownika	Wprowadź nazwę użytkownika.
Hasło	Wprowadź hasło. To pole jest dostępne, jeśli jako metodę uwierzytelniania wybrano „Hasło”.
Plik klucza publicznego	Wprowadź ścieżkę do pliku klucza publicznego. To pole jest dostępne, jeśli jako metodę uwierzytelniania wybrano „Klucz publiczny”.
Plik klucza prywatnego	Wprowadź ścieżkę do pliku klucza prywatnego. To pole jest dostępne, jeśli jako metodę uwierzytelniania wybrano „Klucz publiczny”.
Hasło klucza	Wprowadź hasło klucza. To pole jest dostępne, jeśli jako metodę uwierzytelniania wybrano „Klucz publiczny”.
Port	Wprowadź port zdalnej usługi SSH na docelowym hoście, z którym Zabbix ma się połączyć.
Polecenia	Wprowadź polecenia. Obsługa makr zależy od zakresu skryptu (zobacz *Zakres* powyżej). Obsługiwane są niestandardowe makra użytkownika.
Typ skryptu: **Telnet**	
Nazwa użytkownika	Wprowadź nazwę użytkownika.
Hasło	Wprowadź hasło.
Port	Wprowadź port zdalnej usługi Telnet na docelowym hoście, z którym Zabbix ma się połączyć.
Polecenia	Wprowadź polecenia. Obsługa makr zależy od zakresu skryptu (zobacz *Zakres* powyżej). Obsługiwane są niestandardowe makra użytkownika.

Parametr	Opis
Typ skryptu: **IPMI**	
Polecenie	Wprowadź polecenie IPMI. Obsługa makr zależy od zakresu skryptu (zobacz *Zakres* powyżej). Obsługiwane są niestandardowe makra użytkownika.
Opis	Wprowadź opis skryptu.
Grupa hostów	Wybierz grupę hostów, dla której skrypt będzie dostępny (lub *Wszystkie* dla wszystkich grup hostów).
Grupa użytkowników	Wybierz grupę użytkowników, dla której skrypt będzie dostępny (lub *Wszystkie* dla wszystkich grup użytkowników). To pole jest wyświetlane tylko wtedy, gdy jako *Zakres* wybrano „Ręczna akcja hosta” lub „Ręczna akcja zdarzenia”.
Wymagane uprawnienia do hosta	Wybierz poziom uprawnień dla grupy hostów — *Odczyt* lub *Zapis*. Tylko użytkownicy z wymaganym poziomem uprawnień będą mieli dostęp do wykonywania skryptu. To pole jest wyświetlane tylko wtedy, gdy jako *Zakres* wybrano „Ręczna akcja hosta” lub „Ręczna akcja zdarzenia”.
Konfiguracja zaawansowana	Kliknij etykietę *Konfiguracja zaawansowana*, aby wyświetlić opcje konfiguracji zaawansowanej. To pole jest wyświetlane tylko wtedy, gdy jako *Zakres* wybrano „Ręczna akcja hosta” lub „Ręczna akcja zdarzenia”.

Konfiguracja zaawansowana

Opcje konfiguracji zaawansowanej są dostępne w zwijanej sekcji *Konfiguracja zaawansowana*:



Parametr	Opis
Włącz dane wejściowe użytkownika	Zaznacz pole wyboru, aby włączyć ręczne wprowadzanie danych przez użytkownika przed wykonaniem skryptu. Ręcznie wprowadzone dane zastąpią wartość makra {MANUALINPUT} w skrypcie. Zobacz także: Ręczne dane wejściowe użytkownika.
Monit wejściowy	Wprowadź własny tekst zachęcający do podania danych przez użytkownika. Ten tekst będzie wyświetlany nad polem wejściowym w wyskakującym oknie *Ręczne dane wejściowe*. Aby zobaczyć podgląd wyskakującego okna *Ręczne dane wejściowe*, kliknij *Testuj dane wejściowe użytkownika*. Podgląd umożliwia także sprawdzenie, czy ciąg wejściowy jest zgodny z regułą walidacji danych wejściowych (zobacz parametry poniżej). Obsługa makr i makr użytkownika zależy od zakresu skryptu (zobacz *Zakres* w ogólnych parametrach konfiguracji skryptu).
Typ danych wejściowych	Wybierz typ ręcznie wprowadzanych danych: **Ciąg znaków** — pojedynczy ciąg znaków; **Lista rozwijana** — wartość jest wybierana z wielu opcji listy rozwijanej.
Opcje listy rozwijanej	Wprowadź unikalne wartości dla listy rozwijanej danych wejściowych użytkownika jako listę rozdzielaną przecinkami. Aby uwzględnić pustą opcję na liście rozwijanej, dodaj dodatkowy przecinek na początku, w środku lub na końcu listy. To pole jest wyświetlane tylko wtedy, gdy jako *Typ danych wejściowych* wybrano „Lista rozwijana”.

Parametr	Opis
Domyślny ciąg wejściowy	Wprowadź domyślny ciąg dla danych wejściowych użytkownika (lub pozostaw puste). To pole będzie walidowane względem wyrażenia regularnego podanego w polu *Reguła walidacji danych wejściowych*. Wartość wprowadzona tutaj będzie domyślnie wyświetlana w wyskakującym oknie *Ręczne dane wejściowe*. To pole jest wyświetlane tylko wtedy, gdy jako *Typ danych wejściowych* wybrano „Ciąg znaków”.
Reguła walidacji danych wejściowych	Wprowadź wyrażenie regularne do walidacji ciągu danych wejściowych użytkownika. Obsługiwane są globalne wyrażenia regularne. To pole jest wyświetlane tylko wtedy, gdy jako *Typ danych wejściowych* wybrano „Ciąg znaków”.
Włącz potwierdzenie	Zaznacz pole wyboru, aby przed wykonaniem skryptu wyświetlić komunikat potwierdzający. Ta funkcja może być szczególnie przydatna w przypadku potencjalnie niebezpiecznych operacji (takich jak skrypt restartu) lub takich, które mogą zająć dużo czasu.
Tekst potwierdzenia	Wprowadź własny tekst potwierdzenia dla wyskakującego okna potwierdzenia włączonego za pomocą powyższego pola wyboru (na przykład *Zdalny system zostanie uruchomiony ponownie. Czy na pewno?*). Aby zobaczyć, jak tekst będzie wyglądał, kliknij *Testuj potwierdzenie* obok pola. Obsługiwane są makra oraz niestandardowe makra użytkownika. *Uwaga:* makra nie będą rozwijane podczas testowania komunikatu potwierdzenia.

Jeśli skonfigurowano zarówno ręczne dane wejściowe użytkownika, jak i komunikat potwierdzenia, zostaną one wyświetlone kolejno w następujących po sobie wyskakujących oknach.

Ręczne dane wejściowe użytkownika

Ręczne dane wejściowe użytkownika pozwalają podać własny parametr przy każdym uruchomieniu skryptu. Eliminuje to konieczność tworzenia wielu podobnych skryptów użytkownika różniących się tylko jednym parametrem.

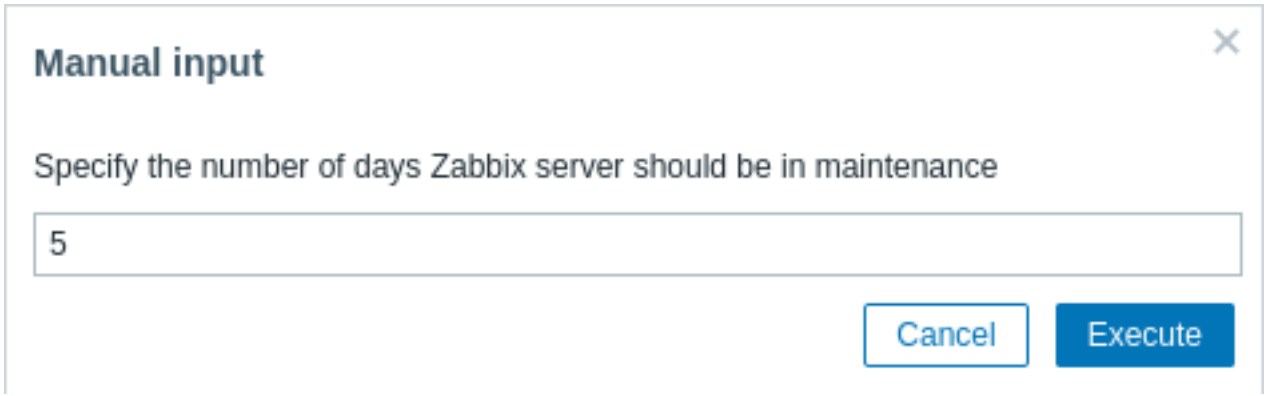
Na przykład podczas uruchamiania skryptu można chcieć podać inną liczbę całkowitą lub inny adres URL.

Aby włączyć ręczne dane wejściowe użytkownika:

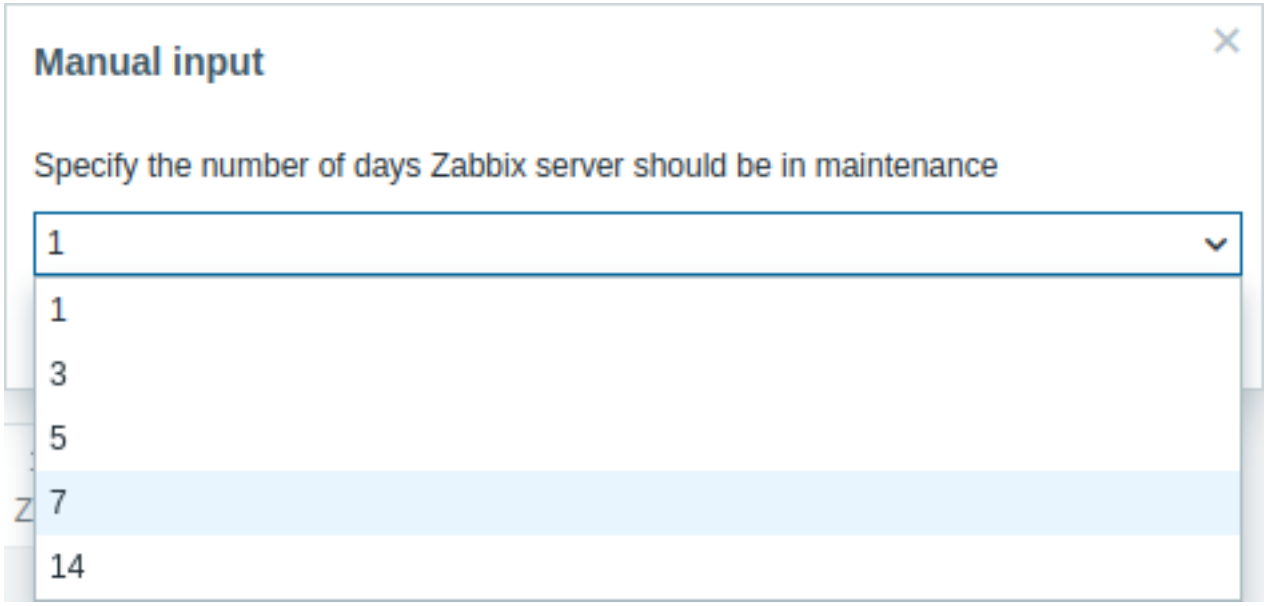
- użyj makra {MANUALINPUT} w skrypcie (polecenia, skrypt, parametr skryptu) tam, gdzie jest to wymagane; lub w polu URL w skryptach URL;
- w zaawansowanej konfiguracji skryptu włącz ręczne dane wejściowe użytkownika i skonfiguruj opcje wejściowe.

Po włączeniu danych wejściowych użytkownika, przed wykonaniem skryptu użytkownikowi zostanie wyświetlone wyskakujące okno *Ręczne dane wejściowe* z prośbą o podanie własnej wartości. Podana wartość zastąpi {MANUALINPUT} w skrypcie.

W zależności od konfiguracji użytkownik zostanie poproszony o wprowadzenie wartości tekstowej:



Lub o wybranie wartości z listy rozwijanej wcześniej zdefiniowanych opcji:



Ręczne dane wejściowe użytkownika są dostępne tylko dla skryptów, w których zakres to „Ręczna akcja hosta” lub „Ręczna akcja zdarzenia”.

Wykonywanie skryptu i wynik

Skrypty uruchamiane przez serwer Zabbix są wykonywane w kolejności opisanej na stronie wykonywania poleceń.

Wynik skryptu jest wyświetlany w wyskakującym oknie, które pojawia się po uruchomieniu skryptu. Wartością zwracaną skryptu jest standardowe wyjście:

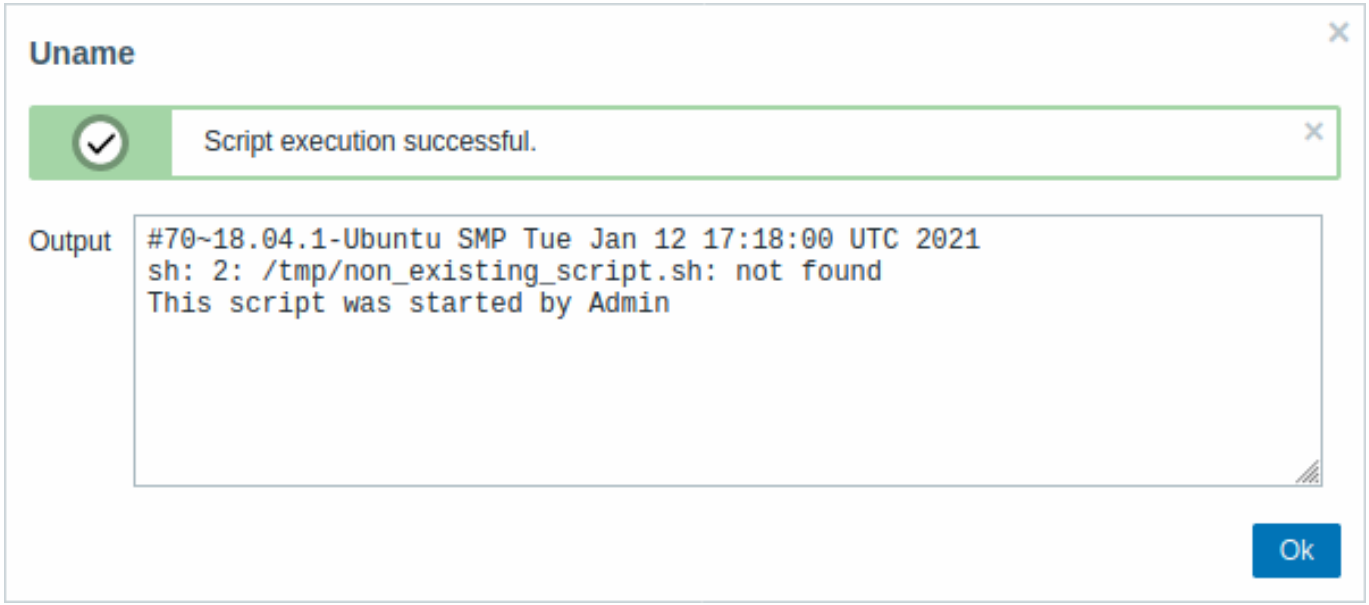
- Jeśli skrypt zakończy się pomyślnie (kod wyjścia 0), wartość zwracana jest ograniczona do 16 MB (włącznie z końcowymi białymi znakami, które są obcinane).
- Jeśli skrypt zakończy się błędem (niezerowy kod wyjścia), wartością zwracaną jest standardowe wyjście błędów ograniczone do 2 KB.

Domyślnie Zabbix nie przechowuje rozszerzonego wyjścia skryptu. Aby zachować pełne szczegóły wyjścia, można zaimplementować rejestrowanie w samym skrypcie (np. przekierować wyjście do lokalnego pliku dziennika).

Należy pamiętać, że w przypadku skryptów wykonywanych zarówno na serwerze Zabbix, jak i na Zabbix proxy, obowiązują również ograniczenia bazy danych.

Poniżej znajduje się przykład skryptu i okna wyniku:

```
uname -v
/tmp/non_existing_script.sh
echo "This script was started by {USER.USERNAME}"
```



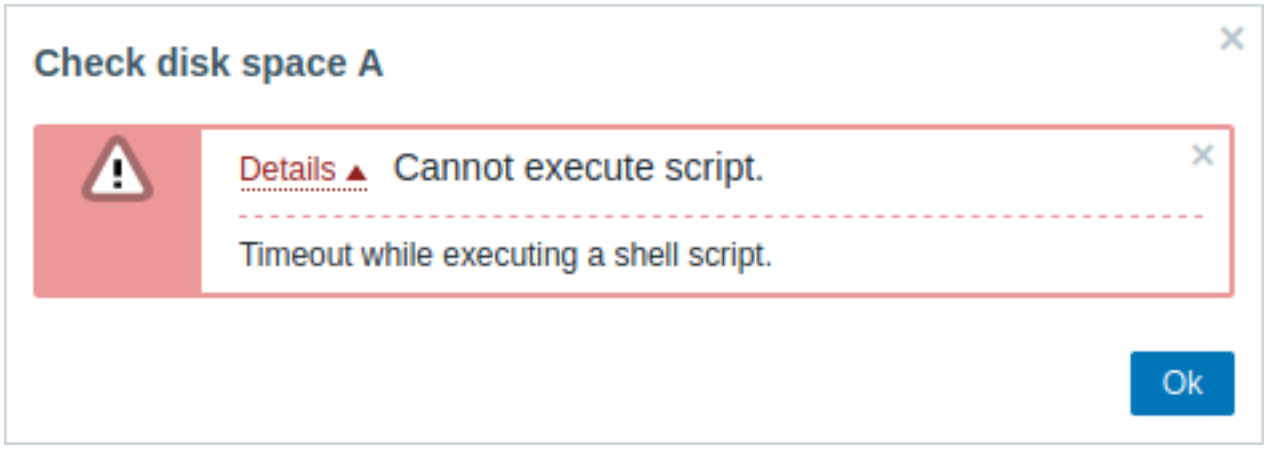
Wynik skryptu nie wyświetla samego skryptu.

Zabbix agent

Możesz napotkać sytuację, w której podczas wykonywania skryptu wystąpi przekroczenie limitu czasu.

Poniżej przedstawiono przykład skryptu uruchamianego przez Zabbix agent oraz okno z wynikiem:

```
sleep 5
df -h
```



Komunikat o błędzie w tym przypadku jest następujący:

```
Timeout while executing a shell script.
```

Aby uniknąć takich sytuacji, zaleca się zoptymalizowanie samego skryptu (w powyższym przykładzie „5") zamiast dostosowywania parametru `Timeout` w konfiguracji Zabbix agent oraz konfiguracji Zabbix serwer. Jednak w przypadku Zabbix agent w trybie aktywnym parametr `Timeout` w konfiguracji Zabbix serwer powinien być co najmniej o kilka sekund dłuższy niż parametr `RefreshActiveChecks` w konfiguracji Zabbix agent. Zapewnia to serwerowi wystarczającą ilość czasu na odebranie wyników aktywnych testów od agenta. Należy pamiętać, że wykonywanie skryptów na aktywnym agencie jest obsługiwane od wersji Zabbix agent 7.0.

Jeśli parametr `Timeout` został zmieniony w konfiguracji Zabbix agent, pojawi się następujący komunikat o błędzie:

```
Get value from agent failed: ZBX_TCP_READ() timed out.
```

Oznacza to, że zmiana została wprowadzona w konfiguracji Zabbix agent, ale konieczne jest również zmodyfikowanie parametru `Timeout` w konfiguracji Zabbix serwer.

Script timeout on active agents

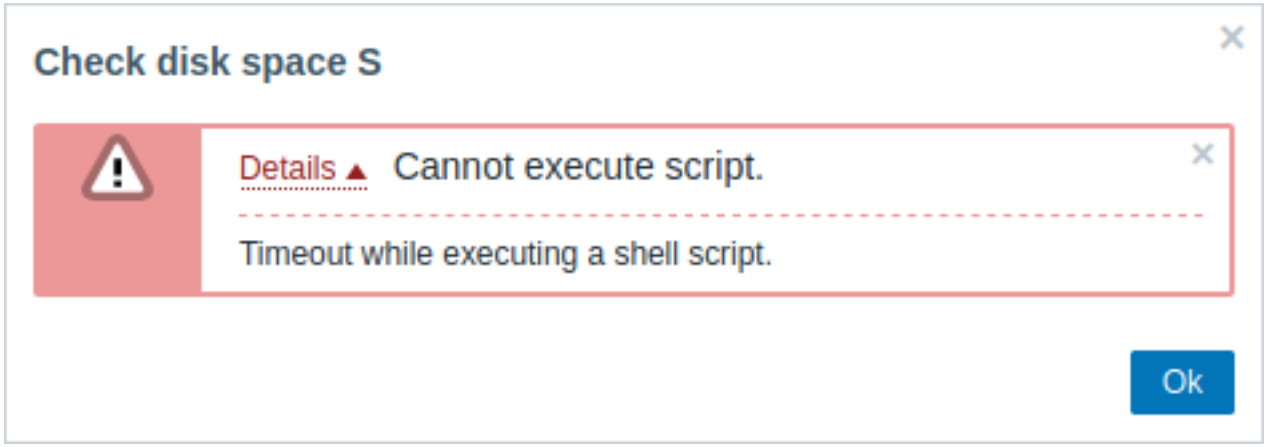
It is possible to execute scripts on agents operating in active mode only. Once the script execution is triggered by action operation or manual script execution, the command is included in active check configuration and executed once the active agent receives it.

These scripts are sent to the active agent along with the server/proxy timeout for script execution. Please increase the default server/proxy timeout for script execution. The timeout must be higher than the active check refresh frequency, otherwise the timeout is exceeded before the active agent receives the script and is able to return the result.

Serwer/proxy Zabbix

Poniżej przedstawiono przykład skryptu uruchamianego na serwerze/proxy Zabbix oraz okno z wynikiem:

```
sleep 11
df -h
```



Zaleca się również zoptymalizowanie samego skryptu (zamiast dostosowywania parametru `TrapperTimeout` do odpowiedniej wartości (w naszym przypadku > 11)) poprzez modyfikację konfiguracji serwera Zabbix.

8 Użytkownicy

Przegląd

To menu zawiera sekcje związane z konfiguracją użytkowników w Zabbix. To menu jest dostępne tylko dla użytkowników typu SuperAdmin.

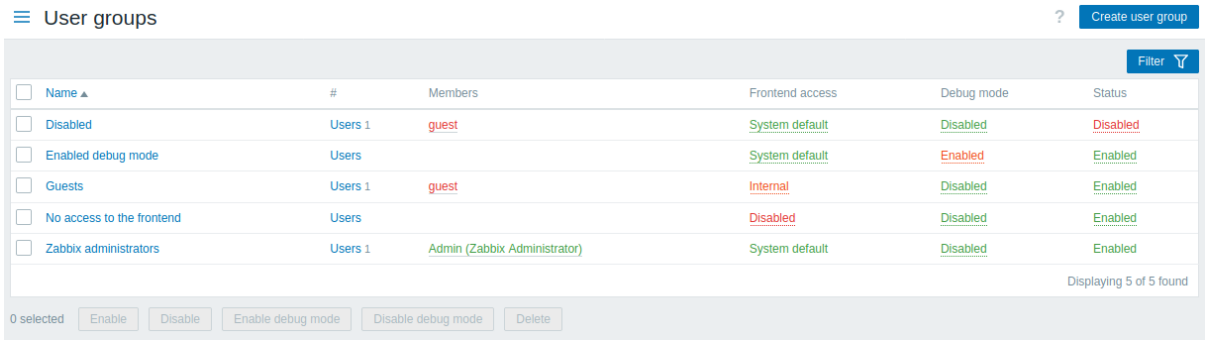
1 Grupy użytkowników

Przegląd

W sekcji *Użytkownicy* → *Grupy użytkowników* zarządza się grupami użytkowników systemu.

Grupy użytkowników

Wyświetlana jest lista istniejących grup użytkowników wraz z ich szczegółami.



Wyświetlane dane:

Column	Description
Name	Nazwa grupy użytkowników. Kliknięcie nazwy grupy użytkowników otwiera formularz konfiguracji grupy użytkowników.
#	Liczba użytkowników w grupie. Kliknięcie *Users* spowoduje wyświetlenie odpowiednich użytkowników odfiltrowanych na liście użytkowników.
Members	Nazwy użytkowników poszczególnych użytkowników w grupie użytkowników (z imieniem i nazwiskiem w nawiasach). Kliknięcie nazwy użytkownika otworzy formularz konfiguracji użytkownika. Użytkownicy z wyłączonych grup są wyświetlani na czerwono.

Column	Description
Frontend access	Wyświetlany jest poziom dostępu do frontend: **System default** - użytkownicy są uwierzytelniani przez Zabbix, LDAP lub HTTP (w zależności od metody authentication ustawionej globalnie); **Internal** - użytkownicy są uwierzytelniani przez Zabbix; ignorowane, jeśli uwierzytelnianie HTTP jest globalnym ustawieniem domyślnym; **LDAP** - użytkownicy są uwierzytelniani przez LDAP; ignorowane, jeśli uwierzytelnianie HTTP jest globalnym ustawieniem domyślnym; **Disabled** - dostęp do frontend Zabbix jest zabroniony dla tej grupy. Klikając bieżący poziom, można go zmienić.
Debug mode	Wyświetlany jest stan trybu debugowania - *Enabled* lub *Disabled*. Klikając stan, można go zmienić.
Status	Wyświetlany jest status grupy użytkowników - *Enabled* lub *Disabled*. Klikając status, można go zmienić.

Aby skonfigurować nową grupę użytkowników, kliknij przycisk *Create user group* w prawym górnym rogu.

Opcje masowej edycji

Przyciski pod listą oferują kilka opcji masowej edycji:

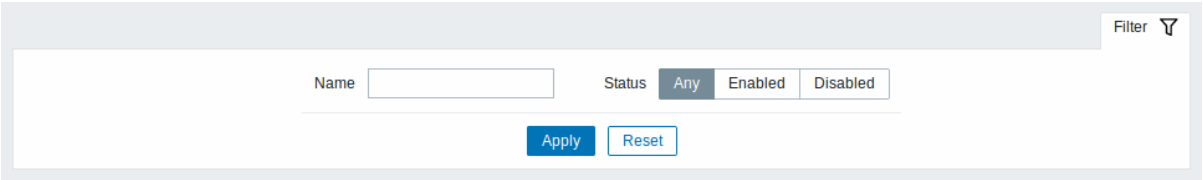
- *Włącz* — zmienia status grupy użytkowników na *Włączona*
- *Wyłącz* — zmienia status grupy użytkowników na *Wyłączona*
- *Włącz tryb debugowania* — włącza tryb debugowania dla grup użytkowników
- *Wyłącz tryb debugowania* — wyłącza tryb debugowania dla grup użytkowników
- *Usuń* — usuwa grupy użytkowników

Aby użyć tych opcji, zaznacz pola wyboru przy odpowiednich grupach użytkowników, a następnie kliknij wymagany przycisk.

Używanie filtra

Możesz użyć filtra, aby wyświetlić tylko te grupy użytkowników, które Cię interesują. Dla lepszej wydajności wyszukiwania dane są przeszukiwane z nierozwiniętymi makrami.

Link *Filtr* jest dostępny nad listą grup użytkowników. Po jego kliknięciu pojawi się filtr, w którym można filtrować grupy użytkowników według nazwy i statusu.



2 Role użytkowników

Przegląd

W sekcji *Użytkownicy* > *Role użytkowników* można tworzyć role użytkowników.

Role użytkowników umożliwiają tworzenie szczegółowych uprawnień na podstawie początkowo wybranego typu użytkownika (*User*, *Admin*, *Super admin*).

Po wybraniu typu użytkownika wszystkie dostępne uprawnienia dla tego typu użytkownika są przyznawane (domyślnie zaznaczone).

Uprawnienia można jedynie odebrać z podzbioru dostępnego dla danego typu użytkownika; nie można ich rozszerzyć poza zakres dostępny dla tego typu użytkownika.

Pola wyboru dla niedostępnych uprawnień są wyszarzone; użytkownicy nie będą mogli uzyskać dostępu do elementu nawet przez wpisanie bezpośredniego adresu URL tego elementu w przeglądarce.

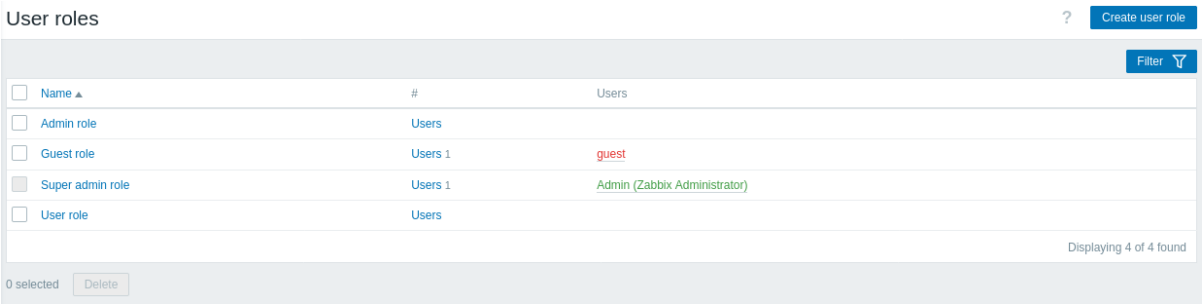
Note:
Ograniczenie dostępu do niektórych elementów interfejsu użytkownika zapobiega jedynie otwarciu tej strony — nie usuwa możliwości dostępu do danych bazowych w innych częściach interfejsu.

Role użytkowników można przypisywać użytkownikom systemu. Każdy użytkownik może mieć przypisaną tylko jedną rolę.

Domyślne role użytkowników

Domyślnie Zabbix jest skonfigurowany z czterema rolami użytkowników, które mają wstępnie zdefiniowany zestaw uprawnień:

- Rola Gość
- Rola Użytkownik
- Rola Administrator
- Rola Super administrator

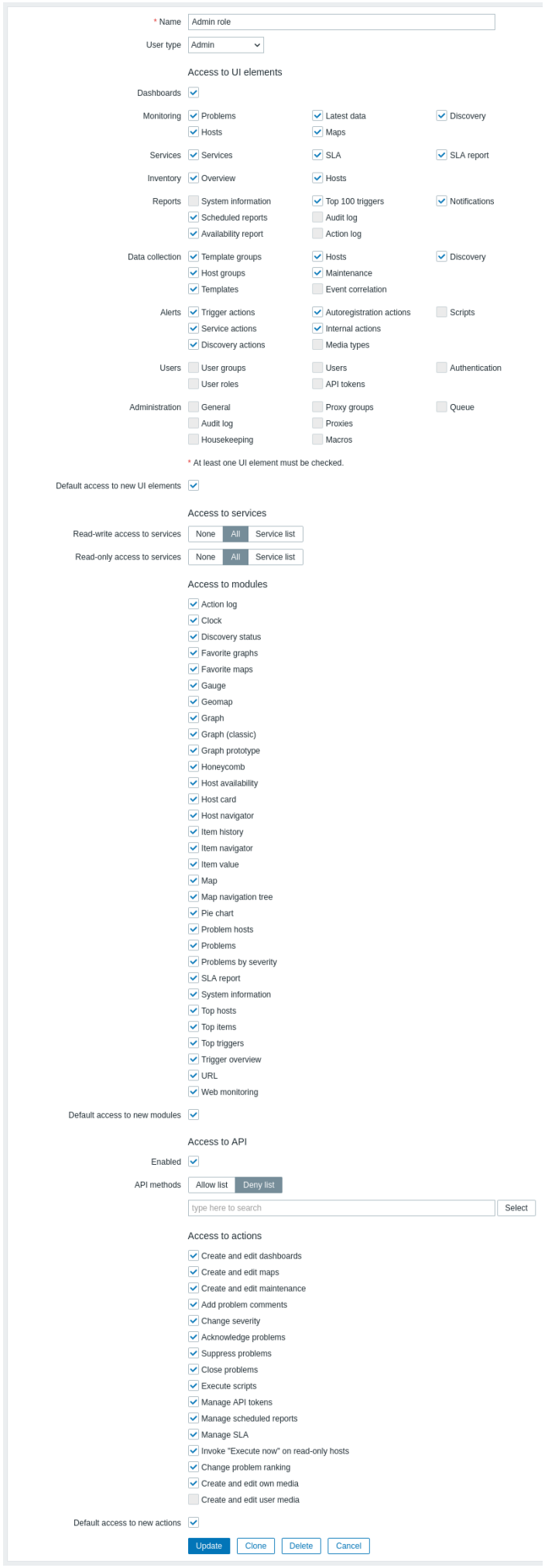


Są one oparte na głównych typach użytkowników w Zabbix. Wyświetlana jest lista wszystkich użytkowników przypisanych do danej roli. Użytkownicy należący do wyłączonych grup są oznaczeni na czerwono. *Rola Gość* jest rolą typu użytkownika z jedynymi uprawnieniami do przeglądania niektórych sekcji frontend.

Note:
Domyślna *Rola Super administrator* nie może być modyfikowana ani usunięta, ponieważ w Zabbix musi istnieć co najmniej jeden użytkownik Super administrator z nieograniczonymi uprawnieniami. Użytkownicy typu *Super administrator* mogą modyfikować ustawienia własnej roli, ale nie typ użytkownika.

Konfiguracja

Aby utworzyć nową rolę, kliknij przycisk *Create user role* w prawym górnym rogu. Aby zaktualizować istniejącą rolę, kliknij nazwę roli, aby otworzyć formularz konfiguracji.


* Name
Admin role
User type
Admin
Access to UI elements
Dashboards
Monitoring
Problems
Latest data
Discovery
Hosts
Maps
Services
Services
SLA
SLA report
Inventory
Overview
Hosts
Reports
System information
Top 100 triggers
Notifications
Scheduled reports
Audit log
Availability report
Action log
Data collection
Template groups
Hosts
Discovery
Host groups
Maintenance
Templates
Event correlation
Alerts
Trigger actions
Autoregistration actions
Scripts
Service actions
Internal actions
Discovery actions
Media types
Users
User groups
Users
Authentication
User roles
API tokens
Administration
General
Proxy groups
Queue
Audit log
Proxies
Housekeeping
Macros
* At least one UI element must be checked.
Default access to new UI elements
Access to services
Read-write access to services
None
All
Service list
Read-only access to services
None
All
Service list
Access to modules
Action log
Clock
Discovery status
Favorite graphs
Favorite maps
Gauge
Geomap
Graph
Graph (classic)
Graph prototype
Honeycomb
Host availability
Host card
Host navigator
Item history
Item navigator
Item value
Map
Map navigation tree
Pie chart
Problem hosts
Problems
Problems by severity
SLA report
System information
Top hosts
Top items
Top triggers
Trigger overview
URL
Web monitoring
Default access to new modules
Access to API
Enabled
API methods
Allow list
Deny list
type here to search
Select
Access to actions
Create and edit dashboards
Create and edit maps
Create and edit maintenance
Add problem comments
Change severity
Acknowledge problems
Suppress problems
Close problems
Execute scripts
Manage API tokens
Manage scheduled reports
Manage SLA
Invoke "Execute now" on read-only hosts
Change problem ranking
Create and edit own media
Create and edit user media
Default access to new actions
Update
Clone
Delete
Cancel

Wyświetlane są dostępne uprawnienia. Aby cofnąć określone uprawnienie, odznacz jego pole wyboru.

Dostępne uprawnienia wraz z wartościami domyślnymi dla każdej wstępnie skonfigurowanej roli użytkownika w Zabbix opisano poniżej.

Domyślne uprawnienia

Dostęp do elementów interfejsu użytkownika

Domyślny dostęp do sekcji menu zależy od typu użytkownika. Zobacz stronę Uprawnienia, aby uzyskać szczegóły.

Dostęp do innych opcji

Parametr	**Opis**	**Domyślne role użytkowników**			
		Rola Super admin	*Rola Admin*	*Rola User*	*Rola Guest*
Domyślny dostęp do nowych elementów interfejsu użytkownika	Ta opcja określa, jak nowe sekcje menu będą dostępne po aktualizacji Zabbix. Istniejące sekcje menu modułów pozostają bez zmian.	Tak	Tak	Tak	Tak
Dostęp do usług					
Dostęp do usług do odczytu i zapisu	Wybierz dostęp do usług do odczytu i zapisu: **Brak** - brak dostępu **Wszystkie** - dostęp do wszystkich usług w trybie odczytu i zapisu **Lista usług** - wybierz usługi z dostępem do odczytu i zapisu Dostęp do odczytu i zapisu, jeśli zostanie przyznany, ma pierwszeństwo przed ustawieniami dostępu tylko do odczytu i jest dynamicznie dziedziczony przez usługi podrzędne.	Wszystkie	Wszystkie	Brak	Brak
Dostęp do usług do odczytu i zapisu z tagiem	Określ nazwę tagu oraz opcjonalnie jego wartość, aby dodatkowo przyznać dostęp do odczytu i zapisu do usług pasujących do tagu. Ta opcja jest dostępna, jeśli w parametrze *Dostęp do usług do odczytu i zapisu* wybrano „Lista usług”. Dostęp do odczytu i zapisu, jeśli zostanie przyznany, ma pierwszeństwo przed ustawieniami dostępu tylko do odczytu i jest dynamicznie dziedziczony przez usługi podrzędne.				

Dostęp do usług tylko do odczytu	Wybierz dostęp do usług tylko do odczytu: **Brak** - brak dostępu **Wszystkie** - dostęp do wszystkich usług tylko do odczytu **Lista usług** - wybierz usługi z dostępem tylko do odczytu Dostęp tylko do odczytu nie ma pierwszeństwa przed dostępem do odczytu i zapisu i jest dynamicznie dziedziczony przez usługi podrzędne.			Wszystkie	Wszystkie
Dostęp do usług tylko do odczytu z tagiem	Określ nazwę tagu oraz opcjonalnie jego wartość, aby dodatkowo przyznać dostęp tylko do odczytu do usług pasujących do tagu. Ta opcja jest dostępna, jeśli w parametrze *Dostęp do usług tylko do odczytu* wybrano „Lista usług”. Dostęp tylko do odczytu nie ma pierwszeństwa przed dostępem do odczytu i zapisu i jest dynamicznie dziedziczony przez usługi podrzędne.				
Dostęp do modułów					
<Nazwa modułu>	Zezwól/zabroń dostępu do określonego modułu. W tej sekcji wyświetlane są tylko włączone moduły. Nie można przyznać ani ograniczyć dostępu do modułu, który jest obecnie wyłączony.	Tak	Tak	Tak	Tak
Domyślny dostęp do nowych modułów	Ta opcja określa, jak nowe moduły i widgety będą dostępne po aktualizacji Zabbix. Dotyczy to również modułów i widgetów dodanych w sekcji *Administracja* > *Ogólne* > *Moduły*.				
Dostęp do API					
Włączone Metody API	Włącz/wyłącz dostęp do API. Wybierz *Listę dozwolonych*, aby zezwolić, lub *Listę zabronionych*, aby zabronić metod API określonych w polu wyszukiwania. Pamiętaj, że nie można zezwolić na niektóre metody API i jednocześnie zabronić innych. W polu wyszukiwania zacznij wpisywać nazwę metody, a następnie wybierz metodę z listy autouzupełniania. Możesz także nacisnąć przycisk Wybierz i wybrać metody z pełnej listy dostępnej dla tego typu użytkownika. Pamiętaj, że jeśli określone działanie w bloku Dostęp do działań jest odznaczone, użytkownicy nie będą mogli używać metod API powiązanych z tym działaniem. Obsługiwane są symbole wieloznaczne. Przykłady: `dashboard.*` (wszystkie metody usługi API „dashboard.”) `*` (dowolna metoda), `*.export` (metody o nazwie „.export” ze wszystkich usług API). Jeśli nie określono żadnych metod, reguła *Lista dozwolonych/zabronionych* zostanie zignorowana.	Tak	Tak	Tak	Nie
Dostęp do działań					

Tworzenie i edycja pulpitów	Wyczyszczenie tego pola wyboru spowoduje również odebranie praw do używania metod API `.create`, `.update` i `.delete` dla odpowiednich elementów.	Tak	Tak	Tak	Nie
Tworzenie i edycja map					
Tworzenie i edycja okresów konserwacji				Nie	
Dodawanie komentarzy do problemów	Wyczyszczenie tego pola wyboru spowoduje również odebranie praw do wykonania odpowiedniego działania za pomocą metody API `event.acknowledge`.			Tak	
Zmiana ważności					
Potwierdzanie problemów					
Tłumienie problemów					
Zamykanie problemów					
Wykonywanie skryptów	Wyczyszczenie tego pola wyboru spowoduje również odebranie praw do używania metody API `script.execute`.				
Zarządzanie tokenami API	Wyczyszczenie tego pola wyboru spowoduje również odebranie praw do używania wszystkich metod API `token.*`.				
Zarządzanie zaplanowanymi raportami	Wyczyszczenie tego pola wyboru spowoduje również odebranie praw do używania wszystkich metod API `report.*`.			Nie	
Zarządzanie SLA	Włącz/wyłącz prawa do zarządzania SLA.				
Wywoływanie „Wykonaj teraz” na hostach tylko do odczytu	Zezwól na używanie opcji „Wykonaj teraz” w najnowszych danych dla pozycji hostów tylko do odczytu.			Tak	
Zmiana rankingu problemu	Zezwól na zmianę rankingu problemu z przyczyny na symptom i odwrotnie.				
Tworzenie i edycja własnych mediów	Zezwól na tworzenie/edycję własnych mediów.				
Tworzenie i edycja mediów użytkowników	Zezwól na tworzenie/edycję mediów dla użytkowników. Ta opcja jest dostępna tylko dla użytkowników Super admin.		Nie	Nie	
Domyślny dostęp do nowych działań	Ta opcja określa, jak nowe działania będą dostępne po aktualizacji Zabbix.		Tak	Tak	

Zobacz także:

- Konfigurowanie użytkownika

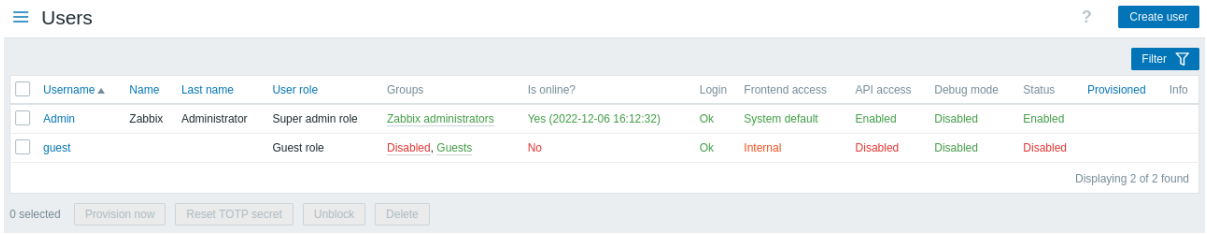
3 Użytkownicy

Przegląd

W sekcji *Użytkownicy* → *Użytkownicy* zarządza się użytkownikami systemu.

Użytkownicy

Wyświetlana jest lista istniejących użytkowników wraz z ich szczegółami.



Wyświetlane dane:

Column	Description
Username	Nazwa użytkownika służąca do logowania do Zabbix. Kliknięcie nazwy użytkownika otwiera formularz konfiguracji użytkownika.
Name	Imię użytkownika.
Last name	Nazwisko użytkownika.
User role	Wyświetlana jest rola użytkownika.
Groups	Wyświetlane są grupy, do których należy użytkownik. Kliknięcie nazwy grupy użytkowników otwiera formularz konfiguracji grupy użytkowników. Wyłączone grupy są wyświetlane na czerwono.
Is online?	Wyświetlany jest status dostępności użytkownika online - *Yes* lub *No*. W nawiasach wyświetlany jest czas ostatniej aktywności użytkownika.
Login	Wyświetlany jest status logowania użytkownika - *Ok* lub *Blocked*. Użytkownik może zostać tymczasowo zablokowany po przekroczeniu liczby nieudanych prób logowania ustawionej w sekcji *Administration → General → Other* (domyślnie pięć). Klikając *Blocked*, można odblokować użytkownika.
Frontend access	Wyświetlany jest poziom dostępu do frontend - *System default*, *Internal*, *LDAP* lub *Disabled*, zależnie od ustawienia dla całej grupy użytkowników.
API access	Wyświetlany jest status dostępu do API - *Enabled* lub *Disabled*, zależnie od ustawienia dla roli użytkownika.
Debug mode	Wyświetlany jest status trybu debugowania - *Enabled* lub *Disabled*, zależnie od ustawienia dla całej grupy użytkowników.
Status	Wyświetlany jest status użytkownika - *Enabled* lub *Disabled*, zależnie od ustawienia dla całej grupy użytkowników.
Provisioned	Wyświetlana jest data ostatniego provisioningu użytkownika. Używane dla użytkowników utworzonych przez provisioning JIT z LDAP/SAML.
Info	Wyświetlane są informacje o błędach. Żółte ostrzeżenie jest wyświetlane dla użytkowników bez grup użytkowników. Czerwone ostrzeżenie jest wyświetlane dla użytkowników bez ról oraz dla użytkowników bez ról i grup użytkowników.

Aby skonfigurować nowego użytkownika, kliknij przycisk *Create user* w prawym górnym rogu.

Opcje masowej edycji

Przyciski pod listą oferują kilka opcji masowej edycji:

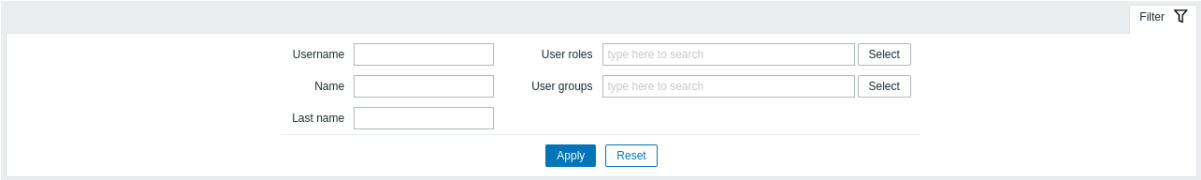
- *Provision now* - zaktualizuj informacje o użytkowniku z LDAP (ta opcja jest włączona tylko wtedy, gdy wybrano użytkownika LDAP)
- *Reset TOTP secret* - zresetuj sekrety TOTP użytkownika dla wszystkich metod TOTP i usuń sesję użytkownika (ta opcja jest włączona tylko wtedy, gdy włączono MFA; w przypadku użytkowników bez sekretów TOTP ich sesja nie zostanie usunięta)
- *Unblock* - ponownie włącz dostęp do systemu dla zablokowanych użytkowników
- *Delete* - usuń użytkowników

Aby użyć tych opcji, zaznacz pola wyboru przy odpowiednich użytkownikach, a następnie kliknij wymagany przycisk.

Używanie filtra

Możesz użyć filtra, aby wyświetlić tylko użytkowników, którymi jesteś zainteresowany. Dla lepszej wydajności wyszukiwania dane są przeszukiwane z nierozwiniętymi makrami.

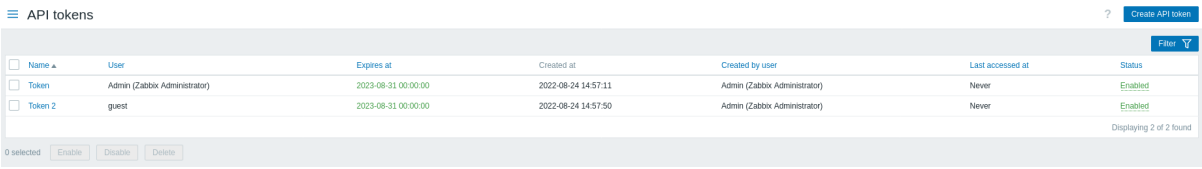
Łącze *Filtr* jest dostępne nad listą użytkowników. Po jego kliknięciu udostępniony zostanie filtr, za pomocą którego można filtrować użytkowników według nazwy użytkownika, imienia, nazwiska, roli użytkownika i grupy użytkowników.



4 Tokeny API

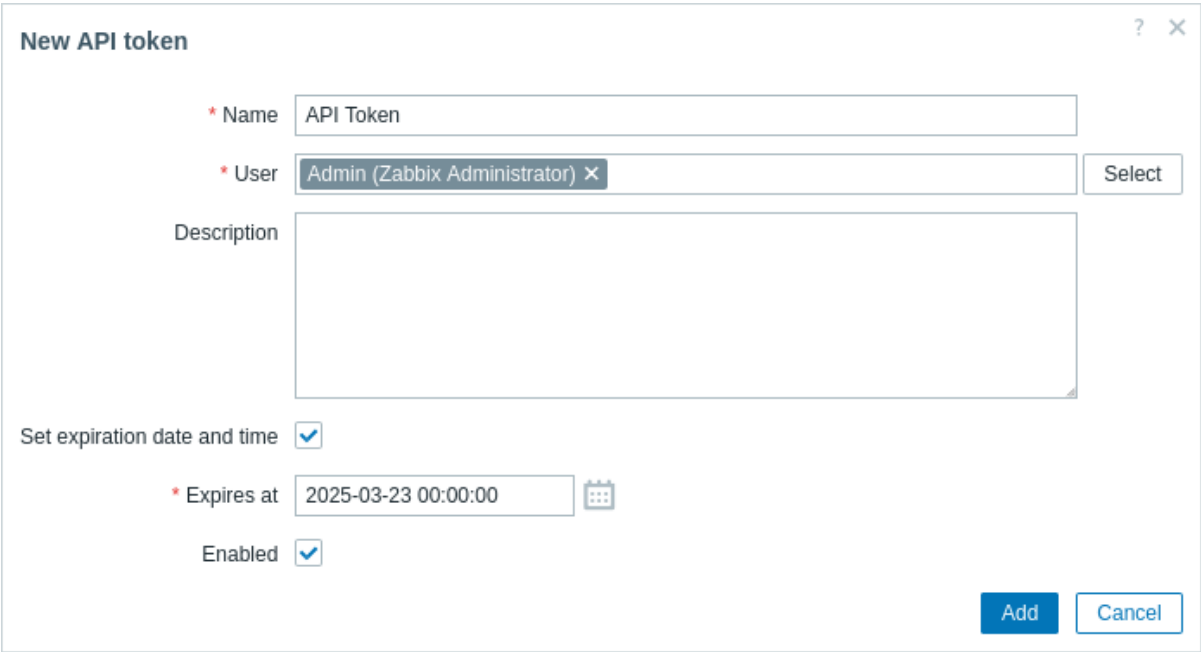
Przegląd

Ta sekcja umożliwia tworzenie tokenów API i zarządzanie nimi.



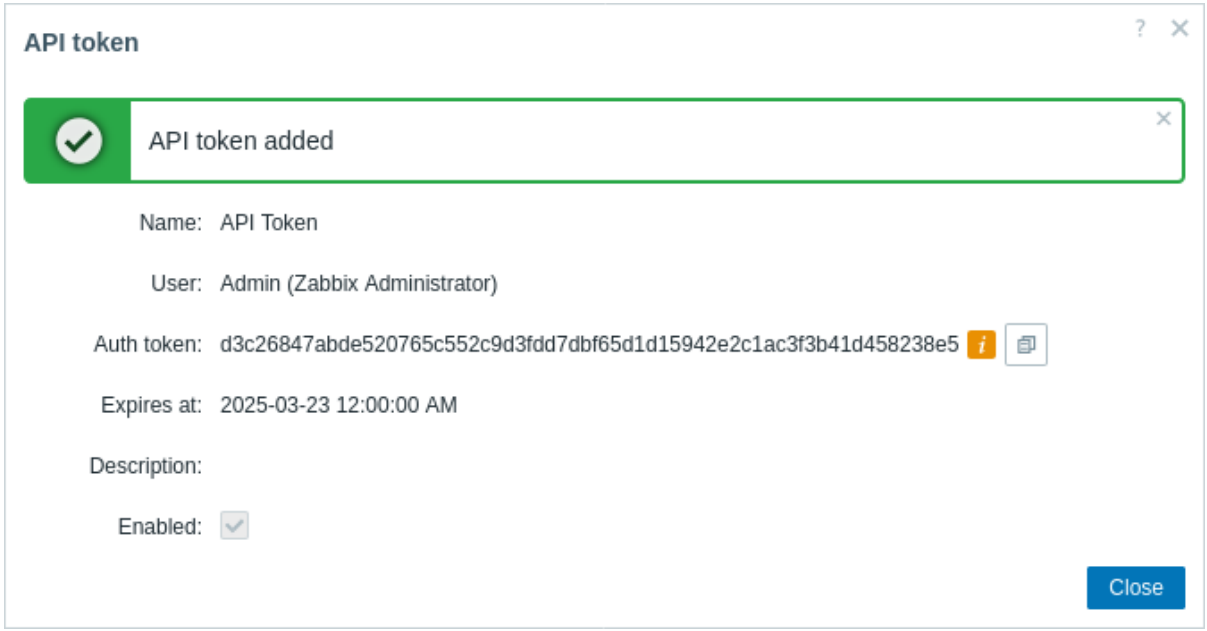
Tokeny API można filtrować według nazwy, użytkowników, do których tokeny są przypisane, daty wygaśnięcia, użytkowników, którzy utworzyli tokeny, lub statusu (włączony/wyłączony). Kliknij status tokenu na liście, aby szybko włączyć/wyłączyć token. Możesz także zbiorczo włączać/wyłączać tokeny, zaznaczając je na liście, a następnie klikając przyciski *Enable/Disable* pod listą.

Aby utworzyć nowy token, naciśnij przycisk *Create API token* w prawym górnym rogu, a następnie wypełnij wymagane pola na ekranie konfiguracji tokenu:



Parameter	Description
Nazwa	Widoczna nazwa tokenu.
Użytkownik	Użytkownik, do którego token ma zostać przypisany. Aby szybko wybrać użytkownika, zacznij wpisywać nazwę użytkownika, imię lub nazwisko, a następnie wybierz wymaganego użytkownika z listy autouzupełniania. Alternatywnie możesz nacisnąć przycisk *Select* i wybrać użytkownika z pełnej listy użytkowników. Token może być przypisany tylko do jednego użytkownika.
Opis	Opcjonalny opis tokenu.
Ustaw datę i godzinę wygaśnięcia	Odznacz to pole wyboru, jeśli token nie powinien mieć daty wygaśnięcia.
Data wygaśnięcia	Kliknij ikonę kalendarza, aby wybrać datę wygaśnięcia tokenu, lub wprowadź datę ręcznie w formacie YYYY-MM-DD hh:mm:ss
Włączony	Odznacz to pole wyboru, jeśli chcesz utworzyć token w stanie wyłączonym.

Naciśnij *Add*, aby utworzyć token.



Skopiuj wartość *Auth token* i zapisz ją w bezpiecznym miejscu **przed zamknięciem strony**, a następnie naciśnij Close. Token pojawi się na liście.

Warning:
Wartości *Auth token* nie będzie można później ponownie wyświetlić. Jest ona dostępna tylko bezpośrednio po utworzeniu tokenu. Jeśli utracisz zapisany token, konieczne będzie jego ponowne wygenerowanie, co spowoduje utworzenie nowego ciągu autoryzacyjnego.

Kliknij nazwę tokenu, aby edytować nazwę, opis, ustawienia daty wygaśnięcia lub status tokenu. Zwróć uwagę, że nie ma możliwości zmiany użytkownika, do którego token jest przypisany. Naciśnij przycisk *Update*, aby zapisać zmiany. Jeśli token został utracony lub ujawniony, możesz nacisnąć przycisk *Regenerate*, aby wygenerować nową wartość tokenu. Pojawi się okno dialogowe z prośbą o potwierdzenie tej operacji, ponieważ po jej wykonaniu wcześniej wygenerowany token stanie się nieważny.

Użytkownicy bez dostępu do sekcji menu *Administration* mogą przeglądać i modyfikować szczegóły tokenów przypisanych do nich w sekcji *User profile* → *API tokens* section tylko wtedy, gdy uprawnienie *Manage API tokens* jest dozwolone w uprawnieniach ich roli użytkownika.

5 Uwierzytelnianie

Przegląd

Sekcja *Użytkownicy* → *Uwierzytelnianie* umożliwia określenie metody uwierzytelniania użytkowników dla Zabbix oraz wewnętrznych wymagań dotyczących haseł.

Dostępne metody uwierzytelniania to uwierzytelnianie wewnętrzne, HTTP, LDAP, SAML oraz MFA.

Domyślne uwierzytelnianie

Domyślnie Zabbix używa **wewnętrznego** uwierzytelniania Zabbix dla wszystkich użytkowników.

Można zmienić domyślną metodę uwierzytelniania na LDAP w całym systemie. Aby to zrobić, przejdź do zakładki *LDAP* i skonfiguruj parametry LDAP, a następnie wróć do zakładki *Authentication* i przełącz selektor *Default authentication* na LDAP.

Należy pamiętać, że metodę uwierzytelniania można precyzyjnie dostosować na poziomie grupy użytkowników. Nawet jeśli uwierzytelnianie LDAP jest ustawione globalnie, niektóre grupy użytkowników nadal mogą być uwierzytelniane przez Zabbix. Dla tych grup frontend access musi być ustawiony na Internal.

Możliwe jest również włączenie uwierzytelniania LDAP tylko dla określonych grup użytkowników, jeśli globalnie używane jest uwierzytelnianie wewnętrzne. W takim przypadku szczegóły uwierzytelniania LDAP mogą zostać określone i użyte dla konkretnych grup użytkowników, których frontend access musi być wtedy ustawiony na LDAP. Jeśli użytkownik należy do co najmniej jednej grupy użytkowników z uwierzytelnianiem LDAP, nie będzie mógł korzystać z metody uwierzytelniania wewnętrznego.

Metody uwierzytelniania HTTP, SAML 2.0 i MFA mogą być używane dodatkowo obok domyślnej metody uwierzytelniania.

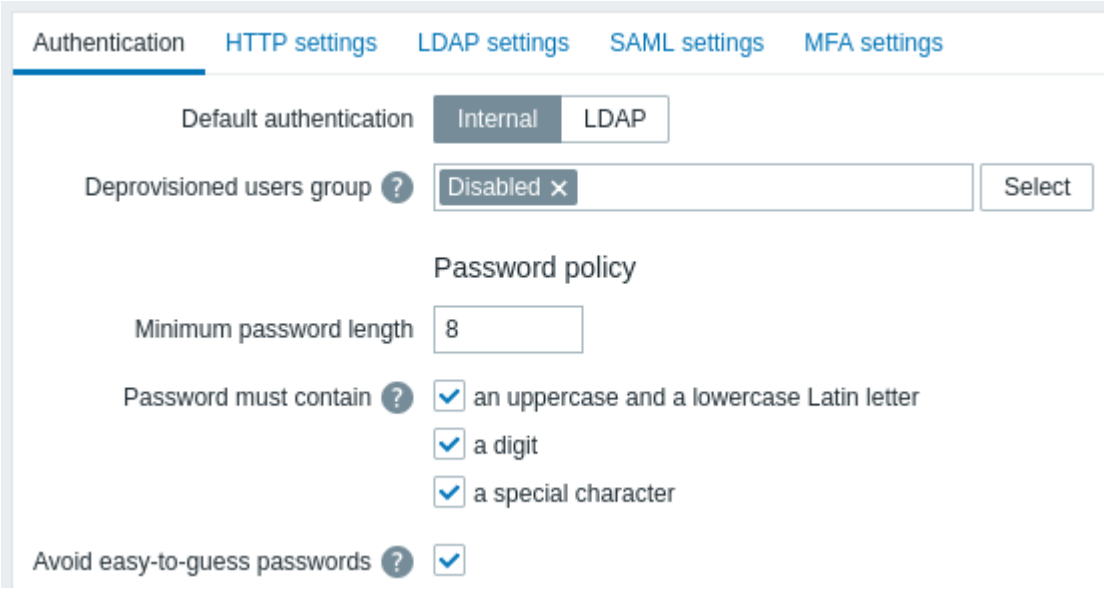
Zabbix obsługuje provisioning just-in-time (JIT), który umożliwia tworzenie kont użytkowników w Zabbix przy pierwszym uwierzytelnieniu użytkownika zewnętrznego oraz provisionowanie tych kont użytkowników. Provisioning JIT jest obsługiwany dla LDAP i SAML.

Zobacz także:

- Uwierzytelnianie HTTP
- Uwierzytelnianie LDAP
- Uwierzytelnianie SAML
- Uwierzytelnianie MFA

Konfiguracja

Zakładka *Authentication* umożliwia ustawienie domyślnej metody uwierzytelniania, określenie grupy dla użytkowników wycofanych z obsługi oraz ustawienie wymagań dotyczących złożoności haseł dla użytkowników Zabbix.



Parametry konfiguracji:

Parametr	Opis
Default authentication	Wybierz domyślną metodę uwierzytelniania w Zabbix — *Internal* lub *LDAP*.
Deprovisioned users group	Określ grupę użytkowników dla użytkowników wycofanych z obsługi. To ustawienie jest wymagane tylko w przypadku aprowizacji JIT, w odniesieniu do użytkowników utworzonych w Zabbix z systemów LDAP lub SAML, którzy nie muszą już być dalej aprowizowani. Należy wskazać wyłączoną grupę użytkowników.
Minimum password length	Domyślnie minimalna długość hasła jest ustawiona na 8. Obsługiwany zakres: 1-70. Należy pamiętać, że hasła dłuższe niż 72 znaki zostaną obcięte.
Password must contain	Zaznacz jedno lub kilka pól wyboru, aby wymagać użycia określonych znaków w haśle: - wielkiej i małej litery alfabetu łacińskiego - cyfry - znaku specjalnego Najedź kursorem na znak zapytania, aby zobaczyć podpowiedź z listą znaków dla każdej opcji.
Avoid easy-to-guess passwords	Jeśli opcja jest zaznaczona, hasło będzie sprawdzane pod kątem następujących wymagań: - nie może zawierać imienia, nazwiska ani nazwy użytkownika - nie może być jednym z popularnych haseł ani haseł specyficznych dla kontekstu. Lista popularnych i specyficznych dla kontekstu haseł jest generowana automatycznie na podstawie listy NCSC „Top 100k passwords”, listy SecLists „Top 1M passwords” oraz listy haseł specyficznych dla kontekstu Zabbix. Użytkownicy wewnętrzni nie będą mogli ustawiać haseł znajdujących się na tej liście, ponieważ takie hasła są uznawane za słabe ze względu na ich powszechne użycie.

Zmiany wymagań dotyczących złożoności haseł nie wpłyną na istniejące hasła użytkowników, ale jeśli istniejący użytkownik zdecyduje się zmienić hasło, nowe hasło będzie musiało spełniać bieżące wymagania. Podpowiedź z listą wymagań będzie wyświetlana obok pola *Password* w profilu użytkownika oraz w formularzu konfiguracji użytkownika dostępnym z menu *Users* → *Users*.

1 HTTP

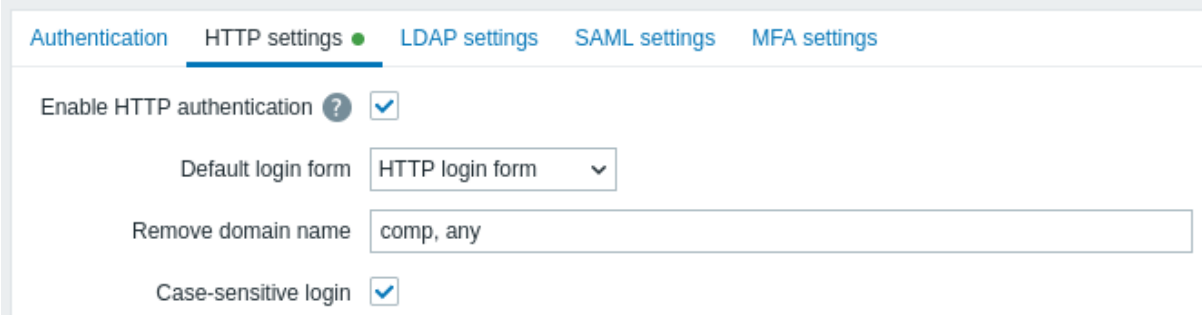
Przegląd

Uwierzytelnianie HTTP lub oparte na serwerze WWW authentication (na przykład: BasicAuthentication, NTLM/Kerberos) może być używane do sprawdzania nazw użytkowników i haseł. Należy jednak pamiętać, że użytkownik musi również istnieć w Zabbix, jednak jego hasło Zabbix nie będzie używane.

Attention:
Uwaga! Upewnij się, że uwierzytelnianie serwera WWW jest skonfigurowane i działa poprawnie przed jego włączeniem.

Uwierzytelnianie HTTP można wyłączyć we frontendzie, konfigurując odpowiednią opcję na karcie *HTTP settings* w sekcji *Users > Authentication*. Gdy uwierzytelnianie HTTP jest wyłączone, karta z opcjami uwierzytelniania HTTP nie będzie wyświetlana we frontendzie. Należy pamiętać, że ponowna instalacja frontendu (uruchomienie setup.php) zresetuje ustawienia uwierzytelniania, w tym konfigurację uwierzytelniania HTTP.

Konfiguracja



Parametry konfiguracji:

Parametr	Opis
Włącz uwierzytelnianie HTTP	Zaznacz pole wyboru, aby włączyć uwierzytelnianie HTTP. Po najechaniu kursorem na zostanie wyświetlona podpowiedź z ostrzeżeniem, że w przypadku uwierzytelniania przez serwer WWW wszyscy użytkownicy (nawet z dostępem do frontend ustawionym na LDAP/Internal) będą uwierzytelniani przez serwer WWW, a nie przez Zabbix.
Domyślny formularz logowania	Określ, czy nieuwierzytelnieni użytkownicy mają być kierowani do: **Formularz logowania Zabbix** - standardowa strona logowania Zabbix. **Formularz logowania HTTP** - strona logowania HTTP. Zaleca się włączenie uwierzytelniania opartego na serwerze WWW tylko dla strony `index_http.php`. Jeśli *Domyślny formularz logowania* jest ustawiony na „Strona logowania HTTP", użytkownik zostanie zalogowany automatycznie, jeśli moduł uwierzytelniania serwera WWW ustawi prawidłowy login użytkownika w zmiennej `$_SERVER`. Obsługiwane klucze `$_SERVER` to `PHP_AUTH_USER`, `REMOTE_USER`, `AUTH_USER`.
Usuń nazwę domeny	Lista nazw domen rozdzielonych przecinkami, które powinny zostać usunięte z nazwy użytkownika. Na przykład `comp,any` — jeśli nazwa użytkownika to 'Admin@any' lub 'comp\Admin', użytkownik zostanie zalogowany jako 'Admin'; jeśli nazwa użytkownika to 'notacompany\Admin', logowanie zostanie odrzucone.
Logowanie z rozróżnianiem wielkości liter	Odznacz pole wyboru, aby wyłączyć logowanie z rozróżnianiem wielkości liter dla nazw użytkowników (domyślnie włączone). Wyłączenie logowania z rozróżnianiem wielkości liter pozwala na przykład zalogować się jako „admin", nawet jeśli użytkownik Zabbix to „Admin" lub „ADMIN". Pamiętaj, że jeśli logowanie z rozróżnianiem wielkości liter jest wyłączone i istnieje wielu użytkowników Zabbix o podobnych nazwach użytkownika (np. Admin i admin), logowanie dla tych użytkowników będzie zawsze odrzucane z następującym komunikatem o błędzie: „Authentication failed: supplied credentials are not unique."

Note:
W przypadku użytkowników wewnętrznych, którzy nie mogą zalogować się przy użyciu poświadczeń HTTP (gdy domyślnie ustawiony jest formularz logowania HTTP), co prowadzi do błędu 401, można dodać w dyrektywach podstawowego uwierzytelniania wiersz `ErrorDocument 401 /index.php?form=default`, który przekieruje do zwykłego formularza logowania Zabbix.

Przegląd

Zewnętrzne uwierzytelnianie LDAP może być używane do sprawdzania nazw użytkowników i haseł.

Uwierzytelnianie LDAP w Zabbix działa co najmniej z Microsoft Active Directory i OpenLDAP.

Jeśli skonfigurowano tylko logowanie LDAP, użytkownik musi również istnieć w Zabbix, jednak jego hasło Zabbix nie będzie używane. Jeśli uwierzytelnianie zakończy się powodzeniem, Zabbix dopasuje lokalną nazwę użytkownika do atrybutu nazwy użytkownika zwróconego przez LDAP.

Provisioning użytkowników

Możliwe jest skonfigurowanie **provisioningu użytkowników** JIT (just-in-time) dla użytkowników LDAP. W takim przypadku nie jest wymagane, aby użytkownik istniał już w Zabbix. Konto użytkownika może zostać utworzone, gdy użytkownik zaloguje się do Zabbix po raz pierwszy.

Gdy użytkownik LDAP wprowadza swój login LDAP i hasło, Zabbix sprawdza *domyślny* serwer LDAP, czy taki użytkownik istnieje. Jeśli użytkownik istnieje i nie ma jeszcze konta w Zabbix, w Zabbix tworzony jest nowy użytkownik, a użytkownik może się zalogować.

Użytkownik utworzony za pomocą provisioningu JIT jest powiązany z serwerem LDAP (katalogiem), który w momencie utworzenia jest ustawiony jako domyślny. Późniejsza zmiana domyślnego serwera LDAP nie zmienia ani nie aktualizuje serwera LDAP powiązanego z użytkownikami, którzy zostali już provisionowani.

Attention:
Jeśli provisioning JIT jest włączony, na karcie *Authentication* należy określić grupę użytkowników dla użytkowników zdeprovisionowanych.

Provisioning JIT umożliwia również aktualizację provisionowanych kont użytkowników na podstawie zmian w LDAP. Na przykład, jeśli użytkownik zostanie przeniesiony z jednej grupy LDAP do innej, użytkownik zostanie również przeniesiony z jednej grupy do innej w Zabbix; jeśli użytkownik zostanie usunięty z grupy LDAP, użytkownik zostanie również usunięty z grupy w Zabbix i, jeśli nie należy do żadnej innej grupy, dodany do grupy użytkowników dla użytkowników zdeprovisionowanych. Provisionowane konta użytkowników są aktualizowane zgodnie ze skonfigurowanym okresem provisioningu lub gdy użytkownik loguje się do Zabbix.

Należy pamiętać, że provisioning w tle jest wykonywany przez frontend Zabbix, gdy użytkownik wchodzi z nim w interakcję lub ma co najmniej jedną otwartą stronę frontend w przeglądarce. Nie ma dedykowanych procesów działających w tle do provisioningu użytkowników.

LDAP obsługuje trzy sposoby wiązania z katalogiem na potrzeby uwierzytelniania i wyszukiwania:

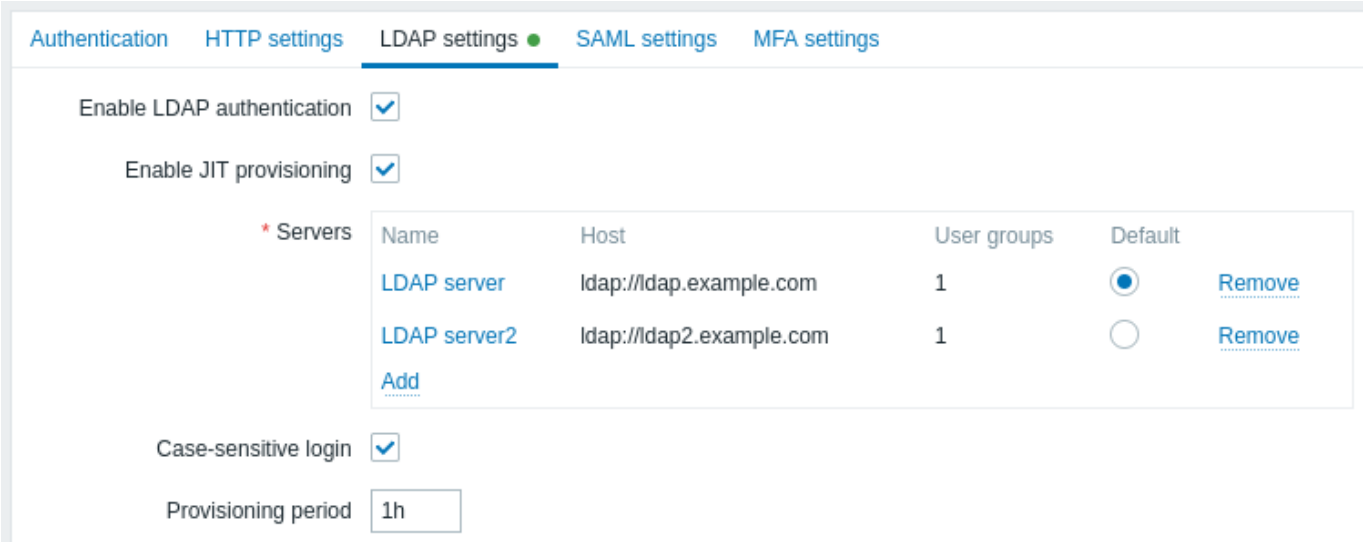
- Wiązanie anonimowe — nie podano *Bind DN* / *Bind password*, a serwer LDAP zezwala na zapytania anonimowe.
- Dedykowany użytkownik wiążący (konto usługi) — określone konto LDAP jest ustawione w *Bind DN* / *Bind password* i jest używane przez Zabbix do wyszukiwania oraz provisioningu. Jest to zalecana i najbardziej elastyczna opcja, ponieważ Zabbix może wykonywać wyszukiwania i provisioning w tle bez poświadczeń użytkownika końcowego.
- Bezpośrednie wiązanie użytkownika — Zabbix wykonuje wiązanie przy użyciu poświadczeń wprowadzonych przez użytkownika podczas logowania (bez skonfigurowanych *Bind DN* / *Bind password*); jest to konfigurowane przez uwzględnienie symbolu zastępczego, takiego jak `uid=%{user}`, w Base DN. W tym trybie Zabbix ma dostęp do hasła użytkownika tylko podczas interaktywnego logowania. W rezultacie działania provisioningowe, które wymagają uwierzytelnienia w LDAP poza sesją logowania użytkownika (na przykład użycie przycisku *Provision now* lub uruchomienie provisioningu w tle, gdy użytkownik nie jest aktywnie zalogowany), nie mogą się uwierzytelnić i dlatego nie będą działać. Provisioning i aktualizacje dla bezpośredniego wiązania użytkownika odbywają się wyłącznie w momencie logowania użytkownika.

Wiele serwerów

W razie potrzeby można zdefiniować kilka serwerów LDAP. Na przykład do uwierzytelniania innej grupy użytkowników można użyć innego serwera. Po skonfigurowaniu serwerów LDAP w konfiguracji grupy użytkowników będzie można wybrać wymagany serwer LDAP dla odpowiedniej grupy użytkowników.

Jeśli użytkownik należy do wielu grup użytkowników i wielu serwerów LDAP, do uwierzytelniania zostanie użyty pierwszy serwer z listy serwerów LDAP posortowanej według nazwy w porządku rosnącym.

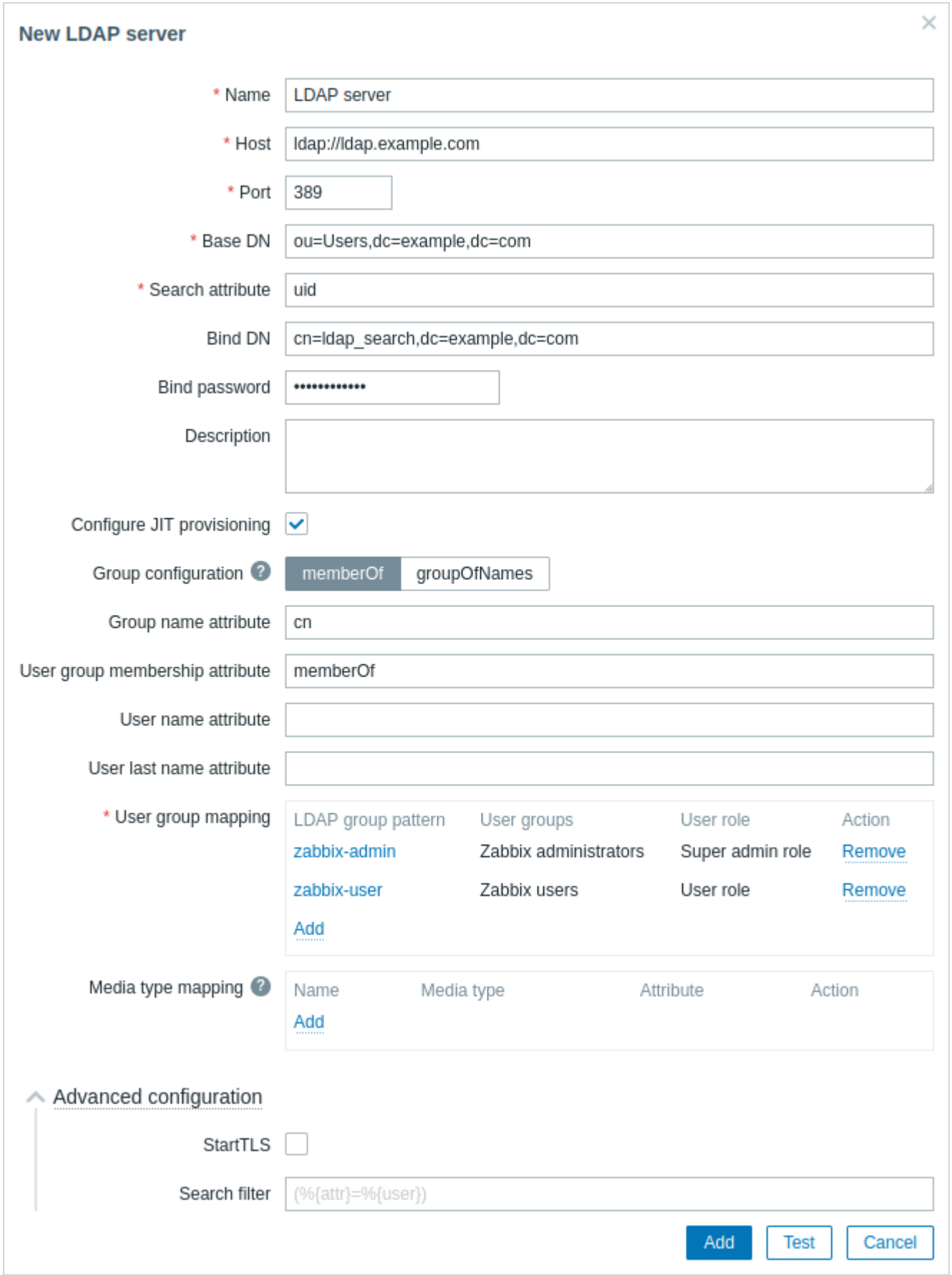
Konfiguracja



Parametry konfiguracji:

Parametr	Opis
Enable LDAP authentication	Zaznacz pole wyboru, aby włączyć uwierzytelnianie LDAP.
Enable JIT provisioning	Zaznacz pole wyboru, aby włączyć aprowizację JIT.
Servers	Kliknij *Add*, aby skonfigurować serwer LDAP (zobacz konfiguracja serwera LDAP poniżej).
Case-sensitive login	Odznacz pole wyboru, aby wyłączyć rozróżnianie wielkości liter podczas logowania dla nazw użytkowników (domyślnie włączone). Wyłączenie rozróżniania wielkości liter podczas logowania pozwala na przykład zalogować się jako „admin”, nawet jeśli użytkownik Zabbix to „Admin” lub „ADMIN”. Pamiętaj, że jeśli rozróżnianie wielkości liter podczas logowania jest wyłączone i istnieje wielu użytkowników Zabbix o podobnych nazwach użytkownika (np. Admin i admin), logowanie dla tych użytkowników będzie zawsze odrzucane z następującym komunikatem o błędzie: „Authentication failed: supplied credentials are not unique.”
Provisioning period	Ustaw okres aprowizacji, tj. jak często zalogowany użytkownik będzie aprowizowany podczas pracy z frontend.

Konfiguracja serwera LDAP



Parametry konfiguracji serwera LDAP:

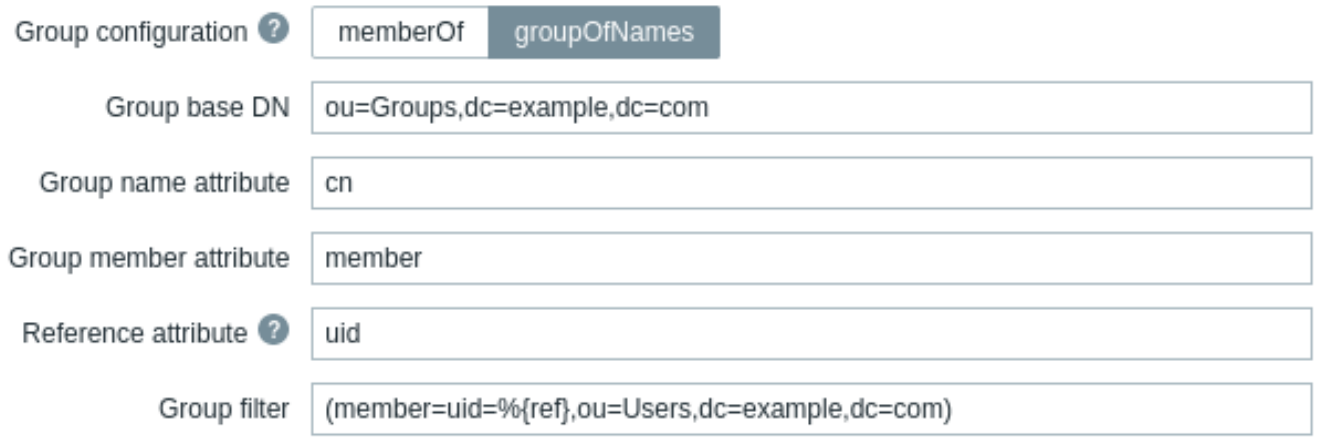
Parameter	Description
Name	Nazwa serwera LDAP w konfiguracji Zabbix.

Parameter	Description
Host	Nazwa hosta, IP lub URI serwera LDAP. Przykłady: ldap.example.com, 127.0.0.1, ldap://ldap.example.com Dla bezpiecznego serwera LDAP użyj protokołu *ldaps* i nazwy hosta. Przykład: ldaps://ldap.example.com W OpenLDAP 2.x.x i nowszych można użyć pełnego URI LDAP w postaci ldap://hostname:port lub ldaps://hostname:port.
Port	Port serwera LDAP. Domyślnie 389. Dla bezpiecznego połączenia LDAP numer portu to zwykle 636. Nie jest używany przy korzystaniu z pełnych URI LDAP.
Base DN	Ścieżka bazowa do kont użytkowników na serwerze LDAP: ou=Users,ou=system (dla OpenLDAP), DC=company,DC=com (dla Microsoft Active Directory) uid=%{user},dc=example,dc=com (dla bezpośredniego wiązania użytkownika, patrz uwaga poniżej)
Search attribute	Atrybut konta LDAP używany do wyszukiwania: uid (dla OpenLDAP), sAMAccountName (dla Microsoft Active Directory)
Bind DN	Konto LDAP do wiązania i wyszukiwania na serwerze LDAP, przykłady: uid=ldap_search,ou=system (dla OpenLDAP), CN=ldap_search,OU=user_group,DC=company,DC=com (dla Microsoft Active Directory) Obsługiwane jest również anonimowe wiązanie. Należy pamiętać, że anonimowe wiązanie może potencjalnie udostępnić konfigurację domeny nieuprawnionym użytkownikom (informacje o użytkownikach, komputerach, serwerach, grupach, usługach itp.). Ze względów bezpieczeństwa wyłącz anonimowe wiązania na hostach LDAP i zamiast tego używaj uwierzytelnionego dostępu.
Bind password	Hasło LDAP konta używanego do wiązania i wyszukiwania na serwerze LDAP.
Description	Opis serwera LDAP.
Configure JIT provisioning	Zaznacz to pole wyboru, aby wyświetlić opcje związane z aprowizacją JIT.
Group configuration	Wybierz metodę konfiguracji grup: **memberOf** - przez wyszukiwanie użytkowników i atrybutu ich przynależności do grup **groupOfNames** - przez wyszukiwanie grup za pomocą atrybutu member Należy pamiętać, że memberOf jest preferowane, ponieważ działa szybciej; użyj groupOfNames, jeśli serwer LDAP nie obsługuje `memberOf` lub wymagane jest filtrowanie grup.
Group name attribute	Określ atrybut, z którego ma być pobierana nazwa grupy ze wszystkich obiektów w atrybucie `memberOf` (zobacz pole *User group membership attribute*) Nazwa grupy jest wymagana do mapowania grup użytkowników.
User group membership attribute	Określ atrybut zawierający informacje o grupach, do których należy użytkownik (np. `memberOf`). Na przykład atrybut memberOf może zawierać informacje takie jak: `memberOf=cn=zabbix-admin,ou=Groups,dc=example,dc=com` To pole jest dostępne tylko dla metody memberOf.
User name attribute	Określ atrybut zawierający imię użytkownika.
User last name attribute	Określ atrybut zawierający nazwisko użytkownika.
User group mapping	Mapuj wzorzec grupy użytkowników LDAP na grupę użytkowników Zabbix i rolę użytkownika. Jest to wymagane do określenia, jaką grupę/rolę otrzyma aprowizowany użytkownik w Zabbix. Kliknij *Add*, aby dodać mapowanie. Pole *LDAP group pattern* obsługuje symbole wieloznaczne. Nazwa grupy musi odpowiadać istniejącej grupie. Jeśli użytkownik LDAP pasuje do kilku grup użytkowników Zabbix, stanie się członkiem wszystkich tych grup. Jeśli użytkownik pasuje do kilku ról użytkowników Zabbix, otrzyma tę z najwyższym poziomem uprawnień.
Media type mapping	Mapuj atrybuty LDAP użytkownika mediów (np. email) na media użytkownika Zabbix do wysyłania powiadomień (wartość atrybutu jest używana jako pole *Send to* mediów użytkownika).
Advanced configuration	Kliknij etykietę *Advanced configuration*, aby wyświetlić zaawansowane opcje konfiguracji (patrz poniżej).
StartTLS	Zaznacz pole wyboru, aby używać operacji StartTLS podczas łączenia z serwerem LDAP. Połączenie nie powiedzie się, jeśli serwer nie obsługuje StartTLS. StartTLS nie może być używany z serwerami korzystającymi z protokołu *ldaps*.

Parameter	Description
Search filter	Zdefiniuj własny ciąg podczas uwierzytelniania użytkownika w LDAP. Obsługiwane są następujące symbole zastępcze: `%{attr}` - nazwa atrybutu wyszukiwania (uid, sAMAccountName) `%{user}` - wartość nazwy użytkownika do uwierzytelnienia Na przykład, aby przeprowadzić wyszukiwanie z rozróżnianiem wielkości liter w środowisku LDAP lub Microsoft Active Directory niewrażliwym na wielkość liter, ciąg można zdefiniować następująco: `(%{attr}:caseExactMatch:=%{user})`. Jeśli filtr nie zostanie dostosowany, LDAP użyje domyślnego: `(%{attr}=%{user})`.

Note:
Aby skonfigurować serwer LDAP do **bezpośredniego wiązania użytkownika**, dodaj atrybut uid=%{user} do parametru *Base DN* (na przykład *uid=%{user},dc=example,dc=com*) i pozostaw parametry *BindDN* oraz *Bind password* puste. Podczas uwierzytelniania symbol zastępczy %{user} zostanie zastąpiony nazwą użytkownika wprowadzoną podczas logowania.
 Przy bezpośrednim wiązaniu użytkownika Zabbix ma dostęp do poświadczeń użytkownika tylko podczas interaktywnego logowania. Dlatego zadania aprowizacji działające bez interaktywnego logowania (na przykład przycisk *Provision now* lub metoda API `user.provision`) będą ignorować użytkowników uwierzytelniających się za pomocą bezpośredniego wiązania użytkownika, ponieważ Zabbix nie może wiązać się w ich imieniu. Użyj anonimowego wiązania lub dedykowanego użytkownika do wiązania (konta usługi), jeśli potrzebujesz, aby aprowizacja i wyszukiwania LDAP działały z frontend bez konieczności zalogowania użytkownika końcowego.

Poniższe pola są specyficzne dla metody *Group configuration* „groupOfNames”:



Parameter	Description
Group base DN	Ścieżka bazowa do grup na serwerze LDAP.
Group name attribute	Określ atrybut, z którego ma być pobierana nazwa grupy w określonej ścieżce bazowej do grup. Nazwa grupy jest wymagana do mapowania grup użytkowników.
Group member attribute	Określ atrybut zawierający informacje o członkach grupy w LDAP (np. `member`).
Reference attribute	Określ atrybut referencyjny dla filtra grupy (zobacz pole *Group filter*). Następnie użyj `%{ref}` w filtrze grupy, aby pobrać wartości dla atrybutu określonego tutaj.
Group filter	Określ filtr do pobrania grupy, której członkiem jest użytkownik. Na przykład `(member=uid=%{ref},ou=Users,dc=example,dc=com)` dopasuje „User1”, jeśli atrybut member grupy ma wartość `uid=User1,ou=Users,dc=example,dc=com`, i zwróci grupę, której członkiem jest „User1”.

Warning:
W przypadku problemów z certyfikatami, aby bezpieczne połączenie LDAP (ldaps) działało, może być konieczne dodanie w pliku konfiguracyjnym /etc/openldap/ldap.conf wiersza `TLS_REQCERT allow`. Może to obniżyć bezpieczeństwo połączenia z katalogiem LDAP.

Note:
Zaleca się utworzenie osobnego konta LDAP (*Bind DN*) do wykonywania wiązania i wyszukiwania na serwerze LDAP z minimalnymi uprawnieniami w LDAP zamiast używania rzeczywistych kont użytkowników (używanych do logowania do frontend Zabbix).
Takie podejście zapewnia większe bezpieczeństwo i nie wymaga zmiany parametru *Bind password*, gdy użytkownik zmieni własne hasło na serwerze LDAP.
W powyższej tabeli jest to nazwa konta *ldap_search*.

Testowanie dostępu

Przycisk *Test* umożliwia przetestowanie dostępu użytkownika:

Parameter	Description
Login	Nazwa użytkownika LDAP do przetestowania (wstępnie wypełniona bieżącą nazwą użytkownika z frontend Zabbix). Ta nazwa użytkownika musi istnieć na serwerze LDAP. Zabbix nie aktywuje uwierzytelniania LDAP, jeśli nie będzie w stanie uwierzytelnić testowanego użytkownika.
User password	Hasło użytkownika LDAP do przetestowania.

3 SAML

Przegląd

Uwierzytelnianie SAML 2.0 authentication może być używane do logowania do Zabbix.

Jeśli skonfigurowano tylko logowanie SAML, użytkownik musi również istnieć w Zabbix, jednak jego hasło Zabbix nie będzie używane. Jeśli uwierzytelnienie zakończy się powodzeniem, Zabbix dopasuje lokalną nazwę użytkownika do atrybutu nazwy użytkownika zwróconego przez SAML.

Provisioning użytkowników

Można skonfigurować **provisioning użytkowników** JIT (just-in-time) dla użytkowników SAML. W takim przypadku nie jest wymagane, aby użytkownik istniał już w Zabbix. Konto użytkownika może zostać utworzone, gdy użytkownik zaloguje się do Zabbix po raz pierwszy.

Attention:
Jeśli provisioning JIT jest włączony, na karcie *Authentication* należy określić grupę użytkowników dla użytkowników, którym odebrano provisioning.

Oprócz provisioningu JIT można również włączyć i skonfigurować provisioning SCIM (System for Cross-domain Identity Management) — *ciągłe* zarządzanie kontami użytkowników dla tych użytkowników, którzy zostali utworzeni przez provisioning użytkowników. Provisioning SCIM wymaga tokena API Zabbix (z uprawnieniami Super admin) do uwierzytelniania w Zabbix.

Na przykład, jeśli użytkownik zostanie przeniesiony z jednej grupy SAML do innej, użytkownik zostanie również przeniesiony z jednej grupy do innej w Zabbix; jeśli użytkownik zostanie usunięty z grupy SAML, użytkownik zostanie również usunięty z grupy w Zabbix i, jeśli nie należy do żadnej innej grupy, zostanie dodany do grupy użytkowników dla użytkowników, którym odebrano provisioning.

Jeśli SCIM jest włączony i skonfigurowany, użytkownik SAML zostanie provisionowany w momencie zalogowania się do Zabbix i będzie stale aktualizowany na podstawie zmian w SAML. Istniejący już użytkownicy SAML nie będą provisionowani, a aktualizowani będą tylko użytkownicy provisionowani. Należy pamiętać, że do użytkownika zostaną dodane tylko prawidłowe media, gdy użytkownik zostanie provisionowany lub zaktualizowany.

Jeśli SCIM nie jest włączony, użytkownik SAML zostanie provisionowany (a później zaktualizowany) w momencie zalogowania się do Zabbix.

Note:
Jeśli uwierzytelnianie SAML jest włączone, użytkownicy będą mogli wybrać logowanie lokalne lub przez logowanie jednokrotne SAML. Jeśli używany jest provisioning JIT, możliwe jest tylko logowanie jednokrotne.

Konfigurowanie dostawcy tożsamości

Aby pracować z Zabbix, dostawca tożsamości SAML (onelogin.com, auth0.com, okta.com itp.) musi zostać skonfigurowany w następujący sposób:

- *Assertion Consumer URL* należy ustawić na `<path_to_zabbix_ui>/index_sso.php?acs`
- *Single Logout URL* należy ustawić na `<path_to_zabbix_ui>/index_sso.php?sls`

Przykłady `<path_to_zabbix_ui>`: `https://example.com/zabbix/ui`, `http://another.example.com/zabbix`, `http://<any_public_ip_address>/zabbix`

Konfigurowanie Zabbix

Attention:
Wymagana jest instalacja php-openssl, jeśli chcesz używać uwierzytelniania SAML we frontend.

Aby używać uwierzytelniania SAML, Zabbix powinien zostać skonfigurowany w następujący sposób:

1. Dostarcz klucz prywatny SP oraz certyfikaty. Aby aktywować SAML przez frontend, należy dostarczyć certyfikat IdP (wkleić lub wybrać plik). Jeśli wybrane są opcje *Sign* lub *Encrypt*, należy dostarczyć certyfikat SP oraz klucz prywatny SP.

Jeśli w zabbix.conf.php ustawiono `$SSO['CERT_STORAGE'] = 'database'`, podczas konfiguracji SAML można wkleić treść certyfikatu lub przesłać plik certyfikatu we frontend — żadne pliki w systemie plików nie są wymagane.

Jeśli w zabbix.conf.php ustawiono `$SSO['CERT_STORAGE'] = 'file'`, certyfikat musi być dostępny w systemie plików (domyślnie w ui/conf/certs lub w ścieżce skonfigurowanej w zabbix.conf.php), a frontend nie będzie przechowywać certyfikatów w bazie danych. Zwróć uwagę, że jeśli `$SSO['CERT_STORAGE']` nie jest ustawione lub jest zakomentowane, zakładane jest przechowywanie w plikach.

Domyślnie Zabbix będzie szukać w następujących lokalizacjach:

- ui/conf/certs/sp.key - plik klucza prywatnego SP
- ui/conf/certs/sp.crt - plik certyfikatu SP
- ui/conf/certs/idp.crt - plik certyfikatu IDP

Attention:
Materiał certyfikatów może zostać zaimportowany przez frontend przez wklejenie tekstu lub przesłanie plików. Chociaż niezaszyfrowany import jest dozwolony dla wygody w niektórych środowiskach, zdecydowanie zaleca się używanie szyfrowanego transportu (na przykład włączenie HTTPS/TLS dla frontend Zabbix). Gdy certyfikaty/klucze SAML są przechowywane w bazie danych, włącz TLS/SSL dla połączeń z bazą danych, aby chronić ruch między aplikacją a bazą danych.
 Szyfruj kopie zapasowe bazy danych, które mogą zawierać certyfikaty SAML lub klucze prywatne, oraz ogranicz dostęp do plików kopii zapasowych i do tabel bazy danych przechowujących materiał SAML. Ogranicz uprawnienia użytkownika bazy danych do niezbędnego minimum.

2. Wszystkie najważniejsze ustawienia można skonfigurować we frontend Zabbix. Możliwe jest jednak określenie dodatkowych ustawień w pliku konfiguracyjnym.



Parametry konfiguracyjne dostępne we frontend Zabbix:

Parameter	Description
Enable SAML authentication	Zaznacz pole wyboru, aby włączyć uwierzytelnianie SAML.
Enable JIT provisioning	Zaznacz pole wyboru, aby włączyć aprowizację użytkowników JIT.
IDP entity ID	Unikalny identyfikator encji w dostawcy tożsamości SAML.
SSO service URL	Adres URL, na który użytkownicy zostaną przekierowani podczas logowania.
SLO service URL	Adres URL, na który użytkownicy zostaną przekierowani podczas wylogowywania. Jeśli pozostanie pusty, usługa SLO nie będzie używana.

Parameter	Description
Username attribute	Atrybut SAML, który będzie używany jako nazwa użytkownika podczas logowania do Zabbix. Lista obsługiwanych wartości jest określana przez dostawcę tożsamości. Przykłady: uid userprincipalname samaccountname username userusername urn:oid:0.9.2342.19200300.100.1.1 urn:oid:1.3.6.1.4.1.5923.1.1.1.13 urn:oid:0.9.2342.19200300.100.1.44
SP entity ID	Unikalny identyfikator dostawcy usług (jeśli nie będzie zgodny, operacja zostanie odrzucona). Można podać adres URL lub dowolny ciąg danych.
SP name ID format	Żądanie określonego formatu name ID w odpowiedzi. Przykłady: urn:oasis:names:tc:SAML:2.0:nameid-format:persistent urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified urn:oasis:names:tc:SAML:2.0:nameid-format:transient
IdP certificate	Zawartość certyfikatu dostawcy usług (SP) do konfiguracji usługi logowania jednokrotnego SAML (SSO).
SP private key	Zawartość klucza prywatnego dostawcy usług (SP) do konfiguracji usługi logowania jednokrotnego SAML (SSO). Zapewnia bezpieczne uwierzytelnianie i wymianę danych z dostawcą tożsamości (IdP).
SP certificate	Zawartość certyfikatu dostawcy usług (SP) do konfiguracji usługi logowania jednokrotnego SAML (SSO).
Sign	Zaznacz pola wyboru, aby wybrać encje, dla których podpis SAML ma być włączony: *Messages* *Assertions* *AuthN requests* *Logout requests* *Logout responses*
Encrypt	Zaznacz pola wyboru, aby wybrać encje, dla których szyfrowanie SAML ma być włączone: *Name ID* *Assertions*
Case-sensitive login	Odznacz pole wyboru, aby wyłączyć rozróżnianie wielkości liter w nazwach użytkowników podczas logowania (domyślnie włączone). Wyłączenie rozróżniania wielkości liter pozwala na przykład zalogować się jako ”admin”, nawet jeśli użytkownik Zabbix to ”Admin” lub ”ADMIN”. Pamiętaj, że jeśli rozróżnianie wielkości liter jest wyłączone i istnieje wielu użytkowników Zabbix o podobnych nazwach użytkownika (np. Admin i admin), logowanie tych użytkowników będzie zawsze odrzucane z następującym komunikatem o błędzie: ”Authentication failed: supplied credentials are not unique.”
Configure JIT provisioning	Zaznacz to pole wyboru, aby wyświetlić opcje związane z aprowizacją użytkowników JIT.
Group name attribute	Określ atrybut nazwy grupy dla aprowizacji użytkowników JIT.
User name attribute	Określ atrybut imienia użytkownika dla aprowizacji użytkowników JIT.
User last name attribute	Określ atrybut nazwiska użytkownika dla aprowizacji użytkowników JIT.
User group mapping	Mapuj wzorzec grupy użytkownika SAML na grupę użytkowników Zabbix i rolę użytkownika. Jest to wymagane do określenia, jaką grupę/rolę użytkownika otrzyma aprowizowany użytkownik w Zabbix. Kliknij *Add*, aby dodać mapowanie. Pole *SAML group pattern* obsługuje symbole wieloznaczne. Nazwa grupy musi odpowiadać istniejącej grupie. Jeśli użytkownik SAML pasuje do kilku grup użytkowników Zabbix, użytkownik stanie się członkiem wszystkich tych grup. Jeśli użytkownik pasuje do kilku ról użytkowników Zabbix, otrzyma najwyższy poziom uprawnień spośród nich.
Media type mapping	Mapuj atrybuty mediów SAML użytkownika (np. email) na media użytkownika Zabbix do wysyłania powiadomień.

Parameter	Description
Enable SCIM provisioning	Zaznacz to pole wyboru, aby włączyć aprowizację SCIM 2.0.

Zobacz przykłady konfiguracji dostawców tożsamości SAML do logowania i aprowizacji użytkowników w Zabbix z użyciem:

- Microsoft Azure AD
- Okta
- Onelogin

Uwagi dotyczące provisioningu SCIM

W przypadku provisioningu SCIM należy określić ścieżkę do frontend Zabbix i dodać do niej `api_scim.php` po stronie dostawcy tożsamości, tj.:

`https://<path-to-zabbix-ui>/api_scim.php`

Atrybuty użytkownika używane w Zabbix (nazwa użytkownika, imię użytkownika, nazwisko użytkownika oraz atrybuty mediów) należy dodać jako atrybuty niestandardowe, a w razie potrzeby zewnętrzna przestrzeń nazw powinna być taka sama jak w schemacie użytkownika: `urn:ietf:params:scim:schemas:core:2.0:User`.

Ustawienia zaawansowane

Dodatkowe parametry SAML można skonfigurować w pliku konfiguracyjnym frontend Zabbix (*zabbix.conf.php*):

- $SSO['SP_KEY'] = '<ścieżka do pliku klucza prywatnego SP>';
- $SSO['SP_CERT'] = '<ścieżka do pliku certyfikatu SP>';
- $SSO['IDP_CERT'] = '<ścieżka do pliku certyfikatu IDP>';
- $SSO['SETTINGS']

Note:
Tablica `$SSO['SETTINGS']` musi mieć taką samą strukturę, jakiej oczekuje biblioteka *SAML PHP Toolkit* (dostarczana z Zabbix). Pełny opis dostępnych opcji konfiguracji znajduje się w oficjalnej dokumentacji biblioteki.

Tylko następujące opcje mogą być ustawiane w ramach $SSO['SETTINGS']:

- *strict*
- *baseurl*
- *compress*
- *contactPerson*
- *organization*
- *sp* (tylko opcje określone na tej liście)
  - *attributeConsumingService*
  - *x509certNew*
- *idp* (tylko opcje określone na tej liście)
  - *singleLogoutService* (tylko jedna opcja)
    - *responseUrl*
  - *certFingerprint*
  - *certFingerprintAlgorithm*
  - *x509certMulti*
- *security* (tylko opcje określone na tej liście)
  - *signMetadata*
  - *wantNameId*
  - *requestedAuthnContext*
  - *requestedAuthnContextComparison*
  - *wantXMLValidation*
  - *relaxDestinationValidation*
  - *destinationStrictlyMatches*
  - *rejectUnsolicitedResponsesWithInResponseTo*
  - *signatureAlgorithm*
  - *digestAlgorithm*
  - *lowercaseUrlencoding*

Wszystkie pozostałe opcje będą pobierane z bazy danych i nie mogą zostać nadpisane. Opcja *debug* zostanie zignorowana.

Dodatkowo, jeśli interfejs użytkownika Zabbix znajduje się za proxy lub load balancerem, można użyć niestandardowej opcji *use_proxy_headers*:

- *false* (domyślnie) - ignoruj opcję;
- *true* - używaj nagłówków HTTP X-Forwarded-* do budowania bazowego URL.

Jeśli do połączenia z instancją Zabbix używany jest load balancer, który korzysta z TLS/SSL, a Zabbix nie, należy określić parametry 'baseurl', 'strict' i 'use_proxy_headers' w następujący sposób:

```
$SSO['SETTINGS'] = [
    'strict' => false,
    'baseurl' => 'https://zabbix.example.com/zabbix/',
    'use_proxy_headers' => true
];
```

Przykład konfiguracji:

```
$SSO['SETTINGS'] = [
    'security' => [
        'signatureAlgorithm' => 'http://www.w3.org/2001/04/xmldsig-more#rsa-sha384'
        'digestAlgorithm' => 'http://www.w3.org/2001/04/xmldsig-more#sha384',
        // ...
    ],
    // ...
];
```

Konfiguracja frontend z Kerberos/ADFS

Plik konfiguracyjny frontend Zabbix (*zabbix.conf.php*) może być używany do konfiguracji SSO z uwierzytelnianiem Kerberos i ADFS:

```
$SSO['SETTINGS'] = [
    'security' => [
        'requestedAuthnContext' => [
            'urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos',
        ],
        'requestedAuthnContextComparison' => 'exact'
    ]
];
```

W takim przypadku w konfiguracji SAML w polu *SP name ID* ustaw:

```
urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
```

4 MFA

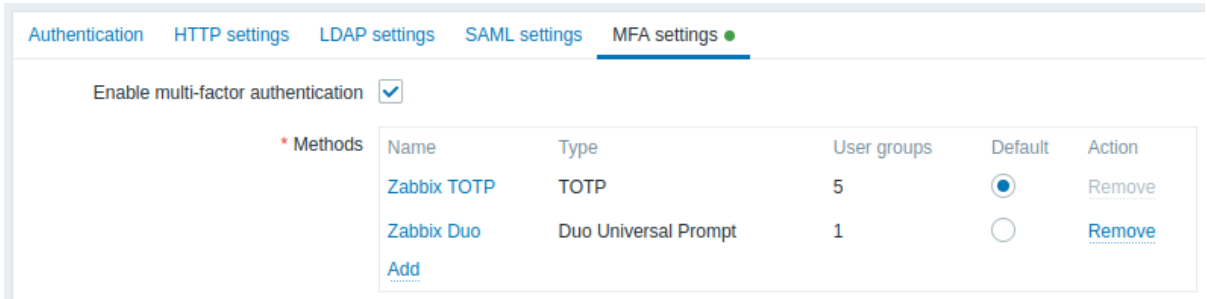
Przegląd

Uwierzytelnianie wieloskładnikowe authentication (MFA) może być używane do logowania do Zabbix, zapewniając dodatkową warstwę bezpieczeństwa poza samą nazwą użytkownika i hasłem.

W przypadku MFA użytkownik musi istnieć w Zabbix, musi podać poświadczenia Zabbix podczas logowania, a także musi potwierdzić swoją tożsamość w inny sposób, zazwyczaj za pomocą kodu wygenerowanego przez aplikację uwierzytelniającą na telefonie użytkownika.

Dostępnych jest wiele metod MFA, co pozwala użytkownikom wybrać opcję najlepiej odpowiadającą ich wymaganiom i preferencjom w zakresie bezpieczeństwa. Metody te to jednorazowe hasło czasowe (TOTP) oraz Duo Universal Prompt.

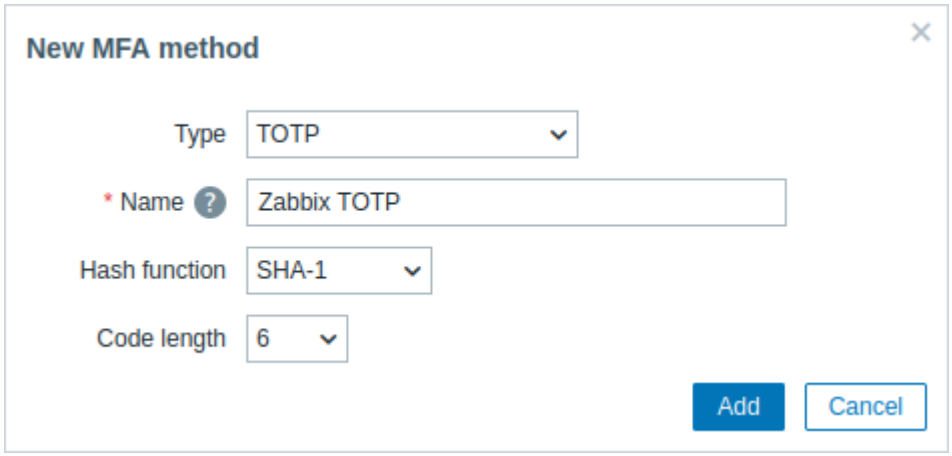
Konfiguracja



Parametry konfiguracji:

Parametr	Opis
Włącz uwierzytelnianie wieloskładnikowe	Zaznacz pole wyboru, aby włączyć uwierzytelnianie wieloskładnikowe.
Metody	Kliknij *Dodaj*, aby skonfigurować metodę MFA (zobacz konfigurację metody poniżej).

Konfiguracja metody



Parametry konfiguracji metody:

Parameter	Description
Type	Wybierz typ metody MFA: **TOTP** — użyj aplikacji uwierzytelniającej do generowania jednorazowych haseł opartych na czasie; **Duo Universal Prompt** — użyj usługi uwierzytelniania Duo do zapewnienia uwierzytelniania wieloskładnikowego.
Name	Wprowadź nazwę wyświetlaną jako nazwa konta dla wszystkich użytkowników MFA w aplikacjach uwierzytelniających (na przykład „Zabbix”).
Hash function	Wybierz funkcję skrótu (SHA-1, SHA-256 lub SHA-512) do generowania kodów TOTP. Ten parametr jest dostępny, jeśli typ metody MFA jest ustawiony na „TOTP”. Należy pamiętać, że wybór SHA-256 lub SHA-512 może znacznie ograniczyć kompatybilność, ponieważ wiele aplikacji obecnie nie obsługuje tych funkcji.
Code length	Wybierz długość kodu weryfikacyjnego (6 lub 8). Ten parametr jest dostępny, jeśli typ metody MFA jest ustawiony na „TOTP”.
API hostname	Wprowadź nazwę hosta API podaną przez usługę uwierzytelniania Duo. Ten parametr jest dostępny, jeśli typ metody MFA jest ustawiony na „Duo Universal Prompt”.
Client ID	Wprowadź identyfikator klienta podany przez usługę uwierzytelniania Duo. Ten parametr jest dostępny, jeśli typ metody MFA jest ustawiony na „Duo Universal Prompt”.
Client secret	Wprowadź klucz tajny klienta podany przez usługę uwierzytelniania Duo. Ten parametr jest dostępny, jeśli typ metody MFA jest ustawiony na „Duo Universal Prompt”.

Przykłady konfiguracji

Ta sekcja zawiera przykłady konfiguracji MFA z użyciem Time-Based One-Time Password (TOTP) oraz Duo Universal Prompt.

TOTP

W przypadku TOTP użytkownicy muszą zweryfikować swoją tożsamość za pomocą aplikacji uwierzytelniającej (na przykład aplikacji Google Authenticator).

1. Przejdź do ustawień MFA w Zabbix w sekcji *Users* → *Authentication* i włącz uwierzytelnianie wieloskładnikowe.
2. Dodaj nową metodę MFA z następującą konfiguracją:

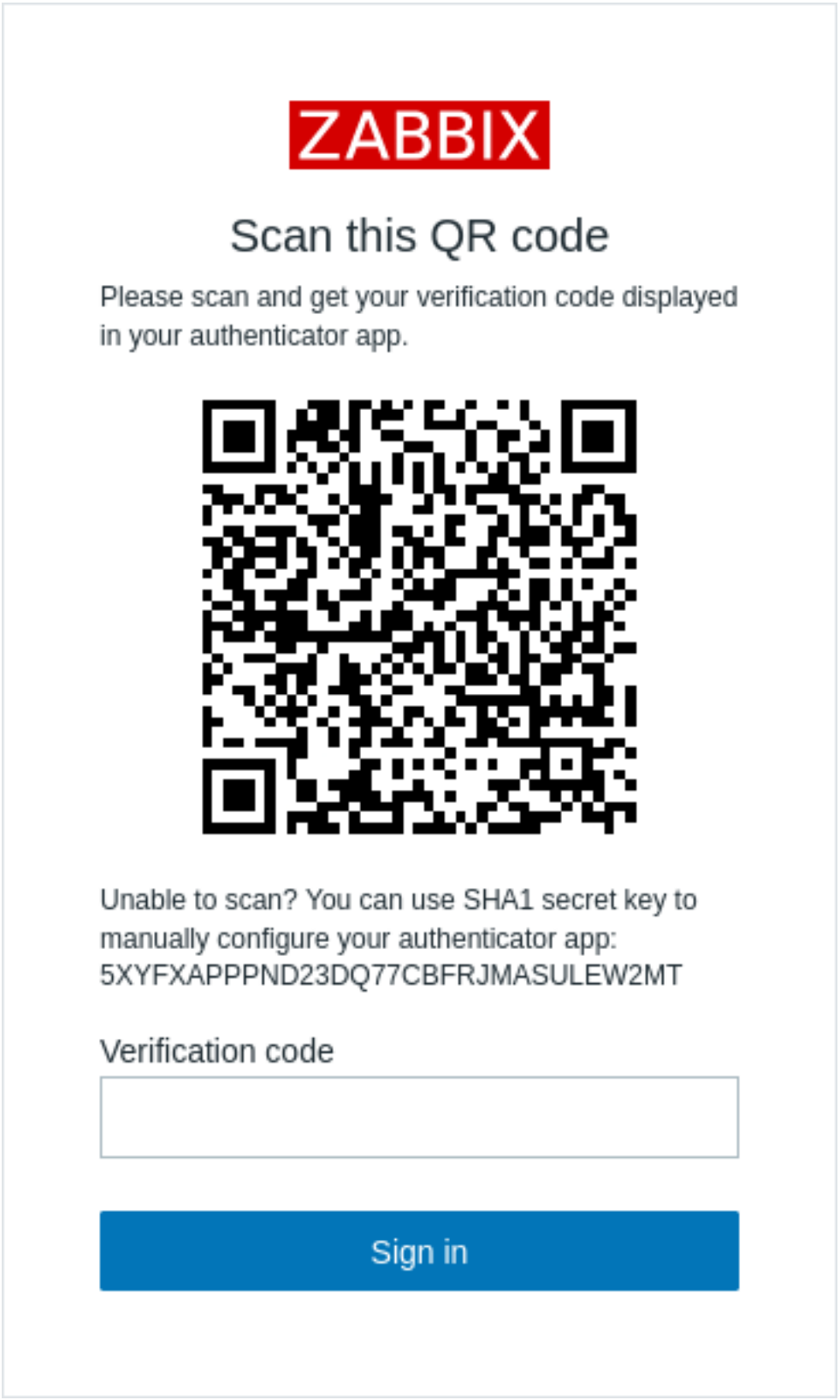
- Typ: TOTP
- Nazwa: Zabbix TOTP
- Funkcja skrótu: SHA-1
- Długość kodu: 6

3. Kliknij przycisk *Add*, a następnie przycisk *Update*.

4. Przejdź do *Users* → *User groups* i utwórz nową grupę użytkowników z następującą konfiguracją:

- Nazwa grupy: grupa TOTP
- Użytkownicy: Admin
- Uwierzytelnianie wieloskładnikowe: Default (lub „Zabbix TOTP”, jeśli nie jest ustawione jako domyślne)

5. Wyloguj się z Zabbix i zaloguj się ponownie, używając swoich poświadczeń. Po pomyślnym zalogowaniu zostaniesz poproszony o zapisanie się do MFA; zostanie wyświetlony kod QR oraz tajny klucz.



6. Zeskanuj kod QR lub wprowadź tajny klucz do aplikacji Google Authenticator. Aplikacja wygeneruje kod weryfikacyjny, który należy wprowadzić, aby zakończyć proces logowania.

7. Przy kolejnych logowaniach pobierz kod weryfikacyjny z aplikacji Google Authenticator i wprowadź go podczas logowania.

Duo Universal Prompt

W przypadku Duo Universal Prompt użytkownicy muszą zweryfikować swoją tożsamość za pomocą aplikacji uwierzytelniającej Duo Mobile.

Attention:
Metoda MFA Duo Universal Prompt wymaga zainstalowania rozszerzenia php-curl, dostępu do Zabbix przez HTTPS oraz uprawnień do połączeń wychodzących do serwerów Duo. Ponadto, jeśli włączono Content Security Policy (CSP) na serwerze WWW, należy dodać „duo.com" do dyrektywy CSP w pliku konfiguracyjnym hosta wirtualnego.

1. Zarejestruj bezpłatne konto administratora Duo na stronie Duo Signup.

2. Otwórz panel administracyjny Duo, przejdź do *Applications* → *Protect an Application*, wyszukaj aplikację *Web SDK* i kliknij *Protect*.

3. Zanotuj dane uwierzytelniające (Client ID, Client secret, API hostname) wymagane do skonfigurowania metody MFA w Zabbix.

4. Przejdź do ustawień MFA w Zabbix w sekcji *Users* → *Authentication* i włącz uwierzytelnianie wieloskładnikowe.

5. Dodaj nową metodę MFA z następującą konfiguracją:

   - Typ: Duo Universal Prompt
   - Nazwa: Zabbix Duo
   - API hostname: (użyj API hostname z Duo)
   - Client ID: (użyj Client ID z Duo)
   - Client secret: (użyj Client secret z Duo)

6. Kliknij przycisk *Add*, a następnie przycisk *Update*.

7. Przejdź do *Users* → *User groups* i utwórz nową grupę użytkowników z następującą konfiguracją:

   - Nazwa grupy: Duo group
   - Użytkownicy: Admin
   - Uwierzytelnianie wieloskładnikowe: Default (lub „Zabbix Duo", jeśli nie jest ustawione jako domyślne)

8. Wyloguj się z Zabbix i zaloguj się ponownie, używając swoich danych uwierzytelniających. Po pomyślnym zalogowaniu pojawi się monit o zapisanie się do MFA i nastąpi przekierowanie do Duo. Dokończ konfigurację Duo i zweryfikuj użytkownika za pomocą aplikacji Duo na telefonie, aby się zalogować.

9. Przy kolejnych logowaniach użyj odpowiedniej metody MFA udostępnianej przez aplikację Duo (takiej jak pobranie kodu weryfikacyjnego, odpowiedź na powiadomienia push lub użycie kluczy sprzętowych) i wprowadź wymagane informacje podczas logowania.

9 Administracja

Przegląd

Menu Administracja służy do funkcji administracyjnych Zabbix. To menu jest dostępne wyłącznie dla użytkowników typu SuperAdmin.

1 Informacje ogólne

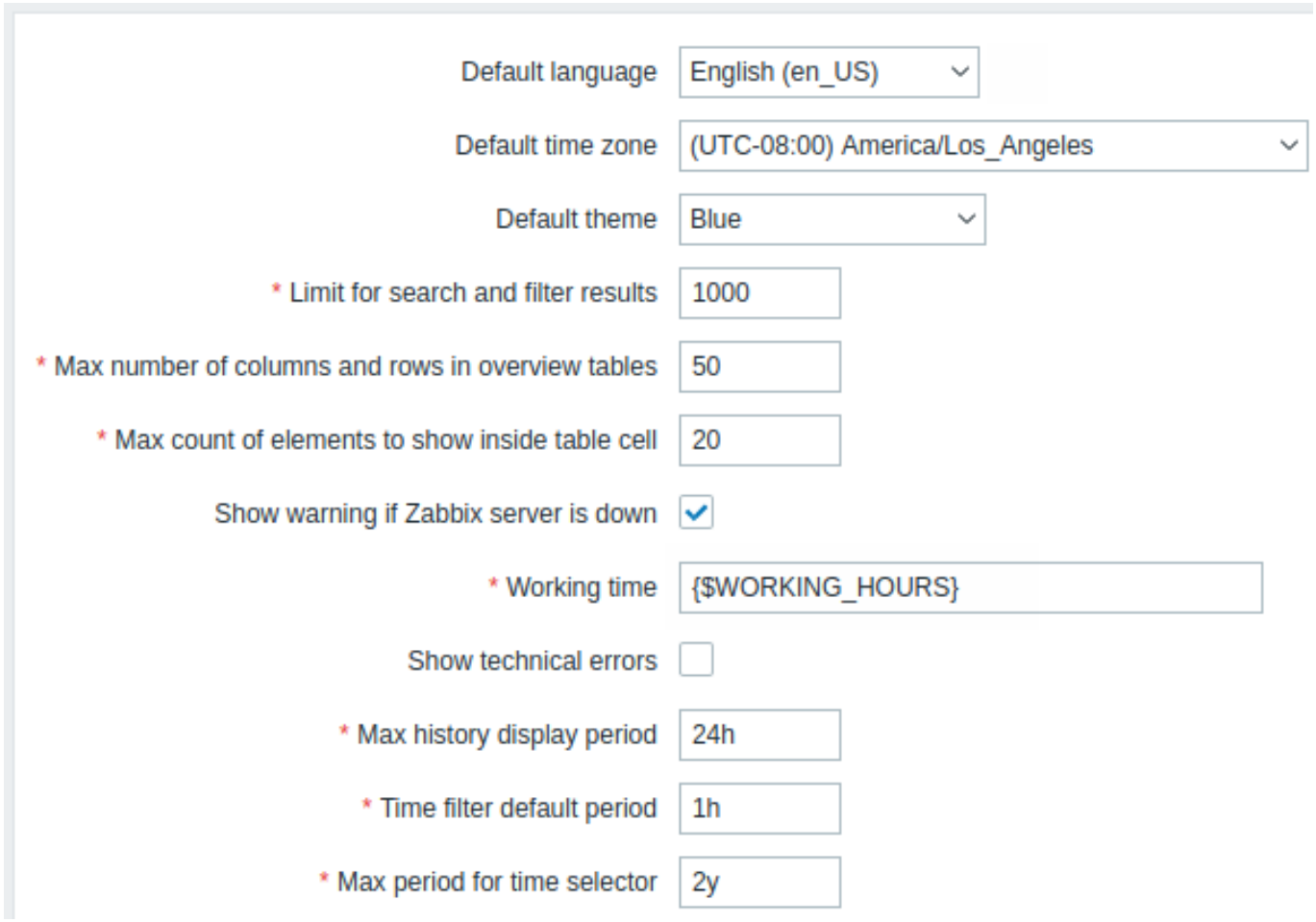
Przegląd

Sekcja *Administracja* → *Ogólne* zawiera szereg podsekcji do ustawiania domyślnych wartości związanych z frontend oraz dostosowywania Zabbix.

Lista dostępnych podsekcji pojawia się po kliknięciu *Ogólne* w sekcji menu *Administracja*. Możliwe jest również przełączanie się między podsekcjami za pomocą rozwijanej listy tytułu w lewym górnym rogu.

GUI

Ta sekcja umożliwia dostosowanie kilku domyślnych ustawień związanych z frontend.



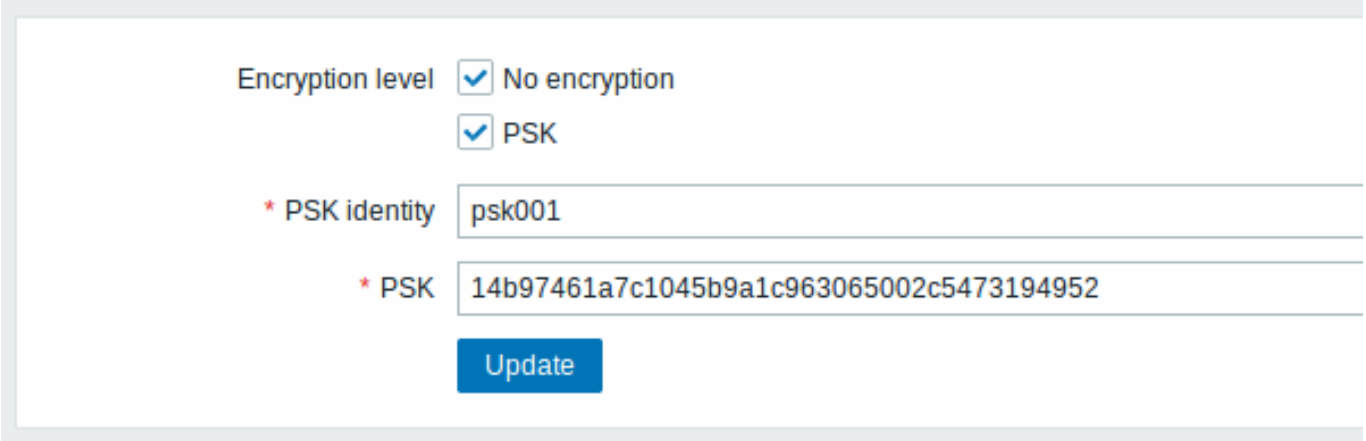
Parametry konfiguracyjne:

Parametr	Opis
Domyślny język	Domyślny język dla użytkowników, którzy nie określili języka w swoich profilach, oraz dla użytkowników gościnnych. Więcej informacji można znaleźć w sekcji Installation of additional frontend languages.
Domyślna strefa czasowa	Domyślna strefa czasowa dla użytkowników, którzy nie określili strefy czasowej w swoich profilach, oraz dla użytkowników gościnnych.
Domyślny motyw	Domyślny motyw dla użytkowników, którzy nie określili motywu w swoich profilach, oraz dla użytkowników gościnnych.
Limit wyników wyszukiwania i filtrowania	Maksymalna liczba elementów (wierszy), które będą wyświetlane na liście w interfejsie webowym, na przykład w *Data collection > Hosts*. *Uwaga*: Jeśli ustawiono na przykład wartość „50”, we wszystkich odpowiednich listach frontend będzie wyświetlał tylko pierwszych 50 elementów. Jeśli jakaś lista zawiera więcej niż pięćdziesiąt elementów, będzie to oznaczone znakiem „+” w *”Displaying 1 to 50 of **50+** found”*. Ponadto, jeśli używane jest filtrowanie i nadal istnieje więcej niż 50 pasujących wyników, wyświetlonych zostanie tylko pierwszych 50. Należy pamiętać, że zwiększenie wartości tego parametru może prowadzić do spadku wydajności i zwiększonego zużycia pamięci po stronie serwera WWW.
Maksymalna liczba kolumn i wierszy w tabelach przeglądu	Maksymalna liczba kolumn i wierszy wyświetlanych w widżecie pulpitu *Trigger overview*. Ten sam limit dotyczy zarówno kolumn, jak i wierszy. Jeśli istnieje więcej wierszy i/lub kolumn niż może zostać pokazanych, system wyświetli ostrzeżenie na dole tabeli: ”Not all results are displayed. Please provide more specific search criteria.”
Maksymalna liczba elementów do pokazania wewnątrz komórki tabeli	W przypadku wpisów wyświetlanych w pojedynczej komórce tabeli nie zostanie pokazanych więcej elementów niż skonfigurowano tutaj.
Pokaż ostrzeżenie, jeśli serwer Zabbix jest niedostępny	Ten parametr włącza wyświetlanie komunikatu ostrzegawczego w oknie przeglądarki, jeśli nie można połączyć się z serwerem Zabbix (może być niedostępny). Komunikat pozostaje widoczny nawet wtedy, gdy użytkownik przewinie stronę w dół. Po najechaniu kursorem komunikat jest tymczasowo ukrywany, aby odsłonić znajdującą się pod nim zawartość.

Parametr	Opis
Czas pracy	Ten parametr ogólnosystemowy definiuje godziny pracy. Na wykresach czas pracy jest wyświetlany na białym tle, a czas poza godzinami pracy na szarym. Opis formatu czasu można znaleźć na stronie Time period specification. Obsługiwane są makra użytkownika.
Pokaż błędy techniczne	Jeśli zaznaczone, wszyscy zarejestrowani użytkownicy będą mogli widzieć błędy techniczne (PHP/SQL). Jeśli nie jest zaznaczone, informacje te są dostępne tylko dla Zabbix Super Admins oraz użytkowników należących do grup użytkowników z włączonym trybem debugowania.
Maksymalny okres wyświetlania historii	Maksymalny okres, dla którego mają być wyświetlane dane historyczne w *Monitoring* > *Latest data*, informacje o scenariuszu WWW hosta w *Monitoring* > *Hosts* oraz w widżecie pulpitu *Top items*. Dozwolony zakres: od 24 godzin (domyślnie) do 1 tygodnia. Obsługiwane są sufiksy czasu, np. 1w (jeden tydzień), 36h (36 godzin).
Domyślny okres filtra czasu	Okres czasu używany domyślnie na wykresach i pulpitach. Dozwolony zakres: od 1 minuty do 10 lat (domyślnie: 1 godzina). Obsługiwane są sufiksy czasu, np. 10m (dziesięć minut), 5w (pięć tygodni). Uwaga: gdy użytkownik zmieni okres czasu podczas przeglądania wykresu, ten okres zostanie zapisany jako preferencja użytkownika, zastępując globalne ustawienie domyślne lub poprzedni wybór użytkownika.
Maksymalny okres dla selektora czasu	Maksymalny dostępny okres czasu dla wykresów i pulpitów. Użytkownicy nie będą mogli wizualizować starszych danych. Dozwolony zakres: od 1 roku do 10 lat (domyślnie: 2 lata). Obsługiwane są sufiksy czasu, np. 1y (jeden rok), 365w (365 tygodni).

Autorejestracja

W tej sekcji można skonfigurować poziom szyfrowania dla aktywnej autorejestracji agent.



Parametry oznaczone gwiazdką są obowiązkowe.

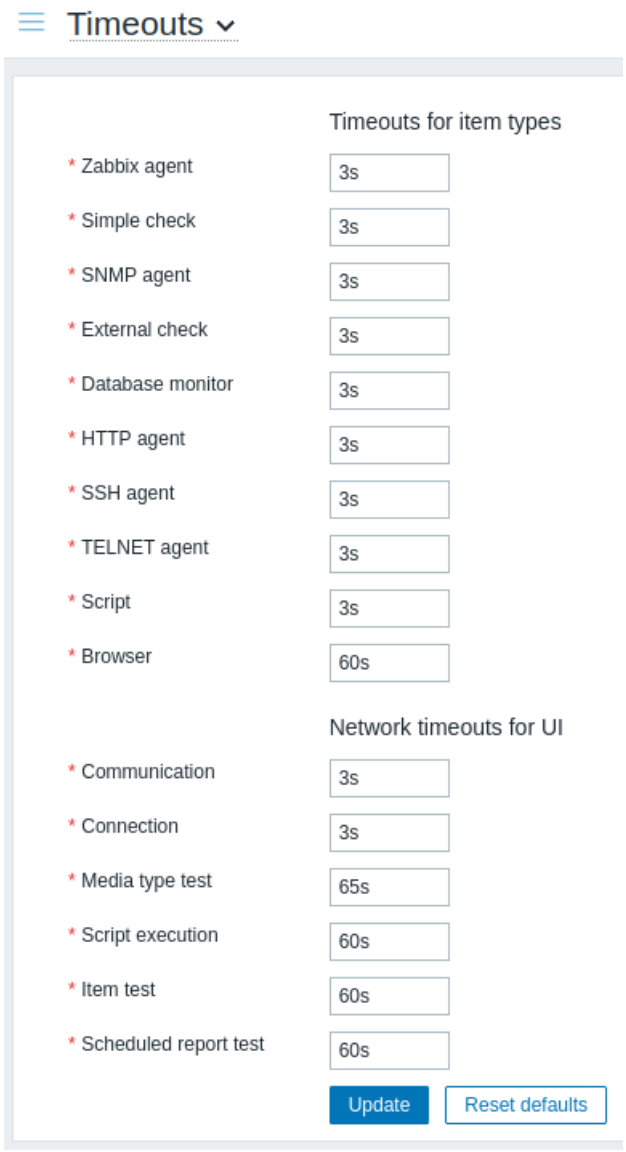
Parametry konfiguracji:

Parameter	Description
Encryption level	Wybierz jedną lub obie opcje poziomu szyfrowania: **No encryption** — dozwolone są połączenia nieszyfrowane **PSK** — dozwolone są połączenia szyfrowane TLS z użyciem klucza współdzielonego
PSK identity	Wprowadź ciąg tożsamości klucza współdzielonego. To pole jest dostępne tylko wtedy, gdy jako *Encryption level* wybrano „PSK”. Nie umieszczaj poufnych informacji w tożsamości PSK, ponieważ jest ona przesyłana przez sieć bez szyfrowania, aby poinformować odbiorcę, którego PSK należy użyć.
PSK	Wprowadź klucz współdzielony (parzystą liczbę znaków szesnastkowych). Maksymalna długość: 512 cyfr szesnastkowych (256-bajtowy PSK), jeśli Zabbix używa biblioteki GnuTLS lub OpenSSL, 64 cyfry szesnastkowe (32-bajtowy PSK), jeśli Zabbix używa biblioteki mbed TLS (PolarSSL). Przykład: 1f87b595725ac58dd977beef14b97461a7c1045b9a1c963065002c5473194952 To pole jest dostępne tylko wtedy, gdy jako *Encryption level* wybrano „PSK”.

Zobacz także: Bezpieczna autorejestracja

Limity czasu

W tej sekcji można ustawić globalne limity czasu dla typów pozycji oraz limity czasu sieci. Wszystkie pola w tym formularzu są obowiązkowe.

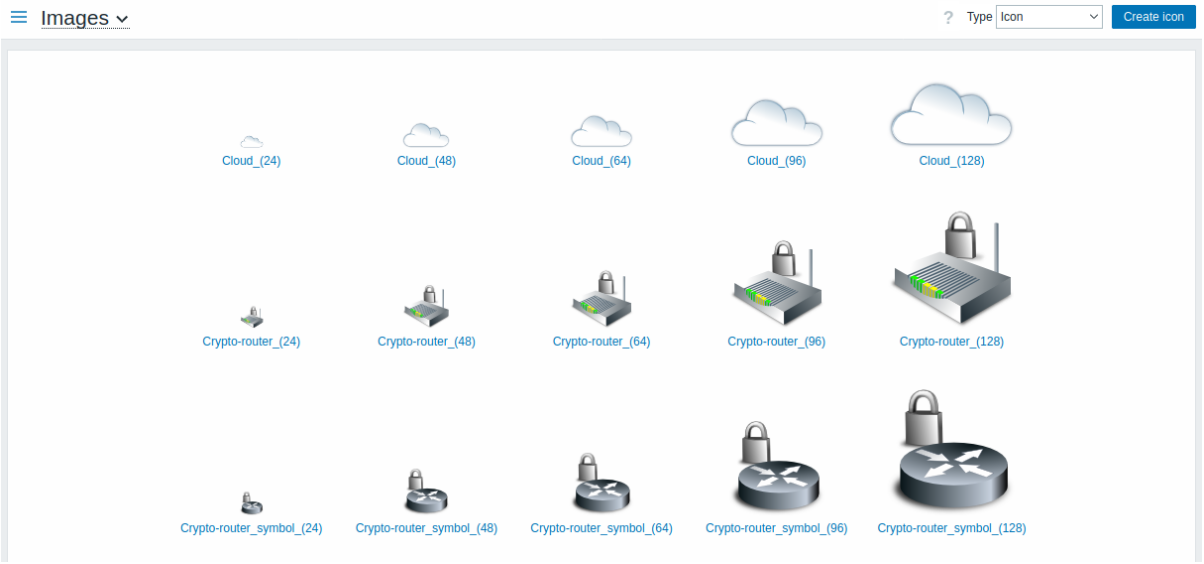


Parametr		Opis
Limity czasu dla typów pozycji		Ile sekund Zabbix powinien czekać przed przerwaniem sprawdzania (na podstawie jego typu). Aby uzyskać dodatkowe informacje i poznać ograniczenia, zobacz limit czasu pozycji. Dozwolony zakres: 1 - 600s (domyślnie: 3s; domyślnie dla pozycji browser: 60s). Obsługiwane są sufiksy czasu, np. 30s, 1m, oraz makra użytkownika. Należy pamiętać, że limity czasu na poziomie proxy, jeśli są skonfigurowane, zastępują te ustawienia globalne. Ponadto, jeśli skonfigurowano limity czasu dla określonych pozycji, zastępują one zarówno ustawienia globalne, jak i ustawienia proxy.
Limity czasu sieci dla UI		
	Komunikacja	Ile sekund czekać przed zamknięciem bezczynnego gniazda (jeśli połączenie z serwerem Zabbix zostało wcześniej nawiązane, ale frontend nie może w tym czasie zakończyć operacji odczytu/wysyłania danych, połączenie zostanie zerwane). Dozwolony zakres: 1 - 300s (domyślnie: 3s).
	Połączenie	Ile sekund czekać przed przerwaniem próby połączenia z serwerem Zabbix. Dozwolony zakres: 1 - 30s (domyślnie: 3s).
	Test typu nośnika	Ile sekund czekać na odpowiedź podczas testowania typu nośnika. Dozwolony zakres: 1 - 300s (domyślnie: 65s).

Parametr		Opis
	Wykonanie skryptu	Ile sekund czekać na odpowiedź podczas wykonywania skryptu. Dozwolony zakres: 1 - 300s (domyślnie: 60s). Ten limit czasu dotyczy całego łańcucha wykonywania skryptu, który może mieć różną długość. Na przykład, jeśli skrypt jest wykonywany na agencie, jest to podróż w obie strony przez serwer (ewentualnie także proxy) do agenta i z powrotem. W przypadku skryptów wykonywanych na agencie obowiązuje limit czasu server lub proxy. W przypadku skryptów wykonywanych tylko na aktywnym agencie prawdopodobne jest, że domyślny limit czasu serwera/proxy musi zostać zwiększony. Limit czasu serwera/proxy musi być wyższy niż częstotliwość odświeżania aktywnego sprawdzania, w przeciwnym razie limit czasu serwera/proxy może zostać przekroczony, zanim aktywny agent w ogóle otrzyma skrypt. Zobacz także: Limit czasu skryptu
	Test pozycji	Ile sekund czekać na zwrócone dane podczas testowania pozycji. Dozwolony zakres: 1 - 600s (domyślnie: 60s).
	Test zaplanowanego raportu	Ile sekund czekać na zwrócone dane podczas testowania zaplanowanego raportu. Dozwolony zakres: 1 - 300s (domyślnie: 60s).

Obrazy

Sekcja Obrazy wyświetla wszystkie obrazy dostępne w Zabbix. Obrazy są przechowywane w bazie danych.

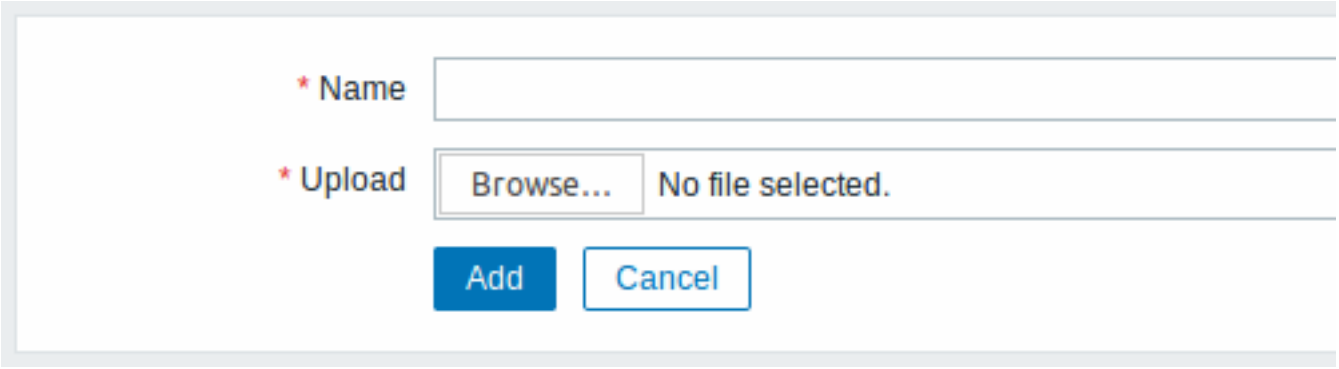


Lista rozwijana *Typ* pozwala przełączać się między ikonami a obrazami tła:

- Ikony są używane do wyświetlania elementów mapy sieci
- Tła są używane jako obrazy tła map sieci

Dodawanie obrazu

Możesz dodać własny obraz, klikając przycisk *Utwórz ikonę* lub *Utwórz tło* w prawym górnym rogu.



Atrybuty obrazu:

Parameter	Description
Name	Unikalna nazwa obrazu.
Upload	Wybierz plik (PNG, JPEG, GIF lub WebP) z lokalnego systemu, który ma zostać przesłany do Zabbix. *Uwaga:* możliwe może być przesłanie także innych formatów, które podczas przesyłania zostaną przekonwertowane do PNG. Do przetwarzania obrazów używana jest biblioteka GD, dlatego obsługiwane formaty zależą od używanej wersji biblioteki (Zabbix wymaga wersji 2.0.28 lub nowszej).

Note:
Maksymalny rozmiar przesyłanego pliku jest ograniczony wartością ZBX_MAX_IMAGE_SIZE, która wynosi 1024x1024 bajtów lub 1 MB.

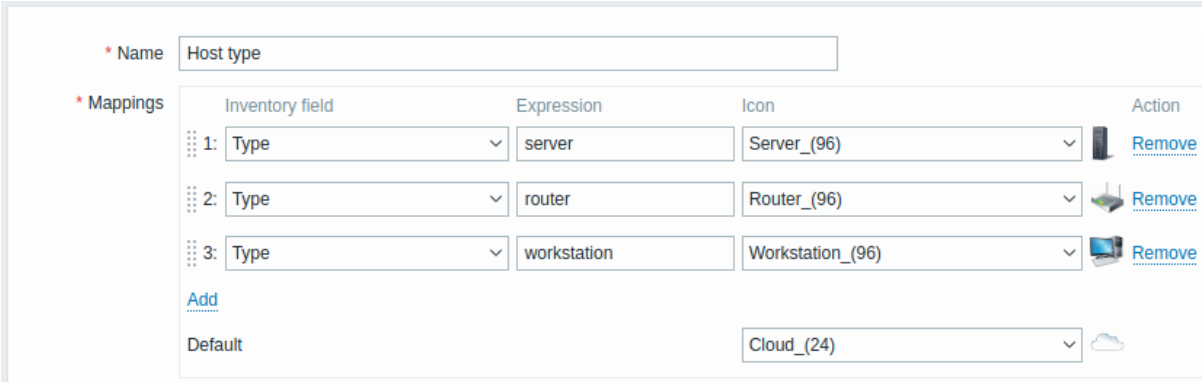
Przesłanie obrazu może się nie powieść, jeśli rozmiar obrazu jest zbliżony do 1 MB, a parametr konfiguracyjny MySQL `max_allowed_packet` ma domyślną wartość 1 MB. W takim przypadku zwiększ parametr max_allowed_packet.

Mapowanie ikon

Ta sekcja umożliwia tworzenie mapowania określonych hostów z określonymi ikonami. Do utworzenia mapowania wykorzystywane są informacje z pól inwentaryzacji hosta.

Mapowania mogą być następnie używane w konfiguracji map sieci do automatycznego przypisywania odpowiednich ikon do pasujących hostów.

Aby utworzyć nową mapę ikon, kliknij *Utwórz mapę ikon* w prawym górnym rogu.



Parametry konfiguracji:

Parametr	Opis
Nazwa	Unikalna nazwa mapy ikon.
Mapowania	Lista mapowań. Kolejność mapowań określa, które z nich będzie miało priorytet. Możesz przesuwać mapowania w górę i w dół listy metodą przeciągnij i upuść.
Pole inwentaryzacji	Pole inwentaryzacji hosta, które będzie sprawdzane w celu znalezienia dopasowania.
Wyrażenie	Wyrażenie regularne opisujące dopasowanie.
Ikona	Ikona używana, jeśli zostanie znalezione dopasowanie do wyrażenia.
Domyślna	Domyślna ikona do użycia.

Wyrażenia regularne

Ta sekcja umożliwia tworzenie niestandardowych wyrażeń regularnych, które mogą być używane w kilku miejscach we frontend. Szczegóły znajdują się w sekcji Wyrażenia regularne.

Opcje wyświetlania wyzwalaczy

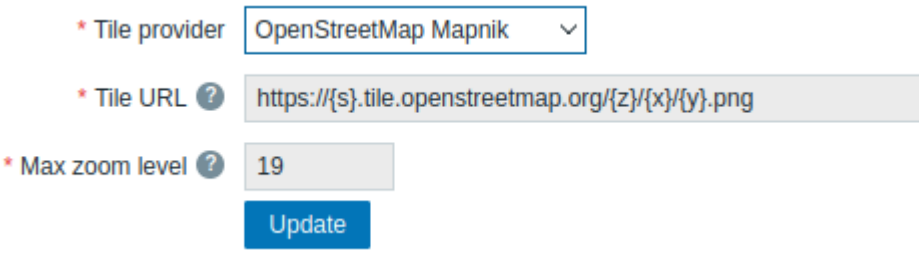
Ta sekcja umożliwia dostosowanie sposobu wyświetlania stanu wyzwalacza we frontendzie oraz nazw i kolorów poziomów ważności wyzwalaczy.



Parametr	Opis
Użyj niestandardowych kolorów statusu zdarzeń	Zaznaczenie tego parametru włącza dostosowanie kolorów dla potwierdzonych/niepotwierdzonych problemów.
Niepotwierdzone zdarzenia PROBLEM, *Potwierdzone zdarzenia PROBLEM*, *Niepotwierdzone zdarzenia RESOLVED*, *Potwierdzone zdarzenia RESOLVED*	Wprowadź nowy kod koloru lub kliknij kolor, aby wybrać nowy z udostępnionej palety. Jeśli pole wyboru *blinking* jest zaznaczone, wyzwalacze będą migać przez pewien czas po zmianie stanu, aby były bardziej widoczne.
Wyświetlaj wyzwalacze OK przez	Okres czasu wyświetlania wyzwalaczy OK. Dozwolony zakres: 0 - 24 godziny. Obsługiwane są sufiksy czasu, np. 5m, 2h, 1d.
Przy zmianie statusu wyzwalacze migają przez	Czas trwania migania wyzwalacza. Dozwolony zakres: 0 - 24 godziny. Obsługiwane są sufiksy czasu, np. 5m, 2h, 1d.
Niesklasyfikowane, *Informacja*, *Ostrzeżenie*, *Średni*, *Wysoki*, *Katastrofa*	Niestandardowe nazwy poziomów ważności i/lub kolory wyświetlane zamiast domyślnych ustawień systemowych. Wprowadź nowy kod koloru lub kliknij kolor, aby wybrać nowy z udostępnionej palety. Zwróć uwagę, że wprowadzone tutaj niestandardowe nazwy poziomów ważności będą używane we wszystkich ustawieniach regionalnych. Jeśli chcesz przetłumaczyć je na inne języki dla określonych użytkowników, zobacz stronę Dostosowywanie poziomów ważności wyzwalaczy.

Mapy geograficzne

Ta sekcja umożliwia wybór dostawcy usługi kafelków map geograficznych oraz konfigurację ustawień dostawcy dla widżetu Geomap na pulpicie nawigacyjnym. Aby zapewnić wizualizację z użyciem map geograficznych, Zabbix korzysta z biblioteki open source Leaflet do interaktywnych map JavaScript. Należy pamiętać, że Zabbix nie ma kontroli nad jakością obrazów dostarczanych przez zewnętrznych dostawców kafelków, w tym predefiniowanych dostawców kafelków.



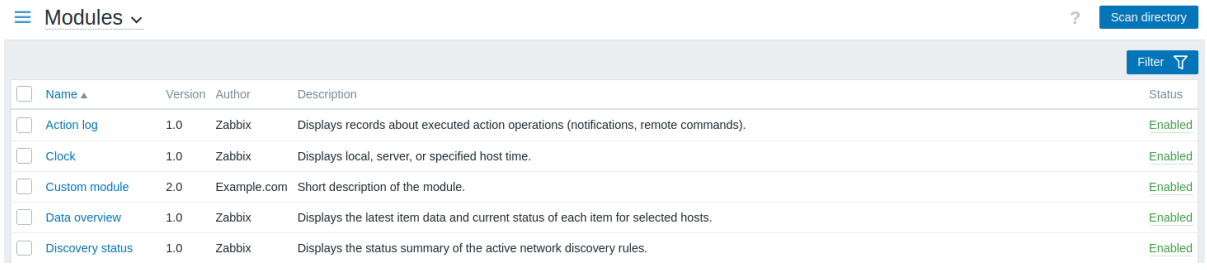
Parametr	Opis
Dostawca kafelków	Wybierz jednego z dostępnych dostawców usługi kafelków lub wybierz *Inne*, aby dodać innego dostawcę kafelków albo kafelki hostowane samodzielnie (zobacz Korzystanie z niestandardowego dostawcy usługi kafelków).
URL kafelków	Szablon adresu URL (do 2048 znaków) do ładowania i wyświetlania warstwy kafelków na mapach geograficznych. To pole można edytować tylko wtedy, gdy *Dostawca kafelków* jest ustawiony na *Inne*. Obsługiwane są następujące symbole zastępcze: *{s}* oznacza jedną z dostępnych subdomen; *{z}* oznacza parametr poziomu powiększenia w adresie URL; *{x}* i *{y}* oznaczają współrzędne kafelka; *{r}* może zostać użyte do dodania „@2x" do adresu URL w celu załadowania kafelków retina. Przykład: `https://{s}.example.com/{z}/{x}/{y}{r}.png`
Tekst atrybucji	Tekst atrybucji dostawcy kafelków wyświetlany w małym polu tekstowym na mapie. To pole jest widoczne tylko wtedy, gdy *Dostawca kafelków* jest ustawiony na *Inne*.
Maksymalny poziom powiększenia	Maksymalny poziom powiększenia mapy. To pole można edytować tylko wtedy, gdy *Dostawca kafelków* jest ustawiony na *Inne*.

Korzystanie z niestandardowego dostawcy usługi kafelków

Widget Geomap może wczytywać rastrowe obrazy kafelków z niestandardowej, samodzielnie hostowanej usługi dostawcy kafelków lub od zewnętrznego dostawcy. Aby użyć niestandardowej usługi zewnętrznego dostawcy kafelków albo samodzielnie hostowanego folderu kafelków lub serwer, wybierz *Other* w polu *Tile provider* i podaj niestandardowy URL w polu *Tile URL*, używając odpowiednich symboli zastępczych.

Moduły

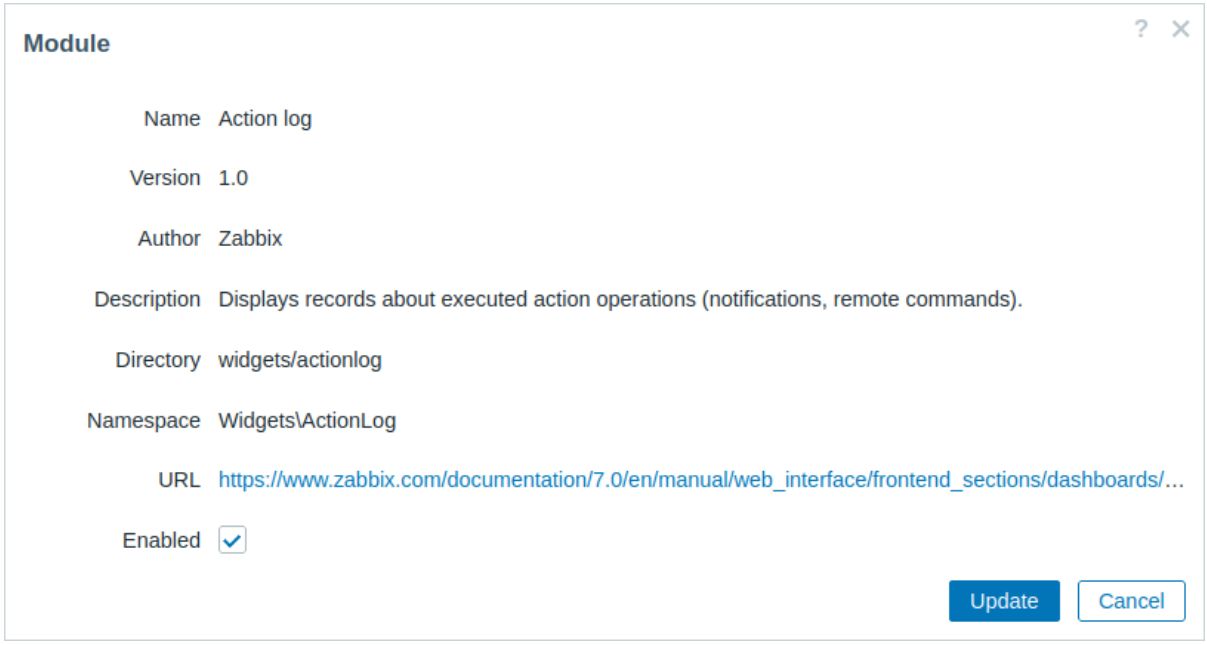
Ta sekcja umożliwia zarządzanie niestandardowymi, a także wbudowanymi modułami frontend.



Kliknij *Skanuj katalog*, aby zarejestrować/wyrejestrować dowolne moduły niestandardowe. Zarejestrowane moduły pojawią się na liście; niezarejestrowane moduły zostaną z niej usunięte.

Kliknij status modułu na liście, aby włączyć/wyłączyć moduł. Możesz także zbiorczo włączać/wyłączać moduły, zaznaczając je na liście, a następnie klikając przyciski *Włącz/Wyłącz* poniżej listy.

Kliknij nazwę modułu na liście, aby wyświetlić jego szczegóły w wyskakującym oknie.

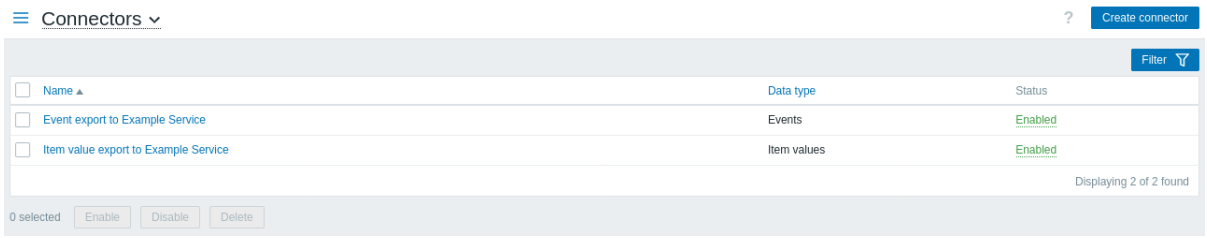


Status modułu można również zaktualizować w wyskakującym oknie szczegółów modułu; w tym celu zaznacz/odznacz pole wyboru *Włączony*, a następnie kliknij *Aktualizuj*.

Możesz filtrować moduły według nazwy lub statusu (włączony/wyłączony).

Konektory

Ta sekcja umożliwia konfigurację konektorów do przesyłania strumieniowego danych Zabbix do systemów zewnętrznych przez HTTP.



Kliknij *Utwórz konektor*, aby skonfigurować nowy konektor.

Możesz filtrować konektory według nazwy lub statusu (włączony/wyłączony). Kliknij status konektora na liście, aby go włączyć/wyłączyć.
Możesz także zbiorczo włączać/wyłączać konektory, zaznaczając je na liście, a następnie klikając przyciski *Włącz/Wyłącz* poniżej listy.

Inne

Ta sekcja umożliwia konfigurację różnych pozostałych parametrów frontend.



Parametr	Opis
URL frontend	Adres URL (do 2048 znaków) do interfejsu webowego Zabbix. Ten parametr jest używany przez usługę webową Zabbix do komunikacji z frontend i powinien zostać określony, aby włączyć raporty cykliczne.
Grupa dla wykrytych hostów	Hosty wykryte przez wykrywanie sieci oraz autorejestrację agent zostaną automatycznie umieszczone w wybranej tutaj grupie hostów.
Domyślny tryb inwentaryzacji hosta	Domyślny tryb inwentaryzacji hosta. Będzie stosowany zawsze, gdy nowy host lub prototyp hosta zostanie utworzony przez serwer lub frontend, chyba że zostanie nadpisany podczas wykrywania/autorejestracji hosta przez operację *Ustaw tryb inwentaryzacji hosta*.

Parametr	Opis
Grupa użytkowników dla komunikatu o niedostępności bazy danych	Grupa użytkowników do wysyłania komunikatu alarmowego lub 'Brak'. Serwer Zabbix zależy od dostępności bazy danych backend. Nie może działać bez bazy danych. Jeśli baza danych jest niedostępna, wybrani użytkownicy mogą zostać powiadomieni przez Zabbix. Powiadomienia będą wysyłane do ustawionej tutaj grupy użytkowników przy użyciu włączonych wpisów mediów użytkownika. Powiadomienia są przesyłane przy użyciu następujących typów mediów (jeśli są włączone): e-mail; SMS; niestandardowe skrypty alertów. Nawet jeśli wpis mediów typu webhook jest skonfigurowany i włączony, nie będzie wyzwalał powiadomień. Serwer Zabbix nie zatrzyma się; będzie czekał, aż baza danych ponownie stanie się dostępna, aby kontynuować przetwarzanie. Powiadomienie składa się z następującej treści: `[MySQL|PostgreSQL] database <DB Name> [on <DB Host>:<DB Port>] is not available: <error message depending on the type of DBMS (database)>` <DB Host> nie jest dodawany do komunikatu, jeśli jest zdefiniowany jako pusta wartość, a <DB Port> nie jest dodawany, jeśli ma wartość domyślną („0"). Menedżer alertów (specjalny proces serwera Zabbix) próbuje ustanowić nowe połączenie z bazą danych co 10 sekund. Jeśli baza danych nadal jest niedostępna, menedżer alertów ponawia wysyłanie alertów, ale nie częściej niż co 15 minut.
Rejestruj niedopasowane pułapki SNMP	Rejestruj pułapkę SNMP, jeśli nie znaleziono odpowiadających interfejsów SNMP.

Autoryzacja

Parametr	Opis
Próby logowania	Liczba nieudanych prób logowania, po której możliwość zalogowania się zostanie zablokowana.
Interwał blokady logowania	Okres, przez który logowanie będzie zabronione po przekroczeniu limitu *Próby logowania*. Dozwolony zakres: 0 - 3600 sekund. Obsługiwane są sufiksy czasu, np. 90s, 5m, 1h.

Przechowywanie sekretów

Parametr	Opis
Dostawca sejfu	Wybierz oprogramowanie do zarządzania sekretami do przechowywania wartości makr użytkownika - *HashiCorp Vault* (domyślnie) lub *CyberArk Vault*.
Rozwiązuj makra sejfu sekretów przez	Rozwiązuj makra sejfu sekretów przez: **serwer Zabbix** - sekrety są pobierane przez serwer Zabbix i przekazywane do proxy, gdy jest to potrzebne (domyślnie); **serwer Zabbix i proxy** - sekrety są pobierane zarówno przez serwer Zabbix, jak i proxy, co pozwala im rozwiązywać makra niezależnie.

Zobacz także: Przechowywanie sekretów.

Bezpieczeństwo

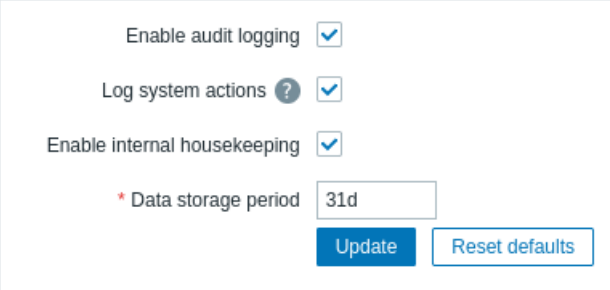
Parametr	Opis
Validate URI schemes	Odznacz to pole wyboru, aby wyłączyć walidację schematów URI (domyślnie włączona). Jeśli jest zaznaczone, możesz określić rozdzieloną przecinkami listę dozwolonych schematów URI (domyślnie: http,https,ftp,file,mailto,tel,ssh). Dotyczy wszystkich pól we frontend, w których używane są URI (na przykład adresów URL elementów mapy).

Parametr	Opis
Use X-Frame-Options HTTP header	Odznacz to pole wyboru, aby wyłączyć nagłówek HTTP X-Frame-options (niezalecane). Jeśli jest zaznaczone, możesz określić wartość nagłówka HTTP X-Frame-options. Obsługiwane wartości: **SAMEORIGIN** (domyślnie) lub **'self'** (musi być ujęte w pojedyncze cudzysłowy) - strona może być wyświetlana w ramce tylko w tym samym źródle co sama strona; **DENY** lub **'none'** (musi być ujęte w pojedyncze cudzysłowy) - strona nie może być wyświetlana w ramce, niezależnie od witryny próbującej to zrobić; **ciąg nazw hostów oddzielonych spacjami**; dodanie **'self'** (musi być ujęte w pojedyncze cudzysłowy) do listy pozwala na wyświetlanie strony w ramce w tym samym źródle co sama strona. Zwróć uwagę, że użycie **'self'** lub **'none'** bez pojedynczych cudzysłowów spowoduje potraktowanie ich jako nazw hostów.
Use iframe sandboxing	Odznacz to pole wyboru, aby wyłączyć umieszczanie zawartości pobranego adresu URL w sandboxie (niezalecane). Jeśli jest zaznaczone, możesz określić wyjątki sandboxingu iframe; nieokreślone ograniczenia nadal będą stosowane. Jeśli to pole jest puste, zastosowanie mają wszystkie ograniczenia atrybutu sandbox. Aby uzyskać więcej informacji, zobacz opis atrybutu `sandbox`.

2 Dziennik audytu

Przegląd

Ta sekcja umożliwia konfigurację ustawień dziennika audytu.



Dostępne są następujące parametry:

Parametr	Opis
Włącz rejestrowanie audytu	Włącz (domyślnie) lub wyłącz rejestrowanie audytu.
Rejestruj działania systemowe	Włącz (domyślnie) lub wyłącz rejestrowanie audytu działań związanych z wykrywaniem niskiego poziomu, wykrywaniem sieci oraz autorejestracją wykonywanych przez serwer (użytkownik systemowy).
Włącz wewnętrzny housekeeping	Włącz (domyślnie) lub wyłącz wewnętrzny housekeeping dla rekordów dziennika audytu.
Okres przechowywania danych	Liczba dni, przez które rekordy dziennika audytu powinny być przechowywane, zanim zostaną usunięte przez housekeeper. Wymagane, jeśli housekeeping jest włączony. Domyślnie: 31 dni.

Parametry kompresji dziennika audytu są dostępne w sekcji *Administracja* > *Housekeeping*, w bloku *Kompresja historii, trendów i dziennika audytu*, który staje się widoczny przy użyciu TimescaleDB.

3 Porządkowanie danych

Przegląd

Sekcja *Administracja* > *Housekeeping* umożliwia skonfigurowanie wewnętrznego mechanizmu housekeeping w Zabbix, który automatycznie usuwa z bazy danych nieaktualne dane lub dane usunięte przez użytkownika. Zapobiega to nieograniczonemu wzrostowi bazy danych, który prowadziłby do niepotrzebnego zużycia miejsca na dysku i pogorszenia wydajności bazy danych.

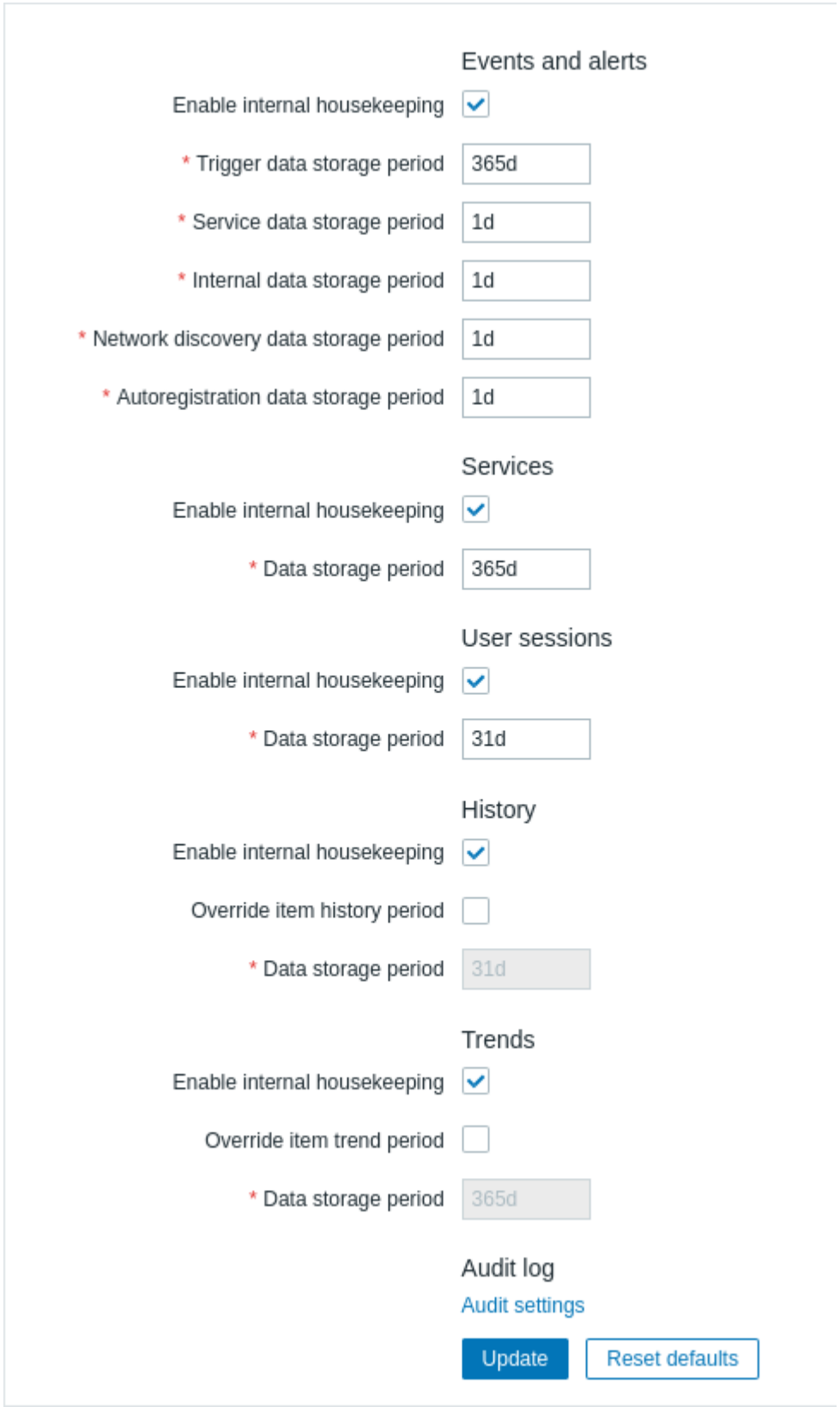
Housekeeping można włączyć i skonfigurować dla następujących typów danych:

- Zdarzenia i alerty z wyzwalaczy, usług, danych wewnętrznych, wykrywania sieci i autorejestracji
- Usługi
- Sesje użytkowników
- Historia i trendy dla pozycji

Note:
Housekeeping dziennika audytu jest konfigurowany oddzielnie.

Konfiguracja

Dostępne są następujące parametry:



Parametr	Opis
Włącz wewnętrzny housekeeping	Włącz lub wyłącz wewnętrzny housekeeping (domyślnie włączony). Jeśli jest włączony, procedura housekeeping automatycznie usuwa z bazy danych dane przekraczające *Okres przechowywania danych*.

Parametr	Opis
Okres przechowywania danych	Określ, jak długo dane mają być przechowywane, zanim zostaną usunięte przez housekeeper. Wymagane, jeśli wewnętrzny housekeeping jest włączony. Zakres: od 1 dnia (1 godzina dla historii) do 25 lat; lub „0". Obsługiwane są sufiksy czasu (np. 1d, 1w). Dla *Zdarzeń i alertów* okres przechowywania danych jest ustawiany oddzielnie dla wyzwalaczy, usług, danych wewnętrznych, wykrywania sieci i autorejestracji. Housekeeper usuwa tylko te zdarzenia, które nie są powiązane z problemami. Na przykład zdarzenie problemu/odzyskania starsze niż *Okres przechowywania danych* nie zostanie usunięte, jeśli jest powiązane z nierozwiązanym problemem. Gdy housekeeper usuwa nieaktualne obiekty, najpierw usuwa problemy, a następnie zdarzenia. Dla *Historii* i *Trendów* okresy przechowywania danych określają również, jak długo dane pozostają widoczne w *Monitoring* > *Najnowsze dane*, nawet jeśli wewnętrzny housekeeping jest wyłączony. Należy pamiętać, że po usunięciu pozycji lub wyzwalacza usuwane są również jego problemy i powiązane zdarzenia.
Zastąp okres historii pozycji	Jeśli opcja jest włączona, okres przechowywania historii/trendów określony w konfiguracji pozycji jest zastępowany ustawieniem *Okres przechowywania danych* (z wyjątkiem pozycji z włączoną opcją *Nie przechowuj*). Tej opcji można używać nawet wtedy, gdy wewnętrzny housekeeping jest wyłączony i używany jest zewnętrzny housekeeper.
Zastąp okres trendów pozycji	

W przypadku używania **TimescaleDB** dostępna staje się sekcja *Kompresja historii, trendów i dziennika audytu*.

Note:
W przypadku TimescaleDB włącz opcje *Zastąp okres historii pozycji*, *Zastąp okres trendów pozycji* oraz *Włącz wewnętrzny housekeeping* dla historii i trendów, aby w pełni korzystać z automatycznego partycjonowania. Jeśli te opcje są wyłączone, dane przechowywane w tabelach historii i trendów nadal będą partycjonowane, ale housekeeper nie będzie usuwał nieaktualnych partycji i będą wyświetlane ostrzeżenia konfiguracyjne. Gdy usuwanie nieaktualnych partycji jest włączone, serwer Zabbix i frontend nie będą już śledzić usuniętych pozycji, a historia tych pozycji zostanie wyczyszczona po usunięciu nieaktualnej partycji.

Przycisk *Przywróć domyślne* umożliwia cofnięcie wszystkich wprowadzonych zmian.

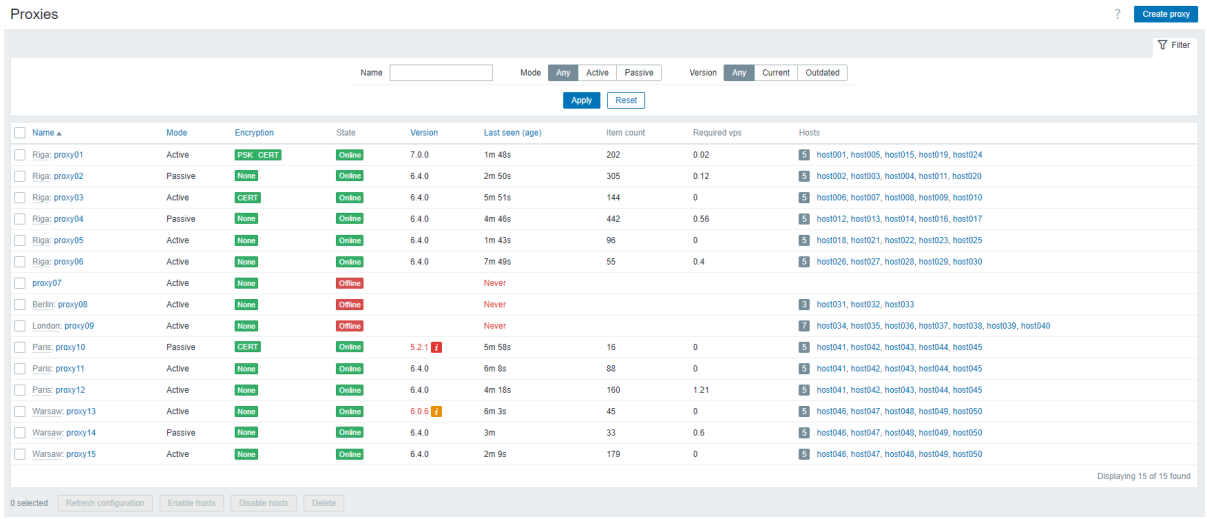
4 Proxy

Przegląd

W sekcji *Administracja* → *Proxy* można skonfigurować proxy do monitorowania rozproszonego w frontendzie Zabbix.

Proxy

Wyświetlana jest lista istniejących proxy wraz z ich szczegółami.



Wyświetlane dane:

Column	Description
Name	Nazwa proxy. Kliknięcie nazwy proxy otwiera formularz konfiguracji proxy. Jeśli proxy należy do grupy proxy, nazwa grupy jest wyświetlana przed nazwą proxy jako szary odnośnik. Kliknięcie nazwy grupy otwiera formularz konfiguracji grupy proxy.
Mode	Tryb proxy — *Aktywny* lub *Pasywny*.
Encryption	Stan szyfrowania połączeń z proxy: **Brak** — brak szyfrowania; **PSK** — użycie klucza współdzielonego; **Cert** — użycie certyfikatu.
State	Stan proxy: **Nieznany** — proxy zostało utworzone, gdy serwer Zabbix był wyłączony, lub serwer nie zaktualizował jeszcze stanu; **Online** — proxy komunikowało się z serwerem Zabbix (pasywny proxy odpowiedział na żądanie serwera; aktywny proxy wysłał żądanie) w okresie failover; **Offline** — proxy nie komunikowało się z serwerem Zabbix w okresie failover.
Version	Wersja proxy (trzycyfrowy numer wersji). Jeśli proxy jest przestarzałe lub nieobsługiwane, numer wersji jest wyróżniony (na czerwono), a wyświetlana jest ikona statusu informacyjnego (żółta lub czerwona). Najedź kursorem na ikonę, aby zobaczyć szczegóły.
Last seen (age)	Czas, kiedy proxy było ostatnio widziane przez serwer.
Item count	Liczba włączonych pozycji na włączonych hostach przypisanych do proxy.
Required vps	Wymagana wydajność proxy (liczba wartości, które muszą być zbierane na sekundę).
Hosts	Liczba włączonych hostów przypisanych do proxy oraz lista hostów monitorowanych przez proxy. Kliknięcie nazwy hosta otwiera formularz konfiguracji hosta.

Aby skonfigurować nowe proxy, kliknij przycisk *Create proxy* w prawym górnym rogu.

Opcje masowej edycji

Przyciski pod listą oferują kilka opcji masowej edycji:

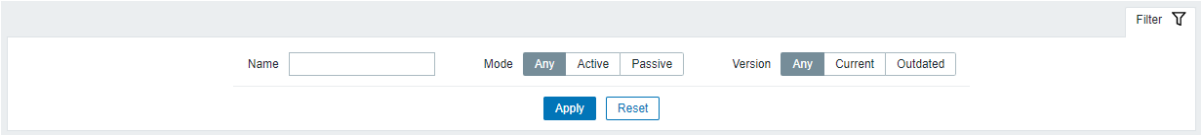
- *Odśwież konfigurację* - odśwież konfigurację proxy;
- *Włącz hosty* - zmień status hostów monitorowanych przez proxy na *Monitorowany*;
- *Wyłącz hosty* - zmień status hostów monitorowanych przez proxy na *Niemonitorowany*;
- *Usuń* - usuń proxy.

Aby użyć tych opcji, zaznacz pola wyboru przy odpowiednich proxy, a następnie kliknij wymagany przycisk.

Używanie filtra

Możesz użyć filtra, aby wyświetlić tylko te proxy, które Cię interesują. Dla lepszej wydajności wyszukiwania dane są przeszukiwane z nierozwiniętymi makrami.

Link *Filtr* jest dostępny nad listą proxy. Po jego kliknięciu pojawi się filtr, w którym można filtrować proxy według nazwy, trybu i wersji. Zwróć uwagę, że opcja filtra *Nieaktualne* wyświetla zarówno nieaktualne (częściowo obsługiwane), jak i nieobsługiwane proxy.



5 Grupy proxy

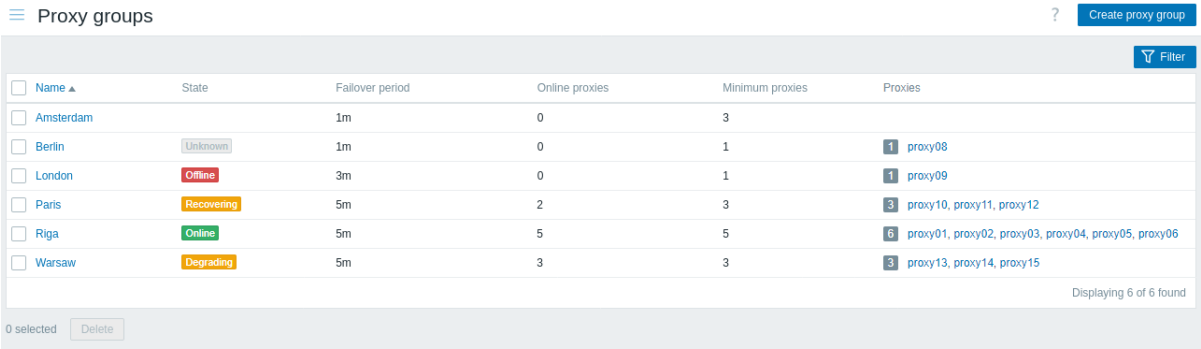
Przegląd

W *Administracja* → *Grupy proxy* można skonfigurować grupy proxy.

Grupy proxy są używane w równoważeniu obciążenia proxy z automatyczną dystrybucją hostów między proxy oraz wysoką dostępnością między proxy.

Grupy proxy

Wyświetlana jest lista istniejących grup proxy wraz z ich szczegółami.



Wyświetlane dane:

Kolumna	Opis
Nazwa	Nazwa grupy proxy. Kliknięcie nazwy grupy proxy otwiera formularz konfiguracji grupy proxy.
Stan	Stan grupy proxy (wyświetlany, jeśli grupa zawiera co najmniej jeden proxy): **Nieznany** — grupa została utworzona, gdy serwer Zabbix był wyłączony, lub serwer nie zaktualizował jeszcze stanu; **Online** — minimalna liczba proxy komunikowała się z serwerem Zabbix w okresie przełączenia awaryjnego; **Pogarszający się** — grupa wkrótce przejdzie w stan offline, ponieważ liczba proxy online spadła poniżej progu *Minimalna liczba proxy*; **Offline** — mniej niż minimalna liczba proxy komunikowała się z serwerem Zabbix w okresie przełączenia awaryjnego; **Odzyskiwanie** — grupa wkrótce wróci do stanu online, ponieważ liczba proxy online osiągnęła próg *Minimalna liczba proxy*. Stan grupy proxy można monitorować za pomocą pozycji zabbix[proxy group,<name>,state] oraz zabbix[proxy group,discovery].
Okres przełączenia awaryjnego	Okres, w którym proxy w grupie proxy musi komunikować się z serwerem Zabbix, aby był uznawany za online.
Proxy online	Liczba proxy online (wyświetlana na czerwono, jeśli jest niższa od minimum grupy).
Minimalna liczba proxy	Minimalna liczba proxy online wymagana do utrzymania grupy proxy w stanie online.
Proxy	Liczba proxy w grupie oraz lista proxy w grupie z odnośnikami do formularza konfiguracji proxy. Maksymalna liczba wyświetlanych proxy jest ograniczona przez wartość *Max count of elements to show inside table cell*.

Aby skonfigurować nową grupę proxy, kliknij przycisk *Create proxy groups* w prawym górnym rogu.

Opcje masowej edycji

Przyciski pod listą oferują kilka opcji masowej edycji:

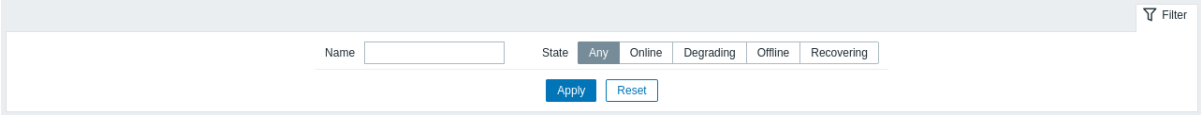
- *Usuń* - usuń grupy proxy.

Aby skorzystać z tych opcji, zaznacz pola wyboru przy odpowiednich grupach proxy, a następnie kliknij wymagany przycisk.

Używanie filtra

Możesz użyć filtra, aby wyświetlić tylko te grupy proxy, które Cię interesują. Dla lepszej wydajności wyszukiwania dane są przeszukiwane z nierozwiniętymi makrami.

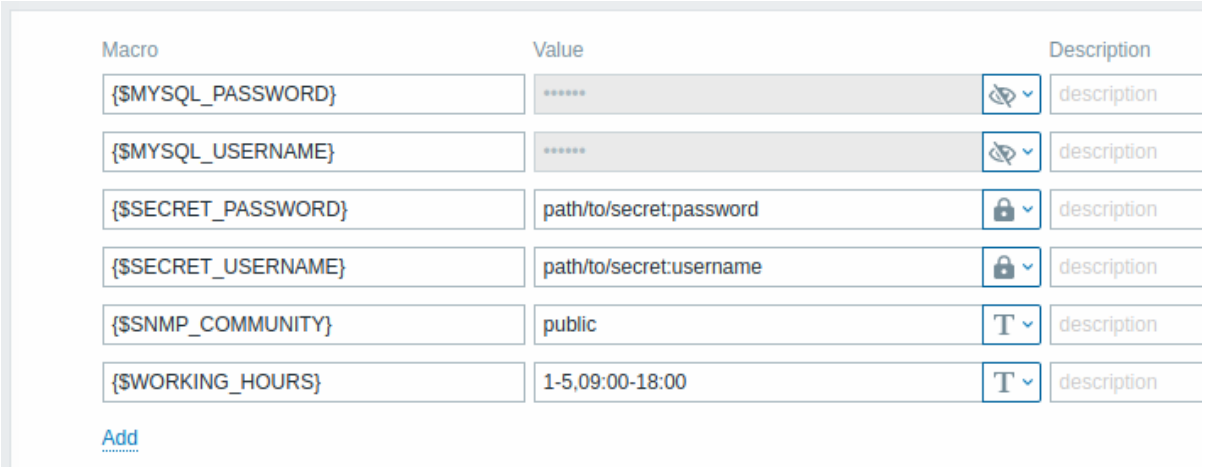
Link *Filtr* jest dostępny nad listą grup proxy. Po jego kliknięciu pojawi się filtr, za pomocą którego można filtrować grupy proxy według nazwy i statusu.



6 Makra

Przegląd

Ta sekcja umożliwia definiowanie globalnych makr użytkownika jako par nazwa-wartość. Należy pamiętać, że wartości makr mogą być przechowywane jako zwykły tekst, tajny tekst lub sekret Vault. Obsługiwane jest również dodawanie opisu.



7 Kolejka

Przegląd

W sekcji *Administracja* → *Kolejka* wyświetlane są pozycje oczekujące na aktualizację.

W idealnej sytuacji po otwarciu tej sekcji wszystko powinno być „zielone”, co oznacza brak pozycji w kolejce. Jeśli wszystkie pozycje są aktualizowane bez opóźnień, żadna z nich nie oczekuje. Jednak z powodu niewystarczającej wydajności serwera niektóre pozycje mogą być opóźnione, a informacje o tym są wyświetlane w tej sekcji. Więcej informacji można znaleźć w sekcji Kolejka.

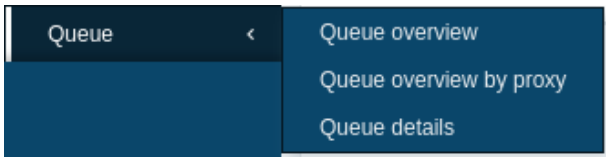
Note:
Zabbix proxy nie uwzględnia okresów konserwacji; szczegóły można znaleźć w sekcji Obliczanie kolejek podczas konserwacji.

Note:
Kolejka jest dostępna tylko wtedy, gdy działa serwer Zabbix. Pozycje nie są uwzględniane w kolejce, jeśli interfejs pozycji staje się niedostępny z powodu problemów z połączeniem lub gdy agent nie działa prawidłowo.

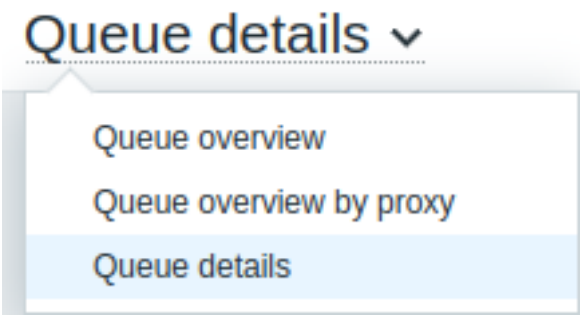
Sekcja *Administracja* → *Kolejka* zawiera następujące strony:

- Przegląd kolejki — wyświetla kolejkę według typu pozycji;
- Przegląd kolejki według proxy — wyświetla kolejkę według proxy;
- Szczegóły kolejki — wyświetla listę opóźnionych pozycji.

Lista dostępnych stron pojawia się po kliknięciu *Kolejka* w sekcji menu *Administracja*. Możliwe jest również przełączanie się między stronami za pomocą listy rozwijanej tytułu w lewym górnym rogu.



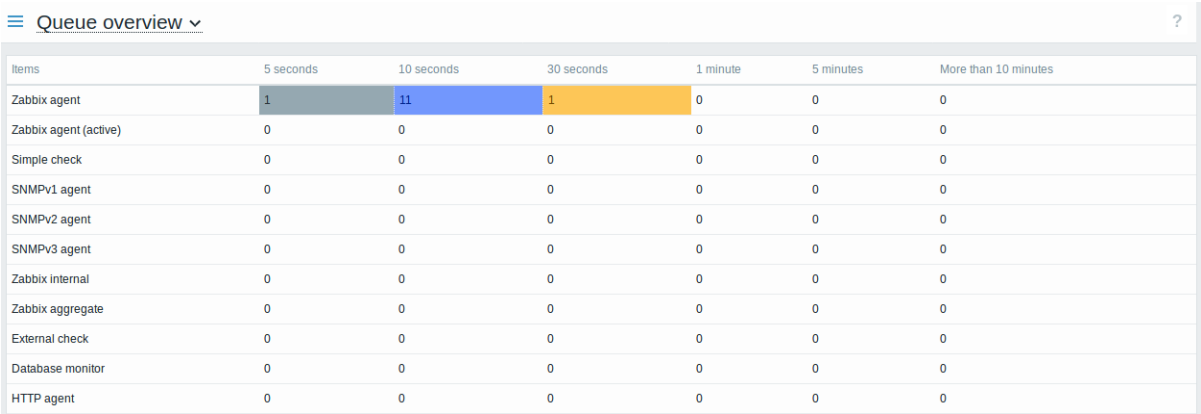
Menu trzeciego poziomu.



Lista rozwijana tytułu.

Przegląd według typu pozycji

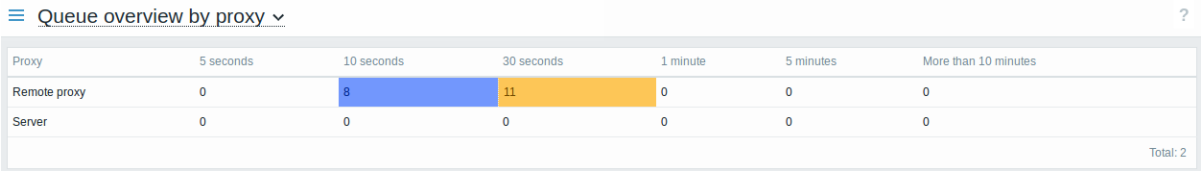
Na tym ekranie łatwo ustalić, czy problem jest związany z jednym czy z kilkoma typami pozycji.



Każdy wiersz zawiera typ pozycji. Każda kolumna pokazuje liczbę oczekujących pozycji — oczekujących odpowiednio przez 5–10 sekund / 10–30 sekund / 30–60 sekund / 1–5 minut / 5–10 minut lub ponad 10 minut.

Przegląd według proxy

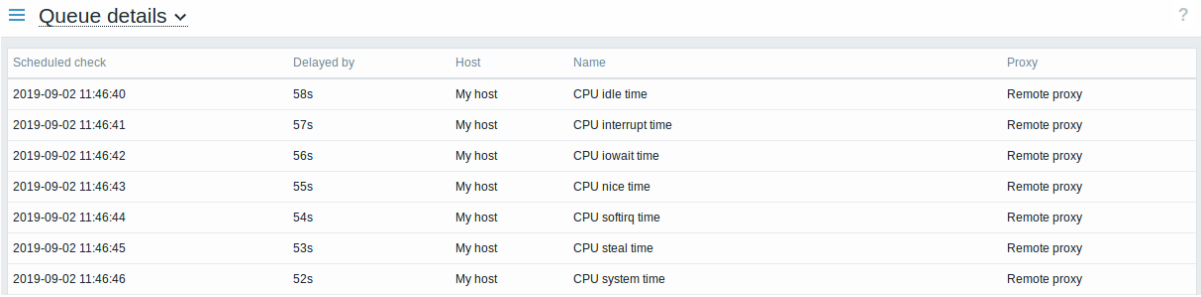
Na tym ekranie łatwo ustalić, czy problem jest związany z jednym z proxy czy z serwerem.



Każdy wiersz zawiera proxy, a na końcu listy znajduje się serwer. Każda kolumna pokazuje liczbę oczekujących pozycji — oczekujących odpowiednio przez 5–10 sekund / 10–30 sekund / 30–60 sekund / 1–5 minut / 5–10 minut lub ponad 10 minut.

Lista oczekujących pozycji

Na tym ekranie wyświetlana jest każda oczekująca pozycja.



Wyświetlane dane:

Kolumna	Opis
Zaplanowane sprawdzenie	Wyświetlany jest czas, w którym sprawdzenie powinno zostać wykonane.
Opóźnienie	Wyświetlana jest długość opóźnienia.
Host	Wyświetlany jest host pozycji.
Nazwa	Wyświetlana jest nazwa oczekującej pozycji.
Proxy	Wyświetlana jest nazwa proxy, jeśli host jest monitorowany przez proxy.

Możliwe komunikaty o błędach

Możesz napotkać sytuację, w której nie są wyświetlane żadne dane i pojawia się następujący komunikat o błędzie:



Komunikat o błędzie w tym przypadku jest następujący:

```
Cannot display item queue. Permission denied
```

Dzieje się tak, gdy parametry konfiguracji PHP w pliku *zabbix.conf.php* — `$ZBX_SERVER` lub oba: `$ZBX_SERVER` i `$ZBX_SERVER_PORT` — wskazują na istniejący serwer Zabbix, który używa innej bazy danych.

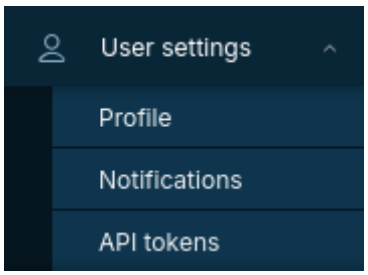
3 Ustawienia użytkownika

Przegląd

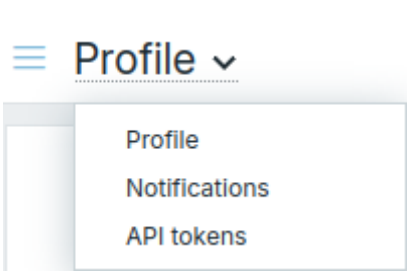
W zależności od uprawnień roli użytkownika sekcja *Ustawienia użytkownika* może zawierać następujące strony:

- *Profil* lub *Profil użytkownika* — do dostosowywania wybranych funkcji frontendu Zabbix;
- *Powiadomienia* — do dostosowywania powiadomień bieżącego użytkownika;
- *Tokeny API* — do zarządzania tokenami API przypisanymi do bieżącego użytkownika.

Lista dostępnych stron pojawia się po kliknięciu ikony użytkownika w dolnej części menu Zabbix (niedostępne dla użytkownika *guest*). Możliwe jest również przełączanie się między stronami za pomocą rozwijanej listy tytułu w lewym górnym rogu.



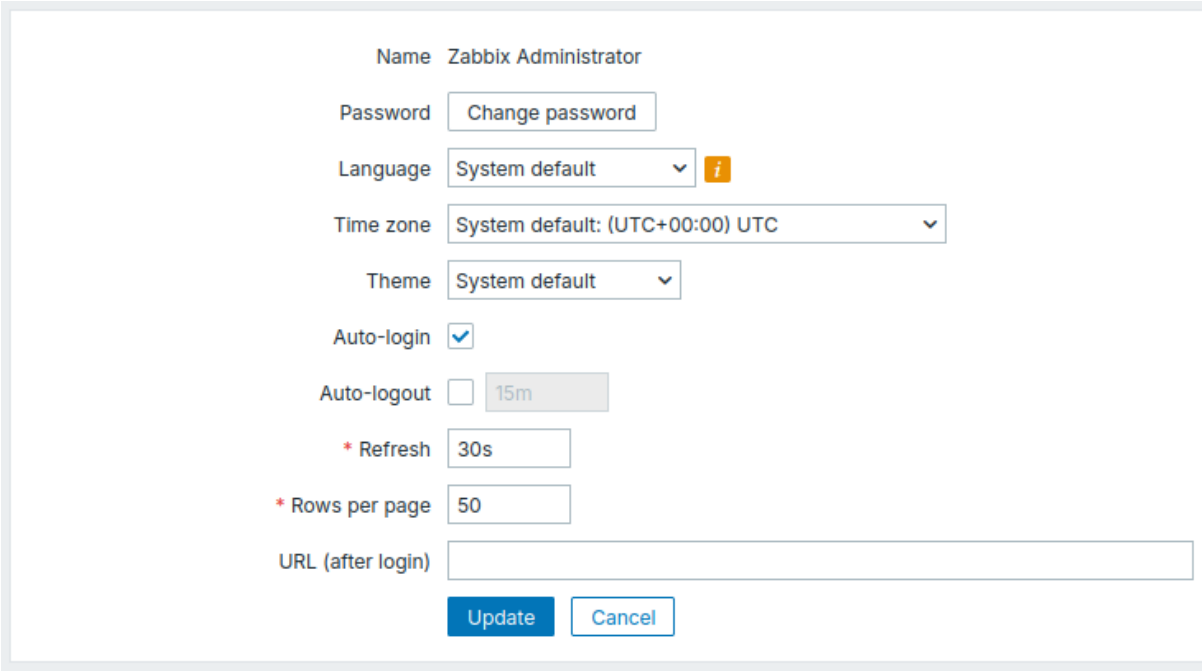
Menu trzeciego poziomu.



Rozwijana lista tytułu.

Profil użytkownika

Sekcja *Profil użytkownika* udostępnia opcje ustawienia niestandardowego języka interfejsu, motywu kolorystycznego, liczby wierszy wyświetlanych na listach itp. Wprowadzone tutaj zmiany zostaną zastosowane tylko do bieżącego użytkownika.



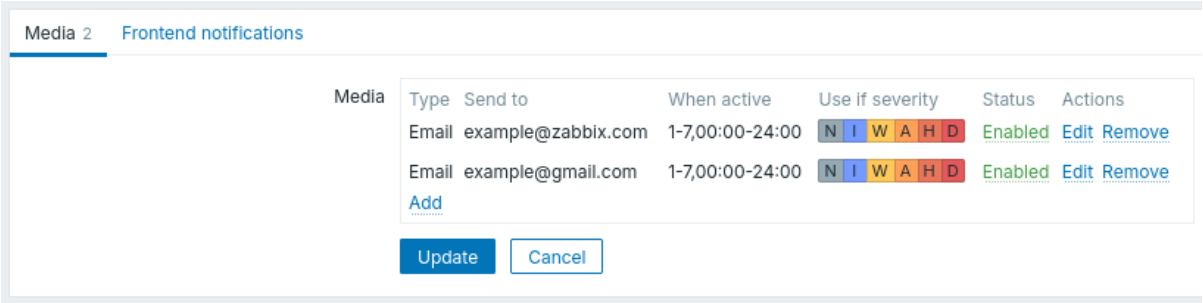
Parametr	Opis
Name	Wyświetlane są imię i nazwisko użytkownika. Jeśli imię i nazwisko nie są dostępne, wyświetlana jest nazwa użytkownika.
Password	Kliknij przycisk *Change password*, aby otworzyć trzy pola: *Old password*, *New password*, *New password (once again)*. Po pomyślnej zmianie hasła użytkownik zostanie wylogowany ze wszystkich aktywnych sesji. Należy pamiętać, że hasło można zmienić tylko dla użytkowników korzystających z uwierzytelniania wewnętrznego Zabbix.
Language	Wybierz preferowany język interfejsu lub wybierz **System default**, aby użyć domyślnych ustawień systemowych. Wybranie *English (en_US)* spowoduje również włączenie amerykańskiego formatu czasu/daty w frontend. Więcej informacji można znaleźć w sekcji Installation of additional frontend languages.
Time zone	Wybierz strefę czasową, aby zastąpić globalną strefę czasową na poziomie użytkownika, lub wybierz **System default**, aby użyć globalnych ustawień strefy czasowej.
Theme	Wybierz motyw kolorystyczny dla swojego profilu: **System default** - użyj domyślnych ustawień systemowych; **Blue** - standardowy niebieski motyw; **Blue (classic)** - standardowy niebieski motyw z użyciem starszych czcionek; **Dark** - alternatywny ciemny motyw; **Dark (classic)** - alternatywny ciemny motyw z użyciem starszych czcionek; **High-contrast light** - jasny motyw o wysokim kontraście; **High-contrast dark** - ciemny motyw o wysokim kontraście.
Auto-login	Zaznacz to pole wyboru, aby Zabbix zapamiętał użytkownika i logował go automatycznie przez 30 dni. Podczas logowania z włączoną opcją *Remember for 30 days*: - Licznik automatycznego wylogowania jest resetowany (sesja trwa do końca 30-dniowego okresu). - Automatyczne logowanie jest włączone przy kolejnych wizytach w ciągu 30 dni. Podczas logowania bez opcji *Remember for 30 days*: - Parametr automatycznego logowania jest czyszczony. - Automatyczne wylogowanie działa zgodnie ze skonfigurowanym limitem czasu jak zwykle. W tym celu używane są pliki cookie przeglądarki.

Parametr	Opis
Auto-logout	Po zaznaczeniu tego pola wyboru użytkownik zostanie automatycznie wylogowany po upływie ustawionej liczby sekund (minimum 90 sekund, maksimum 1 dzień). Obsługiwane są sufiksy czasu, na przykład: 90s, 5m, 2h, 1d. Należy pamiętać, że ta opcja nie będzie działać w następujących przypadkach: * Gdy strony menu *Monitoring* wykonują odświeżanie informacji w tle. Jeśli pozostawione są otwarte strony odświeżające dane w określonym interwale czasu (dashboardy, wykresy, najnowsze dane itp.), czas życia sesji zostaje odpowiednio wydłużony, co wyłącza funkcję automatycznego wylogowania. * W przypadku logowania z zaznaczoną opcją *Remember me for 30 days*; w takim przypadku licznik automatycznego wylogowania jest nadpisywany, a sesja pozostaje aktywna przez cały ten okres. * Gdy uwierzytelnianie jest wykonywane za pośrednictwem dostawcy tożsamości SSO (IdP), automatyczne wylogowanie kończy tylko sesję Zabbix. Sesja SSO z IdP pozostaje aktywna, więc użytkownik może zalogować się ponownie bez podawania hasła. *Auto-logout* może również przyjmować wartość ”0”, co oznacza, że funkcja automatycznego wylogowania zostanie wyłączona po aktualizacji ustawień profilu.
Refresh	Ustaw, jak często informacje na stronach menu *Monitoring* będą odświeżane (minimum 0 sekund, maksimum 1 godzina). Obsługiwane są sufiksy czasu, na przykład: 30s, 90s, 1m, 1h.
Rows per page	Ustaw, ile wierszy będzie wyświetlanych na stronę na listach. Mniejsza liczba wierszy (i mniej rekordów do wyświetlenia) skutkuje szybszym czasem ładowania.
URL (after login)	Ustaw konkretny adres URL, który ma być wyświetlany po zalogowaniu. Zamiast domyślnego widoku *Dashboards* może to być na przykład adres URL *Monitoring* > *Triggers*.

Powiadomienia

Sekcja *Powiadomienia* udostępnia opcje dostosowywania powiadomień bieżącego użytkownika.

Karta *Media* umożliwia określenie szczegółów mediów dla użytkownika, takich jak typy mediów i adresy, których należy używać do dostarczania powiadomień, oraz kiedy należy ich używać.



Jeśli typ mediów został wyłączony:

- po nazwie wyświetlana jest żółta ikona informacyjna;
- w kolumnie *Status* wyświetlane jest ”Wyłączone”.

Note:
Uprawnienia użytkownika do zmiany własnych szczegółów mediów mogą być przyznawane/odbierane na podstawie jego roli użytkownika (zobacz opcję *Create and edit own media*). Uprawnienia użytkownika Super admin do zmiany szczegółów mediów innych użytkowników również mogą być przyznawane/odbierane na podstawie jego roli użytkownika (zobacz opcję *Create and edit user media*)

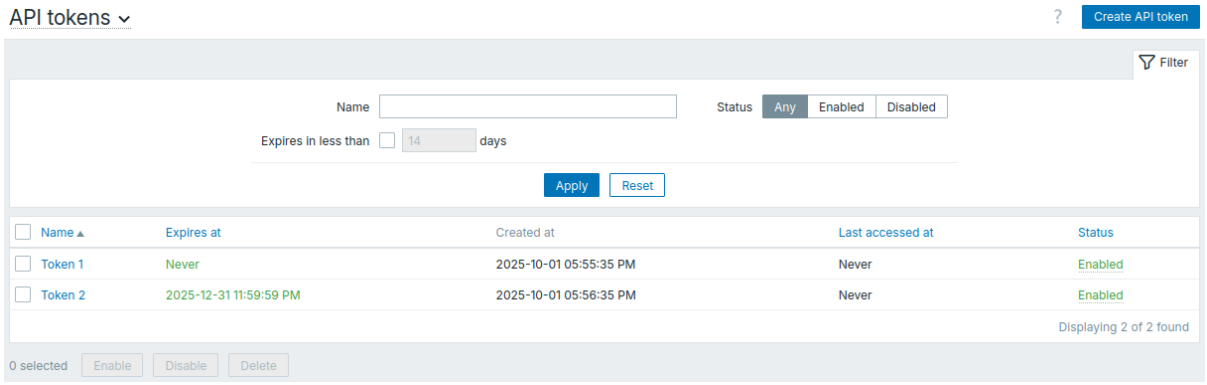
Należy pamiętać, że w przypadku użytkowników provisioned:

- media użytkownika provisioned nie mogą zostać usunięte;
- media użytkownika provisioned mogą zostać wyłączone/włączone;
- takie pola mediów użytkownika provisioned jak *When active*, *Use if severity* i *Enabled* mogą być edytowane ręcznie;
- dodatkowe media użytkownika mogą być dodawane ręcznie dla użytkowników provisioned (na przykład dodatkowe adresy e-mail);
- media użytkownika dodane ręcznie mogą zostać usunięte.

Karta *Powiadomienia frontend* umożliwia ustawienie powiadomień globalnych.

Tokeny API

Sekcja *Tokeny API* umożliwia przeglądanie tokenów przypisanych do użytkownika, edycję szczegółów tokenów oraz tworzenie nowych tokenów. Ta sekcja jest dostępna dla użytkownika tylko wtedy, gdy działanie *Manage API tokens* jest dozwolone w ustawieniach roli użytkownika.



Tokeny API można filtrować według nazwy, daty wygaśnięcia lub statusu (*Włączony/Wyłączony*). Kliknij status tokenu na liście, aby szybko włączyć/wyłączyć token. Możesz także włączyć/wyłączyć wiele tokenów jednocześnie, zaznaczając je na liście, a następnie klikając przyciski *Włącz/Wyłącz* pod listą.

Attention:
Użytkownicy nie mogą wyświetlić wartości *Auth token* tokenów przypisanych do nich w Zabbix. Wartość *Auth token* jest wyświetlana tylko raz — bezpośrednio po utworzeniu tokenu. Jeśli token został utracony, należy go wygenerować ponownie.

1 Globalne powiadomienia

Przegląd

Powiadomienia globalne umożliwiają wyświetlanie problemów w czasie rzeczywistym bezpośrednio na bieżącym ekranie w frontend Zabbix.

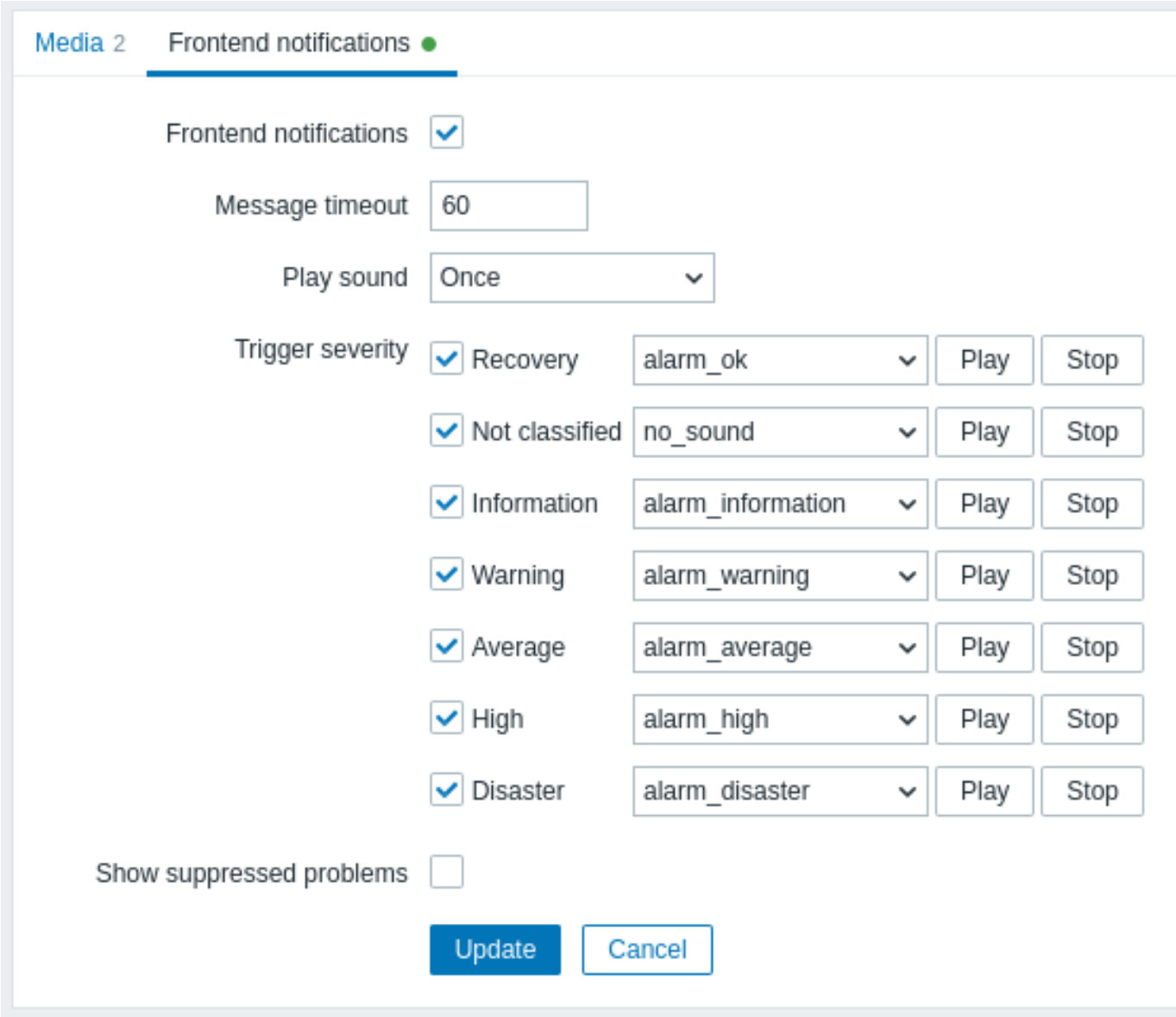
Bez powiadomień globalnych, podczas pracy poza sekcjami *Problemy* lub *Pulpit*, nie otrzymywałbyś żadnych informacji o bieżących problemach. Powiadomienia globalne zapewniają wyświetlanie tych informacji niezależnie od bieżącej lokalizacji w frontend Zabbix.

Powiadomienia globalne obejmują zarówno wyświetlanie komunikatu, jak i odtwarzanie dźwięku.

Attention:
Automatyczne odtwarzanie dźwięków może być wyłączone (domyślnie) w najnowszych wersjach przeglądarek. W takich przypadkach należy włączyć to ustawienie ręcznie.

Konfiguracja

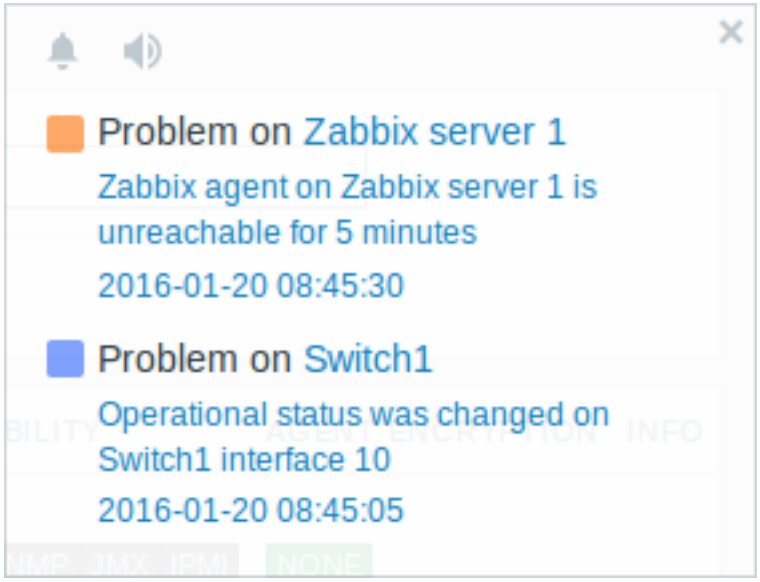
Globalne powiadomienia można włączyć dla każdego użytkownika na karcie **Powiadomienia frontend** w sekcji Powiadomienia.



Parametr	Opis
Powiadomienia frontend	Zaznacz pole wyboru, aby włączyć globalne powiadomienia.
Limit czasu wiadomości	Ustaw czas, przez jaki wiadomość będzie wyświetlana. Domyślnie wiadomości pozostają na ekranie przez 60 sekund. Obsługiwane są sufiksy czasu, na przykład: 30s, 5m, 2h, 1d.
Odtwarzaj dźwięk	Ustaw czas, przez jaki dźwięk będzie odtwarzany. **Raz** - dźwięk jest odtwarzany raz w całości; **10 sekund** - dźwięk jest powtarzany przez 10 sekund; **Limit czasu wiadomości** - dźwięk jest powtarzany, dopóki wiadomość jest widoczna.
Poziom ważności wyzwalacza	Ustaw poziomy ważności wyzwalaczy, dla których będą aktywowane globalne powiadomienia i dźwięki. Możesz także wybrać dźwięki odpowiednie dla różnych poziomów ważności. Jeśli nie zostanie zaznaczony żaden poziom ważności, żadne wiadomości nie będą wyświetlane. Dodatkowo wiadomości o odzyskaniu będą wyświetlane tylko dla zaznaczonych poziomów ważności. Na przykład, jeśli zaznaczone są *Odzyskanie* i *Katastrofa*, globalne powiadomienia będą wyświetlane dla problemów i odzyskań wyzwalaczy o poziomie ważności *Katastrofa*.
Pokaż stłumione problemy	Zaznacz pole wyboru, aby wyświetlać powiadomienia o problemach, które w przeciwnym razie byłyby stłumione (niepokazywane) z powodu konserwacji hosta.

Wyświetlane komunikaty globalne

Gdy komunikaty napływają, są wyświetlane w pływającej sekcji po prawej stronie. Możesz dowolnie zmieniać położenie tej sekcji, przeciągając jej nagłówek.



Dla tej sekcji dostępnych jest kilka elementów sterujących:

- Przycisk **Snooze** wycisza aktualnie aktywny dźwięk alarmu;
- Przycisk **Mute/Unmute** przełącza między odtwarzaniem a całkowitym nieodtwarzaniem dźwięków alarmu.

2 Dźwięk w przeglądarkach

Przegląd

Dźwięk jest używany w powiadomieniach globalnych.

Aby dźwięki były odtwarzane w frontend Zabbix, w profilu użytkownika na karcie *Frontend notifications* musi być włączona opcja *Frontend notifications*, a wszystkie poziomy ważności wyzwalaczy muszą być zaznaczone. Dodatkowo dźwięki powinny być włączone w wyskakującym oknie powiadomień globalnych.

Jeśli z jakiegokolwiek powodu dźwięk nie może być odtwarzany na urządzeniu, przycisk w wyskakującym oknie powiadomień globalnych pozostanie na stałe w stanie „wyciszenia", a po najechaniu kursorem na przycisk zostanie wyświetlony komunikat „Cannot support notification audio for this device".

Dźwięki, w tym domyślne klipy audio, są obsługiwane wyłącznie w formacie MP3.

Dźwięki frontend Zabbix zostały pomyślnie przetestowane w najnowszych przeglądarkach Firefox i Opera w systemie Linux oraz w przeglądarkach Chrome, Firefox, Microsoft Edge i Opera w systemie Windows.

Attention:
Automatyczne odtwarzanie dźwięków może być wyłączone (domyślnie) w najnowszych wersjach przeglądarek. W takich przypadkach należy włączyć to ustawienie ręcznie.

4 Wyszukiwanie globalne

Możliwe jest przeszukiwanie frontend Zabbix pod kątem hostów, grup hostów, szablonów i grup szablonów.

Pole wyszukiwania znajduje się pod logo Zabbix w menu. Wyszukiwanie można rozpocząć, naciskając *Enter* lub klikając ikonę wyszukiwania .



Jeśli istnieje host, który zawiera wprowadzony ciąg znaków w dowolnej części nazwy, pojawi się lista rozwijana zawierająca wszystkie takie hosty (z pasującą częścią wyróżnioną na pomarańczowo). Lista rozwijana wyświetli również host, jeśli widoczna nazwa tego hosta odpowiada nazwie technicznej wprowadzonej jako ciąg wyszukiwania; pasujący host zostanie wyświetlony, ale bez żadnego wyróżnienia.

Atrybuty podlegające wyszukiwaniu

Hosty można wyszukiwać według następujących właściwości:

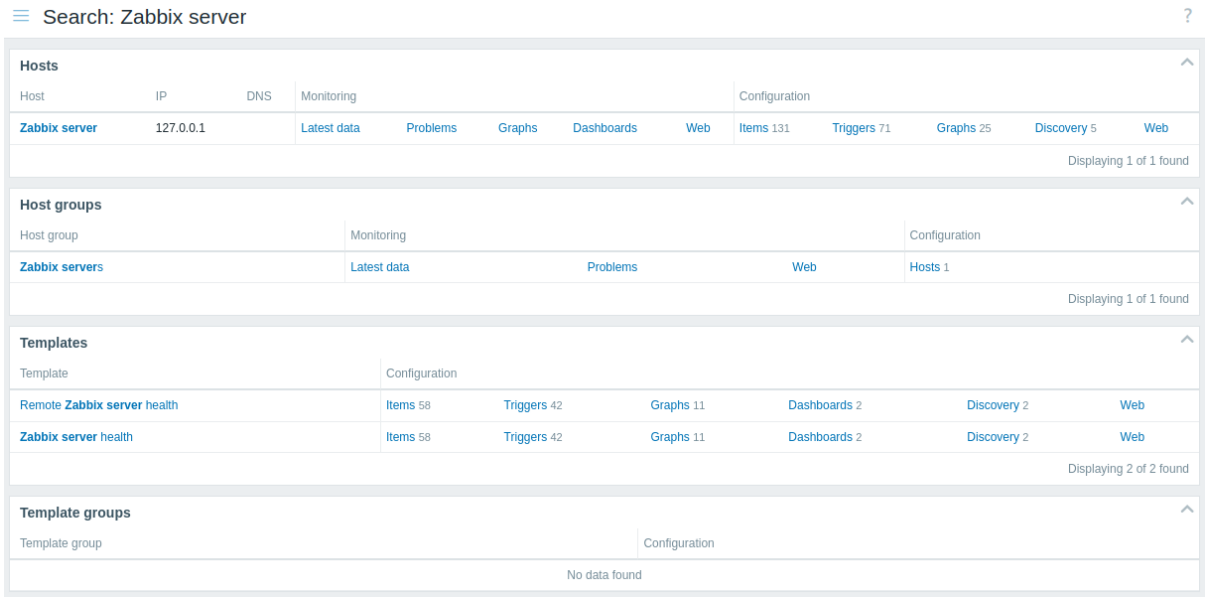
- Nazwa hosta
- Widoczna nazwa
- Adres IP
- Nazwa DNS

Szablony można wyszukiwać według nazwy lub widocznej nazwy. Jeśli wyszukujesz według nazwy, która różni się od widocznej nazwy (szablonu/hosta), w wynikach wyszukiwania jest ona wyświetlana poniżej widocznej nazwy w nawiasach.

Grupy hostów i szablonów można wyszukiwać według nazwy. Określenie grupy nadrzędnej niejawnie wybiera wszystkie grupy zagnieżdżone.

Wyniki wyszukiwania

Wyniki wyszukiwania składają się z czterech oddzielnych bloków dla hostów, grup hostów, szablonów i grup szablonów.



Można zwinąć/rozwinąć każdy pojedynczy blok. Liczba wpisów jest wyświetlana na dole każdego bloku, na przykład: *Wyświetlanie 13 z 13 znalezionych*. Jeśli nie ma żadnych wpisów, liczba wpisów nie jest wyświetlana. Łączna liczba wpisów wyświetlanych w jednym bloku jest ograniczona do 100.

Każdy wpis zawiera odnośniki do danych monitoringu i konfiguracji. Zobacz pełną listę odnośników.

Dla wszystkich danych konfiguracyjnych (takich jak pozycje, wyzwalacze, wykresy) liczba znalezionych encji jest wyświetlana jako liczba obok nazwy encji, w kolorze szarym. **Uwaga:** jeśli encji jest zero, żadna liczba nie jest wyświetlana.

Włączone hosty są wyświetlane na niebiesko, wyłączone hosty na czerwono.

Dostępne linki

Dla każdego wpisu dostępne są następujące linki:

- Hosty
  - Monitorowanie
    - Najnowsze dane
    - Problemy
    - Wykresy
    - Pulpity hosta
    - Scenariusze WWW
  - Konfiguracja
    - Pozycje
    - Wyzwalacze
    - Wykresy
    - Reguły wykrywania
    - Scenariusze WWW
- Grupy hostów
  - Monitorowanie
    - Najnowsze dane
    - Problemy
    - Scenariusze WWW
  - Konfiguracja
    - Hosty
- Szablony
  - Konfiguracja
    - Pozycje
    - Wyzwalacze
    - Wykresy
    - Pulpity szablonu
    - Reguły wykrywania
    - Scenariusze WWW
- Grupy szablonów
  - Konfiguracja
    - Szablony

5 Tryb konserwacji frontendu

Przegląd

Można tymczasowo wyłączyć frontend Zabbix, aby ograniczyć dostęp. Służy do ochrony bazy danych Zabbix przed zmianami wprowadzonymi przez użytkownika, zachowując jej integralność.

Gdy frontend Zabbix jest w trybie konserwacji, możesz bezpiecznie zatrzymać bazę danych i wykonać zadania konserwacyjne.

Użytkownicy ze zdefiniowanych adresów IP będą mogli normalnie wchodzić w interakcję z frontendem w trybie konserwacji.

Konfiguracja

Aby włączyć tryb konserwacji, otwórz plik `maintenance.inc.php` (znajdujący się w `/conf` katalogu dokumentów HTML Zabbix na serwerze WWW) i usuń komentarz z następujących wierszy:

// Tryb konserwacji. define('ZBX_DENY_GUI_ACCESS', 1);

// Tablica adresów IP, które mogą łączyć się z frontendem (opcjonalnie). $ZBX_GUI_ACCESS_IP_RANGE = array('127.0.0.1');

// Komunikat wyświetlany na ekranie ostrzegawczym (opcjonalnie). $ZBX_GUI_ACCESS_MESSAGE = 'Aktualizujemy bazę danych MySQL do godziny 15:00. Bądź na bieżąco...';

Note:
W większości przypadków plik `maintenance.inc.php` znajduje się w katalogu `/conf` katalogu dokumentów HTML Zabbix na serwerze WWW. Jednak niektóre systemy operacyjne i serwery WWW mogą używać innej lokalizacji.
Na przykład lokalizacja dla:

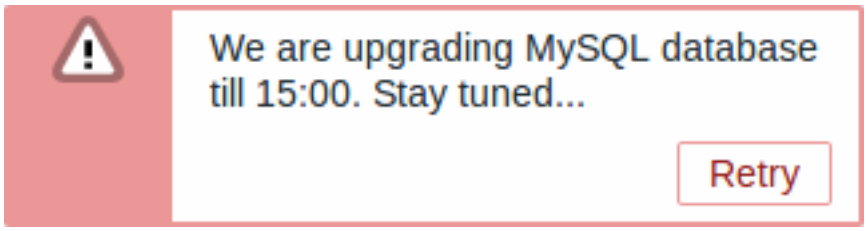
- SUSE i RedHat to `/etc/zabbix/web/maintenance.inc.php`.
- systemów opartych na Debianie to `/usr/share/zabbix/conf/`.

Zobacz także Kopiowanie plików PHP.

Parametr	Szczegóły
ZBX_DENY_GUI_ACCESS	Jeśli zdefiniowano z dowolną wartością, tryb konserwacji zostanie włączony. Aby wyłączyć tryb konserwacji, zakomentuj lub usuń.
ZBX_GUI_ACCESS_IP_RANGE	Tablica adresów IP, którym zezwolono na połączenie z frontendem (opcjonalnie). Na przykład: `array('192.168.1.1', '192.168.1.2')`
ZBX_GUI_ACCESS_MESSAGE	Komunikat informujący użytkowników o pracach konserwacyjnych (opcjonalnie). Jeśli nie jest zdefiniowany, zostanie użyty domyślny komunikat *'Zabbix is under maintenance'*.

Wyświetl

Użytkownicy zobaczą następujący ekran podczas próby dostępu do frontendu Zabbix w trybie konserwacji. Ekran jest odświeżany co 30 sekund, aby powrócić do normalnego stanu bez interwencji użytkownika po zakończeniu konserwacji.



Adresy IP zdefiniowane w *ZBX_GUI_ACCESS_IP_RANGE* będą mogły uzyskać dostęp do frontendu jak zwykle.

6 Parametry strony

Przegląd

Większość stron interfejsu webowego Zabbix obsługuje różne parametry HTTP GET, które określają, co zostanie wyświetlone. Można je przekazywać, podając po adresie URL pary parametr=wartość, oddzielone od adresu URL znakiem zapytania (?) i od siebie nawzajem znakiem ampersand (&).

Monitoring > Problemy

Obsługiwane są następujące parametry:

Parameter	Description	Example
show	Opcja filtra *Pokaż*. Możliwe wartości: 1 - ostatnie problemy; 2 - wszystkie; 3 - w stanie problemu.	show=1
name	Opcja filtra *Problem*: dowolny ciąg znaków.	name=Zabbix agent

Parameter	Description	Example
severities	Opcja filtra *Severity*: tablica wybranych poziomów ważności w formacie `severities[*]=*` (zastąp * poziomem ważności). Możliwe wartości: 0 - niesklasyfikowane; 1 - informacja; 2 - ostrzeżenie; 3 - średni; 4 - wysoki; 5 - katastrofa.	severities[3]=3
inventory	Opcja filtra *Host inventory*: tablica pól inwentarza `[field],[value]`	inventory[0][field]=type&invento
evaltype	Opcja filtra *Tags*: metoda oceny tagów. Możliwe wartości: 0 - and/or; 2 - or.	evaltype=0
tags	Opcja filtra *Tags*: tablica zdefiniowanych tagów `[tag], [operator], [value]` Możliwe wartości operator: 0 - zawiera; 1 - równa się; 2 - nie zawiera; 3 - nie równa się; 4 - istnieje; 5 - nie istnieje.	tags[0][tag]=target&tags[0][ope
show_tags	Opcja filtra *Show tags*. Możliwe wartości: 0 - brak; 1 - jeden; 2 - dwa; 3 - trzy.	show_tags=3
tag_name_format	Opcja filtra *Tag name*. Możliwe wartości: 0 - pełna nazwa; 1 - skrócona nazwa; 2 - brak.	tag_name_format=1
tag_priority	Opcja filtra *Tag display priority*: ciąg rozdzielony przecinkami określający priorytet wyświetlania tagów	tag_priority=customer, target
show_suppressed	Opcja filtra *Show suppressed problems*. Możliwe wartości: 1 - pokaż; 2 - nie pokazuj.	show_suppressed=1
acknowledgement_status	Opcja filtra *Acknowledgement status*. Możliwe wartości: 0 - wszystkie; 1 - niepotwierdzone; 2 - potwierdzone.	acknowledgement_status=0
acknowledged_by_me	Opcja filtra *By me*; obsługiwane tylko z `acknowledgement_status=2`. Możliwe wartości: 0 - wyłączone; 1 - włączone.	acknowledged_by_me=1
compact_view	Opcja filtra *Compact view*. Możliwe wartości: 0 - wyłączone; 1 - włączone.	compact_view=1

Parameter	Description	Example
highlight_row	Opcja filtra *Highlight whole row*. Możliwe wartości: 0 - wyłączone; 1 - włączone.	highlight_row=1
filter_name	Opcja właściwości filtra *Name*: dowolny ciąg znaków	filter_name=Databases
filter_show_counter	Opcja właściwości filtra *Show number of records*. Możliwe wartości: 0 - wyłączone; 1 - włączone.	filter_show_counter=1
filter_custom_time	Opcja właściwości filtra *Set custom time period*. Możliwe wartości: 0 - wyłączone; 1 - włączone.	filter_custom_time=1
sort	Kolumna, według której ma być wykonane sortowanie. Możliwe wartości: clock - sortowanie według kolumny *Time*; host - sortowanie według kolumny *Host*; severity - sortowanie według kolumny *Severity*; name - sortowanie według kolumny *Problem*.	sort=clock
sortorder	Kolejność sortowania wyników. Możliwe wartości: DESC - malejąco; ASC - rosnąco.	sortorder=DESC
age_state	Opcja filtra *Age less than*; obsługiwane tylko z `show`=3. Możliwe wartości: 0 - wyłącz parametr `age`; 1 - włącz parametr `age`.	age_state=1
age	Opcja filtra *Age less than*: liczba całkowita, liczba dni; obsługiwane tylko z `age_state`=1 i `show`=3.	age=7
groupids	Opcja filtra *Host groups*: tablica identyfikatorów grup hostów.	groupids[]=4
hostids	Opcja filtra *Hosts*: tablica identyfikatorów hostów	hostids[]=10084
triggerids	Opcja filtra *Triggers*: tablica identyfikatorów wyzwalaczy	triggerids[]=22382
show_timeline	Opcja filtra *Show timeline*; nieobsługiwane z `compact_view`=1. Możliwe wartości: 0 - nie pokazuj; 1 - pokaż.	show_timeline=1
details	Opcja filtra *Show details*. Możliwe wartości: 0 - nie pokazuj; 1 - pokaż.	details=1
from	Początek zakresu dat, może być względny (np. now-1m); obsługiwane tylko z `filter_custom_time`=1	from=now-2h
to	Koniec zakresu dat, może być względny (np. now-1m); obsługiwane tylko z `filter_custom_time`=1	to=now

Zobacz także: opcje filtrowania strony Problemy.

Tryb kiosku

Tryb kiosku na obsługiwanych stronach frontend można włączyć za pomocą parametrów URL. Na przykład na pulpitach:

- `/zabbix.php?action=dashboard.view&kiosk=1` - włącz tryb kiosku
- `/zabbix.php?action=dashboard.view&kiosk=0` - włącz tryb normalny

Pokaz slajdów

Możliwe jest włączenie pokazu slajdów na pulpicie:

- `/zabbix.php?action=dashboard.view&slideshow=1` - włącz pokaz slajdów

7 Definicje

Przegląd

Chociaż wiele rzeczy we frontend można skonfigurować przy użyciu samego frontend, niektóre dostosowania są obecnie możliwe tylko przez edycję pliku definicji.

Ten plik to `defines.inc.php`, znajdujący się w katalogu /include katalogu dokumentów HTML Zabbix.

Parametry

Parametry w tym pliku, które mogą być interesujące dla użytkowników:

- ZBX_MIN_PERIOD

Minimalny okres wykresu, w sekundach. Domyślnie jedna minuta.

- GRAPH_YAXIS_SIDE_DEFAULT

Domyślne położenie osi Y na prostych wykresach oraz domyślna wartość na liście rozwijanej podczas dodawania pozycji do wykresów niestandardowych. Możliwe wartości: 0 - lewa, 1 - prawa.

Domyślnie: 0

- ZBX_SESSION_NAME

Ciąg znaków używany jako nazwa ciasteczka sesji frontend Zabbix.

Domyślnie: zbx_sessionid

- ZBX_DATA_CACHE_TTL

Limit czasu TTL w sekundach używany do unieważniania pamięci podręcznej danych odpowiedzi Vault. Ustaw 0, aby wyłączyć buforowanie odpowiedzi Vault.

Domyślnie: 60

- SUBFILTER_VALUES_PER_GROUP

Liczba wartości podfiltra na grupę (na przykład w podfiltrze najnowsze dane).

Domyślnie: 1000

- ZBX_MAX_WIDGET_LINES

Maksymalna liczba wierszy widżetu do wyświetlenia.

Domyślnie: 1000

8 Tworzenie własnego motywu

Przegląd

Domyślnie Zabbix udostępnia kilka predefiniowanych motywów. Możesz postępować zgodnie z przedstawioną tutaj procedurą krok po kroku, aby utworzyć własny motyw. Zachęcamy do podzielenia się efektem swojej pracy ze społecznością Zabbix, jeśli uda Ci się stworzyć coś ciekawego.

Krok 1

Aby zdefiniować własny motyw, należy utworzyć plik CSS i zapisać go w folderze `assets/styles/` (na przykład *custom-theme.css*). Można skopiować pliki z innego motywu i utworzyć swój motyw na ich podstawie albo zacząć od zera.

Krok 2

Dodaj swój motyw do listy motywów zwracanych przez metodę APP::getThemes(). Możesz to zrobić, nadpisując metodę ZBase::getThemes() w klasie APP. Można to zrobić, dodając następujący kod przed zamykającym nawiasem klamrowym w pliku *include/classes/core/APP.php*:

```
public static function getThemes() {
    return array_merge(parent::getThemes(), [
        'custom-theme' => _('Custom theme')
    ]);
}
```

Attention:
Zwróć uwagę, że nazwa podana w pierwszej parze cudzysłowów musi odpowiadać nazwie pliku motywu bez rozszerzenia.

Aby dodać wiele motywów, po prostu wypisz je pod pierwszym motywem, na przykład:

```
public static function getThemes() {
    return array_merge(parent::getThemes(), [
        'custom-theme' => _('Custom theme'),
        'anothertheme' => _('Another theme'),
        'onemoretheme' => _('One more theme')
    ]);
}
```

Zwróć uwagę, że każdy motyw oprócz ostatniego musi mieć na końcu przecinek.

Note:
Aby zmienić kolory wykresu, wpis musi zostać dodany do tabeli bazy danych *graph_theme*.

Krok 3

Aktywuj nowy motyw.

W frontend Zabbix możesz ustawić ten motyw jako domyślny lub zmienić swój motyw w profilu użytkownika.

Ciesz się nowym wyglądem i stylem!

9 Tryb debugowania

Przegląd

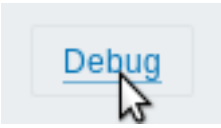
Tryb debugowania może być używany do diagnozowania problemów z wydajnością stron frontend.

Konfiguracja

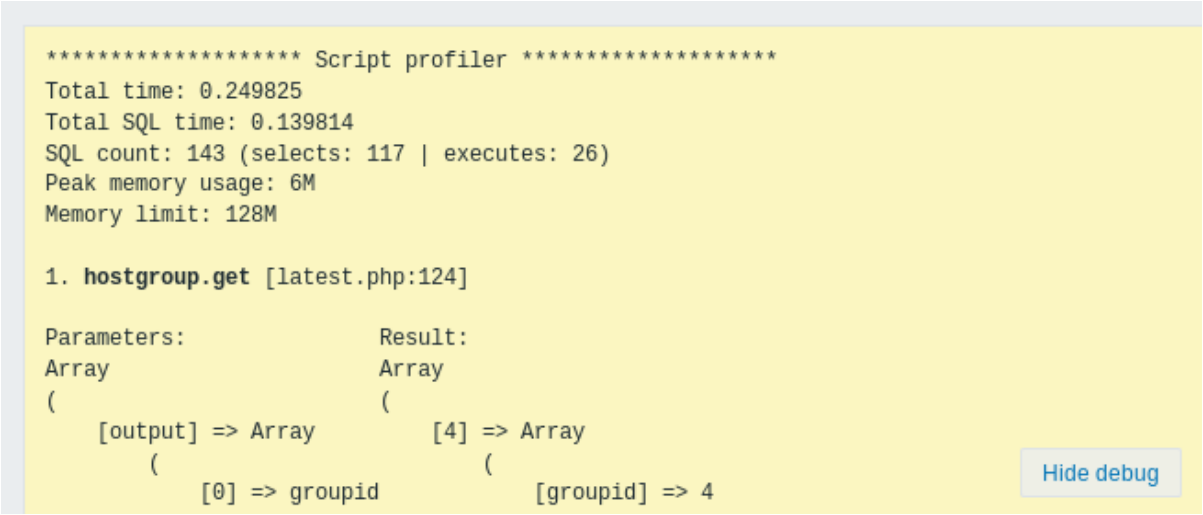
Tryb debugowania można włączyć dla poszczególnych użytkowników należących do grupy użytkowników:

- podczas konfigurowania grupy użytkowników;
- podczas przeglądania skonfigurowanych grup użytkowników.

Gdy opcja *Tryb debugowania* jest włączona dla grupy użytkowników, jej użytkownicy zobaczą przycisk *Debug* w prawym dolnym rogu okna przeglądarki:



Kliknięcie przycisku *Debug* otwiera nowe okno poniżej zawartości strony, które zawiera statystyki SQL dla strony, a także listę wywołań API i poszczególnych instrukcji SQL:



W przypadku problemów z wydajnością strony to okno może zostać użyte do wyszukania głównej przyczyny problemu.

Warning:
Włączony *Tryb debugowania* ma negatywny wpływ na wydajność frontend.

10 Ciasteczka używane przez Zabbix

Przegląd

Ta strona zawiera listę plików cookie używanych przez Zabbix.

Nazwa	Opis	Wartości	Wygasa/Max-Age	HttpOnly[1]	Secure[2]
ZBX_SESSION_NAME	Dane sesji frontend Zabbix, przechowywane jako JSON zakodowany przy użyciu base64		Sesja (wygasa po zakończeniu sesji przeglądania)	+	+ (tylko jeśli HTTPS jest włączony na serwerze WWW)
tab	Numer aktywnej karty; ten plik cookie jest używany tylko na stronach z wieloma kartami (np. na stronie konfiguracji *Host*, *Trigger* lub *Action*) i jest tworzony, gdy użytkownik przechodzi z karty głównej do innej karty (takiej jak karta *Tags* lub *Dependencies*). 0 jest używane dla karty głównej.	Przykład: 1	Sesja (wygasa po zakończeniu sesji przeglądania)	-	-
browserwarning_ignore	Określa, czy ostrzeżenie o używaniu nieaktualnej przeglądarki powinno zostać zignorowane.	yes	Sesja (wygasa po zakończeniu sesji przeglądania)	-	-
system-message-ok	Komunikat do wyświetlenia natychmiast po ponownym załadowaniu strony.	Komunikat w postaci zwykłego tekstu	Sesja (wygasa po zakończeniu sesji przeglądania) lub natychmiast po ponownym załadowaniu strony	+	-

Nazwa	Opis	Wartości	Wygasa/Max-Age	HttpOnly[1]	Secure[2]
system-message-error	Komunikat o błędzie do wyświetlenia natychmiast po ponownym załadowaniu strony.	Komunikat w postaci zwykłego tekstu	Sesja (wygasa po zakończeniu sesji przeglądania) lub natychmiast po ponownym załadowaniu strony	+	-

Note:
Wymuszanie flagi 'HttpOnly' dla plików cookie Zabbix za pomocą dyrektywy serwera WWW nie jest obsługiwane.

Przypisy

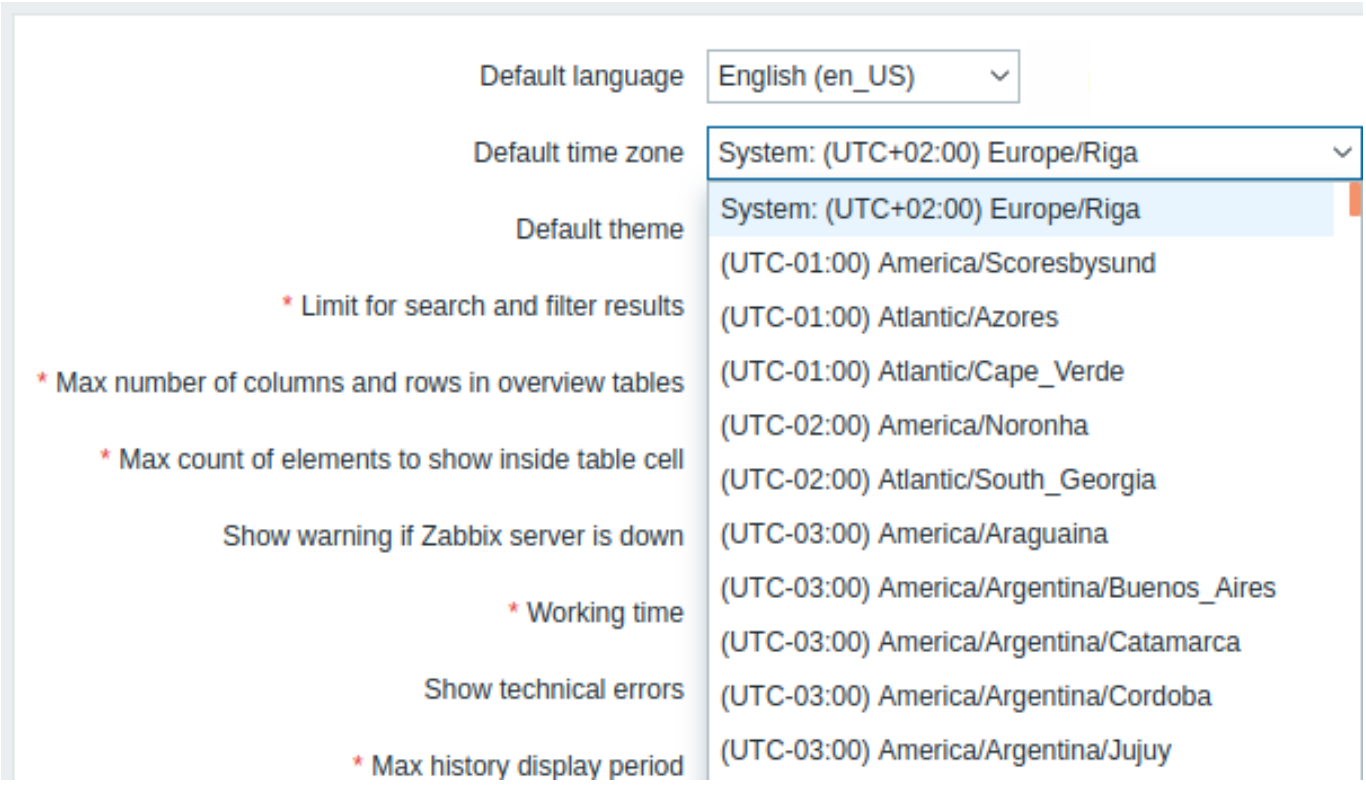
[1] Gdy `HttpOnly` ma wartość 'true', plik cookie będzie dostępny tylko przez protokół HTTP. Oznacza to, że plik cookie nie będzie dostępny dla języków skryptowych, takich jak JavaScript. To ustawienie może skutecznie pomóc ograniczyć kradzież tożsamości poprzez ataki XSS (chociaż nie jest obsługiwane przez wszystkie przeglądarki).

[2] `Secure` wskazuje, że plik cookie powinien być przesyłany wyłącznie przez bezpieczne połączenie HTTPS od klienta. Gdy ma wartość 'true', plik cookie zostanie ustawiony tylko wtedy, gdy istnieje bezpieczne połączenie.

11 Strefy czasowe

Przegląd

Strefę czasową frontend można ustawić globalnie we frontend i dostosować dla poszczególnych użytkowników.



Jeśli wybrano *System*, dla frontend zostanie użyta strefa czasowa serwera WWW (w tym wartość „date.timezone" z php.ini, jeśli jest ustawiona), natomiast serwer Zabbix będzie używać strefy czasowej maszyny, na której działa.

Note:
Serwer Zabbix będzie używać określonej globalnej/strefy czasowej użytkownika tylko podczas rozwijania makr w powiadomieniach (np. {EVENT.TIME} może zostać rozwinięte do innej strefy czasowej dla każdego użytkownika) oraz do limitu czasu przy wysyłaniu powiadomień (zobacz ustawienie „When active" w konfiguracji mediów użytkownika).

Wybór strefy czasowej nie wpływa na format czasu/daty we frontend. Zamiast tego można dostosować język interfejsu (podczas instalacji lub w ustawieniach użytkownika) — wybranie *English (en_US)* spowoduje również włączenie amerykańskiego formatu czasu/daty we frontend.

Konfiguracja

Globalna strefa czasowa:

- może zostać ustawiona ręcznie podczas instalacji frontendu
- może zostać zmodyfikowana w *Administracja* → *Ogólne* → *GUI*

Strefa czasowa na poziomie użytkownika:

- może zostać ustawiona podczas konfigurowania/aktualizacji użytkownika
- może zostać ustawiona przez każdego użytkownika w jego profilu użytkownika

Zobacz także: Wyrównywanie stref czasowych podczas używania interwałów harmonogramu.

12 Resetowanie hasła

Przegląd Ta sekcja opisuje kroki resetowania haseł użytkowników w Zabbix.

Kroki Zwróć się do twojego administratora Zabbix jeżeli zapomniałeś hasła i nie możesz się zalogować.

Użytkownik Super administrator może zmienić hasła wszystkim użytkownikom w Konfiguracja użytkownika.

Jeśli super administrator zapomniał swojego hasła i nie może się zalogować, należy wykonać następujące zapytanie SQL, aby zastosować domyślne hasło dla użytkownika super administratora (zastąp „Admin” na odpowiednią nazwę użytkownika super administratora):

UPDATE users SET passwd = ’$2a$10$ZXIvHAEP2ZM.dLXTm6uPHOMVlARXX7cqjbhM6Fn0cANzkCQBWpMrS’ WHERE username = ’Admin’;

Po uruchomieniu tego zapytania hasło użytkownika zostanie ustawione na *zabbix*. Pamiętaj o zmianie domyślnego hasła przy pierwszym logowaniu.

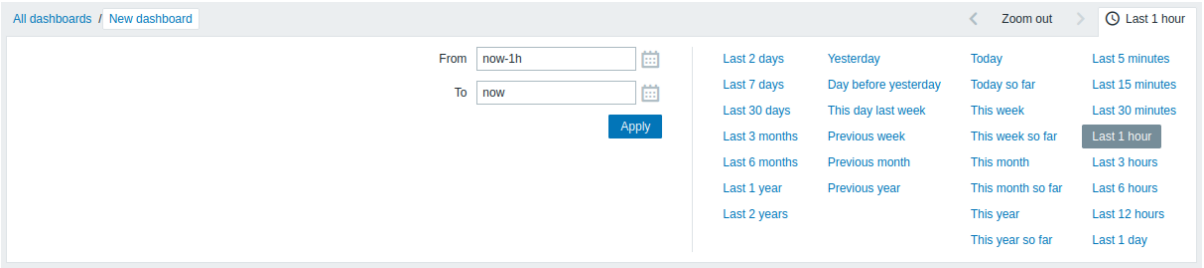
13 Okres czasu i selektory hostów

Przegląd

Ta strona opisuje selektory okresu czasu i hosta dostępne na pulpitach. Te selektory umożliwiają dynamiczne dostosowanie wyświetlanych danych we wszystkich zgodnych widgetach pulpitu bez edytowania ustawień poszczególnych widgetów.

Selektor okresu czasu

Selektor okresu czasu umożliwia wybór często używanych okresów jednym kliknięciem myszy. Można go rozwinąć lub zwinąć, klikając przycisk selektora okresu czasu w prawym górnym rogu pulpitu.



Opcje takie jak *Dzisiaj*, *Ten tydzień* itd. wyświetlają cały okres, łącznie z godzinami/dniami w przyszłości. Opcje takie jak *Dzisiaj do tej pory*, *Ten tydzień do tej pory* itd. wyświetlają tylko godziny, które już upłynęły.

Po wybraniu okresu można go przesuwać wstecz i do przodu w czasie, klikając przyciski strzałek . Przycisk *Pomniejsz* umożliwia oddalenie okresu o 50% w każdym kierunku.

Note:
W przypadku wykresów (z wyjątkiem tych z *Niestandardowym* okresem czasu) wybranie wyświetlanego okresu czasu jest również możliwe przez zaznaczenie obszaru na wykresie lewym przyciskiem myszy. Po zwolnieniu lewego przycisku myszy wykres zostanie powiększony do zaznaczonego obszaru. Pomniejszanie jest również możliwe przez dwukrotne kliknięcie wykresu.

Pola *Od/Do* wyświetlają wybrany okres w składni czasu bezwzględnego (w formacie `Y-m-d H:i:s`) albo w składni czasu względnego. Względny okres czasu może zawierać jedną lub kilka operacji matematycznych (- lub +), na przykład `now-1d` lub `now-1d-2h+5m`.

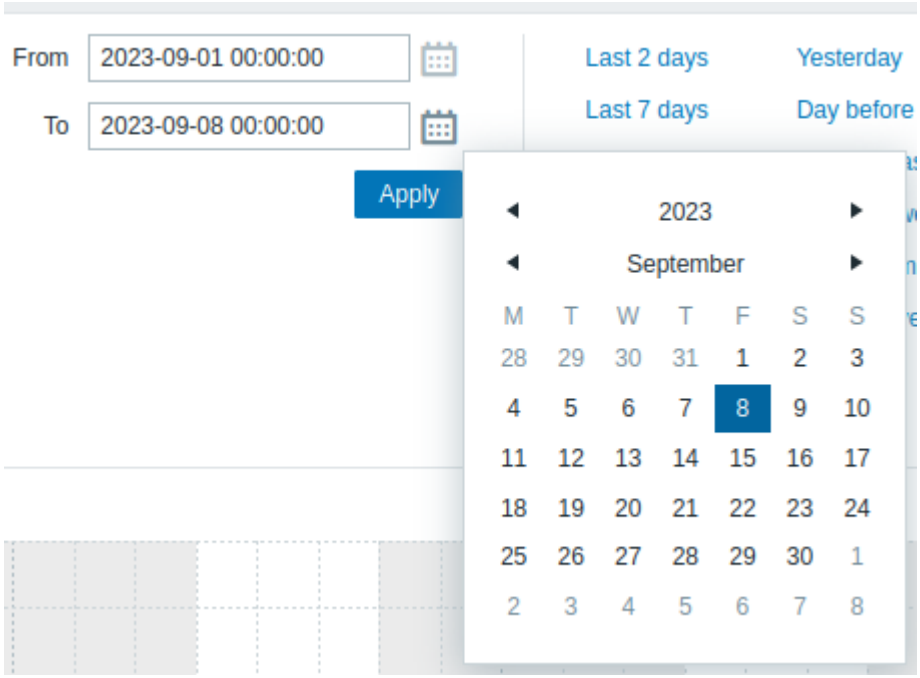
Obsługiwane są następujące skróty czasu względnego:

- `now`
- `s` (sekundy)
- `m` (minuty)
- `h` (godziny)
- `d` (dni)
- `w` (tygodnie)
- `M` (miesiące)
- `y` (lata)

W selektorze okresu czasu obsługiwana jest precyzja (na przykład `/M` w `now-1d/M`). Szczegóły precyzji:

Precyzja	Od	Do
`m`	Y-m-d H:m:00	Y-m-d H:m:59
`h`	Y-m-d H:00:00	Y-m-d H:59:59
`d`	Y-m-d 00:00:00	Y-m-d 23:59:59
`w`	Poniedziałek danego tygodnia 00:00:00	Niedziela danego tygodnia 23:59:59
`M`	Pierwszy dzień miesiąca 00:00:00	Ostatni dzień miesiąca 23:59:59
`y`	1 stycznia danego roku 00:00:00	31 grudnia danego roku 23:59:59

Możliwe jest również wybranie okresu czasu za pomocą selektora daty. Aby go otworzyć, kliknij ikonę kalendarza obok pól *Od/Do*.



Note:
W selektorze daty można przechodzić między rokiem/miesiącem/datą za pomocą `Tab`, `Shift+Tab` oraz klawiszy strzałek. Naciśnięcie `Enter` potwierdza wybór.

Przykłady:

Od	Do	Wybrany okres
`now/d`	`now/d`	00:00 - 23:59 dzisiaj
`now/d`	`now/d+1d`	00:00 dzisiaj - 23:59 jutro
`now/w`	`now/w`	Poniedziałek 00:00:00 - Niedziela 23:59:59 w tym tygodniu
`now-1y/w`	`now-1y/w`	Tydzień od poniedziałku 00:00:00 do niedzieli 23:59:59 rok temu

Attention:
Użycie ”now/M+1M” dla parametru *Do* może dodać 31 dni, co może skutkować przesunięciem daty o 1-3 dni w zależności od liczby dni w miesiącu. Na przykład, jeśli zostanie użyte w styczniu, wynikiem może być 02 marca zamiast oczekiwanego 28 lutego. Aby uniknąć tego problemu, użyj ”now/M-3d+1M/M”, które prawidłowo uwzględnia długość miesiąca. Podobnie, jeśli konfigurujesz parametr *Od* wstecz, użyj ”now/M+3d-1M/M”.

Selektor hosta

Selektor hosta umożliwia wybranie hosta, którego dane będą wyświetlane w zgodnych widżetach pulpitu.

Staje się dostępny po edytowaniu i zapisaniu pulpitu, jeśli co najmniej jeden widżet jest skonfigurowany z parametrem *Override host* ustawionym na użycie pulpitu jako źródła danych.



17 Najlepsze praktyki

Przegląd Ta sekcja przedstawia najlepsze praktyki dotyczące konfiguracji Zabbix.

Chociaż praktyki te nie są obowiązkowe do działania Zabbix, ich wdrożenie jest zdecydowanie zalecane w celu zapewnienia optymalnego i bezpiecznego korzystania z systemu.

1 Najlepsze praktyki bezpieczeństwa

Przegląd

Ta sekcja zawiera najlepsze praktyki dotyczące konfigurowania Zabbix w bezpieczny sposób.

Praktyki opisane w tej sekcji nie są wymagane do działania Zabbix, ale są zalecane w celu zapewnienia lepszego bezpieczeństwa systemu.

Kodowanie UTF-8

UTF-8 jest jedynym kodowaniem obsługiwanym przez Zabbix. Wiadomo, że działa bez żadnych luk bezpieczeństwa. Użytkownicy powinni mieć świadomość, że w przypadku korzystania z niektórych innych kodowań istnieją znane problemy związane z bezpieczeństwem.

Ścieżki instalatora Windows

Podczas korzystania z instalatorów Windows zaleca się używanie domyślnych ścieżek dostarczanych przez instalator. Używanie niestandardowych ścieżek bez odpowiednich uprawnień może zagrozić bezpieczeństwu instalacji.

Makra w skryptach globalnych zdefiniowanych przez użytkownika

Aby zwiększyć bezpieczeństwo, zaleca się używanie funkcji makr zamiast zwykłych makr w zdefiniowanych przez użytkownika globalnych skryptach, ponieważ makra nie są automatycznie poprzedzane znakami ucieczki.

Biuletyny bezpieczeństwa Zabbix i baza danych CVE

Zobacz *Biuletyny bezpieczeństwa Zabbix i baza danych CVE*.

Szablony wiadomości e-mail HTML

Podczas tworzenia lub edytowania szablonów wiadomości używanych w wiadomościach e-mail HTML zawsze opakowuj każdy makro funkcją makra `htmlencode()`. Na przykład:

```
<b>Problem started</b> at {{EVENT.TIME}.htmlencode()} on {{EVENT.DATE}.htmlencode()}<br><b>Problem name:</
{{EVENT.NAME}.htmlencode()}<br><b>Host:</b> {{HOST.NAME}.htmlencode()}
<br><b>Severity:</b>
{{EVENT.SEVERITY}.htmlencode()}<br><b>Operational
data:</b> {{EVENT.OPDATA}.htmlencode()}<br><b>Original problem ID:</b> {{EVENT.ID}.htmlencode()}<br>{{TRIG
```

Użycie `htmlencode()` zapewnia, że wszelkie znaki HTML w wartościach makr są poprzednio kodowane, i zapobiega wstrzyknięciu kodu HTML do powiadomień (na przykład gdy atakujący wstawi do powiadomienia złośliwy/phishingowy link).

Uwaga: domyślne wiadomości e-mail HTML dostarczane przez Zabbix mają już zastosowane `htmlencode()` do makr. To zalecenie ma zastosowanie podczas edytowania istniejących szablonów lub tworzenia nowych — przed użyciem szablonu do wysyłania wiadomości e-mail HTML należy sprawdzić, czy makra są zakodowane.

1 Kontrola dostępu

Przegląd

Ta sekcja zawiera najlepsze praktyki dotyczące bezpiecznej konfiguracji kontroli dostępu.

Zasada najmniejszych uprawnień

Konta użytkowników powinny przez cały czas działać z możliwie najmniejszym zakresem uprawnień. Oznacza to, że konta użytkowników w frontend Zabbix, użytkownicy bazy danych lub użytkownik procesów serwer/proxy/agent Zabbix powinni mieć wyłącznie uprawnienia niezbędne do wykonywania zamierzonych funkcji.

Attention:
Przyznanie dodatkowych uprawnień użytkownikowi „zabbix" umożliwi mu dostęp do plików konfiguracyjnych oraz wykonywanie operacji, które mogą zagrozić bezpieczeństwu infrastruktury.

Podczas konfigurowania uprawnień kont użytkowników należy uwzględnić typy użytkowników frontend w Zabbix. Należy pamiętać, że chociaż typ użytkownika *Admin* ma mniej uprawnień niż typ użytkownika *Super Admin*, nadal może zarządzać konfiguracją i wykonywać skrypty niestandardowe.

Note:
Niektóre informacje są dostępne nawet dla użytkowników bez uprawnień uprzywilejowanych. Na przykład, podczas gdy *Alerts* → *Scripts* jest dostępne tylko dla użytkowników *Super Admin*, skrypty można również pobrać za pośrednictwem Zabbix API. W takim przypadku ograniczenie uprawnień do skryptów oraz wykluczenie informacji wrażliwych ze skryptów (na przykład danych dostępowych) może pomóc uniknąć ujawnienia informacji wrażliwych dostępnych w skryptach globalnych.

Bezpieczny użytkownik dla Zabbix agent

Domyślnie procesy Zabbix serwer, proxy i agent (lub agent 2) współdzielą jednego użytkownika `zabbix`. Aby zapobiec dostępowi Zabbix agent/agent 2 (uruchomionego na tej samej maszynie co serwer/proxy) do poufnych informacji w konfiguracji serwera/proxy (na przykład poświadczeń bazy danych), agent powinien być uruchamiany pod innym użytkownikiem:

Dla Zabbix agent:

1. Utwórz bezpieczną grupę i użytkownika (np. `zabbix-agent`).
2. Ustaw tego użytkownika w parametrze User pliku konfiguracyjnego agent.
3. Uruchom ponownie agent, aby porzucić uprawnienia na rzecz nowego użytkownika.

W przypadku Zabbix agent 2 konfigurację należy zastosować na poziomie usługi, ponieważ plik konfiguracyjny agent 2 nie obsługuje parametru `User`. Przykład znajduje się w ZBX-26442.

Cofnięcie dostępu do zapisu do konfiguracji SSL (Windows)

Jeśli skompilowano agent Zabbix w systemie Windows z biblioteką OpenSSL znajdującą się w niezabezpieczonym katalogu (np. `C:\zabbix`, `c:\openssl-64bit`, `C:\OpenSSL-Win64-111-static` lub `C:\dev\openssl`), należy upewnić się, że użytkownikom niebędącym administratorami odebrano uprawnienia do zapisu do tego katalogu. W przeciwnym razie agent będzie wczytywać ustawienia SSL ze ścieżki, która może zostać zmodyfikowana przez nieuprzywilejowanych użytkowników, co stwarza potencjalną lukę bezpieczeństwa.

Wzmacnianie bezpieczeństwa komponentów Zabbix

Niektóre funkcje można wyłączyć, aby zwiększyć bezpieczeństwo komponentów Zabbix:

- wykonywanie skryptów globalnych na serwerze Zabbix można wyłączyć, ustawiając EnableGlobalScripts=0 w konfiguracji serwera;
- wykonywanie skryptów globalnych na proxy Zabbix jest domyślnie wyłączone (można je włączyć, ustawiając EnableRemoteCommands=1 w konfiguracji proxy);
- wykonywanie skryptów globalnych na agentach Zabbix jest domyślnie wyłączone (można je włączyć, dodając parametr AllowKey=system.run[<command>,*] dla każdego dozwolonego polecenia w konfiguracji agenta);
- uwierzytelnianie użytkowników HTTP można wyłączyć, ustawiając `$ALLOW_HTTP_AUTH=false` w pliku konfiguracyjnym frontendu (zabbix.conf.php). Należy pamiętać, że ponowna instalacja frontendu (uruchomienie setup.php) spowoduje usunięcie tego parametru.

Dostęp do ścieżek UNC w systemie Windows przez agent Zabbix

Agenty Zabbix w systemie Windows obsługują ścieżki UNC (udziały SMB, takie jak `\\server\share\file.txt`) w pozycjach takich jak `vfs.file.*`, `vfs.dir.*`, `modbus.get` oraz `perf_counter*`. W niektórych kontekstach może to stanowić zagrożenie bezpieczeństwa.

Gdy system Windows otrzymuje żądanie dostępu do ścieżki UNC, próbuje uwierzytelnić się na tym serwerze. Oznacza to, że złośliwe żądanie do agent Zabbix może ujawnić skrót NTLM serwerowi żądającego. Użytkownicy mogą ograniczyć to ryzyko za pomocą parametrów konfiguracyjnych AllowKey i DenyKey, jeśli zajdzie taka potrzeba.

1 Zabezpieczanie MySQL/MariaDB

Przegląd

Ta sekcja zawiera najlepsze praktyki dotyczące zabezpieczania bazy danych MySQL/MariaDB.

> **Note:**
> W przypadku podstawowej konfiguracji zobacz domyślne instrukcje tworzenia bazy danych MySQL/MariaDB, które obejmują utworzenie użytkownika „zabbix" z pełnymi uprawnieniami do bazy danych Zabbix. Ten użytkownik jest właścicielem bazy danych i ma również niezbędne uprawnienia do modyfikowania struktury bazy danych podczas aktualizacji Zabbix.

Aby zwiększyć bezpieczeństwo, zaleca się tworzenie dodatkowych ról i użytkowników bazy danych z minimalnymi uprawnieniami. Role i użytkownicy powinni być skonfigurowani zgodnie z zasadą najmniejszych uprawnień, to znaczy powinni mieć tylko te uprawnienia, które są niezbędne do wykonywania zamierzonych funkcji.

Tworzenie ról użytkowników

Utwórz następujące role z odpowiadającymi im uprawnieniami:

- **zbx_srv** - rola do uruchamiania serwera Zabbix i proxy:

```
CREATE ROLE 'zbx_srv';
GRANT DELETE, INSERT, SELECT, UPDATE ON zabbix.* TO 'zbx_srv';
FLUSH PRIVILEGES;
```

- **zbx_web** - rola do uruchamiania frontend Zabbix i API:

```
CREATE ROLE 'zbx_web';
GRANT DELETE, INSERT, SELECT, UPDATE ON zabbix.* TO 'zbx_web';
FLUSH PRIVILEGES;
```

- **zbx_bckp** - rola do tworzenia kopii zapasowych tabel:

```
CREATE ROLE 'zbx_bckp';
GRANT LOCK TABLES, TRIGGER, SELECT ON zabbix.* TO 'zbx_bckp';
GRANT process ON *.* TO 'zbx_bckp';
FLUSH PRIVILEGES;
```

> **Note:**
> Odtwarzanie tabel i aktualizacja powinny być wykonywane przez właściciela bazy danych.

- **zbx_part** - rola z ograniczonym zestawem uprawnień do partycjonowania bazy danych; pamiętaj, że tę rolę można utworzyć dopiero po utworzeniu bazy danych, ponieważ nadaje ona uprawnienia do określonych tabel bazy danych:

```
CREATE ROLE 'zbx_part';
GRANT SELECT, ALTER, DROP ON zabbix.history TO 'zbx_part';
GRANT SELECT, ALTER, DROP ON zabbix.history_uint TO 'zbx_part';
GRANT SELECT, ALTER, DROP ON zabbix.history_str TO 'zbx_part';
GRANT SELECT, ALTER, DROP ON zabbix.history_text TO 'zbx_part';
GRANT SELECT, ALTER, DROP ON zabbix.history_log TO 'zbx_part';
GRANT SELECT, ALTER, DROP ON zabbix.trends TO 'zbx_part';
GRANT SELECT, ALTER, DROP ON zabbix.trends_uint TO 'zbx_part';
-- Dla MariaDB: pomiń następną linię (GRANT session_variables_admin ON *.* TO 'zbx_part';)
GRANT session_variables_admin ON *.* TO 'zbx_part';
GRANT SELECT ON zabbix.dbversion TO 'zbx_part';
GRANT SELECT, DELETE ON zabbix.housekeeper TO 'zbx_part';
FLUSH PRIVILEGES;
```

Po utworzeniu ról można je przypisać użytkownikom.

Przypisywanie ról użytkownikom

Aby przypisać utworzone role użytkownikom, utwórz użytkowników i przypisz im odpowiednie role. W razie potrzeby zastąp <user>, <host>, <role> oraz <password>.

```
CREATE USER '<user>'@'<host>' IDENTIFIED BY '<password>';
GRANT '<role>' TO '<user>'@'<host>';
SET DEFAULT ROLE '<role>' TO '<user>'@'<host>';
-- For MariaDB: SET DEFAULT ROLE '<role>' FOR '<user>'@'<host>'
FLUSH PRIVILEGES;
```

Na przykład, aby utworzyć i przypisać rolę do uruchamiania serwer Zabbix i proxy:

```
CREATE USER 'usr_srv'@'localhost' IDENTIFIED BY 'password';
GRANT 'zbx_srv' TO 'usr_srv'@'localhost';
SET DEFAULT ROLE ALL TO 'usr_srv'@'localhost';
FLUSH PRIVILEGES;
```

2 Zabezpieczanie PostgreSQL/TimescaleDB

Przegląd

Ta sekcja zawiera najlepsze praktyki dotyczące zabezpieczania bazy danych PostgreSQL.

Note:
W przypadku podstawowej konfiguracji zobacz domyślne instrukcje tworzenia bazy danych PostgreSQL, które obejmują utworzenie użytkownika „zabbix" z pełnymi uprawnieniami do bazy danych Zabbix. Ten użytkownik jest właścicielem bazy danych i ma również niezbędne uprawnienia do modyfikowania struktury bazy danych podczas aktualizacji Zabbix.

Aby zwiększyć bezpieczeństwo, zaleca się skonfigurowanie bezpiecznego schematu korzystania ze schematów, a także utworzenie dodatkowych ról i użytkowników bazy danych z minimalnymi uprawnieniami. Te role i konta użytkowników powinny być skonfigurowane zgodnie z zasadą najmniejszych uprawnień, to znaczy powinny mieć wyłącznie uprawnienia niezbędne do wykonywania zamierzonych funkcji.

Konfiguracja bazy danych

Utwórz użytkownika, który będzie właścicielem bazy danych, i utwórz bazę danych Zabbix; właściciel bazy danych to użytkownik określony podczas tworzenia bazy danych:

```
createuser -U postgres -h localhost --pwprompt usr_owner
createdb -U postgres -h localhost -O usr_owner -E Unicode -T template0 zabbix
```

Note:
Czysta instalacja lub aktualizacja bazy danych musi zostać wykonana przez właściciela bazy danych. Wynika to z faktu, że prawo do usunięcia obiektu bazy danych lub zmiany jego definicji jest uprawnieniem przysługującym właścicielowi bazy danych i nie może zostać nadane ani odebrane.

Attention:
Poniższe polecenia na tej stronie muszą zostać wykonane, gdy połączenie z PostgreSQL jest nawiązane konkretnie z bazą danych zabbix.

Utwórz schemat zabbix i ustaw właściciela bazy danych (usr_owner) jako właściciela tego schematu:

```
CREATE SCHEMA zabbix AUTHORIZATION usr_owner;
```

Skonfiguruj bezpieczny wzorzec użycia schematu:

```
REVOKE CREATE ON SCHEMA public FROM PUBLIC;
REVOKE ALL ON DATABASE zabbix FROM PUBLIC;
-- Uwaga: search_path powinien wskazywać na schemat "zabbix":
ALTER ROLE ALL IN DATABASE zabbix SET search_path = "zabbix";
```

Po skonfigurowaniu bazy danych przejdź do tworzenia ról użytkowników.

Tworzenie ról użytkowników

Utwórz następujące role z odpowiadającymi im uprawnieniami:

- **zbx_srv** - rola do uruchamiania serwera Zabbix i proxy:

```
CREATE ROLE zbx_srv;
GRANT CONNECT ON DATABASE zabbix TO zbx_srv;
GRANT USAGE ON SCHEMA zabbix TO zbx_srv;
ALTER DEFAULT PRIVILEGES FOR ROLE usr_owner IN SCHEMA zabbix GRANT DELETE, INSERT, SELECT, UPDATE ON TABLE
ALTER DEFAULT PRIVILEGES FOR ROLE usr_owner IN SCHEMA zabbix GRANT SELECT, UPDATE, USAGE ON sequences TO z
```

- **zbx_web** - rola do uruchamiania frontendu Zabbix i API:

```
CREATE ROLE zbx_web;
GRANT CONNECT ON DATABASE zabbix TO zbx_web;
GRANT USAGE ON SCHEMA zabbix TO zbx_web;
ALTER DEFAULT PRIVILEGES FOR ROLE usr_owner IN SCHEMA zabbix GRANT DELETE, INSERT, SELECT, UPDATE ON TABLE
ALTER DEFAULT PRIVILEGES FOR ROLE usr_owner IN SCHEMA zabbix GRANT SELECT, UPDATE, USAGE ON sequences TO z
```

- **zbx_bckp** - rola do tworzenia kopii zapasowych tabel:

```
CREATE ROLE zbx_bckp;
GRANT CONNECT ON DATABASE zabbix TO zbx_bckp;
GRANT USAGE ON SCHEMA zabbix TO zbx_bckp;
ALTER DEFAULT PRIVILEGES FOR ROLE usr_owner IN SCHEMA zabbix GRANT SELECT ON TABLES TO zbx_bckp;
ALTER DEFAULT PRIVILEGES FOR ROLE usr_owner IN SCHEMA zabbix GRANT SELECT, UPDATE, USAGE ON sequences TO z
```

Note:
Przywracanie tabel jest możliwe tylko przez właściciela bazy danych.

Po utworzeniu ról można je przypisać użytkownikom.

Przypisywanie ról użytkowników

Aby przypisać utworzone role użytkowników, utwórz użytkowników i przypisz im odpowiednie role. W razie potrzeby zastąp `<user>`, `<role>` i `<password>`.

```
CREATE USER <user> WITH ENCRYPTED password '<password>';
GRANT <role> TO <user>;
```

Na przykład, aby utworzyć i przypisać rolę do uruchamiania serwera Zabbix i proxy:

```
CREATE USER usr_srv WITH ENCRYPTED password 'password';
GRANT zbx_srv TO usr_srv;
```

Partycjonowanie bazy danych z TimescaleDB

Partycjonowanie bazy danych jest ułatwione dzięki TimescaleDB. Aby korzystać z TimescaleDB, serwer Zabbix wymaga uprawnień właściciela bazy danych.

Jeśli schemat PostgreSQL `zabbix` został już utworzony w bazie danych `zabbix`, możesz włączyć TimescaleDB za pomocą następującego polecenia:

```
echo "CREATE EXTENSION IF NOT EXISTS timescaledb WITH SCHEMA zabbix CASCADE;" | sudo -u postgres psql zabb
```

2 Kryptografia

Przegląd

Ta sekcja zawiera najlepsze praktyki dotyczące bezpiecznej konfiguracji kryptografii.

Konfigurowanie SSL dla frontend Zabbix

W systemach opartych na RHEL zainstaluj pakiet `mod_ssl`:

```
dnf install mod_ssl
```

Utwórz katalog na klucze SSL:

```
mkdir -p /etc/httpd/ssl/private
chmod 700 /etc/httpd/ssl/private
```

Utwórz certyfikat SSL:

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/httpd/ssl/private/apache-selfsigned.key -
```

Wypełnij odpowiednio wyświetlane monity. Najważniejsza jest linia, w której podawana jest wartość `Common Name`. Musisz wpisać nazwę domeny, która ma być powiązana z twoim serwer. Możesz zamiast tego podać publiczny adres IP, jeśli nie masz nazwy domeny.

```
Country Name (2 letter code) [XX]:
State or Province Name (full name) []:
Locality Name (eg, city) [Default City]:
Organization Name (eg, company) [Default Company Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:example.com
Email Address []:
```

Edytuj plik konfiguracji SSL Apache (`/etc/httpd/conf.d/ssl.conf`):

```
DocumentRoot "/usr/share/zabbix"
ServerName example.com:443
SSLCertificateFile /etc/httpd/ssl/apache-selfsigned.crt
SSLCertificateKeyFile /etc/httpd/ssl/private/apache-selfsigned.key
```

Uruchom ponownie usługę Apache, aby zastosować zmiany:

```
systemctl restart httpd.service
```

3 Serwer WWW

Przegląd

Ta sekcja zawiera najlepsze praktyki dotyczące bezpiecznej konfiguracji serwera WWW.

Wymuszanie przekierowania głównego URL do Zabbix SSL

W systemach opartych na RHEL dodaj virtual host do konfiguracji Apache (`/etc/httpd/conf/httpd.conf`) i ustaw stałe przekierowanie dla katalogu głównego dokumentów do adresu URL Zabbix SSL. Zwróć uwagę, że `example.com` należy zastąpić rzeczywistą nazwą serwera.

```
#### Dodaj linie:

<VirtualHost *:*>
    ServerName example.com
    Redirect permanent / https://example.com
</VirtualHost>
```

Uruchom ponownie usługę Apache, aby zastosować zmiany:

```
systemctl restart httpd.service
```

Włączanie HTTP Strict Transport Security (HSTS) na serwerze WWW

Aby chronić frontend Zabbix przed atakami obniżenia wersji protokołu, zalecamy włączenie polityki HSTS na serwerze WWW.

Aby włączyć politykę HSTS dla frontend Zabbix w konfiguracji Apache, wykonaj następujące kroki:

1. Zlokalizuj plik konfiguracyjny swojego hosta wirtualnego:

   - `/etc/httpd/conf/httpd.conf` w systemach opartych na RHEL
   - `/etc/apache2/sites-available/000-default.conf` w Debian/Ubuntu

2. Dodaj następującą dyrektywę do pliku konfiguracyjnego swojego hosta wirtualnego:

```
<VirtualHost *:*>
    Header set Strict-Transport-Security "max-age=31536000"
</VirtualHost>
```

3. Uruchom ponownie usługę Apache, aby zastosować zmiany:

```
#### On RHEL-based systems:
systemctl restart httpd.service
```

```
#### On Debian/Ubuntu
systemctl restart apache2.service
```

Wymuszanie bezpiecznych i SameSite cookies sesji w Zabbix

Podczas konfigurowania Zabbix należy wymusić atrybuty secure i SameSite dla cookies sesji, aby zwiększyć bezpieczeństwo i zapobiegać atakom typu cross-site request forgery (CSRF). Jednak wymuszenie `SameSite=Strict` może powodować problemy w niektórych scenariuszach, takich jak:

- Widgety URL na pulpicie wyświetlające komunikat „użytkownik nie jest zalogowany” podczas osadzania iframe z tej samej domeny.
- Użytkownicy uzyskujący dostęp do pulpitu przez HTTP zamiast HTTPS mogą napotkać problemy z logowaniem.
- Brak możliwości udostępniania adresów URL do określonych sekcji menu Zabbix lub hostów.

Aby ograniczyć te problemy, użytkownicy powinni mieć możliwość dostosowania polityki SameSite.

1. Bezpieczne cookies

Ustawienie flagi `secure` zapewnia, że cookies są przesyłane wyłącznie przez HTTPS, co zapobiega ich ujawnieniu przez niezaszyfrowane połączenia.

Aby włączyć bezpieczne cookies w Zabbix, dodaj lub zmodyfikuj następujące ustawienie w konfiguracji serwera WWW:

Dla Apache:

```
Header always edit Set-Cookie ^(.*)$ $1;Secure
```

Dla Nginx:

```
proxy_cookie_path / "/; Secure";
```

Upewnij się, że dostęp do frontend Zabbix odbywa się przez HTTPS; w przeciwnym razie cookies z flagą `Secure` nie będą wysyłane.

2. Konfigurowanie atrybutu SameSite

Ustawienia serwera WWW mogą również wymuszać atrybut SameSite:

Dla Apache:

```
<IfModule mod_headers.c>
    Header onsuccess edit Set-Cookie (.*) "$1; SameSite=Strict"
</IfModule>
```

Dla Nginx (wersja 1.19.3+):

```
proxy_cookie_flags ~ samesite=Strict; # Zastąp ~ przez 'zbx_session', aby zwiększyć precyzję
```

Włączanie Content Security Policy (CSP) na serwerze WWW

Aby chronić frontend Zabbix przed atakami typu Cross Site Scripting (XSS), wstrzykiwaniem danych i podobnymi zagrożeniami, zalecamy włączenie Content Security Policy na serwerze WWW. W tym celu skonfiguruj serwer WWW tak, aby zwracał nagłówek HTTP.

> **Attention:**
> Poniższa konfiguracja nagłówka CSP dotyczy wyłącznie domyślnej instalacji frontendu Zabbix oraz przypadków, gdy cała zawartość pochodzi z domeny witryny (z wyłączeniem subdomen). Inna konfiguracja nagłówka CSP może być wymagana, jeśli na przykład konfigurujesz widżet *URL* tak, aby wyświetlał zawartość z subdomen witryny lub domen zewnętrznych, przełączasz się z *OpenStreetMap* na inny silnik map albo dodajesz zewnętrzny CSS lub widżety. Jeśli używasz metody uwierzytelniania wieloskładnikowego Duo Universal Prompt, pamiętaj, aby dodać „duo.com” do dyrektywy CSP w pliku konfiguracji virtual hosta.

Aby włączyć CSP dla frontendu Zabbix w konfiguracji Apache, wykonaj następujące kroki:

1. Zlokalizuj plik konfiguracji virtual hosta:

- `/etc/httpd/conf/httpd.conf` w systemach opartych na RHEL
- `/etc/apache2/sites-available/000-default.conf` w Debian/Ubuntu

2. Dodaj następującą dyrektywę do pliku konfiguracji virtual hosta:

```
<VirtualHost *:*>
    Header set Content-Security-Policy: "default-src 'self' *.openstreetmap.org; script-src 'self' 'unsafe
</VirtualHost>
```

3. Uruchom ponownie usługę Apache, aby zastosować zmiany:

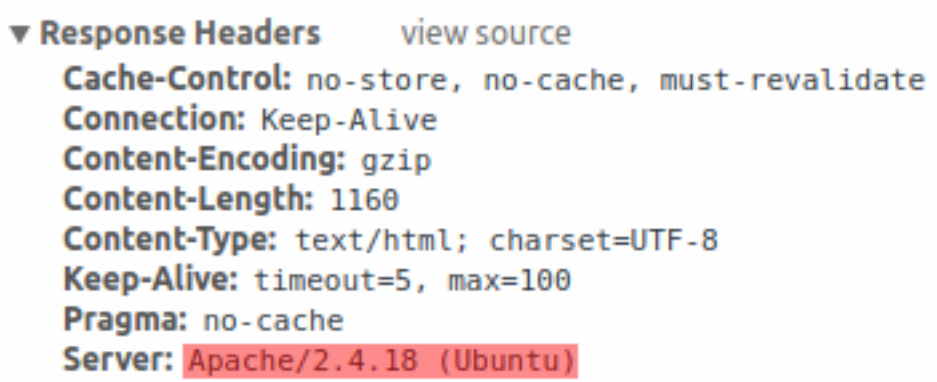
```
#### W systemach opartych na RHEL:
systemctl restart httpd.service

#### W Debian/Ubuntu
systemctl restart apache2.service
```

Wyłączanie ujawniania informacji o serwerze WWW

Aby zwiększyć bezpieczeństwo, zaleca się wyłączenie wszystkich sygnatur serwera WWW.

Domyślnie serwer WWW ujawnia sygnaturę oprogramowania:



Sygnaturę można wyłączyć, dodając następujące parametry do pliku konfiguracyjnego Apache:

```
ServerSignature Off
ServerTokens Prod
```

Sygnaturę PHP (nagłówek HTTP X-Powered-By) można wyłączyć, zmieniając plik konfiguracyjny `php.ini` (domyślnie sygnatura jest wyłączona):

```
expose_php = Off
```

Aby zmiany w plikach konfiguracyjnych zostały zastosowane, wymagane jest ponowne uruchomienie serwera WWW.

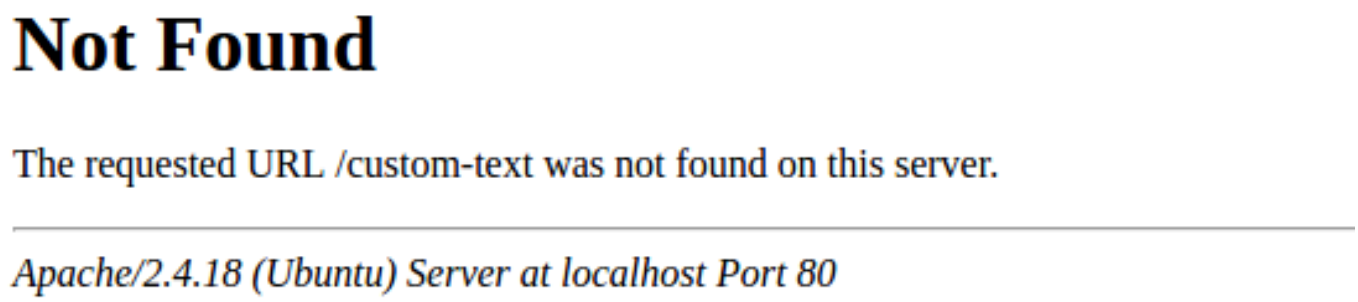
Dla dodatkowego bezpieczeństwa można użyć narzędzia *mod_security* z Apache (pakiet *libapache2-mod-security2*). To narzędzie umożliwia usunięcie sygnatury serwera zamiast usuwania jedynie wersji z sygnatury serwera. Sygnaturę serwera można zmienić na dowolną wartość, ustawiając ”SecServerSignature” na żądaną wartość po zainstalowaniu *mod_security*.

Aby uzyskać pomoc dotyczącą usuwania/zmiany sygnatur oprogramowania, zapoznaj się z dokumentacją swojego serwera WWW.

Wyłączanie domyślnych stron błędów serwera WWW

Aby uniknąć ujawnienia informacji, zaleca się wyłączenie domyślnych stron błędów.

Domyślnie serwer WWW używa wbudowanych stron błędów:



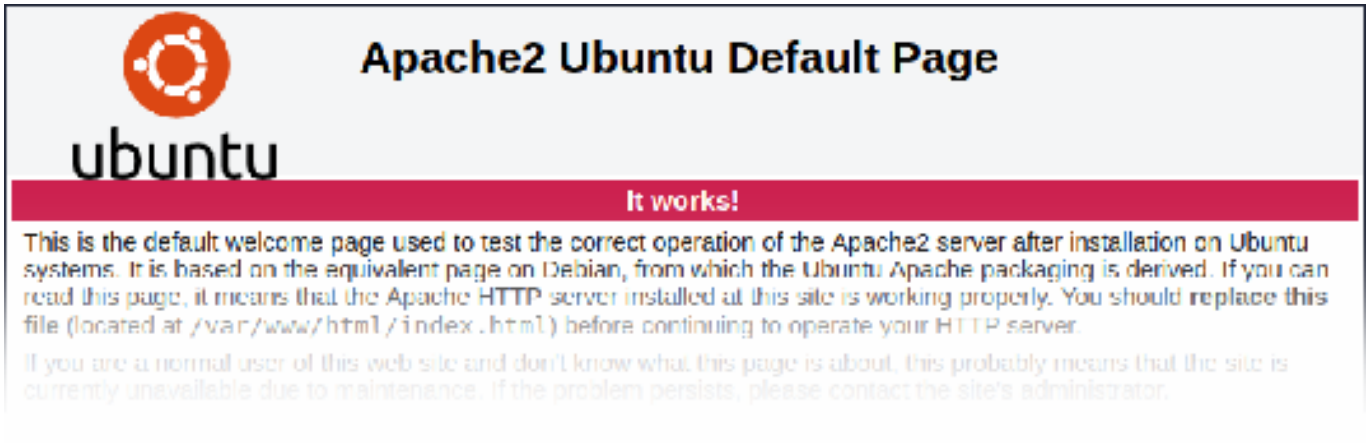
Te domyślne strony błędów należy zastąpić/usunąć. Na przykład dyrektywy „ErrorDocument” można użyć do zdefiniowania niestandardowej strony/tekstu błędu dla serwera WWW Apache.

Aby uzyskać informacje o tym, jak zastąpić/usunąć domyślne strony błędów, zapoznaj się z dokumentacją swojego serwera WWW.

Usuwanie strony testowej serwera WWW

Aby uniknąć ujawnienia informacji, zaleca się usunięcie strony testowej serwera WWW.

Domyślnie katalog główny serwera WWW Apache zawiera testową stronę `index.html`:



Aby uzyskać informacje o tym, jak usunąć domyślne strony testowe, zapoznaj się z dokumentacją swojego serwera WWW.

Ustaw nagłówek odpowiedzi HTTP X-Frame-Options

Domyślnie Zabbix jest skonfigurowany z parametrem *Use X-Frame-Options HTTP header* ustawionym na `SAMEORIGIN`. Oznacza to, że zawartość może być ładowana tylko w ramce, która ma to samo pochodzenie co sama strona.

Elementy frontend Zabbix, które pobierają zawartość z zewnętrznych adresów URL (a mianowicie widżet URL na pulpicie), wyświetlają pobraną zawartość w piaskownicy z włączonymi wszystkimi ograniczeniami sandbox.

Ustawienia te zwiększają bezpieczeństwo frontend Zabbix i zapewniają ochronę przed atakami XSS oraz clickjacking. Użytkownicy *Super admin* mogą w razie potrzeby zmienić parametry *Use iframe sandboxing* i *Use X-Frame-Options HTTP header*. Przed zmianą ustawień domyślnych należy dokładnie rozważyć ryzyko i korzyści. Nie zaleca się całkowitego wyłączania iframe sandboxing ani nagłówka odpowiedzi HTTP X-Frame-Options.

Ukrywanie pliku z listą najczęściej używanych haseł

Aby zwiększyć złożoność ataków brute force na hasła, zaleca się ograniczenie dostępu do pliku `ui/data/top_passwords.txt`. Plik ten zawiera listę najczęściej używanych oraz specyficznych kontekstowo haseł i uniemożliwia użytkownikom ustawianie takich haseł (jeśli parametr *Avoid easy-to-guess passwords* jest włączony w polityce haseł).

Aby ograniczyć dostęp do pliku `top_passwords.txt`, zmodyfikuj konfigurację swojego serwera WWW.

W Apache dostęp do pliku można ograniczyć za pomocą pliku `.htaccess`:

```
<Files "top_passwords.txt">
    Order Allow,Deny
    Deny from all
</Files>
```

W NGINX dostęp do pliku można ograniczyć za pomocą dyrektywy `location`:

```
location = /data/top_passwords.txt {
    deny all;
    return 404;
}
```

2 Najlepsze praktyki konfiguracji

Przegląd

Ta sekcja przedstawia najlepsze praktyki dotyczące konfiguracji Zabbix w celu osiągnięcia optymalnej wydajności i łatwości użytkowania. Zalecenia opierają się na wskazówkach deweloperów Zabbix oraz praktycznym doświadczeniu trenerów Zabbix i inżynierów wsparcia.

Każda instalacja Zabbix jest unikalna i niektóre z tych wytycznych mogą nie być odpowiednie dla Twojej konkretnej konfiguracji. Zaleca się jednak, aby w miarę możliwości stosować się do tych wytycznych, by uniknąć typowych potencjalnych problemów.

Note:
Jeśli uważasz, że tę stronę można ulepszyć, chętnie poznamy Twoją opinię! Zaznacz odpowiedni fragment tekstu i naciśnij **ctrl+Enter**, aby zgłosić błąd lub przekazać swoją opinię.

Hosty i pozycje Definiowanie hosta

Host w Zabbix nie jest fizyczną maszyną ani urządzeniem, lecz logiczną jednostką. Do celów monitorowania możesz tworzyć oddzielne hosty dla bazy danych lub na przykład maszyny wirtualnej. Alternatywnie możesz utworzyć ogólny host *Laptop Johna* i monitorować wszystkie metryki w ramach tego hosta.

Najlepszą praktyką jest utworzenie oddzielnego hosta dla każdej niezależnej instancji, takiej jak maszyna wirtualna, baza danych, kontener lub przełącznik sieciowy. Korzystając z tego podejścia:

1. Unikniesz bałaganu w danych monitorowania dzięki oddzielnym pozycjom, wyzwalaczom i powiadomieniom o alertach dla każdego hosta.
2. Precyzyjnie dostosujesz poziomy dostępu użytkowników. Możesz skonfigurować role użytkowników, aby przyznać dostęp do przeglądania i/lub konfiguracji tylko określonych hostów. Zobacz także zasadę najmniejszych uprawnień.

Hosty ze zduplikowanymi pozycjami

Jeśli masz kilka podobnych hostów, takich jak *Przełącznik sieciowy 1* i *Przełącznik sieciowy 2*, Zabbix udostępnia wiele sposobów na szybkie odtworzenie hosta. Możesz po prostu sklonować hosta wraz ze wszystkimi jego metrykami, naciskając przycisk Clone, ale w takim przypadku, aby później zaktualizować pozycję, trzeba będzie zrobić to ręcznie na każdym hoście.

Najlepszą praktyką jest utworzenie szablonu ze wszystkimi wymaganymi metrykami, na przykład *Szablon przełącznika sieciowego*. Następnie pogrupuj podobne hosty w grupę hostów; w powyższym przykładzie może to być *Przełączniki sieciowe*. Teraz w sekcji *Data Collection -> Hosts* możesz filtrować wszystkie hosty według grupy hostów i użyć przycisku *Mass update*, aby podłączyć szablon do wszystkich swoich przełączników sieciowych.

Pozycje zależne

Aby zminimalizować liczbę żądań do monitorowanego obiektu, Zabbix umożliwia tworzenie pozycji nadrzędnych i zależnych. W takim przypadku pozycja nadrzędna zbiera duży zestaw informacji w ramach jednego żądania. Następnie można skonfigurować pozycje zależne tak, aby wyodrębniały określone fragmenty danych z tego zbioru za pomocą preprocessing i zapisywały je jako osobne metryki.

Na przykład pozycja nadrzędna może pobierać odpowiedź JSON lub XML zawierającą wiele metryk albo wykonywać zapytanie do bazy danych, które zwraca wiele kolumn danych (np. liczbę otwartych połączeń, przerwanych połączeń, maksymalną dozwoloną liczbę jednoczesnych połączeń oraz łączną skumulowaną liczbę połączeń od momentu uruchomienia), a pozycje zależne będą analizować i zapisywać każdą wymaganą wartość osobno.

Najlepszą praktyką dla tej konfiguracji jest odrzucanie historii pozycji nadrzędnej zaraz po zebraniu danych i przechowywanie wyłącznie danych pozycji zależnych.

Serwery i proxy

Jeśli wszystkie hosty znajdują się w tej samej sieci lokalnej co serwer Zabbix i nie ma obaw dotyczących skalowalności ani wydajności, możesz nie potrzebować proxy. W większych lub bardziej złożonych środowiskach bezpośrednie monitorowanie hostów przez serwer Zabbix może nie być wystarczające. Dodanie proxy i przypisanie części hostów do tego proxy pozwala na bardziej równomierne rozłożenie obciążenia.

Najlepszą praktyką jest dodanie proxy Zabbix, gdy:

1. Monitorujesz wiele hostów przy użyciu różnych metod zbierania metryk za zaporą sieciową. Proxy będzie zbierać dane z hostów i przekazywać je do serwera Zabbix, zmniejszając potrzebę otwierania wielu portów zapory sieciowej.
2. Monitorujesz zdalne lokalizacje, oddziały i/lub sieci. W przypadku przerwy w połączeniu sieciowym między serwerem Zabbix a zdalnymi lokalizacjami, proxy Zabbix wdrożone w tych lokalizacjach będą kontynuować zbieranie danych i prześlą zebrane dane z powrotem do serwera Zabbix po przywróceniu połączenia sieciowego.
3. Masz wdrożenie na dużą skalę i chcesz zmniejszyć obciążenie serwera Zabbix oraz poprawić wydajność. Definicja wdrożenia na dużą skalę jest bardzo szeroka i zależy nie tylko od liczby hostów, ale także od liczby wartości zbieranych na sekundę.

Sekretne makra

Możesz używać sekretnych makr użytkownika jako sekretnego tekstu lub sekretnych makr vault.

Aby zwiększyć bezpieczeństwo podczas korzystania z sekretnych makr vault, zaleca się skonfigurowanie pobierania wartości makr niezależnie przez serwer Zabbix i proxy Zabbix. Domyślnie wartości sekretnych makr są pobierane przez serwer Zabbix i przekazywane do proxy Zabbix.

18 API

Przegląd API Zabbix umożliwia programowe pobieranie i modyfikowanie konfiguracji Zabbix oraz zapewnia dostęp do danych historycznych. Jest ono szeroko wykorzystywane do:

- tworzenia nowych aplikacji współpracujących z Zabbix;
- integracji Zabbix z oprogramowaniem innych producentów;
- automatyzacji rutynowych zadań.

API Zabbix jest interfejsem API opartym na HTTP i jest dostarczane jako część web frontend. Wykorzystuje protokół JSON-RPC 2.0, co oznacza dwie rzeczy:

- API składa się z zestawu oddzielnych metod;
- żądania i odpowiedzi między klientami a API są kodowane przy użyciu formatu JSON.

Więcej informacji o protokole i formacie JSON można znaleźć w specyfikacji JSON-RPC 2.0 oraz na stronie głównej formatu JSON.

Więcej informacji o integrowaniu funkcjonalności Zabbix z aplikacjami Python można znaleźć w bibliotece Python dla Zabbix.

> **Note:**
> Dostęp użytkownika w Zabbix, obejmujący zarówno konfigurację, jak i dane historyczne, zależy od typu użytkownika, przypisanej roli użytkownika oraz grup użytkowników.

Struktura API składa się z wielu metod, które są umownie pogrupowane w oddzielne API. Każda z metod wykonuje jedno konkretne zadanie. Na przykład metoda `host.create` należy do API *host* i służy do tworzenia nowych hostów. Historycznie API są czasami określane jako „klasy".

> **Note:**
> Większość API zawiera co najmniej cztery metody: `get`, `create`, `update` i `delete`, służące odpowiednio do pobierania, tworzenia, aktualizowania i usuwania danych, jednak niektóre API mogą udostępniać zupełnie inny zestaw metod.

Wykonywanie żądań Po skonfigurowaniu frontend możesz używać zdalnych żądań HTTP do wywoływania API. W tym celu musisz wysyłać żądania HTTP POST do pliku `api_jsonrpc.php` znajdującego się w katalogu frontend. Na przykład, jeśli Twój frontend Zabbix jest zainstalowany pod adresem `https://example.com/zabbix`, żądanie HTTP wywołujące metodę `apiinfo.version` może wyglądać następująco:

```
curl --request POST \
  --url 'https://example.com/zabbix/api_jsonrpc.php' \
  --header 'Content-Type: application/json-rpc' \
  --data '{"jsonrpc":"2.0","method":"apiinfo.version","params":{},"id":1}'
```

Żądanie musi mieć nagłówek `Content-Type` ustawiony na jedną z tych wartości: `application/json-rpc`, `application/json` lub `application/jsonrequest`.

Obiekt żądania musi zawierać następujące właściwości:

- `jsonrpc` - wersję protokołu JSON-RPC używaną przez API (API Zabbix implementuje JSON-RPC w wersji 2.0);
- `method` - wywoływaną metodę API;
- `params` - parametry, które zostaną przekazane do metody API;
- `id` - dowolny identyfikator żądania (jeśli zostanie pominięty, API traktuje żądanie jako powiadomienie).

Jeśli żądanie jest poprawne, odpowiedź zwrócona przez API powinna wyglądać następująco:

```
{
    "jsonrpc": "2.0",
    "result": "8.0.0",
    "id": 1
}
```

Obiekt odpowiedzi z kolei zawiera następujące właściwości:

- `jsonrpc` - wersję protokołu JSON-RPC;
- `result` - dane zwrócone przez metodę;
- `id` - identyfikator odpowiadającego żądania.

Przykładowy przepływ pracy Poniższa sekcja przeprowadzi Cię przez kilka przykładów użycia bardziej szczegółowo.

Uwierzytelnianie Aby uzyskać dostęp do jakichkolwiek danych w Zabbix, musisz:

- użyć istniejącego tokenu API (utworzonego w Zabbix frontend lub przy użyciu Token API);
- użyć tokenu uwierzytelniającego uzyskanego za pomocą metody user.login.

Na przykład, jeśli chcesz uzyskać nowy token uwierzytelniający, logując się jako standardowy użytkownik *Admin*, żądanie JSON będzie wyglądać następująco:

```
curl --request POST \
  --url 'https://example.com/zabbix/api_jsonrpc.php' \
  --header 'Content-Type: application/json-rpc' \
  --data '{"jsonrpc":"2.0","method":"user.login","params":{"username":"Admin","password":"zabbix"},"id":1}
```

Jeśli podasz poprawne dane logowania, odpowiedź zwrócona przez API powinna zawierać token uwierzytelniający użytkownika:

```
{
    "jsonrpc": "2.0",
    "result": "0424bd59b807674191e7d77572075f33",
    "id": 1
}
```

Metody autoryzacji Za pomocą nagłówka ”Authorization”

Wszystkie żądania API wymagają uwierzytelnienia lub tokenu API. Dane uwierzytelniające można przekazać, używając nagłówka Authorization w żądaniu:

```
curl --request POST \
  --url 'https://example.com/zabbix/api_jsonrpc.php' \
  --header 'Authorization: Bearer 0424bd59b807674191e7d77572075f33'
```

Attention:
Jeśli występują problemy z uwierzytelnianiem, zobacz Przekazywanie nagłówka Authorization.

API Zabbix akceptuje nagłówki bez rozróżniania wielkości liter (np. `authorization`, `Authorization` i `AUTHORIZATION` są traktowane tak samo).

Nagłówek Authorization jest obsługiwany w żądaniach między źródłami (CORS).

Za pomocą pliku cookie Zabbix

Plik cookie *”zbx_session”* jest używany do autoryzacji żądania API z interfejsu Zabbix UI wykonywanego przy użyciu JavaScript (z modułu lub niestandardowego widżetu).

Pobieranie hostów Masz teraz prawidłowy token uwierzytelnienia użytkownika (przedstawiony jako zmienna w poniższych przykładach), którego można użyć do uzyskania dostępu do danych w Zabbix. Na przykład możesz użyć metody host.get, aby pobrać identyfikatory, nazwy hostów i interfejsy wszystkich skonfigurowanych hostów:

Żądanie:

```
curl --request POST \
  --url 'https://example.com/zabbix/api_jsonrpc.php' \
  --header 'Authorization: Bearer ${AUTHORIZATION_TOKEN}' \
  --header 'Content-Type: application/json-rpc' \
  --data @data.json
```

Note:
`data.json` to plik zawierający zapytanie JSON. Zamiast pliku możesz przekazać zapytanie w argumencie `--data`.

data.json

```
{
    "jsonrpc": "2.0",
    "method": "host.get",
    "params": {
        "output": [
            "hostid",
```

```
            "host"
        ],
        "selectInterfaces": [
            "interfaceid",
            "ip"
        ]
    },
    "id": 2
}
```

Obiekt odpowiedzi będzie zawierał żądane dane o hostach:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "hostid": "10084",
            "host": "Zabbix server",
            "interfaces": [
                {
                    "interfaceid": "1",
                    "ip": "127.0.0.1"
                }
            ]
        }
    ],
    "id": 2
}
```

Note:
Ze względów wydajnościowych zawsze zaleca się podawanie na liście właściwości obiektu, które chcesz pobrać. Dzięki temu unikniesz pobierania wszystkiego.

Tworzenie nowej pozycji Teraz utwórz nową pozycję na hoście „Zabbix server", używając danych uzyskanych z poprzedniego żądania `host.get`. Można to zrobić za pomocą metody item.create:

```
curl --request POST \
  --url 'https://example.com/zabbix/api_jsonrpc.php' \
  --header 'Authorization: Bearer ${AUTHORIZATION_TOKEN}' \
  --header 'Content-Type: application/json-rpc' \
  --data '{"jsonrpc":"2.0","method":"item.create","params":{"name":"Free disk space on /home/joe/","key_":
```

Pomyślna odpowiedź będzie zawierać ID nowo utworzonej pozycji, którego można użyć do odwoływania się do tej pozycji w kolejnych żądaniach:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "24759"
        ]
    },
    "id": 3
}
```

Note:
Metoda `item.create`, podobnie jak inne *metody create*, może również przyjmować tablice obiektów i tworzyć wiele pozycji za pomocą jednego wywołania API.

Tworzenie wielu wyzwalaczy Jeśli więc *metody create* akceptują tablice, możesz dodać wiele wyzwalaczy, na przykład takie:

```
curl --request POST \
  --url 'https://example.com/zabbix/api_jsonrpc.php' \
```

```
  --header 'Authorization: Bearer ${AUTHORIZATION_TOKEN}' \
  --header 'Content-Type: application/json-rpc' \
  --data '{"jsonrpc":"2.0","method":"trigger.create","params":[{"description":"Obciążenie procesora jest z
```

Pomyślna odpowiedź będzie zawierać identyfikatory nowo utworzonych wyzwalaczy:

```
{
    "jsonrpc": "2.0",
    "result": {
        "triggerids": [
            "17369",
            "17370"
        ]
    },
    "id": 4
}
```

Aktualizowanie pozycji Włącz pozycję, ustawiając jej status na „0”:

```
curl --request POST \
  --url 'https://example.com/zabbix/api_jsonrpc.php' \
  --header 'Authorization: Bearer ${AUTHORIZATION_TOKEN}' \
  --header 'Content-Type: application/json-rpc' \
  --data '{"jsonrpc":"2.0","method":"item.update","params":{"itemid":"10092","status":0},"id":5}'
```

Pomyślna odpowiedź będzie zawierać ID zaktualizowanej pozycji:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "10092"
        ]
    },
    "id": 5
}
```

> **Note:**
> Metoda `item.update`, podobnie jak inne *metody aktualizacji*, może również przyjmować tablice obiektów i aktualizować wiele pozycji za pomocą jednego wywołania API.

Aktualizowanie wielu wyzwalaczy Włącz wiele wyzwalaczy, ustawiając ich status na „0”:

```
curl --request POST \
  --url 'https://example.com/zabbix/api_jsonrpc.php' \
  --header 'Authorization: Bearer ${AUTHORIZATION_TOKEN}' \
  --header 'Content-Type: application/json-rpc' \
  --data '{"jsonrpc":"2.0","method":"trigger.update","params":[{"triggerid":"13938","status":0},{"triggeri
```

Pomyślna odpowiedź będzie zawierać identyfikatory zaktualizowanych wyzwalaczy:

```
{
    "jsonrpc": "2.0",
    "result": {
        "triggerids": [
            "13938",
            "13939"
        ]
    },
    "id": 6
}
```

Obsługa błędów Do tej pory wszystko, czego próbowano, działało poprawnie. Ale co by się stało, gdyby wykonać nieprawidłowe wywołanie API? Spróbuj utworzyć kolejny host, wywołując host.create, ale pomijając wymagany parametr `groups`:

```
curl --request POST \
  --url 'https://example.com/zabbix/api_jsonrpc.php' \
  --header 'Authorization: Bearer ${AUTHORIZATION_TOKEN}' \
  --header 'Content-Type: application/json-rpc' \
  --data '{"jsonrpc":"2.0","method":"host.create","params":{"host":"Linux server","interfaces":[{"type":1,
```

Odpowiedź będzie wtedy zawierać komunikat o błędzie:

```
{
    "jsonrpc": "2.0",
    "error": {
        "code": -32602,
        "message": "Invalid params.",
        "data": "No groups for host \"Linux server\"."
    },
    "id": 7
}
```

Jeśli wystąpił błąd, zamiast właściwości `result` obiekt odpowiedzi będzie zawierał właściwość `error` z następującymi danymi:

- `code` - kod błędu;
- `message` - krótkie podsumowanie błędu;
- `data` - bardziej szczegółowy komunikat o błędzie.

Błędy mogą wystąpić w różnych przypadkach, na przykład przy użyciu nieprawidłowych wartości wejściowych, przekroczeniu limitu czasu sesji lub próbie uzyskania dostępu do nieistniejących obiektów. Aplikacja powinna potrafić w poprawny sposób obsługiwać tego rodzaju błędy.

Wersje API Aby uprościć wersjonowanie API, od Zabbix 2.0.4 wersja API odpowiada wersji samego Zabbix. Możesz użyć metody apiinfo.version, aby sprawdzić wersję API, z którą pracujesz. Może to być przydatne przy dostosowywaniu aplikacji do korzystania z funkcji specyficznych dla danej wersji.

Zabbix gwarantuje wsteczną kompatybilność funkcji w obrębie wersji głównej. W przypadku wprowadzania zmian niezgodnych wstecznie między głównymi wydaniami Zabbix zwykle pozostawia stare funkcje jako przestarzałe w następnym wydaniu, a usuwa je dopiero w kolejnym. Sporadycznie Zabbix może usuwać funkcje między głównymi wydaniami bez zapewnienia jakiejkolwiek wstecznej kompatybilności. Ważne jest, aby nigdy nie polegać na żadnych przestarzałych funkcjach i jak najszybciej przechodzić na nowsze alternatywy.

> **Note:**
> Możesz śledzić wszystkie zmiany wprowadzone w API w dzienniku zmian API.

Dalsza lektura Masz już wystarczającą wiedzę, aby rozpocząć pracę z API Zabbix, jednak nie poprzestawaj na tym. W ramach dalszej lektury zalecamy zapoznanie się z listą dostępnych API.

Odniesienie do metody

Ta sekcja zawiera przegląd funkcji udostępnianych przez Zabbix API i pomoże Ci odnaleźć się w dostępnych klasach i metodach.

Monitorowanie API Zabbix umożliwia dostęp do historii i innych danych zebranych podczas monitorowania.

Pulpity nawigacyjne

Zarządzaj pulpitami i na ich podstawie twórz zaplanowane raporty.

API pulpitu | API szablonu pulpitu | API raportu

Klaster o wysokiej dostępności

Pobierz listę węzłów serwera i ich status.

API klastra wysokiej dostępności

Historia

Pobierz wartości historyczne zebrane przez procesy monitorowania Zabbix do prezentacji lub dalszego przetwarzania.

API historii

Trendy

Pobierz wartości trendów obliczone przez serwer Zabbix do prezentacji lub dalszego przetwarzania.

Interfejs API trendów

Wydarzenia

Pobierz zdarzenia generowane przez wyzwalacze, wykrywanie sieci i inne systemy Zabbix do bardziej elastycznego zarządzania sytuacjami lub integrację z narzędziami firm trzecich.

Interfejs API zdarzeń

Problemy

Pobierz problemy zgodnie z podanymi parametrami.

Problem API

Mapy

Konfiguruj mapy, aby tworzyć szczegółowe, dynamiczne reprezentacje Twojej infrastruktury IT.

API mapy

Zadania

Interakcja z menedżerem zadań serwera Zabbix, tworzenie zadań i pobieranie odpowiedzi.

API zadań

Usługi API Zabbix umożliwia dostęp do danych zebranych podczas monitorowania usług.

Umowa dotycząca poziomu usług

Zdefiniuj Wytyczne Poziomu Usług (SLO), pobierz szczegółowe Wskaźniki Poziomu Usług (SLI) wydajności usługi.

SLA API

Usługi

Zarządzaj usługami do monitorowania poziomu usług i pobieraj szczegółowe informacje o SLA dowolnej usługi.

API usługi

Zbieranie danych API Zabbix umożliwia zarządzanie konfiguracją systemu monitoringu.

Hosty i grupy hostów

Zarządzaj grupami hostów, hostami i wszystkim, co jest z nimi związane, w tym interfejsami hosta, makrami hosta i okresami konserwacji.

API hosta | APi Grupy gospodarzy | API interfejsu hosta | API makr użytkownika | API map wartości | API konserwacji

Elementy

Zdefiniuj elementy do monitorowania.

API elementu

Wyzwalacze

Skonfiguruj wyzwalacze, aby powiadamiały Cię o problemach w systemie. Zarządzaj zależnościami wyzwalacza.

API Wyzwalaczy

Wykresy

Edytuj wykresy lub oddzielne elementy wykresu, aby lepiej prezentować zebrane dane.

API Wykresów | API elementu wykresu

Szablony i grupy szablonów

Zarządzaj szablonami i łącz je z hostami lub innymi szablonami.

API szablonów | API grup szablonów | API map wartości

Wykrywanie niskiego poziomu

Skonfiguruj reguły wykrywania niskiego poziomu, jak również prototypy elementów, wyzwalaczy i wykresów do monitorowania jednostek dynamicznych.

API reguł LLD | API prototypu elementu | API prototypu wyzwalacza | API prototypu wykresu | API prototypu hosta

Korelacja zdarzeń

Twórz niestandardowe reguły korelacji zdarzeń.

API korelacji

Wykrywanie sieci

Zarządzaj regułami wykrywania na poziomie sieci, aby automatycznie wyszukiwać i monitorować nowe hosty. Uzyskaj pełny dostęp do informacji o wykrytych usługach i hostah.

API reguły wykrywania | API sprawdzenia wykrywania | API wykrycia hosta | API wykrycia usługi

Eksport i import

Eksportuj i importuj dane konfiguracyjne Zabbix do tworzenia kopii zapasowych konfiguracji, migracji lub aktualizacji konfiguracji na dużą skalę.

API konfiguracjiI

Monitorowanie sieci WWW

Skonfiguruj scenariusze internetowe, aby monitorować swoje aplikacje i usługi internetowe.

API monitoringu WWW

Alerty API Zabbix umożliwia zarządzanie akcjami i alertami systemu monitoringu.

Akcje i alerty

Zdefiniuj akcje i operacje, aby powiadamiać użytkowników o określonych zdarzeniach lub automatycznie wykonywać zdalne polecenia. Uzyskaj dostęp do informacji o generowanych alertach i ich odbiorcach.

API akcji | API alarmów

Typy mediów

Skonfiguruj typy mediów i wiele sposobów, na jakie użytkownicy będą otrzymywać alerty.

API typów mediów

Skrypty

Konfiguruj i wykonuj skrypty, które pomogą Ci w codziennych zadaniach.

API skryptu

Użytkownicy API Zabbix umożliwia zarządzanie użytkownikami systemu monitoringu.

Użytkownicy i grupy użytkowników

Dodaj użytkowników, którzy będą mieli dostęp do Zabbix, przypisz ich do grup użytkowników i nadaj uprawnienia. Utwórz role do szczegółowego zarządzania prawami użytkowników.

API użytkowników | API grup użytkowników | API katalogu użytkowników | API ról użytkowników

Tokeny API

Zarządzaj tokenami autoryzacyjnymi.

API tokena

Uwierzytelnianie

Zmień opcje konfiguracji uwierzytelniania.

API uwierzytelniania

Administracja Za pomocą API Zabbix można zmieniać ustawienia administracyjne systemu monitoringu.

Ogólne

Zmień wybrane globalne opcje konfiguracji.

API autorejestracji | API map ikon | API obrazów | API ustawień | API wyrażeń regularnych | API modułów | API konektorów

Dziennik audytu

Śledź zmiany konfiguracji dokonane przez każdego użytkownika.

API dziennika audytu

Porządkowanie

Skonfiguruj porządkowanie.

Housekeeping API

Proxy i grupy proxy

Zarządzaj proxy używanymi w rozproszonej konfiguracji monitorowania.

Proxy API | API grup proxy

Makra

Zarządzaj makrami.

API makr użytkownika

Informacje o interfejsie API Pobierz wersję API Zabbix, aby Twoja aplikacja mogła używać funkcji specyficznych dla wersji.

API informacje o API

Akcja

Ta klasa jest przeznaczona do pracy z akcjami.

Odwołania do obiektów:

- Akcja
- Operacja akcji
  - Wiadomość operacji akcji
  - Warunek operacji akcji
- Operacja odzyskiwania akcji
- Operacja aktualizacji akcji
- Filtr akcji
  - Warunek filtra akcji

Dostępne metody:

- action.create - tworzenie nowych akcji
- action.delete - usuwanie akcji
- action.get - pobieranie akcji
- action.update - aktualizowanie akcji

Obiekt Akcji

Następujące obiekty są bezpośrednio powiązane z API `action`.

Akcja

Obiekt akcji ma następujące właściwości.

Właściwość	Typ	Opis
actionid	ID	ID akcji. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji

Właściwość	Typ	Opis
esc_period	string	Domyślny czas trwania kroku operacji. Musi wynosić co najmniej 60 sekund. Akceptuje sekundy, jednostkę czasu z sufiksem lub makro użytkownika. Zachowanie właściwości: - *obsługiwane* jeśli `eventsource` jest ustawione na „zdarzenie utworzone przez wyzwalacz”, „zdarzenie wewnętrzne” lub „zdarzenie utworzone przy aktualizacji stanu usługi”
eventsource	integer	Typ zdarzeń, które będzie obsługiwać akcja. Zobacz właściwość `source` zdarzenia, aby uzyskać listę obsługiwanych typów zdarzeń. Zachowanie właściwości: - *stałe* - *wymagane* dla operacji tworzenia
name	string	Nazwa akcji. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
status	integer	Określa, czy akcja jest włączona, czy wyłączona. Możliwe wartości: 0 - *(domyślnie)* włączona; 1 - wyłączona.
pause_symptoms	integer	Określa, czy wstrzymać eskalację, jeśli zdarzenie jest zdarzeniem symptomatycznym. Możliwe wartości: 0 - Nie wstrzymuj eskalacji dla problemów symptomatycznych; 1 - *(domyślnie)* Wstrzymaj eskalację dla problemów symptomatycznych. Zachowanie właściwości: - *obsługiwane* jeśli `eventsource` jest ustawione na „zdarzenie utworzone przez wyzwalacz”
pause_suppressed	integer	Określa, czy wstrzymać eskalację w okresach konserwacji. Możliwe wartości: 0 - Nie wstrzymuj eskalacji; 1 - *(domyślnie)* Wstrzymaj eskalację. Zachowanie właściwości: - *obsługiwane* jeśli `eventsource` jest ustawione na „zdarzenie utworzone przez wyzwalacz”
notify_if_canceled	integer	Określa, czy wysyłać powiadomienie po anulowaniu eskalacji. Możliwe wartości: 0 - Nie powiadamiaj po anulowaniu eskalacji; 1 - *(domyślnie)* Powiadamiaj po anulowaniu eskalacji. Zachowanie właściwości: - *obsługiwane* jeśli `eventsource` jest ustawione na „zdarzenie utworzone przez wyzwalacz”

Operacja akcji

Obiekt operacji akcji definiuje operację, która zostanie wykonana, gdy akcja zostanie uruchomiona. Ma następujące właściwości.

Właściwość	Typ	Opis
operationtype	integer	Typ operacji. Możliwe wartości: 0 - wyślij wiadomość; 1 - skrypt globalny; 2 - dodaj host; 3 - usuń host; 4 - dodaj do grupy hostów; 5 - usuń z grupy hostów; 6 - podłącz szablon; 7 - odłącz szablon; 8 - włącz host; 9 - wyłącz host; 10 - ustaw tryb inwentaryzacji hosta; 13 - dodaj tagi hosta; 14 - usuń tagi hosta. Możliwe wartości, jeśli `eventsource` obiektu Action object jest ustawione na „zdarzenie utworzone przez wyzwalacz” lub „zdarzenie utworzone przy aktualizacji stanu usługi”: 0 - ”wyślij wiadomość”; 1 - ”skrypt globalny”. Możliwe wartości, jeśli `eventsource` obiektu Action object jest ustawione na „zdarzenie wewnętrzne”: 0 - ”wyślij wiadomość”. Zachowanie właściwości: - *wymagane*
esc_period	string	Czas trwania kroku eskalacji w sekundach. Musi być większy niż 60 sekund. Akceptuje sekundy, jednostkę czasu z sufiksem lub makro użytkownika. Jeśli ustawiono 0 lub 0s, zostanie użyty domyślny okres eskalacji akcji. Domyślnie: 0s. Zachowanie właściwości: - *obsługiwane*, jeśli `eventsource` obiektu Action object jest ustawione na „zdarzenie utworzone przez wyzwalacz”, „zdarzenie wewnętrzne” lub „zdarzenie utworzone przy aktualizacji stanu usługi”
esc_step_from	integer	Krok, od którego ma się rozpocząć eskalacja. Domyślnie: 1. Zachowanie właściwości: - *obsługiwane*, jeśli `eventsource` obiektu Action object jest ustawione na „zdarzenie utworzone przez wyzwalacz”, „zdarzenie wewnętrzne” lub „zdarzenie utworzone przy aktualizacji stanu usługi”
esc_step_to	integer	Krok, na którym ma się zakończyć eskalacja. Domyślnie: 1. Zachowanie właściwości: - *obsługiwane*, jeśli `eventsource` obiektu Action object jest ustawione na „zdarzenie utworzone przez wyzwalacz”, „zdarzenie wewnętrzne” lub „zdarzenie utworzone przy aktualizacji stanu usługi”
evaltype	integer	Metoda oceny warunku operacji. Możliwe wartości: 0 - *(domyślnie)* And/Or; 1 - And; 2 - Or.

Właściwość	Typ	Opis
opcommand	object	Skrypt globalny do wykonania. Skrypt globalny musi mieć zdefiniowaną właściwość `scriptid`. Zachowanie właściwości: - *wymagane*, jeśli `operationtype` jest ustawione na „skrypt globalny”
opcommand_grp	array	Grupy hostów, na których mają być uruchamiane skrypty globalne. Grupy hostów muszą mieć zdefiniowaną właściwość `groupid`. Zachowanie właściwości: - *wymagane*, jeśli `operationtype` jest ustawione na „skrypt globalny”, a `opcommand_hst` nie jest ustawione
opcommand_hst	array	Host, na którym mają być uruchamiane skrypty globalne. Hosty muszą mieć zdefiniowaną właściwość `hostid`. Zachowanie właściwości: - *wymagane*, jeśli `operationtype` jest ustawione na „skrypt globalny”, a `opcommand_grp` nie jest ustawione
opconditions	array	Warunki operacji używane dla akcji wyzwalaczy. Obiekt warunku operacji jest opisany szczegółowo poniżej.
opgroup	array	Grupy hostów, do których mają zostać dodane hosty. Grupy hostów muszą mieć zdefiniowaną właściwość `groupid`. Zachowanie właściwości: - *wymagane*, jeśli `operationtype` jest ustawione na „dodaj do grupy hostów” lub „usuń z grupy hostów”
opmessage	object	Obiekt zawierający dane o wiadomości wysyłanej przez operację. Obiekt wiadomości operacji jest opisany szczegółowo poniżej. Zachowanie właściwości: - *wymagane*, jeśli `operationtype` jest ustawione na „wyślij wiadomość”
opmessage_grp	array	Grupy użytkowników, do których mają być wysyłane wiadomości. Grupy użytkowników muszą mieć zdefiniowaną właściwość `usrgrpid`. Zachowanie właściwości: - *wymagane*, jeśli `operationtype` jest ustawione na „wyślij wiadomość”, a `opmessage_usr` nie jest ustawione
opmessage_usr	array	Użytkownicy, do których mają być wysyłane wiadomości. Użytkownicy muszą mieć zdefiniowaną właściwość `userid`. Zachowanie właściwości: - *wymagane*, jeśli `operationtype` jest ustawione na „wyślij wiadomość”, a `opmessage_grp` nie jest ustawione
optemplate	array	Szablony do podłączenia do hostów. Szablony muszą mieć zdefiniowaną właściwość `templateid`. Zachowanie właściwości: - *wymagane*, jeśli `operationtype` jest ustawione na „podłącz szablon” lub „odłącz szablon”

Właściwość	Typ	Opis
opinventory	object	Tryb inwentaryzacji ustawiany dla hosta. Inwentaryzacja musi mieć zdefiniowaną właściwość `inventory_mode`. Zachowanie właściwości: - *wymagane*, jeśli `operationtype` jest ustawione na „ustaw tryb inwentaryzacji hosta”
optag	array	Tagi hosta do dodania lub usunięcia. Tagi muszą mieć zdefiniowaną właściwość `tag`. Właściwość `value` jest opcjonalna. Zachowanie właściwości: - *obsługiwane*, jeśli `operationtype` jest ustawione na „dodaj tagi hosta” lub „usuń tagi hosta”.

Wiadomość operacji akcji

Obiekt wiadomości operacji zawiera dane o wiadomości, która zostanie wysłana przez operację. Ma następujące właściwości.

Właściwość	Type	Opis
default_msg	integer	Czy użyć domyślnego tekstu i tematu wiadomości akcji. Możliwe wartości: 0 - użyj danych z operacji; 1 - *(domyślnie)* użyj danych z typu nośnika.
mediatypeid	ID	ID typu nośnika, który zostanie użyty do wysłania wiadomości. Zachowanie właściwości: - *obsługiwane*, jeśli `operationtype` obiektu Action operation object, Action recovery operation object lub Action update operation object jest ustawione na „send message”, albo jeśli `operationtype` obiektu Action update operation object jest ustawione na „notify all involved”
message	string	Tekst wiadomości operacji. Zachowanie właściwości: - *obsługiwane*, jeśli `default_msg` jest ustawione na „use the data from the operation”
subject	string	Temat wiadomości operacji. Zachowanie właściwości: - *obsługiwane*, jeśli `default_msg` jest ustawione na „use the data from the operation”

Warunek operacji akcji

Obiekt warunku operacji akcji definiuje warunek, który musi zostać spełniony, aby wykonać bieżącą operację. Ma następujące właściwości.

Property	Type	Description
conditiontype	integer	Typ warunku. Możliwe wartości: 14 - zdarzenie potwierdzone. Zachowanie właściwości: - *wymagane*

Property	Type	Description
value	string	Wartość do porównania. Zachowanie właściwości: - *wymagane*
operator	integer	Operator warunku. Możliwe wartości: 0 - *(domyślnie)* =

Dla każdego typu warunku operacji obsługiwane są następujące operatory i wartości.

Condition	Condition name	Supported operators	Expected value
14	Zdarzenie potwierdzone	=	Czy zdarzenie jest potwierdzone. Możliwe wartości: 0 - niepotwierdzone; 1 - potwierdzone.

Operacja odzyskiwania akcji

Obiekt operacji odzyskiwania akcji definiuje operację, która zostanie wykonana po rozwiązaniu problemu. Operacje odzyskiwania są możliwe **tylko** dla akcji wyzwalacza, wewnętrznych i usług. Ma następujące właściwości.

Właściwość	Typ	Opis
operationtype	integer	Typ operacji. Możliwe wartości, jeśli `eventsource` obiektu Action object jest ustawione na „zdarzenie utworzone przez wyzwalacz” lub „zdarzenie utworzone przy aktualizacji stanu usługi”: 0 - wyślij wiadomość; 1 - skrypt globalny; 11 - powiadom wszystkich zaangażowanych. Możliwe wartości, jeśli `eventsource` obiektu Action object jest ustawione na „zdarzenie wewnętrzne”: 0 - wyślij wiadomość; 11 - powiadom wszystkich zaangażowanych. Zachowanie właściwości: - *wymagane*
opcommand	object	Skrypt globalny do wykonania. Skrypt globalny musi mieć zdefiniowaną właściwość `scriptid`. Zachowanie właściwości: - *wymagane*, jeśli `operationtype` jest ustawione na „skrypt globalny”
opcommand_grp	array	Grupy hostów, na których mają być uruchamiane skrypty globalne. Grupy hostów muszą mieć zdefiniowaną właściwość `groupid`. Zachowanie właściwości: - *wymagane*, jeśli `eventsource` obiektu Action object jest ustawione na „zdarzenie utworzone przez wyzwalacz”, a `operationtype` jest ustawione na „skrypt globalny”, i `opcommand_hst` nie jest ustawione

Właściwość	Typ	Opis
opcommand_hst	array	Host, na którym mają być uruchamiane skrypty globalne. Hosty muszą mieć zdefiniowaną właściwość `hostid`. Zachowanie właściwości: - *wymagane*, jeśli `eventsource` obiektu Action object jest ustawione na „zdarzenie utworzone przez wyzwalacz”, a `operationtype` jest ustawione na „skrypt globalny”, i `opcommand_grp` nie jest ustawione
opmessage	object	Obiekt zawierający dane o wiadomości wysyłanej przez operację odzyskiwania. Obiekt wiadomości operacji jest opisany szczegółowo powyżej. Zachowanie właściwości: - *wymagane*, jeśli `operationtype` jest ustawione na „wyślij wiadomość”
opmessage_grp	array	Grupy użytkowników, do których mają być wysyłane wiadomości. Grupy użytkowników muszą mieć zdefiniowaną właściwość `usrgrpid`. Zachowanie właściwości: - *wymagane*, jeśli `operationtype` jest ustawione na „wyślij wiadomość” i `opmessage_usr` nie jest ustawione
opmessage_usr	array	Użytkownicy, do których mają być wysyłane wiadomości. Użytkownicy muszą mieć zdefiniowaną właściwość `userid`. Zachowanie właściwości: - *wymagane*, jeśli `operationtype` jest ustawione na „wyślij wiadomość” i `opmessage_grp` nie jest ustawione

Operacja aktualizacji akcji

Obiekt operacji aktualizacji akcji definiuje operację, która zostanie wykonana po zaktualizowaniu problemu (dodaniu komentarza, potwierdzeniu, zmianie ważności lub ręcznym zamknięciu). Operacje aktualizacji są możliwe **tylko** dla akcji wyzwalaczy i usług. Ma następujące właściwości.

Właściwość	Type	Opis
operationtype	integer	Typ operacji. Możliwe wartości: 0 - wyślij wiadomość; 1 - skrypt globalny; 12 - powiadom wszystkich zaangażowanych. Zachowanie właściwości: - *required*
opcommand	object	Skrypt globalny do wykonania. Skrypt globalny musi mieć zdefiniowaną właściwość `scriptid`. Zachowanie właściwości: - *required* jeśli `operationtype` jest ustawione na „skrypt globalny”

Właściwość	Type	Opis
opcommand_grp	array	Grupy hostów, na których mają być uruchamiane skrypty globalne. Grupy hostów muszą mieć zdefiniowaną właściwość `groupid`. Zachowanie właściwości: - *required* jeśli `eventsource` obiektu Action object jest ustawione na „zdarzenie utworzone przez wyzwalacz”, `operationtype` jest ustawione na „skrypt globalny”, a `opcommand_hst` nie jest ustawione
opcommand_hst	array	Host, na którym mają być uruchamiane skrypty globalne. Hosty muszą mieć zdefiniowaną właściwość `hostid`. Zachowanie właściwości: - *required* jeśli `eventsource` obiektu Action object jest ustawione na „zdarzenie utworzone przez wyzwalacz”, `operationtype` jest ustawione na „skrypt globalny”, a `opcommand_grp` nie jest ustawione
opmessage	object	Obiekt zawierający dane o wiadomości wysyłanej przez operację aktualizacji. Obiekt wiadomości operacji jest opisany szczegółowo powyżej.
opmessage_grp	array	Grupy użytkowników, do których mają być wysyłane wiadomości. Grupy użytkowników muszą mieć zdefiniowaną właściwość `usrgrpid`. Zachowanie właściwości: - *required* jeśli `operationtype` jest ustawione na „wyślij wiadomość”, a `opmessage_usr` nie jest ustawione
opmessage_usr	array	Użytkownicy, do których mają być wysyłane wiadomości. Użytkownicy muszą mieć zdefiniowaną właściwość `userid`. Zachowanie właściwości: - *required* jeśli `operationtype` jest ustawione na „wyślij wiadomość”, a `opmessage_grp` nie jest ustawione

Filtr akcji

Obiekt filtra akcji definiuje zestaw warunków, które muszą zostać spełnione, aby wykonać skonfigurowane operacje akcji. Ma następujące właściwości.

Właściwość	Typ	Opis
conditions	array	Zestaw warunków filtra używanych do filtrowania wyników. Warunki zostaną posortowane zgodnie z kolejnością ich występowania w formule. Zachowanie właściwości: - *wymagane*
evaltype	integer	Metoda obliczania warunku filtra. Możliwe wartości: 0 - And/Or; 1 - And; 2 - Or; 3 - Wyrażenie niestandardowe. Zachowanie właściwości: - *wymagane*

Właściwość	Typ	Opis
eval_formula	string	Wygenerowane wyrażenie, które będzie używane do obliczania warunków filtra. Wyrażenie zawiera identyfikatory odnoszące się do określonych warunków filtra przez ich `formulaid`. Wartość `eval_formula` jest równa wartości `formula` dla filtrów z wyrażeniem niestandardowym. Zachowanie właściwości: - *tylko do odczytu*
formula	string	Wyrażenie zdefiniowane przez użytkownika, używane do obliczania warunków filtrów z wyrażeniem niestandardowym. Wyrażenie musi zawierać identyfikatory odnoszące się do określonych warunków filtra przez ich `formulaid`. Identyfikatory użyte w wyrażeniu muszą dokładnie odpowiadać tym zdefiniowanym w warunkach filtra: żaden warunek nie może pozostać nieużyty ani pominięty. Zachowanie właściwości: - *wymagane*, jeśli `evaltype` jest ustawione na „custom expression”

Warunek filtra akcji

Obiekt warunku filtra akcji definiuje określony warunek, który musi zostać sprawdzony przed uruchomieniem operacji akcji.

Właściwość	Typ	Opis
conditiontype	integer	Typ warunku. Możliwe wartości, jeśli `eventsource` obiektu Action object jest ustawione na „zdarzenie utworzone przez wyzwalacz”: 0 - grupa hostów; 1 - host; 2 - wyzwalacz; 3 - nazwa zdarzenia; 4 - ważność wyzwalacza; 6 - okres czasu; 13 - szablon hosta; 16 - problem jest stłumiony; 25 - tag zdarzenia; 26 - wartość tagu zdarzenia. Możliwe wartości, jeśli `eventsource` obiektu Action object jest ustawione na „zdarzenie utworzone przez regułę wykrywania”: 7 - IP hosta; 8 - typ wykrytej usługi; 9 - port wykrytej usługi; 10 - status wykrywania; 11 - czas trwania działania lub niedostępności; 12 - odebrana wartość; 18 - reguła wykrywania; 19 - sprawdzenie wykrywania; 20 - proxy; 21 - obiekt wykrywania. Możliwe wartości, jeśli `eventsource` obiektu Action object jest ustawione na „zdarzenie utworzone przez aktywną autorejestrację agent”: 20 - proxy; 22 - nazwa hosta; 24 - metadane hosta. Możliwe wartości, jeśli `eventsource` obiektu Action object jest ustawione na „zdarzenie wewnętrzne”: 0 - grupa hostów; 1 - host; 13 - szablon hosta; 23 - typ zdarzenia; 25 - tag zdarzenia; 26 - wartość tagu zdarzenia. Możliwe wartości, jeśli `eventsource` obiektu Action object jest ustawione na „zdarzenie utworzone przy aktualizacji statusu usługi”: 25 - tag zdarzenia; 26 - wartość tagu zdarzenia; 27 - usługa; 28 - nazwa usługi. Zachowanie właściwości: - *wymagane*
value	string	Wartość do porównania. Zachowanie właściwości: - *wymagane*

Właściwość	Typ	Opis
value2	string	Dodatkowa wartość do porównania. Zachowanie właściwości: - *wymagane*, jeśli `eventsource` obiektu Action object jest ustawione na „zdarzenie utworzone przez wyzwalacz”, `conditiontype` jest ustawione na dowolną możliwą wartość dla akcji wyzwalaczy, a typ warunku (patrz niżej) to „26” - *wymagane*, jeśli `eventsource` obiektu Action object jest ustawione na „zdarzenie wewnętrzne”, `conditiontype` jest ustawione na dowolną możliwą wartość dla akcji wewnętrznych, a typ warunku (patrz niżej) to „26” - *wymagane*, jeśli `eventsource` obiektu Action object jest ustawione na „zdarzenie utworzone przy aktualizacji statusu usługi”, `conditiontype` jest ustawione na dowolną możliwą wartość dla akcji usług, a typ warunku (patrz niżej) to „26”
formulaid	string	Dowolny unikalny identyfikator używany do odwoływania się do warunku z wyrażenia niestandardowego. Może zawierać tylko wielkie litery. Identyfikator musi zostać zdefiniowany przez użytkownika podczas modyfikowania warunków filtra, ale zostanie wygenerowany ponownie przy późniejszym żądaniu ich pobrania.
operator	integer	Operator warunku. Możliwe wartości: 0 - *(domyślnie)* równa się; 1 - nie równa się; 2 - zawiera; 3 - nie zawiera; 4 - w; 5 - jest większe lub równe; 6 - jest mniejsze lub równe; 7 - nie w; 8 - pasuje; 9 - nie pasuje; 10 - Tak; 11 - Nie.

Note:
Aby lepiej zrozumieć, jak używać filtrów z różnymi typami wyrażeń, zobacz przykłady na stronach metod action.get i action.create.

Dla każdego typu warunku obsługiwane są następujące operatory i wartości.

Warunek	Nazwa warunku	Obsługiwane operatory	Oczekiwana wartość
0	Grupa hostów	równa się, nie równa się	ID grupy hostów.
1	Host	równa się, nie równa się	ID hosta.
2	Wyzwalacz	równa się, nie równa się	ID wyzwalacza.
3	Nazwa zdarzenia	zawiera, nie zawiera	Nazwa zdarzenia.
4	Ważność wyzwalacza	równa się, nie równa się, jest większe lub równe, jest mniejsze lub równe	Ważność wyzwalacza. Listę obsługiwanych ważności wyzwalacza można znaleźć we właściwości trigger `severity` property.

Warunek	Nazwa warunku	Obsługiwane operatory	Oczekiwana wartość
5	Wartość wyzwalacza	równa się	Wartość wyzwalacza. Listę obsługiwanych wartości wyzwalacza można znaleźć we właściwości trigger `value` property.
6	Okres czasu	w, nie w	Czas wystąpienia zdarzenia jako okres czasu.
7	IP hosta	równa się, nie równa się	Jeden lub kilka zakresów IP do sprawdzenia, oddzielonych przecinkami. Więcej informacji o obsługiwanych formatach zakresów IP można znaleźć w sekcji konfiguracja wykrywania sieci.
8	Typ wykrytej usługi	równa się, nie równa się	Typ wykrytej usługi. Typ usługi odpowiada typowi sprawdzenia wykrywania użytego do wykrycia usługi. Listę obsługiwanych typów można znaleźć we właściwości discovery check `type` property.
9	Port wykrytej usługi	równa się, nie równa się	Jeden lub kilka zakresów portów, oddzielonych przecinkami.
10	Status wykrywania	równa się	Status wykrytego obiektu. Możliwe wartości: 0 - host lub usługa działa; 1 - host lub usługa nie działa; 2 - host lub usługa wykryta; 3 - host lub usługa utracona.
11	Czas trwania działania lub niedostępności	jest większe lub równe, jest mniejsze lub równe	Czas w sekundach określający, jak długo wykryty obiekt znajduje się w bieżącym stanie.
12	Odebrane wartości	równa się, nie równa się, jest większe lub równe, jest mniejsze lub równe, zawiera, nie zawiera	Wartość zwrócona podczas wykonywania sprawdzenia wykrywania Zabbix agent, SNMPv1, SNMPv2 lub SNMPv3.
13	Szablon hosta	równa się, nie równa się	ID podłączonego szablonu.
16	Problem jest stłumiony	Tak, Nie	Wartość nie jest wymagana: użycie operatora „Tak” oznacza, że problem musi być stłumiony, „Nie” — niestłumiony.
18	Reguła wykrywania	równa się, nie równa się	ID reguły wykrywania.
19	Sprawdzenie wykrywania	równa się, nie równa się	ID sprawdzenia wykrywania.
20	Proxy	równa się, nie równa się	ID proxy.
21	Obiekt wykrywania	równa się	Typ obiektu, który wywołał zdarzenie wykrywania. Możliwe wartości: 1 - wykryty host; 2 - wykryta usługa.
22	Nazwa hosta	zawiera, nie zawiera, pasuje, nie pasuje	Nazwa hosta. W warunkach autorejestracji dla operatorów *pasuje* i *nie pasuje* obsługiwane jest użycie wyrażenia regularnego.
23	Typ zdarzenia	równa się	Określone zdarzenie wewnętrzne. Możliwe wartości: 0 - pozycja w stanie „nieobsługiwane”; 1 - pozycja w stanie „normalne”; 2 - reguła LLD w stanie „nieobsługiwane”; 3 - reguła LLD w stanie „normalne”; 4 - wyzwalacz w stanie „nieznane”; 5 - wyzwalacz w stanie „normalne”.

Warunek	Nazwa warunku	Obsługiwane operatory	Oczekiwana wartość
24	Metadane hosta	zawiera, nie zawiera, pasuje, nie pasuje	Metadane automatycznie zarejestrowanego hosta. Użycie wyrażenia regularnego jest obsługiwane dla operatorów *pasuje* i *nie pasuje*.
25	Tag	równa się, nie równa się, zawiera, nie zawiera	Tag zdarzenia.
26	Wartość tagu	równa się, nie równa się, zawiera, nie zawiera	Wartość tagu zdarzenia.
27	Usługa	równa się, nie równa się	ID usługi.
28	Nazwa usługi	równa się, nie równa się	Nazwa usługi.

action.create

Opis

`object action.create(object/array actions)`

Ta metoda umożliwia tworzenie nowych akcji.

Note:
Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach ról użytkowników. Więcej informacji znajduje się w sekcji Role użytkowników.

Parametry

`(object/array)` Akcje do utworzenia.

Oprócz standardowych właściwości akcji, metoda akceptuje następujące parametry.

Parametr	Typ	Opis
filter	object	Obiekt filtra akcji dla akcji.
operations	array	Operacje akcji do utworzenia dla akcji.
recovery_operations	array	Operacje odzyskiwania akcji do utworzenia dla akcji.
update_operations	array	Operacje aktualizacji akcji do utworzenia dla akcji.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory ID utworzonych akcji we właściwości `actionids`. Kolejność zwracanych identyfikatorów ID jest zgodna z kolejnością przekazanych akcji.

Przykłady

Utwórz akcję wyzwalacza

Utwórz akcję wyzwalacza, która rozpocznie się, gdy wyzwalacz (zawierający słowo „memory” w nazwie) z hosta „10084” przejdzie do stanu PROBLEM. Akcja będzie miała 4 skonfigurowane operacje. Pierwsza, wykonywana natychmiast operacja wyśle wiadomość do wszystkich użytkowników z grupy użytkowników „7” za pośrednictwem typu mediów „1”. Jeśli zdarzenie nie zostanie rozwiązane w ciągu 30 minut, druga operacja uruchomi skrypt „5” (skrypt o zakresie „Action operation”) na wszystkich hostach z grupy „2”. Jeśli zdarzenie zostanie rozwiązane, operacja odzyskiwania powiadomi wszystkich użytkowników, którzy otrzymali jakiekolwiek wiadomości dotyczące problemu. Jeśli zdarzenie zostanie zaktualizowane, operacja potwierdzenia/aktualizacji powiadomi (z niestandardowym tematem i wiadomością) wszystkich użytkowników, którzy otrzymali jakiekolwiek wiadomości dotyczące problemu.

Żądanie:

```
{
    "jsonrpc": "2.0",
```

```
    "method": "action.create",
    "params": {
        "name": "Trigger action",
        "eventsource": 0,
        "esc_period": "30m",
        "filter": {
            "evaltype": 0,
            "conditions": [
                {
                    "conditiontype": 1,
                    "operator": 0,
                    "value": "10084"
                },
                {
                    "conditiontype": 3,
                    "operator": 2,
                    "value": "memory"
                }
            ]
        },
        "operations": [
            {
                "operationtype": 0,
                "esc_step_from": 1,
                "esc_step_to": 1,
                "opmessage_grp": [
                    {
                        "usrgrpid": "7"
                    }
                ],
                "opmessage": {
                    "default_msg": 1,
                    "mediatypeid": "1"
                }
            },
            {
                "operationtype": 1,
                "esc_step_from": 2,
                "esc_step_to": 2,
                "opconditions": [
                    {
                        "conditiontype": 14,
                        "operator": 0,
                        "value": "0"
                    }
                ],
                "opcommand_grp": [
                    {
                        "groupid": "2"
                    }
                ],
                "opcommand": {
                    "scriptid": "5"
                }
            }
        ],
        "recovery_operations": [
            {
                "operationtype": "11",
                "opmessage": {
                    "default_msg": 1
                }
```

```
            }
        ],
        "update_operations": [
            {
                "operationtype": "12",
                "opmessage": {
                    "default_msg": 0,
                    "message": "Custom update operation message body",
                    "subject": "Custom update operation message subject"
                }
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "actionids": [
            "17"
        ]
    },
    "id": 1
}
```

Utwórz akcję wykrywania

Utwórz akcję wykrywania, która połączy szablon „10001” z wykrytymi hostami.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "action.create",
    "params": {
        "name": "Discovery action",
        "eventsource": 1,
        "filter": {
            "evaltype": 0,
            "conditions": [
                {
                    "conditiontype": 21,
                    "operator": 0,
                    "value": "1"
                },
                {
                    "conditiontype": 10,
                    "operator": 0,
                    "value": "2"
                }
            ]
        },
        "operations": [
            {
                "operationtype": 6,
                "optemplate": [
                    {
                        "templateid": "10001"
                    }
                ]
            }
        ]
```

```
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "actionids": [
            "18"
        ]
    },
    "id": 1
}
```

Używanie niestandardowego filtra wyrażeń

Utwórz akcję wyzwalacza, która używa niestandardowego wyrażenia - „A and (B or C)” - do oceniania warunków akcji. Gdy wyzwalacz o ważności wyższej lub równej „Warning” z hosta „10084” lub hosta „10106” przejdzie do stanu PROBLEM, akcja wyśle wiadomość do wszystkich użytkowników z grupy użytkowników „7” za pośrednictwem typu nośnika „1”. Identyfikatory formuły „A”, „B” i „C” zostały wybrane arbitralnie.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "action.create",
    "params": {
        "name": "Trigger action",
        "eventsource": 0,
        "esc_period": "15m",
        "filter": {
            "evaltype": 3,
            "formula": "A and (B or C)",
            "conditions": [
                {
                    "conditiontype": 4,
                    "operator": 5,
                    "value": "2",
                    "formulaid": "A"
                },
                {
                    "conditiontype": 1,
                    "operator": 0,
                    "value": "10084",
                    "formulaid": "B"
                },
                {
                    "conditiontype": 1,
                    "operator": 0,
                    "value": "10106",
                    "formulaid": "C"
                }
            ]
        },
        "operations": [
            {
                "operationtype": 0,
                "esc_step_from": 1,
                "esc_step_to": 1,
                "opmessage_grp": [
                    {
                        "usrgrpid": "7"
                    }
```

```
                ],
                "opmessage": {
                    "default_msg": 1,
                    "mediatypeid": "1"
                }
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "actionids": [
            "18"
        ]
    },
    "id": 1
}
```

Utwórz regułę autorejestracji agent

Utwórz akcję autorejestracji, która dodaje host do grupy hostów „2”, gdy nazwa hosta zawiera „SRV” lub metadane zawierają „AlmaLinux”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "action.create",
    "params": {
        "name": "Register Linux servers",
        "eventsource": "2",
        "filter": {
            "evaltype": "2",
            "conditions": [
                {
                    "conditiontype": "22",
                    "operator": "2",
                    "value": "SRV"
                },
                {
                    "conditiontype": "24",
                    "operator": "2",
                    "value": "AlmaLinux"
                }
            ]
        },
        "operations": [
            {
                "operationtype": "4",
                "opgroup": [
                    {
                        "groupid": "2"
                    }
                ]
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "actionids": [
            19
        ]
    },
    "id": 1
}
```

Utwórz regułę autorejestracji agent z tagami hosta

Utwórz akcję autorejestracji, która dodaje host do grupy hostów „2” oraz dodaje dwa tagi hosta.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "action.create",
    "params": {
        "name": "Register Linux servers with tags",
        "eventsource": "2",
        "operations": [
            {
                "operationtype": "4",
                "opgroup": [
                    {
                        "groupid": "2"
                    }
                ]
            },
            {
                "operationtype": "13",
                "optag": [
                    {
                        "tag": "location",
                        "value": "office"
                    },
                    {
                        "tag": "city",
                        "value": "Riga"
                    }
                ]
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "actionids": [
            20
        ]
    },
    "id": 1
}
```

Zobacz także

- Filtr akcji
- Operacja akcji
- Skrypt

Źródło

CAction::create() w *ui/include/classes/api/services/CAction.php*.

action.delete

Opis

`object action.delete(array actionIds)`

Ta metoda pozwala na usuwanie akcji.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkowników typu *Admin* i *Super admin*. Uprawnienia do wywoływania metody można odebrać w ustawieniach roli użytkownika. Zobacz Role użytkownika po więcej informacji.

Parametry

`(array)` identyfikatory ID akcji do usunięcia.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory ID usuniętych akcji we właściwości `actionids`.

Przykłady

Usuń wiele akcji

Usuń dwie akcje.

Zapytanie:

```
{
"jsonrpc": "2.0",
"method": "action.delete",
"params": [
"17",
"18"
],
"id": 1
}
```

Odpowiedź:

```
{
"jsonrpc": "2.0",
"result": {
"actionids": [
"17",
"18"
]
},
"id": 1
}
```

Źródło

CAction::delete() w *ui/include/classes/api/services/CAction.php*.

action.get

Description

`integer/array action.get(object parameters)`

Metoda pozwala na pobranie akcji zgodnie z podanymi parametrami.

Note:
Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywoływania metody można odebrać w ustawieniach roli użytkownika. Zobacz Role użytkownika po więcej informacji.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
actionids	ID/array	Zwraca tylko akcje o podanych ID.
groupids	ID/array	Zwraca tylko akcje, które używają podanych grup hostów w warunkach akcji.
hostids	ID/array	Zwraca tylko akcje, które używają podanych hostów w warunkach akcji.
triggerids	ID/array	Zwraca tylko akcje, które używają podanych wyzwalaczy w warunkach akcji.
mediatypeids	ID/array	Zwraca tylko akcje, które używają podanych typów mediów do wysyłania wiadomości.
usrgrpids	ID/array	Zwraca tylko akcje, które są skonfigurowane do wysyłania wiadomości do podanych grup użytkowników.
userids	ID/array	Zwraca tylko akcje, które są skonfigurowane do wysyłania wiadomości do podanych użytkowników.
scriptids	ID/array	Zwraca tylko akcje, które są skonfigurowane do uruchamiania podanych skryptów.
selectFilter	query	Zwraca właściwość `filter` z filtrem warunków akcji.
selectOperations	query	Zwraca właściwość `operations` z operacjami akcji.
selectRecoveryOperations	query	Zwraca właściwość `recovery_operations` z operacjami odzyskiwania akcji.
selectUpdateOperations	query	Zwraca właściwość `update_operations` z operacjami aktualizacji akcji.
sortfield	string/array	Sortuje wynik według podanych właściwości. Możliwe wartości: `actionid`, `name`, `status`.
countOutput	boolean	Te parametry są opisane w komentarzu referencyjnym.
excludeSearch	boolean	
filter	object	
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca jedną z opcji:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli parametr `countOutput` został wykorzystany.

Przykłady

Pobieranie akcji wyzwalaczy

Pobierz wszystkie skonfigurowane akcje wyzwalaczy wraz z warunkami akcji i operacjami.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "action.get",
    "params": {
```

```
        "output": "extend",
        "selectOperations": "extend",
        "selectRecoveryOperations": "extend",
        "selectUpdateOperations": "extend",
        "selectFilter": "extend",
        "filter": {
            "eventsource": 0
        }
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "actionid": "3",
            "name": "Zgłaszanie problemów administratorom Zabbix",
            "eventsource": "0",
            "status": "1",
            "esc_period": "1h",
            "pause_suppressed": "1",
            "filter": {
                "evaltype": "0",
                "formula": "",
                "conditions": [],
                "eval_formula": ""
            },
            "operations": [
                {
                    "operationid": "3",
                    "actionid": "3",
                    "operationtype": "0",
                    "esc_period": "0",
                    "esc_step_from": "1",
                    "esc_step_to": "1",
                    "evaltype": "0",
                    "opconditions": [],
                    "opmessage": [
                        {
                            "default_msg": "1",
                            "subject": "",
                            "message": "",
                            "mediatypeid" => "0"
                        }
                    ],
                    "opmessage_grp": [
                        {
                            "usrgrpid": "7"
                        }
                    ]
                }
            ],
            "recovery_operations": [
                {
                    "operationid": "7",
                    "actionid": "3",
                    "operationtype": "11",
                    "evaltype": "0",
                    "opconditions": [],
                    "opmessage": {
```

```
                        "default_msg": "0",
                        "subject": "{TRIGGER.STATUS}: {TRIGGER.NAME}",
                        "message": "Wyzwalacz: {TRIGGER.NAME}\r\nStan wyzwalacza: {TRIGGER.STATUS}\r\nPozi
                        "mediatypeid": "0"
                    }
                }
            ],
            "update_operations": [
                {
                    "operationid": "31",
                    "operationtype": "12",
                    "evaltype": "0",
                    "opmessage": {
                        "default_msg": "1",
                        "subject": "",
                        "message": "",
                        "mediatypeid": "0"
                    }
                },
                {
                    "operationid": "32",
                    "operationtype": "0",
                    "evaltype": "0",
                    "opmessage": {
                        "default_msg": "0",
                        "subject": "Zaktualizowano: {TRIGGER.NAME}",
                        "message": "{USER.FULLNAME} zaktualizował problem dnia {EVENT.UPDATE.DATE} o {EVEN
                        "mediatypeid": "1"
                    },
                    "opmessage_grp": [
                        {
                            "usrgrpid": "7"
                        }
                    ],
                    "opmessage_usr": []
                },
                {
                    "operationid": "33",
                    "operationtype": "1",
                    "evaltype": "0",
                    "opcommand": {
                        "scriptid": "3"
                    },
                    "opcommand_hst": [
                        {
                            "hostid": "10084"
                        }
                    ],
                    "opcommand_grp": []
                }
            ]
        }
    ],
    "id": 1
}
```


Pobierz akcje wykrywania

Pobierz wszystkie skonfigurowane akcje wykrywania wraz z warunkami i operacjami akcji. Filtr używa typu oceny „and”, więc właściwość `formula` jest pusta, a `eval_formula` jest generowana automatycznie.

Zapytanie:

```
{
  "jsonrpc": "2.0",
  "method": "action.get",
  "params": {
    "output": "extend",
    "selectOperations": "extend",
    "selectFilter": "extend",
    "filter": {
      "eventsource": 1
    }
  },
  "id": 1
}
```

Odpowiedź:

```
{
  "jsonrpc": "2.0",
  "result": [
    {
      "actionid": "2",
      "name": "Auto discovery. Linux servers.",
      "eventsource": "1",
      "status": "1",
      "esc_period": "0s",
      "pause_suppressed": "1",
      "filter": {
        "evaltype": "0",
        "formula": "",
        "conditions": [
          {
            "conditiontype": "10",
            "operator": "0",
            "value": "0",
            "value2": "",
            "formulaid": "B"
          },
          {
            "conditiontype": "8",
            "operator": "0",
            "value": "9",
            "value2": "",
            "formulaid": "C"
          },
          {
            "conditiontype": "12",
            "operator": "2",
            "value": "Linux",
            "value2": "",
            "formulaid": "A"
          }
        ],
        "eval_formula": "A and B and C"
      },
      "operations": [
        {
          "operationid": "1",
          "actionid": "2",
          "operationtype": "6",
          "esc_period": "0s",
          "esc_step_from": "1",
          "esc_step_to": "1",
          "evaltype": "0",
```

```
          "opconditions": [],
          "optemplate": [
            {
              "templateid": "10001"
            }
          ]
        },
        {
          "operationid": "2",
          "actionid": "2",
          "operationtype": "4",
          "esc_period": "0s",
          "esc_step_from": "1",
          "esc_step_to": "1",
          "evaltype": "0",
          "opconditions": [],
          "opgroup": [
            {
              "groupid": "2"
            }
          ]
        }
      ]
    }
  ],
  "id": 1
}
```


Zobacz także

- Filtr akcji
- Operacja akcji

Źródło

CAction::get() w *ui/include/classes/api/services/CAction.php*.

action.update

Description

`object action.update(object/array actions)`

Ta metoda pozwala na aktualizowanie istniejących akcji.

> **Note:**
> Ta metoda jest dostępna wyłącznie użytkownikom typu *Admin* i *Super admin*. Uprawnienia do wywołania metody można odebrać w ustawieniach roli. Zobacz Role użytkownika po więcej informacji.

Parametry

`(object/array)` Właściwości akcji do zaktualizowania.

Właściwość `actionid` musi być zdefiniowana dla każdej akcji, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko przekazane właściwości, wszystkie pozostałe pozostaną bez zmian.

Oprócz standardowych właściwości akcji, metoda akceptuje następujące parametry.

Parametr	Typ	Opis
filter	object	Obiekt filtra akcji, który zastąpi bieżący filtr.
operations	array	Operacje akcji, które zastąpią istniejące operacje.

Parametr	Typ	Opis
recovery_operations	array	Operacje odzyskiwania akcji, które zastąpią istniejące operacje odzyskiwania. Zachowanie parametru: - *obsługiwane*, jeśli `eventsource` obiektu akcji jest ustawione na „zdarzenie utworzone przez wyzwalacz”, „zdarzenie wewnętrzne” lub „zdarzenie utworzone przy aktualizacji stanu usługi”
update_operations	array	Operacje aktualizacji akcji, które zastąpią istniejące operacje aktualizacji. Zachowanie parametru: - *obsługiwane*, jeśli `eventsource` obiektu akcji jest ustawione na „zdarzenie utworzone przez wyzwalacz” lub „zdarzenie utworzone przy aktualizacji stanu usługi”

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory ID zaktualizowanych akcji we właściwości `actionids`.

Przykłady

Wyłącz akcję

Wyłącz akcję, to znaczy ustaw jej status na „1”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "action.update",
    "params": {
        "actionid": "2",
        "status": "1"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "actionids": [
            "2"
        ]
    },
    "id": 1
}
```

Zobacz także

- Filtr akcji
- Operacja akcji

Źródło

CAction::update() in *ui/include/classes/api/services/CAction.php*.

Alarm

Ta klasa jest przeznaczona do pracy z alarmami.

Odwołania do obiektu:

- Alert

Dostępne metody:

- alert.get - pobieranie alarmów

Alert obiektu

Następujące obiekty są bezpośrednio powiązane z API `alert`.

Alert

Note:
Alerty są tworzone przez serwer Zabbix i nie mogą być modyfikowane przez API.

Obiekt alertu zawiera informacje o tym, czy określone operacje akcji zostały wykonane pomyślnie. Ma następujące właściwości.

Właściwość	Typ	Opis
alertid	ID	ID alertu.
actionid	ID	ID akcji, która wygenerowała alert.
alerttype	integer	Typ alertu. Możliwe wartości: 0 - wiadomość; 1 - zdalne polecenie.
clock	timestamp	Czas wygenerowania alertu.
error	string	Tekst błędu, jeśli wystąpiły problemy z wysłaniem wiadomości lub uruchomieniem polecenia.
esc_step	integer	Krok eskalacji akcji, podczas którego został wygenerowany alert.
eventid	ID	ID zdarzenia, które wyzwoliło akcję.
mediatypeid	ID	ID typu nośnika, który został użyty do wysłania wiadomości.
message	text	Treść wiadomości. Zachowanie właściwości: - *obsługiwane* jeśli `alerttype` jest ustawione na ”message”
retries	integer	Liczba prób wysłania wiadomości przez Zabbix.
sendto	string	Adres, nazwa użytkownika lub inny identyfikator odbiorcy. Zachowanie właściwości: - *obsługiwane* jeśli `alerttype` jest ustawione na ”message”
status	integer	Status wskazujący, czy operacja akcji została wykonana pomyślnie. Możliwe wartości, jeśli `alerttype` jest ustawione na ”message”: 0 - wiadomość nie została wysłana; 1 - wiadomość została wysłana; 2 - niepowodzenie po określonej liczbie prób; 3 - nowy alert nie został jeszcze przetworzony przez menedżera alertów. Możliwe wartości, jeśli `alerttype` jest ustawione na ”remote command”: 0 - polecenie nie zostało uruchomione; 1 - polecenie zostało uruchomione; 2 - podjęto próbę uruchomienia polecenia na Zabbix agent, ale był niedostępny.
subject	string	Temat wiadomości. Zachowanie właściwości: - *obsługiwane* jeśli `alerttype` jest ustawione na ”message”
userid	ID	ID użytkownika, do którego wysłano wiadomość.
p_eventid	ID	ID zdarzenia problemu, które wygenerowało alert.
acknowledgeid	ID	ID potwierdzenia, które wygenerowało alert.

alert.get

Opis

`integer/array alert.get(object parameters)`

Metoda pozwala na pobieranie alertów zgodnie z podanymi parametrami.

> **Note:**
> Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywołania metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w User roles.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
alertids	ID/array	Zwraca tylko alerty o podanych identyfikatorach.
actionids	ID/array	Zwraca tylko alerty wygenerowane przez podane akcje.
eventids	ID/array	Zwraca tylko alerty wygenerowane przez podane zdarzenia.
groupids	ID/array	Zwraca tylko alerty wygenerowane przez obiekty z podanych grup hostów.
hostids	ID/array	Zwraca tylko alerty wygenerowane przez obiekty z podanych hostów.
mediatypeids	ID/array	Zwraca tylko alerty wiadomości, w których użyto podanych typów mediów.
objectids	ID/array	Zwraca tylko alerty wygenerowane przez podane obiekty
userids	ID/array	Zwraca tylko alerty wiadomości, które zostały wysłane do podanych użytkowników.
eventobject	integer	Zwraca tylko alerty wygenerowane przez zdarzenia powiązane z obiektami podanego typu. Listę obsługiwanych typów obiektów można znaleźć w `object` zdarzenia. Domyślnie: 0 - wyzwalacz.
eventsource	integer	Zwraca tylko alerty wygenerowane przez zdarzenia podanego typu. Listę obsługiwanych typów zdarzeń można znaleźć w `source` zdarzenia. Domyślnie: 0 - zdarzenia wyzwalacza.
time_from	timestamp	Zwraca tylko alerty wygenerowane po podanym czasie.
time_till	timestamp	Zwraca tylko alerty wygenerowane przed podanym czasem.
selectHosts	query	Zwraca właściwość `hosts` z danymi hostów, które wyzwoliły operację akcji.
selectMediatypes	query	Zwraca właściwość `mediatypes` z tablicą typów mediów użytych dla alertu wiadomości. Ograniczenia zależne od typu użytkownika można znaleźć w `mediatype.get`.
selectUsers	query	Zwraca właściwość `users` z tablicą użytkowników, do których była adresowana wiadomość. Ograniczenia zależne od typu użytkownika można znaleźć w `user.get`.
sortfield	string/array	Sortuje wynik według podanych właściwości. Możliwe wartości: `alertid`, `clock`, `eventid`, `mediatypeid`, `sendto`, `status`.
countOutput	boolean	Parametry te są opisane w komentarzu referencyjnym.
editable	boolean	
excludeSearch	boolean	
filter	object	
limit	integer	

Parametr	Typ	Opis
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów albo;
- liczbę zwracanych obiektów, jeśli parametr `countOutput` został użyty.

Przykłady

Pobieranie alertów według ID akcji

Pobierz wszystkie alerty wygenerowane przez akcję „3”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "alert.get",
    "params": {
        "output": "extend",
        "actionids": "3"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "alertid": "1",
            "actionid": "3",
            "eventid": "21243",
            "userid": "1",
            "clock": "1362128008",
            "mediatypeid": "1",
            "sendto": "support@company.com",
            "subject": "PROBLEM: Zabbix agent na serwerze Linux jest niedostępny przez 5 minut: ",
            "message": "Wyzwalacz: Zabbix agent na serwerze Linux jest niedostępny przez 5 minut: \nStan w
            "status": "0",
            "retries": "3",
            "error": "",
            "esc_step": "1",
            "alerttype": "0",
            "p_eventid": "0",
            "acknowledgeid": "0"
        }
    ],
    "id": 1
}
```

Zobacz także

- Host
- Typ nośnika
- Użytkownik

Źródło

CAlert::get() in *ui/include/classes/api/services/CAlert.php*.

API info

Klasa jest przeznaczona do pobierania metainformacji o interfejsie API.

Dostępne metody:

- apiinfo.version - pobieranie wersji API Zabbix

apiinfo.version

Opis

`string apiinfo.version(array)`

Ta metoda pozwala na pobranie wersji API Zabbix.

> **Attention:**
> Ta metoda jest dostępna tylko dla nieuwierzytelnionych użytkowników.

Parametry

`(array)` Metoda akceptuje pustą tablicę.

Zwracane wartości

`(string)` Zwraca wersję API Zabbix.

> **Note:**
> Zaczynając od wersji Zabbix 2.0.4, wersja API jest taka sama jak wersja Zabbix.

Przykłady

Pobieranie wersji API

Pobierz wersję API Zabbix.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "apiinfo.version",
    "params": [],
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": "8.0.0",
    "id": 1
}
```

Źródło

CAPIInfo::version() in *ui/include/classes/api/services/CAPIInfo.php*.

Autorejestracja

Ta klasa jest przeznaczona do pracy z autorejestracją.

Odniesienia do obiektów:

- Autoregistration

Dostępne metody:

- autoregistration.get - pobierz autorejestrację
- autoregistration.update - aktualizuj autorejestrację

Obiekt Autorejestracja

Następujące obiekty są bezpośrednio powiązane z API `autoregistration`.

Autorejestracja

Obiekt autorejestracji ma następujące właściwości.

Właściwość	Type	Opis
tls_accept	integer	Typ dozwolonych połączeń przychodzących dla autorejestracji. Możliwe wartości: 1 - zezwalaj na połączenia nieszyfrowane; 2 - zezwalaj na TLS z PSK; 3 - zezwalaj zarówno na połączenia nieszyfrowane, jak i TLS z PSK.
tls_psk_identity	string	Tożsamość PSK; musi być sparowana tylko z jednym PSK (w obrębie autoregistration, hosts i proxies). Nie umieszczaj poufnych informacji w tożsamości PSK, ponieważ jest ona przesyłana przez sieć bez szyfrowania, aby poinformować odbiorcę, którego PSK należy użyć. Zachowanie właściwości: - *tylko do zapisu*
tls_psk	string	Klucz współdzielony (PSK); musi mieć co najmniej 32 cyfry szesnastkowe. Zachowanie właściwości: - *tylko do zapisu*

autoregistration.get

Opis

`object autoregistration.get(object parameters)`

Ta metoda pozwala na pobranie obiektu rejestracji automatycznej według podanych parametrów.

Note:
Ta metoda jest dostępna tylko dla użytkownika typu *Super admin*. Uprawnienia do wywoływania metody można odebrać w ustawieniach roli użytkownika. Zobacz Role użytkownika po więcej informacji.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje tylko jeden parametr.

Parametr	Typ	Opis
output	query	Ten parametr jest opisany w komentarzu referencyjnym.

Zwracane wartości

`(object)` Zwraca obiekt rejestracji automatycznej.

Przykład

Zapytanie:

```
{
  "jsonrpc": "2.0",
  "method": "autoregistration.get",
  "params": {
    "output": "extend"
  },
  "id": 1
}
```

Odpowiedź:

```
{
  "jsonrpc": "2.0",
  "result": {
    "tls_accept": "3"
  },
  "id": 1
}
```

Źródło

CAutoregistration::get() w *ui/include/classes/api/services/CAutoregistration.php*.

autoregistration.update

Opis

`object autoregistration.update(object autoregistration)`

Ta metoda pozwala na aktualizację obiektu autorejestracji

Note:
Ta metoda jest dostępna tylko dla użytkownika typu *Super admin*. Uprawnienia do wywoływania metody można odebrać w ustawieniach roli użytkownika. Zobacz Role użytkownika po więcej informacji.

Parametry

`(object)` Właściwości rejestracji automatycznej do aktualizacji.

Zwracane wartości

`(boolean )` Zwraca wartość logiczną true jako wynik po udanej aktualizacji.

Przykłady

Zapytanie:

```
{
    "jsonrpc": "2.0",
    "method": "autoregistration.update",
    "params": {
        "tls_accept": "3",
        "tls_psk_identity": "PSK 001",
        "tls_psk": "11111595725ac58dd977beef14b97461a7c1045b9a1c923453302c5473193478"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": true,
    "id": 1
}
```

Źródło

CAutoregistration::update() w *ui/include/classes/api/services/CAutoregistration.php*.

Connector

Ta klasa jest przeznaczona do pracy z connectorami.

Odwołania do obiektów:

- Connector
- Filtr tagów

Dostępne metody:

- connector.create - tworzenie nowych connectorów
- connector.delete - usuwanie connectorów
- connector.get - pobieranie connectorów
- connector.update - aktualizacja connectorów

Obiekt łącznika

Następujące obiekty są bezpośrednio powiązane z API `connector`.

Connector

Obiekt connector ma następujące właściwości.

Property	Type	Description
connectorid	ID	ID connectora. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji
name	string	Nazwa connectora. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
url	string	Adres URL punktu końcowego, czyli adres URL odbiorcy. Makra użytkownika są obsługiwane. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
protocol	integer	Protokół komunikacji. Możliwe wartości: 0 - *(domyślnie)* Zabbix Streaming Protocol v1.0.
data_type	integer	Typ danych. Możliwe wartości: 0 - *(domyślnie)* Wartości pozycji; 1 - Zdarzenia.
item_value_type	integer	Suma typów wartości pozycji do wysłania. Możliwe wartości: 1 - Numeryczny (float); 2 - Znakowy; 4 - Log; 8 - Numeryczny (unsigned); 16 - Tekst; 32 - Binarny; 64 - JSON. Domyślnie: 31 - Wszystkie typy pozycji (z wyjątkiem binarnych i JSON). Zachowanie właściwości: - *obsługiwane* jeśli `data_type` jest ustawione na ”Item values”.

Property	Type	Description
max_records	integer	Maksymalna liczba zdarzeń lub pozycji, które mogą zostać wysłane w jednej wiadomości. Możliwe wartości: 0-2147483647 (maksymalna wartość 32-bitowej liczby całkowitej ze znakiem). Domyślnie: 0 - Bez ograniczeń.
max_senders	integer	Liczba procesów nadawcy uruchamianych dla tego connectora. Możliwe wartości: 1-100. Domyślnie: 1.
max_attempts	integer	Liczba prób. Możliwe wartości: 1-5. Domyślnie: 1.
attempt_interval	string	Interwał między ponownymi próbami. Akceptuje sekundy. Możliwe wartości: 0s-10s. Domyślnie: 5s.
timeout	string	Zachowanie właściwości: - *obsługiwane* jeśli `max_attempts` jest większe niż 1. Limit czasu. Obsługiwane są sufiksy czasu (np. 30s, 1m). Makra użytkownika są obsługiwane. Możliwe wartości: 1s-60s. Domyślnie: 5s.
http_proxy	string	Ciąg połączenia proxy HTTP(S) podany jako *[protocol]://[username[:password]@]proxy.example.com[:port]*. Makra użytkownika są obsługiwane.
authtype	integer	Metoda uwierzytelniania HTTP. Możliwe wartości: 0 - *(domyślnie)* Brak; 1 - Basic; 2 - NTLM; 3 - Kerberos; 4 - Digest; 5 - Bearer.
username	string	Nazwa użytkownika. Makra użytkownika są obsługiwane. Zachowanie właściwości: - *obsługiwane* jeśli `authtype` jest ustawione na ”Basic”, ”NTLM”, ”Kerberos” lub ”Digest”
password	string	Hasło. Makra użytkownika są obsługiwane. Zachowanie właściwości: - *obsługiwane* jeśli `authtype` jest ustawione na ”Basic”, ”NTLM”, ”Kerberos” lub ”Digest”

Property	Type	Description
token	string	Token Bearer. Makra użytkownika są obsługiwane. Zachowanie właściwości: - *wymagane* jeśli `authtype` jest ustawione na ”Bearer”
verify_peer	integer	Czy weryfikować, że certyfikat hosta jest autentyczny. Możliwe wartości: 0 - Nie weryfikuj; 1 - *(domyślnie)* Weryfikuj.
verify_host	integer	Czy weryfikować, że nazwa hosta dla połączenia jest zgodna z nazwą w certyfikacie hosta. Możliwe wartości: 0 - Nie weryfikuj; 1 - *(domyślnie)* Weryfikuj.
ssl_cert_file	string	Ścieżka do pliku publicznego klucza SSL. Makra użytkownika są obsługiwane.
ssl_key_file	string	Ścieżka do pliku prywatnego klucza SSL. Makra użytkownika są obsługiwane.
ssl_key_password	string	Hasło do pliku klucza SSL. Makra użytkownika są obsługiwane.
description	text	Opis connectora.
status	integer	Czy connector jest włączony. Możliwe wartości: 0 - Wyłączony; 1 - *(domyślnie)* Włączony.
tags_evaltype	integer	Metoda oceny tagów. Możliwe wartości: 0 - *(domyślnie)* And/Or; 2 - Or.

Filtr tagów

Filtr tagów umożliwia eksportowanie tylko pasujących wartości pozycji lub zdarzeń. Jeśli nie jest ustawiony, wyeksportowane zostanie wszystko. Obiekt filtra tagów ma następujące właściwości.

Właściwość	Typ	Opis
tag	string	Nazwa tagu. Zachowanie właściwości: - *wymagane*
operator	integer	Warunek operatora. Możliwe wartości: 0 - *(domyślnie)* Równa się; 1 - Nie równa się; 2 - Zawiera; 3 - Nie zawiera; 12 - Istnieje; 13 - Nie istnieje.
value	string	Wartość tagu.

connector.create

Opis

`object connector.create(object/array connectors)`

Ta metoda umożliwia tworzenie nowych obiektów konektorów.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkownika typu *Super admin*. Uprawnienia do wywoływania tej metody można cofnąć w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Obiekty connectorów do utworzenia.

Oprócz standardowych właściwości connectora metoda akceptuje następujące parametry.

Parametr	Type	Opis
tags	array	Filtr tagów connectora.

Zwracane wartości

`(object)` Zwraca obiekt zawierający ID utworzonych konektorów we właściwości `connectorids`. Kolejność zwróconych identyfikatorów odpowiada kolejności przekazanych konektorów.

Przykłady

Tworzenie konektora

Utwórz konektor, aby eksportować zdarzenia wyzwalaczy z filtrem tagów. Uwierzytelnianie HTTP zostanie wykonane przy użyciu tokenu Bearer.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "connector.create",
    "params": [
        {
            "name": "Export of events",
            "data_type": 1,
            "url": "{$DATA_EXPORT_URL}",
            "authtype": 5,
            "token": "{$DATA_EXPORT_BEARER_TOKEN}",
            "tags": [
                {
                    "tag": "service",
                    "operator": 0,
                    "value": "mysqld"
                }
            ]
        }
    ],
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "connectorid": [
            "3"
        ]
    },
    "id": 1
}
```

Źródło

CConnector::create() w *ui/include/classes/api/services/CConnector.php*.

connector.delete

Opis

`object connector.delete(array connectorids)`

Ta metoda pozwala na usuwanie wpisów konektora.

> **Note:**
> Ta metoda jest dostępna tylko dla typu użytkownika *Super admin*. Uprawnienia do wywołania metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w User roles.

Parametry

`(tablica)` Identyfikatory konektorów do usunięcia.

Wartości zwracane

`(object)` Zwraca obiekt zawierający identyfikatory usuniętych konektorów pod właściwością `connectorids`.

Przykłady

Usuwanie wielu konektorów

Usuń dwa wpisy konektora.

Żądanie:

```
{
"jsonrpc": "2.0",
"method": "connector.delete",
"params": [
3,
5
],
"id": 1
}
```

Odpowiedź:

```
{
"jsonrpc": "2.0",
"result": {
"connectorids": [
"3",
"5"
]
},
"id": 1
}
```

Źródło

CConnector::delete() w *ui/include/classes/api/services/CConnector.php*.

connector.get

Opis

`integer/array connector.get(object parameters)`

Metoda pozwala na pobranie obiektów konektora zgodnie z podanymi parametrami.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkownika *Super admin*. Uprawnienia do wywoływania tej metody można cofnąć w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

(object) Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
connectorids	ID/array	Zwraca tylko connectory o podanych identyfikatorach.
selectTags	query	Zwraca właściwość tags z filtrem tagów connectora. Obsługuje count.
sortfield	string/array	Sortuje wynik według podanych właściwości. Możliwe wartości: connectorid, name, data_type, status.
countOutput	boolean	Te parametry są opisane w komentarzu referencyjnym.
excludeSearch	boolean	
filter	object	
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

(integer/array) Zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli został użyty parametr countOutput.

Przykłady

Pobieranie wszystkich konektorów

Pobierz wszystkie dane o wszystkich konektorach i ich właściwościach.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "connector.get",
    "params": {
        "output": "extend",
        "selectTags": ["tag", "operator", "value"],
        "preservekeys": true
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "connectorid": "1",
            "name": "Export of item values",
            "protocol": "0",
            "data_type": "0",
            "url": "{$DATA_EXPORT_VALUES_URL}",
            "item_value_type": "31",
            "authtype": "4",
            "username": "{$DATA_EXPORT_VALUES_USERNAME}",
            "password": "{$DATA_EXPORT_VALUES_PASSWORD}",
            "token": "",
```

```
            "max_records": "0",
            "max_senders": "4",
            "max_attempts": "2",
            "attempt_interval": "10s",
            "timeout": "10s",
            "http_proxy": "{$DATA_EXPORT_VALUES_PROXY}",
            "verify_peer": "1",
            "verify_host": "1",
            "ssl_cert_file": "{$DATA_EXPORT_VALUES_SSL_CERT_FILE}",
            "ssl_key_file": "{$DATA_EXPORT_VALUES_SSL_KEY_FILE}",
            "ssl_key_password": "",
            "description": "",
            "status": "1",
            "tags_evaltype": "0",
            "tags": [
                {
                    "tag": "component",
                    "operator": "0",
                    "value": "memory"
                }
            ]
        },
        {
            "connectorid": "2",
            "name": "Export of events",
            "protocol": "0",
            "data_type": "1",
            "url": "{$DATA_EXPORT_EVENTS_URL}",
            "item_value_type": "31",
            "authtype": "5",
            "username": "",
            "password": "",
            "token": "{$DATA_EXPORT_EVENTS_BEARER_TOKEN}",
            "max_records": "0",
            "max_senders": "2",
            "max_attempts": "1",
            "attempt_interval": "5s",
            "timeout": "5s",
            "http_proxy": "",
            "verify_peer": "1",
            "verify_host": "1",
            "ssl_cert_file": "",
            "ssl_key_file": "",
            "ssl_key_password": "",
            "description": "",
            "status": "1",
            "tags_evaltype": "0",
            "tags": [
                {
                    "tag": "scope",
                    "operator": "0",
                    "value": "performance"
                }
            ]
        }
    ],
    "id": 1
}
```


Źródło

CConnector:get() w *ui/include/classes/api/services/CConnector.php*.

connector.update

Opis

`object connector.update(object/array connectors)`

Ta metoda pozwala zaktualizować istniejące konektory.

noteclassic Ta metoda jest dostępna tylko dla użytkownika typu *Super admin*. Uprawnienia do wywoływania tej metody można cofnąć w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników. :::

Parametry

`(object/array)` Właściwości connectora do zaktualizowania.

Właściwość `connectorid` musi być zdefiniowana dla każdego connectora, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko przekazane właściwości, wszystkie pozostałe pozostaną bez zmian.

Oprócz standardowych właściwości connectora metoda akceptuje następujące parametry.

Parametr	Typ	Opis
tags	array	Filtr tagów connectora, który zastąpi bieżący filtr tagów.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych konektorów we właściwości `connectorids`.

Przykłady

Zmiana typu uwierzytelniania HTTP

Zmień typ uwierzytelniania HTTP na Bearer dla connectora o ID „3”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "connector.update",
    "params": {
        "connectorid": 3,
        "authtype": 5,
        "token": "{$DATA_EXPORT_BEARER_TOKEN}"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "connectorids": [
            "3"
        ]
    },
    "id": 1
}
```

Aktualizowanie filtra tagów

Zmień filtr tagów dla konektora o ID „5”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "connector.update",
    "params": [
        {
            "connectorid": 5,
```

```
            "tags_evaltype": 2,
            "tags": [
                {
                    "tag": "service",
                    "operator": 0,
                    "value": "mysqld"
                },
                {
                    "tag": "error",
                    "operator": 12,
                    "value": ""
                }
            ]
        }
    ],
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "connectorids": [
            "5"
        ]
    },
    "id": 1
}
```

Źródło

CConnector::update() w *ui/include/classes/api/services/CConnector.php*.

Dziennik audytu

Ta klasa została zaprojektowana do pracy z dziennikiem audytu.

Odwołania do obiektów:

- Dziennik audytu

Dostępne metody:

- auditlog.get - pobieranie rekordów dziennika audytu

Obiekt dziennika audytu

Następujące obiekty są bezpośrednio powiązane z API `auditlog`.

Dziennik audytu

Obiekt dziennika audytu zawiera informacje o działaniach użytkownika. Ma następujące właściwości.

Właściwość	Typ	Opis
auditid	ID	ID wpisu dziennika audytu. Generowane przy użyciu algorytmu CUID.
userid	ID	Userid autora wpisu dziennika audytu.
username	string	Nazwa użytkownika autora wpisu dziennika audytu.
clock	timestamp	Znacznik czasu utworzenia wpisu dziennika audytu.
ip	string	Adres IP autora wpisu dziennika audytu.

Właściwość	Typ	Opis
action	integer	Działanie wpisu dziennika audytu. Możliwe wartości: 0 - Dodanie; 1 - Aktualizacja; 2 - Usunięcie; 4 - Wylogowanie; 7 - Wykonanie; 8 - Logowanie; 9 - Nieudane logowanie; 10 - Czyszczenie historii; 11 - Odświeżenie konfiguracji; 12 - Push.

Właściwość	Typ	Opis
resourcetype	integer	Typ zasobu wpisu dziennika audytu. Możliwe wartości: 0 - Użytkownik; 3 - Typ nośnika; 4 - Host; 5 - Akcja; 6 - Wykres; 11 - Grupa użytkowników; 13 - Wyzwalacz; 14 - Grupa hostów; 15 - Pozycja; 16 - Obraz; 17 - Mapa wartości; 18 - Usługa; 19 - Mapa; 22 - Scenariusz WWW; 23 - Reguła wykrywania; 25 - Skrypt; 26 - Proxy; 27 - Okres utrzymania; 28 - Wyrażenie regularne; 29 - Makro; 30 - Szablon; 31 - Prototyp wyzwalacza; 32 - Mapowanie ikon; 33 - Pulpit; 34 - Korelacja zdarzeń; 35 - Prototyp wykresu; 36 - Prototyp pozycji; 37 - Prototyp hosta; 38 - Autorejestracja; 39 - Moduł; 40 - Ustawienia; 41 - Housekeeping; 42 - Uwierzytelnianie; 43 - Pulpit szablonu; 44 - Rola użytkownika; 45 - Token API; 46 - Zaplanowany raport; 47 - Węzeł wysokiej dostępności; 48 - SLA; 49 - Katalog użytkowników; 50 - Grupa szablonów; 51 - Łącznik; 52 - Reguła LLD; 53 - Historia; 54 - Uwierzytelnianie wieloskładnikowe; 55 - Grupa proxy; 56 - Prototyp reguły LLD.
resourceid	ID	Identyfikator zasobu wpisu dziennika audytu.
resource_cuid	ID	Unikalny identyfikator zasobu wpisu dziennika audytu wygenerowany przy użyciu algorytmu CUID.
resourcename	string	Czytelna dla człowieka nazwa zasobu wpisu dziennika audytu.
recordsetid	ID	ID zestawu rekordów wpisu dziennika audytu. Rekordy dziennika audytu utworzone podczas tej samej operacji będą miały to samo ID zestawu rekordów. Generowane przy użyciu algorytmu CUID.

Właściwość	Typ	Opis
details	text	Szczegóły wpisu dziennika audytu. Szczegóły są przechowywane jako obiekt JSON, gdzie każda nazwa właściwości jest ścieżką do właściwości lub zagnieżdżonego obiektu, w którym wystąpiła zmiana, a każda wartość zawiera dane (w formacie tablicy) o zmianie tej właściwości lub zagnieżdżonego obiektu. Możliwe formaty wartości: ["add"] - Zagnieżdżony obiekt został dodany; ["add", "<value>"] - Właściwość dodanego obiektu jest równa <value>; ["update"] - Zagnieżdżony obiekt został zaktualizowany; ["update", "<new value>", "<old value>"] - Właściwość zaktualizowanego obiektu została zmieniona z <old value> na <new value>; ["delete"] - Zagnieżdżony obiekt został usunięty.

auditlog.get

Opis

`integer/array auditlog.get(object parameters)`

Ta metoda umożliwia pobranie wpisów dziennika audytu zgodnie z podanymi parametrami.

Note:
Ta metoda jest dostępna wyłącznie dla użytkownika typu *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
auditids	ID/array	Zwraca tylko dziennik audytu o podanych ID.
userids	ID/array	Zwraca tylko dziennik audytu utworzony przez podanych użytkowników.
time_from	timestamp	Zwraca tylko wpisy dziennika audytu, które zostały utworzone po podanym czasie lub o podanym czasie.
time_till	timestamp	Zwraca tylko wpisy dziennika audytu, które zostały utworzone przed podanym czasem lub o podanym czasie.
sortfield	string/array	Sortuje wynik według podanych właściwości. Możliwe wartości: `auditid`, `userid`, `clock`.
countOutput	boolean	Te parametry są opisane w komentarzu referencyjnym.
excludeSearch	boolean	
filter	object	
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów;

- liczbę pobranych obiektów, jeśli użyto parametru `countOutput`.

Przykłady

Pobieranie dziennika audytu

Pobierz dwa najnowsze wpisy dziennika audytu.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "auditlog.get",
    "params": {
        "output": "extend",
        "sortfield": "clock",
        "sortorder": "DESC",
        "limit": 2
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "auditid": "cksstgfam0001yhdcc41y20q2",
            "userid": "1",
            "username": "Admin",
            "clock": "1629975715",
            "ip": "127.0.0.1",
            "action": "1",
            "resourcetype": "0",
            "resourceid": "0",
            "resource_cuid": "0",
            "resourcename": "Jim",
            "recordsetid": "cksstgfal0000yhdcso67ondl",
            "details": "{\"user.name\":[\"update\",\"Jim\",\"\"],\"user.medias[37]\":[\"add\"],\"user.medi
        },
        {
            "auditid": "ckssofl0p0001yhdcqxclsg8r",
            "userid": "1",
            "username": "Admin",
            "clock": "1629967278",
            "ip": "127.0.0.1",
            "action": "0",
            "resourcetype": "0",
            "resourceid": "20",
            "resource_cuid": "0",
            "resourcename": "John",
            "recordsetid": "ckssofl0p0000yhdcpxyo1jgo",
            "details": "{\"user.username\":[\"add\",\"John\"], \"user.userid:\":[\"add\",\"20\"],\"user.us
        }
    ],
    "id": 1
}
```

Zobacz także

- Audit log object

Źródło

CAuditLog::get() in *ui/include/classes/api/services/CAuditLog.php*.

Grupa hostów

Ta klasa jest przeznaczona do pracy z grupami hostów.

Odwołania do obiektów:

- Grupa hostów

Dostępne metody:

- hostgroup.create - utwórz nowe grupy hostów
- hostgroup.delete - usuń grupy hostów
- hostgroup.get - pobierz grupy hostów
- hostgroup.massadd - dodaj powiązane obiekty do grup hostów
- hostgroup.massremove - usuń powiązane obiekty z grup hostów
- hostgroup.propagate - propaguj uprawnienia i filtry tagów do podgrup grup hostów
- hostgroup.update - zaktualizuj grupy hostów

Obiekt grupy hostów

Następujące obiekty są bezpośrednio powiązane z API `hostgroup`.

Grupa hostów

Obiekt grupy hostów ma następujące właściwości.

Właściwość	Typ	Opis
groupid	ID	ID grupy hostów. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji
name	string	Nazwa grupy hostów. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
flags	integer	Pochodzenie grupy hostów. Możliwe wartości: 0 - zwykła grupa hostów; 4 - wykryta grupa hostów. Zachowanie właściwości: - *tylko do odczytu*
uuid	string	Uniwersalny unikalny identyfikator używany do łączenia importowanych grup hostów z już istniejącymi. Generowany automatycznie, jeśli nie został podany.

hostgroup.create

Opis

`object hostgroup.create(object/array hostGroups)`

Ta metoda pozwala na tworzenie nowych grup hostów.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkownika *Super admin*. Uprawnienia do wywołania metody można cofnąć w ustawieniach roli użytkownika. Więcej informacji można znaleźć w User roles.

Parametry

`(object/array)` Grupy hostów do utworzenia.

Metoda akceptuje grupy hostów z standardowymi właściwościami grup hostów.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory utworzonych grup hostów we właściwości `groupids`. Kolejność zwróconych ID odpowiada kolejności przekazanych grup hostów.

Przykłady

Tworzenie grupy hostów

Utwórz grupę hostów o nazwie „Serwery Linux”.

Żądanie:

```
{
"jsonrpc": "2.0",
"method": "hostgroup.create",
"params": {
"name": "Serwery Linux"
},
"id": 1
}
```

Odpowiedź:

```
{
"jsonrpc": "2.0",
"result": {
"groupids": [
"107819"
]
},
"id": 1
}
```

Źródło

CHostGroup::create() w *ui/include/classes/api/services/CHostGroup.php*.

hostgroup.delete

Opis

`object hostgroup.delete(array hostGroupIds)`

Ta metoda umożliwia usuwanie grup hostów.

Grupa hostów nie może zostać usunięta, jeśli:

- zawiera hosty, które należą wyłącznie do tej grupy;
- jest oznaczona jako wewnętrzna;
- jest używana przez prototyp hosta;
- jest używana w skrypcie globalnym;
- jest używana w warunku korelacji.

Note:
Ta metoda jest dostępna tylko dla użytkowników typu *Admin* i *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(array)` ID grup hostów do usunięcia.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory usuniętych grup hostów w właściwości `groupids`.

Przykłady

Usuwanie wielu grup hostów

Usuń dwie grupy hostów.

Żądanie:

```
{
"jsonrpc": "2.0",
"method": "hostgroup.delete",
"params": [
"107824",
"107825"
],
"id": 1
}
```

Odpowiedź:

```
{
"jsonrpc": "2.0",
"result": {
"groupids": [
"107824",
"107825"
]
},
"id": 1
}
```

Źródło

CHostGroup::delete() w *ui/include/classes/api/services/CHostGroup.php*.

hostgroup.get

Opis

`integer/array hostgroup.get(object parameters)`

Ta metoda umożliwia pobieranie grup hostów zgodnie z podanymi parametrami.

Note:
Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
graphids	ID/array	Zwraca tylko grupy hostów zawierające hosty z podanymi wykresami.
groupids	ID/array	Zwraca tylko grupy hostów o podanych identyfikatorach grup hostów.
hostids	ID/array	Zwraca tylko grupy hostów zawierające podane hosty.
maintenanceids	ID/array	Zwraca tylko grupy hostów, na które wpływają podane okresy konserwacji.
triggerids	ID/array	Zwraca tylko grupy hostów zawierające hosty z podanymi wyzwalaczami.
with_graphs	boolean	Zwraca tylko grupy hostów zawierające hosty z wykresami.
with_graph_prototypes	boolean	Zwraca tylko grupy hostów zawierające hosty z prototypami wykresów.
with_hosts	boolean	Zwraca tylko grupy hostów zawierające hosty.
with_httptests	boolean	Zwraca tylko grupy hostów zawierające hosty z testami WWW. Nadpisuje parametr `with_monitored_httptests`.
with_items	boolean	Zwraca tylko grupy hostów zawierające hosty z pozycjami. Nadpisuje parametry `with_monitored_items` i `with_simple_graph_items`.

Parametr	Typ	Opis
with_item_prototypes	boolean	Zwraca tylko grupy hostów zawierające hosty z prototypami pozycji. Nadpisuje parametr `with_simple_graph_item_prototypes`.
with_simple_graph_item_prototypes	boolean	Zwraca tylko grupy hostów zawierające hosty z prototypami pozycji, które są włączone do tworzenia i mają numeryczny typ informacji.
with_monitored_httptests	boolean	Zwraca tylko grupy hostów zawierające hosty z włączonymi testami WWW.
with_monitored_hosts	boolean	Zwraca tylko grupy hostów zawierające monitorowane hosty.
with_monitored_items	boolean	Zwraca tylko grupy hostów zawierające hosty z włączonymi pozycjami. Nadpisuje parametr `with_simple_graph_items`.
with_monitored_triggers	boolean	Zwraca tylko grupy hostów zawierające hosty z włączonymi wyzwalaczami. Wszystkie pozycje używane w wyzwalaczu również muszą być włączone.
with_simple_graph_items	boolean	Zwraca tylko grupy hostów zawierające hosty z numerycznymi pozycjami.
with_triggers	boolean	Zwraca tylko grupy hostów zawierające hosty z wyzwalaczami. Nadpisuje parametr `with_monitored_triggers`.
selectDiscoveryRules	query	Zwraca właściwość `discoveryRules` z regułami LLD, które wykryły grupę hostów.
selectDiscoveryData	query	Zwraca właściwość `discoveryData` z obiektami wykrywania grup hostów. Każdy obiekt wykrywania grupy hostów jest prototypem grupy hostów powiązanym z wykrytą grupą hostów i ma następujące właściwości: `parent_group_prototypeid` - `(ID)` identyfikator prototypu grupy hostów, z którego wykryto grupę hostów; `name` - `(string)` nazwa prototypu grupy hostów; `ts_delete` - `(timestamp)` czas, po którym grupa hostów, która nie jest już wykrywana, zostanie usunięta; `status` - `(int)` status wykrywania grupy hostów: 0 - *(domyślnie)* grupa hostów jest wykryta, 1 - grupa hostów nie jest już wykrywana.
selectHostPrototypes	query	Zwraca właściwość `hostPrototypes` z prototypami hostów, które wykryły tę grupę hostów.
selectHosts	query	Zwraca właściwość `hosts` z hostami należącymi do grupy hostów. Obsługuje `count`.
limitSelects	integer	Ogranicza liczbę rekordów zwracanych przez podzapytania. Dotyczy następujących podzapytań: `selectHosts` - wyniki będą sortowane według `host`.
sortfield	string/array	Sortuje wynik według podanych właściwości. Możliwe wartości: `groupid`, `name`.
countOutput	boolean	Te parametry opisano w komentarzu referencyjnym.
editable	boolean	
excludeSearch	boolean	
filter	object	
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Parametr	Typ	Opis
selectGroupDiscoveries	query	Zwraca właściwość `groupDiscoveries` z obiektami wykrywania grup hostów. Każdy obiekt wykrywania grupy hostów jest prototypem grupy hostów powiązanym z wykrytą grupą hostów. To zapytanie jest **przestarzałe**; zamiast niego użyj `selectDiscoveryData`.

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów
- liczbę pobranych obiektów, jeśli użyto parametru `countOutput`

Przykłady

Pobieranie danych według nazwy

Pobierz wszystkie dane o dwóch grupach hostów o nazwach „Zabbix servers” i „Linux servers”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "hostgroup.get",
    "params": {
        "output": "extend",
        "filter": {
            "name": [
                "Zabbix servers",
                "Linux servers"
            ]
        }
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "groupid": "2",
            "name": "Linux servers",
            "flags": "0",
            "uuid": "dc579cd7a1a34222933f24f52a68bcd8"
        },
        {
            "groupid": "4",
            "name": "Zabbix servers",
            "flags": "0",
            "uuid": "6f6799aa69e844b4b3918f779f2abf08"
        }
    ],
    "id": 1
}
```

Zobacz także

- Host

Źródło

CHostGroup::get() w *ui/include/classes/api/services/CHostGroup.php*.

hostgroup.massadd

Opis

`object hostgroup.massadd(object parameters)`

Ta metoda umożliwia jednoczesne dodanie wielu powiązanych obiektów do wszystkich podanych grup hostów.

> **Note:**
> Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach ról użytkowników. Więcej informacji znajduje się w sekcji Role użytkowników.

Parametry

`(object)` Parametry zawierające identyfikatory grup hostów do zaktualizowania oraz obiekty do dodania do wszystkich grup hostów.

Metoda akceptuje następujące parametry.

Parametr	Type	Opis
groups	object/array	Grupy hostów, które mają zostać zaktualizowane. Grupy hostów muszą mieć zdefiniowaną tylko właściwość `groupid`. Zachowanie parametrów: - *wymagane*
hosts	object/array	Hosty do dodania do wszystkich grup hostów. Hosty muszą mieć zdefiniowaną tylko właściwość `hostid`.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych grup hostów we właściwości `groupids`.

Przykłady

Dodawanie hostów do grup hostów

Dodaj dwa hosty do grup hostów o identyfikatorach 5 i 6.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "hostgroup.massadd",
    "params": {
        "groups": [
            {
                "groupid": "5"
            },
            {
                "groupid": "6"
            }
        ],
        "hosts": [
            {
                "hostid": "30050"
            },
            {
                "hostid": "30001"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "groupids": [
            "5",
            "6"
        ]
    },
    "id": 1
}
```

Zobacz także

- Host

Źródło

CHostGroup::massAdd() w *ui/include/classes/api/services/CHostGroup.php*.

hostgroup.massremove

Opis

`object hostgroup.massremove(object parameters)`

Ta metoda pozwala na usuwanie powiązanych obiektów z wielu grup hostów.

Note:
Ta metoda jest dostępna tylko dla użytkowników typu *Admin* i *Super admin*. Uprawnienia do wywołania metody można odwołać w ustawieniach roli użytkownika. Więcej informacji można znaleźć w User roles.

Parametry

`(object)` Parametry zawierające identyfikatory grup hostów do zaktualizowania oraz obiekty, które powinny zostać usunięte.

Parametr	Type	Opis
groupids	ID/array	Identyfikatory grup hostów, które mają zostać zaktualizowane. Zachowanie parametru: - *wymagany*
hostids	ID/array	Identyfikatory hostów, które mają zostać usunięte ze wszystkich grup hostów.

Wartości zwracane

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych grup hostów we właściwości `groupids`.

Przykłady

Usuwanie hostów z grup hostów

Usuń dwa hosty z podanych grup hostów.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "hostgroup.massremove",
    "params": {
        "groupids": [
            "5",
            "6"
        ],
        "hostids": [
            "30050",
```

```
            "30001"
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "groupids": [
            "5",
            "6"
        ]
    },
    "id": 1
}
```

Źródło

CHostGroup::massRemove() w *ui/include/classes/api/services/CHostGroup.php*.

hostgroup.propagate

Opis

`object hostgroup.propagate(object parameters)`

Ta metoda umożliwia zastosowanie uprawnień i filtrów tagów do wszystkich podgrup grupy hostów.

Note:
Ta metoda jest dostępna tylko dla użytkowników typu *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji znajduje się w sekcji Role użytkowników.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

|Parametr|Type|Opis|

|--|--|------|

|groups|object/array|Grupy hostów do propagowania.

Grupy hostów muszą mieć zdefiniowaną właściwość `groupid`.

Zach
parametrów:
- *wymagane*|

|permissions|boolean|Ustaw na ”true”, aby propagować uprawnienia.

Zachowanie parametrów:
- *wymagane*, jeśli `tag_filters` nie jest ustawione|

|tag_filters|boolean|Ustaw na ”true”, aby propagować filtry tagów.

Zachowanie parametrów:
- *wymagane*, jeśli `permissions` nie jest ustawione|

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory propagowanych grup hostów

we właściwości `groupids`.

Przykłady

Propagowanie uprawnień grupy hostów i filtrów tagów do jej podgrup.

Propagowanie uprawnień grupy hostów i filtrów tagów do jej podgrup.

Żądanie:

```
{

    "jsonrpc": "2.0",
```

```
    "method": "hostgroup.propagate",
    "params": {
        "groups": [
            {
                "groupid": "6"
            }
        ],
        "permissions": true,
        "tag_filters": true
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "groupids": [
            "6",
        ]
    },
    "id": 1
}
```

Zobacz także

- hostgroup.update
- hostgroup.massadd
- Host

Źródło

CHostGroup::propagate() w *ui/include/classes/api/services/CHostGroup.php*.

hostgroup.update

Opis

`object hostgroup.update(object/array hostGroups)`

Ta metoda umożliwia aktualizację istniejących grup hostów.

Note:
Ta metoda jest dostępna tylko dla użytkowników typu *Admin* i *Super admin*. Uprawnienia do wywołania metody mogą być cofnięte w ustawieniach ról użytkownika. Zobacz Role użytkownika aby uzyskać więcej informacji.

Parametry

`(object/array)` Właściwości grupy hostów, które mają zostać zaktualizowane.

Właściwość `groupid` musi być zdefiniowana dla każdej grupy hostów, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko podane właściwości, wszystkie pozostałe pozostaną bez zmian.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych grup hostów we właściwości `groupids`.

Przykłady

Zmiana nazwy grupy hostów

Zmień nazwę grupy hostów na „Linux hosts”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "hostgroup.update",
    "params": {
        "groupid": "7",
        "name": "Linux hosts"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "groupids": [
            "7"
        ]
    },
    "id": 1
}
```

Zmiana nazw wielu grup hostów

Zmień nazwy dwóch grup hostów, aby uwzględnić w nich informacje o regionie.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "hostgroup.update",
    "params": [
        {
            "groupid": "8",
            "name": "Europe/Linux hosts"
        },
        {
            "groupid": "9",
            "name": "Europe/Windows hosts"
        }
    ],
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "groupids": [
            "8",
            "9"
        ]
    },
    "id": 1
}
```

Źródło

CHostGroup::update() w *ui/include/classes/api/services/CHostGroup.php*.

Grupa proxy

Ta klasa jest przeznaczona do pracy z grupami proxy.

Odwołania do obiektów:

- Grupa proxy

Dostępne metody:

- proxygroup.create - utwórz nowe grupy proxy
- proxygroup.delete - usuń grupy proxy
- proxygroup.get - pobierz grupy proxy
- proxygroup.update - zaktualizuj grupy proxy

Obiekt grupy proxy

Następujące obiekty są bezpośrednio powiązane z API `proxygroup`.

Grupa proxy

Obiekt grupy proxy ma następujące właściwości.

Właściwość	Typ	Opis
proxy_groupid	ID	ID grupy proxy. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji
name	string	Nazwa grupy proxy. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
description	text	Opis grupy proxy.
failover_delay	string	Okres, w którym proxy w grupie proxy musi komunikować się z serwer Zabbix, aby było uznawane za online. Obsługiwane są sufiksy czasu, np. 30s, 1m. Obsługiwane są makra użytkownika. Możliwe wartości: 10s-15m. Domyślnie: 1m.

Właściwość	Typ	Opis
min_online	string	Minimalna liczba proxy online wymagana do utrzymania grupy proxy w stanie online. Obsługiwane są makra użytkownika. Zakres możliwych wartości: 1-1000. Domyślnie: 1.
state	integer	Stan grupy proxy. Możliwe wartości: 0 - Nieznany; 1 - Offline; 2 - Odzyskiwanie; 3 - Online; 4 - Pogarszanie. Zachowanie właściwości: *- tylko do odczytu*

proxygroup.create

Opis

`object proxygroup.create(object/array proxyGroups)`

Ta metoda umożliwia tworzenie nowych grup proxy.

Note:
Ta metoda jest dostępna tylko dla użytkowników typu *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach ról użytkowników. Więcej informacji znajduje się w Rolach użytkowników.

Parametry

`(object/array)` Grupy proxy do utworzenia.

Metoda akceptuje grupy proxy ze standardowymi właściwościami grup proxy.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory utworzonych grup proxy we właściwości `proxy_groupids`. Kolejność zwróconych identyfikatorów odpowiada kolejności przekazanych grup proxy.

Przykłady

Utwórz grupę proxy

Utwórz grupę proxy z niestandardowymi ustawieniami.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "proxygroup.create",
    "params": {
        "name": "Proxy group",
        "failover_delay": "5m",
        "min_online": "10"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
```

```
    "result": {
        "proxy_groupids": [
            "5"
        ]
    },
    "id": 1
}
```

Źródło

CProxyGroup::create() w *ui/include/classes/api/services/CProxyGroup.php*.

proxygroup.delete

Opis

`object proxygroup.delete(array proxyGroupIds)`

Ta metoda umożliwia usuwanie grup proxy.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkowników typu *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach ról użytkowników. Więcej informacji znajduje się w sekcji Role użytkowników.

Parametry

`(array)` ID grup proxy do usunięcia.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory usuniętych grup proxy we właściwości `proxy_groupids`.

Przykłady

Usuń wiele grup proxy

Usuń dwie grupy proxy.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "proxygroup.delete",
    "params": [
        "5",
        "10"
    ],
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "proxy_groupids": [
            "5",
            "10"
        ]
    },
    "id": 1
}
```

Źródło

CProxyGroup::delete() w *ui/include/classes/api/services/CProxyGroup.php*.

proxygroup.get

Opis

`integer/array proxygroup.get(object parameters)`

Ta metoda umożliwia pobieranie grup proxy zgodnie z podanymi parametrami.

> **Note:**
> Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
proxy_groupids	ID/array	Zwraca tylko grupy proxy o podanych identyfikatorach.
proxyids	ID/array	Zwraca tylko grupy proxy zawierające podane proxy.
selectProxies	query	Zwraca właściwość `proxies` z proxy należącymi do grupy proxy. Obsługuje `count`.
sortfield	string/array	Sortuje wynik według podanych właściwości. Możliwe wartości: `proxy_groupid`, `name`.
countOutput	boolean	Te parametry opisano w komentarzu referencyjnym.
editable	boolean	
excludeSearch	boolean	
filter	object	
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli został użyty parametr `countOutput`.

Przykłady

Pobieranie wszystkich grup proxy

Pobierz wszystkie skonfigurowane grupy proxy wraz z proxy.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "proxygroup.get",
    "params": {
        "output": "extend",
        "selectProxies": ["proxyid", "name"]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "proxy_groupid": "1",
            "name": "Proxy group 1",
            "failover_delay": "1m",
            "min_online": "3",
            "description": "",
            "state": "1",
            "proxies": [
                {
                    "proxyid": "1",
                    "name": "proxy 1"
                },
                {
                    "proxyid": "2",
                    "name": "proxy 2"
                }
            ]
        },
        {
            "proxy_groupid": "2",
            "name": "Proxy group 2",
            "failover_delay": "10m",
            "min_online": "3",
            "description": "",
            "state": "3",
            "proxies": [
                {
                    "proxyid": "3",
                    "name": "proxy 3"
                },
                {
                    "proxyid": "4",
                    "name": "proxy 4"
                },
                {
                    "proxyid": "5",
                    "name": "proxy 5"
                }
            ]
        }
    ],
    "id": 1
}
```


Zobacz także

- Proxy

Źródło

CProxyGroup::get() w *ui/include/classes/api/services/CProxyGroup.php*.

proxygroup.update

Opis

`object proxygroup.update(object/array proxyGroups)`

Ta metoda umożliwia aktualizację istniejących grup proxy.

Note:
Ta metoda jest dostępna tylko dla użytkowników typu *Super admin*. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w User roles.

Parametry

`(object/array)` Właściwości grupy proxy do zaktualizowania.

Właściwość `proxy_groupid` musi być zdefiniowana dla każdej grupy proxy, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko przekazane właściwości, wszystkie pozostałe pozostaną bez zmian.

Metoda akceptuje grupy proxy ze standardowymi właściwościami grupy proxy.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych grup proxy we właściwości `proxy_groupids`.

Przykłady

Zmień minimalną liczbę proxy online

Zmień minimalną liczbę proxy online wymaganą, aby grupa była online.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "proxygroup.update",
    "params": {
        "proxy_groupid": "5",
        "min_online": "3"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "proxy_groupids": [
            "5"
        ]
    },
    "id": 1
}
```

Źródło

CProxyGroup::update() w *ui/include/classes/api/services/CProxyGroup.php*.

Grupa szablonów

Ta klasa jest przeznaczona do pracy z grupami szablonów.

Odwołania do obiektów:

- Grupa szablonów

Dostępne metody:

- templategroup.create - utwórz nowe grupy szablonów
- templategroup.delete - usuń grupy szablonów
- templategroup.get - pobierz grupy szablonów
- templategroup.massadd - dodaj powiązane obiekty do grup szablonów
- templategroup.massremove - usuń powiązane obiekty z grup szablonów
- templategroup.propagate - propaguj uprawnienia do podgrup grup szablonów
- templategroup.update - zaktualizuj grupy szablonów

Obiekt grupy szablonów

Następujące obiekty są bezpośrednio powiązane z API `templategroup`.

Grupa szablonów

Obiekt grupy szablonów ma następujące właściwości.

Właściwość	Typ	Opis
groupid	ID	ID grupy szablonów. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji
name	string	Nazwa grupy szablonów. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
uuid	string	Uniwersalny unikalny identyfikator, używany do łączenia importowanych grup szablonów z już istniejącymi. Generowany automatycznie, jeśli nie został podany.

templategroup.create

Opis

`object templategroup.create(object/array templateGroups)`

Ta metoda umożliwia tworzenie nowych grup szablonów.

> **Note:**
> Ta metoda jest dostępna wyłącznie dla użytkowników typu *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Grupy szablonów do utworzenia. Metoda akceptuje grupy szablonów ze standardowymi właściwościami grup szablonów.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory utworzonych grup szablonów we właściwości `groupids`. Kolejność zwróconych identyfikatorów odpowiada kolejności przekazanych grup szablonów.

Przykłady

Tworzenie grupy szablonów

Utwórz grupę szablonów o nazwie "Templates/Databases".

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "templategroup.create",
    "params": {
        "name": "Templates/Databases"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "groupids": [
```

```
            "107820"
        ]
    },
    "id": 1
}
```

Źródło

CTemplateGroup::create() w *ui/include/classes/api/services/CTemplateGroup.php*.

templategroup.delete

Opis

`object templategroup.delete(array templateGroupIds)`

Ta metoda umożliwia usuwanie grup szablonów.

Grupa szablonów nie może zostać usunięta, jeśli zawiera szablony należące wyłącznie do tej grupy.

> **Note:**
> Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach ról użytkowników. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(array)` ID grup szablonów do usunięcia.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory usuniętych grup szablonów we właściwości `groupids`.

Przykłady

Usuwanie wielu grup szablonów

Usuń dwie grupy szablonów.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "templategroup.delete",
    "params": [
        "107814",
        "107815"
    ],
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "groupids": [
            "107814",
            "107815"
        ]
    },
    "id": 1
}
```

Źródło

CTemplateGroup::delete() w *ui/include/classes/api/services/CTemplateGroup.php*.

templategroup.get

Opis

`integer/array templategroup.get(object parameters)`

Ta metoda umożliwia pobieranie grup szablonów zgodnie z podanymi parametrami.

> **Note:**
> Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
graphids	ID/array	Zwracaj tylko grupy szablonów zawierające szablony z podanymi wykresami.
groupids	ID/array	Zwracaj tylko grupy szablonów o podanych identyfikatorach grup szablonów.
templateids	ID/array	Zwracaj tylko grupy szablonów zawierające podane szablony.
triggerids	ID/array	Zwracaj tylko grupy szablonów zawierające szablony z podanymi wyzwalaczami.
with_graphs	boolean	Zwracaj tylko grupy szablonów zawierające szablony z wykresami.
with_graph_prototypes	boolean	Zwracaj tylko grupy szablonów zawierające szablony z prototypami wykresów.
with_httptests	boolean	Zwracaj tylko grupy szablonów zawierające szablony z testami WWW.
with_items	boolean	Zwracaj tylko grupy szablonów zawierające szablony z pozycjami. Nadpisuje parametry `with_simple_graph_items`.
with_item_prototypes	boolean	Zwracaj tylko grupy szablonów zawierające szablony z prototypami pozycji. Nadpisuje parametr `with_simple_graph_item_prototypes`.
with_simple_graph_item_prototypes	boolean	Zwracaj tylko grupy szablonów zawierające szablony z prototypami pozycji, które są włączone do tworzenia i mają numeryczny typ informacji.
with_simple_graph_items	boolean	Zwracaj tylko grupy szablonów zawierające szablony z numerycznymi pozycjami.
with_templates	boolean	Zwracaj tylko grupy szablonów zawierające szablony.
with_triggers	boolean	Zwracaj tylko grupy szablonów zawierające szablony z wyzwalaczami.
selectTemplates	query	Zwracaj właściwość `templates` zawierającą szablony należące do grupy szablonów. Obsługuje `count`.
limitSelects	integer	Ogranicza liczbę rekordów zwracanych przez podzapytania. Dotyczy następujących podzapytań: `selectTemplates` - wyniki będą sortowane według `template`.
sortfield	string/array	Sortuj wynik według podanych właściwości. Możliwe wartości: `groupid`, `name`.
countOutput	boolean	Te parametry opisano w komentarzu referencyjnym.
editable	boolean	
excludeSearch	boolean	
filter	object	
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	

Parametr	Typ	Opis
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli został użyty parametr `countOutput`.

Przykłady

Pobieranie danych według nazwy

Pobierz wszystkie dane o dwóch grupach szablonów o nazwach „Templates/Databases” oraz „Templates/Modules”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "templategroup.get",
    "params": {
        "output": "extend",
        "filter": {
            "name": [
                "Templates/Databases",
                "Templates/Modules"
            ]
        }
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "groupid": "13",
            "name": "Templates/Databases",
            "uuid": "748ad4d098d447d492bb935c907f652f"
        },
        {
            "groupid": "8",
            "name": "Templates/Modules",
            "uuid": "57b7ae836ca64446ba2c296389c009b7"
        }
    ],
    "id": 1
}
```

Zobacz także

- Szablon

Źródło

CTemplateGroup::get() w *ui/include/classes/api/services/CTemplateGroup.php*.

templategroup.massadd

Opis

`object templategroup.massadd(object parameters)`

Ta metoda umożliwia jednoczesne dodanie wielu powiązanych obiektów do wszystkich podanych grup szablonów.

> **Note:**
> Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji znajduje się w sekcji Role użytkowników.

Parametry

`(object)` Parametry zawierające identyfikatory grup szablonów do zaktualizowania oraz obiekty do dodania do wszystkich grup szablonów.

Metoda akceptuje następujące parametry.

Parametr	Typ	Opis
groups	object/array	Grupy szablonów, które mają zostać zaktualizowane. Grupy szablonów muszą mieć zdefiniowaną wyłącznie właściwość `groupid`. Zachowanie parametrów: - *wymagane*
templates	object/array	Szablony do dodania do wszystkich grup szablonów. Szablony muszą mieć zdefiniowaną wyłącznie właściwość `templateid`. Zachowanie parametrów: - *wymagane*

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych grup szablonów we właściwości `groupids`.

Przykłady

Dodawanie szablonów do grup szablonów

Dodaj dwa szablony do grup szablonów o identyfikatorach 12 i 13.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "templategroup.massadd",
    "params": {
        "groups": [
            {
                "groupid": "12"
            },
            {
                "groupid": "13"
            }
        ],
        "templates": [
            {
                "templateid": "10486"
            },
            {
                "templateid": "10487"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "groupids": [
            "12",
            "13"
        ]
    },
    "id": 1
}
```

Zobacz także

- Szablon

Źródło

CTemplateGroup::massAdd() w *ui/include/classes/api/services/CTemplateGroup.php*.

templategroup.massremove

Opis

`object templategroup.massremove(object parameters)`

Ta metoda umożliwia usunięcie powiązanych obiektów z wielu grup szablonów.

Note:
Ta metoda jest dostępna tylko dla użytkowników typu *Admin* i *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object)` Parametry zawierające identyfikatory grup szablonów do zaktualizowania oraz obiekty, które powinny zostać usunięte.

Parametr	Typ	Opis
groupids	ID/array	Identyfikatory grup szablonów, które mają zostać zaktualizowane. Zachowanie parametrów: - *wymagane*
templateids	ID/array	Identyfikatory szablonów, które mają zostać usunięte ze wszystkich grup szablonów. Zachowanie parametrów: - *wymagane*

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych grup szablonów we właściwości `groupids`.

Przykłady

Usuwanie szablonów z grup szablonów

Usuń dwa szablony z podanych grup szablonów.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "templategroup.massremove",
    "params": {
        "groupids": [
            "5",
            "6"
        ],
```

```
        "templateids": [
            "30050",
            "30001"
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "groupids": [
            "5",
            "6"
        ]
    },
    "id": 1
}
```

Źródło

CTemplateGroup::massRemove() w *ui/include/classes/api/services/CTemplateGroup.php*.

templategroup.propagate

Opis

`object templategroup.propagate(object parameters)`

Ta metoda umożliwia zastosowanie uprawnień do wszystkich podgrup grup szablonów.

> **Note:**
> Ta metoda jest dostępna tylko dla typów użytkowników *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

|Parametr|Type|Opis|

|--|--|------|

|groups|object/array|Grupy szablonów do propagowania.

Grupy szablonów muszą mieć zdefiniowaną tylko właściwość `groupid`.

Zachowanie parametrów:
- *wymagane*|

|permissions|boolean|Ustaw `true`, jeśli należy propagować uprawnienia.

Zachowanie parametrów:
- *wymagane*|

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory propagowanych grup szablonów

we właściwości `groupids`.

Przykłady

Propagowanie uprawnień grupy szablonów do jej podgrup.

Propaguj uprawnienia grupy szablonów do jej podgrup.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "templategroup.propagate",
    "params": {
        "groups": [
```

```
            {
                "groupid": "15"
            }
        ],
        "permissions": true
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "groupids": [
            "15",
        ]
    },
    "id": 1
}
```

Zobacz też

- templategroup.update
- templategroup.massadd
- Szablon

Źródło

CTemplateGroup::propagate() w *ui/include/classes/api/services/CTemplateGroup.php*.

templategroup.update

Opis

`object templategroup.update(object/array templateGroups)`

Ta metoda umożliwia aktualizację istniejących grup szablonów.

Note:
Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji User roles.

Parametry

`(object/array)` Właściwości grupy szablonów, które mają zostać zaktualizowane.

Właściwość `groupid` musi być zdefiniowana dla każdej grupy szablonów, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko podane właściwości, wszystkie pozostałe pozostaną bez zmian.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych grup szablonów we właściwości `groupids`.

Przykłady

Zmiana nazwy grupy szablonów

Zmień nazwę grupy szablonów na ”Templates/Databases”

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "templategroup.update",
    "params": {
        "groupid": "7",
        "name": "Templates/Databases"
    },
```

```
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "groupids": [
            "7"
        ]
    },
    "id": 1
}
```

Źródło

CTemplateGroup::update() w *ui/include/classes/api/services/CTemplateGroup.php*.

Grupa użytkowników

Ta klasa została zaprojektowana do pracy z grupami użytkowników.

Odwołania do obiektów:

- Grupa użytkowników
- Uprawnienie
- Uprawnienie oparte na tagach

Dostępne metody:

- usergroup.create - utwórz nowe grupy użytkowników
- usergroup.delete - usuń grupy użytkowników
- usergroup.get - pobierz grupy użytkowników
- usergroup.update - zaktualizuj grupy użytkowników

Obiekt grupy użytkowników

Następujące obiekty są bezpośrednio powiązane z API `usergroup`.

Grupa użytkowników

Obiekt grupy użytkowników ma następujące właściwości.

Właściwość	Typ	Opis
usrgrpid	ID	ID grupy użytkowników. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji
name	string	Nazwa grupy użytkowników. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
debug_mode	integer	Określa, czy tryb debugowania jest włączony czy wyłączony. Możliwe wartości: 0 - *(domyślnie)* wyłączony; 1 - włączony.

Właściwość	Typ	Opis
gui_access	integer	Metoda uwierzytelniania we frontend użytkowników w grupie. Możliwe wartości: 0 - *(domyślnie)* użyj domyślnej metody uwierzytelniania systemu; 1 - użyj uwierzytelniania wewnętrznego; 2 - użyj uwierzytelniania LDAP; 3 - wyłącz dostęp do frontend.
mfa_status	integer	Określa, czy MFA jest włączone czy wyłączone dla użytkowników w grupie. Możliwe wartości: 0 - wyłączone (dla wszystkich skonfigurowanych metod MFA); 1 - włączone (dla wszystkich skonfigurowanych metod MFA).
mfaid	ID	Metoda MFA używana dla użytkowników w grupie. Zachowanie właściwości: - *obsługiwane* dla użytkowników typu *Super admin* - *obsługiwane*, jeśli `mfa_status` obiektu Authentication object jest ustawione na ”Enabled”
users_status	integer	Określa, czy grupa użytkowników jest włączona czy wyłączona. Dla użytkowników deprovisioned grupa użytkowników nie może być włączona. Możliwe wartości: 0 - *(domyślnie)* włączona; 1 - wyłączona.
userdirectoryid	ID	ID katalogu użytkowników używanego do uwierzytelniania. Zachowanie właściwości: - *obsługiwane* dla użytkowników typu *Super admin* - *obsługiwane*, jeśli `gui_access` jest ustawione na ”use the system default authentication method” lub ”use LDAP authentication”

Uprawnienie

Obiekt uprawnienia ma następujące właściwości.

Właściwość	Typ	Opis
id	ID	ID grupy hostów lub grupy szablonów, do której ma zostać dodane uprawnienie. Zachowanie właściwości: - *wymagane*
permission	integer	Poziom dostępu do grupy hostów lub grupy szablonów. Możliwe wartości: 0 - dostęp zabroniony; 2 - dostęp tylko do odczytu; 3 - dostęp do odczytu i zapisu. Zachowanie właściwości: - *wymagane* dla operacji tworzenia

Uprawnienie oparte na tagach

Obiekt uprawnienia opartego na tagach ma następujące właściwości.

Właściwość	Typ	Opis
groupid	ID	ID grupy hostów, do której należy dodać uprawnienie. Zachowanie właściwości: - *wymagane*
tag	string	Nazwa tagu.
value	string	Wartość tagu.

usergroup.create

Opis

`object usergroup.create(object/array userGroups)`

Ta metoda umożliwia tworzenie nowych grup użytkowników.

Note:
Ta metoda jest dostępna tylko dla użytkowników typu *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Grupy użytkowników do utworzenia.

Oprócz standardowych właściwości grupy użytkowników, metoda akceptuje następujące parametry.

Parametr	Typ	Opis
hostgroup_rights	object/array	Uprawnienia grup hostów do przypisania do grupy użytkowników.
templategroup_rights	object/array	Uprawnienia grup szablonów do przypisania do grupy użytkowników.
tag_filters	array	Uprawnienia oparte na tagach do przypisania do grupy użytkowników.
users	object/array	Użytkownicy do dodania do grupy użytkowników. Użytkownik musi mieć zdefiniowaną wyłącznie właściwość `userid`.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory utworzonych grup użytkowników we właściwości `usrgrpids`. Kolejność zwróconych identyfikatorów odpowiada kolejności przekazanych grup użytkowników.

Przykłady

Tworzenie grupy użytkowników

Utwórz grupę użytkowników *Operation managers* z zabronionym dostępem do grupy hostów „2” i dodaj do niej użytkownika.

Request:

```
{
    "jsonrpc": "2.0",
    "method": "usergroup.create",
    "params": {
        "name": "Operation managers",
        "hostgroup_rights": {
            "id": "2",
            "permission": 0
        },
        "users": [
            {
                "userid": "12"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "usrgrpids": [
            "20"
        ]
    },
    "id": 1
}
```

Zobacz także

- Uprawnienie

Źródło

CUserGroup::create() w *ui/include/classes/api/services/CUserGroup.php*.

usergroup.delete

Opis

`object usergroup.delete(array userGroupIds)`

Ta metoda umożliwia usunięcie grup użytkownika.

Attention:
Deprovisioned users group (grupa użytkowników określona dla `disabled_usrgrpid` w Authentication) nie może zostać usunięta.

Note:
Ta metoda jest dostępna tylko dla typu użytkownika *Super admin*. Uprawnienia do wywołania metody można cofnąć w ustawieniach roli użytkownika. Więcej informacji można znaleźć w User roles.

Parametry

`(array)` ID grup użytkowników do usunięcia.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory usuniętych grup użytkowników we właściwości `usrgrpids`.

Przykłady

Usuwanie wielu grup użytkowników

Usuń dwie grupy użytkowników.

Żądanie:

```
{
"jsonrpc": "2.0",
"method": "usergroup.delete",
"params": [
"20",
"21"
],
"id": 1
}
```

Odpowiedź:

```
{
"jsonrpc": "2.0",
"result": {
"usrgrpids": [
"20",
```

```
"21"
]
},
"id": 1
}
```

Źródło

CUserGroup::delete() w *ui/include/classes/api/services/CUserGroup.php*.

usergroup.get

Opis

`integer/array usergroup.get(object parameters)`

Ta metoda umożliwia pobieranie grup użytkowników zgodnie z podanymi parametrami.

Note:
Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywoływania tej metody mogą zostać odebrane w ustawieniach roli użytkownika. Więcej informacji znajduje się w sekcji Role użytkowników.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
mfaids	ID/array	Zwraca tylko grupy użytkowników z podanymi metodami MFA. Zachowanie parametrów: - *obsługiwane* dla użytkowników typu *Super admin*
mfa_status	integer	Zwraca tylko grupy użytkowników z podanym statusem MFA. Listę obsługiwanych statusów można znaleźć na stronie grupy użytkowników.
status	integer	Zwraca tylko grupy użytkowników z podanym statusem. Listę obsługiwanych statusów można znaleźć na stronie grupy użytkowników.
userids	ID/array	Zwraca tylko grupy użytkowników zawierające podanych użytkowników.
usrgrpids	ID/array	Zwraca tylko grupy użytkowników o podanych identyfikatorach.
selectTagFilters	query	Zwraca uprawnienia grup użytkowników oparte na tagach we właściwości `tag_filters`.
selectUsers	query	Zwraca użytkowników z grupy użytkowników we właściwości `users`. Zobacz `user.get`, aby sprawdzić ograniczenia zależne od typu użytkownika.
selectHostGroupRights	query	Zwraca uprawnienia grup użytkowników do grup hostów we właściwości `hostgroup_rights`. Listę poziomów dostępu do grup hostów można znaleźć na stronie grupy użytkowników.
selectTemplateGroupRights	query	Zwraca uprawnienia grup użytkowników do grup szablonów we właściwości `templategroup_rights`. Listę poziomów dostępu do grup szablonów można znaleźć na stronie grupy użytkowników.
limitSelects	integer	Ogranicza liczbę rekordów zwracanych przez podzapytania.

Parametr	Typ	Opis
output	query	Właściwości obiektu grupy użytkowników, które mają zostać zwrócone. Użytkownicy typu *Admin* i *User* mogą pobierać tylko następujące właściwości: `usrgrpid`, `name`, `gui_access`, `users_status`, `debug_mode`, `mfa_status`. Domyślnie: `extend`.
sortfield	string/array	Sortuje wynik według podanych właściwości. Możliwe wartości: `usrgrpid`, `name`.
countOutput	boolean	Te parametry opisano w komentarzu referencyjnym.
editable	boolean	
excludeSearch	boolean	
filter	object	
limit	integer	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli został użyty parametr `countOutput`.

Przykłady

Pobieranie włączonych grup użytkowników

Pobierz wszystkie włączone grupy użytkowników.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "usergroup.get",
    "params": {
        "output": "extend",
        "status": 0
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "usrgrpid": "7",
            "name": "Zabbix administrators",
            "gui_access": "0",
            "users_status": "0",
            "debug_mode": "1",
            "userdirectoryid": "0",
            "mfa_status": "0",
            "mfaid": "0"
        },
        {
            "usrgrpid": "8",
            "name": "Guests",
```

```
            "gui_access": "0",
            "users_status": "0",
            "debug_mode": "0",
            "userdirectoryid": "0",
            "mfa_status": "0",
            "mfaid": "0"
        },
        {
            "usrgrpid": "11",
            "name": "Enabled debug mode",
            "gui_access": "0",
            "users_status": "0",
            "debug_mode": "1",
            "userdirectoryid": "0",
            "mfa_status": "0",
            "mfaid": "0"
        },
        {
            "usrgrpid": "12",
            "name": "No access to the frontend",
            "gui_access": "2",
            "users_status": "0",
            "debug_mode": "0",
            "userdirectoryid": "0",
            "mfa_status": "0",
            "mfaid": "0"
        },
        {
            "usrgrpid": "14",
            "name": "Read only",
            "gui_access": "0",
            "users_status": "0",
            "debug_mode": "0",
            "userdirectoryid": "0",
            "mfa_status": "0",
            "mfaid": "0"
        },
        {
            "usrgrpid": "18",
            "name": "Deny",
            "gui_access": "0",
            "users_status": "0",
            "debug_mode": "0",
            "userdirectoryid": "0",
            "mfa_status": "0",
            "mfaid": "0"
        }
    ],
    "id": 1
}
```


Zobacz także

- Użytkownik

Źródło

CUserGroup::get() w *ui/include/classes/api/services/CUserGroup.php*.

usergroup.update

Opis

`object usergroup.update(object/array userGroups)`

Ta metoda umożliwia aktualizację istniejących grup użytkowników.

> **Note:**
> Ta metoda jest dostępna tylko dla typu użytkownika *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Właściwości grup użytkowników do zaktualizowania.

Właściwość `usrgrpid` musi być zdefiniowana dla każdej grupy użytkowników, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko przekazane właściwości, wszystkie pozostałe pozostaną bez zmian.

Oprócz standardowych właściwości grup użytkowników, metoda akceptuje następujące parametry.

Parametr	Typ	Opis
hostgroup_rights	object/array	Uprawnienia do grup hostów, które zastąpią bieżące uprawnienia przypisane do grupy użytkowników.
templategroup_rights	object/array	Uprawnienia do grup szablonów, które zastąpią bieżące uprawnienia przypisane do grupy użytkowników.
tag_filters	array	Uprawnienia oparte na tagach, które zastąpią bieżące uprawnienia przypisane do grupy użytkowników.
users	object/array	Użytkownicy, którzy zastąpią bieżących użytkowników przypisanych do grupy użytkowników. Użytkownik musi mieć zdefiniowaną tylko właściwość `userid`.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych grup użytkowników we właściwości `usrgrpids`.

Przykłady

Włączanie grupy użytkowników i aktualizacja uprawnień

Włącz grupę użytkowników i zapewnij jej dostęp do odczytu i zapisu do grup hostów „2” i „4”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "usergroup.update",
    "params": {
        "usrgrpid": "17",
        "users_status": "0",
        "hostgroup_rights": [
            {
                "id": "2",
                "permission": 3
            },
            {
                "id": "4",
                "permission": 3
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "usrgrpids": [
            "17"
        ]
```

```
    },
    "id": 1
}
```

Zobacz także

- Uprawnienie

Źródło

CUserGroup::update() w *ui/include/classes/api/services/CUserGroup.php*.

Historia

Ta klasa jest przeznaczona do pracy z danymi historii.

Odwołania do obiektów:

- Historia typu float
- Historia typu integer
- Historia typu string
- Historia tekstowa
- Historia logów

Dostępne metody:

- history.clear - wyczyść dane historii
- history.get - pobierz dane historii
- history.push - wyślij dane historii do serwer Zabbix

Obiekt Historia

Następujące obiekty są bezpośrednio powiązane z API `history`.

Note:
Obiekty historii różnią się w zależności od typu informacji elementu. Są tworzone przez serwer Zabbix i nie mogą być modyfikowane za pośrednictwem API.

Historia wartości zmiennoprzecinkowych

Obiekt historii wartości zmiennoprzecinkowych ma następujące właściwości.

Właściwość	Type	Opis
clock	timestamp	Czas otrzymania tej wartości.
itemid	ID	ID powiązanej pozycji.
ns	integer	Nanosekundy w momencie otrzymania wartości.
value	float	Otrzymana wartość.

Historia liczb całkowitych

Obiekt historii liczb całkowitych ma następujące właściwości.

Właściwość	Typ	Opis
clock	timestamp	Czas, kiedy ta wartość została odebrana.
itemid	ID	ID powiązanej pozycji.
ns	integer	Nanosekundy w momencie odebrania wartości.
value	integer	Odebrana wartość.

Historia ciągów znaków

Obiekt historii ciągów znaków ma następujące właściwości.

Właściwość	Type	Opis
clock	timestamp	Czas otrzymania tej wartości.
itemid	ID	ID powiązanej pozycji.
ns	integer	Nanosekundy w momencie otrzymania wartości.
value	string	Otrzymana wartość.

Historia tekstu

Obiekt historii tekstu ma następujące właściwości.

Właściwość	Typ	Opis
id	ID	ID wpisu historii.
clock	timestamp	Czas otrzymania tej wartości.
itemid	ID	ID powiązanej pozycji.
ns	integer	Nanosekundy w momencie otrzymania wartości.
value	text	Otrzymana wartość.

Historia logów

Obiekt historii logów ma następujące właściwości.

Właściwość	Typ	Opis
id	ID	ID wpisu historii.
clock	timestamp	Czas otrzymania tej wartości.
itemid	ID	ID powiązanej pozycji.
logeventid	integer	ID wpisu dziennika zdarzeń systemu Windows.
ns	integer	Nanosekundy w momencie otrzymania wartości.
severity	integer	Poziom wpisu dziennika zdarzeń systemu Windows.
source	string	Źródło wpisu dziennika zdarzeń systemu Windows.
timestamp	timestamp	Czas wpisu dziennika zdarzeń systemu Windows.
value	text	Otrzymana wartość.

Historia binarna

Obiekt historii binarnej ma następujące właściwości.

Właściwość	Typ	Opis
clock	timestamp	Czas otrzymania tej wartości.
itemid	ID	ID powiązanej pozycji.
ns	integer	Nanosekundy w momencie otrzymania wartości.
value	text	Otrzymana wartość.

Historia JSON

Obiekt historii JSON ma następujące właściwości.

Właściwość	Typ	Opis
clock	timestamp	Czas otrzymania tej wartości.
itemid	ID	ID powiązanej pozycji.
ns	integer	Nanosekundy w momencie otrzymania wartości.
value	text	Otrzymana wartość.

history.clear

Opis

```
object history.clear(array itemids)
```

Ta metoda pozwala wyczyścić historię pozycji.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania metody można odwołać w ustawieniach roli użytkownika. Więcej informacji można znaleźć w User roles.

Parametry

`(array)` Identyfikatory pozycji do wyczyszczenia.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory wyczyszczonych pozycji we właściwości `itemids`.

Przykłady

Wyczyść historię

Żądanie:

```
{
"jsonrpc": "2.0",
"metoda": "history.clear",
"params": [
"10325",
"13205"
],
"id": 1
}
```

Odpowiedź:

```
{
"jsonrpc": "2.0",
"wynik": {
"itemids": [
"10325",
"13205"
]
},
"id": 1
}
```

Źródło

CHistory::clear() w *ui/include/classes/api/services/CHistory.php*.

history.get

Opis

`integer/array history.get(object parameters)`

Ta metoda umożliwia pobranie danych historycznych zgodnie z podanymi parametrami.

> **Attention:**
> Ta metoda może zwrócić dane historyczne usuniętej encji, jeśli dane te nie zostały jeszcze usunięte przez housekeeper.

> **Note:**
> Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji znajduje się w sekcji Role użytkowników.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
history	integer	Typy obiektów historii do zwrócenia. Możliwe wartości: 0 - numeryczny float; 1 - znakowy; 2 - log; 3 - *(domyślnie)* numeryczny bez znaku; 4 - tekst; 5 - binarny; 6 - JSON.
hostids	ID/array	Zwracaj tylko historię z podanych hostów.
itemids	ID/array	Zwracaj tylko historię z podanych pozycji.
maxValueSize	integer	Maksymalna liczba bajtów do zwrócenia we właściwości `value`. Zakres możliwych wartości: 1-134217728 (1 bajt do 128MiB). Jeśli ustawiono `null`, limit nie jest stosowany. Domyślnie: 65536 (64KiB). Zachowanie parametru: - *obsługiwane*, jeśli `history` jest ustawione na ”binary” lub ”JSON”
time_from	timestamp	Zwracaj tylko wartości, które zostały odebrane po podanym czasie lub dokładnie o podanym czasie.
time_till	timestamp	Zwracaj tylko wartości, które zostały odebrane przed podanym czasem lub dokładnie o podanym czasie.
sortfield	string/array	Sortuj wynik według podanych właściwości. Możliwe wartości: `itemid`, `clock`, `ns`.
search	object	Zwracaj wyniki pasujące do podanego wzorca (bez rozróżniania wielkości liter). Akceptuje obiekt, w którym klucze są nazwami właściwości, a wartości są ciągami znaków do wyszukania. Jeśli nie podano dodatkowych opcji, zostanie wykonane wyszukiwanie `LIKE "%…%"`. Nie obsługuje wyszukiwania według `value`, jeśli `history` jest ustawione na 6 (JSON).
countOutput	boolean	Te parametry są opisane w komentarzu referencyjnym.
editable	boolean	
excludeSearch	boolean	
filter	object	
limit	integer	
output	query	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli został użyty parametr `countOutput`.

Przykłady

Pobieranie danych historii pozycji

Zwraca 10 najnowszych wartości otrzymanych z pozycji typu numeric(float).

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "history.get",
    "params": {
        "output": "extend",
        "history": 0,
        "itemids": "23296",
        "sortfield": "clock",
        "sortorder": "DESC",
        "limit": 10
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "itemid": "23296",
            "clock": "1351090996",
            "value": "0.085",
            "ns": "563157632"
        },
        {
            "itemid": "23296",
            "clock": "1351090936",
            "value": "0.16",
            "ns": "549216402"
        },
        {
            "itemid": "23296",
            "clock": "1351090876",
            "value": "0.18",
            "ns": "537418114"
        },
        {
            "itemid": "23296",
            "clock": "1351090816",
            "value": "0.21",
            "ns": "522659528"
        },
        {
            "itemid": "23296",
            "clock": "1351090756",
            "value": "0.215",
            "ns": "507809457"
        },
        {
            "itemid": "23296",
            "clock": "1351090696",
            "value": "0.255",
            "ns": "495509699"
        },
        {
            "itemid": "23296",
            "clock": "1351090636",
            "value": "0.36",
            "ns": "477708209"
        },
        {
            "itemid": "23296",
```

```
            "clock": "1351090576",
            "value": "0.375",
            "ns": "463251343"
        },
        {
            "itemid": "23296",
            "clock": "1351090516",
            "value": "0.315",
            "ns": "447947017"
        },
        {
            "itemid": "23296",
            "clock": "1351090456",
            "value": "0.275",
            "ns": "435307141"
        }
    ],
    "id": 1
}
```


Źródło

CHistory::get() w *ui/include/classes/api/services/CHistory.php*.

history.push

Opis

`object history.push(object/array itemHistoryData)`

Ta metoda umożliwia wysyłanie danych historii pozycji do serwer Zabbix.

Note:
Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji znajduje się w sekcji Role użytkowników.

Parametry

`(object/array)` Dane historii pozycji do wysłania.

Metoda obsługuje następujące parametry.

Parametr	Type	Opis
itemid	ID	ID powiązanej pozycji. Zachowanie parametru: - *wymagany*, jeśli `host` i `key` nie są ustawione
host	string	Nazwa techniczna hosta. Zachowanie parametru: - *wymagany*, jeśli `itemid` nie jest ustawione
key	string	Klucz pozycji. Zachowanie parametru: - *wymagany*, jeśli `itemid` nie jest ustawione
value	mixed	Wartość pozycji. Zachowanie parametru: - *wymagany*
clock	timestamp	Czas otrzymania wartości.
ns	integer	Nanosekundy w momencie otrzymania wartości.

Zwracane wartości

(object) Zwraca wynik operacji wysyłania danych.

Przykłady

Wysyłanie danych historii pozycji

Wyślij dane historii pozycji do serwera Zabbix dla pozycji „10600”, „10601” i „999999”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "history.push",
    "params": [
        {
            "itemid": 10600,
            "value": 0.5,
            "clock": 1690891294,
            "ns": 45440940
        },
        {
            "itemid": 10600,
            "value": 0.6,
            "clock": 1690891295,
            "ns": 312431
        },
        {
            "itemid": 10601,
            "value": "[Tue Aug 01 15:01:35 2023] [error] [client 1.2.3.4] File does not exist: /var/www/ht
        },
        {
            "itemid": 999999,
            "value": 123
        }
    ],
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "response": "success",
        "data": [
            {
                "itemid": "10600"
            },
            {
                "itemid": "10600"
            },
            {
                "itemid": "10601",
                "error": "Item is disabled."
            },
            {
                "error": "No permissions to referred object or it does not exist."
            }
        ]
    },
    "id": 1
}
```

Zobacz także

- Pozycje trapper
- pozycje HTTP agent

- Host
- Pozycja

Źródło

CHistory::push() w *ui/include/classes/api/services/CHistory.php*.

Host

Ta klasa jest przeznaczona do pracy z hostami.

Odwołania do obiektów:

- Host
- Inwentarz hosta
- Tag hosta

Dostępne metody:

- host.create - utwórz nowe hosty
- host.delete - usuń hosty
- host.get - pobierz hosty
- host.massadd - dodaj powiązane obiekty do hostów
- host.massremove - usuń powiązane obiekty z hostów
- host.update - zaktualizuj hosty

Obiekt hosta

Następujące obiekty są bezpośrednio powiązane z interfejsem API hosta.

Host

Obiekt host ma następujące właściwości.

Właściwość	Typ	Opis
hostid	ID	ID hosta. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji
host	string	Techniczna nazwa hosta. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
description	text	Opis hosta.
flags	integer	Pochodzenie hosta. Możliwe wartości: 0 - zwykły host; 4 - host przekonwertowany z prototypu. Zachowanie właściwości: - *tylko do odczytu*
inventory_mode	integer	Tryb wypełniania inwentarza hosta. Możliwe wartości: -1 - *(domyślnie)* wyłączony; 0 - ręczny; 1 - automatyczny.

Właściwość	Typ	Opis
ipmi_authtype	integer	Algorytm uwierzytelniania IPMI. Możliwe wartości: -1 - *(domyślnie)* domyślny; 0 - brak; 1 - MD2; 2 - MD5 4 - straight; 5 - OEM; 6 - RMCP+.
ipmi_password	string	Hasło IPMI.
ipmi_privilege	integer	Poziom uprawnień IPMI. Możliwe wartości: 1 - callback; 2 - *(domyślnie)* użytkownik; 3 - operator; 4 - administrator; 5 - OEM.
ipmi_username	string	Nazwa użytkownika IPMI.
maintenance_from	timestamp	Czas rozpoczęcia obowiązującego okresu utrzymaniowego. Zachowanie właściwości: - *tylko do odczytu*
maintenance_status	integer	Status obowiązującego okresu utrzymaniowego. Możliwe wartości: 0 - *(domyślnie)* brak utrzymania; 1 - utrzymanie obowiązuje. Zachowanie właściwości: - *tylko do odczytu*
maintenance_type	integer	Typ obowiązującego okresu utrzymaniowego. Możliwe wartości: 0 - *(domyślnie)* utrzymanie z gromadzeniem danych; 1 - utrzymanie bez gromadzenia danych. Zachowanie właściwości: - *tylko do odczytu*
maintenanceid	ID	ID utrzymania, które obecnie obowiązuje dla hosta. Zachowanie właściwości: - *tylko do odczytu*
name	string	Widoczna nazwa hosta. Domyślnie: wartość właściwości `host`.
monitored_by	integer	Źródło używane do monitorowania hosta. Możliwe wartości: 0 - *(domyślnie)* serwer Zabbix; 1 - proxy; 2 - grupa proxy.
proxyid	ID	ID proxy używanego do monitorowania hosta. Zachowanie właściwości: - *wymagane* jeśli `monitored_by` jest ustawione na ”Proxy”
proxy_groupid	ID	ID grupy proxy używanej do monitorowania hosta. Zachowanie właściwości: - *wymagane* jeśli `monitored_by` jest ustawione na ”Proxy group”

Właściwość	Typ	Opis
status	integer	Status i funkcja hosta. Możliwe wartości: 0 - *(domyślnie)* włączony; 1 - wyłączony.
tls_connect	integer	Połączenia do hosta. Możliwe wartości: 1 - *(domyślnie)* bez szyfrowania; 2 - PSK; 4 - certyfikat.
tls_accept	integer	Połączenia od hosta. Możliwe wartości bitmapy: 1 - *(domyślnie)* bez szyfrowania; 2 - PSK; 4 - certyfikat. To pole jest maską bitową; akceptowalna jest dowolna suma możliwych wartości bitmapy (na przykład 6 dla PSK i certyfikatu).
tls_issuer	string	Wystawca certyfikatu.
tls_subject	string	Podmiot certyfikatu.
tls_psk_identity	string	Tożsamość PSK; musi być sparowana tylko z jednym PSK (w autoregistration, hosts i proxies). Nie umieszczaj poufnych informacji w tożsamości PSK, ponieważ jest ona wysyłana przez sieć bez szyfrowania, aby poinformować odbiorcę, którego PSK użyć. Zachowanie właściwości: - *tylko do zapisu* - *wymagane* jeśli `tls_connect` jest ustawione na ”PSK” lub `tls_accept` zawiera bit ”PSK”
tls_psk	string	Klucz współdzielony (PSK); musi mieć co najmniej 32 cyfry szesnastkowe. Zachowanie właściwości: - *tylko do zapisu* - *wymagane* jeśli `tls_connect` jest ustawione na ”PSK” lub `tls_accept` zawiera bit ”PSK”
active_available	integer	Status dostępności aktywnego interfejsu hosta. Możliwe wartości: 0 - status interfejsu jest nieznany; 1 - interfejs jest dostępny; 2 - interfejs jest niedostępny. Zachowanie właściwości: - *tylko do odczytu*
assigned_proxyid	ID	ID proxy przypisanego przez serwer Zabbix, jeśli host jest monitorowany przez grupę proxy. Zachowanie właściwości: - *tylko do odczytu*

Inwentaryzacja hosta

Obiekt inwentaryzacji hosta ma następujące właściwości.

Note:
Każda właściwość ma własny unikalny numer ID, który jest używany do powiązania pól inwentaryzacji hosta z pozycjami.

ID	Właściwość	Type	Opis	Maksymalna długość
4	alias	string	Alias.	128 znaków
11	asset_tag	string	Znacznik zasobu.	64 znaki
28	chassis	string	Obudowa.	64 znaki
23	contact	string	Osoba kontaktowa.	65535 znaków dla baz danych SQL
32	contract_number	string	Numer umowy.	64 znaki
47	date_hw_decomm	string	Data wycofania sprzętu z eksploatacji.	64 znaki
46	date_hw_expiry	string	Data wygaśnięcia konserwacji sprzętu.	64 znaki
45	date_hw_install	string	Data instalacji sprzętu.	64 znaki
44	date_hw_purchase	string	Data zakupu sprzętu.	64 znaki
34	deployment_status	string	Status wdrożenia.	64 znaki
14	hardware	string	Sprzęt.	255 znaków
15	hardware_full	string	Szczegółowe informacje o sprzęcie.	65535 znaków dla baz danych SQL
39	host_netmask	string	Maska podsieci hosta.	39 znaków
38	host_networks	string	Sieci hosta.	65535 znaków dla baz danych SQL
40	host_router	string	Router hosta.	39 znaków
30	hw_arch	string	Architektura sprzętu.	32 znaki
33	installer_name	string	Nazwa instalatora.	64 znaki
24	location	string	Lokalizacja.	65535 znaków dla baz danych SQL
25	location_lat	string	Szerokość geograficzna lokalizacji.	16 znaków
26	location_lon	string	Długość geograficzna lokalizacji.	16 znaków
12	macaddress_a	string	Adres MAC A.	64 znaki
13	macaddress_b	string	Adres MAC B.	64 znaki
29	model	string	Model.	64 znaki
3	name	string	Nazwa.	128 znaków
27	notes	string	Uwagi.	65535 znaków dla baz danych SQL
41	oob_ip	string	Adres IP OOB.	39 znaków
42	oob_netmask	string	Maska podsieci hosta OOB.	39 znaków
43	oob_router	string	Router OOB.	39 znaków
5	os	string	Nazwa systemu operacyjnego.	128 znaków
6	os_full	string	Pełna nazwa systemu operacyjnego.	255 znaków
7	os_short	string	Krótka nazwa systemu operacyjnego.	128 znaków
61	poc_1_cell	string	Numer telefonu komórkowego głównego punktu kontaktowego.	64 znaki
58	poc_1_email	string	Główny adres e-mail.	128 znaków
57	poc_1_name	string	Nazwa głównego punktu kontaktowego.	128 znaków
63	poc_1_notes	string	Uwagi dotyczące głównego punktu kontaktowego.	65535 znaków dla baz danych SQL
59	poc_1_phone_a	string	Telefon A głównego punktu kontaktowego.	64 znaki
60	poc_1_phone_b	string	Telefon B głównego punktu kontaktowego.	64 znaki
62	poc_1_screen	string	Nazwa ekranowa głównego punktu kontaktowego.	64 znaki
68	poc_2_cell	string	Numer telefonu komórkowego dodatkowego punktu kontaktowego.	64 znaki
65	poc_2_email	string	Dodatkowy adres e-mail.	128 znaków
64	poc_2_name	string	Nazwa dodatkowego punktu kontaktowego.	128 znaków
70	poc_2_notes	string	Uwagi dotyczące dodatkowego punktu kontaktowego.	65535 znaków dla baz danych SQL
66	poc_2_phone_a	string	Telefon A dodatkowego punktu kontaktowego.	64 znaki
67	poc_2_phone_b	string	Telefon B dodatkowego punktu kontaktowego.	64 znaki
69	poc_2_screen	string	Nazwa ekranowa dodatkowego punktu kontaktowego.	64 znaki
8	serialno_a	string	Numer seryjny A.	64 znaki

ID	Właściwość	Type	Opis	Maksymalna długość
9	serialno_b	string	Numer seryjny B.	64 znaki
48	site_address_a	string	Adres lokalizacji A.	128 znaków
49	site_address_b	string	Adres lokalizacji B.	128 znaków
50	site_address_c	string	Adres lokalizacji C.	128 znaków
51	site_city	string	Miasto lokalizacji.	128 znaków
53	site_country	string	Kraj lokalizacji.	64 znaki
56	site_notes	string	Uwagi dotyczące lokalizacji.	65535 znaków dla baz danych SQL
55	site_rack	string	Lokalizacja szafy rack w obiekcie.	128 znaków
52	site_state	string	Stan/województwo lokalizacji.	64 znaki
54	site_zip	string	Kod ZIP/pocztowy lokalizacji.	64 znaki
16	software	string	Oprogramowanie.	255 znaków
18	software_app_a	string	Aplikacja programowa A.	64 znaki
19	software_app_b	string	Aplikacja programowa B.	64 znaki
20	software_app_c	string	Aplikacja programowa C.	64 znaki
21	software_app_d	string	Aplikacja programowa D.	64 znaki
22	software_app_e	string	Aplikacja programowa E.	64 znaki
17	software_full	string	Szczegóły oprogramowania.	65535 znaków dla baz danych SQL
10	tag	string	Znacznik.	64 znaki
1	type	string	Typ.	64 znaki
2	type_full	string	Szczegóły typu.	64 znaki
35	url_a	string	URL A.	2048 znaków
36	url_b	string	URL B.	2048 znaków
37	url_c	string	URL C.	2048 znaków
31	vendor	string	Dostawca.	64 znaki

Tag hosta

Obiekt tagu hosta ma następujące właściwości.

Właściwość	Typ	Opis
tag	string	Nazwa tagu hosta. Zachowanie właściwości: - *wymagane*
value	string	Wartość tagu hosta. Zachowanie właściwości: - *tylko do odczytu*.
automatic	integer	Typ tagu hosta. Możliwe wartości: 0 - *(domyślnie)* ręczny (tag utworzony przez użytkownika); 1 - automatyczny (tag utworzony przez wykrywanie niskopoziomowe) Zachowanie właściwości: - *tylko do odczytu*
object	integer	Typ obiektu, z którego tag został odziedziczony. Możliwe wartości: 0 - szablon. Zachowanie właściwości: - *tylko do odczytu*.
objectid	ID	ID obiektu, z którego tag został odziedziczony. Zachowanie właściwości: - *tylko do odczytu*.

host.create

Opis

`object host.create(object/array hosts)`

Ta metoda pozwala tworzyć nowe hosty.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania metody można odwołać w ustawieniach roli użytkownika. Więcej informacji można znaleźć w User roles.

Parametry

`(object/array)` Hosty do utworzenia.

Oprócz standardowych właściwości hosta, metoda akceptuje następujące parametry.

Parametr	Typ	Opis
groups	object/array	Grupy hostów, do których należy dodać host. Grupy hostów muszą mieć zdefiniowaną tylko właściwość `groupid`. Zachowanie parametru: - *wymagany*
interfaces	object/array	Interfejsy, które mają zostać utworzone dla hosta.
tags	object/array	Tagi hosta.
templates	object/array	Szablony, które mają zostać podłączone do hosta. Szablony muszą mieć zdefiniowaną tylko właściwość `templateid`.
macros	object/array	Makra użytkownika, które mają zostać utworzone dla hosta.
inventory	object	Właściwości inwentarza hosta.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory utworzonych hostów we właściwości `hostids`. Kolejność zwracanych identyfikatorów odpowiada kolejności przekazanych hostów.

Przykłady

Tworzenie hosta

Utwórz host o nazwie „Linux server” z interfejsem IP i tagami, dodaj go do grupy, podłącz do niego szablon i ustaw adresy MAC w inwentarzu hosta.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "host.create",
    "params": {
        "host": "Linux server",
        "interfaces": [
            {
                "type": 1,
                "main": 1,
                "useip": 1,
                "ip": "192.168.3.1",
                "dns": "",
                "port": "10050"
            }
        ],
        "groups": [
            {
                "groupid": "50"
            }
        ],
        "tags": [
```

```
            {
                "tag": "host-name",
                "value": "linux-server"
            }
        ],
        "templates": [
            {
                "templateid": "20045"
            }
        ],
        "macros": [
            {
                "macro": "{$USER_ID}",
                "value": "123321"
            },
            {
                "macro": "{$USER_LOCATION}",
                "value": "0:0:0",
                "description": "latitude, longitude and altitude coordinates"
            }
        ],
        "inventory_mode": 0,
        "inventory": {
            "macaddress_a": "01234",
            "macaddress_b": "56768"
        }
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "hostids": [
            "107819"
        ]
    },
    "id": 1
}
```

Tworzenie hosta z interfejsem SNMP

Utwórz host o nazwie ”SNMP host” z interfejsem SNMPv3 ze szczegółami.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "host.create",
    "params": {
        "host": "SNMP host",
        "interfaces": [
            {
                "type": 2,
                "main": 1,
                "useip": 1,
                "ip": "127.0.0.1",
                "dns": "",
                "port": "161",
                "details": {
                    "version": 3,
                    "bulk": 0,
                    "securityname": "mysecurityname",
```

```
                    "contextname": "",
                    "securitylevel": 1
                }
            }
        ],
        "groups": [
            {
                "groupid": "4"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "hostids": [
            "10658"
        ]
    },
    "id": 1
}
```

Tworzenie hosta z szyfrowaniem PSK

Utwórz host o nazwie „PSK host" ze skonfigurowanym szyfrowaniem PSK. Pamiętaj, że host musi być wstępnie skonfigurowany do używania PSK.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "host.create",
    "params": {
        "host": "PSK host",
        "interfaces": [
            {
                "type": 1,
                "ip": "192.168.3.1",
                "dns": "",
                "port": "10050",
                "useip": 1,
                "main": 1
            }
        ],
        "groups": [
            {
                "groupid": "2"
            }
        ],
        "tls_accept": 2,
        "tls_connect": 2,
        "tls_psk_identity": "PSK 001",
        "tls_psk": "1f87b595725ac58dd977beef14b97461a7c1045b9a1c963065002c5473194952"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
```

```
        "hostids": [
            "10590"
        ]
    },
    "id": 1
}
```

Tworzenie hosta monitorowanego przez proxy

Utwórz host, który będzie monitorowany przez proxy o ID „1”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "host.create",
    "params": {
        "host": "Host monitored by proxy",
        "groups": [
            {
                "groupid": "2"
            }
        ],
        "monitored_by": 1,
        "proxyid": 1
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "hostids": [
            "10591"
        ]
    },
    "id": 1
}
```

Tworzenie hosta monitorowanego przez grupę proxy

Utwórz host, który będzie monitorowany przez grupę proxy o ID „1”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "host.create",
    "params": {
        "host": "Host monitored by proxy group",
        "groups": [
            {
                "groupid": "2"
            }
        ],
        "monitored_by": 2,
        "proxy_groupid": 1
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
```

```
        "hostids": [
            "10592"
        ]
    },
    "id": 1
}
```

Zobacz także

- Grupa hostów
- Szablon
- Makro użytkownika
- Interfejs hosta
- Inwentaryzacja hosta
- Tag hosta
- Proxy
- Grupa proxy

Źródło

CHost::create() w *ui/include/classes/api/services/CHost.php*.

host.delete

Opis

`object host.delete(array hosts)`

Ta metoda umożliwia usuwanie hostów.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania metody można odwołać w ustawieniach roli użytkownika. Więcej informacji można znaleźć w User roles.

Parametry

`(array)` ID hostów do usunięcia.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory usuniętych hostów w właściwości `hostids`.

Przykłady

Usuwanie wielu hostów

Usuń dwa hosty.

Żądanie:

```
{
"jsonrpc": "2.0",
"method": "host.delete",
"params": [
"13",
"32"
],
"id": 1
}
```

Odpowiedź:

```
{
"jsonrpc": "2.0",
"result": {
"hostids": [
"13",
"32"
]
```

```
},
"id": 1
}
```

Źródło

CHost::delete() w *ui/include/classes/api/services/CHost.php*.

host.get

Opis

`integer/array host.get(object parameters)`

Metoda pozwala na pobieranie hostów zgodnie z podanymi parametrami.

> **Note:**
> Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywołania metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w User roles.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
groupids	ID/array	Zwracaj tylko hosty należące do podanych grup.
dserviceids	ID/array	Zwracaj tylko hosty powiązane z podanymi wykrytymi usługami.
graphids	ID/array	Zwracaj tylko hosty, które mają podane wykresy.
hostids	ID/array	Zwracaj tylko hosty o podanych identyfikatorach hostów.
httptestids	ID/array	Zwracaj tylko hosty, które mają podane testy WWW.
interfaceids	ID/array	Zwracaj tylko hosty używające podanych interfejsów.
itemids	ID/array	Zwracaj tylko hosty, które mają podane pozycje.
maintenanceids	ID/array	Zwracaj tylko hosty objęte podanymi okresami konserwacji.
monitored_hosts	flag	Zwracaj tylko monitorowane hosty.
proxyids	ID/array	Zwracaj tylko hosty monitorowane przez podane proxy.
proxy_groupids	ID/array	Zwracaj tylko hosty monitorowane przez podane grupy proxy.
templated_hosts	flag	Zwracaj zarówno hosty, jak i szablony.
templateids	ID/array	Zwracaj tylko hosty połączone z podanymi szablonami.
triggerids	ID/array	Zwracaj tylko hosty, które mają podane wyzwalacze.
with_items	flag	Zwracaj tylko hosty, które mają pozycje. Nadpisuje parametry `with_monitored_items` i `with_simple_graph_items`.
with_item_prototypes	flag	Zwracaj tylko hosty, które mają prototypy pozycji. Nadpisuje parametr `with_simple_graph_item_prototypes`.
with_simple_graph_item_prototypes	flag	Zwracaj tylko hosty, które mają prototypy pozycji włączone do tworzenia i z numerycznym typem informacji.
with_graphs	flag	Zwracaj tylko hosty, które mają wykresy.
with_graph_prototypes	flag	Zwracaj tylko hosty, które mają prototypy wykresów.
with_httptests	flag	Zwracaj tylko hosty, które mają testy WWW. Nadpisuje parametr `with_monitored_httptests`.
with_monitored_httptests	flag	Zwracaj tylko hosty, które mają włączone testy WWW.
with_monitored_items	flag	Zwracaj tylko hosty, które mają włączone pozycje. Nadpisuje parametr `with_simple_graph_items`.
with_monitored_triggers	flag	Zwracaj tylko hosty, które mają włączone wyzwalacze. Wszystkie pozycje używane w wyzwalaczu również muszą być włączone.
with_simple_graph_items	flag	Zwracaj tylko hosty, które mają pozycje z numerycznym typem informacji.

Parametr	Typ	Opis
with_triggers	flag	Zwracaj tylko hosty, które mają wyzwalacze. Nadpisuje parametr `with_monitored_triggers`.
withProblemsSuppressed	boolean	Jeśli ustawiono na `true`, zwracaj tylko hosty z wyciszonymi problemami.
evaltype	integer	Metoda oceny tagów. Możliwe wartości: 0 - *(domyślnie)* And/Or; 2 - Or.
severities	integer/array	Zwracaj hosty, które mają tylko problemy o podanych poziomach ważności. Dotyczy tylko sytuacji, gdy obiektem problemu jest wyzwalacz.
tags	object/array	Zwracaj tylko hosty z podanymi tagami. Format: `[{"tag": "<tag>", "value": "<value>", "operator": "<operator>"}, ...]`. Pusta tablica zwraca wszystkie hosty. Możliwe wartości operatora: 0 - *(domyślnie)* Zawiera; 1 - Równe; 2 - Nie zawiera; 3 - Nie jest równe; 4 - Istnieje; 5 - Nie istnieje.
inheritedTags	boolean	Zwracaj hosty, które mają podane `tags` również we wszystkich połączonych z nimi szablonach. Możliwe wartości: `true` - połączone szablony również muszą mieć podane `tags`; `false` - *(domyślnie)* tagi połączonych szablonów są ignorowane.
selectDiscoveryData	query	Zwracaj właściwość `discoveryData` z danymi obiektu wykrywania hosta. Obiekt wykrywania hosta łączy wykryty host z prototypem hosta, z którego został wykryty. Ma następujące właściwości: `host` - `(string)` identyfikator hosta; `parent_hostid` - `(string)` identyfikator prototypu hosta, z którego host został utworzony; `status` - `(int)` status wykrywania hosta: 0 - *(domyślnie)* host jest wykryty, 1 - host nie jest już wykryty; `ts_delete` - `(timestamp)` czas, kiedy host, który nie jest już wykryty, zostanie usunięty; `ts_disable` - `(timestamp)` czas, kiedy host, który nie jest już wykryty, zostanie wyłączony; `disable_source` - `(int)` wskaźnik określający, czy host został wyłączony przez regułę LLD czy ręcznie: 0 - *(domyślnie)* wyłączony automatycznie, 1 - wyłączony przez regułę LLD.
selectDiscoveryRule	query	Zwracaj właściwość `discoveryRule` z regułą wykrywania niskiego poziomu, która utworzyła host (z prototypu hosta w monitorowaniu VMware).
selectDiscoveryRules	query	Zwracaj właściwość `discoveryRules` z regułami LLD hosta. Obsługuje `count`.
selectGraphs	query	Zwracaj właściwość `graphs` z wykresami hosta. Obsługuje `count`.
selectHostGroups	query	Zwracaj właściwość `hostgroups` z danymi grup hostów, do których należy host.

Parametr	Typ	Opis
selectHttpTests	query	Zwracaj właściwość `httpTests` ze scenariuszami WWW hosta. Obsługuje `count`.
selectInterfaces	query	Zwracaj właściwość `interfaces` z interfejsami hosta. Obsługuje `count`.
selectInventory	query	Zwracaj właściwość `inventory` z danymi inwentarza hosta.
selectItems	query	Zwracaj właściwość `items` z pozycjami hosta. Obsługuje `count`.
selectMacros	query	Zwracaj właściwość `macros` z makrami hosta.
selectParentTemplates	query	Zwracaj właściwość `parentTemplates` z szablonami, z którymi host jest połączony. Oprócz pól obiektu Template zawiera ona `link_type` - `(integer)` sposób, w jaki szablon jest połączony z hostem. Możliwe wartości: 0 - *(domyślnie)* połączony ręcznie; 1 - połączony automatycznie przez LLD. Obsługuje `count`.
selectDashboards	query	Zwracaj właściwość `dashboards`. Obsługuje `count`.
selectTags	query	Zwracaj właściwość `tags` z tagami hosta.
selectInheritedTags	query	Zwracaj właściwość `inheritedTags` z tagami obecnymi we wszystkich szablonach połączonych z hostem.
selectTriggers	query	Zwracaj właściwość `triggers` z wyzwalaczami hosta. Obsługuje `count`.
selectValueMaps	query	Zwracaj właściwość `valuemaps` z mapowaniami wartości hosta.
filter	object	Zwracaj tylko te wyniki, które dokładnie odpowiadają podanemu filtrowi. Akceptuje obiekt, w którym klucze są nazwami właściwości, a wartościami są pojedyncza wartość lub tablica wartości do dopasowania. Nie obsługuje właściwości typu danych `text` data type. Obsługuje dodatkowe właściwości: właściwości interfejsu hosta.
limitSelects	integer	Ogranicza liczbę rekordów zwracanych przez podzapytania. Dotyczy następujących podzapytań: `selectParentTemplates` - wyniki będą sortowane według `host`; `selectInterfaces`; `selectItems` - sortowane według `name`; `selectDiscoveryRules` - sortowane według `name`; `selectTriggers` - sortowane według `description`; `selectGraphs` - sortowane według `name`; `selectDashboards` - sortowane według `name`.
search	object	Zwracaj wyniki pasujące do podanego wzorca (bez rozróżniania wielkości liter). Akceptuje obiekt, w którym klucze są nazwami właściwości, a wartościami są ciągi znaków do wyszukania. Jeśli nie podano dodatkowych opcji, zostanie wykonane wyszukiwanie `LIKE "%…%"`. Obsługuje tylko właściwości typu danych `string` i `text` data type. Obsługuje dodatkowe właściwości: właściwości interfejsu hosta.

Parametr	Typ	Opis
searchInventory	object	Zwracaj hosty, których dane inwentarza pasują do podanego wzorca (bez rozróżniania wielkości liter). Akceptuje obiekt, w którym klucze są nazwami właściwości, a wartościami są ciągi znaków do wyszukania. Jeśli nie podano dodatkowych opcji, zostanie wykonane wyszukiwanie `LIKE "%…%"`. Obsługuje tylko właściwości typu danych `string` i `text` data type.
sortfield	string/array	Sortuj wynik według podanych właściwości. Możliwe wartości: `hostid`, `host`, `name`, `status`.
countOutput	boolean	Te parametry są opisane w komentarzu referencyjnym.
editable	boolean	
excludeSearch	boolean	
limit	integer	
output	query	
preservekeys	boolean	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	
selectDiscoveries	query	Zwracaj właściwość `discoveries` z regułami wykrywania niskiego poziomu hosta. Obsługuje `count`.
selectHostDiscovery	query	To zapytanie jest **przestarzałe**; użyj zamiast tego `selectDiscoveryRules`. Zwracaj właściwość `hostDiscovery` z danymi obiektu wykrywania hosta. To zapytanie jest **przestarzałe**; użyj zamiast tego `selectDiscoveryData`.

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli użyto parametru `countOutput`.

Przykłady

Pobieranie danych według nazwy

Pobierz wszystkie dane o dwóch hostach o nazwach „Zabbix server” i „Linux server”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "host.get",
    "params": {
        "filter": {
            "host": [
                "Zabbix server",
                "Linux server"
            ]
        }
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "hostid": "10160",
            "proxyid": "0",
            "host": "Zabbix server",
            "status": "0",
            "ipmi_authtype": "-1",
            "ipmi_privilege": "2",
            "ipmi_username": "",
            "ipmi_password": "",
            "maintenanceid": "0",
            "maintenance_status": "0",
            "maintenance_type": "0",
            "maintenance_from": "0",
            "name": "Zabbix server",
            "flags": "0",
            "description": "Serwer monitorowania Zabbix.",
            "tls_connect": "1",
            "tls_accept": "1",
            "tls_issuer": "",
            "tls_subject": "",
            "proxy_groupid": "0",
            "monitored_by": "0",
            "inventory_mode": "1",
            "active_available": "1",
            "assigned_proxyid": "0"
        },
        {
            "hostid": "10167",
            "proxyid": "0",
            "host": "Linux server",
            "status": "0",
            "ipmi_authtype": "-1",
            "ipmi_privilege": "2",
            "ipmi_username": "",
            "ipmi_password": "",
            "maintenanceid": "0",
            "maintenance_status": "0",
            "maintenance_type": "0",
            "maintenance_from": "0",
            "name": "Linux server",
            "flags": "0",
            "description": "",
            "tls_connect": "1",
            "tls_accept": "1",
            "tls_issuer": "",
            "tls_subject": "",
            "proxy_groupid": "0",
            "monitored_by": "0",
            "inventory_mode": "1",
            "active_available": "1",
            "assigned_proxyid": "0"
        }
    ],
    "id": 1
}
```


Pobieranie grup hostów

Pobierz grupy hostów, do których należy host „Zabbix server”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "host.get",
    "params": {
        "output": ["hostid"],
        "selectHostGroups": "extend",
        "filter": {
            "host": [
                "Zabbix server"
            ]
        }
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "hostid": "10085",
            "hostgroups": [
                {
                    "groupid": "2",
                    "name": "Linux servers",
                    "flags": "0",
                    "uuid": "dc579cd7a1a34222933f24f52a68bcd8"
                },
                {
                    "groupid": "4",
                    "name": "Zabbix servers",
                    "flags": "0",
                    "uuid": "6f6799aa69e844b4b3918f779f2abf08"
                }
            ]
        }
    ],
    "id": 1
}
```

Pobieranie podłączonych szablonów

Pobierz identyfikatory i nazwy szablonów podłączonych do hosta „10084”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "host.get",
    "params": {
        "output": ["hostid"],
        "selectParentTemplates": [
            "templateid",
            "name"
        ],
        "hostids": "10084"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
```

```
        {
            "hostid": "10084",
            "parentTemplates": [
                {
                    "name": "Linux",
                    "templateid": "10001"
                },
                {
                    "name": "Zabbix Server",
                    "templateid": "10047"
                }
            ]
        }
    ],
    "id": 1
}
```

Pobieranie hostów według szablonu

Pobierz hosty, które mają podłączony szablon „10001” (*Linux by Zabbix agent*).

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "host.get",
    "params": {
        "output": ["hostid", "name"],
        "templateids": "10001"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "templateid": "10001",
            "hosts": [
                {
                    "hostid": "10084",
                    "name": "Zabbix server"
                },
                {
                    "hostid": "10603",
                    "name": "Host 1"
                },
                {
                    "hostid": "10604",
                    "name": "Host 2"
                }
            ]
        }
    ],
    "id": 1
}
```

Wyszukiwanie według danych inwentaryzacyjnych hosta

Pobierz hosty, które zawierają „Linux” w polu inwentaryzacyjnym hosta „OS”.

Żądanie:

```
{
    "jsonrpc": "2.0",
```

```
    "method": "host.get",
    "params": {
        "output": [
            "host"
        ],
        "selectInventory": [
            "os"
        ],
        "searchInventory": {
            "os": "Linux"
        }
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "hostid": "10084",
            "host": "Zabbix server",
            "inventory": {
                "os": "Linux Ubuntu"
            }
        },
        {
            "hostid": "10107",
            "host": "Linux server",
            "inventory": {
                "os": "Linux Mint"
            }
        }
    ],
    "id": 1
}
```

Wyszukiwanie według tagów hosta

Pobierz hosty, które mają tag ”host-name” równy ”linux-server”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "host.get",
    "params": {
        "output": ["hostid"],
        "selectTags": "extend",
        "evaltype": 0,
        "tags": [
            {
                "tag": "host-name",
                "value": "linux-server",
                "operator": 1
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
```

```
    "result": [
        {
            "hostid": "10085",
            "tags": [
                {
                    "tag": "host-name",
                    "value": "linux-server",
                    "automatic": "0"
                },
                {
                    "tag": "os",
                    "value": "rhel-7",
                    "automatic": "0"
                }
            ]
        }
    ],
    "id": 1
}
```

Pobierz hosty, które mają te tagi nie tylko na poziomie hosta, ale także w swoich podłączonych nadrzędnych szablonach.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "host.get",
    "params": {
        "output": ["name"],
        "tags": [
            {
                "tag": "os",
                "value": "rhel-7",
                "operator": 1
            }
        ],
        "inheritedTags": true
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "hostid": "10623",
            "name": "PC room 1"
        },
        {
            "hostid": "10601",
            "name": "Office"
        }
    ],
    "id": 1
}
```

Pobierz hosty z wyłączeniem tych, które mają tag ”component”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "host.get",
    "params": {
```

```
        "output": ["hostid"],
        "selectTags": "extend",
        "evaltype": 0,
        "tags": [
            {
                "tag": "component",
                "value": "",
                "operator": 5
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "hostid": "10084",
            "tags": [
                {
                    "tag": "class",
                    "value": "os",
                    "automatic": "0"
                },
                {
                    "tag": "target",
                    "value": "linux",
                    "automatic": "0"
                }
            ]
        },
        {
            "hostid": "10629",
            "tags": [
                {
                    "tag": "class",
                    "value": "application",
                    "automatic": "0"
                },
                {
                    "tag": "target",
                    "value": "browser",
                    "automatic": "0"
                }
            ]
        }
    ],
    "id": 1
}
```

Wyszukiwanie hosta za pomocą tagów i tagów szablonu

Pobierz host z tagami oraz wszystkimi tagami, które są powiązane z nadrzędnymi szablonami.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "host.get",
    "params": {
        "output": ["name"],
        "hostids": 10502,
```

```
        "selectTags": ["tag", "value"],
        "selectInheritedTags": ["tag", "value"]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "hostid": "10502",
            "name": "Desktop",
            "tags": [
                {
                    "tag": "host-name",
                    "value": "linux-server"
                },
                {
                    "tag": "os",
                    "value": "rhel-7"
                }
            ],
            "inheritedTags": [
                {
                    "tag": "class",
                    "value": "os"
                },
                {
                    "tag": "target",
                    "value": "linux"
                },
                {
                    "tag": "os",
                    "value": "rhel-7"
                }
            ]
        }
    ],
    "id": 1
}
```

Wyszukiwanie hostów według ważności problemu

Pobierz hosty, które mają problemy o ważności „Disaster”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "host.get",
    "params": {
        "output": ["name"],
        "severities": 5
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "hostid": "10160",
```

```
            "name": "Zabbix server"
        }
    ],
    "id": 1
}
```

Pobierz hosty, które mają problemy o ważności „Average” i „High”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "host.get",
    "params": {
        "output": ["name"],
        "severities": [3, 4]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "hostid": "20170",
            "name": "Database"
        },
        {
            "hostid": "20183",
            "name": "workstation"
        }
    ],
    "id": 1
}
```

Pobieranie pozycji hosta

Pobierz pozycje dla hosta „Zabbix server”. Żądanie jest ograniczone do właściwości pozycji `itemid`, `name` i `status`. Ze względu na duży rozmiar odpowiedzi w przykładzie pokazano tylko podzbiór pozycji.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "host.get",
    "params": {
        "output": ["hostid"],
        "selectItems": ["itemid","name","status"],
        "filter": {
            "host": [
                "Zabbix server"
            ]
        }
    },
    "id": 1
}
```

Odpowiedź:

```
{
  "jsonrpc": "2.0",
  "result": [
    {
      "hostid": "10084",
      "items": [
```

```
    {
      "itemid": "42227",
      "name": "Host name of Zabbix agent running",
      "status": "0"
    },
    {
      "itemid": "42237",
      "name": "Zabbix agent ping",
      "status": "0"
    },
    {
      "itemid": "42250",
      "name": "Version of Zabbix agent running",
      "status": "0"
    },
    {
      "itemid": "42251",
      "name": "Maximum number of open file descriptors",
      "status": "0"
    },
    {
      "itemid": "42252",
      "name": "Maximum number of processes",
      "status": "0"
    },
    {
      "itemid": "69869",
      "name": "Interface enp0s3: Inbound packets discarded",
      "status": "0"
    },
    {
      "itemid": "69870",
      "name": "Interface enp0s3: Inbound packets with errors",
      "status": "0"
    },
    {
      "itemid": "69871",
      "name": "Interface enp0s3: Bits received",
      "status": "0"
    },
    {
      "itemid": "69872",
      "name": "Interface enp0s3: Outbound packets discarded",
      "status": "0"
    },
    {
      "itemid": "69873",
      "name": "Interface enp0s3: Outbound packets with errors",
      "status": "0"
    },
    {
      "itemid": "69874",
      "name": "Interface enp0s3: Bits sent",
      "status": "0"
    },
    {
      "itemid": "42253",
      "name": "Number of processes",
      "status": "0"
    },
    {
      "itemid": "42254",
```

```
            "name": "Number of running processes",
            "status": "0"
          },
          {
            "itemid": "42255",
            "name": "System boot time",
            "status": "0"
          }
        ]
      }
    ],
    "id": 1
}
```


Zobacz także

- Grupa hostów
- Szablon
- Makro użytkownika
- Interfejs hosta
- Proxy
- Grupa proxy

Źródło

CHost::get() w *ui/include/classes/api/services/CHost.php*.

host.massadd

Opis

`object host.massadd(object parameters)`

Ta metoda umożliwia jednoczesne dodanie wielu powiązanych obiektów do wszystkich podanych hostów.

Note:
Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object)` Parametry zawierające identyfikatory hostów do zaktualizowania oraz obiekty do dodania do wszystkich hostów.

Metoda akceptuje następujące parametry.

Parametr	Type	Opis
hosts	object/array	Hosty do zaktualizowania. Hosty muszą mieć zdefiniowaną wyłącznie właściwość `hostid`. Zachowanie parametrów: - *wymagane*
groups	object/array	Grupy hostów do dodania do podanych hostów. Grupy hostów muszą mieć zdefiniowaną wyłącznie właściwość `groupid`.
interfaces	object/array	Interfejsy hostów do utworzenia dla podanych hostów.
macros	object/array	Makra użytkownika do utworzenia dla podanych hostów.
templates	object/array	Szablony do podłączenia do podanych hostów. Szablony muszą mieć zdefiniowaną wyłącznie właściwość `templateid`.

Zwracane wartości

(object) Zwraca obiekt zawierający identyfikatory zaktualizowanych hostów we właściwości hostids.

Przykłady

Dodawanie makr

Dodaj dwa nowe makra do dwóch hostów.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "host.massadd",
    "params": {
        "hosts": [
            {
                "hostid": "10160"
            },
            {
                "hostid": "10167"
            }
        ],
        "macros": [
            {
                "macro": "{$TEST1}",
                "value": "MACROTEST1"
            },
            {
                "macro": "{$TEST2}",
                "value": "MACROTEST2",
                "description": "Opis testowy"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "hostids": [
            "10160",
            "10167"
        ]
    },
    "id": 1
}
```

Zobacz także

- host.update
- Grupa hostów
- Szablon
- Makro użytkownika
- Interfejs hosta

Źródło

CHost::massAdd() w *ui/include/classes/api/services/CHost.php*.

host.massremove

Opis

`object host.massremove(object parameters)`

Ta metoda umożliwia usuwanie powiązanych obiektów z wielu hostów.

Note:
Ta metoda jest dostępna tylko dla użytkowników typu *Admin* i *Super admin*. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object)` Parametry zawierające identyfikatory hostów do zaktualizowania oraz obiekty, które należy usunąć.

Parametr	Typ	Opis
hostids	ID/array	Identyfikatory hostów, które mają zostać zaktualizowane. Zachowanie parametru: - *wymagany*
groupids	ID/array	Identyfikatory grup hostów, z których należy usunąć podane hosty.
interfaces	object/array	Interfejsy hosta do usunięcia z podanych hostów. Obiekt interfejsu hosta musi mieć zdefiniowane tylko właściwości `ip`, `dns` i `port`.
macros	string/array	Makra użytkownika do usunięcia z podanych hostów.
templateids	ID/array	Identyfikatory szablonów, które należy odłączyć od podanych hostów.
templateids_clear	ID/array	Identyfikatory szablonów, które należy odłączyć i wyczyścić z podanych hostów.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych hostów we właściwości `hostids`.

Przykłady

Odłączanie szablonów

Odłącz szablon od dwóch hostów i usuń wszystkie encje pochodzące z szablonu.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "host.massremove",
    "params": {
        "hostids": ["69665", "69666"],
        "templateids_clear": "325"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "hostids": [
            "69665",
            "69666"
        ]
    },
    "id": 1
}
```

Zobacz także

- host.update
- Makro użytkownika
- Interfejs hosta

Źródło

CHost::massRemove() w *ui/include/classes/api/services/CHost.php*.

host.update

Opis

`object host.update(object/array hosts)`

Ta metoda umożliwia aktualizację istniejących hostów.

> **Note:**
> Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji User roles.

Parametry

`(object/array)` Właściwości hosta do zaktualizowania.

Właściwość `hostid` musi być zdefiniowana dla każdego hosta, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko podane właściwości, wszystkie pozostałe pozostaną bez zmian.

Należy jednak pamiętać, że aktualizacja technicznej nazwy hosta spowoduje również aktualizację widocznej nazwy hosta (jeśli nie została podana osobno) na wartość technicznej nazwy hosta.

Oprócz standardowych właściwości hosta, metoda akceptuje następujące parametry.

Parameter	Type	Description
groups	object/array	Grupy hostów zastępujące bieżące grupy hostów, do których należy host. Wszystkie grupy hostów, które nie zostały wymienione w żądaniu, zostaną odłączone. Grupy hostów muszą mieć zdefiniowaną wyłącznie właściwość `groupid`.
interfaces	object/array	Interfejsy hosta zastępujące bieżące interfejsy hosta. Wszystkie interfejsy, które nie zostały wymienione w żądaniu, zostaną usunięte.
tags	object/array	Tagi hosta zastępujące bieżące tagi hosta. Wszystkie tagi, które nie zostały wymienione w żądaniu, zostaną usunięte.
inventory	object	Właściwości inwentarza hosta.
macros	object/array	Makra użytkownika zastępujące bieżące makra użytkownika. Wszystkie makra, które nie zostały wymienione w żądaniu, zostaną usunięte.
templates	object/array	Szablony zastępujące aktualnie podłączone szablony. Wszystkie szablony, które nie zostały wymienione w żądaniu, zostaną jedynie odłączone. Szablony muszą mieć zdefiniowaną wyłącznie właściwość `templateid`.
templates_clear	object/array	Szablony do odłączenia i wyczyszczenia z hosta. Szablony muszą mieć zdefiniowaną wyłącznie właściwość `templateid`.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych hostów we właściwości `hostids`.

Przykłady

Włączanie monitorowania hosta

Włącz monitorowanie hosta, czyli ustaw jego status na „0”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "host.update",
    "params": {
        "hostid": "10126",
        "status": 0
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "hostids": [
            "10126"
        ]
    },
    "id": 1
}
```

Włączanie wielu hostów

Włącz monitorowanie dwóch hostów, tj. ustaw ich status na „0”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "host.update",
    "params": [
        {
            "hostid": "10127",
            "status": 0
        },
        {
            "hostid": "10128",
            "status": 0
        }
    ],
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "hostids": [
            "10127",
            "10128"
        ]
    },
    "id": 1
}
```

Odłączanie szablonów

Odłącz i wyczyść dwa szablony z hosta.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "host.update",
    "params": {
        "hostid": "10126",
```

```
        "templates_clear": [
            {
                "templateid": "10124"
            },
            {
                "templateid": "10125"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "hostids": [
            "10126"
        ]
    },
    "id": 1
}
```

Aktualizowanie makr hosta

Zastąp wszystkie makra hosta dwoma nowymi.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "host.update",
    "params": {
        "hostid": "10126",
        "macros": [
            {
                "macro": "{$PASS}",
                "value": "password"
            },
            {
                "macro": "{$DISC}",
                "value": "sda",
                "description": "Updated description"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "hostids": [
            "10126"
        ]
    },
    "id": 1
}
```

Aktualizowanie inwentarza hosta

Zmień tryb inwentarza i dodaj lokalizację

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "host.update",
    "params": {
        "hostid": "10387",
        "inventory_mode": 0,
        "inventory": {
            "location": "Latvia, Riga"
        }
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "hostids": [
            "10387"
        ]
    },
    "id": 1
}
```

Aktualizowanie tagów hosta

Zastąp wszystkie tagi hosta nowym tagiem.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "host.update",
    "params": {
        "hostid": "10387",
        "tags": {
            "tag": "os",
            "value": "rhel-7"
        }
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "hostids": [
            "10387"
        ]
    },
    "id": 1
}
```

Aktualizowanie makr wykrytego hosta

Przekształć makro utworzone przez regułę wykrywania z trybu „automatic” na „manual” i zmień jego wartość na „new-value”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "host.update",
    "params": {
        "hostid": "10387",
        "macros": {
```

```
            "hostmacroid": "5541",
            "value": "new-value",
            "automatic": "0"
        }
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "hostids": [
            "10387"
        ]
    },
    "id": 1
}
```

Aktualizacja szyfrowania hosta

Zaktualizuj host „10590”, aby używał wyłącznie szyfrowania PSK dla połączeń z hosta do serwera Zabbix, oraz zmień tożsamość PSK i klucz PSK. Zwróć uwagę, że host musi być wstępnie skonfigurowany do używania PSK.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "host.update",
    "params": {
        "hostid": "10590",
        "tls_connect": 1,
        "tls_accept": 2,
        "tls_psk_identity": "PSK 002",
        "tls_psk": "e560cb0d918d26d31b4f642181f5f570ad89a390931102e5391d08327ba434e9"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "hostids": [
            "10590"
        ]
    },
    "id": 1
}
```

Zobacz także

- host.massadd
- host.massremove
- Grupa hostów
- Szablon
- Makro użytkownika
- Interfejs hosta
- Inwentarz hosta
- Tag hosta
- Proxy
- Grupa proxy

Źródło

CHost::update() w *ui/include/classes/api/services/CHost.php*.

Interfejs hosta

Ta klasa jest przeznaczona do pracy z interfejsami hosta.

Odwołania do obiektów:

- Interfejs hosta
  - Szczegóły

Dostępne metody:

- hostinterface.create - tworzenie nowych interfejsów hosta
- hostinterface.delete - usuwanie interfejsów hosta
- hostinterface.get - pobieranie interfejsów hosta
- hostinterface.massadd - dodawanie interfejsów hosta do hostów
- hostinterface.massremove - usuwanie interfejsów hosta z hostów
- hostinterface.update - aktualizowanie interfejsów hosta

Obiekt interfejsu hosta

Następujące obiekty są bezpośrednio powiązane z API `hostinterface`.

Interfejs hosta

Obiekt interfejsu hosta ma następujące właściwości.

Attention:
Należy pamiętać, że zarówno właściwości `ip`, jak i `dns` są *wymagane* dla operacji tworzenia. Jeśli nie chcesz używać DNS, ustaw go jako pusty ciąg znaków.

Właściwość	Type	Opis
interfaceid	ID	ID interfejsu. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji
available	integer	Dostępność interfejsu hosta. Możliwe wartości: 0 - *(domyślnie)* nieznana; 1 - dostępny; 2 - niedostępny. Zachowanie właściwości: - *tylko do odczytu*
hostid	ID	ID hosta, do którego należy interfejs. Zachowanie właściwości: - *stała* - *wymagane* dla operacji tworzenia
type	integer	Typ interfejsu. Możliwe wartości: 1 - Agent; 2 - SNMP; 3 - IPMI; 4 - JMX. Zachowanie właściwości: - *wymagane* dla operacji tworzenia

Właściwość	Type	Opis
ip	string	Adres IP używany przez interfejs. Może być pusty, jeśli połączenie jest nawiązywane przez DNS. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
dns	string	Nazwa DNS używana przez interfejs. Może być pusta, jeśli połączenie jest nawiązywane przez IP. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
port	string	Numer portu używany przez interfejs. Może zawierać makra użytkownika. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
useip	integer	Czy połączenie powinno być nawiązywane przez IP. Możliwe wartości: 0 - połącz przy użyciu nazwy DNS hosta; 1 - połącz przy użyciu adresu IP hosta. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
main	integer	Czy interfejs jest używany jako domyślny na hoście. Tylko jeden interfejs danego typu może być ustawiony jako domyślny na hoście. Możliwe wartości: 0 - nie jest domyślny; 1 - domyślny. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
details	object	Dodatkowy obiekt details dla interfejsu. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”SNMP”
disable_until	timestamp	Czas następnego odpytywania niedostępnego interfejsu hosta. Zachowanie właściwości: - *tylko do odczytu*
error	string	Tekst błędu, jeśli interfejs hosta jest niedostępny. Zachowanie właściwości: - *tylko do odczytu*
errors_from	timestamp	Czas, kiedy interfejs hosta stał się niedostępny. Zachowanie właściwości: - *tylko do odczytu*

Szczegóły

Obiekt szczegółów ma następujące właściwości.

Właściwość	Typ	Opis
version	integer	Wersja interfejsu SNMP. Możliwe wartości: 1 - SNMPv1; 2 - SNMPv2c; 3 - SNMPv3. Zachowanie właściwości: - *wymagane*
bulk	integer	Czy używać zbiorczych żądań SNMP. Możliwe wartości: 0 - nie używaj zbiorczych żądań; 1 - (domyślnie) - używaj zbiorczych żądań.
community	string	Społeczność SNMP. Używana tylko przez interfejsy SNMPv1 i SNMPv2. Zachowanie właściwości: - *wymagane* jeśli `version` jest ustawione na ”SNMPv1” lub ”SNMPv2c”
max_repetitions	integer	Maksymalna wartość powtórzeń dla natywnych zbiorczych żądań SNMP (GetBulkRequest-PDUs). Używane tylko dla pozycji `discovery[]` i `walk[]` w SNMPv2 i v3. Domyślnie: 10.
securityname	string	Nazwa bezpieczeństwa SNMPv3. Używana tylko przez interfejsy SNMPv3.
securitylevel	integer	Poziom bezpieczeństwa SNMPv3. Używany tylko przez interfejsy SNMPv3. Możliwe wartości: 0 - (domyślnie) - noAuthNoPriv; 1 - authNoPriv; 2 - authPriv.
authpassphrase	string	Hasło uwierzytelniania SNMPv3. Używane tylko przez interfejsy SNMPv3.
privpassphrase	string	Hasło prywatności SNMPv3. Używane tylko przez interfejsy SNMPv3.
authprotocol	integer	Protokół uwierzytelniania SNMPv3. Używany tylko przez interfejsy SNMPv3. Możliwe wartości: 0 - (domyślnie) - MD5; 1 - SHA1; 2 - SHA224; 3 - SHA256; 4 - SHA384; 5 - SHA512.
privprotocol	integer	Protokół prywatności SNMPv3. Używany tylko przez interfejsy SNMPv3. Możliwe wartości: 0 - (domyślnie) - DES; 1 - AES128; 2 - AES192; 3 - AES256; 4 - AES192C; 5 - AES256C.
contextname	string	Nazwa kontekstu SNMPv3. Używana tylko przez interfejsy SNMPv3.

hostinterface.create

Opis

```
object hostinterface.create(object/array hostInterfaces)
```

Ta metoda umożliwia tworzenie nowych interfejsów hosta.

> **Note:**
> Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Interfejsy hosta do utworzenia.

Metoda akceptuje interfejsy hosta ze standardowymi właściwościami interfejsu hosta.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory utworzonych interfejsów hosta we właściwości `interfaceids`. Kolejność zwróconych identyfikatorów odpowiada kolejności przekazanych interfejsów hosta.

Przykłady

Utwórz nowy interfejs

Utwórz dodatkowy interfejs IP agenta na hoście „30052”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "hostinterface.create",
    "params": {
        "hostid": "30052",
        "main": "0",
        "type": "1",
        "useip": "1",
        "ip": "127.0.0.1",
        "dns": "",
        "port": "10050"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "interfaceids": [
            "30062"
        ]
    },
    "id": 1
}
```

Utwórz interfejs ze szczegółami SNMP

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "hostinterface.create",
    "params": {
        "hostid": "10456",
        "main": "0",
        "type": "2",
        "useip": "1",
        "ip": "127.0.0.1",
        "dns": "",
        "port": "1601",
        "details": {
            "version": "2",
```

```
            "bulk": "1",
            "community": "{$SNMP_COMMUNITY}"
        }
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "interfaceids": [
            "30063"
        ]
    },
    "id": 1
}
```

Zobacz także

- hostinterface.massadd
- host.massadd

Źródło

CHostInterface::create() w *ui/include/classes/api/services/CHostInterface.php*.

hostinterface.delete

Opis

`object hostinterface.delete(array hostInterfaceIds)`

Ta metoda umożliwia usuwanie interfejsów hosta.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkowników typu *Admin* i *Super admin*. Uprawnienia do wywołania metody można odwołać w ustawieniach roli użytkownika. Więcej informacji można znaleźć w User roles.

Parametry

`(array)` ID interfejsów hosta do usunięcia.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory usuniętych interfejsów hosta we właściwości `interfaceids`.

Przykłady

Usuń interfejs hosta

Usuń interfejs hosta o identyfikatorze 30062.

Żądanie:

```
{
"jsonrpc": "2.0",
"method": "hostinterface.delete",
"params": [
"30062"
],
"id": 1
}
```

Odpowiedź:

```
{
"jsonrpc": "2.0",
"result": {
```

```
"interfaceids": [
"30062"
]
},
"id": 1
}
```

Zobacz również

- hostinterface.massremove
- host.massremove

Źródło

CHostInterface::delete() w *ui/include/classes/api/services/CHostInterface.php*.

hostinterface.get

Opis

`integer/array hostinterface.get(object parameters)`

Ta metoda umożliwia pobieranie interfejsów hosta zgodnie z podanymi parametrami.

> **Note:**
> Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
hostids	ID/array	Zwraca tylko interfejsy hosta używane przez podane hosty.
interfaceids	ID/array	Zwraca tylko interfejsy hosta o podanych identyfikatorach.
itemids	ID/array	Zwraca tylko interfejsy hosta używane przez podane pozycje.
triggerids	ID/array	Zwraca tylko interfejsy hosta używane przez pozycje w podanych wyzwalaczach.
selectItems	query	Zwraca właściwość `items` z pozycjami, które używają interfejsu. Obsługuje `count`.
selectHosts	query	Zwraca właściwość `hosts` z tablicą hostów używających interfejsu.
limitSelects	integer	Ogranicza liczbę rekordów zwracanych przez podzapytania. Dotyczy następujących podzapytań: `selectItems`.
sortfield	string/array	Sortuje wynik według podanych właściwości. Możliwe wartości: `interfaceid`, `dns`, `ip`.
countOutput	boolean	Te parametry opisano w komentarzu referencyjnym.
editable	boolean	
excludeSearch	boolean	
filter	object	
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli został użyty parametr `countOutput`.

Przykłady

Pobieranie interfejsów hosta

Pobierz wszystkie dane o interfejsach używanych przez host „30057”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "hostinterface.get",
    "params": {
        "output": "extend",
        "hostids": "30057"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "interfaceid": "50039",
            "hostid": "30057",
            "main": "1",
            "type": "1",
            "useip": "0",
            "ip": "",
            "dns": "localhost",
            "port": "10050",
            "available": "0",
            "error": "",
            "errors_from": "0",
            "disable_until": "0",
            "details": []
        },
        {
            "interfaceid": "55082",
            "hostid": "30057",
            "main": "1",
            "type": "2",
            "useip": "1",
            "ip": "127.0.0.1",
            "dns": "",
            "port": "161",
            "available": "0",
            "error": "",
            "errors_from": "0",
            "disable_until": "0",
            "details": {
                "version": "2",
                "bulk": "0",
                "community": "{$SNMP_COMMUNITY}",
                "max_repetitions": "10"
            }
        }
    ],
    "id": 1
```

```
}
```

Zobacz także

- Host
- Item

Źródło

CHostInterface::get() w *ui/include/classes/api/services/CHostInterface.php*.

hostinterface.massadd

Opis

`object hostinterface.massadd(object parameters)`

Ta metoda umożliwia jednoczesne dodanie interfejsów hosta do wielu hostów.

> **Note:**
> Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach ról użytkowników. Więcej informacji można znaleźć w sekcji User roles.

Parametry

`(object)` Parametry zawierające interfejsy hosta, które mają zostać utworzone na podanych hostach.

Metoda akceptuje następujące parametry.

Parametr	Typ	Opis
interfaces	object/array	Interfejsy hosta, które mają zostać utworzone na podanych hostach. Zachowanie parametru: - *wymagany*
hosts	object/array	Hosty, które mają zostać zaktualizowane. Hosty muszą mieć zdefiniowaną wyłącznie właściwość `hostid`. Zachowanie parametru: - *wymagany*

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory utworzonych interfejsów hosta we właściwości `interfaceids`.

Przykłady

Tworzenie interfejsów

Utwórz interfejs na dwóch hostach.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "hostinterface.massadd",
    "params": {
        "hosts": [
            {
                "hostid": "30050"
            },
            {
                "hostid": "30052"
            }
        ],
        "interfaces": {
            "dns": "",
```

```
            "ip": "127.0.0.1",
            "main": 0,
            "port": "10050",
            "type": 1,
            "useip": 1
        }
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "interfaceids": [
            "30069",
            "30070"
        ]
    },
    "id": 1
}
```

Zobacz także

- hostinterface.create
- host.massadd
- Host

Źródło

CHostInterface::massAdd() w *ui/include/classes/api/services/CHostInterface.php*.

hostinterface.massremove

Opis

`object hostinterface.massremove(object parameters)`

Ta metoda pozwala na usuwanie interfejsów hosta z podanych hostów.

Note:
Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania metody można odwołać w ustawieniach roli użytkownika. Więcej informacji można znaleźć w User roles.

Parametry

`(object)` Parametry zawierające identyfikatory hostów do zaktualizowania oraz interfejsy do usunięcia.

Parametr	Typ	Opis
interfaces	object/array	Interfejsy hosta do usunięcia z podanych hostów. Obiekt interfejsu hosta musi mieć zdefiniowane tylko właściwości `ip`, `dns` i `port`. Zachowanie parametru: - *wymagany*
hostids	ID/array	Identyfikatory hostów do zaktualizowania. Zachowanie parametru: - *wymagany*

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory usuniętych interfejsów hosta we właściwości `interfaceids`.

Przykłady

Usuwanie interfejsów

Usuń interfejs SNMP „127.0.0.1” z dwóch hostów.

Żądanie:

```
{
"jsonrpc": "2.0",
"metoda": "hostinterface.massremove",
"parametry": {
"idy hosta": [
"30050",
"30052"
],
"interfejsy": {
"dns": "",
"ip": "127.0.0.1",
"port": "161"
}
},
"id": 1
}
```

Odpowiedź:

```
{
"jsonrpc": "2.0",
"wynik": {
"idy interfejsu": [
"30069",
"30070"
]
},
"id": 1
}
```

Zobacz także

- hostinterface.delete
- host.massremove

Źródło

CHostInterface::massRemove() w *ui/include/classes/api/services/CHostInterface.php*.

hostinterface.update

Opis

`object hostinterface.update(object/array hostInterfaces)`

Ta metoda umożliwia aktualizację istniejących interfejsów hosta.

> **Note:**
> Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w User roles.

Parametry

`(object/array)` Właściwości interfejsu hosta, które mają zostać zaktualizowane.

Właściwość `interfaceid` musi być zdefiniowana dla każdego interfejsu hosta, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko podane właściwości, wszystkie pozostałe pozostaną bez zmian.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych interfejsów hosta we właściwości `interfaceids`.

Przykłady

Zmiana portu interfejsu hosta

Zmień port interfejsu hosta.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "hostinterface.update",
    "params": {
        "interfaceid": "30048",
        "port": "10055"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "interfaceids": [
            "30048"
        ]
    },
    "id": 1
}
```

Zmiana portów wielu interfejsów hosta

Zmień port wielu interfejsów hosta.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "hostinterface.update",
    "params": [
        {
            "interfaceid": "30049",
            "port": "10055"
        },
        {
            "interfaceid": "30050",
            "port": "10055"
        },
        {
            "interfaceid": "30051",
            "port": "10055"
        }
    ],
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "interfaceids": [
            "30049",
            "30050",
            "30051"
        ]
    },
    "id": 1
```

```
}
```

Źródło

CHostInterface::update() w *ui/include/classes/api/services/CHostInterface.php*.

Katalog użytkowników

Ta klasa jest przeznaczona do pracy z katalogami użytkowników.

Odwołania do obiektów:

- Katalog użytkowników
  - Mapowania typów mediów
  - Mapowania grup provisioningu

Dostępne metody:

- userdirectory.create - utwórz nowy katalog użytkowników
- userdirectory.delete - usuń katalog użytkowników
- userdirectory.get - pobierz katalog użytkowników
- userdirectory.update - zaktualizuj katalog użytkowników
- userdirectory.test - przetestuj połączenie z katalogiem użytkowników

Obiekt katalogu użytkownika

Następujące obiekty są bezpośrednio powiązane z API `userdirectory`.

Katalog użytkowników

Obiekt katalogu użytkowników ma następujące właściwości.

Property	Type	Description
userdirectoryid	ID	ID katalogu użytkowników. Jeśli katalog użytkowników zostanie usunięty, wartość właściwości `userdirectoryid` obiektu User object zostanie ustawiona na ”0” dla wszystkich użytkowników powiązanych z usuniętym katalogiem użytkowników. Property behavior: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji
idp_type	integer	Typ protokołu uwierzytelniania używanego przez dostawcę tożsamości dla katalogu użytkowników. Zwróć uwagę, że może istnieć tylko jeden katalog użytkowników typu SAML. Możliwe wartości: 1 - katalog użytkowników typu LDAP; 2 - katalog użytkowników typu SAML. Property behavior: - *wymagane* dla operacji tworzenia
group_name	string	Atrybut katalogu użytkowników LDAP/SAML zawierający nazwę grupy używaną do mapowania grup między katalogiem użytkowników LDAP/SAML a Zabbix. Przykład: *cn* Property behavior: - *wymagane*, jeśli `provision_status` jest ustawione na ”Enabled”, a `saml_jit_status` obiektu Authentication object jest ustawione na ”Enabled for configured SAML IdPs”

Property	Type	Description
user_username	string	Atrybut katalogu użytkowników LDAP/SAML (również atrybut SCIM, jeśli `scim_status` jest ustawione na ”SCIM provisioning is enabled”) zawierający imię użytkownika, które jest używane jako wartość właściwości `name` obiektu User object podczas provisioningu użytkownika. Przykłady: *cn*, *commonName*, *displayName*, *name*
user_lastname	string	Atrybut katalogu użytkowników LDAP/SAML (również atrybut SCIM, jeśli `scim_status` jest ustawione na ”SCIM provisioning is enabled”) zawierający nazwisko użytkownika, które jest używane jako wartość właściwości `surname` obiektu User object podczas provisioningu użytkownika. Przykłady: *sn*, *surname*, *lastName*
provision_status	integer	Status provisioningu katalogu użytkowników. Możliwe wartości: 0 - *(domyślnie)* Wyłączone (provisioning użytkowników tworzonych przez ten katalog użytkowników jest wyłączony); 1 - Włączone (provisioning użytkowników tworzonych przez ten katalog użytkowników jest włączony; dodatkowo musi być włączony status provisioningu LDAP lub SAML (`ldap_jit_status` lub `saml_jit_status` obiektu Authentication object)).
provision_groups	array	Tablica obiektów provisioning groups mappings do mapowania wzorca grupy użytkowników LDAP/SAML na grupę użytkowników Zabbix i rolę użytkownika. Property behavior: - *wymagane*, jeśli `provision_status` jest ustawione na ”Enabled”
provision_media	array	Tablica obiektów media type mappings do mapowania atrybutów mediów LDAP/SAML użytkownika (np. email) na media użytkownika Zabbix do wysyłania powiadomień.
LDAP-specific properties:		
name	string	Unikalna nazwa katalogu użytkowników. Property behavior: - *wymagane*, jeśli `idp_type` jest ustawione na ”User directory of type LDAP”
host	string	Nazwa hosta, IP lub URI serwera LDAP. URI musi zawierać schemat (`ldap://` lub `ldaps://`), host i port (opcjonalnie). Przykłady: *host.example.com* *127.0.0.1* *ldap://ldap.example.com:389* Property behavior: - *wymagane*, jeśli `idp_type` jest ustawione na ”User directory of type LDAP”
port	integer	Port serwera LDAP. Property behavior: - *wymagane*, jeśli `idp_type` jest ustawione na ”User directory of type LDAP”

Property	Type	Description
base_dn	string	Ścieżka bazowa katalogu użytkowników LDAP do kont użytkowników. Przykłady: *ou=Users,dc=example,dc=org* *ou=Users,ou=system* (dla OpenLDAP) *DC=company,DC=com* (dla Microsoft Active Directory) *uid=%{user},dc=example,dc=com* (dla bezpośredniego wiązania użytkownika; symbol zastępczy "*%{user}*" jest obowiązkowy) Property behavior: - *wymagane*, jeśli `idp_type` jest ustawione na "User directory of type LDAP"
search_attribute	string	Atrybut katalogu użytkowników LDAP, według którego identyfikowane jest konto użytkownika na podstawie informacji podanych w żądaniu logowania. Przykłady: *uid* (dla OpenLDAP) *sAMAccountName* (dla Microsoft Active Directory) Property behavior: - *wymagane*, jeśli `idp_type` jest ustawione na "User directory of type LDAP"
bind_dn	string	Konto serwera LDAP używane do wiązania i wyszukiwania na serwerze LDAP. W przypadku bezpośredniego wiązania użytkownika i wiązania anonimowego `bind_dn` musi być puste. Przykłady: *uid=ldap_search,ou=system* (dla OpenLDAP) *CN=ldap_search,OU=user_group,DC=company,DC=com* (dla Microsoft Active Directory) *CN=Admin,OU=Users,OU=Zabbix,DC=zbx,DC=local* Property behavior: - *obsługiwane*, jeśli `idp_type` jest ustawione na "User directory of type LDAP"
bind_password	string	Hasło LDAP konta używanego do wiązania i wyszukiwania na serwerze LDAP. W przypadku bezpośredniego wiązania użytkownika i wiązania anonimowego `bind_password` musi być puste. Property behavior: - *obsługiwane*, jeśli `idp_type` jest ustawione na "User directory of type LDAP"
description	string	Opis katalogu użytkowników. Property behavior: - *obsługiwane*, jeśli `idp_type` jest ustawione na "User directory of type LDAP"

Property	Type	Description
group_basedn	string	Ścieżka bazowa katalogu użytkowników LDAP do grup; używana do skonfigurowania sprawdzania członkostwa użytkownika w katalogu użytkowników LDAP. Ignorowane podczas provisioningu użytkownika, jeśli ustawiono `group_membership`. Przykład: *ou=Groups,dc=example,dc=com* Property behavior: - *obsługiwane*, jeśli `idp_type` jest ustawione na ”User directory of type LDAP”
group_filter	string	Ciąg filtra do pobierania grup katalogu użytkowników LDAP, których członkiem jest użytkownik; używany do skonfigurowania sprawdzania członkostwa użytkownika w katalogu użytkowników LDAP. Ignorowane podczas provisioningu użytkownika, jeśli ustawiono `group_membership`. Obsługiwane symbole zastępcze `group_filter`: *%{attr}* - atrybut wyszukiwania (zastępowany wartością właściwości `search_attribute`); *%{groupattr}* - atrybut grupy (zastępowany wartością właściwości `group_member`); *%{host}* - nazwa hosta, IP lub URI serwera LDAP (zastępowane wartością właściwości `host`); *%{user}* - nazwa użytkownika Zabbix. Domyślnie: *(%{groupattr}=%{user})* Przykłady: - *(member=uid=%{ref},ou=Users,dc=example,dc=com)* dopasuje ”User1”, jeśli obiekt grupy LDAP zawiera atrybut ”*member*” o wartości ”*uid=User1,ou=Users,dc=example,dc=com*”, i zwróci grupę, której członkiem jest ”User1”; - *(%{groupattr}=cn=%{ref},ou=Users,ou=Zabbix,DC=example,DC=com)* dopasuje ”User1”, jeśli obiekt grupy LDAP zawiera atrybut określony we właściwości `group_member` o wartości ”*cn=User1,ou=Users,ou=Zabbix,DC=example,DC=com*”, i zwróci grupę, której członkiem jest ”User1”. Property behavior: - *obsługiwane*, jeśli `idp_type` jest ustawione na ”User directory of type LDAP”
group_member	string	Atrybut katalogu użytkowników LDAP zawierający informacje o członkach grupy; używany do skonfigurowania sprawdzania członkostwa użytkownika w katalogu użytkowników LDAP. Ignorowane podczas provisioningu użytkownika, jeśli ustawiono `group_membership`. Property behavior: - *obsługiwane*, jeśli `idp_type` jest ustawione na ”User directory of type LDAP”

Property	Type	Description
group_membership	string	Atrybut katalogu użytkowników LDAP zawierający informacje o grupach, do których należy użytkownik. Przykład: *memberOf* Property behavior: - *obsługiwane*, jeśli `idp_type` jest ustawione na ”User directory of type LDAP”
search_filter	string	Niestandardowy ciąg filtra używany do lokalizowania i uwierzytelniania użytkownika w katalogu użytkowników LDAP na podstawie informacji podanych w żądaniu logowania. Obsługiwane symbole zastępcze `search_filter`: *%{attr}* - nazwa atrybutu wyszukiwania (np. *uid*, *sAMAccountName*); *%{user}* - nazwa użytkownika Zabbix. Domyślnie: *(%{attr}=%{user})* Property behavior: - *obsługiwane*, jeśli `idp_type` jest ustawione na ”User directory of type LDAP”
start_tls	integer	Opcja konfiguracji serwera LDAP, która umożliwia zabezpieczenie komunikacji z serwerem LDAP przy użyciu Transport Layer Security (TLS). Zwróć uwagę, że `start_tls` musi być ustawione na ”Disabled” dla hostów używających protokołu `ldaps://`. Możliwe wartości: 0 - *(domyślnie)* Wyłączone; 1 - Włączone. Property behavior: - *obsługiwane*, jeśli `idp_type` jest ustawione na ”User directory of type LDAP”
user_ref_attr	string	Atrybut katalogu użytkowników LDAP używany do odwoływania się do obiektu użytkownika. Wartość `user_ref_attr` jest używana do pobierania wartości z określonego atrybutu w katalogu użytkowników i umieszczania ich zamiast symbolu zastępczego *%{ref}* w ciągu `group_filter`. Przykłady: *cn*, *uid*, *member*, *uniqueMember* Property behavior: - *obsługiwane*, jeśli `idp_type` jest ustawione na ”User directory of type LDAP”
SAML-specific properties:		
idp_entityid	string	URI identyfikujący dostawcę tożsamości i używany do komunikacji z dostawcą tożsamości w komunikatach SAML. Przykład: *https://idp.example.com/idp* Property behavior: - *wymagane*, jeśli `idp_type` jest ustawione na ”User directory of type SAML”

Property	Type	Description
sp_entityid	string	URL lub dowolny ciąg identyfikujący dostawcę usług dostawcy tożsamości. Przykłady: *https://idp.example.com/sp* *zabbix* Property behavior: - *wymagane*, jeśli `idp_type` jest ustawione na ”User directory of type SAML”
username_attribute	string	Atrybut katalogu użytkowników SAML (również atrybut SCIM, jeśli `scim_status` jest ustawione na ”SCIM provisioning is enabled”) zawierający nazwę użytkownika, która jest porównywana z wartością właściwości `username` obiektu User object podczas uwierzytelniania. Przykłady: *uid*, *userprincipalname*, *samaccountname*, *username*, *userusername*, *urn:oid:0.9.2342.19200300.100.1.1*, *urn:oid:1.3.6.1.4.1.5923.1.1.1.13*, *urn:oid:0.9.2342.19200300.100.1.44* Property behavior: - *wymagane*, jeśli `idp_type` jest ustawione na ”User directory of type SAML”
sso_url	string	URL usługi logowania jednokrotnego SAML dostawcy tożsamości, do której Zabbix będzie wysyłał żądania uwierzytelniania SAML. Przykład: *http://idp.example.com/idp/sso/saml* Property behavior: - *wymagane*, jeśli `idp_type` jest ustawione na ”User directory of type SAML”
slo_url	string	URL usługi pojedynczego wylogowania SAML dostawcy tożsamości, do której Zabbix będzie wysyłał żądania wylogowania SAML. Przykład: *https://idp.example.com/idp/slo/saml* Property behavior: - *obsługiwane*, jeśli `idp_type` jest ustawione na ”User directory of type SAML”
encrypt_nameid	integer	Czy identyfikator nazwy SAML powinien być szyfrowany. Możliwe wartości: 0 - *(domyślnie)* Nie szyfruj identyfikatora nazwy; 1 - Szyfruj identyfikator nazwy. Property behavior: - *obsługiwane*, jeśli `idp_type` jest ustawione na ”User directory of type SAML”
encrypt_assertions	integer	Czy asercje SAML powinny być szyfrowane. Możliwe wartości: 0 - *(domyślnie)* Nie szyfruj asercji; 1 - Szyfruj asercje. Property behavior: - *obsługiwane*, jeśli `idp_type` jest ustawione na ”User directory of type SAML”

Property	Type	Description
nameid_format	string	Format identyfikatora nazwy dostawcy usług dostawcy tożsamości SAML. Przykłady: *urn:oasis:names:tc:SAML:2.0:nameid-format:persistent* *urn:oasis:names:tc:SAML:2.0:nameid-format:transient* *urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos* *urn:oasis:names:tc:SAML:2.0:nameid-format:entity* Property behavior: - *obsługiwane*, jeśli `idp_type` jest ustawione na ”User directory of type SAML”
scim_status	integer	Czy provisioning SCIM dla SAML jest włączony czy wyłączony. Możliwe wartości: 0 - *(domyślnie)* Provisioning SCIM jest wyłączony; 1 - Provisioning SCIM jest włączony. Property behavior: - *obsługiwane*, jeśli `idp_type` jest ustawione na ”User directory of type SAML”
sign_assertions	integer	Czy asercje SAML powinny być podpisywane podpisem SAML. Możliwe wartości: 0 - *(domyślnie)* Nie podpisuj asercji; 1 - Podpisuj asercje. Property behavior: - *obsługiwane*, jeśli `idp_type` jest ustawione na ”User directory of type SAML”
sign_authn_requests	integer	Czy żądania AuthN SAML powinny być podpisywane podpisem SAML. Możliwe wartości: 0 - *(domyślnie)* Nie podpisuj żądań AuthN; 1 - Podpisuj żądania AuthN. Property behavior: - *obsługiwane*, jeśli `idp_type` jest ustawione na ”User directory of type SAML”
sign_messages	integer	Czy komunikaty SAML powinny być podpisywane podpisem SAML. Możliwe wartości: 0 - *(domyślnie)* Nie podpisuj komunikatów; 1 - Podpisuj komunikaty. Property behavior: - *obsługiwane*, jeśli `idp_type` jest ustawione na ”User directory of type SAML”
sign_logout_requests	integer	Czy żądania wylogowania SAML powinny być podpisywane podpisem SAML. Możliwe wartości: 0 - *(domyślnie)* Nie podpisuj żądań wylogowania; 1 - Podpisuj żądania wylogowania. Property behavior: - *obsługiwane*, jeśli `idp_type` jest ustawione na ”User directory of type SAML”

Property	Type	Description
sign_logout_responses	integer	Czy odpowiedzi wylogowania SAML powinny być podpisywane podpisem SAML. Możliwe wartości: 0 - *(domyślnie)* Nie podpisuj odpowiedzi wylogowania; 1 - Podpisuj odpowiedzi wylogowania. Property behavior: - *obsługiwane*, jeśli `idp_type` jest ustawione na ”User directory of type SAML”.
idp_certificate	string	Zawartość certyfikatu Service Provider (SP) do konfiguracji usługi logowania jednokrotnego SAML (SSO). Przykłady: *-----BEGIN CERTIFICATE----- ...more encoded data... -----END CERTIFICATE-----* Property behavior: - *obsługiwane*, jeśli `idp_type` jest ustawione na ”User directory of type SAML”, a `$SSO['CERT_STORAGE']` jest ustawione na `database` w zabbix.conf.php - *tylko do zapisu*
sp_private_key	string	Zawartość klucza prywatnego Service Provider (SP) do konfiguracji usługi logowania jednokrotnego SAML (SSO). Zapewnia bezpieczne uwierzytelnianie i wymianę danych z Identity Provider (IdP). Przykłady: *-----BEGIN CERTIFICATE----- ...more encoded data... -----END CERTIFICATE-----* Property behavior: - *obsługiwane*, jeśli `idp_type` jest ustawione na ”User directory of type SAML”, a `$SSO['CERT_STORAGE']` jest ustawione na `database` w zabbix.conf.php - *tylko do zapisu*
sp_certificate	string	Zawartość certyfikatu Service Provider (SP) do konfiguracji usługi logowania jednokrotnego SAML (SSO). Przykłady: *-----BEGIN CERTIFICATE----- ...more encoded data... -----END CERTIFICATE-----* Property behavior: - *obsługiwane*, jeśli `idp_type` jest ustawione na ”User directory of type SAML”, a `$SSO['CERT_STORAGE']` jest ustawione na `database` w zabbix.conf.php - *tylko do zapisu*
idp_certificate_hash	string	Skrót md5 wartości idp_certificate. Zwróci pusty ciąg dla pustego idp_certificate. Property behavior: - *obsługiwane*, jeśli `idp_type` jest ustawione na ”User directory of type SAML”, a `$SSO['CERT_STORAGE']` jest ustawione na `database` w zabbix.conf.php - *tylko do odczytu*

Property	Type	Description
sp_private_key_hash	string	Skrót md5 wartości sp_private_key. Zwróci pusty ciąg dla pustego sp_private_key. Property behavior: - *obsługiwane*, jeśli `idp_type` jest ustawione na "User directory of type SAML", a `$SSO['CERT_STORAGE']` jest ustawione na `database` w zabbix.conf.php - *tylko do odczytu*
sp_certificate_hash	string	Skrót md5 wartości sp_certificate. Zwróci pusty ciąg dla pustego sp_certificate. Property behavior: - *obsługiwane*, jeśli `idp_type` jest ustawione na "User directory of type SAML", a `$SSO['CERT_STORAGE']` jest ustawione na `database` w zabbix.conf.php - *tylko do odczytu*

Mapowania typów mediów

Obiekt mapowań typów mediów ma następujące właściwości.

Właściwość	Typ	Opis
userdirectory_mediaid	ID	ID mapowania typu mediów. Zachowanie właściwości: - *tylko do odczytu*
name	string	Widoczna nazwa na liście mapowań typów mediów. Zachowanie właściwości: - *wymagane*
mediatypeid	ID	ID typu mediów, który ma zostać utworzony; używane jako wartość właściwości `mediatypeid` obiektu Media. Zachowanie właściwości: - *wymagane*
attribute	string	Atrybut katalogu użytkowników LDAP/SAML (również atrybut SCIM, jeśli `scim_status` jest ustawione na „Udostępnianie SCIM jest włączone"), który zawiera media użytkownika (np. *user@example.com*), używane jako wartość właściwości `sendto` obiektu Media. Jeśli występuje w danych otrzymanych od dostawcy tożsamości LDAP/SAML, a wartość nie jest pusta, spowoduje to utworzenie mediów dla udostępnionego użytkownika. Zachowanie właściwości: - *wymagane*
active	integer	Wartość właściwości `active` mediów użytkownika podczas tworzenia mediów dla udostępnionego użytkownika. Możliwe wartości: 0 - *(domyślnie)* włączone; 1 - wyłączone.
severity	integer	Wartość właściwości `severity` mediów użytkownika podczas tworzenia mediów dla udostępnionego użytkownika. Domyślnie: 63.
period	string	Wartość właściwości `period` mediów użytkownika podczas tworzenia mediów dla udostępnionego użytkownika. Domyślnie: 1-7,00:00-24:00.

Mapowania grup provisioningu

Mapowania grup provisioningu mają następujące właściwości.

Właściwość	Typ	Opis
name	string	Pełna nazwa grupy (np. *Zabbix administrators*) w katalogu użytkowników LDAP/SAML (również SCIM, jeśli `scim_status` jest ustawione na „SCIM provisioning is enabled”). Obsługuje znak wieloznaczny „*”. Unikalna wśród wszystkich mapowań grup provisioningu. Zachowanie właściwości: - *wymagane*
roleid	ID	ID roli użytkownika, która ma zostać przypisana użytkownikowi. Jeśli dopasowanych zostanie wiele mapowań grup provisioningu, użytkownikowi zostanie przypisana rola o najwyższym typie użytkownika (*User*, *Admin* lub *Super admin*). Jeśli istnieje wiele ról z tym samym typem użytkownika, użytkownikowi zostanie przypisana pierwsza rola (posortowana alfabetycznie). Zachowanie właściwości: - *wymagane*
user_groups	array	Tablica obiektów ID grup użytkowników Zabbix. Każdy obiekt ma następujące właściwości: `usrgrpid` - `(ID)` ID grupy użytkowników Zabbix, która ma zostać przypisana użytkownikowi. Jeśli dopasowanych zostanie wiele mapowań grup provisioningu, użytkownikowi zostaną przypisane grupy użytkowników Zabbix ze wszystkich dopasowanych mapowań. Zachowanie właściwości: - *wymagane*

userdirectory.create

Opis

`object userdirectory.create(object/array userDirectory)`

Ta metoda umożliwia tworzenie nowych katalogów użytkowników.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkownika typu *Super admin*.

Parametry

`(object/array)` Katalogi użytkowników do utworzenia.

Metoda akceptuje katalogi użytkowników ze standardowymi właściwościami katalogu użytkownika.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory utworzonych katalogów użytkowników we właściwości `userdirectoryids`. Kolejność zwróconych identyfikatorów odpowiada kolejności przekazanych katalogów użytkowników.

Przykłady

Tworzenie katalogu użytkowników

Utwórz katalog użytkowników, aby uwierzytelniać użytkowników za pomocą StartTLS przez LDAP. Pamiętaj, że aby uwierzytelniać użytkowników przez LDAP, musi być włączone uwierzytelnianie LDAP.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "userdirectory.create",
    "params": {
        "idp_type": "1",
        "name": "LDAP API server #1",
        "host": "ldap://local.ldap",
```

```
        "port": "389",
        "base_dn": "ou=Users,dc=example,dc=org",
        "bind_dn": "cn=ldap_search,dc=example,dc=org",
        "bind_password": "ldapsecretpassword",
        "search_attribute": "uid",
        "start_tls": "1"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "userdirectoryids": [
            "3"
        ]
    },
    "id": 1
}
```

Tworzenie katalogu użytkowników (z włączonym udostępnianiem JIT)

Utwórz katalog użytkowników, aby uwierzytelniać użytkowników przez LDAP (z włączonym udostępnianiem JIT). Pamiętaj, że aby uwierzytelniać użytkowników przez LDAP, należy włączyć uwierzytelnianie LDAP.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "userdirectory.create",
    "params": {
            "idp_type": "1",
            "name": "AD server",
            "provision_status": "1",
            "description": "",
            "host": "host.example.com",
            "port": "389",
            "base_dn": "DC=zbx,DC=local",
            "search_attribute": "sAMAccountName",
            "bind_dn": "CN=Admin,OU=Users,OU=Zabbix,DC=zbx,DC=local",
            "start_tls": "0",
            "search_filter": "",
            "group_basedn": "OU=Zabbix,DC=zbx,DC=local",
            "group_name": "CN",
            "group_member": "member",
            "group_filter": "(%{groupattr}=CN=%{ref},OU=Users,OU=Zabbix,DC=zbx,DC=local)",
            "group_membership": "",
            "user_username": "givenName",
            "user_lastname": "sn",
            "user_ref_attr": "CN",
            "provision_media": [
                {
                    "name": "example.com",
                    "mediatypeid": "1",
                    "attribute": "user@example.com"
                }
            ],
            "provision_groups": [
                {
                    "name": "*",
                    "roleid": "4",
                    "user_groups": [
                        {
```

```
                            "usrgrpid": "8"
                        }
                    ]
                },
                {
                    "name": "Zabbix administrators",
                    "roleid": "2",
                    "user_groups": [
                        {
                            "usrgrpid": "7"
                        },
                        {
                            "usrgrpid": "8"
                        }
                    ]
                }
            ]
        },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "userdirectoryids": [
            "2"
        ]
    },
    "id": 1
}
```

Źródło

CUserDirectory::create() w *ui/include/classes/api/services/CUserDirectory.php*.

userdirectory.delete

Opis

`object userdirectory.delete(array userDirectoryIds)`

Ta metoda pozwala na usuwanie katalogów użytkownika. Katalogu użytkownika nie można usunąć, gdy jest on bezpośrednio używany przez co najmniej jedną grupę użytkownika.
Domyślnego katalogu użytkownika LDAP nie można usunąć, gdy `authentication.ldap_configured` jest ustawiony na 1 lub gdy pozostało więcej katalogów użytkownika.

> **Note:**
> Ta metoda jest dostępna tylko dla typu użytkownika *Super admin*.

Parametry

`(tablica)` Identyfikatory katalogów użytkownika do usunięcia.

Wartości zwracane

`(object)` Zwraca obiekt zawierający identyfikatory usuniętych katalogów użytkownika w ramach właściwości `userdirectoryids`.

Przykłady

Usuwanie wielu katalogów użytkowników

Usuń dwa katalogi użytkowników.

Żądanie:

```
{
"jsonrpc": "2.0",
"method": "userdirectory.delete",
"params": [
"2",
"12"
],
"id": 1
}
```

Odpowiedź:

```
{
"jsonrpc": "2.0",
"result": {
"userdirectoryids": [
"2",
"12"
]
},
"id": 1
}
```

Źródło

CUserDirectory::delete() w *ui/include/classes/api/services/CUserDirectory.php*.

userdirectory.get

Opis

`integer/array userdirectory.get(object parameters)`

Ta metoda umożliwia pobieranie katalogów użytkowników zgodnie z podanymi parametrami.

Note:
Ta metoda jest dostępna tylko dla użytkowników typu *Super admin*.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
userdirectoryids	ID/array	Zwracaj tylko katalogi użytkowników o podanych identyfikatorach.
selectUsrgrps	query	Zwracaj właściwość `usrgrps` z grupami użytkowników powiązanymi z katalogiem użytkowników. Obsługuje `count`.
selectProvisionMedia	query	Zwracaj właściwość `provision_media` z mapowaniami typów mediów powiązanymi z katalogiem użytkowników.
selectProvisionGroups	query	Zwracaj właściwość `provision_groups` z mapowaniami grup provisioningu powiązanymi z katalogiem użytkowników.
sortfield	string/array	Sortuj wynik według podanych właściwości. Możliwe wartości: `name`.
filter	object	Zwracaj tylko te wyniki, które dokładnie odpowiadają podanemu filtrowi. Akceptuje obiekt, w którym kluczami są nazwy właściwości, a wartościami są pojedyncza wartość lub tablica wartości. Obsługiwane właściwości: `userdirectoryid`, `idp_type`, `provision_status`.

Parametr	Typ	Opis
search	object	Zwracaj wyniki pasujące do podanego wzorca (bez rozróżniania wielkości liter). Akceptuje obiekt, w którym kluczami są nazwy właściwości, a wartościami są ciągami znaków do wyszukania. Jeśli nie podano dodatkowych opcji, zostanie wykonane wyszukiwanie `LIKE "%…%"`. Obsługiwane właściwości: `name`, `description`. Katalog użytkowników typu SAML będzie miał pustą wartość zarówno dla właściwości `name`, jak i `description`. Obie właściwości można zmienić za pomocą operacji `userdirectory.update`.
countOutput	boolean	Te parametry opisano w komentarzu referencyjnym.
excludeSearch	boolean	
limit	integer	
output	query	
preservekeys	boolean	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów
- liczbę pobranych obiektów, jeśli został użyty parametr `countOutput`

Przykłady

Pobieranie katalogów użytkowników

Pobierz wszystkie katalogi użytkowników z dodatkowymi właściwościami wyświetlającymi mapowania typów mediów oraz mapowania grup provisioningu powiązane z każdym katalogiem użytkowników.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "userdirectory.get",
    "params": {
        "output": "extend",
        "selectProvisionMedia": "extend",
        "selectProvisionGroups": "extend"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
       {
            "userdirectoryid": "1",
            "idp_type": "2",
            "name": "",
            "provision_status": "1",
            "description": "",
            "group_name": "groups",
            "user_username": "",
            "user_lastname": "",
            "idp_entityid": "http://example.com/simplesaml/saml2/idp/metadata.php",
            "sso_url": "http://example.com/simplesaml/saml2/idp/SSOService.php",
```

```
            "slo_url": "",
            "username_attribute": "uid",
            "sp_entityid": "zabbix",
            "nameid_format": "",
            "sign_messages": "0",
            "sign_assertions": "0",
            "sign_authn_requests": "0",
            "sign_logout_requests": "0",
            "sign_logout_responses": "0",
            "encrypt_nameid": "0",
            "encrypt_assertions": "0",
            "scim_status": "1",
            "provision_media": [
                {
                    "userdirectory_mediaid": "1",
                    "name": "example.com",
                    "mediatypeid": "1",
                    "attribute": "user@example.com",
                    "active": "0",
                    "severity": "63",
                    "period": "1-7,00:00-24:00"
                }
            ],
            "provision_groups": [
                {
                    "name": "*",
                    "roleid": "1",
                    "user_groups": [
                        {
                            "usrgrpid": "13"
                        }
                    ]
                }
            ]
        },
        {
            "userdirectoryid": "2",
            "idp_type": "1",
            "name": "AD server",
            "provision_status": "1",
            "description": "",
            "host": "host.example.com",
            "port": "389",
            "base_dn": "DC=zbx,DC=local",
            "search_attribute": "sAMAccountName",
            "bind_dn": "CN=Admin,OU=Users,OU=Zabbix,DC=zbx,DC=local",
            "start_tls": "0",
            "search_filter": "",
            "group_basedn": "OU=Zabbix,DC=zbx,DC=local",
            "group_name": "CN",
            "group_member": "member",
            "group_filter": "(%{groupattr}=CN=%{ref},OU=Users,OU=Zabbix,DC=zbx,DC=local)",
            "group_membership": "",
            "user_username": "givenName",
            "user_lastname": "sn",
            "user_ref_attr": "CN",
            "provision_media": [
                {
                    "userdirectory_mediaid": "2",
                    "name": "example.com",
                    "mediatypeid": "1",
                    "attribute": "user@example.com",
```

```
                    "active": "0",
                    "severity": "63",
                    "period": "1-7,00:00-24:00"
                }
            ],
            "provision_groups": [
                {
                    "name": "*",
                    "roleid": "4",
                    "user_groups": [
                        {
                            "usrgrpid": "8"
                        }
                    ]
                },
                {
                    "name": "Zabbix administrators",
                    "roleid": "2",
                    "user_groups": [
                        {
                            "usrgrpid": "7"
                        },
                        {
                            "usrgrpid": "8"
                        }
                    ]
                }
            ]
        },
        {
            "userdirectoryid": "3",
            "idp_type": "1",
            "name": "LDAP API server #1",
            "provision_status": "0",
            "description": "",
            "host": "ldap://local.ldap",
            "port": "389",
            "base_dn": "ou=Users,dc=example,dc=org",
            "search_attribute": "uid",
            "bind_dn": "cn=ldap_search,dc=example,dc=org",
            "start_tls": "1",
            "search_filter": "",
            "group_basedn": "",
            "group_name": "",
            "group_member": "",
            "group_filter": "",
            "group_membership": "",
            "user_username": "",
            "user_lastname": "",
            "user_ref_attr": "",
            "provision_media": [],
            "provision_groups": []
        }
    ],
    "id": 1
}
```


Zobacz także

- Grupa użytkowników

Źródło

CUserDirectory::get() w *ui/include/classes/api/services/CUserDirectory.php*.

userdirectory.test

Opis

`object userdirectory.test(array userDirectory)`

Ta metoda umożliwia przetestowanie ustawień połączenia katalogu użytkowników.

Note:
Ta metoda umożliwia również sprawdzenie, jakie skonfigurowane dane odpowiadają ustawieniom katalogu użytkowników na potrzeby provisioningu użytkowników (np. jaka rola użytkownika, grupy użytkowników i media użytkownika zostaną przypisane użytkownikowi). Dla tego typu testu żądanie API powinno zostać wykonane dla katalogu użytkowników, który ma parametr `provision_status` ustawiony na enabled.

Note:
Ta metoda jest dostępna tylko dla użytkownika typu *Super admin*.

Parametry

`(object)` Właściwości katalogu użytkowników.

Ponieważ API `userdirectory.get` nie zwraca pola `bind_password`, należy podać `userdirectoryid` i/lub `bind_password`. Oprócz standardowych właściwości katalogu użytkowników metoda akceptuje następujące parametry.

Parametr	Type	Opis
test_username	string	Nazwa użytkownika do przetestowania w katalogu użytkowników.
test_password	string	Hasło powiązane z nazwą użytkownika do przetestowania w katalogu użytkowników.

Zwracane wartości

`(bool)` Zwraca true w przypadku powodzenia.

Przykłady

Testuj katalog użytkowników dla istniejącego użytkownika

Przetestuj katalog użytkowników „3” dla „user1”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "userdirectory.test",
    "params": {
        "userdirectoryid": "3",
        "host": "127.0.0.1",
        "port": "389",
        "base_dn": "ou=Users,dc=example,dc=org",
        "search_attribute": "uid",
        "bind_dn": "cn=ldap_search,dc=example,dc=org",
        "bind_password": "password",
        "test_username": "user1",
        "test_password": "password"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": true,
    "id": 1
}
```

Testuj katalog użytkowników dla nieistniejącego użytkownika

Przetestuj katalog użytkowników „3” dla nieistniejącego użytkownika „user2”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "userdirectory.test",
    "params": {
        "userdirectoryid": "3",
        "host": "127.0.0.1",
        "port": "389",
        "base_dn": "ou=Users,dc=example,dc=org",
        "search_attribute": "uid",
        "bind_dn": "cn=ldap_search,dc=example,dc=org",
        "test_username": "user2",
        "test_password": "password"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "error": {
        "code": -32500,
        "message": "Application error.",
        "data": "Incorrect user name or password or account is temporarily blocked."
    },
    "id": 1
}
```

Testuj katalog użytkowników na potrzeby provisioningu użytkowników

Przetestuj katalog użytkowników „3”, aby sprawdzić, które skonfigurowane dane odpowiadają ustawieniom katalogu użytkowników dla provisioningu użytkownika „user3” (np. jaka rola użytkownika, grupy użytkowników i media użytkownika zostaną przypisane temu użytkownikowi).

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "userdirectory.test",
    "params": {
        "userdirectoryid": "2",
        "host": "host.example.com",
        "port": "389",
        "base_dn": "DC=zbx,DC=local",
        "search_attribute": "sAMAccountName",
        "bind_dn": "CN=Admin,OU=Users,OU=Zabbix,DC=zbx,DC=local",
        "test_username": "user3",
        "test_password": "password"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "username": "user3",
        "name": "John",
        "surname": "Doe",
        "medias": [],
        "usrgrps": [
```

```
            {
                "usrgrpid": "8"
            },
            {
                "usrgrpid": "7"
            }
        ],
        "roleid": "2",
        "userdirectoryid": "2"
    },
    "id": 1
}
```

Źródło

CUserDirectory::test() w *ui/include/classes/api/services/CUserDirectory.php*.

userdirectory.update

Opis

`object userdirectory.update(object/array userDirectory)`

Ta metoda umożliwia aktualizację istniejących katalogów użytkowników.

Note:
Ta metoda jest dostępna tylko dla użytkownika typu *Super admin*.

Parametry

`(object/array)` Właściwości katalogu użytkowników, które mają zostać zaktualizowane.

Właściwość `userdirectoryid` musi być zdefiniowana dla każdego katalogu użytkowników, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko przekazane właściwości, wszystkie pozostałe pozostaną bez zmian.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych katalogów użytkowników we właściwości `userdirectoryids`.

Przykłady

Aktualizacja hasła bind dla katalogu użytkowników

Ustaw nowe hasło bind dla katalogu użytkowników.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "userdirectory.update",
    "params": {
        "userdirectoryid": "3",
        "bind_password": "newldappassword"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "userdirectoryids": [
            "3"
        ]
    },
    "id": 1
}
```

Zaktualizuj mapowania dla katalogu użytkowników

Zaktualizuj mapowania grup udostępniania oraz mapowania typów mediów dla katalogu użytkowników „2”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "userdirectory.update",
    "params": {
        "userdirectoryid": "2",
        "provision_media": [
                {
                    "userdirectory_mediaid": "2"
                }
            ],
            "provision_groups": [
                {
                    "name": "Zabbix administrators",
                    "roleid": "2",
                    "user_groups": [
                        {
                            "usrgrpid": "7"
                        },
                        {
                            "usrgrpid": "8"
                        },
                        {
                            "usrgrpid": "11"
                        }
                    ]
                }
            ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "userdirectoryids": [
            "2"
        ]
    },
    "id": 1
}
```

Źródło

CUserDirectory::update() w *ui/include/classes/api/services/CUserDirectory.php*.

Konfiguracja

Ta klasa jest przeznaczona do eksportowania i importowania danych konfiguracji Zabbix.

Dostępne metody:

- configuration.export - eksport konfiguracji
- configuration.import - import konfiguracji
- configuration.importcompare - porównanie pliku importu z bieżącymi elementami systemu

configuration.export

Opis

`string configuration.export(object parameters)`

Ta metoda umożliwia eksport danych konfiguracyjnych jako serializowanego ciągu znaków.

> **Note:**
> Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji User roles.

Parametry

`(object)` Parametry definiujące obiekty do wyeksportowania oraz format, który ma zostać użyty.

Parametr	Typ	Opis
format	string	Format, w jakim dane muszą zostać wyeksportowane. Możliwe wartości: `yaml` - YAML; `xml` - XML; `json` - JSON; `raw` - nieprzetworzona tablica PHP. Zachowanie parametrów: - *wymagany*
prettyprint	boolean	Sprawia, że dane wyjściowe są bardziej czytelne dla człowieka przez dodanie wcięć. Możliwe wartości: `true` - dodaj wcięcia; `false` - *(domyślnie)* nie dodawaj wcięć.
options	object	Obiekty do wyeksportowania. Obiekt `options` ma następujące parametry: `host_groups` - `(array)` ID grup hostów do wyeksportowania; `hosts` - `(array)` ID hostów do wyeksportowania; `images` - `(array)` ID obrazów do wyeksportowania; `maps` - `(array)` ID map do wyeksportowania; `mediaTypes` - `(array)` ID typów mediów do wyeksportowania; `template_groups` - `(array)` ID grup szablonów do wyeksportowania; `templates` - `(array)` ID szablonów do wyeksportowania. Użytkownicy typu *Admin* i *User* mogą eksportować tylko te obiekty, do których mają uprawnienia *read-only* lub *read-write* permission, a także obrazy, ale nie typy mediów. Zachowanie parametrów: - *wymagany*

Zwracane wartości

`(string)` Zwraca serializowany ciąg znaków zawierający żądane dane konfiguracyjne.

Przykłady

Eksportowanie szablonu

Wyeksportuj konfigurację szablonu „10571” jako ciąg XML.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "configuration.export",
    "params": {
        "options": {
```

```
            "templates": [
                "10571"
            ]
        },
        "format": "xml"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": "<?xml version=\"1.0\" encoding=\"UTF-8\"?>\n<zabbix_export><version>8.0</version><template_
    "id": 1
}
```

Źródło

CConfiguration::export() w *ui/include/classes/api/services/CConfiguration.php*.

configuration.import

Opis

`boolean configuration.import(object parameters)`

Ta metoda umożliwia import danych konfiguracyjnych z serializowanego ciągu znaków.

Note:
Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object)` Parametry zawierające dane do importu oraz reguły określające sposób obsługi tych danych.

Parametr	Typ	Opis
format	string	Format serializowanego ciągu znaków. Możliwe wartości: `yaml` - YAML; `xml` - XML; `json` - JSON. Zachowanie parametru: - *wymagany*
source	string	Serializowany ciąg znaków zawierający dane konfiguracyjne. Zachowanie parametru: - *wymagany*

Parametr	Typ	Opis
rules	object	Reguły określające sposób importowania nowych i istniejących obiektów. Użytkownicy typu *Admin* mogą importować tylko te obiekty, do których mają uprawnienia *odczyt-zapis* permission, a także mapy. Na przykład host i jego encje (pozycje, wyzwalacze, wykresy itd.) mogą zostać zaimportowane tylko wtedy, gdy grupa użytkowników użytkownika ma uprawnienia do grupy hostów, do której będzie należał importowany host. Obrazy i typy nośników nie mogą być importowane przez użytkowników typu *Admin*. Parametr `rules` został szczegółowo opisany w poniższej tabeli. Zachowanie parametru: - *wymagany*

Attention:
Jeśli nie podano żadnych reguł, konfiguracja nie zostanie zaktualizowana.

Obiekt `rules` obsługuje następujące parametry.

Parametr	Typ	Opis
discoveryRules	object	Reguły określające sposób importowania reguł LLD. Obsługiwane parametry: `createMissing` - `(boolean)` jeśli ustawiono na `true`, zostaną utworzone nowe reguły LLD; domyślnie: `false`; `updateExisting` - `(boolean)` jeśli ustawiono na `true`, istniejące reguły LLD zostaną zaktualizowane; domyślnie: `false`; `deleteMissing` - `(boolean)` jeśli ustawiono na `true`, reguły LLD nieobecne w importowanych danych zostaną usunięte z bazy danych; domyślnie: `false`.
graphs	object	Reguły określające sposób importowania wykresów. Obsługiwane parametry: `createMissing` - `(boolean)` jeśli ustawiono na `true`, zostaną utworzone nowe wykresy; domyślnie: `false`; `updateExisting` - `(boolean)` jeśli ustawiono na `true`, istniejące wykresy zostaną zaktualizowane; domyślnie: `false`; `deleteMissing` - `(boolean)` jeśli ustawiono na `true`, wykresy nieobecne w importowanych danych zostaną usunięte z bazy danych; domyślnie: `false`.
host_groups	object	Reguły określające sposób importowania grup hostów. Obsługiwane parametry: `createMissing` - `(boolean)` jeśli ustawiono na `true`, zostaną utworzone nowe grupy hostów; domyślnie: `false`; `updateExisting` - `(boolean)` jeśli ustawiono na `true`, istniejące grupy hostów zostaną zaktualizowane; domyślnie: `false`.
template_groups	object	Reguły określające sposób importowania grup szablonów. Obsługiwane parametry: `createMissing` - `(boolean)` jeśli ustawiono na `true`, zostaną utworzone nowe grupy szablonów; domyślnie: `false`; `updateExisting` - `(boolean)` jeśli ustawiono na `true`, istniejące grupy szablonów zostaną zaktualizowane; domyślnie: `false`.

Parametr	Typ	Opis
hosts	object	Reguły określające sposób importowania hostów. Obsługiwane parametry: `createMissing` - `(boolean)` jeśli ustawiono na `true`, zostaną utworzone nowe hosty; domyślnie: `false`; `updateExisting` - `(boolean)` jeśli ustawiono na `true`, istniejące hosty zostaną zaktualizowane; domyślnie: `false`.
httptests	object	Reguły określające sposób importowania scenariuszy WWW. Obsługiwane parametry: `createMissing` - `(boolean)` jeśli ustawiono na `true`, zostaną utworzone nowe scenariusze WWW; domyślnie: `false`; `updateExisting` - `(boolean)` jeśli ustawiono na `true`, istniejące scenariusze WWW zostaną zaktualizowane; domyślnie: `false`; `deleteMissing` - `(boolean)` jeśli ustawiono na `true`, scenariusze WWW nieobecne w importowanych danych zostaną usunięte z bazy danych; domyślnie: `false`.
images	object	Reguły określające sposób importowania obrazów. Obsługiwane parametry: `createMissing` - `(boolean)` jeśli ustawiono na `true`, zostaną utworzone nowe obrazy; domyślnie: `false`; `updateExisting` - `(boolean)` jeśli ustawiono na `true`, istniejące obrazy zostaną zaktualizowane; domyślnie: `false`.
items	object	Reguły określające sposób importowania pozycji. Obsługiwane parametry: `createMissing` - `(boolean)` jeśli ustawiono na `true`, zostaną utworzone nowe pozycje; domyślnie: `false`; `updateExisting` - `(boolean)` jeśli ustawiono na `true`, istniejące pozycje zostaną zaktualizowane; domyślnie: `false`; `deleteMissing` - `(boolean)` jeśli ustawiono na `true`, pozycje nieobecne w importowanych danych zostaną usunięte z bazy danych; domyślnie: `false`.
maps	object	Reguły określające sposób importowania map. Obsługiwane parametry: `createMissing` - `(boolean)` jeśli ustawiono na `true`, zostaną utworzone nowe mapy; domyślnie: `false`; `updateExisting` - `(boolean)` jeśli ustawiono na `true`, istniejące mapy zostaną zaktualizowane; domyślnie: `false`.
mediaTypes	object	Reguły określające sposób importowania typów nośników. Obsługiwane parametry: `createMissing` - `(boolean)` jeśli ustawiono na `true`, zostaną utworzone nowe typy nośników; domyślnie: `false`; `updateExisting` - `(boolean)` jeśli ustawiono na `true`, istniejące typy nośników zostaną zaktualizowane; domyślnie: `false`.
templateLinkage	object	Reguły określające sposób importowania powiązań szablonów. Obsługiwane parametry: `createMissing` - `(boolean)` jeśli ustawiono na `true`, szablony, które nie są powiązane z importowanym hostem lub szablonem, ale są obecne w importowanych danych, zostaną powiązane; domyślnie: `false`; `deleteMissing` - `(boolean)` jeśli ustawiono na `true`, szablony powiązane z importowanym hostem lub szablonem, ale nieobecne w importowanych danych, zostaną odłączone bez usuwania encji (pozycji, wyzwalaczy itd.) dziedziczonych z odłączonych szablonów; domyślnie: `false`.

Parametr	Typ	Opis
templates	object	Reguły określające sposób importowania szablonów. Obsługiwane parametry: `createMissing` - `(boolean)` jeśli ustawiono na `true`, zostaną utworzone nowe szablony; domyślnie: `false`; `updateExisting` - `(boolean)` jeśli ustawiono na `true`, istniejące szablony zostaną zaktualizowane; domyślnie: `false`.
templateDashboards	object	Reguły określające sposób importowania pulpitów szablonów. Obsługiwane parametry: `createMissing` - `(boolean)` jeśli ustawiono na `true`, zostaną utworzone nowe pulpity szablonów; domyślnie: `false`; `updateExisting` - `(boolean)` jeśli ustawiono na `true`, istniejące pulpity szablonów zostaną zaktualizowane; domyślnie: `false`; `deleteMissing` - `(boolean)` jeśli ustawiono na `true`, pulpity szablonów nieobecne w importowanych danych zostaną usunięte z bazy danych; domyślnie: `false`.
triggers	object	Reguły określające sposób importowania wyzwalaczy. Obsługiwane parametry: `createMissing` - `(boolean)` jeśli ustawiono na `true`, zostaną utworzone nowe wyzwalacze; domyślnie: `false`; `updateExisting` - `(boolean)` jeśli ustawiono na `true`, istniejące wyzwalacze zostaną zaktualizowane; domyślnie: `false`; `deleteMissing` - `(boolean)` jeśli ustawiono na `true`, wyzwalacze nieobecne w importowanych danych zostaną usunięte z bazy danych; domyślnie: `false`.
valueMaps	object	Reguły określające sposób importowania map wartości hosta lub szablonu. Obsługiwane parametry: `createMissing` - `(boolean)` jeśli ustawiono na `true`, zostaną utworzone nowe mapy wartości; domyślnie: `false`; `updateExisting` - `(boolean)` jeśli ustawiono na `true`, istniejące mapy wartości zostaną zaktualizowane; domyślnie: `false`; `deleteMissing` - `(boolean)` jeśli ustawiono na `true`, mapy wartości nieobecne w importowanych danych zostaną usunięte z bazy danych; domyślnie: `false`.

Zwracane wartości

`(boolean)` Zwraca `true` jeżeli importowanie się powiodło.

Przykłady

Importowanie szablonu

Zaimportuj konfigurację szablonu zawartą w ciągu XML. Jeśli w ciągu XML brakuje jakichkolwiek pozycji lub wyzwalaczy, zostaną one usunięte z bazy danych, a wszystko pozostałe pozostanie bez zmian.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "configuration.import",
    "params": {
        "format": "xml",
        "rules": {
            "templates": {
                "createMissing": true,
                "updateExisting": true
            },
            "items": {
                "createMissing": true,
```

```
                "updateExisting": true,
                "deleteMissing": true
            },
            "triggers": {
                "createMissing": true,
                "updateExisting": true,
                "deleteMissing": true
            },
            "valueMaps": {
                "createMissing": true,
                "updateExisting": false
            }
        },
        "source": "<?xml version=\"1.0\" encoding=\"UTF-8\"?>\n<zabbix_export><version>8.0</version><templ
    },
    "id": 1
}
```


Odpowiedź:


```
{
    "jsonrpc": "2.0",
    "result": true,
    "id": 1
}
```


Źródło

CConfiguration::import() w *ui/include/classes/api/services/CConfiguration.php*.

configuration.importcompare

Opis

`array configuration.importcompare(object parameters)`

Ta metoda umożliwia porównanie pliku importu z bieżącymi elementami systemu i pokazuje, co zostanie zmienione, jeśli ten plik importu zostanie zaimportowany.

noteclassic Metoda ta jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywoływania tej metody można cofnąć w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników. :::

Parametry

`(object)` Parametry zawierające możliwe do zaimportowania dane oraz reguły określające sposób obsługi tych danych.

Parametr	Type	Opis
format	string	Format serializowanego ciągu znaków. Możliwe wartości: `yaml` - YAML; `xml` - XML; `json` - JSON. Zachowanie parametru: - *wymagany*
source	string	Serializowany ciąg znaków zawierający dane konfiguracyjne. Zachowanie parametru: - *wymagany*

Parametr	Type	Opis
rules	object	Reguły określające sposób porównywania nowych i istniejących obiektów. Użytkownicy typu *Admin* i *User* mogą porównywać nowe obiekty tylko z istniejącymi obiektami, do których mają uprawnienia *read-only* lub *read-write* permission. Parametr `rules` został szczegółowo opisany w poniższej tabeli. Zachowanie parametru: - *wymagany*

Attention:
Jeśli nie zostaną podane żadne reguły, nie będzie nic do zaktualizowania, a wynik będzie pusty.

Note:
Porównanie zostanie wykonane tylko dla grup hostów i szablonów. Wyzwalacze i wykresy będą porównywane tylko dla importowanych szablonów, wszystkie pozostałe zostaną uznane za „nowe”.

Obiekt `rules` obsługuje następujące parametry.

Parametr	Type	Opis
discoveryRules	object	Reguły określające sposób importowania reguł LLD. Obsługiwane parametry: `createMissing` - `(boolean)` jeśli ustawione na `true`, nowe reguły LLD zostaną utworzone; domyślnie: `false`; `updateExisting` - `(boolean)` jeśli ustawione na `true`, istniejące reguły LLD zostaną zaktualizowane; domyślnie: `false`; `deleteMissing` - `(boolean)` jeśli ustawione na `true`, reguły LLD nieobecne w importowanych danych zostaną usunięte z bazy danych; domyślnie: `false`.
graphs	object	Reguły określające sposób importowania wykresów. Obsługiwane parametry: `createMissing` - `(boolean)` jeśli ustawione na `true`, nowe wykresy zostaną utworzone; domyślnie: `false`; `updateExisting` - `(boolean)` jeśli ustawione na `true`, istniejące wykresy zostaną zaktualizowane; domyślnie: `false`; `deleteMissing` - `(boolean)` jeśli ustawione na `true`, wykresy nieobecne w importowanych danych zostaną usunięte z bazy danych; domyślnie: `false`.
host_groups	object	Reguły określające sposób importowania grup hostów. Obsługiwane parametry: `createMissing` - `(boolean)` jeśli ustawione na `true`, nowe grupy hostów zostaną utworzone; domyślnie: `false`; `updateExisting` - `(boolean)` jeśli ustawione na `true`, istniejące grupy hostów zostaną zaktualizowane; domyślnie: `false`.
template_groups	object	Reguły określające sposób importowania grup szablonów. Obsługiwane parametry: `createMissing` - `(boolean)` jeśli ustawione na `true`, nowe grupy szablonów zostaną utworzone; domyślnie: `false`; `updateExisting` - `(boolean)` jeśli ustawione na `true`, istniejące grupy szablonów zostaną zaktualizowane; domyślnie: `false`.

Parametr	Type	Opis
hosts	object	Reguły określające sposób importowania hostów. Obsługiwane parametry: `createMissing` - `(boolean)` jeśli ustawione na `true`, nowe hosty zostaną utworzone; domyślnie: `false`; `updateExisting` - `(boolean)` jeśli ustawione na `true`, istniejące hosty zostaną zaktualizowane; domyślnie: `false`. Ten parametr nie wpłynie na wynik. Jest dozwolony wyłącznie dla zachowania spójności z `configuration.import`.
httptests	object	Reguły określające sposób importowania scenariuszy WWW. Obsługiwane parametry: `createMissing` - `(boolean)` jeśli ustawione na `true`, nowe scenariusze WWW zostaną utworzone; domyślnie: `false`; `updateExisting` - `(boolean)` jeśli ustawione na `true`, istniejące scenariusze WWW zostaną zaktualizowane; domyślnie: `false`; `deleteMissing` - `(boolean)` jeśli ustawione na `true`, scenariusze WWW nieobecne w importowanych danych zostaną usunięte z bazy danych; domyślnie: `false`.
images	object	Reguły określające sposób importowania obrazów. Obsługiwane parametry: `createMissing` - `(boolean)` jeśli ustawione na `true`, nowe obrazy zostaną utworzone; domyślnie: `false`; `updateExisting` - `(boolean)` jeśli ustawione na `true`, istniejące obrazy zostaną zaktualizowane; domyślnie: `false`. Ten parametr nie wpłynie na wynik. Jest dozwolony wyłącznie dla zachowania spójności z `configuration.import`.
items	object	Reguły określające sposób importowania pozycji. Obsługiwane parametry: `createMissing` - `(boolean)` jeśli ustawione na `true`, nowe pozycje zostaną utworzone; domyślnie: `false`; `updateExisting` - `(boolean)` jeśli ustawione na `true`, istniejące pozycje zostaną zaktualizowane; domyślnie: `false`; `deleteMissing` - `(boolean)` jeśli ustawione na `true`, pozycje nieobecne w importowanych danych zostaną usunięte z bazy danych; domyślnie: `false`.
maps	object	Reguły określające sposób importowania map. Obsługiwane parametry: `createMissing` - `(boolean)` jeśli ustawione na `true`, nowe mapy zostaną utworzone; domyślnie: `false`; `updateExisting` - `(boolean)` jeśli ustawione na `true`, istniejące mapy zostaną zaktualizowane; domyślnie: `false`. Ten parametr nie wpłynie na wynik. Jest dozwolony wyłącznie dla zachowania spójności z `configuration.import`.
mediaTypes	object	Reguły określające sposób importowania typów mediów. Obsługiwane parametry: `createMissing` - `(boolean)` jeśli ustawione na `true`, nowe typy mediów zostaną utworzone; domyślnie: `false`; `updateExisting` - `(boolean)` jeśli ustawione na `true`, istniejące typy mediów zostaną zaktualizowane; domyślnie: `false`. Ten parametr nie wpłynie na wynik. Jest dozwolony wyłącznie dla zachowania spójności z `configuration.import`.

Parametr	Type	Opis
templateLinkage	object	Reguły określające sposób importowania powiązań szablonów. Obsługiwane parametry: `createMissing` - `(boolean)` jeśli ustawione na `true`, szablony, które nie są powiązane z importowanym hostem lub szablonem, ale są obecne w importowanych danych, zostaną powiązane; domyślnie: `false`; `deleteMissing` - `(boolean)` jeśli ustawione na `true`, szablony powiązane z importowanym hostem lub szablonem, ale nieobecne w importowanych danych, zostaną odłączone bez usuwania encji (pozycji, wyzwalaczy itp.) dziedziczonych z odłączonych szablonów; domyślnie: `false`.
templates	object	Reguły określające sposób importowania szablonów. Obsługiwane parametry: `createMissing` - `(boolean)` jeśli ustawione na `true`, nowe szablony zostaną utworzone; domyślnie: `false`; `updateExisting` - `(boolean)` jeśli ustawione na `true`, istniejące szablony zostaną zaktualizowane; domyślnie: `false`.
templateDashboards	object	Reguły określające sposób importowania pulpitów szablonów. Obsługiwane parametry: `createMissing` - `(boolean)` jeśli ustawione na `true`, nowe pulpity szablonów zostaną utworzone; domyślnie: `false`; `updateExisting` - `(boolean)` jeśli ustawione na `true`, istniejące pulpity szablonów zostaną zaktualizowane; domyślnie: `false`; `deleteMissing` - `(boolean)` jeśli ustawione na `true`, pulpity szablonów nieobecne w importowanych danych zostaną usunięte z bazy danych; domyślnie: `false`.
triggers	object	Reguły określające sposób importowania wyzwalaczy. Obsługiwane parametry: `createMissing` - `(boolean)` jeśli ustawione na `true`, nowe wyzwalacze zostaną utworzone; domyślnie: `false`; `updateExisting` - `(boolean)` jeśli ustawione na `true`, istniejące wyzwalacze zostaną zaktualizowane; domyślnie: `false`; `deleteMissing` - `(boolean)` jeśli ustawione na `true`, wyzwalacze nieobecne w importowanych danych zostaną usunięte z bazy danych; domyślnie: `false`.
valueMaps	object	Reguły określające sposób importowania map wartości hosta lub szablonu. Obsługiwane parametry: `createMissing` - `(boolean)` jeśli ustawione na `true`, nowe mapy wartości zostaną utworzone; domyślnie: `false`; `updateExisting` - `(boolean)` jeśli ustawione na `true`, istniejące mapy wartości zostaną zaktualizowane; domyślnie: `false`; `deleteMissing` - `(boolean)` jeśli ustawione na `true`, mapy wartości nieobecne w importowanych danych zostaną usunięte z bazy danych; domyślnie: `false`.

Zwracane wartości

`(array)` Zwraca tablicę ze zmianamy w konfiguracji, które zostaną wprowadzone.

Przykłady

Porównanie importu szablonu

Porównaj szablon zawarty w ciągu XML z bieżącymi elementami systemu i pokaż, co zostanie zmienione, jeśli ten szablon zostanie zaimportowany.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "configuration.importcompare",
    "params": {
        "format": "xml",
        "rules": {
            "discoveryRules": {
                "createMissing": true,
                "updateExisting": true,
                "deleteMissing": true
            },
            "graphs": {
                "createMissing": true,
                "updateExisting": true,
                "deleteMissing": true
            },
            "host_groups": {
                "createMissing": true,
                "updateExisting": true
            },
            "template_groups": {
                "createMissing": true,
                "updateExisting": true
            },
            "httptests": {
                "createMissing": true,
                "updateExisting": true,
                "deleteMissing": true
            },
            "items": {
                "createMissing": true,
                "updateExisting": true,
                "deleteMissing": true
            },
            "templateLinkage": {
                "createMissing": true,
                "deleteMissing": true
            },
            "templates": {
                "createMissing": true,
                "updateExisting": true
            },
            "templateDashboards": {
                "createMissing": true,
                "updateExisting": true,
                "deleteMissing": true
            },
            "triggers": {
                "createMissing": true,
                "updateExisting": true,
                "deleteMissing": true
            },
            "valueMaps": {
                "createMissing": true,
                "updateExisting": true,
                "deleteMissing": true
            }
        },
        "source": "<?xml version=\"1.0\" encoding=\"UTF-8\"?>\n<zabbix_export><version>8.0</version><templ
    },
    "id": 1
}
```

Odpowiedź:


```
{
    "jsonrpc": "2.0",
    "result": {
        "templates": {
            "updated": [
                {
                    "before": {
                        "uuid": "5aef0444a82a4d8cb7a95dc4c0c85330",
                        "template": "New template",
                        "name": "New template",
                        "groups": [
                            {
                                "name": "Templates"
                            }
                        ]
                    },
                    "after": {
                        "uuid": "5aef0444a82a4d8cb7a95dc4c0c85330",
                        "template": "New template",
                        "name": "New template",
                        "groups": [
                            {
                                "name": "Templates"
                            }
                        ]
                    },
                    "items": {
                        "added": [
                            {
                                "after": {
                                    "uuid": "648006da5971424ead0c47ddbbf1ea2e",
                                    "name": "CPU utilization",
                                    "key": "system.cpu.util",
                                    "value_type": "FLOAT",
                                    "units": "%"
                                },
                                "triggers": {
                                    "added": [
                                        {
                                            "after": {
                                                "uuid": "736225012c534ec480c2a66a91322ce0",
                                                "expression": "avg(/New template/system.cpu.util,3m)>70",
                                                "name": "CPU utilization too high on 'New host' for 3 minu
                                                "priority": "WARNING"
                                            }
                                        }
                                    ]
                                }
                            }
                        ],
                        "removed": [
                            {
                                "before": {
                                    "uuid": "6805d4c39a624a8bab2cc8ab63df1ab3",
                                    "name": "CPU load",
                                    "key": "system.cpu.load",
                                    "value_type": "FLOAT"
                                },
                                "triggers": {
                                    "removed": [
                                        {
```

```
                                        "before": {
                                            "uuid": "ab4c2526c2bc42e48a633082255ebcb3",
                                            "expression": "avg(/New template/system.cpu.load,3m)>2",
                                            "name": "CPU load too high on 'New host' for 3 minutes",
                                            "priority": "WARNING"
                                        }
                                    }
                                ]
                            }
                        }
                    ],
                    "updated": [
                        {
                            "before": {
                                "uuid": "7f1e6f1e48aa4a128e5b6a958a5d11c3",
                                "name": "Zabbix agent ping",
                                "key": "agent.ping"
                            },
                            "after": {
                                "uuid": "7f1e6f1e48aa4a128e5b6a958a5d11c3",
                                "name": "Zabbix agent ping",
                                "key": "agent.ping",
                                "delay": "3m"
                            }
                        }
                    ]
                }
            }
        ]
    }
},
"id": 1
}
```


Źródło

CConfiguration::importcompare() w *ui/include/classes/api/services/CConfiguration.php*.

Konserwacja

Ta klasa jest przeznaczona do pracy z okresami konserwacji.

Odwołania do obiektów:

- Konserwacja
- Okres czasu
- Tag problemu

Dostępne metody:

- maintenance.create - utwórz nowe okresy konserwacji
- maintenance.delete - usuń okresy konserwacji
- maintenance.get - pobierz okresy konserwacji
- maintenance.update - zaktualizuj okresy konserwacji

Obiekt konserwacji

Następujące obiekty są bezpośrednio powiązane z API `maintenance`.

Konserwacja

Obiekt konserwacji ma następujące właściwości.

Właściwość	Type	Opis
maintenanceid	ID	ID konserwacji. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji
name	string	Nazwa konserwacji. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
active_since	timestamp	Czas, od którego konserwacja staje się aktywna (włącznie). Podana wartość zostanie zaokrąglona w dół do pełnych minut. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
active_till	timestamp	Czas, do którego konserwacja pozostaje aktywna (z wyłączeniem tej chwili). Podana wartość zostanie zaokrąglona w dół do pełnych minut. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
description	string	Opis konserwacji.
maintenance_type	integer	Typ konserwacji. Możliwe wartości: 0 - *(domyślnie)* ze zbieraniem danych; 1 - bez zbierania danych.
tags_evaltype	integer	Metoda oceny tagów problemów. Możliwe wartości: 0 - *(domyślnie)* I/Lub; 2 - Lub.

Okres czasu

Obiekt okresu czasu służy do definiowania okresów, w których konserwacja ma wejść w życie. Ma następujące właściwości.

Property	Type	Description
period	integer	Czas trwania okresu konserwacji w sekundach. Podana wartość zostanie zaokrąglona w dół do pełnych minut. Możliwy zakres wartości: 300 - 86399940. Domyślnie: 3600.
timeperiod_type	integer	Typ okresu czasu. Możliwe wartości: 0 - *(domyślnie)* tylko jeden raz; 2 - codziennie; 3 - co tydzień; 4 - co miesiąc.

Property	Type	Description
start_date	timestamp	Data, kiedy okres konserwacji ma wejść w życie. Podana wartość zostanie zaokrąglona w dół do pełnych minut. Domyślnie: bieżąca data. Zachowanie właściwości: - *obsługiwane*, jeśli `timeperiod_type` jest ustawione na ”one time only”
start_time	integer	Pora dnia, o której konserwacja rozpoczyna się, wyrażona w sekundach. Podana wartość zostanie zaokrąglona w dół do pełnych minut. Domyślnie: 0. Zachowanie właściwości: - *obsługiwane*, jeśli `timeperiod_type` jest ustawione na ”daily”, ”weekly” lub ”monthly”
every	integer	Dla okresów dziennych i tygodniowych `every` określa interwały dni lub tygodni, z jakimi konserwacja ma wejść w życie. Wartość domyślna, jeśli `timeperiod_type` jest ustawione na ”daily” lub ”weekly”: 1. Dla okresów miesięcznych, gdy ustawiono `day`, właściwość `every` określa dzień miesiąca, w którym konserwacja ma wejść w życie. Wartość domyślna, jeśli `timeperiod_type` jest ustawione na ”monthly” i ustawiono `day`: 1. Dla okresów miesięcznych, gdy ustawiono `dayofweek`, właściwość `every` określa tydzień miesiąca, w którym konserwacja ma wejść w życie. Możliwe wartości, jeśli `timeperiod_type` jest ustawione na ”monthly” i ustawiono `dayofweek`: 1 - *(domyślnie)* pierwszy tydzień; 2 - drugi tydzień; 3 - trzeci tydzień; 4 - czwarty tydzień; 5 - ostatni tydzień. Zachowanie właściwości: - *obsługiwane*, jeśli `timeperiod_type` jest ustawione na ”daily”, ”weekly” lub ”monthly”
dayofweek	integer	Dni tygodnia, w których konserwacja ma wejść w życie. Możliwe wartości bitmapy: 1 - poniedziałek; 2 - wtorek; 4 - środa; 8 - czwartek; 16 - piątek; 32 - sobota; 64 - niedziela. To pole jest maską bitową; akceptowalna jest dowolna suma możliwych wartości bitmapy (na przykład 21 dla poniedziałku, środy i piątku). Zachowanie właściwości: - *wymagane*, jeśli `timeperiod_type` jest ustawione na ”weekly” lub jeśli `timeperiod_type` jest ustawione na ”monthly” i `day` nie jest ustawione

Property	Type	Description
day	integer	Dzień miesiąca, w którym konserwacja ma wejść w życie. Zachowanie właściwości: - *wymagane*, jeśli `timeperiod_type` jest ustawione na ”monthly” i `dayofweek` nie jest ustawione
month	integer	Miesiące, w których konserwacja ma wejść w życie. Możliwe wartości bitmapy: 1 - styczeń; 2 - luty; 4 - marzec; 8 - kwiecień; 16 - maj; 32 - czerwiec; 64 - lipiec; 128 - sierpień; 256 - wrzesień; 512 - październik; 1024 - listopad; 2048 - grudzień. To pole jest maską bitową; akceptowalna jest dowolna suma możliwych wartości bitmapy (na przykład 585 dla stycznia, kwietnia, lipca i października). Zachowanie właściwości: - *wymagane*, jeśli `timeperiod_type` jest ustawione na ”monthly”

Znacznik problemu

Obiekt znacznika problemu służy do definiowania, które problemy mają być tłumione, gdy konserwacja stanie się aktywna. Znaczniki można określić tylko wtedy, gdy `maintenance_type` obiektu Maintenance object jest ustawione na „with data collection”. Ma on następujące właściwości.

Właściwość	Type	Opis
tag	string	Nazwa znacznika problemu. Zachowanie właściwości: - *wymagane*
operator	integer	Warunek operatora. Możliwe wartości: 0 - Równa się; 2 - *(domyślnie)* Zawiera.
value	string	Wartość znacznika problemu.

maintenance.create

Opis

`object maintenance.create(object/array maintenances)`

Ta metoda pozwala na tworzenie nowych konserwacji.

Note:
Ta metoda jest dostępna tylko dla użytkowników typu *Admin* i *Super admin*. Uprawnienia do wywołania metody można odwołać w ustawieniach roli użytkownika. Więcej informacji można znaleźć w User roles.

Parametry

`(object/array)` Okna konserwacyjne do utworzenia.

Oprócz standardowych właściwości okna konserwacyjnego, metoda akceptuje następujące parametry.

Parametr	Typ	Opis
groups	object/array	Grupy hostów, które zostaną objęte konserwacją. Grupy hostów muszą mieć zdefiniowaną tylko właściwość `groupid`. Zachowanie parametru: - *wymagany*, jeśli `hosts` nie jest ustawione
hosts	object/array	Hosty, które zostaną objęte konserwacją. Hosty muszą mieć zdefiniowaną tylko właściwość `hostid`. Zachowanie parametru: - *wymagany*, jeśli `groups` nie jest ustawione
timeperiods	object/array	Okresy czasu konserwacji. Zachowanie parametru: - *wymagany*
tags	object/array	Tagi problemów. Określają, które problemy mają być tłumione. Jeśli nie podano tagów, wszystkie problemy hostów z aktywnej konserwacji będą tłumione. Zachowanie parametru: - *obsługiwany*, jeśli `maintenance_type` obiektu Maintenance object jest ustawione na "with data collection"

Wartości zwracane

`(object)` Zwraca obiekt zawierający identyfikatory utworzonych konserwacji w ramach właściwości `maintenanceids`. Kolejność zwróconych identyfikatorów odpowiada kolejności przekazanych konserwacji.

Przykłady

Tworzenie okresu konserwacji

Utwórz okres konserwacji ze zbieraniem danych dla grupy hostów o ID „2" oraz z tagami problemów **service:mysqld** i **error**. Musi on być aktywny od 17.03.2026 do 17.03.2027, wchodzić w życie w każdą niedzielę o 18:00 i trwać jedną godzinę.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "maintenance.create",
    "params": {
        "name": "Sunday maintenance",
        "active_since": 1773720240,
        "active_till": 1805256240,
        "tags_evaltype": 0,
        "groups": [
            {"groupid": "2"}
        ],
        "timeperiods": [
            {
                "period": 3600,
                "timeperiod_type": 3,
                "start_time": 64800,
                "every": 1,
                "dayofweek": 64
            }
        ],
        "tags": [
            {
```

```
                "tag": "service",
                "operator": "0",
                "value": "mysqld"
            },
            {
                "tag": "error",
                "operator": "2",
                "value": ""
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "maintenanceids": [
            "3"
        ]
    },
    "id": 1
}
```

Zobacz także

- Okres czasu

Źródło

CMaintenance::create() w *ui/include/classes/api/services/CMaintenance.php*.

maintenance.delete

Opis

`object maintenance.delete(array maintenanceIds)`

Ta metoda pozwala na usuwanie okresów konserwacji.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania metody można odwołać w ustawieniach roli użytkownika. Więcej informacji można znaleźć w User roles.

Parametry

`(array)` Identyfikatory okresów konserwacji do usunięcia.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory usuniętych okresów konserwacji we właściwości `maintenanceids`.

Przykłady

Usuwanie wielu okresów konserwacji

Usuń dwa okresy konserwacji.

Żądanie:

```
{
"jsonrpc": "2.0",
"method": "maintenance.delete",
"params": [
"3",
"1"
],
```

```
"id": 1
}
```

Odpowiedź:

```
{
"jsonrpc": "2.0",
"result": {
"maintenanceids": [
"3",
"1"
]
},
"id": 1
}
```

Źródło

CMaintenance::delete() w *ui/include/classes/api/services/CMaintenance.php*.

maintenance.get

Opis

`integer/array maintenance.get(object parameters)`

Ta metoda umożliwia pobieranie okresów konserwacji zgodnie z podanymi parametrami.

> **Note:**
> Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w Rolach użytkowników.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
groupids	ID/array	Zwraca tylko okresy konserwacji przypisane do podanych grup hostów.
hostids	ID/array	Zwraca tylko okresy konserwacji przypisane do podanych hostów.
maintenanceids	ID/array	Zwraca tylko okresy konserwacji o podanych ID.
selectHostGroups	query	Zwraca właściwość `hostgroups` zawierającą grupy hostów przypisane do okresu konserwacji.
selectHosts	query	Zwraca właściwość `hosts` zawierającą hosty przypisane do okresu konserwacji.
selectTags	query	Zwraca właściwość `tags` zawierającą tagi problemów okresu konserwacji.
selectTimeperiods	query	Zwraca właściwość `timeperiods` zawierającą okresy czasu okresu konserwacji.
sortfield	string/array	Sortuje wynik według podanych właściwości. Możliwe wartości: `maintenanceid`, `name`, `maintenance_type`, `active_since`, `active_till`.
countOutput	boolean	Te parametry opisano w komentarzu referencyjnym.
editable	boolean	
excludeSearch	boolean	
filter	object	
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	

Parametr	Typ	Opis
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli został użyty parametr `countOutput`.

Przykłady

Pobieranie okresów konserwacji

Pobierz wszystkie skonfigurowane okresy konserwacji oraz dane o przypisanych grupach hostów, zdefiniowanych okresach czasu i tagach problemów.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "maintenance.get",
    "params": {
        "output": "extend",
        "selectHostGroups": "extend",
        "selectTimeperiods": "extend",
        "selectTags": "extend"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "maintenanceid": "3",
            "name": "Sunday maintenance",
            "maintenance_type": "0",
            "description": "",
            "active_since": "1358844540",
            "active_till": "1390466940",
            "tags_evaltype": "0",
            "hostgroups": [
                {
                    "groupid": "4",
                    "name": "Zabbix servers",
                    "flags": "0",
                    "uuid": "6f6799aa69e844b4b3918f779f2abf08"
                }
            ],
            "timeperiods": [
                {
                    "timeperiod_type": "3",
                    "every": "1",
                    "month": "0",
                    "dayofweek": "1",
                    "day": "0",
                    "start_time": "64800",
                    "period": "3600",
                    "start_date": "2147483647"
                }
            ],
            "tags": [
                {
```

```
                    "tag": "service",
                    "operator": "0",
                    "value": "mysqld",
                },
                {
                    "tag": "error",
                    "operator": "2",
                    "value": ""
                }
            ]
        }
    ],
    "id": 1
}
```

Zobacz także

- Host
- Grupa hostów
- Okres czasu

Źródło

CMaintenance::get() w *ui/include/classes/api/services/CMaintenance.php*.

maintenance.update

Opis

`object maintenance.update(object/array maintenances)`

Ta metoda umożliwia aktualizację istniejących konserwacji.

Note:
Ta metoda jest dostępna tylko dla użytkowników typu *Admin* i *Super admin*. Uprawnienia do wywołania metody można odwołać w ustawieniach roli użytkownika. Więcej informacji można znaleźć w User roles.

Parametry

`(object/array)` Właściwości maintenance do zaktualizowania.

Właściwość `maintenanceid` musi być zdefiniowana dla każdego maintenance, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko przekazane właściwości, wszystkie pozostałe pozostaną bez zmian.

Oprócz standardowych właściwości maintenance, metoda akceptuje następujące parametry.

Parametr	Typ	Opis
groups	object/array	Grupy hostów zastępujące bieżące grupy. Grupy hostów muszą mieć zdefiniowaną tylko właściwość `groupid`. Zachowanie parametru: - *wymagane*, jeśli `hosts` nie jest ustawione
hosts	object/array	Hosty zastępujące bieżące hosty. Hosty muszą mieć zdefiniowaną tylko właściwość `hostid`. Zachowanie parametru: - *wymagane*, jeśli `groups` nie jest ustawione
timeperiods	object/array	Okresy czasu maintenance zastępujące bieżące okresy.
tags	object/array	Tagi problemów zastępujące bieżące tagi. Zachowanie parametru: - *obsługiwane*, jeśli `maintenance_type` obiektu Maintenance object jest ustawione na ”with data collection”

Wartości zwracane

(object) Zwraca obiekt zawierający identyfikatory zaktualizowanych konserwacji w ramach właściwości maintenanceids.

Przykłady

Przypisywanie różnych hostów

Zastąp hosty aktualnie przypisane do konserwacji dwoma innymi.

Żądanie:

```
{
"jsonrpc": "2.0",
"method": "maintenance.update",
"params": {
"maintenanceid": "3",
"hosts": [
{"hostid": "10085"},
{"hostid": "10084"}
]
},
"id": 1
}
```

Odpowiedź:

```
{
"jsonrpc": "2.0",
"result": {
"maintenanceids": [
"3"
]
},
"id": 1
}
```

Zobacz także

- Okres czasu

Źródło

CMaintenance::update() w *ui/include/classes/api/services/CMaintenance.php*.

Kontrola wykrywania

Ta klasa została zaprojektowana do pracy z kontrolami wykrywania.

Odwołania do obiektów:

- Kontrola wykrywania

Dostępne metody:

- dcheck.get - pobieranie kontroli wykrywania

Obiekt sprawdzania odkrycia

Następujące obiekty są bezpośrednio powiązane z API dcheck.

Kontrola wykrywania

Obiekt kontroli wykrywania definiuje konkretną kontrolę wykonywaną przez regułę wykrywania sieci. Ma następujące właściwości.

Właściwość	Typ	Opis
dcheckid	ID	ID kontroli wykrywania.
druleid	ID	ID reguły wykrywania, do której należy ta kontrola.

Właściwość	Typ	Opis
key_	string	Klucz pozycji (jeśli `type` jest ustawione na ”Zabbix agent”) lub OID SNMP (jeśli `type` jest ustawione na ”SNMPv1 agent”, ”SNMPv2 agent” lub ”SNMPv3 agent”). Zachowanie właściwości: - *wymagane* jeśli `type` jest ustawione na ”Zabbix agent”, ”SNMPv1 agent”, ”SNMPv2 agent” lub ”SNMPv3 agent”
ports	string	Jeden lub kilka zakresów portów do sprawdzenia, oddzielonych przecinkami. Domyślnie: 0. Zachowanie właściwości: - *obsługiwane* jeśli `type` jest ustawione na ”SSH” (0), ”LDAP” (1), ”SMTP” (2), ”FTP” (3), ”HTTP” (4), ”POP” (5), ”NNTP” (6), ”IMAP” (7), ”TCP” (8), ”Zabbix agent” (9), ”SNMPv1 agent” (10), ”SNMPv2 agent” (11), ”SNMPv3 agent” (13), ”HTTPS” (14) lub ”Telnet” (15)
snmp_community	string	Społeczność SNMP. Zachowanie właściwości: - *wymagane* jeśli `type` jest ustawione na ”SNMPv1 agent” lub ”SNMPv2 agent”
snmpv3_authpassphrase	string	Hasło uwierzytelniania. Zachowanie właściwości: - *obsługiwane* jeśli `type` jest ustawione na ”SNMPv3 agent” i `snmpv3_securitylevel` jest ustawione na ”authNoPriv” lub ”authPriv”
snmpv3_authprotocol	integer	Protokół uwierzytelniania. Możliwe wartości: 0 - *(domyślnie)* MD5; 1 - SHA1; 2 - SHA224; 3 - SHA256; 4 - SHA384; 5 - SHA512. Zachowanie właściwości: - *obsługiwane* jeśli `type` jest ustawione na ”SNMPv3 agent” i `snmpv3_securitylevel` jest ustawione na ”authNoPriv” lub ”authPriv”
snmpv3_contextname	string	Nazwa kontekstu SNMPv3. Zachowanie właściwości: - *obsługiwane* jeśli `type` jest ustawione na ”SNMPv3 agent”
snmpv3_privpassphrase	string	Hasło prywatności. Zachowanie właściwości: - *obsługiwane* jeśli `type` jest ustawione na ”SNMPv3 agent” i `snmpv3_securitylevel` jest ustawione na ”authPriv”

Właściwość	Typ	Opis
snmpv3_privprotocol	integer	Protokół prywatności. Możliwe wartości: 0 - *(domyślnie)* DES; 1 - AES128; 2 - AES192; 3 - AES256; 4 - AES192C; 5 - AES256C. Zachowanie właściwości: - *obsługiwane* jeśli `type` jest ustawione na ”SNMPv3 agent” i `snmpv3_securitylevel` jest ustawione na ”authPriv”
snmpv3_securitylevel	string	Poziom bezpieczeństwa. Możliwe wartości: 0 - noAuthNoPriv; 1 - authNoPriv; 2 - authPriv. Zachowanie właściwości: - *obsługiwane* jeśli `type` jest ustawione na ”SNMPv3 agent”
snmpv3_securityname	string	Nazwa bezpieczeństwa. Zachowanie właściwości: - *obsługiwane* jeśli `type` jest ustawione na ”SNMPv3 agent”
type	integer	Typ kontroli. Możliwe wartości: 0 - SSH; 1 - LDAP; 2 - SMTP; 3 - FTP; 4 - HTTP; 5 - POP; 6 - NNTP; 7 - IMAP; 8 - TCP; 9 - Zabbix agent; 10 - SNMPv1 agent; 11 - SNMPv2 agent; 12 - ICMP ping; 13 - SNMPv3 agent; 14 - HTTPS; 15 - Telnet. Zachowanie właściwości: - *wymagane*
uniq	integer	Czy używać tej kontroli jako kryterium unikalności urządzenia. Dla reguły wykrywania można skonfigurować tylko jedną unikalną kontrolę. Możliwe wartości: 0 - *(domyślnie)* nie używaj tej kontroli jako kryterium unikalności; 1 - użyj tej kontroli jako kryterium unikalności. Zachowanie właściwości: - *obsługiwane* jeśli `type` jest ustawione na ”Zabbix agent”, ”SNMPv1 agent”, ”SNMPv2 agent” lub ”SNMPv3 agent”

Właściwość	Typ	Opis
host_source	integer	Źródło nazwy hosta. Możliwe wartości: 1 - *(domyślnie)* DNS; 2 - IP; 3 - wartość wykrywania tej kontroli.
name_source	integer	Źródło widocznej nazwy. Możliwe wartości: 0 - *(domyślnie)* nie określono; 1 - DNS; 2 - IP; 3 - wartość wykrywania tej kontroli.
allow_redirect	integer	Zezwalaj na sytuację, w której cel sprawdzany za pomocą ICMP ping odpowiada z innego adresu IP. Możliwe wartości: 0 - *(domyślnie)* traktuj przekierowane odpowiedzi tak, jakby docelowy host był niedostępny (niepowodzenie); 1 - traktuj przekierowane odpowiedzi tak, jakby docelowy host był dostępny (sukces). Zachowanie właściwości: - *obsługiwane* jeśli `type` jest ustawione na ”ICMP ping”

dcheck.get

Opis

`integer/array dcheck.get(object parameters)`

Metoda służy do pobierania danych wykrywania na podstawie podanych parametrów.

Note:
Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywoływania metody można odebrać w ustawieniach roli użytkownika. Zobacz [Role użytkownika] (/manual/web_interface/frontend_sections/users/user_roles) po więcej informacji.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
dcheckids	ID/array	Zwraca tylko kontrole wykrywania o podanych identyfikatorach.
druleids	ID/array	Zwraca tylko kontrole wykrywania należące do podanych reguł wykrywania.
dserviceids	ID/array	Zwraca tylko kontrole wykrywania, które wykryły podane wykryte usługi.
selectDRules	query	Zwraca reguły wykrywania powiązane z kontrolami wykrywania.
sortfield	string/array	Sortuje wynik według podanych właściwości. Możliwe wartości: `dcheckid`, `druleid`.
countOutput	boolean	Te parametry są opisane w komentarzu referencyjnym.
editable	boolean	
excludeSearch	boolean	
filter	object	
limit	integer	
output	query	
preservekeys	boolean	

Parametr	Typ	Opis
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca jedną z opcji:

- tablicę obiektów;
- liczbę otrzymanych obiektów, jeżeli parametr `countOutput` został użyty.

Przykłady

Pobieranie testów wykrywania dla reguły wykrywania

Pobierz wszystkie testy wykrywania, które są używane przez regułę ”6”.

Zapytanie:

```
{
  "jsonrpc": "2.0",
  "method": "dcheck.get",
  "params": {
    "output": "extend",
    "dcheckids": "6"
  },
  "id": 1
}
```

Odpowiedź:

```
{
  "jsonrpc": "2.0",
  "result": [
    {
      "dcheckid": "6",
      "druleid": "4",
      "type": "3",
      "key_": "",
      "snmp_community": "",
      "ports": "21",
      "snmpv3_securityname": "",
      "snmpv3_securitylevel": "0",
      "snmpv3_authpassphrase": "",
      "snmpv3_privpassphrase": "",
      "uniq": "0",
      "snmpv3_authprotocol": "0",
      "snmpv3_privprotocol": "0",
      "snmpv3_contextname": "",
      "host_source": "1",
      "name_source": "0",
      "allow_redirect": "0"
    }
  ],
  "id": 1
}
```

Źródło

CDCheck::get() w *ui/include/classes/api/services/CDCheck.php*.

Korelacja

Ta klasa jest przeznaczona do pracy z korelacjami.

Odwołania do obiektów:

- Korelacja
- Operacja korelacji
- Filtr korelacji
  - Warunek filtra korelacji

Dostępne metody:

- correlation.create - utwórz nowe korelacje
- correlation.delete - usuń korelacje
- correlation.get - pobierz korelacje
- correlation.update - zaktualizuj korelacje

Obiekt Correlation =

Następujące obiekty są bezpośrednio powiązane z API `correlation`.

Korelacja

Obiekt korelacji ma następujące właściwości.

Właściwość	Typ	Opis
correlationid	ID	ID korelacji. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji
name	string	Nazwa korelacji. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
description	string	Opis korelacji.
status	integer	Określa, czy korelacja jest włączona czy wyłączona. Możliwe wartości: 0 - *(domyślnie)* włączona; 1 - wyłączona.

Operacja korelacji

Obiekt operacji korelacji definiuje operację, która zostanie wykonana po uruchomieniu korelacji. Ma następujące właściwości.

Właściwość	Type	Opis
type	integer	Typ operacji. Możliwe wartości: 0 - zamknij stare zdarzenia; 1 - zamknij nowe zdarzenie. Zachowanie właściwości: - *wymagane*

Filtr korelacji

Obiekt filtra korelacji definiuje zestaw warunków, które muszą zostać spełnione, aby wykonać skonfigurowane operacje korelacji. Ma następujące właściwości.

Właściwość	Typ	Opis
conditions	array	Zestaw warunków filtra używanych do filtrowania wyników. Warunki zostaną posortowane zgodnie z kolejnością ich występowania w formule. Zachowanie właściwości: - *wymagane*
evaltype	integer	Metoda oceny warunków filtra. Możliwe wartości: 0 - And/Or; 1 - And; 2 - Or; 3 - Wyrażenie niestandardowe. Zachowanie właściwości: - *wymagane*
eval_formula	string	Wygenerowane wyrażenie, które będzie używane do oceny warunków filtra. Wyrażenie zawiera identyfikatory odnoszące się do określonych warunków filtra za pomocą ich `formulaid`. Wartość `eval_formula` jest równa wartości `formula` dla filtrów z wyrażeniem niestandardowym. Zachowanie właściwości: - *tylko do odczytu*
formula	string	Wyrażenie zdefiniowane przez użytkownika, używane do oceny warunków filtrów z wyrażeniem niestandardowym. Wyrażenie musi zawierać identyfikatory odnoszące się do określonych warunków filtra za pomocą ich `formulaid`. Identyfikatory użyte w wyrażeniu muszą dokładnie odpowiadać tym zdefiniowanym w warunkach filtra: żaden warunek nie może pozostać nieużyty ani pominięty. Zachowanie właściwości: - *wymagane*, jeśli `evaltype` jest ustawione na „custom expression”

Warunek filtra korelacji

Obiekt warunku filtra korelacji definiuje określony warunek, który musi zostać sprawdzony przed uruchomieniem operacji korelacji.

Property	Type	Description
type	integer	Typ warunku. Możliwe wartości: 0 - tag starego zdarzenia; 1 - tag nowego zdarzenia; 2 - grupa hostów nowego zdarzenia; 3 - para tagów zdarzenia; 4 - wartość tagu starego zdarzenia; 5 - wartość tagu nowego zdarzenia. Zachowanie właściwości: - *wymagane*
tag	string	Tag zdarzenia (starego lub nowego). Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na „tag starego zdarzenia”, „tag nowego zdarzenia”, „wartość tagu starego zdarzenia” lub „wartość tagu nowego zdarzenia”

Property	Type	Description
groupid	ID	ID grupy hostów. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na „grupa hostów nowego zdarzenia”
oldtag	string	Tag starego zdarzenia. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na „para tagów zdarzenia”
newtag	string	Tag starego zdarzenia. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na „para tagów zdarzenia”
value	string	Wartość tagu zdarzenia (starego lub nowego). Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na „wartość tagu starego zdarzenia” lub „wartość tagu nowego zdarzenia”
formulaid	string	Dowolny unikalny identyfikator używany do odwoływania się do warunku z wyrażenia niestandardowego. Może zawierać wyłącznie wielkie litery. Identyfikator musi zostać zdefiniowany przez użytkownika podczas modyfikowania warunków filtra, ale zostanie wygenerowany ponownie przy późniejszym żądaniu ich pobrania.
operator	integer	Operator warunku. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na „grupa hostów nowego zdarzenia”, „wartość tagu starego zdarzenia” lub „wartość tagu nowego zdarzenia”

Note:
Aby lepiej zrozumieć, jak używać filtrów z różnymi typami wyrażeń, zobacz przykłady na stronach metod correlation.get i correlation.create.

Dla każdego typu warunku obsługiwane są następujące operatory i wartości.

Condition	Condition name	Supported operators	Expected value
2	Grupa hostów	=, <>	ID grupy hostów.
4	Wartość tagu starego zdarzenia	=, <>, like, not like	string
5	Wartość tagu nowego zdarzenia	=, <>, like, not like	string

correlation.create

Opis

`object correlation.create(object/array correlations)`

Ta metoda umożliwia tworzenie nowych korelacji.

Note:
Ta metoda jest dostępna tylko dla użytkowników typu *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Korelacje do utworzenia.

Oprócz standardowych właściwości korelacji, metoda akceptuje następujące parametry.

Parametr	Type	Opis
operations	array	Operacje korelacji do utworzenia dla korelacji. Zachowanie parametru: - *wymagany*
filter	object	Obiekt filtra korelacji dla korelacji. Zachowanie parametru: - *wymagany*

Zwracane wartości

`(object)` Zwraca obiekt zawierający ID utworzonych korelacji we właściwości `correlationids`. Kolejność zwracanych ID są zgodne z kolejności przekazanych korelacji.

Przykłady

Utwórz nową korelację tagów zdarzeń

Utwórz korelację, używając metody oceny `AND/OR`, z jednym warunkiem i jedną operacją. Domyślnie korelacja będzie włączona.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "correlation.create",
    "params": {
        "name": "new event tag correlation",
        "filter": {
            "evaltype": 0,
            "conditions": [
                {
                    "type": 1,
                    "tag": "ok"
                }
            ]
        },
        "operations": [
            {
                "type": 0
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "correlationids": [
            "1"
        ]
    },
    "id": 1
}
```

Używanie niestandardowego filtra wyrażenia

Utwórz korelację, która będzie używać niestandardowego warunku filtra. Identyfikatory formuły „A” lub „B” zostały wybrane arbitralnie. Typ warunku będzie „Grupa hostów” z operatorem „<>”.

Żądanie:

```
{
    "jsonrpc": "2.0",
```

```
    "method": "correlation.create",
    "params": {
        "name": "new host group correlation",
        "description": "a custom description",
        "status": 0,
        "filter": {
            "evaltype": 3,
            "formula": "A or B",
            "conditions": [
                {
                    "type": 2,
                    "operator": 1,
                    "formulaid": "A"
                },
                {
                    "type": 2,
                    "operator": 1,
                    "formulaid": "B"
                }
            ]
        },
        "operations": [
            {
                "type": 1
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "correlationids": [
            "2"
        ]
    },
    "id": 1
}
```

Zobacz także

- Filtr korelacji
- Operacja korelacji

Źródło

CCorrelation::create() w *ui/include/classes/api/services/CCorrelation.php*.

correlation.delete

Opis

`object correlation.delete(array correlationids)`

Ta metoda umożliwia usuwanie korelacji.

Note:
Ta metoda jest dostępna tylko dla typu użytkownika *Super admin*. Uprawnienia do wywołania metody można cofnąć w ustawieniach roli użytkownika. Więcej informacji można znaleźć w User roles.

Parametry

`(array)` IDs korelacji do usunięcia.

Zwracane wartości

`(object)` Zwraca obiekt zawierający ID usuniętych korelacji we właściwości `correlationids`.

Przykład

Usuń wiele korelacji

Usuń dwie korelacje.

Żądanie:

```
{
"jsonrpc": "2.0",
"method": "correlation.delete",
"params": [
"1",
"2"
],
"id": 1
}
```

Odpowiedź:

```
{
"jsonrpc": "2.0",
"result": {
"correlationids": [
"1",
"2"
]
},
"id": 1
}
```

Źródło

CCorrelation::delete() w *ui/include/classes/api/services/CCorrelation.php*.

correlation.get

Opis

`integer/array correlation.get(object parameters)`

Ta metoda umożliwia pobieranie korelacji zgodnie z podanymi parametrami.

Note:
Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w User roles.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
correlationids	ID/array	Zwraca tylko korelacje o podanych identyfikatorach.
selectFilter	query	Zwraca właściwość `filter` z warunkami korelacji.
selectOperations	query	Zwraca właściwość `operations` z operacjami korelacji.
sortfield	string/array	Sortuje wynik według podanych właściwości. Możliwe wartości: `correlationid`, `name`, `status`.
countOutput	boolean	Te parametry są opisane w komentarzu referencyjnym.
editable	boolean	
excludeSearch	boolean	
filter	object	

Parametr	Typ	Opis
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca jedną z opcji:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli parametr `countOutput` został użyty.

Przykłady

Pobieranie korelacji

Pobierz wszystkie skonfigurowane korelacje wraz z warunkami i operacjami korelacji. Filtr używa typu oceny „and/or”, dlatego właściwość `formula` jest pusta, a `eval_formula` jest generowana automatycznie.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "correlation.get",
    "params": {
        "output": "extend",
        "selectOperations": "extend",
        "selectFilter": "extend"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "correlationid": "1",
            "name": "Correlation 1",
            "description": "",
            "status": "0",
            "filter": {
                "evaltype": "0",
                "formula": "",
                "conditions": [
                    {
                        "type": "3",
                        "oldtag": "error",
                        "newtag": "ok",
                        "formulaid": "A"
                    }
                ],
                "eval_formula": "A"
            },
            "operations": [
                {
                    "type": "0"
                }
            ]
        }
```

```
    ],
    "id": 1
}
```

Zobacz także

- Filtr korelacji
- Operacja korelacji

Źródło

CCorrelation::get() w *ui/include/classes/api/services/CCorrelation.php*.

correlation.update

Opis

`object correlation.update(object/array correlations)`

Ta metoda umożliwia aktualizację istniejących korelacji.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkownika typu *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Właściwości korelacji do zaktualizowania.

Właściwość `correlationid` musi być zdefiniowana dla każdej korelacji, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko przekazane właściwości, wszystkie pozostałe pozostaną bez zmian.

Oprócz standardowych właściwości korelacji, metoda akceptuje następujące parametry.

Parametr	Typ	Opis
filter	object	Obiekt filtra korelacji zastępujący bieżący filtr.
operations	array	Operacje korelacji zastępujące istniejące operacje.

Zwracane wartości

`(object)` Zwraca obiekt zawierajacy identyfikatory zaktualizowanych korelacji we właściwości ‘correlationids.

Przykłady

Wyłącz korelację

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "correlation.update",
    "params": {
        "correlationid": "1",
        "status": "1"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "correlationids": [
            "1"
        ]
    },
```

```
    "id": 1
}
```

Zastąp warunki, ale zachowaj metodę oceny

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "correlation.update",
    "params": {
        "correlationid": "1",
        "filter": {
            "conditions": [
                {
                    "type": 3,
                    "oldtag": "error",
                    "newtag": "ok"
                }
            ]
        }
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "correlationids": [
            "1"
        ]
    },
    "id": 1
}
```

Zobacz także

- Filtr korelacji
- Operacja korelacji

Źródło

CCorrelation::update() w *ui/include/classes/api/services/CCorrelation.php*.

Makro użytkownika

Ta klasa jest przeznaczona do pracy z makrami użytkownika na poziomie hosta oraz globalnymi makrami użytkownika.

Odwołania do obiektów:

- Makro globalne
- Makro hosta
    - Konfiguracja makra

Dostępne metody:

- usermacro.create - utwórz nowe makra hosta
- usermacro.createglobal - utwórz nowe makra globalne
- usermacro.delete - usuń makra hosta
- usermacro.deleteglobal - usuń makra globalne
- usermacro.get - pobierz makra hosta i makra globalne
- usermacro.update - zaktualizuj makra hosta
- usermacro.updateglobal - zaktualizuj makra globalne

Obiekt makra użytkownika

Następujące obiekty są bezpośrednio powiązane z API `usermacro`.

Makro globalne

Obiekt makra globalnego ma następujące właściwości.

Właściwość	Typ	Opis
globalmacroid	ID	ID makra globalnego. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji
description	string	Opis makra.
macro	string	Ciąg makra. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
type	integer	Typ makra. Możliwe wartości: 0 - *(domyślnie)* Makro tekstowe; 1 - Makro sekretne; 2 - Sekret Vault.
value	string	Wartość makra. Zachowanie właściwości: - *tylko do zapisu*, jeśli `type` jest ustawione na „Makro sekretne” - *wymagane* dla operacji tworzenia

Makro hosta

Obiekt makra hosta definiuje makro dostępne na hoście, prototypie hosta lub szablonie. Ma następujące właściwości.

Właściwość	Typ	Opis
hostmacroid	ID	ID makra. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji
automatic	integer	Określa, czy makro jest kontrolowane przez regułę wykrywania. Możliwe wartości: 0 - *(domyślnie)* Makro jest zarządzane przez użytkownika; 1 - Makro jest zarządzane przez regułę wykrywania. Użytkownik nie może tworzyć automatycznego makra. Aby zaktualizować automatyczne makro, musi ono zostać przekształcone na ręczne.
config	object/array	Konfiguracja makra odpowiedzialna za sposób wyświetlania makra w Kreatorze hosta.
description	string	Opis makra.
hostid	ID	ID hosta, prototypu hosta lub szablonu, do którego należy makro. Zachowanie właściwości: - *stała* - *wymagane* dla operacji tworzenia
macro	string	Ciąg makra. Zachowanie właściwości: - *wymagane* dla operacji tworzenia

Właściwość	Typ	Opis
type	integer	Typ makra. Możliwe wartości: 0 - *(domyślnie)* Makro tekstowe; 1 - Makro tajne; 2 - Sekret z magazynu.
value	string	Wartość makra. Zachowanie właściwości: - *tylko do zapisu*, jeśli `type` jest ustawione na „Makro tajne” - *wymagane* dla operacji tworzenia

Konfiguracja makr

Obiekt konfiguracji makr definiuje sposób wyświetlania makra w Kreatorze hosta.

Właściwość	Typ	Opis
type	integer	Typ pola wejściowego makra. Możliwe wartości: 0 - Makro nie jest używane w Kreatorze hosta; 1 - Pole tekstowe; 2 - Lista; 3 - Pole wyboru. Zachowanie właściwości: - *wymagane*
label	string	Etykieta pola wejściowego makra. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na „Pole tekstowe”, „Lista” lub „Pole wyboru”
description	text	Tekst pomocy wyświetlany obok pola wejściowego makra. Obsługuje formatowanie Markdown.
priority	integer	Pozycja pola wejściowego makra na liście makr. Jeśli `priority` nie jest ustawione, makro jest dodawane na końcu listy niepogrupowanych makr.
required	integer	Oznacza makro jako obowiązkowe. Możliwe wartości: 0 - Nieobowiązkowe; 1 - Obowiązkowe. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na „Pole tekstowe” lub „Lista”
regex	string	Wyrażenie regularne służące do walidacji danych wejściowych użytkownika w polu tekstowym. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na „Pole tekstowe”
section_name	string	Etykieta zwijanej sekcji, w której makro jest grupowane. Jeśli `section_name` nie jest ustawione, makro nie jest grupowane. Niepogrupowane makra są wyświetlane jako pierwsze; pogrupowane makra są wyświetlane poniżej, uporządkowane według ich `priority` w obrębie każdej zwijanej sekcji.

Właściwość	Typ	Opis
options	text	Ciąg JSON definiujący elementy listy lub wartości pola wyboru. Dla list: tablica obiektów z właściwościami `value` i `text`. Przykład: `[{"value": "http", "text": "HTTP"}, {"value": "https", "text": "HTTPS"}]` Dla pól wyboru: obiekt z właściwościami `checked` i `unchecked`. Przykład: `{"checked": true, "unchecked": false}` Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na „Lista” lub „Pole wyboru”

usermacro.create

Opis

`object usermacro.create(object/array hostMacros)`

Ta metoda umożliwia tworzenie nowych makr hosta.

Note:
Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Makra hosta do utworzenia.

Metoda akceptuje makra hosta ze standardowymi właściwościami makr hosta.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory utworzonych makr hosta we właściwości `hostmacroids`. Kolejność zwróconych identyfikatorów odpowiada kolejności przekazanych makr hosta.

Przykłady

Tworzenie makra hosta

Utwórz makro hosta ”{$SNMP_COMMUNITY}” o wartości ”public” na hoście ”10198”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "usermacro.create",
    "params": {
        "hostid": "10198",
        "macro": "{$SNMP_COMMUNITY}",
        "value": "public"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "hostmacroids": [
            "11"
        ]
    },
    "id": 1
}
```

Źródło

CUserMacro::create() w *ui/include/classes/api/services/CUserMacro.php*.

usermacro.createglobal

Opis

`object usermacro.createglobal(object/array globalMacros)`

Ta metoda umożliwia tworzenie nowych makr globalnych.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkowników typu *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Zobacz User roles , aby uzyskać więcej informacji.

Parametry

`(object/array)` Makra globalne do utworzenia.

Metoda akceptuje makra globalne ze standardowymi właściwościami makr globalnych.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory utworzonych makr globalnych we właściwości `globalmacroids`. Kolejność zwróconych identyfikatorów odpowiada kolejności przekazanych makr globalnych.

Przykłady

Tworzenie makra globalnego

Utwórz makro globalne "{$SNMP_COMMUNITY}" o wartości "public".

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "usermacro.createglobal",
    "params":  {
        "macro": "{$SNMP_COMMUNITY}",
        "value": "public"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "globalmacroids": [
            "6"
        ]
    },
    "id": 1
}
```

Źródło

CUserMacro::createGlobal() w *ui/include/classes/api/services/CUserMacro.php*.

usermacro.delete

Opis

`object usermacro.delete(array hostMacroIds)`

Ta metoda pozwala na usuwanie makr hosta.

Note:
Ta metoda jest dostępna tylko dla użytkowników typu *Admin* i *Super admin*. Uprawnienia do wywołania metody można odwołać w ustawieniach roli użytkownika. Więcej informacji można znaleźć w Role użytkownika.

Parametry

`(array)` ID makr hosta do usunięcia.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory usuniętych makr hosta we właściwości `hostmacroids`.

Przykłady

Usuwanie wielu makr hosta

Usuń dwa makra hosta.

Żądanie:

```
{
"jsonrpc": "2.0",
"method": "usermacro.delete",
"params": [
"32",
"11"
],
"id": 1
}
```

Odpowiedź:

```
{
"jsonrpc": "2.0",
"result": {
"hostmacroids": [
"32",
"11"
]
},
"id": 1
}
```

Źródło

CUserMacro::delete() w *ui/include/classes/api/services/CUserMacro.php*.

usermacro.deleteglobal

Opis

`object usermacro.deleteglobal(array globalMacroIds)`

Ta metoda pozwala na usuwanie makr globalnych.

Note:
Ta metoda jest dostępna tylko dla typu użytkownika *Super admin*. Uprawnienia do wywołania metody można cofnąć w ustawieniach roli użytkownika. Więcej informacji można znaleźć w User roles.

Parametry

`(array)` ID globalnych makr do usunięcia.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory usuniętych globalnych makr we właściwości `globalmacroids`.

Przykłady

Usuwanie wielu makr globalnych

Usuń dwie makra globalne.

Żądanie:

```
{
"jsonrpc": "2.0",
"method": "usermacro.deleteglobal",
"params": [
"32",
"11"
],
"id": 1
}
```

Odpowiedź:

```
{
"jsonrpc": "2.0",
"result": {
"globalmacroids": [
"32",
"11"
]
},
"id": 1
}
```

Źródło

CUserMacro::deleteGlobal() w *ui/include/classes/api/services/CUserMacro.php*.

usermacro.get

Opis

`integer/array usermacro.get(object parameters)`

Ta metoda umożliwia pobieranie makr hosta i makr globalnych zgodnie z podanymi parametrami.

> **Note:**
> Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
globalmacro	flag	Zwraca makra globalne zamiast makr hosta.
globalmacroids	ID/array	Zwraca tylko makra globalne o podanych identyfikatorach.
groupids	ID/array	Zwraca tylko makra hosta należące do hostów lub szablonów z podanych grup hostów lub grup szablonów.
hostids	ID/array	Zwraca tylko makra należące do podanych hostów lub szablonów.
hostmacroids	ID/array	Zwraca tylko makra hosta o podanych identyfikatorach.
inherited	boolean	Jeśli ustawione na `true`, zwraca tylko makra użytkownika prototypu hosta dziedziczone z szablonu.
selectHostGroups	query	Zwraca grupy hostów, do których należy makro hosta, we właściwości `hostgroups`. Używane tylko podczas pobierania makr hosta.
selectHosts	query	Zwraca hosty, do których należy makro hosta, we właściwości `hosts`. Używane tylko podczas pobierania makr hosta.

Parametr	Typ	Opis
selectTemplateGroups	query	Zwraca grupy szablonów, do których należy makro szablonu, we właściwości `templategroups`. Używane tylko podczas pobierania makr szablonu.
selectTemplates	query	Zwraca szablony, do których należy makro hosta, we właściwości `templates`. Używane tylko podczas pobierania makr hosta.
sortfield	string/array	Sortuje wynik według podanych właściwości. Możliwe wartości: `macro`.
countOutput	boolean	Te parametry opisano w komentarzu referencyjnym.
editable	boolean	
excludeSearch	boolean	
filter	object	
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli został użyty parametr `countOutput`.

Przykłady

Pobieranie makr hosta dla hosta

Pobierz wszystkie makra hosta zdefiniowane dla hosta „10198”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "usermacro.get",
    "params": {
        "output": "extend",
        "hostids": "10198"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "hostmacroid": "9",
            "hostid": "10198",
            "macro": "{$INTERFACE}",
            "value": "eth0",
            "description": "",
            "type": "0",
            "automatic": "0"
        },
        {
            "hostmacroid": "11",
```

```
            "hostid": "10198",
            "macro": "{$SNMP_COMMUNITY}",
            "value": "public",
            "description": "",
            "type": "0",
            "automatic": "0"
        }
    ],
    "id": 1
}
```

Pobieranie makr hosta dla szablonu

Pobierz makra hosta zdefiniowane dla szablonu „10265”, które zawierają „STATUS” w nazwie makra.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "usermacro.get",
    "params": {
        "output": "extend",
        "hostids": "10265",
        "search": {
            "macro": "STATUS"
        }
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "hostmacroid": "6709",
            "hostid": "10265",
            "macro": "{$APACHE.STATUS.HOST}",
            "value": "",
            "description": "Nazwa hosta lub adres IP hosta strony statusu Apache.",
            "type": "0",
            "automatic": "0",
            "config": {
                "type": "1",
                "priority": "1",
                "section_name": "",
                "label": "Host statusu Apache",
                "description": "Nazwa hosta lub adres IP hosta strony statusu Apache.",
                "required": "1",
                "regex": "",
                "options": []
            }
        },
        {
            "hostmacroid": "814",
            "hostid": "10265",
            "macro": "{$APACHE.STATUS.PATH}",
            "value": "server-status?auto",
            "description": "Ścieżka URL strony statusu Apache.",
            "type": "0",
            "automatic": "0",
            "config": {
                "type": "1",
                "priority": "3",
```

```
                "section_name": "",
                "label": "Ścieżka strony statusu Apache",
                "description": "Ścieżka URL strony statusu Apache.",
                "required": "1",
                "regex": "",
                "options": []
            }
        },
        {
            "hostmacroid": "815",
            "hostid": "10265",
            "macro": "{$APACHE.STATUS.PORT}",
            "value": "80",
            "description": "Port strony statusu Apache.",
            "type": "0",
            "automatic": "0",
            "config": {
                "type": "1",
                "priority": "2",
                "section_name": "",
                "label": "Port strony statusu Apache",
                "description": "W zakresie od 1 do 65535 włącznie.",
                "required": "1",
                "regex": "^-?([0-9]+|(([0-9]+)\\.([0-9]+)))$",
                "options": []
            }
        },
        {
            "hostmacroid": "816",
            "hostid": "10265",
            "macro": "{$APACHE.STATUS.SCHEME}",
            "value": "http",
            "description": "Schemat żądania, którym może być HTTP lub HTTPS.",
            "type": "0",
            "automatic": "0",
            "config": {
                "type": "2",
                "priority": "4",
                "section_name": "",
                "label": "Schemat żądania",
                "description": "Schemat żądania, którym może być HTTP lub HTTPS.",
                "required": "0",
                "regex": "",
                "options": [
                    {
                        "value": "http",
                        "text": "HTTP"
                    },
                    {
                        "value": "https",
                        "text": "HTTPS"
                    }
                ]
            }
        }
    ],
    "id": 1
}
```


Pobieranie makr globalnych

Pobierz wszystkie makra globalne.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "usermacro.get",
    "params": {
        "output": "extend",
        "globalmacro": true
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "globalmacroid": "6",
            "macro": "{$SNMP_COMMUNITY}",
            "value": "public",
            "description": "",
            "type": "0"
        }
    ],
    "id": 1
}
```

Źródło

CUserMacro::get() w *ui/include/classes/api/services/CUserMacro.php*.

usermacro.update

Opis

`object usermacro.update(object/array hostMacros)`

Ta metoda umożliwia aktualizację istniejących makr hosta.

Note:
Ta metoda jest dostępna tylko dla użytkowników typu *Admin* i *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Właściwości makra hosta, które mają zostać zaktualizowane.

Właściwość `hostmacroid` musi być zdefiniowana dla każdego makra hosta, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko przekazane właściwości, wszystkie pozostałe pozostaną bez zmian.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych makr hosta we właściwości `hostmacroids`.

Przykłady

Zmiana wartości makra hosta

Zmień wartość makra hosta na „public”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "usermacro.update",
    "params": {
        "hostmacroid": "1",
        "value": "public"
    },
```

```
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "hostmacroids": [
            "1"
        ]
    },
    "id": 1
}
```

Zmień wartość makra utworzonego przez regułę wykrywania

Zmień utworzone przez regułę wykrywania makro „automatic” na „manual” i zmień jego wartość na „new-value”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "usermacro.update",
    "params": {
        "hostmacroid": "1",
        "value": "new-value",
        "automatic": "0"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "hostmacroids": [
            "1"
        ]
    },
    "id": 1
}
```

Źródło

CUserMacro::update() w *ui/include/classes/api/services/CUserMacro.php*.

usermacro.updateglobal

Opis

`object usermacro.updateglobal(object/array globalMacros)`

Ta metoda umożliwia aktualizację istniejących globalnych makr.

> **Note:**
> Ta metoda jest dostępna wyłącznie dla użytkowników typu *Super admin*. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Właściwości makra globalnego, które mają zostać zaktualizowane.

Właściwość `globalmacroid` musi być zdefiniowana dla każdego makra globalnego, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko przekazane właściwości, wszystkie pozostałe pozostaną bez zmian.

Zwracane wartości

(object) Zwraca obiekt zawierający identyfikatory zaktualizowanego globalnego makra pod właściwością globalmacroids.

Przykłady

Zmiana wartości makra globalnego

Zmień wartość makra globalnego na „public”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "usermacro.updateglobal",
    "params": {
        "globalmacroid": "1",
        "value": "public"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "globalmacroids": [
            "1"
        ]
    },
    "id": 1
}
```

Źródło

CUserMacro::updateGlobal() in *ui/include/classes/api/services/CUserMacro.php*.

Mapa

Ta klasa jest przeznaczona do pracy z mapami.

Odwołania do obiektów:

- Mapa
- Element mapy
  - Element mapy Host
  - Element mapy Grupa hostów
  - Element mapy Mapa
  - Element mapy Wyzwalacz
  - Element mapy Tag
  - Element mapy URL
- Łącze mapy
  - Wyzwalacz łącza mapy
  - Wskaźniki łącza mapy
- URL mapy
- Użytkownik mapy
- Grupa użytkowników mapy
- Kształty mapy
- Linie mapy

Dostępne metody:

- map.create - utwórz nowe mapy
- map.delete - usuń mapy
- map.get - pobierz mapy
- map.update - zaktualizuj mapy

Obiekt mapy

Następujące obiekty są bezpośrednio powiązane z API `map`.

Mapa

Obiekt mapy ma następujące właściwości.

Właściwość	Typ	Opis
sysmapid	ID	ID mapy. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji
height	integer	Wysokość mapy w pikselach. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
name	string	Nazwa mapy. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
width	integer	Szerokość mapy w pikselach. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
backgroundid	ID	ID obrazu używanego jako tło mapy.
background_scale	integer	Czy włączyć proporcjonalne skalowanie obrazu tła. Możliwe wartości: 0 - wyłącz skalowanie; 1 - *(domyślnie)* włącz skalowanie obrazu.
expand_macros	integer	Czy rozwijać makra w etykietach podczas konfigurowania mapy. Możliwe wartości: 0 - *(domyślnie)* nie rozwijaj makr; 1 - rozwijaj makra.
expandproblem	integer	Czy wyzwalacz problemu będzie wyświetlany dla elementów z pojedynczym problemem. Możliwe wartości: 0 - zawsze wyświetlaj liczbę problemów; 1 - *(domyślnie)* wyświetlaj wyzwalacz problemu, jeśli istnieje tylko jeden problem.
grid_align	integer	Czy włączyć wyrównywanie do siatki. Możliwe wartości: 0 - wyłącz wyrównywanie do siatki; 1 - *(domyślnie)* włącz wyrównywanie do siatki.
grid_show	integer	Czy wyświetlać siatkę na mapie. Możliwe wartości: 0 - nie wyświetlaj siatki; 1 - *(domyślnie)* wyświetlaj siatkę.
grid_size	integer	Rozmiar siatki mapy w pikselach. Obsługiwane wartości: 20, 40, 50, 75 i 100. Domyślnie: 50.
highlight	integer	Czy podświetlanie ikon jest włączone. Możliwe wartości: 0 - podświetlanie wyłączone; 1 - *(domyślnie)* podświetlanie włączone.
iconmapid	ID	ID mapy ikon używanej na mapie.

Właściwość	Typ	Opis
label_format	integer	Czy włączyć zaawansowane etykiety. Możliwe wartości: 0 - *(domyślnie)* wyłącz zaawansowane etykiety; 1 - włącz zaawansowane etykiety.
label_location	integer	Położenie etykiety elementu mapy. Możliwe wartości: 0 - *(domyślnie)* dół; 1 - lewo; 2 - prawo; 3 - góra.
label_string_host	string	Niestandardowa etykieta dla elementów typu host. Zachowanie właściwości: - *wymagane*, jeśli `label_type_host` jest ustawione na ”custom”
label_string_hostgroup	string	Niestandardowa etykieta dla elementów grupy hostów. Zachowanie właściwości: - *wymagane*, jeśli `label_type_hostgroup` jest ustawione na ”custom”
label_string_image	string	Niestandardowa etykieta dla elementów obrazu. Zachowanie właściwości: - *wymagane*, jeśli `label_type_image` jest ustawione na ”custom”
label_string_map	string	Niestandardowa etykieta dla elementów mapy. Zachowanie właściwości: - *wymagane*, jeśli `label_type_map` jest ustawione na ”custom”
label_string_trigger	string	Niestandardowa etykieta dla elementów wyzwalacza. Zachowanie właściwości: - *wymagane*, jeśli `label_type_trigger` jest ustawione na ”custom”
label_type	integer	Typ etykiety elementu mapy. Możliwe wartości: 0 - etykieta; 1 - adres IP; 2 - *(domyślnie)* nazwa elementu; 3 - tylko status; 4 - nic.
label_type_host	integer	Typ etykiety dla elementów typu host. Możliwe wartości: 0 - etykieta; 1 - adres IP; 2 - *(domyślnie)* nazwa elementu; 3 - tylko status; 4 - nic; 5 - niestandardowa.
label_type_hostgroup	integer	Typ etykiety dla elementów grupy hostów. Możliwe wartości: 0 - etykieta; 2 - *(domyślnie)* nazwa elementu; 3 - tylko status; 4 - nic; 5 - niestandardowa.

Właściwość	Typ	Opis
label_type_image	integer	Typ etykiety dla elementów grupy hostów. Możliwe wartości: 0 - etykieta; 2 - *(domyślnie)* nazwa elementu; 4 - nic; 5 - niestandardowa.
label_type_map	integer	Typ etykiety dla elementów mapy. Możliwe wartości: 0 - etykieta; 2 - *(domyślnie)* nazwa elementu; 3 - tylko status; 4 - nic; 5 - niestandardowa.
label_type_trigger	integer	Typ etykiety dla elementów wyzwalacza. Możliwe wartości: 0 - etykieta; 2 - *(domyślnie)* nazwa elementu; 3 - tylko status; 4 - nic; 5 - niestandardowa.
markelements	integer	Czy podświetlać elementy mapy, których status ostatnio się zmienił. Możliwe wartości: 0 - *(domyślnie)* nie podświetlaj elementów; 1 - podświetlaj elementy.
severity_min	integer	Minimalny poziom ważności wyzwalaczy, które będą wyświetlane na mapie. Zobacz właściwość `severity` wyzwalacza, aby uzyskać listę obsługiwanych poziomów ważności wyzwalaczy.
show_element_label	integer	Jak domyślnie wyświetlać etykiety elementów. Możliwe wartości: 0 - zawsze wyświetlaj; 1 - *(domyślnie)* ukrywaj automatycznie.
show_link_label	integer	Jak domyślnie wyświetlać etykiety łączy. Możliwe wartości: 0 - zawsze wyświetlaj; 1 - *(domyślnie)* ukrywaj automatycznie.
show_unack	integer	Jak mają być wyświetlane problemy. Możliwe wartości: 0 - *(domyślnie)* wyświetlaj liczbę wszystkich problemów; 1 - wyświetlaj tylko liczbę niepotwierdzonych problemów; 2 - wyświetlaj osobno liczbę potwierdzonych i niepotwierdzonych problemów.
userid	ID	ID użytkownika będącego właścicielem mapy.
private	integer	Typ udostępniania mapy. Możliwe wartości: 0 - mapa publiczna; 1 - *(domyślnie)* mapa prywatna.
show_suppressed	integer	Czy wyciszone problemy są wyświetlane. Możliwe wartości: 0 - *(domyślnie)* ukrywaj wyciszone problemy; 1 - wyświetlaj wyciszone problemy.

Element mapy

Obiekt elementu mapy definiuje obiekt wyświetlany na mapie. Ma on następujące właściwości.

Właściwość	Typ	Opis
selementid	ID	ID elementu mapy. Zachowanie właściwości: - *tylko do odczytu*
elements	array	Obiekt danych elementu. Zachowanie właściwości: - *wymagane*, jeśli `elementtype` jest ustawione na ”host”, ”map”, ”trigger” lub ”host group”
elementtype	integer	Typ elementu mapy. Możliwe wartości: 0 - host; 1 - mapa; 2 - wyzwalacz; 3 - grupa hostów; 4 - obraz. Zachowanie właściwości: - *wymagane*
iconid_off	ID	ID obrazu używanego do wyświetlania elementu w stanie domyślnym. Zachowanie właściwości: - *wymagane*
areatype	integer	Sposób wyświetlania oddzielnych hostów grupy hostów. Możliwe wartości: 0 - *(domyślnie)* element grupy hostów zajmie całą mapę; 1 - element grupy hostów będzie miał stały rozmiar.
elementsubtype	integer	Sposób wyświetlania elementu grupy hostów na mapie. Możliwe wartości: 0 - *(domyślnie)* wyświetl grupę hostów jako pojedynczy element; 1 - wyświetl każdy host w grupie oddzielnie.
evaltype	integer	Warunek filtrowania tagów elementu mapy, metoda obliczania. Możliwe wartości: 0 - *(domyślnie)* And/Or; 2 - Or.
height	integer	Wysokość elementu grupy hostów o stałym rozmiarze w pikselach. Domyślnie: 200.
iconid_disabled	ID	ID obrazu używanego do wyświetlania wyłączonych elementów mapy. Zachowanie właściwości: - *obsługiwane*, jeśli `elementtype` jest ustawione na ”host”, ”map”, ”trigger” lub ”host group”
iconid_maintenance	ID	ID obrazu używanego do wyświetlania elementów mapy w konserwacji. Zachowanie właściwości: - *obsługiwane*, jeśli `elementtype` jest ustawione na ”host”, ”map”, ”trigger” lub ”host group”
iconid_on	ID	ID obrazu używanego do wyświetlania elementów mapy z problemami. Zachowanie właściwości: - *obsługiwane*, jeśli `elementtype` jest ustawione na ”host”, ”map”, ”trigger” lub ”host group”
label	string	Etykieta elementu.

Właściwość	Typ	Opis
label_location	integer	Położenie etykiety elementu mapy. Możliwe wartości: -1 - *(domyślnie)* położenie domyślne; 0 - dół; 1 - lewo; 2 - prawo; 3 - góra.
permission	integer	Typ poziomu uprawnień. Możliwe wartości: -1 - brak; 2 - tylko do odczytu; 3 - odczyt-zapis.
show_label	integer	Sposób wyświetlania etykiety elementu. Możliwe wartości: -1 - *(domyślnie)* domyślne ustawienie mapy; 0 - zawsze wyświetlaj; 1 - ukrywaj automatycznie.
sysmapid	ID	ID mapy, do której należy element. Zachowanie właściwości: - *tylko do odczytu*
urls	array	Adresy URL elementu mapy. Obiekt URL elementu mapy jest opisany szczegółowo poniżej.
use_iconmap	integer	Czy mapowanie ikon musi być używane dla elementów typu host. Możliwe wartości: 0 - nie używaj mapowania ikon; 1 - *(domyślnie)* używaj mapowania ikon.
viewtype	integer	Algorytm rozmieszczania elementu grupy hostów. Możliwe wartości: 0 - *(domyślnie)* siatka.
width	integer	Szerokość elementu grupy hostów o stałym rozmiarze w pikselach. Domyślnie: 200.
x	integer	Współrzędna X elementu w pikselach. Domyślnie: 0.
y	integer	Współrzędna Y elementu w pikselach. Domyślnie: 0.
zindex	integer	Wartość używana do porządkowania elementów mapy (z-index). Domyślnie: 0.

Element mapy Host

Obiekt elementu mapy Host definiuje jeden element hosta.

Właściwość	Typ	Opis
hostid	ID	ID hosta.

Element mapy Grupa hostów

Obiekt elementu mapy Grupa hostów definiuje jeden element grupy hostów.

Właściwość	Typ	Opis
groupid	ID	ID grupy hostów.

Obiekt elementu mapy Map

Obiekt elementu mapy Map definiuje jeden element mapy.

Właściwość	Type	Opis
sysmapid	ID	ID mapy.

Wyzwalacz elementu mapy

Obiekt wyzwalacza elementu mapy definiuje jeden lub więcej elementów wyzwalacza.

Właściwość	Type	Opis
triggerid	ID	ID wyzwalacza.

Tag elementu mapy

Obiekt Tag elementu mapy ma następujące właściwości.

Właściwość	Typ	Opis
tag	string	Nazwa tagu elementu mapy. Zachowanie właściwości: - *wymagane*
operator	integer	Warunek operatora tagu elementu mapy. Możliwe wartości: 0 - *(domyślnie)* Zawiera; 1 - Równa się; 2 - Nie zawiera; 3 - Nie równa się; 4 - Istnieje; 5 - Nie istnieje.
value	string	Wartość tagu elementu mapy.

URL elementu mapy

Obiekt URL elementu mapy definiuje klikalny link, który będzie dostępny dla określonego elementu mapy. Ma następujące właściwości:

Właściwość	Typ	Opis
sysmapelementurlid	ID	ID URL elementu mapy. Zachowanie właściwości: - *tylko do odczytu*
name	string	Podpis linku. Zachowanie właściwości: - *wymagane*
url	string	URL linku. Zachowanie właściwości: - *wymagane*
selementid	ID	ID elementu mapy, do którego należy URL.

Łącze mapy

Obiekt łącza mapy definiuje połączenie między dwoma elementami mapy. Ma następujące właściwości.

Właściwość	Typ	Opis
linkid	ID	ID łącza mapy. Zachowanie właściwości: - *tylko do odczytu*
sysmapid	ID	ID mapy, do której należy łącze.
selementid1	ID	ID pierwszego elementu mapy połączonego z jednej strony. Zachowanie właściwości: - *wymagane*
selementid2	ID	ID pierwszego elementu mapy połączonego z drugiej strony. Zachowanie właściwości: - *wymagane*
drawtype	integer	Styl rysowania linii łącza. Możliwe wartości: 0 - *(domyślnie)* linia; 2 - linia pogrubiona; 3 - linia kropkowana; 4 - linia kreskowana.
color	string	Kolor linii jako szesnastkowy kod koloru. Domyślnie: 000000.
label	string	Etykieta łącza.
show_label	integer	Sposób wyświetlania etykiety łącza. Możliwe wartości: -1 - *(domyślnie)* domyślne ustawienie mapy; 0 - zawsze wyświetlaj; 1 - ukrywaj automatycznie.
indicator_type	integer	Wybór typu wskaźnika łącza. Możliwe wartości: 0 - *(domyślnie)* łącze statyczne; 1 - wyzwalacz; 2 - wartość pozycji.
linktriggers	array	Wyzwalacze łącza mapy używane jako wskaźniki stanu łącza. Obiekt wyzwalacza łącza mapy jest opisany szczegółowo poniżej. Zachowanie właściwości: - *wymagane*, jeśli `indicator_type` jest ustawione na ”trigger” (1).
itemid	ID	ID pozycji. Zachowanie właściwości: - *wymagane*, jeśli `indicator_type` jest ustawione na ”item value” (2).
highlights	array	Wyróżnienia łącza mapy używane jako wskaźniki stanu łącza. Obiekt wskaźników łącza mapy jest opisany szczegółowo poniżej. Zachowanie właściwości: - *wymagane*, jeśli `indicator_type` jest ustawione na ”item value” (2).

Właściwość	Typ	Opis
thresholds	array	Progi łącza mapy używane jako wskaźniki stanu łącza. Obiekt wskaźników łącza mapy jest opisany szczegółowo poniżej. Zachowanie właściwości: - *wymagane*, jeśli `indicator_type` jest ustawione na ”item value” (2).
permission	integer	Typ poziomu uprawnień. Możliwe wartości: -1 - brak; 2 - tylko do odczytu; 3 - odczyt-zapis.

Wyzwalacz łącza mapy

Obiekt wyzwalacza łącza mapy definiuje wskaźnik stanu łącza mapy na podstawie stanu wyzwalacza. Ma następujące właściwości:

Właściwość	Typ	Opis
triggerid	ID	ID wyzwalacza używanego jako wskaźnik łącza. Zachowanie właściwości: - *wymagane*
color	string	Kolor wskaźnika jako szesnastkowy kod koloru. Domyślnie: `DD0000`.
drawtype	integer	Styl rysowania wskaźnika. Możliwe wartości: 0 - *(domyślnie)* linia; 2 - linia pogrubiona; 3 - linia kropkowana; 4 - linia przerywana.

Wskaźniki łączy mapy

Obiekt wskaźników łączy mapy definiuje wskaźnik stanu łącza mapy na podstawie wartości pozycji. Ma następujące właściwości:

Właściwość	Typ	Opis
pattern	string	Wyrażenie regularne do porównania. Dostępne tylko dla wyróżnień.
sortorder	integer	Używane do definiowania kolejności sortowania wyróżnień. Dostępne tylko dla wyróżnień.
threshold	string	Wartość liczbowa do porównania. Dostępne tylko dla progów.
drawtype	integer	Styl rysowania wskaźnika. Możliwe wartości: 0 - *(domyślnie)* linia; 2 - linia pogrubiona; 3 - linia kropkowana; 4 - linia kreskowana.
color	string	Kolor wskaźnika jako szesnastkowy kod koloru. Domyślnie: `DD0000`. Zachowanie właściwości: - *wymagane*

URL mapy

Obiekt URL mapy definiuje klikalny link, który będzie dostępny dla wszystkich elementów określonego typu na mapie. Ma następujące właściwości:

Właściwość	Typ	Opis
sysmapurlid	ID	ID URL mapy. Zachowanie właściwości: - *tylko do odczytu*
name	string	Podpis linku. Zachowanie właściwości: - *wymagane*
url	string	URL linku. Zachowanie właściwości: - *wymagane*
elementtype	integer	Typ elementu mapy, dla którego URL będzie dostępny. Listę obsługiwanych typów można znaleźć we właściwości `type` elementu mapy. Domyślnie: 0.
sysmapid	ID	ID mapy, do której należy URL.

Użytkownik mapy

Lista uprawnień do mapy na podstawie użytkowników. Ma następujące właściwości:

Właściwość	Typ	Opis
sysmapuserid	ID	ID użytkownika mapy. Zachowanie właściwości: - *tylko do odczytu*
userid	ID	ID użytkownika. Zachowanie właściwości: - *wymagane*
permission	integer	Typ poziomu uprawnień. Możliwe wartości: 2 - tylko do odczytu; 3 - odczyt-zapis. Zachowanie właściwości: - *wymagane*

Grupa użytkowników mapy

Lista uprawnień do mapy opartych na grupach użytkowników. Ma następujące właściwości:

Właściwość	Type	Opis
sysmapusrgrpid	ID	ID grupy użytkowników mapy. Property behavior: - *tylko do odczytu*
usrgrpid	ID	ID grupy użytkowników. Property behavior: - *wymagane*

Właściwość	Type	Opis
permission	integer	Typ poziomu uprawnień. Możliwe wartości: 2 - tylko do odczytu; 3 - odczyt-zapis. Property behavior: - *wymagane*

Kształty mapy

Obiekt kształtu mapy definiuje kształt geometryczny (z tekstem lub bez) wyświetlany na mapie. Ma następujące właściwości:

Właściwość	Typ	Opis
sysmap_shapeid	ID	ID elementu kształtu mapy. Zachowanie właściwości: - *tylko do odczytu*
type	integer	Typ elementu kształtu mapy. Możliwe wartości: 0 - prostokąt; 1 - elipsa. Właściwość jest wymagana podczas tworzenia nowych kształtów. Zachowanie właściwości: - *wymagane*
x	integer	Współrzędne X kształtu w pikselach. Domyślnie: 0.
y	integer	Współrzędne Y kształtu w pikselach. Domyślnie: 0.
width	integer	Szerokość kształtu w pikselach. Domyślnie: 200.
height	integer	Wysokość kształtu w pikselach. Domyślnie: 200.
text	string	Tekst kształtu.
font	integer	Czcionka tekstu wewnątrz kształtu. Możliwe wartości: 0 - Georgia, serif 1 - “Palatino Linotype”, “Book Antiqua”, Palatino, serif 2 - “Times New Roman”, Times, serif 3 - Arial, Helvetica, sans-serif 4 - “Arial Black”, Gadget, sans-serif 5 - “Comic Sans MS”, cursive, sans-serif 6 - Impact, Charcoal, sans-serif 7 - “Lucida Sans Unicode”, “Lucida Grande”, sans-serif 8 - Tahoma, Geneva, sans-serif 9 - “Trebuchet MS”, Helvetica, sans-serif 10 - Verdana, Geneva, sans-serif 11 - “Courier New”, Courier, monospace 12 - “Lucida Console”, Monaco, monospace Domyślnie: 9.

Właściwość	Typ	Opis
font_size	integer	Rozmiar czcionki w pikselach. Domyślnie: 11.
font_color	string	Kolor czcionki. Domyślnie: 000000.
text_halign	integer	Poziome wyrównanie tekstu. Możliwe wartości: 0 - środek; 1 - do lewej; 2 - do prawej. Domyślnie: 0.
text_valign	integer	Pionowe wyrównanie tekstu. Możliwe wartości: 0 - środek; 1 - góra; 2 - dół. Domyślnie: 0.
border_type	integer	Typ obramowania. Możliwe wartości: 0 - brak; 1 - ──────; 2 - ┅; 3 - ╌ ╌ ╌. Domyślnie: 0.
border_width	integer	Szerokość obramowania w pikselach. Domyślnie: 0.
border_color	string	Kolor obramowania. Domyślnie: 000000.
background_color	string	Kolor tła (kolor wypełnienia). Domyślnie: (puste).
zindex	integer	Wartość używana do porządkowania wszystkich kształtów i linii (z-index). Domyślnie: 0.

Linie mapy

Obiekt linii mapy definiuje linię wyświetlaną na mapie. Ma następujące właściwości:

Właściwość	Typ	Opis
sysmap_shapeid	ID	ID elementu kształtu mapy. Zachowanie właściwości: *- tylko do odczytu*
x1	integer	Współrzędne X punktu 1 linii w pikselach. Domyślnie: 0.
y1	integer	Współrzędne Y punktu 1 linii w pikselach. Domyślnie: 0.

Właściwość	Typ	Opis
x2	integer	Współrzędne X punktu 2 linii w pikselach. Domyślnie: 200.
y2	integer	Współrzędne Y punktu 2 linii w pikselach. Domyślnie: 200.
line_type	integer	Typ linii. Możliwe wartości: 0 - brak; 1 - ——————; 2 - ┅; 3 - – – –. Domyślnie: 0.
line_width	integer	Szerokość linii w pikselach. Domyślnie: 0.
line_color	string	Kolor linii. Domyślnie: 000000.
zindex	integer	Wartość używana do porządkowania wszystkich kształtów i linii (z-index). Domyślnie: 0.

map.create

Opis

`object map.create(object/array maps)`

Ta metoda umożliwia tworzenie nowych map.

> **Note:**
> Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w Rolach użytkowników.

Parametry

`(object/array)` Mapy do utworzenia.

Oprócz standardowych właściwości mapy, metoda akceptuje następujące parametry.

Parametr	Typ	Opis
links	array	Łącza mapy do utworzenia na mapie.
selements	array	Elementy mapy do utworzenia na mapie.
urls	array	Adresy URL mapy do utworzenia na mapie.
users	array	Udostępnienia użytkownikowi mapy do utworzenia na mapie.
userGroups	array	Udostępnienia grupie użytkowników mapy do utworzenia na mapie.
shapes	array	Kształty mapy do utworzenia na mapie.
lines	array	Linie mapy do utworzenia na mapie.

> **Note:**
> Aby utworzyć łącza mapy, należy ustawić `selementid` elementu mapy na dowolną wartość, a następnie użyć tej wartości do odwołania się do tego elementu we właściwościach łączy `selementid1` lub `selementid2`. Po utworzeniu elementu wartość ta zostanie zastąpiona poprawnym identyfikatorem wygenerowanym przez Zabbix. Zobacz przykład.

Zwracane wartości

(object) Zwraca obiekt zawierający identyfikatory utworzonych map we właściwości sysmapids. Kolejność zwróconych identyfikatorów odpowiada kolejności przekazanych map.

Przykłady

Utwórz pustą mapę

Utwórz mapę bez elementów.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "map.create",
    "params": {
        "name": "Map",
        "width": 600,
        "height": 600
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "sysmapids": [
            "8"
        ]
    },
    "id": 1
}
```

Utwórz mapę hostów

Utwórz mapę z dwoma elementami hostów i łączem między nimi. Zwróć uwagę na użycie tymczasowych wartości „selementid1” i „selementid2” w obiekcie łącza mapy do odwoływania się do elementów mapy.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "map.create",
    "params": {
        "name": "Host map",
        "width": 600,
        "height": 600,
        "selements": [
            {
                "selementid": "1",
                "elements": [
                    {"hostid": "1033"}
                ],
                "elementtype": 0,
                "iconid_off": "2"
            },

            {
                "selementid": "2",
                "elements": [
                    {"hostid": "1037"}
                ],
                "elementtype": 0,
                "iconid_off": "2"
            }
        ],
        "links": [
```

```
            {
                "selementid1": "1",
                "selementid2": "2"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "sysmapids": [
            "9"
        ]
    },
    "id": 1
}
```

Utwórz mapę wyzwalaczy

Utwórz mapę z elementem wyzwalacza, który zawiera dwa wyzwalacze.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "map.create",
    "params": {
        "name": "Mapa wyzwalaczy",
        "width": 600,
        "height": 600,
        "selements": [
            {
                "elements": [
                    {"triggerid": "12345"},
                    {"triggerid": "67890"}
                ],
                "elementtype": 2,
                "iconid_off": "2"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "sysmapids": [
            "10"
        ]
    },
    "id": 1
}
```

Udostępnianie mapy

Utwórz mapę z dwoma typami udostępniania (użytkownik i grupa użytkowników).

Żądanie:

```
{
    "jsonrpc": "2.0",
```

```
    "method": "map.create",
    "params": {
        "name": "Map sharing",
        "width": 600,
        "height": 600,
        "users": [
            {
                "userid": "4",
                "permission": "3"
            }
        ],
        "userGroups": [
            {
                "usrgrpid": "7",
                "permission": "2"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "sysmapids": [
            "9"
        ]
    },
    "id": 1
}
```

Kształty mapy

Utwórz mapę z tytułem będącym nazwą mapy.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "map.create",
    "params": {
        "name": "Host map",
        "width": 600,
        "height": 600,
        "shapes": [
            {
                "type": 0,
                "x": 0,
                "y": 0,
                "width": 600,
                "height": 11,
                "text": "{MAP.NAME}"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "sysmapids": [
```

```
            "10"
        ]
    },
    "id": 1
}
```

Linie mapy

Utwórz linię mapy.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "map.create",
    "params": {
        "name": "Map API lines",
        "width": 500,
        "height": 500,
        "lines": [
            {
                "x1": 30,
                "y1": 10,
                "x2": 100,
                "y2": 50,
                "line_type": 1,
                "line_width": 10,
                "line_color": "009900"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "sysmapids": [
            "11"
        ]
    },
    "id": 1
}
```

Zobacz także

- Element mapy
- Łącze mapy
- URL mapy
- Użytkownik mapy
- Grupa użytkowników mapy
- Kształt mapy
- Linia mapy

Źródło

CMap::create() w *ui/include/classes/api/services/CMap.php*.

map.delete

Opis

`object map.delete(array mapIds)`

Ta metoda umożliwia usuwanie map.

Note:
Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(array)` ID map do usunięcia.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory usuniętych map we właściwości `sysmapids`.

Przykłady

Usuń wiele map

Usuń dwie mapy.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "map.delete",
    "params": [
        "12",
        "34"
    ],
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "sysmapids": [
            "12",
            "34"
        ]
    },
    "id": 1
}
```

Źródło

CMap::delete() w *ui/include/classes/api/services/CMap.php*.

map.get

Opis

`integer/array map.get(object parameters)`

Ta metoda umożliwia pobieranie map zgodnie z podanymi parametrami.

Note:
Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w User roles.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
sysmapids	ID/array	Zwraca tylko mapy o podanych identyfikatorach.
userids	ID/array	Zwraca tylko mapy należące do użytkowników o podanych identyfikatorach.

Parametr	Typ	Opis
expandUrls	flag	Dodaje globalne adresy URL map do odpowiednich elementów mapy i rozwija makra we wszystkich adresach URL elementów mapy.
selectIconMap	query	Zwraca właściwość `iconmap` z mapą ikon używaną na mapie.
selectLinks	query	Zwraca właściwość `links` z połączeniami mapy między elementami.
selectSelements	query	Zwraca właściwość `selements` z elementami mapy.
selectUrls	query	Zwraca właściwość `urls` z adresami URL mapy.
selectUsers	query	Zwraca właściwość `users` z użytkownikami, którym mapa jest udostępniona.
selectUserGroups	query	Zwraca właściwość `userGroups` z grupami użytkowników, którym mapa jest udostępniona.
selectShapes	query	Zwraca właściwość `shapes` z kształtami mapy.
selectLines	query	Zwraca właściwość `lines` z liniami mapy.
sortfield	string/array	Sortuje wynik według podanych właściwości. Możliwe wartości: `name`, `width`, `height`.
countOutput	boolean	Te parametry opisano w komentarzu referencyjnym.
editable	boolean	
excludeSearch	boolean	
filter	object	
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli został użyty parametr `countOutput`.

Przykłady

Pobieranie mapy

Pobierz wszystkie dane o mapie „3”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "map.get",
    "params": {
        "output": "extend",
        "selectSelements": "extend",
        "selectLinks": "extend",
        "selectUsers": "extend",
        "selectUserGroups": "extend",
        "selectShapes": "extend",
        "selectLines": "extend",
        "sysmapids": "3"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
```

```
        "selements": [
            {
                "selementid": "10",
                "sysmapid": "3",
                "elementtype": "4",
                "evaltype": "0",
                "iconid_off": "1",
                "iconid_on": "0",
                "label": "Zabbix server",
                "label_location": "3",
                "x": "11",
                "y": "141",
                "iconid_disabled": "0",
                "iconid_maintenance": "0",
                "elementsubtype": "0",
                "areatype": "0",
                "width": "200",
                "height": "200",
                "viewtype": "0",
                "use_iconmap": "1",
                "show_label": "-1",
                "zindex":"0",
                "elements": [],
                "urls": [],
                "tags": [
                    {
                        "tag": "service",
                        "value": "mysqld",
                        "operator": "0"
                    }
                ]
            },
            {
                "selementid": "11",
                "sysmapid": "3",
                "elementtype": "4",
                "evaltype": "0",
                "iconid_off": "1",
                "iconid_on": "0",
                "label": "Web server",
                "label_location": "3",
                "x": "211",
                "y": "191",
                "iconid_disabled": "0",
                "iconid_maintenance": "0",
                "elementsubtype": "0",
                "areatype": "0",
                "width": "200",
                "height": "200",
                "viewtype": "0",
                "use_iconmap": "1",
                "show_label": "0",
                "zindex":"0",
                "elements": [],
                "urls": [],
                "tags": []
            },
            {
                "selementid": "12",
                "sysmapid": "3",
                "elementtype": "0",
                "evaltype": "0",
```

```
                "iconid_off": "185",
                "iconid_on": "0",
                "label": "{HOST.NAME}\r\n{HOST.CONN}",
                "label_location": "0",
                "x": "111",
                "y": "61",
                "iconid_disabled": "0",
                "iconid_maintenance": "0",
                "elementsubtype": "0",
                "areatype": "0",
                "width": "200",
                "height": "200",
                "viewtype": "0",
                "use_iconmap": "0",
                "show_label": "1",
                "zindex":"0",
                "elements": [
                    {
                        "hostid": "10084"
                    }
                ],
                "urls": [],
                "tags": []
            }
        ],
        "links": [
            {
                "linkid": "23",
                "sysmapid": "3",
                "selementid1": "10",
                "selementid2": "11",
                "drawtype": "0",
                "color": "00CC00",
                "label": "",
                "show_label": "1",
                "indicator_type": "0",
                "itemid": "0",
                "linktriggers": [],
                "thresholds": [],
                "highlights": []
            }
        ],
        "users": [
            {
                "sysmapuserid": "1",
                "userid": "2",
                "permission": "2"
            }
        ],
        "userGroups": [
            {
                "sysmapusrgrpid": "1",
                "usrgrpid": "7",
                "permission": "2"
            }
        ],
        "shapes":[
            {
                "sysmap_shapeid":"1",
                "type":"0",
                "x":"0",
                "y":"0",
```

```
                "width":"680",
                "height":"15",
                "text":"{MAP.NAME}",
                "font":"9",
                "font_size":"11",
                "font_color":"000000",
                "text_halign":"0",
                "text_valign":"0",
                "border_type":"0",
                "border_width":"0",
                "border_color":"000000",
                "background_color":"",
                "zindex":"0"
            }
        ],
        "lines":[
            {
                "sysmap_shapeid":"2",
                "x1": 30,
                "y1": 10,
                "x2": 100,
                "y2": 50,
                "line_type": 1,
                "line_width": 10,
                "line_color": "009900",
                "zindex":"1"
            }
        ],
        "sysmapid": "3",
        "name": "Local network",
        "width": "400",
        "height": "400",
        "backgroundid": "0",
        "background_scale": "1",
        "label_type": "2",
        "label_location": "3",
        "show_element_label": "0",
        "show_link_label": "1",
        "highlight": "1",
        "expandproblem": "1",
        "markelements": "0",
        "show_unack": "0",
        "grid_size": "50",
        "grid_show": "1",
        "grid_align": "1",
        "label_format": "0",
        "label_type_host": "2",
        "label_type_hostgroup": "2",
        "label_type_trigger": "2",
        "label_type_map": "2",
        "label_type_image": "2",
        "label_string_host": "",
        "label_string_hostgroup": "",
        "label_string_trigger": "",
        "label_string_map": "",
        "label_string_image": "",
        "iconmapid": "0",
        "expand_macros": "0",
        "severity_min": "0",
        "userid": "1",
        "private": "1",
        "show_suppressed": "1"
```

```
        }
    ],
    "id": 1
}
```

Zobacz także

- Mapa ikon
- Element mapy
- Łącze mapy
- URL mapy
- Użytkownik mapy
- Grupa użytkowników mapy
- Kształty mapy
- Linie mapy

Źródło

CMap::get() w *ui/include/classes/api/services/CMap.php*.

map.update

Opis

`object map.update(object/array maps)`

Ta metoda umożliwia aktualizację istniejących map.

> **Note:**
> Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywołania tej metody mogą zostać odebrane w ustawieniach roli użytkownika. Więcej informacji można znaleźć w Rolach użytkowników.

Parametry

`(object/array)` Właściwości mapy do zaktualizowania.

Właściwość `mapid` musi być zdefiniowana dla każdej mapy, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko przekazane właściwości, wszystkie pozostałe pozostaną bez zmian.

Oprócz standardowych właściwości mapy metoda akceptuje następujące parametry.

Parametr	Type	Opis
links	array	Łącza mapy zastępujące istniejące łącza.
selements	array	Elementy mapy zastępujące istniejące elementy.
urls	array	Adresy URL mapy zastępujące istniejące adresy URL.
users	array	Udostępnienia użytkownikowi mapy zastępujące istniejące elementy.
userGroups	array	Udostępnienia grupie użytkowników mapy zastępujące istniejące elementy.
shapes	array	Kształty mapy zastępujące istniejące kształty.
lines	array	Linie mapy zastępujące istniejące linie.

> **Note:**
> Aby utworzyć łącza mapy między nowymi elementami mapy, należy ustawić `selementid` elementu na dowolną wartość, a następnie użyć tej wartości do odwołania się do tego elementu we właściwościach łączy `selementid1` lub `selementid2`. Po utworzeniu elementu wartość ta zostanie zastąpiona poprawnym ID wygenerowanym przez Zabbix. Zobacz przykład dla map.create.

Wartości zwracane

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych map we właściwości `sysmapids`.

Przykłady

Zmień rozmiar mapy

Zmień rozmiar mapy na 1200x1200 pikseli.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "map.update",
    "params": {
        "sysmapid": "8",
        "width": 1200,
        "height": 1200
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "sysmapids": [
            "8"
        ]
    },
    "id": 1
}
```

Zmień właściciela mapy

Dostępne tylko dla administratorów i super administratorów.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "map.update",
    "params": {
        "sysmapid": "9",
        "userid": "1"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "sysmapids": [
            "9"
        ]
    },
    "id": 1
}
```

Zobacz także

- Element mapy
- Łącze mapy
- URL mapy
- Użytkownik mapy
- Grupa użytkowników mapy
- Kształty mapy
- Linie mapy

Źródło

CMap::update() w *ui/include/classes/api/services/CMap.php*.

Mapa ikon

Ta klasa jest przeznaczona do pracy z mapami ikon.

Odwołania do obiektów:

- Mapa ikon
- Mapowanie ikon

Dostępne metody:

- iconmap.create - utwórz nowe mapy ikon
- iconmap.delete - usuń mapy ikon
- iconmap.get - pobierz mapy ikon
- iconmap.update - zaktualizuj mapy ikon

Obiekt mapy ikon

Następujące obiekty są bezpośrednio powiązane z API `iconmap`.

Mapa ikon

Obiekt mapy ikon ma następujące właściwości.

Właściwość	Typ	Opis
iconmapid	ID	ID mapy ikon. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji
default_iconid	ID	ID domyślnej ikony. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
name	string	Nazwa mapy ikon. Zachowanie właściwości: - *wymagane* dla operacji tworzenia

Mapowanie ikon

Obiekt mapowania ikon definiuje konkretną ikonę, która ma być używana dla hostów o określonej wartości pola inwentarza. Ma następujące właściwości.

Właściwość	Typ	Opis
iconid	ID	ID ikony używanej przez mapowanie ikon. Zachowanie właściwości: - *wymagane*
expression	string	Wyrażenie służące do dopasowania do pola inwentarza. Zachowanie właściwości: - *wymagane*
inventory_link	integer	ID pola inwentarza hosta. Listę obsługiwanych pól inwentarza można znaleźć w obiekcie inwentarza hosta. Zachowanie właściwości: - *wymagane*
sortorder	integer	Pozycja mapowania ikon na mapie ikon. Zachowanie właściwości: - *tylko do odczytu*

iconmap.create

Opis

`object iconmap.create(object/array iconMaps)`

Ta metoda umożliwia tworzenie nowych map ikon.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkownika typu *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Mapy ikon do utworzenia.

Oprócz standardowych właściwości map ikon, metoda akceptuje następujące parametry.

Parametr	Type	Opis
mappings	array	Mapowania ikon, które mają zostać utworzone dla mapy ikon. Zachowanie parametrów: - *wymagane*

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory utworzonych map ikon we właściwości `iconmapids`. Kolejność zwróconych identyfikatorów odpowiada kolejności przekazanych map ikon.

Przykłady

Utwórz mapę ikon

Utwórz mapę ikon, aby wyświetlać hosty różnych typów.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "iconmap.create",
    "params": {
        "name": "Type icons",
        "default_iconid": "2",
        "mappings": [
            {
                "inventory_link": 1,
                "expression": "server",
                "iconid": "3"
            },
            {
                "inventory_link": 1,
                "expression": "switch",
                "iconid": "4"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "iconmapids": [
            "2"
        ]
```

```
    },
    "id": 1
}
```

Zobacz także

- Mapowanie ikon

Źródło

CIconMap::create() w *ui/include/classes/api/services/CIconMap.php*.

iconmap.delete

Opis

`object iconmap.delete(array iconMapIds)`

Ta metoda umożliwia usuwanie map ikon.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkowników typu *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(array)` ID map ikon do usunięcia.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory usuniętych map ikon we właściwości `iconmapids`.

Przykłady

Usuń wiele map ikon

Usuń dwie mapy ikon.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "iconmap.delete",
    "params": [
        "2",
        "5"
    ],
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "iconmapids": [
            "2",
            "5"
        ]
    },
    "id": 1
}
```

Źródło

CIconMap::delete() w *ui/include/classes/api/services/CIconMap.php*.

iconmap.get

Opis

`integer/array iconmap.get(object parameters)`

Ta metoda umożliwia pobieranie map ikon zgodnie z podanymi parametrami.

> **Note:**
> Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji znajduje się w sekcji Role użytkowników.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
iconmapids	ID/array	Zwraca tylko mapy ikon o podanych identyfikatorach.
sysmapids	ID/array	Zwraca tylko mapy ikon używane w podanych mapach.
selectMappings	query	Zwraca właściwość `mappings` z używanymi mapowaniami ikon.
sortfield	string/array	Sortuje wynik według podanych właściwości. Możliwe wartości: `iconmapid`, `name`.
countOutput	boolean	Te parametry są opisane w komentarzu referencyjnym.
editable	boolean	
excludeSearch	boolean	
filter	object	
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli został użyty parametr `countOutput`.

Przykłady

Pobieranie mapy ikon

Pobierz wszystkie dane o mapie ikon „3”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "iconmap.get",
    "params": {
        "iconmapids": "3",
        "output": "extend",
        "selectMappings": "extend"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "mappings": [
                {
                    "iconmappingid": "3",
                    "iconmapid": "3",
                    "iconid": "6",
                    "inventory_link": "1",
                    "expression": "server",
                    "sortorder": "0"
                },
                {
                    "iconmappingid": "4",
                    "iconmapid": "3",
                    "iconid": "10",
                    "inventory_link": "1",
                    "expression": "switch",
                    "sortorder": "1"
                }
            ],
            "iconmapid": "3",
            "name": "Host type icons",
            "default_iconid": "2"
        }
    ],
    "id": 1
}
```


Zobacz także

- Mapowanie ikon

Źródło

CIconMap::get() w *ui/include/classes/api/services/CIconMap.php*.

iconmap.update

Opis

`object iconmap.update(object/array iconMaps)`

Ta metoda umożliwia aktualizację istniejących map ikon.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkowników typu *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Zobacz Role użytkowników aby uzyskać więcej informacji.

Parametry

`(object/array)` Właściwości mapy ikon do zaktualizowania.

Właściwość `iconmapid` musi być zdefiniowana dla każdej mapy ikon, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko przekazane właściwości, wszystkie pozostałe pozostaną bez zmian.

Oprócz standardowych właściwości mapy ikon metoda akceptuje następujące parametry.

Parametr	Type	Opis
mappings	array	Mapowania ikon zastępujące istniejące mapowania ikon.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych map ikon we właściwości `iconmapids`.

Przykłady

Zmień nazwę mapy ikon

Zmień nazwę mapy ikon na „OS icons”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "iconmap.update",
    "params": {
        "iconmapid": "1",
        "name": "OS icons"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "iconmapids": [
            "1"
        ]
    },
    "id": 1
}
```

Zobacz także

- Mapowanie ikon

Źródło

CIconMap::update() w *ui/include/classes/api/services/CIconMap.php*.

Mapa wartości

Ta klasa jest przeznaczona do pracy z mapami wartości.

Odwołania do obiektów:

- Mapa wartości
  - Mapowania wartości

Dostępne metody:

- valuemap.create - tworzenie nowych map wartości
- valuemap.delete - usuwanie map wartości
- valuemap.get - pobieranie map wartości
- valuemap.update - aktualizowanie map wartości

Obiekt mapy wartości

Następujące obiekty są bezpośrednio powiązane z API `valuemap`.

Mapa wartości

Obiekt mapy wartości ma następujące właściwości.

Właściwość	Typ	Opis
valuemapid	ID	ID mapy wartości. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji

Właściwość	Typ	Opis
hostid	ID	ID hosta lub szablonu, do którego należy mapa wartości. Zachowanie właściwości: - *stałe* - *wymagane* dla operacji tworzenia
name	string	Nazwa mapy wartości. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
mappings	array	Mapowania wartości dla bieżącej mapy wartości. Obiekt mapowania jest opisany szczegółowo poniżej. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
uuid	string	Uniwersalny unikalny identyfikator, używany do łączenia importowanych map wartości z już istniejącymi. Generowany automatycznie, jeśli nie został podany. Zachowanie właściwości: - *obsługiwane*, jeśli mapa wartości należy do szablonu

Mapowania wartości

Obiekt mapowań wartości definiuje mapowania wartości mapy wartości. Ma następujące właściwości.

Właściwość	Type	Opis
type	integer	Typ dopasowania mapowania. Możliwe wartości: 0 - mapowanie zostanie zastosowane, jeśli wartość jest równa; 1 - mapowanie zostanie zastosowane, jeśli wartość jest większa lub równa[1]; 2 - mapowanie zostanie zastosowane, jeśli wartość jest mniejsza lub równa[1]; 3 - mapowanie zostanie zastosowane, jeśli wartość mieści się w zakresie (zakresy są domknięte; można zdefiniować wiele zakresów oddzielonych przecinkiem)[1]; 4 - mapowanie zostanie zastosowane, jeśli wartość pasuje do wyrażenia regularnego[2]; 5 - jeśli nie zostaną znalezione żadne dopasowania, mapowanie nie zostanie zastosowane i zostanie użyta wartość domyślna. Jeśli `type` jest ustawione na ”0”, ”1”, ”2”, ”3”, ”4”, wtedy `value` nie może być puste. Jeśli `type` jest ustawione na ”5”, wtedy `value` musi być puste.
value	string	Wartość oryginalna. Zachowanie właściwości: - *wymagane* jeśli `type` jest ustawione na ”1”, ”2”, ”3”, ”4” - *obsługiwane* jeśli `type` jest ustawione na ”5”
newvalue	string	Wartość, na którą mapowana jest wartość oryginalna. Zachowanie właściwości: - *wymagane*

[1] obsługiwane tylko dla pozycji mających typ wartości ”numeric unsigned”, ”numeric float”.
[2] obsługiwane tylko dla pozycji mających typ wartości ”character”.

valuemap.create

Opis

`object valuemap.create(object/array valuemaps)`

Ta metoda umożliwia tworzenie nowych map wartości.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkowników typu *Super admin*. Uprawnienia do wywołania tej metody mogą zostać odebrane w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Mapowania wartości do utworzenia.

Metoda akceptuje mapowania wartości ze standardowymi właściwościami mapowania wartości.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory właściwości `valuemapids` utworzonych map wartości. Kolejność zwróconych identyfikatorów jest zgodna z kolejnością przekazywanych map wartości.

Przykłady

Tworzenie mapowania wartości

Utwórz jedno mapowanie wartości z dwoma odwzorowaniami.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "valuemap.create",
    "params": {
        "hostid": "50009",
        "name": "Stan usługi",
        "mappings": [
            {
                "type": "1",
                "value": "1",
                "newvalue": "Działa"
            },
            {
                "type": "5",
                "newvalue": "Niedostępna"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "valuemapids": [
            "1"
        ]
    },
    "id": 1
}
```

Źródło

CValueMap::create() in *ui/include/classes/api/services/CValueMap.php*.

valuemap.delete

Opis

`object valuemap.delete(array valuemapids)`

Ta metoda pozwala na usuwanie map wartości.

> **Note:**
> Ta metoda jest dostępna tylko dla typu użytkownika *Super admin*. Uprawnienia do wywołania metody można cofnąć w ustawieniach roli użytkownika. Więcej informacji można znaleźć w User roles.

Parametry

`(array)` Identyfikatory map wartości do usunięcia.

Zwracane wartości

`(array)` Zwraca obiekt zawierający identyfikatory usuniętych map wartości we właściwości `valuemapids`.

Przykłady

Usuwanie wielu map wartości

Usuń dwie mapy wartości.

Żądanie:

```
{
"jsonrpc": "2.0",
"method": "valuemap.delete",
"params": [
"1",
"2"
],
"id": 1
}
```

Odpowiedź:

```
{
"jsonrpc": "2.0",
"result": {
"valuemapids": [
"1",
"2"
]
},
"id": 1
}
```

Źródło

CValueMap::delete() in *ui/include/classes/api/services/CValueMap.php*.

valuemap.get

Opis

`integer/array valuemap.get(object parameters)`

Ta metoda umożliwia pobieranie map wartości zgodnie z podanymi parametrami.

> **Note:**
> Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji znajduje się w sekcji Role użytkowników.

Parametry

(object) Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
valuemapids	ID/array	Zwracaj tylko mapowania wartości o podanych identyfikatorach.
selectMappings	query	Zwracaj mapowania wartości dla bieżącej mapy wartości we właściwości `mappings`. Obsługuje `count`.
sortfield	string/array	Sortuj wynik według podanych właściwości. Możliwe wartości: `valuemapid`, `name`.
countOutput	boolean	Te parametry opisano w komentarzu referencyjnym.
editable	boolean	
excludeSearch	boolean	
filter	object	
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwróć wartości

(integer/array) Zwraca albo:

- tablicę obiektów;
- ilość pobranych obiektów, jeśli parametr `countOutput` został użyty.

Przykłady

Pobieranie map wartości

Pobierz wszystkie skonfigurowane mapy wartości.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "valuemap.get",
    "params": {
        "output": "extend"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "valuemapid": "4",
            "name": "APC Battery Replacement Status"
        },
        {
            "valuemapid": "5",
            "name": "APC Battery Status"
        },
        {
            "valuemapid": "7",
            "name": "Dell Open Manage System Status"
```

```
        }
    ],
    "id": 1
}
```

Pobierz jedną mapę wartości wraz z jej mapowaniami.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "valuemap.get",
    "params": {
        "output": "extend",
        "selectMappings": "extend",
        "valuemapids": ["4"]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "valuemapid": "4",
            "name": "APC Battery Replacement Status",
            "mappings": [
                {
                    "type": "0",
                    "value": "1",
                    "newvalue": "unknown"
                },
                {
                    "type": "0",
                    "value": "2",
                    "newvalue": "notInstalled"
                },
                {
                    "type": "0",
                    "value": "3",
                    "newvalue": "ok"
                },
                {
                    "type": "0",
                    "value": "4",
                    "newvalue": "failed"
                },
                {
                    "type": "0",
                    "value": "5",
                    "newvalue": "highTemperature"
                },
                {
                    "type": "0",
                    "value": "6",
                    "newvalue": "replaceImmediately"
                },
                {
                    "type": "0",
                    "value": "7",
                    "newvalue": "lowCapacity"
                }
            ]
```

```
        }
    ],
    "id": 1
}
```

Źródło

CValueMap::get() in *ui/include/classes/api/services/CValueMap.php*.

valuemap.update

Opis

`object valuemap.update(object/array valuemaps)`

Ta metoda umożliwia aktualizację istniejących map wartości.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkowników typu *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Właściwości mapy wartości, które mają zostać zaktualizowane.

Właściwość `valuemapid` musi być zdefiniowana dla każdej mapy wartości, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko przekazane właściwości, wszystkie pozostałe pozostaną bez zmian.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory ID zaktualizowanych wartości map we własności `valuemapids`.

Przykłady

Zmiana nazwy mapy wartości

Zmień nazwę mapy wartości na „Device status”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "valuemap.update",
    "params": {
        "valuemapid": "2",
        "name": "Device status"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "valuemapids": [
            "2"
        ]
    },
    "id": 1
}
```

Zmienianie mapowań dla jednej mapy wartości.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "valuemap.update",
    "params": {
```

```
        "valuemapid": "2",
        "mappings": [
            {
                "type": "0",
                "value": "0",
                "newvalue": "Online"
            },
            {
                "type": "0",
                "value": "1",
                "newvalue": "Offline"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "valuemapids": [
            "2"
        ]
    },
    "id": 1
}
```

Źródło

CValueMap::update() w *ui/include/classes/api/services/CValueMap.php*.

MFA

Ta klasa jest przeznaczona do pracy z metodami MFA (uwierzytelnianie wieloskładnikowe).

Odwołania do obiektów:

- MFA

Dostępne metody:

- mfa.create - tworzenie nowych metod MFA
- mfa.delete - usuwanie metod MFA
- mfa.get - pobieranie metod MFA
- mfa.update - aktualizowanie metod MFA

Obiekt MFA (Multi-Factor Authentication)

Następujące obiekty są bezpośrednio powiązane z API `mfa`.

MFA

Obiekt MFA (uwierzytelnianie wieloskładnikowe) ma następujące właściwości.

Właściwość	Typ	Opis
mfaid	ID	ID metody MFA. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji

Właściwość	Typ	Opis
type	integer	Typ metody MFA. Możliwe wartości: 1 - TOTP (jednorazowe hasła oparte na czasie); 2 - Duo Universal Prompt.
name	string	Unikalna nazwa metody MFA. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
hash_function	integer	Typ funkcji skrótu do generowania kodów TOTP. Możliwe wartości: 1 - SHA-1; 2 - SHA-256; 3 - SHA-512. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na „TOTP”
code_length	integer	Długość kodu weryfikacyjnego. Możliwe wartości: 6 - 6 cyfr; 8 - 8 cyfr. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na „TOTP”
api_hostname	string	Nazwa hosta API dostarczona przez usługę uwierzytelniania Duo. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na „Duo Universal Prompt”
clientid	string	ID klienta dostarczone przez usługę uwierzytelniania Duo. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na „Duo Universal Prompt”
client_secret	string	Tajny klucz klienta dostarczony przez usługę uwierzytelniania Duo. Zachowanie właściwości: - *tylko do zapisu* - *wymagane*, jeśli `type` jest ustawione na „Duo Universal Prompt”

mfa.create

Opis

`object mfa.create(object/array MFA methods)`

Ta metoda umożliwia tworzenie nowych metod MFA.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkownika typu *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w Rolach użytkowników.

Parametry

`(object/array)` Metody MFA do utworzenia.

Ta metoda akceptuje metody MFA ze standardowymi właściwościami metod MFA.

Wartości zwracane

`(object)` Zwraca obiekt zawierający identyfikatory utworzonych metod MFA we właściwości `mfaids`. Kolejność zwróconych identyfikatorów odpowiada kolejności przekazanych pozycji.

Przykłady

Tworzenie metod MFA

Utwórz metodę MFA „Zabbix TOTP” wykorzystującą jednorazowe hasła oparte na czasie (TOTP), z funkcją skrótu do generowania kodów TOTP ustawioną na SHA-1 oraz długością kodu weryfikacyjnego ustawioną na 6 cyfr.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "mfa.create",
    "params": {
        "type": 1,
        "name": "Zabbix TOTP",
        "hash_function": 1,
        "code_length": 6
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "mfaids": [
            "1"
        ]
    },
    "id": 1
}
```

Źródło

CMfa::create() w *ui/include/classes/api/services/CMfa.php*.

mfa.delete

Opis

`object mfa.delete(array mfaids)`

Ta metoda umożliwia usuwanie metod MFA.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkownika typu *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji znajduje się w sekcji Role użytkowników.

Parametry

`(array)` ID metod MFA do usunięcia.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory usuniętych metod MFA we właściwości `mfaids`.

Przykłady

Usuwanie metod MFA

Usuń metodę MFA.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "mfa.delete",
    "params": [
        "2"
    ],
```

```
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "mfaids": [
            "2"
        ]
    },
    "id": 1
}
```

Źródło

CMfa::delete() w *ui/include/classes/api/services/CMfa.php*.

mfa.get

Opis

`integer/array mfa.get(object parameters)`

Ta metoda umożliwia pobieranie metod MFA zgodnie z podanymi parametrami.

Note:
Ta metoda jest dostępna tylko dla użytkownika typu *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji User roles.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
mfaids	ID/array	Zwraca tylko metody MFA o podanych identyfikatorach.
selectUsrgrps	query	Zwraca właściwość `usrgrps` z grupami użytkowników powiązanymi z metodami MFA. Obsługuje `count`.
filter	object	Zwraca tylko te wyniki, które dokładnie odpowiadają podanemu filtrowi. Akceptuje obiekt, w którym kluczami są nazwy właściwości, a wartościami są pojedyncza wartość lub tablica wartości do dopasowania. Obsługiwane właściwości: `mfaid` - identyfikator metody MFA; `type` - typ metody MFA.
sortfield	string/array	Sortuje wynik według podanych właściwości. Możliwe wartości: `name`.
search	object	Zwraca wyniki pasujące do podanego wzorca (bez rozróżniania wielkości liter). Akceptuje obiekt, w którym kluczami są nazwy właściwości, a wartościami są ciągi znaków do wyszukania. Jeśli nie podano dodatkowych opcji, zostanie wykonane wyszukiwanie `LIKE "%…%"`. Obsługiwane właściwości: `name`.
countOutput excludeSearch	boolean boolean	Te parametry opisano w komentarzu referencyjnym.

Parametr	Typ	Opis
limit	integer	
output	query	
preservekeys	boolean	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli użyto parametru `countOutput`.

Przykłady

Wyszukiwanie metod MFA po nazwie

Pobierz wszystkie metody MFA, które mają w nazwie „Zabbix”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "mfa.get",
    "params": {
        "output": "extend",
        "search": {
            "name": "Zabbix"
        }
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "mfaid": "1",
            "type": "1",
            "name": "Zabbix TOTP 1",
            "hash_function": "1",
            "code_length": "6",
            "api_hostname": "",
            "clientid": ""
        },
        {
            "mfaid": "2",
            "type": "1",
            "name": "Zabbix TOTP 2",
            "hash_function": "3",
            "code_length": "8",
            "api_hostname": "",
            "clientid": ""
        }
    ],
    "id": 1
}
```

Źródło

CMfa::get() w *ui/include/classes/api/services/CMfa.php*.

mfa.update

Opis

`object mfa.update(object/array MFA methods)`

Ta metoda umożliwia aktualizację istniejących metod MFA.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkowników typu *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w Rolach użytkowników.

Parametry

`(object/array)` Właściwości metody MFA do zaktualizowania.

Właściwość `mfaid` musi być zdefiniowana dla każdej pozycji, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko przekazane właściwości, wszystkie pozostałe pozostaną bez zmian.

Metoda akceptuje metody MFA ze standardowymi właściwościami metody MFA.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych metod MFA we właściwości `mfaids`.

Przykłady

Aktualizowanie właściwości metody

Zaktualizuj funkcję skrótu używaną do generowania kodów TOTP oraz długość kodu weryfikacyjnego dla metody MFA „Zabbix TOTP” wykorzystującej jednorazowe hasła oparte na czasie (TOTP).

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "mfa.update",
    "params": {
        "mfaid": "1",
        "hash_function": 3,
        "code_length": 8
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "mfaids": [
            "1"
        ]
    },
    "id": 1
}
```

Źródło

CMfa::update() w *ui/include/classes/api/services/CMfa.php*.

Moduły

Ta klasa została zaprojektowana do współpracy z modułami frontend.

Odwołania do obiektów:

- Module

Dostępne metody:

- module.create - instalowanie nowych modułów
- module.delete - odinstalowywanie modułów
- module.get - pobieranie modułów
- module.update - aktualizowanie modułów

Obiekt modułu

Następujące obiekty są bezpośrednio powiązane z API `module`.

Moduł

Obiekt modułu ma następujące właściwości.

Właściwość	Typ	Opis
moduleid	ID	ID modułu zapisane w bazie danych. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji
id	string	Unikalny identyfikator modułu zdefiniowany przez dewelopera w pliku manifest.json modułu. Możliwe wartości dla wbudowanych modułów: zobacz opis właściwości „type” w widżecie pulpitu. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
relative_path	string	Ścieżka do katalogu modułu względem katalogu frontend Zabbix. Możliwe wartości: `widgets/*` - dla wbudowanych modułów widżetów; `modules/*` - dla modułów innych firm. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
status	integer	Określa, czy moduł jest włączony, czy wyłączony. Możliwe wartości: 0 - *(domyślnie)* Wyłączony; 1 - Włączony.
config	object	Konfiguracja modułu.

module.create

Opis

`object module.create(object/array modules)`

Ta metoda umożliwia instalację nowych modułów frontend.

Note:
Ta metoda jest dostępna tylko dla użytkowników typu *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji znajduje się w Rolach użytkowników.

Attention:
Pliki modułów muszą zostać ręcznie rozpakowane do odpowiednich podkatalogów, zgodnie z właściwością `relative_path` modułów.

Parametry

`(object/array)` Moduły do utworzenia.

Metoda akceptuje moduły ze standardowymi właściwościami modułu.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory zainstalowanych modułów we właściwości `moduleids`. Kolejność zwracanych identyfikatorów odpowiada kolejności przekazanych modułów.

Przykłady

Instalowanie modułu

Zainstaluj moduł ze statusem „Włączony”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "module.create",
    "params": {
        "id": "example_module",
        "relative_path": "modules/example_module",
        "status": 1
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "moduleids": [
            "25"
        ]
    },
    "id": 1
}
```

Zobacz również

- Moduł
- Moduły frontendowe

Źródło

CModule::create() w *ui/include/classes/api/services/CModule.php*.

module.delete

Opis

`object module.delete(array moduleids)`

Ta metoda umożliwia odinstalowanie modułów.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkowników typu *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji znajduje się w User roles.

> **Attention:**
> Pliki modułów muszą zostać usunięte ręcznie.

Parametry

`(array)` ID modułów do odinstalowania.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory odinstalowanych modułów we właściwości `moduleids`.

Przykłady

Odinstalowywanie wielu modułów

Odinstaluj moduły „27” i „28”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "module.delete",
    "params": [
        "27",
        "28"
    ],
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "moduleids": [
            "27",
            "28"
        ]
    },
    "id": 1
}
```

Źródło

CModule::delete() w *ui/include/classes/api/services/CModule.php*.

module.get

Opis

`integer/array module.get(object parameters)`

Ta metoda umożliwia pobieranie modułów zgodnie z podanymi parametrami.

Note:
Ta metoda jest dostępna wyłącznie dla użytkownika typu *Super admin*. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w Rolach użytkowników.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
moduleids	ID/array	Zwraca tylko moduły o podanych identyfikatorach.
sortfield	string/array	Sortuje wynik według podanych właściwości. Możliwe wartości: `moduleid`, `relative_path`.
countOutput	boolean	Te parametry są opisane w komentarzu referencyjnym.
excludeSearch	boolean	
filter	object	
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli użyto parametru `countOutput`.

Przykłady

Pobieranie modułu według ID

Pobierz wszystkie dane o modułach „1”, „2” i „25”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "module.get",
    "params": {
        "output": "extend",
        "moduleids": [
            "1",
            "2",
            "25"
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "moduleid": "1",
            "id": "actionlog",
            "relative_path": "widgets/actionlog",
            "status": "1",
            "config": []
        },
        {
            "moduleid": "2",
            "id": "clock",
            "relative_path": "widgets/clock",
            "status": "1",
            "config": []
        },
        {
            "moduleid": "25",
            "id": "example",
            "relative_path": "modules/example_module",
            "status": "1",
            "config": []
        }
    ],
    "id": 1
}
```

Zobacz także

- Moduł
- Widget pulpitu
- Moduły frontend

Źródło

CModule::get() w *ui/include/classes/api/services/CModule.php*.

module.update

Opis

`object module.update(object/array modules)`

Ta metoda umożliwia aktualizację istniejących modułów.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkownika typu *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Właściwości modułu do zaktualizowania.

Właściwość `moduleid` musi być zdefiniowana dla każdego modułu, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko określone właściwości.

Metoda akceptuje moduły ze standardowymi właściwościami modułu.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych modułów we właściwości `moduleids`.

Przykłady

Wyłączanie modułu

Wyłącz moduł „25”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "module.update",
    "params": {
        "moduleid": "25",
        "status": 0
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "moduleids": [
            "25"
        ]
    },
    "id": 1
}
```

Zobacz także

- Moduł
- Moduły frontend

Źródło

CModule::update() w *ui/include/classes/api/services/CModule.php*.

Obraz

Ta klasa została zaprojektowana do pracy z obrazami.

Odwołania do obiektów:

- Image

Dostępne metody:

- image.create - tworzenie nowych obrazów
- image.delete - usuwanie obrazów
- image.get - pobieranie obrazów
- image.update - aktualizacja obrazów

Obiekt obrazu

Następujące obiekty są bezpośrednio powiązane z API `image`.

Obraz

Obiekt obrazu ma następujące właściwości.

Właściwość	Typ	Opis
imageid	ID	ID obrazu. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji
name	string	Nazwa obrazu. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
imagetype	integer	Typ obrazu. Możliwe wartości: 1 - *(domyślnie)* ikona; 2 - obraz tła. Zachowanie właściwości: - *stałe* - *wymagane* dla operacji tworzenia
image	string	Obraz zakodowany w Base64. Maksymalny rozmiar zakodowanego obrazu wynosi 1 MB. Maksymalny rozmiar można dostosować, zmieniając wartość stałej `ZBX_MAX_IMAGE_SIZE`. Obsługiwane formaty obrazów: PNG, JPEG, GIF i WebP. Zachowanie właściwości: - *wymagane* dla operacji tworzenia

image.create

Opis

`object image.create(object/array images)`

Ta metoda umożliwia tworzenie nowych obrazów.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkownika typu *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Obrazy do utworzenia.

Metoda akceptuje obrazy ze standardowymi właściwościami obrazu.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory utworzonych obrazów we właściwości `imageids`. Kolejność zwróconych identyfikatorów odpowiada kolejności przekazanych obrazów.

Przykłady

Utwórz obraz ikony

Utwórz ikonę chmury.

Żądanie:


```
{
    "jsonrpc": "2.0",
    "method": "image.create",
    "params": {
        "imagetype": 1,
        "name": "Cloud_(24)",
        "image": "iVBORw0KGgoAAAANSUhEUgAAABgAAAANCAYAAACzbK7QAAAABHNCSVQICAgIfAhkiAAAAAlwSFlzAAACmAAAApgB
    },
    "id": 1
}
```


Odpowiedź:


```
{
    "jsonrpc": "2.0",
    "result": {
        "imageids": [
            "188"
        ]
    },
    "id": 1
}
```


Utwórz obraz tła

Utwórz mały obraz tła, który będzie używany jako wzorzec.

Żądanie:


```
{
    "jsonrpc": "2.0",
    "method": "image.create",
    "params": {
        "imagetype": 2,
        "name": "background_image",
        "image": "iVBORw0KGgoAAAANSUhEUgAAABgAAAAYCAIAAABvFaqvAAABhWlDQ1BJQ0MgcHJvZmlsZQAAKJF9kb1Lw0AYxp+m
    },
    "id": 1
}
```


Odpowiedź:


```
{
    "jsonrpc": "2.0",
    "result": {
        "imageids": [
            "189"
        ]
    },
    "id": 1
}
```


Źródło

CImage::create() w *ui/include/classes/api/services/CImage.php*.

image.delete

Opis

`object image.delete(array imageIds)`

Ta metoda umożliwia usuwanie obrazów.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkownika *Super admin*. Uprawnienia do wywołania metody można cofnąć w ustawieniach roli użytkownika. Więcej informacji można znaleźć w User roles.

Parametry

`(array)` IDs obrazów do usunięcia.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory usuniętych obrazów w właściwości `imageids`.

Przykłady

Usuń wiele obrazów

Usuń dwa obrazy.

Żądanie:

```
{
"jsonrpc": "2.0",
"method": "image.delete",
"params": [
"188",
"192"
],
"id": 1
}
```

Odpowiedź:

```
{
"jsonrpc": "2.0",
"result": {
"imageids": [
"188",
"192"
]
},
"id": 1
}
```

Źródło

CImage::delete() w *ui/include/classes/api/services/CImage.php*.

image.get

Opis

`integer/array image.get(object parameters)`

Ta metoda umożliwia pobieranie obrazów zgodnie z podanymi parametrami.

> **Note:**
> Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
imageids	ID/array	Zwraca tylko obrazy o podanych identyfikatorach.

Parametr	Typ	Opis
sysmapids	ID/array	Zwraca obrazy używane na podanych mapach.
select_image	flag	Zwraca właściwość `image` zawierającą obraz zakodowany w Base64.
sortfield	string/array	Sortuje wynik według podanych właściwości. Możliwe wartości: `imageid`, `name`.
countOutput	boolean	Te parametry są opisane w komentarzu referencyjnym.
editable	boolean	
excludeSearch	boolean	
filter	object	
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli został użyty parametr `countOutput`.

Przykłady

Pobieranie obrazu

Pobierz wszystkie dane obrazu o ID „2”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "image.get",
    "params": {
        "output": "extend",
        "select_image": true,
        "imageids": "2"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "imageid": "2",
            "imagetype": "1",
            "name": "Cloud_(24)",
            "image": "iVBORw0KGgoAAAANSUhEUgAAABgAAAANCAYAAACzbK7QAAAABHNCSVQICAgIfAhkiAAAAAlwSFlzAAACmAAA
        }
    ],
    "id": 1
}
```

Źródło

CImage::get() w *ui/include/classes/api/services/CImage.php*.

image.update

Opis

`object image.update(object/array images)`

Ta metoda umożliwia aktualizację istniejących obrazów.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkownika typu *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Właściwości obrazu do zaktualizowania.

Właściwość `imageid` musi być zdefiniowana dla każdego obrazu, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko przekazane właściwości, wszystkie pozostałe pozostaną bez zmian.

Metoda akceptuje obrazy ze standardowymi właściwościami obrazu.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych obrazów we właściwości `imageids`.

Przykłady

Zmień nazwę obrazu

Zmień nazwę obrazu na „Cloud icon”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "image.update",
    "params": {
        "imageid": "2",
        "name": "Cloud icon"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "imageids": [
            "2"
        ]
    },
    "id": 1
}
```

Źródło

CImage::update() w *ui/include/classes/api/services/CImage.php*.

Porządkowanie

Ta klasa jest zaprojektowana do pracy z porządkowaniem.

Referencje obiektu:

- Housekeeping

Dostępne metody:

- housekeeping.get - retrieve housekeeping
- housekeeping.update - update housekeeping

Obiekt sprzątania (housekeeping)

Następujące obiekty są bezpośrednio powiązane z API `housekeeping`.

Housekeeping

Obiekt ustawień ma następujące właściwości.

Właściwość	Typ	Opis
hk_events_mode	integer	Włącza wewnętrzny housekeeping dla zdarzeń i alertów. Możliwe wartości: 0 - Wyłącz; 1 - *(domyślnie)* Włącz.
hk_events_trigger	string	Okres przechowywania danych wyzwalaczy. Akceptuje sekundy oraz jednostkę czasu z sufiksem. Domyślnie: 365d.
hk_events_service	string	Okres przechowywania danych usług. Akceptuje sekundy oraz jednostkę czasu z sufiksem. Domyślnie: 1d.
hk_events_internal	string	Okres przechowywania danych wewnętrznych. Akceptuje sekundy oraz jednostkę czasu z sufiksem. Domyślnie: 1d.
hk_events_discovery	string	Okres przechowywania danych wykrywania sieci. Akceptuje sekundy oraz jednostkę czasu z sufiksem. Domyślnie: 1d.
hk_events_autoreg	string	Okres przechowywania danych autorejestracji. Akceptuje sekundy oraz jednostkę czasu z sufiksem. Domyślnie: 1d.
hk_services_mode	integer	Włącza wewnętrzny housekeeping dla usług. Możliwe wartości: 0 - Wyłącz; 1 - *(domyślnie)* Włącz.
hk_services	string	Okres przechowywania danych usług. Akceptuje sekundy oraz jednostkę czasu z sufiksem. Domyślnie: 365d.
hk_audit_mode	integer	Włącza wewnętrzny housekeeping dla audytu. Możliwe wartości: 0 - Wyłącz; 1 - *(domyślnie)* Włącz.
hk_audit	string	Okres przechowywania danych audytu. Akceptuje sekundy oraz jednostkę czasu z sufiksem. Domyślnie: 31d.
hk_sessions_mode	integer	Włącza wewnętrzny housekeeping dla sesji. Możliwe wartości: 0 - Wyłącz; 1 - *(domyślnie)* Włącz.
hk_sessions	string	Okres przechowywania danych sesji. Akceptuje sekundy oraz jednostkę czasu z sufiksem. Domyślnie: 31d.

Właściwość	Typ	Opis
hk_history_mode	integer	Włącza wewnętrzny housekeeping dla historii. Możliwe wartości: 0 - Wyłącz; 1 - *(domyślnie)* Włącz.
hk_history_global	integer	Zastępuje okres historii pozycji. Możliwe wartości: 0 - Nie zastępuj; 1 - *(domyślnie)* Zastąp.
hk_history	string	Okres przechowywania danych historii. Akceptuje sekundy oraz jednostkę czasu z sufiksem. Domyślnie: 31d.
hk_trends_mode	integer	Włącza wewnętrzny housekeeping dla trendów. Możliwe wartości: 0 - Wyłącz; 1 - *(domyślnie)* Włącz.
hk_trends_global	integer	Zastępuje okres trendów pozycji. Możliwe wartości: 0 - Nie zastępuj; 1 - *(domyślnie)* Zastąp.
hk_trends	string	Okres przechowywania danych trendów. Akceptuje sekundy oraz jednostkę czasu z sufiksem. Domyślnie: 365d.
db_extension	string	Flaga konfiguracji rozszerzenia DB. Jeśli ta flaga jest ustawiona na ”timescaledb”, serwer zmienia swoje zachowanie w zakresie housekeeping i usuwania pozycji. Zachowanie właściwości: - *tylko do odczytu*
compression_availability	integer	Czy kompresja danych jest obsługiwana przez bazę danych (lub jej rozszerzenie). Możliwe wartości: 0 - Niedostępna; 1 - Dostępna. Zachowanie właściwości: - *tylko do odczytu*
compression_status	integer	Włącza kompresję TimescaleDB dla historii i trendów. Możliwe wartości: 0 - *(domyślnie)* Wyłączona; 1 - Włączona.
compress_older	string	Kompresuje rekordy historii i trendów starsze niż określony okres. Akceptuje sekundy oraz jednostkę czasu z sufiksem. Domyślnie: 7d.

housekeeping.get

Opis

`object housekeeping.get(object parameters)`

Ta metoda umożliwia pobranie obiektu housekeeping zgodnie z podanymi parametrami.

Note:
Ta metoda jest dostępna dla użytkowników każdego typu. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji znajduje się w sekcji User roles.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje tylko jeden parametr.

Parametr	Typ	Opis
output	query	Ten parametr jest opisany w komentarzu referencyjnym.

Wartości zwracane

`(object)` Zwraca obiekt housekeeping.

Przykłady

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "housekeeping.get",
    "params": {
        "output": "extend"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "hk_events_mode": "1",
        "hk_events_trigger": "365d",
        "hk_events_service": "1d",
        "hk_events_internal": "1d",
        "hk_events_discovery": "1d",
        "hk_events_autoreg": "1d",
        "hk_services_mode": "1",
        "hk_services": "365d",
        "hk_audit_mode": "1",
        "hk_audit": "31d",
        "hk_sessions_mode": "1",
        "hk_sessions": "365d",
        "hk_history_mode": "1",
        "hk_history_global": "0",
        "hk_history": "31d",
        "hk_trends_mode": "1",
        "hk_trends_global": "0",
        "hk_trends": "365d",
        "db_extension": "",
        "compression_status": "0",
        "compress_older": "7d"
    },
    "id": 1
}
```

Źródło

CHousekeeping ::get() w *ui/include/classes/api/services/CHousekeeping.php*.

housekeeping.update

Opis

`object housekeeping.update(object housekeeping)`

Ta metoda umożliwia aktualizację istniejących ustawień housekeeping.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkownika typu *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object)` Właściwości housekeeping do zaktualizowania.

Zwracane wartości

`(array)` Zwraca tablicę z nazwami zaktualizowanych parametrów.

Przykłady

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "housekeeping.update",
    "params": {
        "hk_events_mode": "1",
        "hk_events_trigger": "200d",
        "hk_events_internal": "2d",
        "hk_events_discovery": "2d"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        "hk_events_mode",
        "hk_events_trigger",
        "hk_events_internal",
        "hk_events_discovery"
    ],
    "id": 1
}
```

Źródło

CHousekeeping::update() w *ui/include/classes/api/services/CHousekeeping.php*.

Pozycja

Ta klasa jest przeznaczona do pracy z pozycjami.

Odwołania do obiektów:

- Pozycja
  - Nagłówek HTTP
  - Pole zapytania HTTP
- Tag pozycji
- Przetwarzanie wstępne pozycji

Dostępne metody:

- item.create - utwórz nowe pozycje
- item.delete - usuń pozycje

- item.get - pobierz pozycje
- item.update - zaktualizuj pozycje

Obiekt pozycji

Następujące obiekty są bezpośrednio powiązane z API `item`.

Pozycja

Note:
Pozycje web nie mogą być bezpośrednio tworzone, aktualizowane ani usuwane za pomocą Zabbix API.

Obiekt pozycji ma następujące właściwości.

Właściwość	Typ	Opis
itemid	ID	ID pozycji. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji
delay	string	Interwał aktualizacji pozycji. Akceptuje sekundy lub jednostkę czasu z sufiksem (np. 30s, 1m, 2h, 1d) oraz opcjonalnie jeden lub więcej interwałów niestandardowych, wszystkie oddzielone średnikami. Interwały niestandardowe mogą być kombinacją interwałów elastycznych i harmonogramowanych. Akceptuje makra użytkownika. Jeśli są używane, wartość musi być pojedynczym makrem. Wiele makr lub makra zmieszane z tekstem nie są obsługiwane. Interwały elastyczne mogą być zapisane jako dwa makra oddzielone ukośnikiem (np. `{$FLEX_INTERVAL}/{$FLEX_PERIOD}`). Przykład: `1h;wd1-5h9-18;{$Macro1}/1-7,00:00-24:00;0/6-7,12:00-24:00;{$Macr` Zachowanie właściwości: - *wymagane* jeśli `type` jest ustawione na ”Zabbix agent” (0), ”Simple check” (3), ”Zabbix internal” (5), ”External check” (10), ”Database monitor” (11), ”IPMI agent” (12), ”SSH agent” (13), ”TELNET agent” (14), ”Calculated” (15), ”JMX agent” (16), ”HTTP agent” (19), ”SNMP agent” (20), ”Script” (21), ”Browser” (22), lub jeśli `type` jest ustawione na ”Zabbix agent (active)” (7) i `key_` nie zawiera ”mqtt.get”
hostid	ID	ID hosta lub szablonu, do którego należy pozycja. Zachowanie właściwości: - *stałe* - *wymagane* dla operacji tworzenia
interfaceid	ID	ID interfejsu hosta pozycji. Zachowanie właściwości: - *wymagane* jeśli pozycja należy do hosta i `type` jest ustawione na ”Zabbix agent”, ”IPMI agent”, ”JMX agent”, ”SNMP trap” lub ”SNMP agent” - *obsługiwane* jeśli pozycja należy do hosta i `type` jest ustawione na ”Simple check”, ”External check”, ”SSH agent”, ”TELNET agent” lub ”HTTP agent” - *tylko do odczytu* dla obiektów wykrytych

Właściwość	Typ	Opis
key_	string	Klucz pozycji. Zachowanie właściwości: - *wymagane* dla operacji tworzenia - *tylko do odczytu* dla obiektów dziedziczonych lub wykrytych
name	string	Nazwa pozycji. Obsługuje makra użytkownika. Zachowanie właściwości: - *wymagane* dla operacji tworzenia - *tylko do odczytu* dla obiektów dziedziczonych lub wykrytych
name_resolved	string	Nazwa pozycji z rozwiniętymi makrami użytkownika. Zachowanie właściwości: - *tylko do odczytu*
type	integer	Typ pozycji. Możliwe wartości: 0 - Zabbix agent; 2 - Zabbix trapper; 3 - Simple check; 5 - Zabbix internal; 7 - Zabbix agent (active); 9 - pozycja web; 10 - External check; 11 - Database monitor; 12 - IPMI agent; 13 - SSH agent; 14 - TELNET agent; 15 - Calculated; 16 - JMX agent; 17 - SNMP trap; 18 - pozycja zależna; 19 - HTTP agent; 20 - SNMP agent; 21 - Script; 22 - Browser. Zachowanie właściwości: - *wymagane* dla operacji tworzenia - *tylko do odczytu* dla obiektów dziedziczonych lub wykrytych
url	string	Ciąg URL. Obsługuje makra użytkownika, {HOST.IP}, {HOST.CONN}, {HOST.DNS}, {HOST.HOST}, {HOST.NAME}, {HOST.PORT}, {ITEM.ID}, {ITEM.KEY}. Zachowanie właściwości: - *wymagane* jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych lub wykrytych

Właściwość	Typ	Opis
value_type	integer	Typ informacji pozycji. Możliwe wartości: 0 - liczba zmiennoprzecinkowa; 1 - znakowy; 2 - log; 3 - liczba bez znaku; 4 - tekst; 5 - binarny; 6 - JSON. Zachowanie właściwości: - *wymagane* dla operacji tworzenia - *tylko do odczytu* dla obiektów dziedziczonych lub wykrytych
allow_traps	integer	Zezwala na wypełnianie wartości podobnie jak w pozycji trapper. 0 - *(domyślnie)* Nie zezwalaj na przyjmowanie danych przychodzących; 1 - Zezwalaj na przyjmowanie danych przychodzących. Zachowanie właściwości: - *obsługiwane* jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów wykrytych
authtype	integer	Metoda uwierzytelniania. Możliwe wartości, jeśli `type` jest ustawione na ”SSH agent”: 0 - *(domyślnie)* hasło; 1 - klucz publiczny. Możliwe wartości, jeśli `type` jest ustawione na ”HTTP agent”: 0 - *(domyślnie)* brak; 1 - basic; 2 - NTLM; 3 - Kerberos; 4 - Digest. Zachowanie właściwości: - *obsługiwane* jeśli `type` jest ustawione na ”SSH agent” lub ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych (jeśli `type` jest ustawione na ”HTTP agent”) lub wykrytych
description	string	Opis pozycji. Zachowanie właściwości: - *tylko do odczytu* dla obiektów wykrytych
error	string	Tekst błędu, jeśli występują problemy z aktualizacją wartości pozycji. Zachowanie właściwości: - *tylko do odczytu*
flags	integer	Pochodzenie pozycji. Możliwe wartości: 0 - zwykła pozycja; 4 - pozycja przekonwertowana z prototypu. Zachowanie właściwości: - *tylko do odczytu*

Właściwość	Typ	Opis
follow_redirects	integer	Podążaj za przekierowaniami odpowiedzi podczas odpytywania o dane. Możliwe wartości: 0 - Nie podążaj za przekierowaniami; 1 - *(domyślnie)* Podążaj za przekierowaniami. Zachowanie właściwości: - *obsługiwane* jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych lub wykrytych
headers	array	Tablica nagłówków, które zostaną wysłane podczas wykonywania żądania HTTP. Zachowanie właściwości: - *obsługiwane* jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych lub wykrytych
history	string	Jednostka czasu określająca, jak długo dane historii powinny być przechowywane. Akceptuje również makro użytkownika. Domyślnie: 31d. Zachowanie właściwości: - *tylko do odczytu* dla obiektów wykrytych
http_proxy	string	Ciąg połączenia proxy HTTP(S). Zachowanie właściwości: - *obsługiwane* jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych lub wykrytych
inventory_link	integer	ID pola inwentarza hosta, które jest wypełniane przez pozycję. Zobacz stronę inwentarza hosta, aby uzyskać listę obsługiwanych pól inwentarza hosta i ich ID. Domyślnie: 0. Zachowanie właściwości: - *obsługiwane* jeśli `value_type` jest ustawione na ”numeric float”, ”character”, ”numeric unsigned” lub ”text” - *tylko do odczytu* dla obiektów wykrytych
ipmi_sensor	string	Czujnik IPMI. Zachowanie właściwości: - *wymagane* jeśli `type` jest ustawione na ”IPMI agent” i `key_` nie jest ustawione na ”ipmi.get” - *obsługiwane* jeśli `type` jest ustawione na ”IPMI agent” - *tylko do odczytu* dla obiektów dziedziczonych lub wykrytych
jmx_endpoint	string	Niestandardowy ciąg połączenia JMX agent. Wartość domyślna: service:jmx:rmi:///jndi/rmi://{HOST.CONN}:{HOST.PORT}/jmxrmi Zachowanie właściwości: - *obsługiwane* jeśli `type` jest ustawione na ”JMX agent” - *tylko do odczytu* dla obiektów wykrytych
lastclock	timestamp	Czas ostatniej aktualizacji wartości pozycji. Domyślnie wyświetlane są tylko wartości z ostatnich 24 godzin. Możesz wydłużyć ten okres, zmieniając wartość parametru *Max history display period* w sekcji menu *Administration → General*. Zachowanie właściwości: - *tylko do odczytu*

Właściwość	Typ	Opis
lastns	integer	Nanosekundy ostatniej aktualizacji wartości pozycji. Domyślnie wyświetlane są tylko wartości z ostatnich 24 godzin. Możesz wydłużyć ten okres, zmieniając wartość parametru *Max history display period* w sekcji menu *Administration → General*. Zachowanie właściwości: - *tylko do odczytu*
lastvalue	string	Ostatnia wartość pozycji. Domyślnie wyświetlane są tylko wartości z ostatnich 24 godzin. Możesz wydłużyć ten okres, zmieniając wartość parametru *Max history display period* w sekcji menu *Administration → General*. Zachowanie właściwości: - *tylko do odczytu*
logtimefmt	string	Format czasu we wpisach logu. Zachowanie właściwości: - *obsługiwane* jeśli `value_type` jest ustawione na ”log” - *tylko do odczytu* dla obiektów dziedziczonych lub wykrytych
master_itemid	ID	ID pozycji nadrzędnej. Zachowanie właściwości: - *wymagane* jeśli `type` jest ustawione na ”Dependent item” - *tylko do odczytu* dla obiektów dziedziczonych lub wykrytych
output_format	integer	Czy odpowiedź powinna zostać przekonwertowana do JSON. 0 - *(domyślnie)* Przechowuj surowe dane; 1 - Konwertuj do JSON. Zachowanie właściwości: - *obsługiwane* jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych lub wykrytych
params	string	Dodatkowe parametry zależne od typu pozycji: - wykonywany skrypt dla pozycji SSH agent i TELNET agent; - zapytanie SQL dla pozycji monitorowania bazy danych; - formuła dla pozycji obliczanych; - skrypt dla pozycji typu Script i Browser. Zachowanie właściwości: - *wymagane* jeśli `type` jest ustawione na ”Database monitor”, ”SSH agent”, ”TELNET agent”, ”Calculated”, ”Script” lub ”Browser” - *tylko do odczytu* dla obiektów dziedziczonych (jeśli `type` jest ustawione na ”Script” lub ”Browser”) lub wykrytych
parameters	object/array	Dodatkowe parametry, jeśli `type` jest ustawione na ”Script” lub ”Browser”. Tablica obiektów z właściwościami `name` i `value`, gdzie `name` musi być unikalne. Zachowanie właściwości: - *obsługiwane* jeśli `type` jest ustawione na ”Script” lub ”Browser” - *tylko do odczytu* dla obiektów dziedziczonych lub wykrytych
password	string	Hasło do uwierzytelniania. Zachowanie właściwości: - *wymagane* jeśli `type` jest ustawione na ”JMX agent” i `username` jest ustawione - *obsługiwane* jeśli `type` jest ustawione na ”Simple check”, ”SSH agent”, ”TELNET agent”, ”Database monitor” lub ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych (jeśli `type` jest ustawione na ”HTTP agent”) lub wykrytych

Właściwość	Typ	Opis
post_type	integer	Typ treści danych POST przechowywanych we właściwości `posts`. Możliwe wartości: 0 - *(domyślnie)* Surowe dane; 2 - Dane JSON; 3 - Dane XML. Zachowanie właściwości: - *obsługiwane* jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych lub wykrytych
posts	string	Dane treści żądania HTTP(S). Zachowanie właściwości: - *wymagane* jeśli `type` jest ustawione na ”HTTP agent” i `post_type` jest ustawione na ”JSON data” lub ”XML data” - *obsługiwane* jeśli `type` jest ustawione na ”HTTP agent” i `post_type` jest ustawione na ”Raw data” - *tylko do odczytu* dla obiektów dziedziczonych lub wykrytych
prevvalue	string	Poprzednia wartość pozycji. Domyślnie wyświetlane są tylko wartości z ostatnich 24 godzin. Możesz wydłużyć ten okres, zmieniając wartość parametru *Max history display period* w sekcji menu *Administration → General*. Zachowanie właściwości: - *tylko do odczytu*
privatekey	string	Nazwa pliku klucza prywatnego. Zachowanie właściwości: - *wymagane* jeśli `type` jest ustawione na ”SSH agent” i `authtype` jest ustawione na ”public key” - *tylko do odczytu* dla obiektów wykrytych
publickey	string	Nazwa pliku klucza publicznego. Zachowanie właściwości: - *wymagane* jeśli `type` jest ustawione na ”SSH agent” i `authtype` jest ustawione na ”public key” - *tylko do odczytu* dla obiektów wykrytych
query_fields	array	Tablica pól zapytania, które zostaną wysłane podczas wykonywania żądania HTTP. Zachowanie właściwości: - *obsługiwane* jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych lub wykrytych
request_method	integer	Typ metody żądania. Możliwe wartości: 0 - *(domyślnie)* GET; 1 - POST; 2 - PUT; 3 - HEAD. Zachowanie właściwości: - *obsługiwane* jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych lub wykrytych

Właściwość	Typ	Opis
retrieve_mode	integer	Która część odpowiedzi powinna zostać zapisana. Możliwe wartości, jeśli `request_method` jest ustawione na ”GET”, ”POST” lub ”PUT”: 0 - *(domyślnie)* Treść; 1 - Nagłówki; 2 - Zostaną zapisane zarówno treść, jak i nagłówki. Możliwe wartości, jeśli `request_method` jest ustawione na ”HEAD”: 1 - Nagłówki.
snmp_oid	string	Zachowanie właściwości: - *obsługiwane* jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych lub wykrytych SNMP OID. Zachowanie właściwości: - *wymagane* jeśli `type` jest ustawione na ”SNMP agent” - *tylko do odczytu* dla obiektów dziedziczonych lub wykrytych
ssl_cert_file	string	Ścieżka do pliku publicznego klucza SSL. Zachowanie właściwości: - *obsługiwane* jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych lub wykrytych
ssl_key_file	string	Ścieżka do pliku prywatnego klucza SSL. Zachowanie właściwości: - *obsługiwane* jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych lub wykrytych
ssl_key_password	string	Hasło do pliku klucza SSL. Zachowanie właściwości: - *obsługiwane* jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych lub wykrytych
state	integer	Stan pozycji. Możliwe wartości: 0 - *(domyślnie)* normalny; 1 - nieobsługiwane. Zachowanie właściwości: - *tylko do odczytu*
status	integer	Status pozycji. Możliwe wartości: 0 - *(domyślnie)* pozycja włączona; 1 - pozycja wyłączona.
status_codes	string	Zakresy wymaganych kodów statusu HTTP, oddzielone przecinkami. Obsługuje również makra użytkownika jako część listy rozdzielanej przecinkami. Przykład: 200,200-{$M},{$M},200-400 Zachowanie właściwości: - *obsługiwane* jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych lub wykrytych

Właściwość	Typ	Opis
templateid	ID	ID pozycji nadrzędnego szablonu. *Wskazówka*: Użyj właściwości `hostid`, aby określić szablon, do którego należy pozycja. Zachowanie właściwości: - *tylko do odczytu*
timeout	string	Limit czasu żądania odpytywania danych pozycji. Akceptuje sekundy lub jednostkę czasu z sufiksem (np. 30s, 1m). Akceptuje również makra użytkownika. Zakres możliwych wartości: 1-600s. Domyślnie: "" - użyj ustawień proxy/globalnych. Zachowanie właściwości: - *obsługiwane* jeśli `type` jest ustawione na "Zabbix agent" (0), "Simple check" (3) i `key_` nie zaczyna się od "`vmware.`" i "`icmpping`", "Zabbix agent (active)" (7), "External check" (10), "Database monitor" (11), "SSH agent" (13), "TELNET agent" (14), "HTTP agent" (19), "SNMP agent" (20) i `snmp_oid` zaczyna się od "`walk[`" lub "`get[`", "Script" (21), "Browser" (22) - *tylko do odczytu* dla obiektów dziedziczonych i wykrytych
trapper_hosts	string	Dozwolone hosty. Zachowanie właściwości: - *tylko do odczytu* dla obiektów wykrytych - *obsługiwane* jeśli `type` jest ustawione na "Zabbix trapper", lub jeśli `type` jest ustawione na "HTTP agent" i `allow_traps` jest ustawione na "Allow to accept incoming data"
trends	string	Jednostka czasu określająca, jak długo dane trendów powinny być przechowywane. Akceptuje również makro użytkownika. Domyślnie: 365d. Zachowanie właściwości: - *obsługiwane* jeśli `value_type` jest ustawione na "numeric float" lub "numeric unsigned" - *tylko do odczytu* dla obiektów wykrytych
units	string	Jednostki wartości. Zachowanie właściwości: - *obsługiwane* jeśli `value_type` jest ustawione na "numeric float" lub "numeric unsigned" - *tylko do odczytu* dla obiektów dziedziczonych lub wykrytych
username	string	Nazwa użytkownika do uwierzytelniania. Zachowanie właściwości: - *wymagane* jeśli `type` jest ustawione na "SSH agent", "TELNET agent", lub jeśli `type` jest ustawione na "JMX agent" i `password` jest ustawione - *obsługiwane* jeśli `type` jest ustawione na "Simple check", "Database monitor" lub "HTTP agent" - *tylko do odczytu* dla obiektów dziedziczonych (jeśli `type` jest ustawione na "HTTP agent") lub wykrytych
uuid	string	Uniwersalny unikalny identyfikator, używany do powiązania importowanej pozycji z już istniejącymi. Generowany automatycznie, jeśli nie zostanie podany. Zachowanie właściwości: - *obsługiwane* jeśli pozycja należy do szablonu

Właściwość	Typ	Opis
valuemapid	ID	ID skojarzonej mapy wartości. Zachowanie właściwości: - *obsługiwane* jeśli `value_type` jest ustawione na ”numeric float”, ”character” lub ”numeric unsigned” - *tylko do odczytu* dla obiektów dziedziczonych lub wykrytych
verify_host	integer	Czy weryfikować, że nazwa hosta dla połączenia odpowiada nazwie w certyfikacie hosta. Możliwe wartości: 0 - *(domyślnie)* Nie weryfikuj; 1 - Weryfikuj. Zachowanie właściwości: - *obsługiwane* jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych lub wykrytych
verify_peer	integer	Czy weryfikować, że certyfikat hosta jest autentyczny. Możliwe wartości: 0 - *(domyślnie)* Nie weryfikuj; 1 - Weryfikuj. Zachowanie właściwości: - *obsługiwane* jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych lub wykrytych

Nagłówek HTTP

Obiekt nagłówka ma następujące właściwości:

Właściwość	Typ	Opis
name	string	Nazwa nagłówka HTTP. Zachowanie właściwości: - *wymagane*
value	string	Wartość nagłówka. Zachowanie właściwości: - *wymagane*

Pole zapytania HTTP

Obiekt pola zapytania definiuje nazwę i wartość używane do określenia parametru URL. Ma następujące właściwości:

Właściwość	Type	Opis
name	string	Nazwa parametru. Zachowanie właściwości: - *wymagane*

Właściwość	Type	Opis
value	string	Wartość parametru. Zachowanie właściwości: - *wymagane*

Tag pozycji

Obiekt tagu pozycji ma następujące właściwości.

Właściwość	Type	Opis
tag	string	Nazwa tagu pozycji. Zachowanie właściwości: - *wymagane*
value	string	Wartość tagu pozycji. Zachowanie właściwości: - *tylko do odczytu*.
object	integer	Typ obiektu, z którego tag został odziedziczony. Możliwe wartości: 0 - szablon; 1 - host. Zachowanie właściwości: - *tylko do odczytu*.
objectid	ID	ID obiektu, z którego tag został odziedziczony. Zachowanie właściwości: - *tylko do odczytu*.

Wstępne przetwarzanie pozycji

Obiekt wstępnego przetwarzania pozycji ma następujące właściwości.

Property	Type	Description
type	integer	Typ opcji wstępnego przetwarzania. Możliwe wartości: 1 - Mnożnik niestandardowy; 2 - Przytnij z prawej; 3 - Przytnij z lewej; 4 - Przytnij; 5 - Wyrażenie regularne; 6 - Wartość logiczna na dziesiętną; 7 - Ósemkowa na dziesiętną; 8 - Szesnastkowa na dziesiętną; 9 - Prosta zmiana; 10 - Zmiana na sekundę; 11 - XML XPath; 12 - JSONPath; 13 - W zakresie; 14 - Pasuje do wyrażenia regularnego; 15 - Nie pasuje do wyrażenia regularnego; 16 - Sprawdź błąd w JSON; 17 - Sprawdź błąd w XML; 18 - Sprawdź błąd przy użyciu wyrażenia regularnego; 19 - Odrzuć niezmienione; 20 - Odrzuć niezmienione z heartbeat; 21 - JavaScript; 22 - Wzorzec Prometheus; 23 - Prometheus do JSON; 24 - CSV do JSON; 25 - Zamień; 26 - Sprawdź unsupported; 27 - XML do JSON; 28 - Wartość SNMP walk; 29 - SNMP walk do JSON; 30 - Wartość SNMP get. Property behavior: - *required*
params	string	Dodatkowe parametry używane przez opcję wstępnego przetwarzania. Wiele parametrów jest rozdzielanych znakiem nowej linii (\n). Jeśli `type` jest ustawione na ”Check unsupported”, parametry mają składnię `<scope>[\n<pattern>]`, gdzie *pattern* jest wyrażeniem regularnym, a *scope* jest jednym z: -1 - dopasuj dowolny błąd; 0 - sprawdź, czy komunikat błędu pasuje do *pattern*; 1 - sprawdź, czy komunikat błędu nie pasuje do *pattern*. Property behavior: - *required* jeśli `type` jest ustawione na ”Custom multiplier” (1), ”Right trim” (2), ”Left trim” (3), ”Trim” (4), ”Regular expression” (5), ”XML XPath” (11), ”JSONPath” (12), ”In range” (13), ”Matches regular expression” (14), ”Does not match regular expression” (15), ”Check for error in JSON” (16), ”Check for error in XML” (17), ”Check for error using regular expression” (18), ”Discard unchanged with heartbeat” (20), ”JavaScript” (21), ”Prometheus pattern” (22), ”Prometheus to JSON” (23), ”CSV to JSON” (24), ”Replace” (25), Check unsupported (26), ”SNMP walk value” (28), ”SNMP walk to JSON” (29) lub ”SNMP get value” (30)

Property	Type	Description
error_handler	integer	Typ akcji używanej w przypadku niepowodzenia kroku wstępnego przetwarzania. Możliwe wartości: 0 - Komunikat błędu jest ustawiany przez Zabbix server; 1 - Odrzuć wartość; 2 - Ustaw wartość niestandardową; 3 - Ustaw niestandardowy komunikat błędu. Możliwe wartości, jeśli `type` jest ustawione na ”Check unsupported”: 1 - Odrzuć wartość; 2 - Ustaw wartość niestandardową; 3 - Ustaw niestandardowy komunikat błędu. Property behavior: - *required* jeśli `type` jest ustawione na ”Custom multiplier” (1), ”Regular expression” (5), ”Boolean to decimal” (6), ”Octal to decimal” (7), ”Hexadecimal to decimal” (8), ”Simple change” (9), ”Change per second” (10), ”XML XPath” (11), ”JSONPath” (12), ”In range” (13), ”Matches regular expression” (14), ”Does not match regular expression” (15), ”Check for error in JSON” (16), ”Check for error in XML” (17), ”Check for error using regular expression” (18), ”Prometheus pattern” (22), ”Prometheus to JSON” (23), ”CSV to JSON” (24), ”Check unsupported” (26), ”XML to JSON” (27), ”SNMP walk value” (28), ”SNMP walk to JSON” (29) lub ”SNMP get value” (30)
error_handler_params	string	Parametry obsługi błędów. Property behavior: - *required* jeśli `error_handler` jest ustawione na ”Set custom value” lub ”Set custom error message”

Następujące parametry i procedury obsługi błędów są obsługiwane dla każdego typu wstępnego przetwarzania.

Preprocessing type	Name	Parameter 1	Parameter 2	Parameter 3	Supported error handlers
1	Mnożnik niestandardowy	liczba[1, 6]			0, 1, 2, 3
2	Przytnij z prawej	lista znaków[2]			
3	Przytnij z lewej	lista znaków[2]			
4	Przytnij	lista znaków[2]			
5	Wyrażenie regularne	wzorzec[3]	wynik[2]		0, 1, 2, 3
6	Wartość logiczna na dziesiętną				0, 1, 2, 3
7	Ósemkowa na dziesiętną				0, 1, 2, 3
8	Szesnastkowa na dziesiętną				0, 1, 2, 3

Preprocessing type	Name	Parameter 1	Parameter 2	Parameter 3	Supported error handlers
9	Prosta zmiana				0, 1, 2, 3
10	Zmiana na sekundę				0, 1, 2, 3
11	XML XPath	ścieżka[4]			0, 1, 2, 3
12	JSONPath	ścieżka[4]			0, 1, 2, 3
13	W zakresie	min[1, 6]	max[1, 6]		0, 1, 2, 3
14	Pasuje do wyrażenia regularnego	wzorzec[3]			0, 1, 2, 3
15	Nie pasuje do wyrażenia regularnego	wzorzec[3]			0, 1, 2, 3
16	Sprawdź błąd w JSON	ścieżka[4]			0, 1, 2, 3
17	Sprawdź błąd w XML	ścieżka[4]			0, 1, 2, 3
18	Sprawdź błąd przy użyciu wyrażenia regularnego	wzorzec[3]	wynik[2]		0, 1, 2, 3
19	Odrzuć niezmienione				
20	Odrzuć niezmienione z heartbeat	sekundy[5, 6]			
21	JavaScript	skrypt[2]			
22	Wzorzec Prometheus	wzorzec[6, 7]	`value`, `label`, `function`	wynik[8, 9]	0, 1, 2, 3
23	Prometheus do JSON	wzorzec[6, 7]			0, 1, 2, 3
24	CSV do JSON	znak[2]	znak[2]	0,1	0, 1, 2, 3
25	Zamień	szukany ciąg[2]	zamiennik[2]		

Preprocessing type	Name	Parameter 1	Parameter 2	Parameter 3	Supported error handlers
26	Check unsupported	scope[1]	wzorzec[3, 6]		1, 2, 3
27	XML do JSON				0, 1, 2, 3
28	Wartość SNMP walk	OID[2]	Format: 0 - Bez zmian 1 - UTF-8 z Hex-STRING 2 - MAC z Hex-STRING 3 - Liczba całkowita z BITS		0, 1, 2, 3
29	SNMP walk do JSON[10]	Nazwa pola[2]	Prefiks OID[2]	Format: 0 - Bez zmian 1 - UTF-8 z Hex-STRING 2 - MAC z Hex-STRING 3 - Liczba całkowita z BITS	0, 1, 2, 3
30	Wartość SNMP get	Format: 1 - UTF-8 z Hex-STRING 2 - MAC z Hex-STRING 3 - Liczba całkowita z BITS			0, 1, 2, 3

[1] liczba zmiennoprzecinkowa (liczby całkowite są niejawnie konwertowane na wartości zmiennoprzecinkowe)
[2] ciąg znaków
[3] wyrażenie regularne
[4] JSONPath lub XML XPath
[5] dodatnia liczba całkowita (z obsługą sufiksów czasu, np. 30s, 1m, 2h, 1d)
[6] makro użytkownika
[7] Wzorzec Prometheus zgodny ze składnią: `<metric name>{<label name>="<label value>", ...} == <value>`. Każdy składnik wzorca Prometheus (metryka, nazwa etykiety, wartość etykiety i wartość metryki) może być makrem użytkownika.
[8] Wynik Prometheus zgodny ze składnią: `<label name>` (może być makrem użytkownika), jeśli jako drugi parametr wybrano `label`.
[9] Jedna z funkcji agregujących: `sum`, `min`, `max`, `avg`, `count`, jeśli jako drugi parametr wybrano `function`.
[10] Obsługuje wiele rekordów "Nazwa pola,Prefiks OID,Format", rozdzielonych znakiem nowej linii.

item.create

Opis

`object item.create(object/array items)`

Ta metoda umożliwia tworzenie nowych pozycji.

> **Note:**
> Pozycje web nie mogą być tworzone za pomocą Zabbix API.

Note:
Ta metoda jest dostępna tylko dla użytkowników typu *Admin* i *Super admin*. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji znajduje się w sekcji Role użytkowników.

Parametry

`(object/array)` Pozycje do utworzenia.

Oprócz standardowych właściwości pozycji, metoda akceptuje następujące parametry.

Parametr	Typ	Opis
preprocessing	array	Opcje wstępnego przetwarzania pozycji.
tags	array	Tagi pozycji.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory utworzonych pozycji we właściwości `itemids`. Kolejność zwróconych identyfikatorów odpowiada kolejności przekazanych pozycji.

Przykłady

Tworzenie pozycji

Utwórz numeryczną pozycję typu Zabbix agent z 2 tagami pozycji do monitorowania wolnego miejsca na dysku na hoście o ID „30074”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "item.create",
    "params": {
        "name": "Free disk space on /home/joe/",
        "key_": "vfs.fs.size[/home/joe/,free]",
        "hostid": "30074",
        "type": 0,
        "value_type": 3,
        "interfaceid": "30084",
        "tags": [
            {
                "tag": "component",
                "value": "storage"
            },
            {
                "tag": "equipment",
                "value": "workstation"
            }
        ],
        "delay": "30s"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "24758"
        ]
    },
    "id": 1
}
```

Tworzenie pozycji inwentaryzacji hosta

Utwórz pozycję agenta Zabbix, aby wypełnić pole inwentaryzacji hosta „OS”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "item.create",
    "params": {
        "name": "uname",
        "key_": "system.uname",
        "hostid": "30021",
        "type": 0,
        "interfaceid": "30007",
        "value_type": 1,
        "delay": "10s",
        "inventory_link": 5
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "24759"
        ]
    },
    "id": 1
}
```

Tworzenie pozycji z przetwarzaniem wstępnym

Utwórz pozycję przy użyciu niestandardowego mnożnika.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "item.create",
    "params": {
        "name": "Device uptime",
        "key_": "sysUpTime",
        "hostid": "10084",
        "type": 20,
        "snmp_oid": "SNMPv2-MIB::sysUpTime.0",
        "value_type": 1,
        "delay": "60s",
        "interfaceid": "83",
        "preprocessing": [
            {
                "type": 1,
                "params": "0.01",
                "error_handler": 1,
                "error_handler_params": ""
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
```

```
        "itemids": [
            "44210"
        ]
    },
    "id": 1
}
```

Tworzenie zależnej pozycji

Utwórz zależną pozycję dla nadrzędnej pozycji o ID 24759. Dozwolone są tylko zależności w obrębie tego samego hosta, dlatego nadrzędna i zależna pozycja powinny mieć ten sam hostid.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "item.create",
    "params": {
      "hostid": "30074",
      "name": "Dependent test item",
      "key_": "dependent.item",
      "type": 18,
      "master_itemid": "24759",
      "value_type": 2
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "44211"
        ]
    },
    "id": 1
}
```

Utwórz pozycję HTTP agent

Utwórz pozycję z metodą żądania POST z preprocessingiem odpowiedzi JSON.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "item.create",
    "params": {
        "url":"http://127.0.0.1/http.php",
        "query_fields": [
            {
                "name": "mode",
                "value": "json"
            },
            {
                "name": "min",
                "value": "10"
            },
            {
                "name": "max",
                "value": "100"
            }
        ],
        "interfaceid": "1",
        "type": 19,
```

```
        "hostid": "10254",
        "delay": "5s",
        "key_": "json",
        "name": "HTTP agent example JSON",
        "value_type": 0,
        "output_format": 1,
        "preprocessing": [
            {
                "type": 12,
                "params": "$.random",
                "error_handler": 0,
                "error_handler_params": ""
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "23865"
        ]
    },
    "id": 1
}
```

Utwórz pozycję skryptową

Utwórz proste zbieranie danych za pomocą pozycji skryptowej.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "item.create",
    "params": {
        "name": "Script example",
        "key_": "custom.script.item",
        "hostid": "12345",
        "type": 21,
        "value_type": 4,
        "params": "var request = new HttpRequest();\nreturn request.post(\"https://postman-echo.com/post\"
        "parameters": [
            {
                "name": "host",
                "value": "{HOST.CONN}"
            }
        ],
        "timeout": "6s",
        "delay": "30s"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "23865"
        ]
```

```
    },
    "id": 1
}
```

Źródło

CItem::create() w *ui/include/classes/api/services/CItem.php*.

item.delete

Opis

`object item.delete(array itemIds)`

Ta metoda umożliwia usuwanie pozycji.

Note:
Pozycje web nie mogą być usuwane za pomocą Zabbix API.

Note:
Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(array)` ID pozycji do usunięcia.

Wartości zwracane

`(object)` Zwraca obiekt zawierający identyfikatory usuniętych pozycji we właściwości `itemids`.

Przykłady

Usuwanie wielu pozycji

Usuń dwie pozycje.
Pozycje zależne i prototypy pozycji są usuwane automatycznie, jeśli główna pozycja zostanie usunięta.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "item.delete",
    "params": [
        "22982",
        "22986"
    ],
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "22982",
            "22986"
        ]
    },
    "id": 1
}
```

Źródło

CItem::delete() w *ui/include/classes/api/services/CItem.php*.

item.get

Opis

`integer/array item.get(object parameters)`

Ta metoda umożliwia pobieranie pozycji zgodnie z podanymi parametrami.

> **Note:**
> Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji znajduje się w sekcji Role użytkowników.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
itemids	ID/array	Zwraca tylko pozycje o podanych ID.
groupids	ID/array	Zwraca tylko pozycje należące do hostów z podanych grup.
templateids	ID/array	Zwraca tylko pozycje należące do podanych szablonów.
hostids	ID/array	Zwraca tylko pozycje należące do podanych hostów.
proxyids	ID/array	Zwraca tylko pozycje monitorowane przez podane proxy.
interfaceids	ID/array	Zwraca tylko pozycje używające podanych interfejsów hosta.
graphids	ID/array	Zwraca tylko pozycje używane na podanych wykresach.
triggerids	ID/array	Zwraca tylko pozycje używane w podanych wyzwalaczach.
webitems	flag	Uwzględnia pozycje web w wyniku.
inherited	boolean	Jeśli ustawione na `true`, zwraca tylko pozycje dziedziczone z szablonu.
inheritedTags	boolean	Zwraca pozycje, które mają podane `tags` również w host/szablon/podłączonych szablonach. Możliwe wartości: `true` - szablon/host/podłączone szablony również muszą mieć podane tagi; `false` - *(domyślnie)* tagi z szablonu/hosta/podłączonych szablonów są ignorowane.
templated	boolean	Jeśli ustawione na `true`, zwraca tylko pozycje należące do szablonów.
monitored	boolean	Jeśli ustawione na `true`, zwraca tylko włączone pozycje należące do monitorowanych hostów.
group	string	Zwraca tylko pozycje należące do grupy o podanej nazwie.
host	string	Zwraca tylko pozycje należące do hosta o podanej nazwie.
evaltype	integer	Metoda oceny tagów. Możliwe wartości: 0 - *(domyślnie)* And/Or; 2 - Or.
tags	array	Zwraca tylko pozycje z podanymi tagami. Format: `[{"tag": "<tag>", "value": "<value>", "operator": "<operator>"}, ...]`. Pusta tablica zwraca wszystkie pozycje. Możliwe wartości operatora: 0 - *(domyślnie)* Zawiera; 1 - Równa się; 2 - Nie zawiera; 3 - Nie równa się; 4 - Istnieje; 5 - Nie istnieje.
with_triggers	boolean	Jeśli ustawione na `true`, zwraca tylko pozycje używane w wyzwalaczach.
selectHosts	query	Zwraca właściwość `hosts` z tablicą hostów, do których należy pozycja.
selectInterfaces	query	Zwraca właściwość `interfaces` z tablicą interfejsów hosta używanych przez pozycję.

Parametr	Typ	Opis
selectTriggers	query	Zwraca właściwość `triggers` z wyzwalaczami, w których używana jest pozycja. Obsługuje `count`.
selectGraphs	query	Zwraca właściwość `graphs` z wykresami zawierającymi pozycję. Obsługuje `count`.
selectDiscoveryData	query	Zwraca właściwość `discoveryData` z danymi obiektu wykrywania pozycji. Obiekt wykrywania pozycji łączy wykrytą pozycję z prototypem pozycji, z którego została wykryta. Ma następujące właściwości: `parent_itemid` - `(string)` ID prototypu pozycji, z którego pozycja została utworzona; `key_` - `(string)` klucz prototypu pozycji; `status` - `(int)` status wykrywania pozycji: 0 - *(domyślnie)* pozycja jest wykryta, 1 - pozycja nie jest już wykrywana; `ts_delete` - `(timestamp)` czas, kiedy pozycja, która nie jest już wykrywana, zostanie usunięta; `ts_disable` - `(timestamp)` czas, kiedy pozycja, która nie jest już wykrywana, zostanie wyłączona; `disable_source` - `(int)` wskaźnik określający, czy pozycja została wyłączona przez regułę LLD czy ręcznie: 0 - *(domyślnie)* wyłączona automatycznie, 1 - wyłączona przez regułę LLD.
selectDiscoveryRule	query	Zwraca właściwość `discoveryRule` z regułą LLD, która utworzyła pozycję.
selectInheritedTags	query	Zwraca właściwość `inheritedTags` z tagami znajdującymi się w szablonie/hoście/podłączonych szablonach.
selectPreprocessing	query	Zwraca właściwość `preprocessing` z opcjami przetwarzania wstępnego pozycji.
selectTags	query	Zwraca tagi pozycji we właściwości `tags`.
selectValueMap	query	Zwraca właściwość `valuemap` z mapą wartości pozycji.
filter	object	Zwraca tylko te wyniki, które dokładnie odpowiadają podanemu filtrowi. Akceptuje obiekt, w którym kluczami są nazwy właściwości, a wartościami są pojedyncza wartość lub tablica wartości do dopasowania. Nie obsługuje właściwości typu danych `text` data type. Obsługuje dodatkowe właściwości: `host` - techniczna nazwa hosta, do którego należy pozycja.
limitSelects	integer	Ogranicza liczbę rekordów zwracanych przez podzapytania. Dotyczy następujących podzapytań: `selectGraphs` - wyniki będą sortowane według `name`; `selectTriggers` - wyniki będą sortowane według `description`.
sortfield	string/array	Sortuje wynik według podanych właściwości. Możliwe wartości: `itemid`, `name`, `key_`, `delay`, `history`, `trends`, `type`, `status`.
countOutput	boolean	Te parametry są opisane w komentarzu referencyjnym.
editable	boolean	
excludeSearch	boolean	
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	

Parametr	Typ	Opis
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	
selectItemDiscovery	query	Zwraca właściwość `itemDiscovery` z obiektem wykrywania pozycji. Obiekt wykrywania pozycji łączy pozycję z prototypem pozycji, z którego została utworzona. To zapytanie jest **przestarzałe**; zamiast niego użyj `selectDiscoveryData`.

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli został użyty parametr `countOutput`.

Przykłady

Wyszukiwanie pozycji według klucza

Pobierz wszystkie pozycje używane w wyzwalaczach dla określonego ID hosta, które zawierają słowo „system.cpu” w kluczu pozycji, i posortuj wyniki według nazwy.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "item.get",
    "params": {
        "output": "extend",
        "hostids": "10084",
        "with_triggers": true,
        "search": {
            "key_": "system.cpu"
        },
        "sortfield": "name"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "itemid": "42269",
            "type": "18",
            "snmp_oid": "",
            "hostid": "10084",
            "name": "CPU utilization",
            "key_": "system.cpu.util",
            "delay": "0",
            "history": "7d",
            "trends": "365d",
            "status": "0",
            "value_type": "0",
            "trapper_hosts": "",
            "units": "%",
            "formula": "",
            "logtimefmt": "",
            "templateid": "42267",
            "valuemapid": "0",
            "params": "",
```

```
        "ipmi_sensor": "",
        "authtype": "0",
        "username": "",
        "password": "",
        "publickey": "",
        "privatekey": "",
        "flags": "0",
        "interfaceid": "0",
        "description": "CPU utilization in %.",
        "inventory_link": "0",
        "lifetime": "7d",
        "evaltype": "0",
        "jmx_endpoint": "",
        "master_itemid": "42264",
        "timeout": "",
        "url": "",
        "query_fields": [],
        "posts": "",
        "status_codes": "200",
        "follow_redirects": "1",
        "post_type": "0",
        "http_proxy": "",
        "headers": [],
        "retrieve_mode": "0",
        "request_method": "0",
        "output_format": "0",
        "ssl_cert_file": "",
        "ssl_key_file": "",
        "ssl_key_password": "",
        "verify_peer": "0",
        "verify_host": "0",
        "allow_traps": "0",
        "uuid": "",
        "lifetime_type": "0",
        "enabled_lifetime_type": "2",
        "enabled_lifetime": "0",
        "state": "0",
        "error": "",
        "name_resolved": "CPU utilization",
        "parameters": [],
        "lastclock": "0",
        "lastns": "0",
        "lastvalue": "0",
        "prevvalue": "0"
    },
    {
        "itemid": "42259",
        "type": "0",
        "snmp_oid": "",
        "hostid": "10084",
        "name": "Load average (15m avg)",
        "key_": "system.cpu.load[all,avg15]",
        "delay": "1m",
        "history": "7d",
        "trends": "365d",
        "status": "0",
        "value_type": "0",
        "trapper_hosts": "",
        "units": "",
        "formula": "",
        "logtimefmt": "",
        "templateid": "42219",
```

```
            "valuemapid": "0",
            "params": "",
            "ipmi_sensor": "",
            "authtype": "0",
            "username": "",
            "password": "",
            "publickey": "",
            "privatekey": "",
            "flags": "0",
            "interfaceid": "1",
            "description": "",
            "inventory_link": "0",
            "lifetime": "7d",
            "evaltype": "0",
            "jmx_endpoint": "",
            "master_itemid": "0",
            "timeout": "",
            "url": "",
            "query_fields": [],
            "posts": "",
            "status_codes": "200",
            "follow_redirects": "1",
            "post_type": "0",
            "http_proxy": "",
            "headers": [],
            "retrieve_mode": "0",
            "request_method": "0",
            "output_format": "0",
            "ssl_cert_file": "",
            "ssl_key_file": "",
            "ssl_key_password": "",
            "verify_peer": "0",
            "verify_host": "0",
            "allow_traps": "0",
            "uuid": "",
            "lifetime_type": "0",
            "enabled_lifetime_type": "2",
            "enabled_lifetime": "0",
            "state": "0",
            "error": "",
            "name_resolved": "Load average (15m avg)",
            "parameters": [],
            "lastclock": "0",
            "lastns": "0",
            "lastvalue": "0",
            "prevvalue": "0"
        },
        {
            "itemid": "42249",
            "type": "0",
            "snmp_oid": "",
            "hostid": "10084",
            "name": "Load average (1m avg)",
            "key_": "system.cpu.load[all,avg1]",
            "delay": "1m",
            "history": "7d",
            "trends": "365d",
            "status": "0",
            "value_type": "0",
            "trapper_hosts": "",
            "units": "",
            "formula": "",
```

```
            "logtimefmt": "",
            "templateid": "42209",
            "valuemapid": "0",
            "params": "",
            "ipmi_sensor": "",
            "authtype": "0",
            "username": "",
            "password": "",
            "publickey": "",
            "privatekey": "",
            "flags": "0",
            "interfaceid": "1",
            "description": "",
            "inventory_link": "0",
            "lifetime": "7d",
            "evaltype": "0",
            "jmx_endpoint": "",
            "master_itemid": "0",
            "timeout": "",
            "url": "",
            "query_fields": [],
            "posts": "",
            "status_codes": "200",
            "follow_redirects": "1",
            "post_type": "0",
            "http_proxy": "",
            "headers": [],
            "retrieve_mode": "0",
            "request_method": "0",
            "output_format": "0",
            "ssl_cert_file": "",
            "ssl_key_file": "",
            "ssl_key_password": "",
            "verify_peer": "0",
            "verify_host": "0",
            "allow_traps": "0",
            "uuid": "",
            "lifetime_type": "0",
            "enabled_lifetime_type": "2",
            "enabled_lifetime": "0",
            "state": "0",
            "error": "",
            "name_resolved": "Load average (1m avg)",
            "parameters": [],
            "lastclock": "0",
            "lastns": "0",
            "lastvalue": "0",
            "prevvalue": "0"
        },
        {
            "itemid": "42257",
            "type": "0",
            "snmp_oid": "",
            "hostid": "10084",
            "name": "Load average (5m avg)",
            "key_": "system.cpu.load[all,avg5]",
            "delay": "1m",
            "history": "7d",
            "trends": "365d",
            "status": "0",
            "value_type": "0",
            "trapper_hosts": "",
```

```
        "units": "",
        "formula": "",
        "logtimefmt": "",
        "templateid": "42217",
        "valuemapid": "0",
        "params": "",
        "ipmi_sensor": "",
        "authtype": "0",
        "username": "",
        "password": "",
        "publickey": "",
        "privatekey": "",
        "flags": "0",
        "interfaceid": "1",
        "description": "",
        "inventory_link": "0",
        "lifetime": "7d",
        "evaltype": "0",
        "jmx_endpoint": "",
        "master_itemid": "0",
        "timeout": "",
        "url": "",
        "query_fields": [],
        "posts": "",
        "status_codes": "200",
        "follow_redirects": "1",
        "post_type": "0",
        "http_proxy": "",
        "headers": [],
        "retrieve_mode": "0",
        "request_method": "0",
        "output_format": "0",
        "ssl_cert_file": "",
        "ssl_key_file": "",
        "ssl_key_password": "",
        "verify_peer": "0",
        "verify_host": "0",
        "allow_traps": "0",
        "uuid": "",
        "lifetime_type": "0",
        "enabled_lifetime_type": "2",
        "enabled_lifetime": "0",
        "state": "0",
        "error": "",
        "name_resolved": "Load average (5m avg)",
        "parameters": [],
        "lastclock": "0",
        "lastns": "0",
        "lastvalue": "0",
        "prevvalue": "0"
    },
    {
        "itemid": "42260",
        "type": "0",
        "snmp_oid": "",
        "hostid": "10084",
        "name": "Number of CPUs",
        "key_": "system.cpu.num",
        "delay": "1m",
        "history": "7d",
        "trends": "365d",
        "status": "0",
```

```
            "value_type": "3",
            "trapper_hosts": "",
            "units": "",
            "formula": "",
            "logtimefmt": "",
            "templateid": "42220",
            "valuemapid": "0",
            "params": "",
            "ipmi_sensor": "",
            "authtype": "0",
            "username": "",
            "password": "",
            "publickey": "",
            "privatekey": "",
            "flags": "0",
            "interfaceid": "1",
            "description": "",
            "inventory_link": "0",
            "lifetime": "7d",
            "evaltype": "0",
            "jmx_endpoint": "",
            "master_itemid": "0",
            "timeout": "",
            "url": "",
            "query_fields": [],
            "posts": "",
            "status_codes": "200",
            "follow_redirects": "1",
            "post_type": "0",
            "http_proxy": "",
            "headers": [],
            "retrieve_mode": "0",
            "request_method": "0",
            "output_format": "0",
            "ssl_cert_file": "",
            "ssl_key_file": "",
            "ssl_key_password": "",
            "verify_peer": "0",
            "verify_host": "0",
            "allow_traps": "0",
            "uuid": "",
            "lifetime_type": "0",
            "enabled_lifetime_type": "2",
            "enabled_lifetime": "0",
            "state": "0",
            "error": "",
            "name_resolved": "Number of CPUs",
            "parameters": [],
            "lastclock": "0",
            "lastns": "0",
            "lastvalue": "0",
            "prevvalue": "0"
        }
    ],
    "id": 1
}
```


Wyszukiwanie pozycji zależnych według klucza

Pobierz wszystkie pozycje zależne z hosta o ID „10116”, które mają słowo „apache” w kluczu.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "item.get",
    "params": {
        "output": "extend",
        "hostids": "10116",
        "search": {
            "key_": "apache"
        },
        "filter": {
            "type": 18
        }
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "itemid": "25550",
            "type": "18",
            "snmp_oid": "",
            "hostid": "10116",
            "name": "Days",
            "key_": "apache.status.uptime.days",
            "delay": "0",
            "history": "90d",
            "trends": "365d",
            "status": "0",
            "value_type": "3",
            "trapper_hosts": "",
            "units": "",
            "formula": "",
            "logtimefmt": "",
            "templateid": "0",
            "valuemapid": "0",
            "params": "",
            "ipmi_sensor": "",
            "authtype": "0",
            "username": "",
            "password": "",
            "publickey": "",
            "privatekey": "",
            "flags": "0",
            "interfaceid": "0",
            "description": "",
            "inventory_link": "0",
            "lifetime": "7d",
            "evaltype": "0",
            "jmx_endpoint": "",
            "master_itemid": "25545",
            "timeout": "",
            "url": "",
            "query_fields": [],
            "posts": "",
            "status_codes": "200",
            "follow_redirects": "1",
            "post_type": "0",
            "http_proxy": "",
            "headers": [],
```

```
            "retrieve_mode": "0",
            "request_method": "0",
            "output_format": "0",
            "ssl_cert_file": "",
            "ssl_key_file": "",
            "ssl_key_password": "",
            "verify_peer": "0",
            "verify_host": "0",
            "allow_traps": "0",
            "uuid": "",
            "lifetime_type": "0",
            "enabled_lifetime_type": "2",
            "enabled_lifetime": "0",
            "state": "0",
            "error": "",
            "name_resolved": "Days",
            "parameters": [],
            "lastclock": "0",
            "lastns": "0",
            "lastvalue": "0",
            "prevvalue": "0"
        },
        {
            "itemid": "25555",
            "type": "18",
            "snmp_oid": "",
            "hostid": "10116",
            "name": "Hours",
            "key_": "apache.status.uptime.hours",
            "delay": "0",
            "history": "90d",
            "trends": "365d",
            "status": "0",
            "value_type": "3",
            "trapper_hosts": "",
            "units": "",
            "formula": "",
            "logtimefmt": "",
            "templateid": "0",
            "valuemapid": "0",
            "params": "",
            "ipmi_sensor": "",
            "authtype": "0",
            "username": "",
            "password": "",
            "publickey": "",
            "privatekey": "",
            "flags": "0",
            "interfaceid": "0",
            "description": "",
            "inventory_link": "0",
            "lifetime": "7d",
            "evaltype": "0",
            "jmx_endpoint": "",
            "master_itemid": "25545",
            "timeout": "",
            "url": "",
            "query_fields": [],
            "posts": "",
            "status_codes": "200",
            "follow_redirects": "1",
            "post_type": "0",
```

```
            "http_proxy": "",
            "headers": [],
            "retrieve_mode": "0",
            "request_method": "0",
            "output_format": "0",
            "ssl_cert_file": "",
            "ssl_key_file": "",
            "ssl_key_password": "",
            "verify_peer": "0",
            "verify_host": "0",
            "allow_traps": "0",
            "uuid": "",
            "lifetime_type": "0",
            "enabled_lifetime_type": "2",
            "enabled_lifetime": "0",
            "state": "0",
            "error": "",
            "name_resolved": "Hours",
            "parameters": [],
            "lastclock": "0",
            "lastns": "0",
            "lastvalue": "0",
            "prevvalue": "0"
        }
    ],
    "id": 1
}
```


Znajdowanie pozycji HTTP agent

Znajdź pozycję HTTP agent z typem treści POST XML dla określonego ID hosta.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "item.get",
    "params": {
        "hostids": "10255",
        "filter": {
            "type": 19,
            "post_type": 3
        }
    },
    "id": 1
}
```

Odpowiedź:


```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "itemid": "28252",
            "type": "19",
            "snmp_oid": "",
            "hostid": "10255",
            "name": "template item",
            "key_": "ti",
            "delay": "30s",
            "history": "90d",
            "trends": "365d",
            "status": "0",
            "value_type": "3",
            "trapper_hosts": "",
```

```
            "units": "",
            "formula": "",
            "logtimefmt": "",
            "templateid": "0",
            "valuemapid": "0",
            "params": "",
            "ipmi_sensor": "",
            "authtype": "0",
            "username": "",
            "password": "",
            "publickey": "",
            "privatekey": "",
            "flags": "0",
            "interfaceid": "0",
            "description": "",
            "inventory_link": "0",
            "lifetime": "7d",
            "evaltype": "0",
            "jmx_endpoint": "",
            "master_itemid": "0",
            "timeout": "",
            "url": "localhost",
            "query_fields": [
                {
                    "name": "mode",
                    "value": "xml"
                }
            ],
            "posts": "<body>\r\n<![CDATA[{$MACRO}<foo></bar>]]>\r\n</body>",
            "status_codes": "200",
            "follow_redirects": "0",
            "post_type": "3",
            "http_proxy": "",
            "headers": [],
            "retrieve_mode": "1",
            "request_method": "3",
            "output_format": "0",
            "ssl_cert_file": "",
            "ssl_key_file": "",
            "ssl_key_password": "",
            "verify_peer": "0",
            "verify_host": "0",
            "allow_traps": "0",
            "uuid": "",
            "lifetime_type": "0",
            "enabled_lifetime_type": "2",
            "enabled_lifetime": "0",
            "state": "0",
            "error": "",
            "name_resolved": "template item",
            "parameters": [],
            "lastclock": "0",
            "lastns": "0",
            "lastvalue": "",
            "prevvalue": ""
        }
    ],
    "id": 1
}
```


Pobieranie pozycji z regułami przetwarzania wstępnego

Pobierz wszystkie pozycje i ich reguły przetwarzania wstępnego dla określonego ID hosta.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "item.get",
    "params": {
        "output": ["itemid", "name", "key_"],
        "selectPreprocessing": "extend",
        "hostids": "10254"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemid": "23865",
        "name": "HTTP agent example JSON",
        "key_": "json",
        "preprocessing": [
            {
                "type": "12",
                "params": "$.random",
                "error_handler": "1",
                "error_handler_params": ""
            }
        ]
    },
    "id": 1
}
```

Zobacz także

- Reguła wykrywania
- Wykres
- Host
- Interfejs hosta
- Wyzwalacz

Źródło

CItem::get() w *ui/include/classes/api/services/CItem.php*.

item.update

Opis

`object item.update(object/array items)`

Ta metoda umożliwia aktualizację istniejących pozycji.

Note:
Pozycje web nie mogą być aktualizowane za pomocą Zabbix API.

Note:
Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji znajduje się w sekcji Role użytkowników.

Parametry

`(object/array)` Właściwości pozycji do zaktualizowania.

Właściwość `itemid` musi być zdefiniowana dla każdej pozycji, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko przekazane właściwości, wszystkie pozostałe pozostaną bez zmian.

Oprócz standardowych właściwości pozycji, metoda akceptuje następujące parametry.

Parametr	Typ	Opis
preprocessing	array	Opcje wstępnego przetwarzania pozycji, które zastąpią bieżące opcje wstępnego przetwarzania. Zachowanie parametru: - *tylko do odczytu* dla obiektów dziedziczonych lub obiektów wykrytych
tags	array	Tagi pozycji. Zachowanie parametru: - *tylko do odczytu* dla obiektów wykrytych

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych pozycji we właściwości `itemids`.

Przykłady

Włączanie pozycji

Włącz pozycję, czyli ustaw jej status na „0”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "item.update",
    "params": {
        "itemid": "10092",
        "status": 0
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "10092"
        ]
    },
    "id": 1
}
```

Aktualizacja zależnej pozycji

Zaktualizuj nazwę zależnej pozycji oraz ID pozycji nadrzędnej. Dozwolone są tylko zależności w obrębie tego samego hosta, dlatego pozycja nadrzędna i zależna pozycja powinny mieć ten sam `hostid`.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "item.update",
    "params": {
        "name": "Dependent item updated name",
        "master_itemid": "25562",
        "itemid": "189019"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "189019"
        ]
    },
    "id": 1
}
```

Aktualizacja pozycji HTTP agent

Włącz przechwytywanie wartości pozycji.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "item.update",
    "params": {
        "itemid": "23856",
        "allow_traps": 1
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "23856"
        ]
    },
    "id": 1
}
```

Aktualizacja pozycji z przetwarzaniem wstępnym

Zaktualizuj pozycję za pomocą reguły przetwarzania wstępnego pozycji „W zakresie”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "item.update",
    "params": {
        "itemid": "23856",
        "preprocessing": [
            {
                "type": 13,
                "params": "\n100",
                "error_handler": 1,
                "error_handler_params": ""
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "23856"
```

```
        ]
    },
    "id": 1
}
```

Aktualizowanie pozycji skryptowej

Zaktualizuj pozycję skryptową innym skryptem i usuń niepotrzebne parametry, które były używane przez poprzedni skrypt.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "item.update",
    "params": {
        "itemid": "23865",
        "parameters": [],
        "params": "Zabbix.log(3, 'Log test');\nreturn 1;"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "23865"
        ]
    },
    "id": 1
}
```

Źródło

CItem::update() w *ui/include/classes/api/services/CItem.php*.

Pozycja wykresu

Ta klasa jest przeznaczona do pracy z pozycjami wykresu.

Odwołania do obiektów:

- Pozycja wykresu

Dostępne metody:

- graphitem.get - pobieranie pozycji wykresu

Obiekt elementu wykresu

Następujące obiekty są bezpośrednio powiązane z API `graphitem`.

Element wykresu

Note:
Elementy wykresu można modyfikować wyłącznie przez API `graph`.

Obiekt elementu wykresu ma następujące właściwości.

Właściwość	Typ	Opis
gitemid	ID	ID elementu wykresu. Zachowanie właściwości: *- tylko do odczytu*

Właściwość	Typ	Opis
color	string	Kolor rysowania elementu wykresu jako szesnastkowy kod koloru. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
itemid	ID	ID pozycji. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
calc_fnc	integer	Wartość pozycji, która będzie wyświetlana. Możliwe wartości: 1 - wartość minimalna; 2 - *(domyślnie)* wartość średnia; 4 - wartość maksymalna; 7 - wszystkie wartości; 9 - ostatnia wartość, używana tylko przez wykresy kołowe i rozbite.
drawtype	integer	Styl rysowania elementu wykresu. Możliwe wartości: 0 - *(domyślnie)* linia; 1 - wypełniony obszar; 2 - pogrubiona linia; 3 - kropka; 4 - linia przerywana; 5 - linia gradientowa.
graphid	ID	ID wykresu, do którego należy element wykresu.
sortorder	integer	Pozycja pozycji na wykresie. Domyślnie: zaczyna się od „0” i zwiększa o jeden dla każdego wpisu.
type	integer	Typ elementu wykresu. Możliwe wartości: 0 - *(domyślnie)* prosty; 2 - suma wykresu, używana tylko przez wykresy kołowe i rozbite.
yaxisside	integer	Strona wykresu, po której będzie rysowana skala Y elementu wykresu. Możliwe wartości: 0 - *(domyślnie)* lewa strona; 1 - prawa strona.

graphitem.get

Opis

`integer/array graphitem.get(object parameters)`

Ta metoda umożliwia pobieranie elementów wykresu zgodnie z podanymi parametrami.

> **Note:**
> Ta metoda jest dostępna dla użytkowników każdego typu. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w Rolach użytkowników.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
graphids	ID/array	Zwraca tylko pozycje wykresu należące do podanych wykresów.
itemids	ID/array	Zwraca tylko pozycje wykresu o podanych identyfikatorach pozycji.

Parametr	Typ	Opis
type	integer	Zwraca tylko pozycje wykresu o podanym typie. Listę obsługiwanych typów pozycji wykresu można znaleźć na stronie obiektu pozycji wykresu.
selectGraphs	query	Zwraca właściwość `graphs` zawierającą tablicę wykresów, do których należy pozycja.
sortfield	string/array	Sortuje wynik według podanych właściwości. Możliwe wartości: `gitemid`.
countOutput	boolean	Te parametry opisano w komentarzu referencyjnym.
editable	boolean	
limit	integer	
output	query	
preservekeys	boolean	
sortorder	string/array	

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli został użyty parametr `countOutput`.

Przykłady

Pobieranie pozycji wykresu z wykresu

Pobierz wszystkie pozycje wykresu używane na wykresie wraz z dodatkowymi informacjami o pozycji i hoście.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "graphitem.get",
    "params": {
        "output": "extend",
        "graphids": "387"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "gitemid": "1242",
            "graphid": "387",
            "itemid": "22665",
            "drawtype": "1",
            "sortorder": "1",
            "color": "FF5555",
            "yaxisside": "0",
            "calc_fnc": "2",
            "type": "0"
        },
        {
            "gitemid": "1243",
            "graphid": "387",
            "itemid": "22668",
            "drawtype": "1",
            "sortorder": "2",
            "color": "55FF55",
            "yaxisside": "0",
```

```
            "calc_fnc": "2",
            "type": "0"
        },
        {
            "gitemid": "1244",
            "graphid": "387",
            "itemid": "22671",
            "drawtype": "1",
            "sortorder": "3",
            "color": "009999",
            "yaxisside": "0",
            "calc_fnc": "2",
            "type": "0"
        }
    ],
    "id": 1
}
```


Zobacz także

- Wykres

Źródło

CGraphItem::get() w *ui/include/classes/api/services/CGraphItem.php*.

Problem

Ta klasa jest przeznaczona do pracy z problemami.

Odwołania do obiektów:

- Problem
  - URL typu nośnika
- Tag problemu

Dostępne metody:

- problem.get - pobieranie problemów

Obiekt problemu

Następujące obiekty są bezpośrednio powiązane z API `problem`.

Problem

Note:
Problemy są tworzone przez serwer Zabbix i nie mogą być modyfikowane przez API.

Obiekt problemu ma następujące właściwości.

Właściwość	Typ	Opis
eventid	ID	ID zdarzenia problemu.
source	integer	Typ zdarzenia problemu. Możliwe wartości: 0 - zdarzenie utworzone przez wyzwalacz; 3 - zdarzenie wewnętrzne; 4 - zdarzenie utworzone podczas aktualizacji stanu usługi.

Właściwość	Typ	Opis
object	integer	Typ obiektu powiązanego ze zdarzeniem problemu. Możliwe wartości, jeśli `source` jest ustawione na „zdarzenie utworzone przez wyzwalacz”: 0 - wyzwalacz. Możliwe wartości, jeśli `source` jest ustawione na „zdarzenie wewnętrzne”: 0 - wyzwalacz; 4 - pozycja; 5 - reguła LLD. Możliwe wartości, jeśli `source` jest ustawione na „zdarzenie utworzone podczas aktualizacji stanu usługi”: 6 - usługa.
objectid	ID	ID powiązanego obiektu.
clock	timestamp	Czas utworzenia zdarzenia problemu.
ns	integer	Nanosekundy w momencie utworzenia zdarzenia problemu.
r_eventid	ID	ID zdarzenia przywrócenia.
r_clock	timestamp	Czas utworzenia zdarzenia przywrócenia.
r_ns	integer	Nanosekundy w momencie utworzenia zdarzenia przywrócenia.
cause_eventid	ID	ID zdarzenia przyczyny.
correlationid	ID	ID reguły korelacji, jeśli to zdarzenie zostało przywrócone przez globalną regułę korelacji.
userid	ID	ID użytkownika, który zamknął problem (jeśli problem został zamknięty ręcznie).
name	string	Rozwiązana nazwa problemu.
acknowledged	integer	Stan potwierdzenia problemu. Możliwe wartości: 0 - niepotwierdzony; 1 - potwierdzony.
severity	integer	Bieżący poziom ważności problemu. Możliwe wartości: 0 - niesklasyfikowany; 1 - informacja; 2 - ostrzeżenie; 3 - średni; 4 - wysoki; 5 - katastrofa.
suppressed	integer	Czy problem jest stłumiony. Możliwe wartości: 0 - problem jest w stanie normalnym; 1 - problem jest stłumiony.
opdata	string	Dane operacyjne z rozwiniętymi makrami.
urls	array	Aktywne adresy URL typu nośnika.

URL typu nośnika

Obiekt URL typu nośnika ma następujące właściwości.

Właściwość	Typ	Opis
name	string	Nazwa URL zdefiniowanego typu nośnika.
url	string	Wartość URL zdefiniowanego typu nośnika.

Wyniki będą zawierać wpisy tylko dla aktywnych typów nośników z włączonym wpisem menu zdarzeń. Makra użyte we właściwościach zostaną rozwinięte, ale jeśli jedna z właściwości zawiera nierozwinięte makro, obie właściwości zostaną wykluczone z wyników. Obsługiwane makra opisano w sekcji *Obsługiwane makra*.

Znacznik problemu

Obiekt znacznika problemu ma następujące właściwości.

Właściwość	Typ	Opis
tag	string	Nazwa znacznika problemu.
value	string	Wartość znacznika problemu.

problem.get

Opis

`integer/array problem.get(object parameters)`

Ta metoda umożliwia pobieranie problemów zgodnie z podanymi parametrami.

Ta metoda służy do pobierania nierozwiązanych problemów. Możliwe jest również, jeśli to określono, dodatkowe pobieranie niedawno rozwiązanych problemów. Okres, który określa, jak stare oznacza „niedawno", jest zdefiniowany w *Administracja* → *Ogólne*. Problemy, które zostały rozwiązane przed tym okresem, nie są przechowywane w tabeli problemów. Aby pobrać problemy, które zostały rozwiązane wcześniej w przeszłości, użyj metody `event.get`.

Attention:
Ta metoda może zwracać problemy usuniętej jednostki, jeśli problemy te nie zostały jeszcze usunięte przez housekeeper.

Note:
Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji znajduje się w sekcji Role użytkowników.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
eventids	ID/array	Zwraca tylko problemy o podanych ID.
groupids	ID/array	Zwraca tylko problemy utworzone przez obiekty należące do podanych grup hostów.
hostids	ID/array	Zwraca tylko problemy utworzone przez obiekty należące do podanych hostów.
objectids	ID/array	Zwraca tylko problemy utworzone przez podane obiekty.
source	integer	Zwraca tylko problemy o podanym typie. Listę obsługiwanych typów zdarzeń można znaleźć na stronie obiektu zdarzenia problemu. Domyślnie: 0 - problem utworzony przez wyzwalacz.
object	integer	Zwraca tylko problemy utworzone przez obiekty podanego typu. Listę obsługiwanych typów obiektów można znaleźć na stronie obiektu zdarzenia problemu. Domyślnie: 0 - wyzwalacz.
acknowledged	boolean	Jeśli ustawiono na `true`, zwraca tylko potwierdzone problemy.
action	integer	Zwraca tylko problemy, dla których wykonano podane akcje aktualizacji zdarzenia. W przypadku wielu akcji użyj sumy dowolnych akceptowalnych wartości bitmapy jako maski bitowej (na przykład 34 dla potwierdzenia i wyciszenia zdarzenia).
action_userids	ID/array	Zwraca tylko problemy z podanymi ID użytkowników, którzy wykonali akcje aktualizacji zdarzenia problemu.
suppressed	boolean	Jeśli ustawiono na `true`, zwraca tylko wyciszone problemy.

Parametr	Typ	Opis
symptom	boolean	Jeśli ustawiono na `true`, zwraca tylko zdarzenia problemów będące symptomami.
severities	integer/array	Zwraca tylko problemy o podanych poziomach ważności zdarzeń. Ma zastosowanie tylko wtedy, gdy object to trigger.
evaltype	integer	Metoda oceny tagów. Możliwe wartości: 0 - *(domyślnie)* And/Or; 2 - Or.
tags	array	Zwraca tylko problemy z podanymi tagami. Format: `[{"tag": "<tag>", "value": "<value>", "operator": "<operator>"}, ...]`. Pusta tablica zwraca wszystkie problemy. Możliwe wartości operatora: 0 - *(domyślnie)* Zawiera; 1 - Równe; 2 - Nie zawiera; 3 - Nie równa się; 4 - Istnieje; 5 - Nie istnieje.
recent	boolean	Jeśli ustawiono na `true`, zwraca tylko niedawno rozwiązane problemy (zależy od `ok_period`).
eventid_from	string	Zwraca tylko problemy o ID większym lub równym podanemu ID.
eventid_till	string	Zwraca tylko problemy o ID mniejszym lub równym podanemu ID.
time_from	timestamp	Zwraca tylko problemy utworzone po podanym czasie lub dokładnie o podanym czasie.
time_till	timestamp	Zwraca tylko problemy utworzone przed podanym czasem lub dokładnie o podanym czasie.
selectAcknowledges	query	Zwraca właściwość `acknowledges` z aktualizacjami problemu. Aktualizacje problemu są sortowane w odwrotnej kolejności chronologicznej. Obiekt aktualizacji problemu ma następujące właściwości: `acknowledgeid` - `(ID)` ID aktualizacji; `userid` - `(ID)` ID użytkownika, który zaktualizował zdarzenie; `eventid` - `(ID)` ID zaktualizowanego zdarzenia; `clock` - `(timestamp)` czas aktualizacji zdarzenia; `message` - `(string)` treść wiadomości; `action` - `(integer)` typ akcji aktualizacji (zobacz `event.acknowledge`); `old_severity` - `(integer)` ważność zdarzenia przed tą akcją aktualizacji; `new_severity` - `(integer)` ważność zdarzenia po tej akcji aktualizacji; `suppress_until` - `(timestamp)` czas, do którego zdarzenie będzie wyciszone; `taskid` - `(ID)` ID zadania, jeśli bieżące zdarzenie przechodzi zmianę rangi. Obsługuje `count`.
selectTags	query	Zwraca właściwość `tags` z tagami problemu. Format wyjściowy: `[{"tag": "<tag>", "value": "<value>"}, ...]`.
selectSuppressionData	query	Zwraca właściwość `suppression_data` z listą aktywnych okresów konserwacji i ręcznych wyciszeń: `maintenanceid` - `(ID)` ID okresu konserwacji; `userid` - `(ID)` ID użytkownika, który wyciszył problem; `suppress_until` - `(integer)` czas, do którego problem jest wyciszony.

Parametr	Typ	Opis
filter	object	Zwraca tylko te wyniki, które dokładnie odpowiadają podanemu filtrowi. Akceptuje obiekt, w którym klucze są nazwami właściwości, a wartości są pojedynczą wartością lub tablicą wartości do dopasowania. Nie obsługuje właściwości typu danych `text` data type.
sortfield	string/array	Sortuje wynik według podanych właściwości. Możliwe wartości: `eventid`.
countOutput	boolean	Te parametry są opisane w komentarzu referencyjnym.
editable	boolean	
excludeSearch	boolean	
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli został użyty parametr `countOutput`.

Przykłady

Pobieranie zdarzeń problemów wyzwalacza

Pobierz ostatnie zdarzenia dla wyzwalacza „15112”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "problem.get",
    "params": {
        "output": "extend",
        "selectAcknowledges": "extend",
        "selectTags": "extend",
        "selectSuppressionData": "extend",
        "objectids": "15112",
        "recent": true,
        "sortfield": ["eventid"],
        "sortorder": "DESC"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "eventid": "1245463",
            "source": "0",
            "object": "0",
            "objectid": "15112",
            "clock": "1472457242",
            "ns": "209442442",
            "r_eventid": "1245468",
```

```
            "r_clock": "1472457285",
            "r_ns": "125644870",
            "correlationid": "0",
            "userid": "1",
            "name": "Agent Zabbix na localhost jest niedostępny przez 5 minut",
            "acknowledged": "1",
            "severity": "3",
            "cause_eventid": "0",
            "opdata": "",
            "acknowledges": [
                {
                    "acknowledgeid": "14443",
                    "userid": "1",
                    "eventid": "1245463",
                    "clock": "1472457281",
                    "message": "problem rozwiązany",
                    "action": "6",
                    "old_severity": "0",
                    "new_severity": "0",
                    "suppress_until": "1472511600",
                    "taskid": "0"
                }
            ],
            "suppression_data": [
                {
                    "maintenanceid": "15",
                    "suppress_until": "1472511600",
                    "userid": "0"
                }
            ],
            "suppressed": "1",
            "tags": [
                {
                    "tag": "test-tag",
                    "value": "test-value"
                }
            ]
        }
    ],
    "id": 1
}
```


Pobieranie problemów potwierdzonych przez określonego użytkownika

Pobieranie problemów potwierdzonych przez użytkownika o ID=10

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "problem.get",
    "params": {
        "output": "extend",
        "action": 2,
        "action_userids": [10],
        "selectAcknowledges": ["userid", "action"],
        "sortfield": ["eventid"],
        "sortorder": "DESC"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "eventid": "1248566",
            "source": "0",
            "object": "0",
            "objectid": "15142",
            "clock": "1472457242",
            "ns": "209442442",
            "r_eventid": "1245468",
            "r_clock": "1472457285",
            "r_ns": "125644870",
            "correlationid": "0",
            "userid": "10",
            "name": "Agent Zabbix na localhost jest niedostępny przez 5 minut",
            "acknowledged": "1",
            "severity": "3",
            "cause_eventid": "0",
            "opdata": "",
            "acknowledges": [
                {
                    "userid": "10",
                    "action": "2"
                }
            ],
            "suppressed": "0"
        }
    ],
    "id": 1
}
```


Zobacz także

- Alert
- Pozycja
- Host
- Reguła LLD
- Wyzwalacz

Źródło

CEvent::get() w *ui/include/classes/api/services/CProblem.php*.

Prototyp hosta

Ta klasa jest przeznaczona do pracy z prototypami hostów.

Odwołania do obiektów:

- Prototyp hosta
- Powiązanie grupy
- Prototyp grupy
- Tag prototypu hosta
- Niestandardowy interfejs
    - Szczegóły niestandardowego interfejsu

Dostępne metody:

- hostprototype.create - tworzenie nowych prototypów hostów
- hostprototype.delete - usuwanie prototypów hostów
- hostprototype.get - pobieranie prototypów hostów
- hostprototype.update - aktualizacja prototypów hostów

Obiekt prototypu hosta

Następujące obiekty są bezpośrednio powiązane z API `hostprototype`.

Prototyp hosta

Obiekt prototypu hosta ma następujące właściwości.

Właściwość	Type	Opis
hostid	ID	ID prototypu hosta. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji
host	string	Nazwa techniczna prototypu hosta. Zachowanie właściwości: - *wymagane* dla operacji tworzenia - *tylko do odczytu* dla obiektów dziedziczonych
name	string	Widoczna nazwa prototypu hosta. Domyślnie: wartość właściwości `host`. Zachowanie właściwości: - *tylko do odczytu* dla obiektów dziedziczonych
status	integer	Status prototypu hosta. Możliwe wartości: 0 - *(domyślnie)* monitorowany host; 1 - niemonitorowany host.
flags	integer	Pochodzenie prototypu hosta. Możliwe wartości: 2 - prototyp hosta; 6 - wykryty prototyp hosta Zachowanie właściwości: - *tylko do odczytu*
inventory_mode	integer	Tryb uzupełniania inwentarza hosta. Możliwe wartości: -1 - *(domyślnie)* wyłączony; 0 - ręczny; 1 - automatyczny.
templateid	ID	ID nadrzędnego szablonu prototypu hosta. Zachowanie właściwości: - *tylko do odczytu*
discover	integer	Status wykrywania prototypu hosta. Możliwe wartości: 0 - *(domyślnie)* nowe hosty będą wykrywane; 1 - nowe hosty nie będą wykrywane, a istniejące hosty zostaną oznaczone jako utracone.
custom_interfaces	integer	Źródło niestandardowych interfejsów dla hostów utworzonych przez prototyp hosta. Możliwe wartości: 0 - *(domyślnie)* dziedziczenie interfejsów z nadrzędnego hosta; 1 - użycie niestandardowych interfejsów prototypów hostów. Zachowanie właściwości: - *tylko do odczytu* dla obiektów dziedziczonych

Właściwość	Type	Opis
uuid	string	Uniwersalny unikatowy identyfikator używany do łączenia importowanych prototypów hostów z już istniejącymi. Generowany automatycznie, jeśli nie został podany. Zachowanie właściwości: - *obsługiwane* jeśli prototyp hosta należy do szablonu

Łącze grupy

Obiekt łącza grupy łączy prototyp hosta z grupą hostów. Ma następujące właściwości.

Właściwość	Type	Opis
groupid	ID	ID grupy hostów. Zachowanie właściwości: - *wymagane*

Prototyp grupy

Obiekt prototypu grupy definiuje grupę, która zostanie utworzona dla wykrytego hosta. Ma następujące właściwości.

Właściwość	Type	Opis
group_prototypeid	ID	ID prototypu grupy. Zachowanie właściwości: - *tylko do odczytu*
name	string	Nazwa prototypu grupy. Zachowanie właściwości: - *wymagane* dla operacji tworzenia

Tag prototypu hosta

Obiekt tagu prototypu hosta ma następujące właściwości.

Właściwość	Typ	Opis
tag	string	Nazwa tagu prototypu hosta. Zachowanie właściwości: - *wymagane*
value	string	Wartość tagu prototypu hosta. Zachowanie właściwości: - *tylko do odczytu*.
object	integer	Typ obiektu, z którego tag został odziedziczony. Możliwe wartości: 0 - szablon. Zachowanie właściwości: - *tylko do odczytu*.
objectid	ID	ID obiektu, z którego tag został odziedziczony. Zachowanie właściwości: - *tylko do odczytu*.

Interfejs niestandardowy

Interfejsy niestandardowe są obsługiwane, jeśli `custom_interfaces` obiektu Host prototype object jest ustawione na „użyj niestandardowych interfejsów prototypów hostów”. Obiekt interfejsu niestandardowego ma następujące właściwości.

Właściwość	Typ	Opis
type	integer	Typ interfejsu. Możliwe wartości: 1 - Agent; 2 - SNMP; 3 - IPMI; 4 - JMX. Zachowanie właściwości: - *wymagane*
useip	integer	Czy połączenie powinno być nawiązywane przez IP. Możliwe wartości: 0 - połącz przy użyciu nazwy DNS hosta; 1 - połącz przy użyciu adresu IP hosta. Zachowanie właściwości: - *wymagane*
ip	string	Adres IP używany przez interfejs. Może zawierać makra. Zachowanie właściwości: - *wymagane*, jeśli `useip` jest ustawione na „połącz przy użyciu adresu IP hosta”
dns	string	Nazwa DNS używana przez interfejs. Może zawierać makra. Zachowanie właściwości: - *wymagane*, jeśli `useip` jest ustawione na „połącz przy użyciu nazwy DNS hosta”
port	string	Numer portu używany przez interfejs. Może zawierać makra użytkownika i LLD. Zachowanie właściwości: - *wymagane*
main	integer	Czy interfejs jest używany jako domyślny na hoście. Tylko jeden interfejs danego typu może być ustawiony jako domyślny na hoście. Możliwe wartości: 0 - nie jest domyślny; 1 - domyślny. Zachowanie właściwości: - *wymagane*
details	object	Dodatkowy obiekt dla szczegółów interfejsu niestandardowego. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na „SNMP”

Szczegóły niestandardowego interfejsu

Obiekt szczegółów ma następujące właściwości.

Właściwość	Typ	Opis
version	integer	Wersja interfejsu SNMP. Możliwe wartości: 1 - SNMPv1; 2 - SNMPv2c; 3 - SNMPv3. Zachowanie właściwości: - *wymagane*
bulk	integer	Czy używać zbiorczych żądań SNMP. Możliwe wartości: 0 - nie używaj zbiorczych żądań; 1 - *(domyślnie)* - używaj zbiorczych żądań.
community	string	Społeczność SNMP. Zachowanie właściwości: - *wymagane* jeśli `version` jest ustawione na ”SNMPv1” lub ”SNMPv2c”
max_repetitions	integer	Maksymalna wartość powtórzeń dla natywnych zbiorczych żądań SNMP (GetBulkRequest-PDUs). Używane tylko dla pozycji `discovery[]` i `walk[]` w SNMPv2 i v3. Domyślnie: 10.
securityname	string	Nazwa bezpieczeństwa SNMPv3. Zachowanie właściwości: - *obsługiwane* jeśli `version` jest ustawione na ”SNMPv3”
securitylevel	integer	Poziom bezpieczeństwa SNMPv3. Możliwe wartości: 0 - *(domyślnie)* - noAuthNoPriv; 1 - authNoPriv; 2 - authPriv.
authpassphrase	string	Hasło uwierzytelniania SNMPv3. Zachowanie właściwości: - *obsługiwane* jeśli `version` jest ustawione na ”SNMPv3”
privpassphrase	string	Hasło prywatności SNMPv3. Zachowanie właściwości: - *obsługiwane* jeśli `version` jest ustawione na ”SNMPv3” i `securitylevel` jest ustawione na ”authNoPriv” lub ”authPriv”
authprotocol	integer	Protokół uwierzytelniania SNMPv3. Możliwe wartości: 0 - *(domyślnie)* - MD5; 1 - SHA1; 2 - SHA224; 3 - SHA256; 4 - SHA384; 5 - SHA512. Zachowanie właściwości: - *obsługiwane* jeśli `version` jest ustawione na ”SNMPv3” i `securitylevel` jest ustawione na ”authNoPriv” lub ”authPriv”

Właściwość	Typ	Opis
privprotocol	integer	Protokół prywatności SNMPv3. Używany tylko przez interfejsy SNMPv3. Możliwe wartości: 0 - *(domyślnie)* - DES; 1 - AES128; 2 - AES192; 3 - AES256; 4 - AES192C; 5 - AES256C. Zachowanie właściwości: - *obsługiwane* jeśli `version` jest ustawione na ”SNMPv3” i `securitylevel` jest ustawione na ”authPriv”
contextname	string	Nazwa kontekstu SNMPv3. Zachowanie właściwości: - *obsługiwane* jeśli `version` jest ustawione na ”SNMPv3”

hostprototype.create

Opis

`object hostprototype.create(object/array hostPrototypes)`

Ta metoda umożliwia tworzenie nowych prototypów hostów.

Note:
Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Prototypy hostów do utworzenia.

Oprócz standardowych właściwości prototypu hosta, metoda akceptuje następujące parametry.

Parametr	Typ	Opis
groupLinks	array	Powiązania grup, które mają zostać utworzone dla prototypu hosta. Zachowanie parametru: - *wymagany*
ruleid	ID	ID reguły LLD, do której należy prototyp hosta. Zachowanie parametru: - *wymagany*
groupPrototypes	array	Prototypy grup, które mają zostać utworzone dla prototypu hosta.
macros	object/array	Makra użytkownika, które mają zostać utworzone dla prototypu hosta.
tags	object/array	Tagi prototypu hosta.
interfaces	object/array	Niestandardowe interfejsy prototypu hosta.
templates	object/array	Szablony, które mają zostać podlinkowane do prototypu hosta. Szablony muszą mieć zdefiniowaną wyłącznie właściwość `templateid`.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory utworzonych prototypów hostów we właściwości `hostids`. Kolejność zwróconych identyfikatorów odpowiada kolejności przekazanych prototypów hostów.

Przykłady

Tworzenie prototypu hosta

Utwórz prototyp hosta "{#VM.NAME}" w regule LLD "23542" z prototypem grupy "{#HV.NAME}", parą tagów "datacenter": "{#DATACENTER.NAME}" oraz niestandardowym interfejsem SNMPv2 127.0.0.1:161 ze społecznością {$SNMP_COMMUNITY}. Połącz go z grupą hostów "2".

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "hostprototype.create",
    "params": {
        "host": "{#VM.NAME}",
        "ruleid": "23542",
        "custom_interfaces": "1",
        "groupLinks": [
            {
                "groupid": "2"
            }
        ],
        "groupPrototypes": [
            {
                "name": "{#HV.NAME}"
            }
        ],
        "tags": [
            {
                "tag": "datacenter",
                "value": "{#DATACENTER.NAME}"
            }
        ],
        "interfaces": [
            {
                "main": "1",
                "type": "2",
                "useip": "1",
                "ip": "127.0.0.1",
                "dns": "",
                "port": "161",
                "details": {
                    "version": "2",
                    "bulk": "1",
                    "community": "{$SNMP_COMMUNITY}"
                }
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "hostids": [
            "10103"
        ]
    },
    "id": 1
}
```

Zobacz także

- Powiązanie grupy
- Prototyp grupy
- Tag prototypu hosta
- Niestandardowy interfejs

- Makro użytkownika

Źródło

CHostPrototype::create() w *ui/include/classes/api/services/CHostPrototype.php*.

hostprototype.delete

Opis

`object hostprototype.delete(array hostPrototypeIds)`

Ta metoda umożliwia usuwanie prototypów hosta.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania metody można odwołać w ustawieniach roli użytkownika. Więcej informacji można znaleźć w Role użytkownika.

Parametry

`(array)` ID prototypów hostów do usunięcia.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory usuniętych prototypów hostów we właściwości `hostids`.

Przykłady

Usuwanie wielu prototypów hosta

Usuń dwa prototypy hosta.

Żądanie:

```
{
"jsonrpc": "2.0",
"method": "hostprototype.delete",
"params": [
"10103",
"10105"
],
"id": 1
}
```

Odpowiedź:

```
{
"jsonrpc": "2.0",
"result": {
"hostids": [
"10103",
"10105"
]
},
"id": 1
}
```

Źródło

CHostPrototype::delete() w *ui/include/classes/api/services/CHostPrototype.php*.

hostprototype.get

Opis

`integer/array hostprototype.get(object parameters)`

Ta metoda umożliwia pobieranie prototypów hostów zgodnie z podanymi parametrami.

Note:
Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w Rolach użytkowników.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
hostids	ID/array	Zwracaj tylko prototypy hostów o podanych ID.
discoveryids	ID/array	Zwracaj tylko prototypy hostów należące do podanych reguł LLD.
inherited	boolean	Jeśli ustawiono `true`, zwracaj tylko pozycje dziedziczone z szablonu.
selectDiscoveryData	query	Zwracaj właściwość `discoveryData` z danymi obiektu wykrywania prototypu hosta. Obiekt wykrywania prototypu hosta łączy wykryty prototyp hosta z prototypem hosta, z którego został wykryty. Ma następujące właściwości: `host` - `(string)` ID hosta; `parent_hostid` - `(string)` ID prototypu hosta, z którego utworzono prototyp hosta; `status` - `(int)` status wykrywania prototypu hosta: 0 - *(domyślnie)* prototyp hosta jest wykryty, 1 - prototyp hosta nie jest już wykrywany; `ts_delete` - `(timestamp)` czas, kiedy prototyp hosta, który nie jest już wykrywany, zostanie usunięty; `ts_disable` - `(timestamp)` czas, kiedy prototyp hosta, który nie jest już wykrywany, zostanie wyłączony; `disable_source` - `(int)` wskaźnik określający, czy prototyp hosta został wyłączony przez regułę LLD czy ręcznie: 0 - *(domyślnie)* wyłączony automatycznie, 1 - wyłączony przez regułę LLD.
selectDiscoveryRule	query	Zwracaj właściwość `discoveryRule` z regułą LLD, do której należy prototyp hosta.
selectDiscoveryRulePrototype	query	Zwracaj właściwość `discoveryRulePrototype` z nadrzędnym prototypem reguły LLD, do którego należy prototyp hosta.
selectInterfaces	query	Zwracaj właściwość `interfaces` z niestandardowymi interfejsami prototypu hosta.
selectGroupLinks	query	Zwracaj właściwość `groupLinks` z powiązaniami grup prototypu hosta.
selectGroupPrototypes	query	Zwracaj właściwość `groupPrototypes` z prototypami grup prototypu hosta.
selectInheritedTags	query	Zwracaj właściwość `inheritedTags` z tagami znajdującymi się w podłączonych szablonach.
selectMacros	query	Zwracaj właściwość `macros` z makrami prototypu hosta.
selectParentHost	query	Zwracaj właściwość `parentHost` z hostem, do którego należy prototyp hosta.
selectTags	query	Zwracaj właściwość `tags` z tagami prototypu hosta.
selectTemplates	query	Zwracaj właściwość `templates` z szablonami podłączonymi do prototypu hosta. Obsługuje `count`.
sortfield	string/array	Sortuj wynik według podanych właściwości. Możliwe wartości: `hostid`, `host`, `name`, `status`, `discovered`.
countOutput	boolean	Te parametry opisano w komentarzu referencyjnym.
editable	boolean	
excludeSearch	boolean	
filter	object	
limit	integer	
output	query	
preservekeys	boolean	

Parametr	Typ	Opis
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli został użyty parametr `countOutput`.

Przykłady

Pobieranie prototypów hostów z reguły LLD

Pobierz wszystkie prototypy hostów, ich powiązania z grupami, prototypy grup oraz tagi z reguły LLD.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "hostprototype.get",
    "params": {
        "output": "extend",
        "selectInterfaces": "extend",
        "selectGroupLinks": "extend",
        "selectGroupPrototypes": "extend",
        "selectTags": "extend",
        "discoveryids": "23554"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "hostid": "10092",
            "host": "{#HV.UUID}",
            "name": "{#HV.UUID}",
            "status": "0",
            "templateid": "0",
            "discover": "0",
            "custom_interfaces": "1",
            "uuid": "051a1469d4d045cbbf818fcc843a352e",
            "flags": "2",
            "inventory_mode": "-1",
            "tags": [
                {
                    "tag": "datacenter",
                    "value": "{#DATACENTER.NAME}"
                },
                {
                    "tag": "instance-type",
                    "value": "{#INSTANCE_TYPE}"
                }
            ],
            "groupLinks": [
                {
                    "group_prototypeid": "4",
                    "hostid": "10092",
```

```
                    "groupid": "7",
                    "templateid": "0"
                }
            ],
            "groupPrototypes": [
                {
                    "group_prototypeid": "7",
                    "hostid": "10092",
                    "name": "{#CLUSTER.NAME}",
                    "templateid": "0"
                }
            ],
            "interfaces": [
                {
                    "main": "1",
                    "type": "2",
                    "useip": "1",
                    "ip": "127.0.0.1",
                    "dns": "",
                    "port": "161",
                    "available": "0",
                    "error": "",
                    "errors_from": "0",
                    "disable_until": "0",
                    "details": {
                        "version": "2",
                        "bulk": "1",
                        "community": "{$SNMP_COMMUNITY}",
                        "max_repetitions": "10"
                    }
                }
            ]
        }
    ],
    "id": 1
}
```


Zobacz także

- Powiązanie grupy
- Prototyp grupy
- Makro użytkownika

Źródło

CHostPrototype::get() w *ui/include/classes/api/services/CHostPrototype.php*.

hostprototype.update

Opis

`object hostprototype.update(object/array hostPrototypes)`

Ta metoda umożliwia aktualizację istniejących prototypów hostów.

> **Note:**
> Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Właściwości prototypu hosta do zaktualizowania.

Właściwość `hostid` musi być zdefiniowana dla każdego prototypu hosta, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko przekazane właściwości, wszystkie pozostałe pozostaną bez zmian.

Oprócz standardowych właściwości prototypu hosta, metoda akceptuje następujące parametry.

Parametr	Typ	Opis
groupLinks	array	Dowiązania grup zastępujące bieżące dowiązania grup w prototypie hosta. Zachowanie parametru: - *tylko do odczytu* dla obiektów dziedziczonych
groupPrototypes	array	Prototypy grup zastępujące istniejące prototypy grup w prototypie hosta. Wszystkie prototypy grup, które nie zostały wymienione w żądaniu, zostaną usunięte. Zachowanie parametru: - *tylko do odczytu* dla obiektów dziedziczonych
macros	object/array	Makra użytkownika zastępujące bieżące makra użytkownika. Wszystkie makra, które nie zostały wymienione w żądaniu, zostaną usunięte.
tags	object/array	Tagi prototypu hosta zastępujące bieżące tagi. Wszystkie tagi, które nie zostały wymienione w żądaniu, zostaną usunięte. Zachowanie parametru: - *tylko do odczytu* dla obiektów dziedziczonych
interfaces	object/array	Niestandardowe interfejsy prototypu hosta zastępujące bieżące interfejsy. Obiekt niestandardowego interfejsu powinien zawierać wszystkie swoje parametry. Wszystkie interfejsy, które nie zostały wymienione w żądaniu, zostaną usunięte. Zachowanie parametru: - *obsługiwane*, jeśli `custom_interfaces` obiektu Host prototype object jest ustawione na ”use host prototypes custom interfaces” - *tylko do odczytu* dla obiektów dziedziczonych
templates	object/array	Szablony zastępujące aktualnie podlinkowane szablony. Szablony muszą mieć zdefiniowaną tylko właściwość `templateid`.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych prototypów hostów we właściwości `hostids`.

Przykłady

Wyłączanie prototypu hosta

Wyłącz prototyp hosta, czyli ustaw jego status na „1”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "hostprototype.update",
    "params": {
        "hostid": "10092",
        "status": 1
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "hostids": [
            "10092"
        ]
    },
    "id": 1
}
```

Aktualizowanie tagów prototypu hosta

Zastąp tagi prototypu hosta nowymi.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "hostprototype.update",
    "params": {
        "hostid": "10092",
        "tags": [
            {
                "tag": "datacenter",
                "value": "{#DATACENTER.NAME}"
            },
            {
                "tag": "instance-type",
                "value": "{#INSTANCE_TYPE}"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "hostids": [
            "10092"
        ]
    },
    "id": 1
}
```

Aktualizowanie niestandardowych interfejsów prototypu hosta

Zastąp dziedziczone interfejsy niestandardowymi interfejsami prototypu hosta.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "hostprototype.update",
    "params": {
        "hostid": "10092",
        "custom_interfaces": "1",
        "interfaces": [
            {
                "main": "1",
                "type": "2",
                "useip": "1",
                "ip": "127.0.0.1",
                "dns": "",
                "port": "161",
```

```
                "details": {
                    "version": "2",
                    "bulk": "1",
                    "community": "{$SNMP_COMMUNITY}"
                }
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "hostids": [
            "10092"
        ]
    },
    "id": 1
}
```

Zobacz także

- Łącze grupy
- Prototyp grupy
- Tag prototypu hosta
- Niestandardowy interfejs
- Makro użytkownika

Źródło

CHostPrototype::update() w *ui/include/classes/api/services/CHostPrototype.php*.

Prototyp pozycji

Ta klasa jest przeznaczona do pracy z prototypami pozycji.

Odwołania do obiektów:

- Prototyp pozycji
  - Nagłówek HTTP
  - Pole zapytania HTTP
- Tag prototypu pozycji
- Przetwarzanie wstępne prototypu pozycji

Dostępne metody:

- itemprototype.create - utwórz nowe prototypy pozycji
- itemprototype.delete - usuń prototypy pozycji
- itemprototype.get - pobierz prototypy pozycji
- itemprototype.update - zaktualizuj prototypy pozycji

Obiekt prototypu pozycji

Następujące obiekty są bezpośrednio powiązane z API `itemprototype`.

Prototyp pozycji

Obiekt prototypu pozycji ma następujące właściwości.

Właściwość	Typ	Opis
itemid	ID	ID prototypu pozycji. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji
delay	string	Interwał aktualizacji prototypu pozycji. Akceptuje sekundy lub jednostkę czasu z sufiksem (np. 30s, 1m, 2h, 1d) oraz opcjonalnie jeden lub więcej niestandardowych interwałów, wszystkie oddzielone średnikami. Niestandardowe interwały mogą być kombinacją interwałów elastycznych i harmonogramowanych. Akceptuje makra użytkownika i makra LLD. Jeśli są używane, wartość musi być pojedynczym makrem. Wiele makr lub makra połączone z tekstem nie są obsługiwane. Interwały elastyczne mogą być zapisane jako dwa makra oddzielone ukośnikiem (np. `{$FLEX_INTERVAL}/{$FLEX_PERIOD}`). Przykład: `1h;wd1-5h9-18;{$Macro1}/1-7,00:00-24:00;0/6-7,12:00-24:00;{$Macr` Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”Zabbix agent” (0), ”Simple check” (3), ”Zabbix internal” (5), ”External check” (10), ”Database monitor” (11), ”IPMI agent” (12), ”SSH agent” (13), ”TELNET agent” (14), ”Calculated” (15), ”JMX agent” (16), ”HTTP agent” (19), ”SNMP agent” (20), ”Script” (21), ”Browser” (22), lub jeśli `type` jest ustawione na ”Zabbix agent (active)” (7) i `key_` nie zawiera ”mqtt.get”
hostid	ID	ID hosta, do którego należy prototyp pozycji. Zachowanie właściwości: - *stałe* - *wymagane* dla operacji tworzenia
interfaceid	ID	ID interfejsu hosta prototypu pozycji. Zachowanie właściwości: - *wymagane*, jeśli prototyp pozycji należy do hosta i `type` jest ustawione na ”Zabbix agent”, ”IPMI agent”, ”JMX agent”, ”SNMP trap” lub ”SNMP agent” - *obsługiwane*, jeśli prototyp pozycji należy do hosta i `type` jest ustawione na ”Simple check”, ”External check”, ”SSH agent”, ”TELNET agent” lub ”HTTP agent”
key_	string	Klucz prototypu pozycji. Zachowanie właściwości: - *wymagane* dla operacji tworzenia - *tylko do odczytu* dla obiektów dziedziczonych
name	string	Nazwa prototypu pozycji. Obsługuje makra użytkownika. Zachowanie właściwości: - *wymagane* dla operacji tworzenia - *tylko do odczytu* dla obiektów dziedziczonych

Właściwość	Typ	Opis
type	integer	Typ prototypu pozycji. Możliwe wartości: 0 - Zabbix agent; 2 - Zabbix trapper; 3 - Simple check; 5 - Zabbix internal; 7 - Zabbix agent (active); 10 - External check; 11 - Database monitor; 12 - IPMI agent; 13 - SSH agent; 14 - TELNET agent; 15 - Calculated; 16 - JMX agent; 17 - SNMP trap; 18 - pozycja zależna; 19 - HTTP agent; 20 - SNMP agent; 21 - Script; 22 - Browser. Zachowanie właściwości: - *wymagane* dla operacji tworzenia - *tylko do odczytu* dla obiektów dziedziczonych
url	string	Ciąg URL. Obsługuje makra LLD, makra użytkownika, {HOST.IP}, {HOST.CONN}, {HOST.DNS}, {HOST.HOST}, {HOST.NAME}, {HOST.PORT}, {ITEM.ID}, {ITEM.KEY}. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych
value_type	integer	Typ informacji prototypu pozycji. Możliwe wartości: 0 - liczba zmiennoprzecinkowa; 1 - znakowy; 2 - log; 3 - liczba całkowita bez znaku; 4 - tekst; 5 - binarny; 6 - JSON. Zachowanie właściwości: - *wymagane* dla operacji tworzenia - *tylko do odczytu* dla obiektów dziedziczonych
allow_traps	integer	Zezwala na wypełnianie wartości podobnie jak w pozycji trapper. 0 - *(domyślnie)* Nie zezwalaj na przyjmowanie danych przychodzących; 1 - Zezwalaj na przyjmowanie danych przychodzących. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent”

Właściwość	Typ	Opis
authtype	integer	Metoda uwierzytelniania. Możliwe wartości, jeśli `type` jest ustawione na ”SSH agent”: 0 - *(domyślnie)* hasło; 1 - klucz publiczny. Możliwe wartości, jeśli `type` jest ustawione na ”HTTP agent”: 0 - *(domyślnie)* brak; 1 - basic; 2 - NTLM; 3 - Kerberos; 4 - Digest. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”SSH agent” lub ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych (jeśli `type` jest ustawione na ”HTTP agent”)
description	string	Opis prototypu pozycji.
flags	integer	Pochodzenie prototypu pozycji. Możliwe wartości: 2 - prototyp pozycji; 6 - wykryty prototyp pozycji Zachowanie właściwości: - *tylko do odczytu*
follow_redirects	integer	Podążanie za przekierowaniami odpowiedzi podczas odpytywania o dane. Możliwe wartości: 0 - Nie podążaj za przekierowaniami; 1 - *(domyślnie)* Podążaj za przekierowaniami. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych
headers	array	Tablica nagłówków, które zostaną wysłane podczas wykonywania żądania HTTP. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych
history	string	Jednostka czasu określająca, jak długo dane historii powinny być przechowywane. Akceptuje również makro użytkownika i makro LLD. Domyślnie: 31d.
http_proxy	string	Ciąg połączenia proxy HTTP(S). Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych
ipmi_sensor	string	Czujnik IPMI. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”IPMI agent” i `key_` nie jest ustawione na ”ipmi.get” - *obsługiwane*, jeśli `type` jest ustawione na ”IPMI agent” - *tylko do odczytu* dla obiektów dziedziczonych

Właściwość	Typ	Opis
jmx_endpoint	string	Niestandardowy ciąg połączenia JMX agent. Domyślnie: service:jmx:rmi:///jndi/rmi://{HOST.CONN}:{HOST.PORT}/jmxrmi Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”JMX agent”
logtimefmt	string	Format czasu we wpisach logu. Zachowanie właściwości: - *obsługiwane*, jeśli `value_type` jest ustawione na ”log” - *tylko do odczytu* dla obiektów dziedziczonych
master_itemid	ID	ID nadrzędnej pozycji. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”Dependent item” - *tylko do odczytu* dla obiektów dziedziczonych
output_format	integer	Czy odpowiedź powinna zostać przekonwertowana do JSON. Możliwe wartości: 0 - *(domyślnie)* Przechowuj surowe dane; 1 - Konwertuj do JSON. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych
params	string	Dodatkowe parametry zależne od typu prototypu pozycji: - wykonywany skrypt dla prototypów pozycji SSH agent i TELNET agent; - zapytanie SQL dla prototypów pozycji monitorowania bazy danych; - formuła dla obliczanych prototypów pozycji; - skrypt dla prototypów pozycji typu Script i Browser. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”Database monitor”, ”SSH agent”, ”TELNET agent”, ”Calculated”, ”Script” lub ”Browser” - *tylko do odczytu* dla obiektów dziedziczonych (jeśli `type` jest ustawione na ”Script” lub ”Browser”)
parameters	object/array	Dodatkowe parametry, jeśli `type` jest ustawione na ”Script” lub ”Browser”. Tablica obiektów z właściwościami `name` i `value`, gdzie `name` musi być unikalne. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”Script” lub ”Browser” - *tylko do odczytu* dla obiektów dziedziczonych
password	string	Hasło do uwierzytelniania. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”JMX agent” i `username` jest ustawione - *obsługiwane*, jeśli `type` jest ustawione na ”Simple check”, ”SSH agent”, ”TELNET agent”, ”Database monitor” lub ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych (jeśli `type` jest ustawione na ”HTTP agent”)

Właściwość	Typ	Opis
post_type	integer	Typ treści danych POST przechowywanych we właściwości `posts`. Możliwe wartości: 0 - *(domyślnie)* Surowe dane. 2 - Dane JSON. 3 - Dane XML. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych
posts	string	Dane treści żądania HTTP(S). Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”HTTP agent” i `post_type` jest ustawione na ”JSON data” lub ”XML data” - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” i `post_type` jest ustawione na ”Raw data” - *tylko do odczytu* dla obiektów dziedziczonych
privatekey	string	Nazwa pliku klucza prywatnego. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”SSH agent” i `authtype` jest ustawione na ”public key”
publickey	string	Nazwa pliku klucza publicznego. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”SSH agent” i `authtype` jest ustawione na ”public key”
query_fields	array	Tablica pól zapytania, które zostaną wysłane podczas wykonywania żądania HTTP. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych
request_method	integer	Typ metody żądania. Możliwe wartości: 0 - *(domyślnie)* GET; 1 - POST; 2 - PUT; 3 - HEAD. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych
retrieve_mode	integer	Która część odpowiedzi powinna zostać zapisana. Możliwe wartości, jeśli `request_method` jest ustawione na ”GET”, ”POST” lub ”PUT”: 0 - *(domyślnie)* Treść; 1 - Nagłówki; 2 - Zostaną zapisane zarówno treść, jak i nagłówki. Możliwe wartości, jeśli `request_method` jest ustawione na ”HEAD”: 1 - Nagłówki. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych

Właściwość	Typ	Opis
snmp_oid	string	OID SNMP. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”SNMP agent” - *tylko do odczytu* dla obiektów dziedziczonych
ssl_cert_file	string	Ścieżka do pliku publicznego klucza SSL. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych
ssl_key_file	string	Ścieżka do pliku prywatnego klucza SSL. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych
ssl_key_password	string	Hasło do pliku klucza SSL. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych
status	integer	Status prototypu pozycji. Możliwe wartości: 0 - *(domyślnie)* włączony prototyp pozycji; 1 - wyłączony prototyp pozycji; 3 - nieobsługiwany prototyp pozycji.
status_codes	string	Zakresy wymaganych kodów statusu HTTP, oddzielone przecinkami. Obsługuje również makra użytkownika lub makra LLD jako część listy rozdzielonej przecinkami. Przykład: 200,200-{$M},{$M},200-400 Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych
templateid	ID	ID nadrzędnego prototypu pozycji szablonu. Zachowanie właściwości: - *tylko do odczytu*
timeout	string	Limit czasu żądania odpytywania danych pozycji. Akceptuje sekundy lub jednostkę czasu z sufiksem (np. 30s, 1m). Akceptuje również makra użytkownika i makra LLD. Zakres możliwych wartości: 1-600s. Domyślnie: ”” - użyj ustawień proxy/globalnych. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”Zabbix agent” (0), ”Simple check” (3) i `key_` nie zaczyna się od ”`vmware.`” i ”`icmpping`”, ”Zabbix agent (active)” (7), ”External check” (10), ”Database monitor” (11), ”SSH agent” (13), ”TELNET agent” (14), ”HTTP agent” (19), ”SNMP agent” (20) i `snmp_oid` zaczyna się od ”`walk[`” lub ”`get[`”, ”Script” (21), ”Browser” (22) - *tylko do odczytu* dla obiektów dziedziczonych
trapper_hosts	string	Dozwolone hosty. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”Zabbix trapper”, lub jeśli `type` jest ustawione na ”HTTP agent” i `allow_traps` jest ustawione na ”Allow to accept incoming data”

Właściwość	Typ	Opis
trends	string	Jednostka czasu określająca, jak długo dane trendów powinny być przechowywane. Akceptuje również makro użytkownika i makro LLD. Domyślnie: 365d. Zachowanie właściwości: - *obsługiwane*, jeśli `value_type` jest ustawione na ”numeric float” lub ”numeric unsigned”
units	string	Jednostki wartości. Zachowanie właściwości: - *obsługiwane*, jeśli `value_type` jest ustawione na ”numeric float” lub ”numeric unsigned” - *tylko do odczytu* dla obiektów dziedziczonych
username	string	Nazwa użytkownika do uwierzytelniania. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”SSH agent” lub ”TELNET agent”, lub jeśli `type` jest ustawione na ”JMX agent” i `password` jest ustawione - *obsługiwane*, jeśli `type` jest ustawione na ”Simple check”, ”Database monitor” lub ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych (jeśli `type` jest ustawione na ”HTTP agent”)
uuid	string	Uniwersalny unikalny identyfikator używany do łączenia importowanych prototypów pozycji z już istniejącymi. Generowany automatycznie, jeśli nie został podany. Zachowanie właściwości: - *obsługiwane*, jeśli prototyp pozycji należy do szablonu
valuemapid	ID	ID skojarzonej mapy wartości. Zachowanie właściwości: - *obsługiwane*, jeśli `value_type` jest ustawione na ”numeric float”, ”character” lub ”numeric unsigned” - *tylko do odczytu* dla obiektów dziedziczonych
verify_host	integer	Czy weryfikować, że nazwa hosta dla połączenia odpowiada nazwie w certyfikacie hosta. Możliwe wartości: 0 - *(domyślnie)* Nie weryfikuj; 1 - Weryfikuj. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych
verify_peer	integer	Czy weryfikować autentyczność certyfikatu hosta. Możliwe wartości: 0 - *(domyślnie)* Nie weryfikuj; 1 - Weryfikuj. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych

Właściwość	Typ	Opis
discover	integer	Status wykrywania prototypu pozycji. Możliwe wartości: 0 - *(domyślnie)* nowe pozycje będą wykrywane; 1 - nowe pozycje nie będą wykrywane, a istniejące pozycje zostaną oznaczone jako utracone.

Nagłówek HTTP

Obiekt nagłówka ma następujące właściwości:

Właściwość	Typ	Opis
name	string	Nazwa nagłówka HTTP. Zachowanie właściwości: - *wymagane*
value	string	Wartość nagłówka. Zachowanie właściwości: - *wymagane*

Pole zapytania HTTP

Obiekt pola zapytania definiuje nazwę i wartość używane do określenia parametru URL. Ma następujące właściwości:

Właściwość	Typ	Opis
name	string	Nazwa parametru. Zachowanie właściwości: - *wymagane*
value	string	Wartość parametru. Zachowanie właściwości: - *wymagane*

Tag prototypu pozycji

Obiekt tagu prototypu pozycji ma następujące właściwości.

Właściwość	Typ	Opis
tag	string	Nazwa tagu prototypu pozycji. Zachowanie właściwości: - *wymagane*
value	string	Wartość tagu prototypu pozycji. Zachowanie właściwości: - *tylko do odczytu*.

Właściwość	Typ	Opis
object	integer	Typ obiektu, z którego tag został odziedziczony. Możliwe wartości: 0 - szablon; 1 - host. Zachowanie właściwości: - *tylko do odczytu*.
objectid	ID	ID obiektu, z którego tag został odziedziczony. Zachowanie właściwości: - *tylko do odczytu*.

Wstępne przetwarzanie prototypu pozycji

Obiekt wstępnego przetwarzania prototypu pozycji ma następujące właściwości.

Właściwość	Typ	Opis
type	integer	Typ opcji wstępnego przetwarzania. Możliwe wartości: 1 - Mnożnik niestandardowy; 2 - Przytnij z prawej; 3 - Przytnij z lewej; 4 - Przytnij; 5 - Wyrażenie regularne; 6 - Wartość logiczna na dziesiętną; 7 - Ósemkowa na dziesiętną; 8 - Szesnastkowa na dziesiętną; 9 - Prosta zmiana; 10 - Zmiana na sekundę; 11 - XML XPath; 12 - JSONPath; 13 - W zakresie; 14 - Pasuje do wyrażenia regularnego; 15 - Nie pasuje do wyrażenia regularnego; 16 - Sprawdź błąd w JSON; 17 - Sprawdź błąd w XML; 18 - Sprawdź błąd przy użyciu wyrażenia regularnego; 19 - Odrzuć niezmienione; 20 - Odrzuć niezmienione z heartbeat; 21 - JavaScript; 22 - Wzorzec Prometheus; 23 - Prometheus do JSON; 24 - CSV do JSON; 25 - Zamień; 26 - Sprawdź nieobsługiwane; 27 - XML do JSON; 28 - Wartość SNMP walk; 29 - SNMP walk do JSON; 30 - Wartość SNMP get. Zachowanie właściwości: - *wymagane*

Właściwość	Typ	Opis
params	string	Dodatkowe parametry używane przez opcję wstępnego przetwarzania. Wiele parametrów jest rozdzielanych znakiem nowej linii (\n). Jeśli `type` jest ustawione na ”Check unsupported”, parametry mają składnię `<scope>[\n<pattern>]`, gdzie *pattern* jest wyrażeniem regularnym, a *scope* jest jednym z: -1 - dopasuj dowolny błąd; 0 - sprawdź, czy komunikat błędu pasuje do *pattern*; 1 - sprawdź, czy komunikat błędu nie pasuje do *pattern*. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”Custom multiplier” (1), ”Right trim” (2), ”Left trim” (3), ”Trim” (4), ”Regular expression” (5), ”XML XPath” (11), ”JSONPath” (12), ”In range” (13), ”Matches regular expression” (14), ”Does not match regular expression” (15), ”Check for error in JSON” (16), ”Check for error in XML” (17), ”Check for error using regular expression” (18), ”Discard unchanged with heartbeat” (20), ”JavaScript” (21), ”Prometheus pattern” (22), ”Prometheus to JSON” (23), ”CSV to JSON” (24), ”Replace” (25), ”Check unsupported” (26), ”SNMP walk value” (28), ”SNMP walk to JSON” (29) lub ”SNMP get value” (30)
error_handler	integer	Typ działania używanego w przypadku niepowodzenia kroku wstępnego przetwarzania. Możliwe wartości: 0 - Komunikat błędu jest ustawiany przez Zabbix server; 1 - Odrzuć wartość; 2 - Ustaw wartość niestandardową; 3 - Ustaw niestandardowy komunikat błędu. Możliwe wartości, jeśli `type` jest ustawione na ”Check unsupported”: 1 - Odrzuć wartość; 2 - Ustaw wartość niestandardową; 3 - Ustaw niestandardowy komunikat błędu. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”Custom multiplier” (1), ”Regular expression” (5), ”Boolean to decimal” (6), ”Octal to decimal” (7), ”Hexadecimal to decimal” (8), ”Simple change” (9), ”Change per second” (10), ”XML XPath” (11), ”JSONPath” (12), ”In range” (13), ”Matches regular expression” (14), ”Does not match regular expression” (15), ”Check for error in JSON” (16), ”Check for error in XML” (17), ”Check for error using regular expression” (18), ”Prometheus pattern” (22), ”Prometheus to JSON” (23), ”CSV to JSON” (24), ”Check unsupported” (26), ”XML to JSON” (27), ”SNMP walk value” (28), ”SNMP walk to JSON” (29) lub ”SNMP get value” (30)
error_handler_params	string	Parametry obsługi błędów. Zachowanie właściwości: - *wymagane*, jeśli `error_handler` jest ustawione na ”Set custom value” lub ”Set custom error message”

Dla każdego typu wstępnego przetwarzania obsługiwane są następujące parametry i procedury obsługi błędów.

Typ wstępnego przetwarzania	Nazwa	Parametr 1	Parametr 2	Parametr 3	Obsługiwane procedury obsługi błędów
1	Mnożnik niestandardowy	number[1, 6]			0, 1, 2, 3
2	Przytnij z prawej	lista znaków[2]			
3	Przytnij z lewej	lista znaków[2]			
4	Przytnij	lista znaków[2]			
5	Wyrażenie regularne	pattern[3]	output[2]		0, 1, 2, 3
6	Wartość logiczna na dziesiętną				0, 1, 2, 3
7	Ósemkowa na dziesiętną				0, 1, 2, 3
8	Szesnastkowa na dziesiętną				0, 1, 2, 3
9	Prosta zmiana				0, 1, 2, 3
10	Zmiana na sekundę				0, 1, 2, 3
11	XML XPath	path[4]			0, 1, 2, 3
12	JSONPath	path[4]			0, 1, 2, 3
13	W zakresie	min[1, 6]	max[1, 6]		0, 1, 2, 3
14	Pasuje do wyrażenia regularnego	pattern[3]			0, 1, 2, 3
15	Nie pasuje do wyrażenia regularnego	pattern[3]			0, 1, 2, 3
16	Sprawdź błąd w JSON	path[4]			0, 1, 2, 3
17	Sprawdź błąd w XML	path[4]			0, 1, 2, 3

Typ wstępnego przetwarzania	Nazwa	Parametr 1	Parametr 2	Parametr 3	Obsługiwane procedury obsługi błędów
18	Sprawdź błąd przy użyciu wyrażenia regularnego	pattern[3]	output[2]		0, 1, 2, 3
19	Odrzuć niezmienione				
20	Odrzuć niezmienione z heartbeat	seconds[5, 6]			
21	JavaScript	script[2]			
22	Wzorzec Prometheus	pattern[6, 7]	`value`, `label`, `function`	output[8, 9]	0, 1, 2, 3
23	Prometheus do JSON	pattern[6, 7]			0, 1, 2, 3
24	CSV do JSON	character[2]	character[2]	0,1	0, 1, 2, 3
25	Zamień	szukany ciąg[2]	zamiennik[2]		
26	Sprawdź nieobsługiwane	scope[1]	pattern[3, 6]		1, 2, 3
27	XML do JSON				0, 1, 2, 3
28	Wartość SNMP walk	OID[2]	Format: 0 - Bez zmian 1 - UTF-8 z Hex-STRING 2 - MAC z Hex-STRING 3 - Integer z BITS		0, 1, 2, 3
29	SNMP walk do JSON[10]	Nazwa pola[2]	Prefiks OID[2]	Format: 0 - Bez zmian 1 - UTF-8 z Hex-STRING 2 - MAC z Hex-STRING 3 - Integer z BITS	0, 1, 2, 3
30	Wartość SNMP get	Format: 1 - UTF-8 z Hex-STRING 2 - MAC z Hex-STRING 3 - Integer z BITS			0, 1, 2, 3

[1] liczba całkowita lub zmiennoprzecinkowa
[2] ciąg znaków
[3] wyrażenie regularne

[4] JSONPath lub XML XPath
[5] dodatnia liczba całkowita (z obsługą sufiksów czasu, np. 30s, 1m, 2h, 1d)
[6] makro użytkownika, makro LLD
[7] Wzorzec Prometheus zgodny ze składnią: `<metric name>{<label name>="<label value>", ...} == <value>`. Każdy składnik wzorca Prometheus (metryka, nazwa etykiety, wartość etykiety i wartość metryki) może być makrem użytkownika lub makrem LLD.
[8] Dane wyjściowe Prometheus zgodne ze składnią: `<label name>` (może być makrem użytkownika lub makrem LLD), jeśli jako drugi parametr wybrano `label`.
[9] Jedna z funkcji agregujących: `sum`, `min`, `max`, `avg`, `count`, jeśli jako drugi parametr wybrano `function`.
[10] Obsługuje wiele rekordów "Nazwa pola,Prefiks OID,Format" rozdzielonych znakiem nowej linii.

itemprototype.create

Opis

`object itemprototype.create(object/array itemPrototypes)`

Ta metoda umożliwia tworzenie nowych prototypów pozycji.

> **Note:**
> Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Prototyp pozycji do utworzenia.

Oprócz standardowych właściwości prototypu pozycji, metoda akceptuje następujące parametry.

Parametr	Typ	Opis
ruleid	ID	ID reguły LLD, do której należy pozycja. Zachowanie parametru: - *wymagany*
preprocessing	array	Opcje przetwarzania wstępnego prototypu pozycji.
tags	array	Tagi prototypu pozycji.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory utworzonych prototypów pozycji we właściwości `itemids`. Kolejność zwróconych identyfikatorów odpowiada kolejności przekazanych prototypów pozycji.

Przykłady

Tworzenie prototypu pozycji

Utwórz prototyp pozycji, aby monitorować wolne miejsce na dysku w wykrytym systemie plików. Wykryte pozycje powinny być numerycznymi pozycjami agenta Zabbix, aktualizowanymi co 30 sekund.

Request:

```
{
    "jsonrpc": "2.0",
    "method": "itemprototype.create",
    "params": {
        "name": "Free disk space on {#FSNAME}",
        "key_": "vfs.fs.size[{#FSNAME},free]",
        "hostid": "10197",
        "ruleid": "27665",
        "type": 0,
        "value_type": 3,
        "interfaceid": "112",
        "delay": "30s"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "27666"
        ]
    },
    "id": 1
}
```

Tworzenie prototypu pozycji z przetwarzaniem wstępnym

Utwórz pozycję, używając zmiany na sekundę oraz niestandardowego mnożnika jako drugiego kroku.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "itemprototype.create",
    "params": {
        "name": "Incoming network traffic on {#IFNAME}",
        "key_": "net.if.in[{#IFNAME}]",
        "hostid": "10001",
        "ruleid": "27665",
        "type": 0,
        "value_type": 3,
        "delay": "60s",
        "units": "bps",
        "interfaceid": "1155",
        "preprocessing": [
            {
                "type": 10,
                "params": "",
                "error_handler": 0,
                "error_handler_params": ""
            },
            {
                "type": 1,
                "params": "8",
                "error_handler": 2,
                "error_handler_params": "10"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "44211"
        ]
    },
    "id": 1
}
```

Tworzenie prototypu zależnej pozycji

Utwórz prototyp zależnej pozycji dla prototypu pozycji nadrzędnej o ID 44211. Dozwolone są tylko zależności w obrębie tego samego hosta (szablonu/reguły wykrywania), dlatego pozycja nadrzędna i zależna pozycja powinny mieć takie samo hostid i ruleid.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "itemprototype.create",
    "params": {
      "hostid": "10001",
      "ruleid": "27665",
      "name": "Dependent test item prototype",
      "key_": "dependent.prototype",
      "type": 18,
      "master_itemid": "44211",
      "value_type": 3
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "44212"
        ]
    },
    "id": 1
}
```

Utwórz prototyp pozycji HTTP agent

Utwórz prototyp pozycji z adresem URL używającym makra użytkownika, pól zapytania i niestandardowych nagłówków.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "itemprototype.create",
    "params": {
        "type": "19",
        "hostid": "10254",
        "ruleid": "28256",
        "interfaceid": "2",
        "name": "api item prototype example",
        "key_": "api_http_item",
        "value_type": 3,
        "url": "{$URL_PROTOTYPE}",
        "query_fields": [
            {
                "name": "min",
                "value": "10"
            },
            {
                "name": "max",
                "value" "100"
            }
        ],
        "headers": [
            {
                "name": "X-Source",
                "value": "api"
            }
        ],
        "delay": "35"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "28305"
        ]
    },
    "id": 1
}
```

Utwórz prototyp pozycji skryptowej

Utwórz proste zbieranie danych przy użyciu prototypu pozycji skryptowej.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "itemprototype.create",
    "params": {
        "name": "Script example",
        "key_": "custom.script.itemprototype",
        "hostid": "12345",
        "type": 21,
        "value_type": 4,
        "params": "var request = new HttpRequest();\nreturn request.post(\"https://postman-echo.com/post\"
        "parameters": [
            {
                "name": "host",
                "value": "{HOST.CONN}"
            }
        ],
        "timeout": "6s",
        "delay": "30s"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "23865"
        ]
    },
    "id": 1
}
```

Źródło

CItemPrototype::create() w *ui/include/classes/api/services/CItemPrototype.php*.

itemprototype.delete

Opis

`object itemprototype.delete(array itemPrototypeIds)`

Ta metoda pozwala na usuwanie prototypów pozycji.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania metody można odwołać w ustawieniach roli użytkownika. Więcej informacji można znaleźć w Role użytkownika.

Parametry

`(array)` ID prototypów pozycji do usunięcia.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory usuniętych prototypów pozycji we właściwości `prototypeids`.

Przykłady

Usuwanie wielu prototypów elementów

Usuń dwa prototypy pozycji.
Zależne prototypy pozycji są usuwane automatycznie, jeśli element główny lub prototyp pozycji zostanie usunięty.

Żądanie:

```
{
"jsonrpc": "2.0",
"method": "itemprototype.delete",
"params": [
"27352",
"27356"
],
"id": 1
}
```

Odpowiedź:

```
{
"jsonrpc": "2.0",
"result": {
"prototypeids": [
"27352",
"27356"
]
},
"id": 1
}
```

Źródło

CItemPrototype::delete() w *ui/include/classes/api/services/CItemPrototype.php*.

itemprototype.get

Opis

`integer/array itemprototype.get(object parameters)`

Ta metoda umożliwia pobieranie prototypów pozycji zgodnie z podanymi parametrami.

Note:
Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji znajduje się w sekcji User roles.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
discoveryids	ID/array	Zwracaj tylko prototypy pozycji należące do podanych reguł LLD.
graphids	ID/array	Zwracaj tylko prototypy pozycji używane w podanych prototypach wykresów.
hostids	ID/array	Zwracaj tylko prototypy pozycji należące do podanych hostów.
inherited	boolean	Jeśli ustawiono na `true`, zwracaj tylko prototypy pozycji odziedziczone z szablonu.

Parametr	Typ	Opis
itemids	ID/array	Zwracaj tylko prototypy pozycji o podanych ID.
monitored	boolean	Jeśli ustawiono na `true`, zwracaj tylko włączone prototypy pozycji należące do monitorowanych hostów.
templated	boolean	Jeśli ustawiono na `true`, zwracaj tylko prototypy pozycji należące do szablonów.
templateids	ID/array	Zwracaj tylko prototypy pozycji należące do podanych szablonów.
triggerids	ID/array	Zwracaj tylko prototypy pozycji używane w podanych prototypach wyzwalaczy.
selectDiscoveryData	query	Zwracaj właściwość `discoveryData` z danymi obiektu wykrywania prototypu pozycji. Obiekt wykrywania prototypu pozycji łączy wykryty prototyp pozycji z prototypem pozycji, z którego został wykryty. Ma następujące właściwości: `parent_itemid` - `(string)` ID prototypu pozycji, z którego utworzono prototyp pozycji; `key_` - `(string)` klucz prototypu pozycji; `status` - `(int)` status wykrywania prototypu pozycji: 0 - *(domyślnie)* prototyp pozycji jest wykryty, 1 - prototyp pozycji nie jest już wykrywany; `ts_delete` - `(timestamp)` czas, kiedy prototyp pozycji, który nie jest już wykrywany, zostanie usunięty; `ts_disable` - `(timestamp)` czas, kiedy prototyp pozycji, który nie jest już wykrywany, zostanie wyłączony; `disable_source` - `(int)` wskaźnik określający, czy prototyp pozycji został wyłączony przez regułę LLD czy ręcznie: 0 - *(domyślnie)* wyłączony automatycznie, 1 - wyłączony przez regułę LLD.
selectDiscoveryRule	query	Zwracaj właściwość `discoveryRule` z regułą wykrywania niskiego poziomu, do której należy prototyp pozycji.
selectDiscoveryRulePrototype	query	Zwracaj właściwość `discoveryRulePrototype` z nadrzędnym prototypem reguły LLD, do którego należy prototyp pozycji.
selectGraphs	query	Zwracaj właściwość `graphs` z prototypami wykresów, w których używany jest prototyp pozycji. Obsługuje `count`.
selectHosts	query	Zwracaj właściwość `hosts` z tablicą hostów, do których należy prototyp pozycji.
selectInheritedTags	query	Zwracaj właściwość `inheritedTags` z tagami znajdującymi się na szablonie/hoście/podłączonych szablonach.
selectTags	query	Zwracaj tagi prototypu pozycji we właściwości `tags`.
selectTriggers	query	Zwracaj właściwość `triggers` z prototypami wyzwalaczy, w których używany jest prototyp pozycji. Obsługuje `count`.
selectPreprocessing	query	Zwracaj właściwość `preprocessing` z opcjami przetwarzania wstępnego prototypu pozycji.
selectValueMap	query	Zwracaj właściwość `valuemap` z mapą wartości prototypu pozycji.
filter	object	Zwracaj tylko te wyniki, które dokładnie odpowiadają podanemu filtrowi. Akceptuje obiekt, w którym klucze są nazwami właściwości, a wartościami są pojedyncza wartość lub tablica wartości do dopasowania. Nie obsługuje właściwości typu danych `text` data type. Obsługuje dodatkowe właściwości: `host` - techniczna nazwa hosta, do którego należy prototyp pozycji.

Parametr	Typ	Opis
limitSelects	integer	Ogranicza liczbę rekordów zwracanych przez subselecty. Ma zastosowanie do następujących subselectów: `selectGraphs` - wyniki będą sortowane według `name`; `selectTriggers` - wyniki będą sortowane według `description`.
sortfield	string/array	Sortuj wynik według podanych właściwości. Możliwe wartości: `itemid`, `name`, `key_`, `delay`, `type`, `status`, `history`, `trends`, `discovered`.
countOutput	boolean	Te parametry są opisane w reference commentary.
editable	boolean	
excludeSearch	boolean	
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli został użyty parametr `countOutput`.

Przykłady

Pobieranie prototypów pozycji z reguły LLD

Pobierz wszystkie prototypy pozycji dla określonego identyfikatora reguły LLD.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "itemprototype.get",
    "params": {
        "output": "extend",
        "discoveryids": "27426"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "itemid": "23077",
            "type": "0",
            "snmp_oid": "",
            "hostid": "10079",
            "name": "Incoming network traffic on en0",
            "key_": "net.if.in[en0]",
            "delay": "1m",
            "history": "1w",
            "trends": "365d",
            "status": "0",
            "value_type": "3",
            "trapper_hosts": "",
            "units": "bps",
```

```
        "formula": "",
        "logtimefmt": "",
        "templateid": "0",
        "valuemapid": "0",
        "params": "",
        "ipmi_sensor": "",
        "authtype": "0",
        "username": "",
        "password": "",
        "publickey": "",
        "privatekey": "",
        "flags": "2",
        "interfaceid": "0",
        "description": "",
        "inventory_link": "0",
        "lifetime": "7d",
        "evaltype": "0",
        "jmx_endpoint": "",
        "master_itemid": "0",
        "timeout": "",
        "url": "",
        "query_fields": [],
        "posts": "",
        "status_codes": "200",
        "follow_redirects": "1",
        "post_type": "0",
        "http_proxy": "",
        "headers": [],
        "retrieve_mode": "0",
        "request_method": "0",
        "output_format": "0",
        "ssl_cert_file": "",
        "ssl_key_file": "",
        "ssl_key_password": "",
        "verify_peer": "0",
        "verify_host": "0",
        "allow_traps": "0",
        "discover": "0",
        "uuid": "",
        "lifetime_type": "0",
        "enabled_lifetime_type": "2",
        "enabled_lifetime": "0",
        "parameters": []
    },
    {
        "itemid": "10010",
        "type": "0",
        "snmp_oid": "",
        "hostid": "10001",
        "name": "Processor load (1 min average per core)",
        "key_": "system.cpu.load[percpu,avg1]",
        "delay": "1m",
        "history": "1w",
        "trends": "365d",
        "status": "0",
        "value_type": "0",
        "trapper_hosts": "",
        "units": "",
        "formula": "",
        "logtimefmt": "",
        "templateid": "0",
        "valuemapid": "0",
```

```
            "params": "",
            "ipmi_sensor": "",
            "authtype": "0",
            "username": "",
            "password": "",
            "publickey": "",
            "privatekey": "",
            "flags": "2",
            "interfaceid": "0",
            "description": "The processor load is calculated as system CPU load divided by number of CPU c
            "inventory_link": "0",
            "lifetime": "7d",
            "evaltype": "0",
            "jmx_endpoint": "",
            "master_itemid": "0",
            "timeout": "",
            "url": "",
            "query_fields": [],
            "posts": "",
            "status_codes": "200",
            "follow_redirects": "1",
            "post_type": "0",
            "http_proxy": "",
            "headers": [],
            "retrieve_mode": "0",
            "request_method": "0",
            "output_format": "0",
            "ssl_cert_file": "",
            "ssl_key_file": "",
            "ssl_key_password": "",
            "verify_peer": "0",
            "verify_host": "0",
            "allow_traps": "0",
            "discover": "0",
            "uuid": "",
            "lifetime_type": "0",
            "enabled_lifetime_type": "2",
            "enabled_lifetime": "0",
            "parameters": []
        }
    ],
    "id": 1
}
```


Znajdowanie zależnej pozycji

Znajdź jedną zależną pozycję dla określonego ID pozycji.

Żądanie:


```
{
    "jsonrpc": "2.0",
    "method": "itemprototype.get",
    "params": {
        "output": "extend",
        "filter": {
            "type": 18,
            "master_itemid": "25545"
        },
        "limit": "1"
    },
    "id": 1
}
```


Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "itemid": "25547",
            "type": "18",
            "snmp_oid": "",
            "hostid": "10116",
            "name": "Seconds",
            "key_": "apache.status.uptime.seconds",
            "delay": "0",
            "history": "90d",
            "trends": "365d",
            "status": "0",
            "value_type": "3",
            "trapper_hosts": "",
            "units": "",
            "formula": "",
            "logtimefmt": "",
            "templateid": "0",
            "valuemapid": "0",
            "params": "",
            "ipmi_sensor": "",
            "authtype": "0",
            "username": "",
            "password": "",
            "publickey": "",
            "privatekey": "",
            "flags": "0",
            "interfaceid": "0",
            "description": "",
            "inventory_link": "0",
            "lifetime": "7d",
            "evaltype": "0",
            "jmx_endpoint": "",
            "master_itemid": "25545",
            "timeout": "",
            "url": "",
            "query_fields": [],
            "posts": "",
            "status_codes": "200",
            "follow_redirects": "1",
            "post_type": "0",
            "http_proxy": "",
            "headers": [],
            "retrieve_mode": "0",
            "request_method": "0",
            "output_format": "0",
            "ssl_cert_file": "",
            "ssl_key_file": "",
            "ssl_key_password": "",
            "verify_peer": "0",
            "verify_host": "0",
            "allow_traps": "0",
            "discover": "0",
            "uuid": "",
            "lifetime_type": "0",
            "enabled_lifetime_type": "2",
            "enabled_lifetime": "0",
            "parameters": []
        }
    ],
```

```
    "id": 1
}
```

Znajdowanie prototypu pozycji HTTP agent

Znajdź prototyp pozycji HTTP agent z metodą żądania HEAD dla określonego ID hosta.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "itemprototype.get",
    "params": {
        "hostids": "10254",
        "filter": {
            "type": 19,
            "request_method": 3
        }
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "itemid": "28257",
            "type": "19",
            "snmp_oid": "",
            "hostid": "10254",
            "name": "discovered",
            "key_": "item[{#INAME}]",
            "delay": "{#IUPDATE}",
            "history": "90d",
            "trends": "30d",
            "status": "0",
            "value_type": "3",
            "trapper_hosts": "",
            "units": "",
            "formula": "",
            "logtimefmt": "",
            "templateid": "28255",
            "valuemapid": "0",
            "params": "",
            "ipmi_sensor": "",
            "authtype": "0",
            "username": "",
            "password": "",
            "publickey": "",
            "privatekey": "",
            "flags": "2",
            "interfaceid": "2",
            "description": "",
            "inventory_link": "0",
            "lifetime": "7d",
            "evaltype": "0",
            "jmx_endpoint": "",
            "master_itemid": "0",
            "timeout": "",
            "url": "{#IURL}",
            "query_fields": [],
            "posts": "",
            "status_codes": "",
```

```
            "follow_redirects": "0",
            "post_type": "0",
            "http_proxy": "",
            "headers": [],
            "retrieve_mode": "0",
            "request_method": "3",
            "output_format": "0",
            "ssl_cert_file": "",
            "ssl_key_file": "",
            "ssl_key_password": "",
            "verify_peer": "0",
            "verify_host": "0",
            "allow_traps": "0",
            "discover": "0",
            "uuid": "",
            "lifetime_type": "0",
            "enabled_lifetime_type": "2",
            "enabled_lifetime": "0",
            "parameters": []
        }
    ],
    "id": 1
}
```


Zobacz także

- Host
- Prototyp wykresu
- Prototyp wyzwalacza

Źródło

CItemPrototype::get() w *ui/include/classes/api/services/CItemPrototype.php*.

itemprototype.update

Opis

`object itemprototype.update(object/array itemPrototypes)`

Ta metoda umożliwia aktualizację istniejących prototypów pozycji.

Note:
Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Właściwości prototypu pozycji do zaktualizowania.

Właściwość `itemid` musi być zdefiniowana dla każdego prototypu pozycji, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko przekazane właściwości, wszystkie pozostałe pozostaną bez zmian.

Oprócz standardowych właściwości prototypu pozycji, metoda akceptuje następujące parametry.

Parametr	Type	Opis
preprocessing	array	Opcje wstępnego przetwarzania prototypu pozycji, które zastąpią bieżące opcje wstępnego przetwarzania. Zachowanie parametrów: - *tylko do odczytu* dla obiektów dziedziczonych
tags	array	Tagi prototypu pozycji.

Zwracane wartości

(`object`) Zwraca obiekt zawierający identyfikatory zaktualizowanych prototypów pozycji we właściwości `itemids`.

Przykłady

Zmiana interfejsu prototypu pozycji

Zmień interfejs hosta, który będzie używany przez wykryte pozycje.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "itemprototype.update",
    "params": {
        "itemid": "27428",
        "interfaceid": "132"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "27428"
        ]
    },
    "id": 1
}
```

Aktualizacja prototypu zależnej pozycji

Zaktualizuj prototyp zależnej pozycji, podając nowe ID prototypu pozycji nadrzędnej. Dozwolone są tylko zależności w obrębie tego samego hosta (szablonu/reguły wykrywania), dlatego pozycja nadrzędna i zależna pozycja powinny mieć takie samo `hostid` i `ruleid`.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "itemprototype.update",
    "params": {
        "master_itemid": "25570",
        "itemid": "189030"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "189030"
        ]
    },
    "id": 1
}
```

Aktualizacja prototypu pozycji HTTP agent

Zmień pola zapytania i usuń wszystkie niestandardowe nagłówki.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "itemprototype.update",
```

```
    "params": {
        "itemid":"28305",
        "query_fields": [
            {
                "name": "random",
                "value": "qwertyuiopasdfghjklzxcvbnm"
            }
        ],
        "headers": []
    }
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "28305"
        ]
    },
    "id": 1
}
```

Aktualizacja opcji przetwarzania wstępnego pozycji

Zaktualizuj prototyp pozycji za pomocą reguły przetwarzania wstępnego pozycji „Mnożnik niestandardowy”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "itemprototype.update",
    "params": {
        "itemid": "44211",
        "preprocessing": [
            {
                "type": 1,
                "params": "4",
                "error_handler": 2,
                "error_handler_params": "5"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "44211"
        ]
    },
    "id": 1
}
```

Aktualizowanie prototypu pozycji skryptowej

Zaktualizuj prototyp pozycji skryptowej, używając innego skryptu, i usuń zbędne parametry, które były używane przez poprzedni skrypt.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "itemprototype.update",
    "params": {
        "itemid": "23865",
        "parameters": [],
        "script": "Zabbix.log(3, 'Log test');\nreturn 1;"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "23865"
        ]
    },
    "id": 1
}
```

Źródło

CItemPrototype::update() w *ui/include/classes/api/services/CItemPrototype.php*.

Prototyp reguły LLD

Ta klasa jest przeznaczona do pracy z prototypami reguł wykrywania niskiego poziomu.

Odwołania do obiektów:

- Prototyp reguły LLD
  - Nagłówek HTTP
  - Pole zapytania HTTP
- Filtr prototypu reguły LLD
  - Warunek filtra prototypu reguły LLD
- Ścieżka makra prototypu LLD
- Przetwarzanie wstępne prototypu reguły LLD
- Nadpisania prototypu reguły LLD
  - Filtr nadpisania prototypu reguły LLD
    - Warunek filtra nadpisania prototypu reguły LLD
  - Operacja nadpisania prototypu reguły LLD
    - Status operacji nadpisania prototypu reguły LLD
    - Wykrywanie operacji nadpisania prototypu reguły LLD
    - Okres operacji nadpisania prototypu reguły LLD
    - Historia operacji nadpisania prototypu reguły LLD
    - Trendy operacji nadpisania prototypu reguły LLD
    - Istotność operacji nadpisania prototypu reguły LLD
    - Tag operacji nadpisania prototypu reguły LLD
    - Szablon operacji nadpisania prototypu reguły LLD
    - Inwentarz operacji nadpisania prototypu reguły LLD

Dostępne metody:

- discoveryruleprototype.create - utwórz nowe prototypy reguł LLD
- discoveryruleprototype.delete - usuń prototypy reguł LLD
- discoveryruleprototype.get - pobierz prototypy reguł LLD
- discoveryruleprototype.update - zaktualizuj prototypy reguł LLD

Obiekt prototypu reguły LLD

Następujące obiekty są bezpośrednio powiązane z API `discoveryruleprototype`.

Prototyp reguły LLD

Obiekt prototypu reguły wykrywania niskiego poziomu ma następujące właściwości.

Property	Type	Description
itemid	ID	ID prototypu reguły LLD. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji
ruleid	ID	ID nadrzędnej reguły LLD/prototypu reguły LLD. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji tworzenia
delay	string	Interwał aktualizacji prototypu reguły LLD. Akceptuje sekundy lub jednostkę czasu z sufiksem (np. 30s, 1m, 2h, 1d) oraz opcjonalnie jeden lub więcej niestandardowych interwałów, oddzielonych średnikami. Niestandardowe interwały mogą być kombinacją interwałów elastycznych i harmonogramowanych. Akceptuje makra użytkownika. Jeśli są używane, wartość musi być pojedynczym makrem. Wiele makr lub makra zmieszane z tekstem nie są obsługiwane. Interwały elastyczne mogą być zapisane jako dwa makra oddzielone ukośnikiem (np. `{$FLEX_INTERVAL}/{$FLEX_PERIOD}`). Przykład: `1h;wd1-5h9-18;{$Macro1}/1-7,00:00-24:00;0/6-7,12:00-24:00;{$Macr` Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”Zabbix agent” (0), ”Simple check” (3), ”Zabbix internal” (5), ”External check” (10), ”Database monitor” (11), ”IPMI agent” (12), ”SSH agent” (13), ”TELNET agent” (14), ”JMX agent” (16), ”HTTP agent” (19), ”SNMP agent” (20), ”Script” (21), ”Browser” (22), lub jeśli `type` jest ustawione na ”Zabbix agent (active)” (7), a `key_` nie zawiera ”mqtt.get”
hostid	ID	ID hosta, do którego należy prototyp reguły LLD. Zachowanie właściwości: - *stałe* - *wymagane* dla operacji tworzenia
flags	integer	Pochodzenie prototypu reguły LLD. Możliwe wartości: 3 - prototyp reguły wykrywania niskiego poziomu; 7 - wykryty prototyp reguły wykrywania niskiego poziomu. Zachowanie właściwości: - *tylko do odczytu*
interfaceid	ID	ID interfejsu hosta prototypu reguły LLD. Zachowanie właściwości: - *wymagane*, jeśli prototyp reguły LLD należy do hosta, a `type` jest ustawione na ”Zabbix agent”, ”IPMI agent”, ”JMX agent” lub ”SNMP agent” - *obsługiwane*, jeśli prototyp reguły LLD należy do hosta, a `type` jest ustawione na ”Simple check”, ”External check”, ”SSH agent”, ”TELNET agent” lub ”HTTP agent”

Property	Type	Description
key_	string	Klucz prototypu reguły LLD. Wymagane jest co najmniej jedno makro LLD. Zachowanie właściwości: - *wymagane* dla operacji tworzenia - *tylko do odczytu* dla obiektów dziedziczonych
name	string	Nazwa prototypu reguły LLD. Zachowanie właściwości: - *wymagane* dla operacji tworzenia - *tylko do odczytu* dla obiektów dziedziczonych
type	integer	Typ prototypu reguły LLD. Możliwe wartości: 0 - Zabbix agent; 2 - Zabbix trapper; 3 - Simple check; 5 - Zabbix internal; 7 - Zabbix agent (active); 10 - External check; 11 - Database monitor; 12 - IPMI agent; 13 - SSH agent; 14 - TELNET agent; 16 - JMX agent; 18 - Dependent item; 19 - HTTP agent; 20 - SNMP agent; 21 - Script; 22 - Browser; 23 - Nested. Zachowanie właściwości: - *wymagane* dla operacji tworzenia - *tylko do odczytu* dla obiektów dziedziczonych
url	string	Ciąg URL. Obsługuje makra użytkownika, {HOST.IP}, {HOST.CONN}, {HOST.DNS}, {HOST.HOST}, {HOST.NAME}, {HOST.PORT}, {ITEM.ID}, {ITEM.KEY}. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych
allow_traps	integer	Zezwala na wypełnianie wartości podobnie jak w pozycji trapper. Możliwe wartości: 0 - *(domyślnie)* Nie zezwalaj na przyjmowanie danych przychodzących; 1 - Zezwalaj na przyjmowanie danych przychodzących. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent”

Property	Type	Description
authtype	integer	Metoda uwierzytelniania. Możliwe wartości, jeśli `type` jest ustawione na ”SSH agent”: 0 - *(domyślnie)* hasło; 1 - klucz publiczny. Możliwe wartości, jeśli `type` jest ustawione na ”HTTP agent”: 0 - *(domyślnie)* brak; 1 - basic; 2 - NTLM. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”SSH agent” lub ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych (jeśli `type` jest ustawione na ”HTTP agent”)
description	string	Opis prototypu reguły LLD.
error	string	Tekst błędu, jeśli występują problemy z aktualizacją wartości prototypu reguły LLD. Zachowanie właściwości: - *tylko do odczytu*
follow_redirects	integer	Podążaj za przekierowaniami odpowiedzi podczas odpytywania danych. Możliwe wartości: 0 - Nie podążaj za przekierowaniami; 1 - *(domyślnie)* Podążaj za przekierowaniami. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych
headers	array	Tablica nagłówków, które zostaną wysłane podczas wykonywania żądania HTTP. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych
http_proxy	string	Ciąg połączenia proxy HTTP(S). Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych
ipmi_sensor	string	Czujnik IPMI. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”IPMI agent”, a `key_` nie jest ustawione na ”ipmi.get” - *obsługiwane*, jeśli `type` jest ustawione na ”IPMI agent” - *tylko do odczytu* dla obiektów dziedziczonych
jmx_endpoint	string	Niestandardowy ciąg połączenia JMX agent. Domyślnie: service:jmx:rmi:///jndi/rmi://{HOST.CONN}:{HOST.PORT}/jmxrmi Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”JMX agent”
lifetime	string	Okres czasu, po którym pozycje, które nie są już wykrywane, zostaną usunięte. Akceptuje sekundy, jednostkę czasu z sufiksem lub makro użytkownika. Domyślnie: 7d.

Property	Type	Description
lifetime_type	integer	Scenariusz usuwania utraconych zasobów LLD. Możliwe wartości: 0 - *(domyślnie)* Usuń po osiągnięciu progu lifetime; 1 - Nie usuwaj; 2 - Usuń natychmiast.
enabled_lifetime	string	Okres czasu, po którym pozycje, które nie są już wykrywane, zostaną wyłączone. Akceptuje sekundy, jednostkę czasu z sufiksem lub makro użytkownika. Domyślnie: 0.
enabled_lifetime_type	integer	Scenariusz wyłączania utraconych zasobów LLD. Możliwe wartości: 0 - Wyłącz po osiągnięciu progu lifetime; 1 - Nie wyłączaj; 2 - *(domyślnie)* Wyłącz natychmiast.
master_itemid	ID	ID nadrzędnej pozycji. Reguła wykrywania nie może być nadrzędną pozycją dla innej reguły wykrywania. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”Dependent item” - *tylko do odczytu* dla obiektów dziedziczonych
output_format	integer	Czy odpowiedź powinna zostać przekonwertowana do JSON. Możliwe wartości: 0 - *(domyślnie)* Przechowuj surowe dane; 1 - Konwertuj do JSON. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych
params	string	Dodatkowe parametry zależne od typu prototypu reguły LLD: - wykonywany skrypt dla reguł LLD SSH i Telnet; - zapytanie SQL dla reguł LLD monitorowania bazy danych; - formuła dla obliczanych reguł LLD; - skrypt dla reguł LLD typu Script i Browser. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”Database monitor”, ”SSH agent”, ”TELNET agent”, ”Script” lub ”Browser” - *tylko do odczytu* dla obiektów dziedziczonych (jeśli `type` jest ustawione na ”Script” lub ”Browser”)
parameters	object/array	Dodatkowe parametry, jeśli `type` jest ustawione na ”Script” lub ”Browser”. Tablica obiektów z właściwościami `name` i `value`, gdzie `name` musi być unikalne. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”Script” lub ”Browser” - *tylko do odczytu* dla obiektów dziedziczonych
password	string	Hasło do uwierzytelniania. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”JMX agent”, a `username` jest ustawione - *obsługiwane*, jeśli `type` jest ustawione na ”Simple check”, ”Database monitor”, ”SSH agent”, ”TELNET agent” lub ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych (jeśli `type` jest ustawione na ”HTTP agent”)

Property	Type	Description
post_type	integer	Typ treści danych POST przechowywanej we właściwości `posts`. Możliwe wartości: 0 - *(domyślnie)* Surowe dane; 2 - Dane JSON; 3 - Dane XML. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych
posts	string	Dane treści żądania HTTP(S). Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”HTTP agent”, a `post_type` jest ustawione na ”JSON data” lub ”XML data” - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent”, a `post_type` jest ustawione na ”Raw data” - *tylko do odczytu* dla obiektów dziedziczonych
privatekey	string	Nazwa pliku klucza prywatnego. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”SSH agent”, a `authtype` jest ustawione na ”public key”
publickey	string	Nazwa pliku klucza publicznego. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”SSH agent”, a `authtype` jest ustawione na ”public key”
query_fields	array	Tablica pól zapytania, które zostaną wysłane podczas wykonywania żądania HTTP. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych
request_method	integer	Typ metody żądania. Możliwe wartości: 0 - *(domyślnie)* GET; 1 - POST; 2 - PUT; 3 - HEAD. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych
retrieve_mode	integer	Która część odpowiedzi powinna zostać zapisana. Możliwe wartości, jeśli `request_method` jest ustawione na ”GET”, ”POST” lub ”PUT”: 0 - *(domyślnie)* Treść; 1 - Nagłówki; 2 - Zostaną zapisane zarówno treść, jak i nagłówki. Możliwe wartości, jeśli `request_method` jest ustawione na ”HEAD”: 1 - Nagłówki. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych

Property	Type	Description
snmp_oid	string	OID SNMP. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”SNMP agent” - *tylko do odczytu* dla obiektów dziedziczonych
ssl_cert_file	string	Ścieżka do pliku publicznego klucza SSL. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych
ssl_key_file	string	Ścieżka do pliku prywatnego klucza SSL. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych
ssl_key_password	string	Hasło do pliku klucza SSL. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych
state	integer	Stan prototypu reguły LLD. Możliwe wartości: 0 - *(domyślnie)* normalny; 1 - nieobsługiwany. Zachowanie właściwości: - *tylko do odczytu*
status	integer	Status prototypu reguły LLD. Możliwe wartości: 0 - *(domyślnie)* włączony prototyp reguły LLD; 1 - wyłączony prototyp reguły LLD.
status_codes	string	Zakresy wymaganych kodów statusu HTTP, oddzielone przecinkami. Obsługuje również makra użytkownika jako część listy oddzielonej przecinkami. Przykład: 200,200-{$M},{$M},200-400 Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych
templateid	ID	ID nadrzędnego prototypu reguły LLD szablonu. Zachowanie właściwości: - *tylko do odczytu*
timeout	string	Limit czasu żądania odpytywania danych pozycji. Akceptuje sekundy lub jednostkę czasu z sufiksem (np. 30s, 1m). Akceptuje również makra użytkownika. Możliwy zakres wartości: 1-600s. Domyślnie: ”” - użyj ustawień proxy/globalnych. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”Zabbix agent” (0), ”Simple check” (3) i `key_` nie zaczyna się od ”`vmware.`” ani ”`icmpping`”, ”Zabbix agent (active)” (7), ”External check” (10), ”Database monitor” (11), ”SSH agent” (13), ”TELNET agent” (14), ”HTTP agent” (19), ”SNMP agent” (20), a `snmp_oid` zaczyna się od ”`walk[`” lub ”`get[`”, ”Script” (21), ”Browser” (22) - *tylko do odczytu* dla obiektów dziedziczonych

Property	Type	Description
trapper_hosts	string	Dozwolone hosty. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”Zabbix trapper”, lub jeśli `type` jest ustawione na ”HTTP agent”, a `allow_traps` jest ustawione na ”Allow to accept incoming data”
username	string	Nazwa użytkownika do uwierzytelniania. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”SSH agent”, ”TELNET agent”, lub jeśli `type` jest ustawione na ”JMX agent”, a `password` jest ustawione - *obsługiwane*, jeśli `type` jest ustawione na ”Simple check”, ”Database monitor” lub ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych (jeśli `type` jest ustawione na ”HTTP agent”)
uuid	string	Uniwersalny unikalny identyfikator, używany do łączenia importowanych prototypów reguł LLD z już istniejącymi. Generowany automatycznie, jeśli nie został podany. Zachowanie właściwości: - *obsługiwane*, jeśli prototyp reguły LLD należy do szablonu
verify_host	integer	Czy weryfikować, że nazwa hosta dla połączenia odpowiada nazwie w certyfikacie hosta. Możliwe wartości: 0 - *(domyślnie)* Nie weryfikuj; 1 - Weryfikuj. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych
verify_peer	integer	Czy weryfikować, że certyfikat hosta jest autentyczny. Możliwe wartości: 0 - *(domyślnie)* Nie weryfikuj; 1 - Weryfikuj. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych

Nagłówek HTTP

Obiekt nagłówka ma następujące właściwości:

Właściwość	Typ	Opis
name	string	Nazwa nagłówka HTTP. Zachowanie właściwości: - *wymagane*
value	string	Wartość nagłówka. Zachowanie właściwości: - *wymagane*

Pole zapytania HTTP

Obiekt pola zapytania definiuje nazwę i wartość używane do określenia parametru URL. Ma następujące właściwości:

Właściwość	Typ	Opis
name	string	Nazwa parametru. Zachowanie właściwości: - *wymagane*
value	string	Wartość parametru. Zachowanie właściwości: - *wymagane*

Filtr prototypu reguły LLD

Obiekt filtra prototypu reguły LLD definiuje zestaw warunków, które mogą być używane do filtrowania wykrytych obiektów. Ma następujące właściwości:

Właściwość	Type	Opis
conditions	object/array	Zestaw warunków filtra używanych do filtrowania wyników. Warunki zostaną posortowane zgodnie z kolejnością ich występowania w formule. Zachowanie właściwości: - *wymagane*
evaltype	integer	Metoda oceny warunków filtra. Możliwe wartości: 0 - And/Or; 1 - And; 2 - Or; 3 - Wyrażenie niestandardowe. Zachowanie właściwości: - *wymagane*
eval_formula	string	Wygenerowane wyrażenie, które będzie używane do oceny warunków filtra. Wyrażenie zawiera identyfikatory odwołujące się do określonych warunków filtra przez ich `formulaid`. Wartość `eval_formula` jest równa wartości `formula` dla filtrów z wyrażeniem niestandardowym. Zachowanie właściwości: - *tylko do odczytu*
formula	string	Wyrażenie zdefiniowane przez użytkownika, używane do oceny warunków filtrów z wyrażeniem niestandardowym. Wyrażenie musi zawierać identyfikatory odwołujące się do określonych warunków filtra przez ich `formulaid`. Identyfikatory użyte w wyrażeniu muszą dokładnie odpowiadać tym zdefiniowanym w warunkach filtra: żaden warunek nie może pozostać nieużyty ani pominięty. Zachowanie właściwości: - *wymagane*, jeśli `evaltype` jest ustawione na „wyrażenie niestandardowe”

Warunek filtra prototypu reguły LLD

Obiekt warunku filtra prototypu reguły LLD definiuje oddzielne sprawdzenie wykonywane na wartości makra LLD. Ma następujące właściwości:

Właściwość	Type	Opis
macro	string	Makro LLD, na którym ma zostać wykonane sprawdzenie. Zachowanie właściwości: - *wymagane*
value	string	Wartość do porównania. Zachowanie właściwości: - *wymagane*, jeśli `operator` jest ustawiony na „matches regular expression” lub „does not match regular expression”
formulaid	string	Dowolny unikalny identyfikator używany do odwoływania się do warunku z niestandardowego wyrażenia. Może zawierać wyłącznie wielkie litery. Identyfikator musi zostać zdefiniowany przez użytkownika podczas modyfikowania warunków filtra, ale zostanie wygenerowany ponownie przy późniejszym żądaniu tych warunków. Zachowanie właściwości: - *wymagane*, jeśli `evaltype` obiektu filtra prototypu reguły LLD jest ustawiony na „custom expression”
operator	integer	Operator warunku. Możliwe wartości: 8 - *(domyślnie)* pasuje do wyrażenia regularnego; 9 - nie pasuje do wyrażenia regularnego; 12 - istnieje; 13 - nie istnieje.

Note:
Aby lepiej zrozumieć, jak używać filtrów z różnymi typami wyrażeń, zobacz przykłady na stronach metod discoveryruleprototype.get oraz discoveryruleprototype.create.

Ścieżka makra LLD

Ścieżka makra LLD ma następujące właściwości:

Właściwość	Type	Opis
lld_macro	string	Makro LLD. Zachowanie właściwości: - *wymagane*
path	string	Selektor wartości, która zostanie przypisana do odpowiadającego jej makra. Zachowanie właściwości: - *wymagane*

Wstępne przetwarzanie prototypu reguły LLD

Obiekt wstępnego przetwarzania prototypu reguły LLD ma następujące właściwości.

Właściwość	Type	Opis
type	integer	Typ opcji wstępnego przetwarzania. Możliwe wartości: 5 - Wyrażenie regularne; 11 - XML XPath; 12 - JSONPath; 14 - Pasuje do wyrażenia regularnego; 15 - Nie pasuje do wyrażenia regularnego; 16 - Sprawdź błąd w JSON; 17 - Sprawdź błąd w XML; 20 - Odrzuć niezmienione z heartbeat; 21 - JavaScript; 23 - Prometheus do JSON; 24 - CSV do JSON; 25 - Zamień; 27 - XML do JSON; 28 - Wartość SNMP walk; 29 - SNMP walk do JSON; 30 - Wartość SNMP get. Zachowanie właściwości: - *wymagane*
params	string	Dodatkowe parametry używane przez opcję wstępnego przetwarzania. Wiele parametrów jest rozdzielanych znakiem nowej linii (\n). Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na „Wyrażenie regularne” (5), „XML XPath” (11), „JSONPath” (12), „Pasuje do wyrażenia regularnego” (14), „Nie pasuje do wyrażenia regularnego” (15), „Sprawdź błąd w JSON” (16), „Sprawdź błąd w XML” (17), „Odrzuć niezmienione z heartbeat” (20), „JavaScript” (21), „Prometheus do JSON” (23), „CSV do JSON” (24), „Zamień” (25), „Wartość SNMP walk” (28), „SNMP walk do JSON” (29) lub „Wartość SNMP get” (30)
error_handler	integer	Typ działania używanego w przypadku niepowodzenia kroku wstępnego przetwarzania. Możliwe wartości: 0 - Komunikat o błędzie jest ustawiany przez Zabbix server; 1 - Odrzuć wartość; 2 - Ustaw własną wartość; 3 - Ustaw własny komunikat o błędzie. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na „Wyrażenie regularne” (5), „XML XPath” (11), „JSONPath” (12), „Pasuje do wyrażenia regularnego” (14), „Nie pasuje do wyrażenia regularnego” (15), „Sprawdź błąd w JSON” (16), „Sprawdź błąd w XML” (17), „Prometheus do JSON” (23), „CSV do JSON” (24), „XML do JSON” (27), „Wartość SNMP walk” (28), „SNMP walk do JSON” (29) lub „Wartość SNMP get” (30)
error_handler_params	string	Parametry obsługi błędów. Zachowanie właściwości: - *wymagane*, jeśli `error_handler` jest ustawione na „Ustaw własną wartość” lub „Ustaw własny komunikat o błędzie”

Dla każdego typu wstępnego przetwarzania obsługiwane są następujące parametry i procedury obsługi błędów.

Typ wstępnego przetwarzania	Nazwa	Parametr 1	Parametr 2	Parametr 3	Obsługiwane procedury obsługi błędów
5	Wyrażenie regularne	wzorzec[1]	wynik[2]		0, 1, 2, 3
11	XML XPath	ścieżka[3]			0, 1, 2, 3
12	JSONPath	ścieżka[3]			0, 1, 2, 3
14	Pasuje do wyrażenia regularnego	wzorzec[1]			0, 1, 2, 3
15	Nie pasuje do wyrażenia regularnego	wzorzec[1]			0, 1, 2, 3
16	Sprawdź błąd w JSON	ścieżka[3]			0, 1, 2, 3
17	Sprawdź błąd w XML	ścieżka[3]			0, 1, 2, 3
20	Odrzuć niezmienione z heartbeat	sekundy[4, 5]			
21	JavaScript	skrypt[2]			
23	Prometheus do JSON	wzorzec[5, 6]			0, 1, 2, 3
24	CSV do JSON	znak[2]	znak[2]	0,1	0, 1, 2, 3
25	Zamień	szukany ciąg[2]	zamiennik[2]		
27	XML do JSON				0, 1, 2, 3
28	Wartość SNMP walk	OID[2]	Format: 0 - Bez zmian 1 - UTF-8 z Hex-STRING 2 - MAC z Hex-STRING 3 - Integer z BITS		0, 1, 2, 3
29	SNMP walk do JSON[7]	Nazwa pola[2]	Prefiks OID[2]	Format: 0 - Bez zmian 1 - UTF-8 z Hex-STRING 2 - MAC z Hex-STRING 3 - Integer z BITS	0, 1, 2, 3

Typ wstępnego przetwarzania	Nazwa	Parametr 1	Parametr 2	Parametr 3	Obsługiwane procedury obsługi błędów
30	Wartość SNMP get	Format: 1 - UTF-8 z Hex-STRING 2 - MAC z Hex-STRING 3 - Integer z BITS			0, 1, 2, 3

[1] wyrażenie regularne
[2] ciąg znaków
[3] JSONPath lub XML XPath
[4] dodatnia liczba całkowita (z obsługą sufiksów czasu, np. 30s, 1m, 2h, 1d)
[5] makro użytkownika
[6] Wzorzec Prometheus zgodny ze składnią: `<metric name>{<label name>="<label value>", ...} == <value>`. Każdy komponent wzorca Prometheus (metryka, nazwa etykiety, wartość etykiety i wartość metryki) może być makrem użytkownika.
[7] Obsługuje wiele rekordów „Nazwa pola,Prefiks OID,Format”, rozdzielonych znakiem nowej linii.

Nadpisania prototypów reguł LLD

Obiekt nadpisań prototypów reguł LLD definiuje zestaw reguł (filtrów, warunków i operacji), które są używane do nadpisywania właściwości różnych obiektów prototypów. Ma następujące właściwości:

Właściwość	Typ	Opis
name	string	Unikalna nazwa nadpisania. Zachowanie właściwości: - *wymagane*
step	integer	Unikalny numer porządkowy nadpisania. Zachowanie właściwości: - *wymagane*
stop	integer	Zatrzymaj przetwarzanie kolejnych nadpisań, jeśli wystąpi dopasowanie. Możliwe wartości: 0 - *(domyślnie)* nie zatrzymuj przetwarzania nadpisań; 1 - zatrzymaj przetwarzanie nadpisań, jeśli filtr pasuje.
filter	object	Filtr nadpisania.
operations	object/array	Operacje nadpisania.

Filtr nadpisania prototypu reguły LLD

Obiekt filtra nadpisania prototypu reguły LLD definiuje zestaw warunków, które po dopasowaniu do wykrytego obiektu powodują zastosowanie nadpisania. Ma on następujące właściwości:

Property	Type	Description
conditions	object/array	Zestaw warunków filtra nadpisania używanych do dopasowywania wykrytych obiektów. Warunki zostaną posortowane zgodnie z kolejnością ich umieszczenia w formule. Property behavior: - *required*

Property	Type	Description
evaltype	integer	Metoda oceny warunku filtra nadpisania. Możliwe wartości: 0 - And/Or; 1 - And; 2 - Or; 3 - Wyrażenie niestandardowe. Property behavior: - *required*
eval_formula	string	Wygenerowane wyrażenie, które będzie używane do oceny warunków filtra nadpisania. Wyrażenie zawiera identyfikatory odwołujące się do konkretnych warunków filtra nadpisania za pomocą ich `formulaid`. Wartość `eval_formula` jest równa wartości `formula` dla filtrów z wyrażeniem niestandardowym. Property behavior: - *read-only*
formula	string	Wyrażenie zdefiniowane przez użytkownika, używane do oceny warunków filtrów nadpisania z wyrażeniem niestandardowym. Wyrażenie musi zawierać identyfikatory odwołujące się do konkretnych warunków filtra nadpisania za pomocą ich `formulaid`. Identyfikatory użyte w wyrażeniu muszą dokładnie odpowiadać tym zdefiniowanym w warunkach filtra nadpisania: żaden warunek nie może pozostać nieużyty ani pominięty. Property behavior: - *required* jeśli `evaltype` jest ustawione na ”custom expression”

Warunek filtra nadpisania prototypu reguły LLD

Obiekt warunku filtra nadpisania prototypu reguły LLD definiuje osobne sprawdzenie wykonywane na wartości makra LLD. Ma następujące właściwości:

Właściwość	Type	Opis
macro	string	Makro LLD, na którym ma zostać wykonane sprawdzenie. Property behavior: - *wymagane*
value	string	Wartość do porównania. Property behavior: - *wymagane*, jeśli `operator` jest ustawiony na „matches regular expression” lub „does not match regular expression”
formulaid	string	Dowolny unikalny identyfikator używany do odwoływania się do warunku z niestandardowego wyrażenia. Może zawierać wyłącznie wielkie litery. Identyfikator musi zostać zdefiniowany przez użytkownika podczas modyfikowania warunków filtra, ale zostanie wygenerowany ponownie przy późniejszym żądaniu tych warunków. Property behavior: - *wymagane*, jeśli `evaltype` obiektu LLD rule prototype override filter object jest ustawione na „custom expression”
operator	integer	Operator warunku. Możliwe wartości: 8 - *(domyślnie)* matches regular expression; 9 - does not match regular expression; 12 - exists; 13 - does not exist.

Operacja nadpisania prototypu reguły LLD

Operacja nadpisania prototypu reguły LLD jest połączeniem warunków i działań wykonywanych na obiekcie prototypu. Ma następujące właściwości:

Właściwość	Type	Opis
operationobject	integer	Typ wykrytego obiektu, dla którego ma zostać wykonane działanie. Możliwe wartości: 0 - Prototyp pozycji; 1 - Prototyp wyzwalacza; 2 - Prototyp wykresu; 3 - Prototyp hosta. Zachowanie właściwości: - *wymagane*
operator	integer	Warunek nadpisania operator. Możliwe wartości: 0 - *(domyślnie)* równa się; 1 - nie równa się; 2 - zawiera; 3 - nie zawiera; 8 - pasuje; 9 - nie pasuje.
value	string	Wzorzec do dopasowania do nazwy prototypu pozycji, wyzwalacza, wykresu lub hosta, zależnie od wybranego obiektu.
opstatus	object	Obiekt statusu operacji nadpisania dla obiektów prototypu pozycji, wyzwalacza i hosta.
opdiscover	object	Obiekt statusu wykrywania operacji nadpisania (wszystkie typy obiektów).
opperiod	object	Obiekt okresu operacji nadpisania (interwału aktualizacji) dla obiektu prototypu pozycji.
ophistory	object	Obiekt historii operacji nadpisania dla obiektu prototypu pozycji.
optrends	object	Obiekt trendów operacji nadpisania dla obiektu prototypu pozycji.
opseverity	object	Obiekt ważności operacji nadpisania dla obiektu prototypu wyzwalacza.
optag	object/array	Obiekt tagu operacji nadpisania dla obiektów prototypu wyzwalacza i hosta.
optemplate	object/array	Obiekt szablonu operacji nadpisania dla obiektu prototypu hosta.
opinventory	object	Obiekt inwentaryzacji operacji nadpisania dla obiektu prototypu hosta.

Status operacji nadpisania prototypu reguły LLD

Status operacji nadpisania prototypu reguły LLD ustawiany dla wykrytego obiektu. Ma następujące właściwości:

Właściwość	Typ	Opis
status	integer	Nadpisuje status dla wybranego obiektu. Możliwe wartości: 0 - Utwórz jako włączone; 1 - Utwórz jako wyłączone. Zachowanie właściwości: - *wymagane*

Operacja discover nadpisania prototypu reguły LLD

Status discover operacji nadpisania prototypu reguły LLD jest ustawiany dla wykrytego obiektu. Ma następujące właściwości:

Właściwość	Typ	Opis
discover	integer	Nadpisuje status discover dla wybranego obiektu. Możliwe wartości: 0 - Tak, kontynuuj wykrywanie obiektów; 1 - Nie, nowe obiekty nie będą wykrywane, a istniejące zostaną oznaczone jako utracone. Zachowanie właściwości: - *wymagane*

Okres operacji nadpisania prototypu reguły LLD

Okres operacji nadpisania prototypu reguły LLD jest wartością interwału aktualizacji ustawianą dla wykrytej pozycji. Ma następujące właściwości:

Właściwość	Type	Opis
delay	string	Nadpisuje interwał aktualizacji prototypu pozycji. Akceptuje sekundy lub jednostkę czasu z sufiksem (np. 30s, 1m, 2h, 1d) oraz opcjonalnie jeden lub więcej interwałów niestandardowych, wszystkie rozdzielone średnikami. Interwały niestandardowe mogą stanowić mieszankę interwałów elastycznych i harmonogramowanych. Akceptuje makra użytkownika lub makra LLD. Jeśli są używane, wartość musi być pojedynczym makrem. Wiele makr lub makra zmieszane z tekstem nie są obsługiwane. Interwały elastyczne mogą być zapisane jako dwa makra rozdzielone ukośnikiem (np. `{$FLEX_INTERVAL}/{$FLEX_PERIOD}`). Przykład: `1h;wd1-5h9-18;{$Macro1}/1-7,00:00-24:00;0/6-7,12:00-24:00;{$Macr` Zachowanie właściwości: - *required*

Historia operacji nadpisania prototypu reguły LLD

Wartość historii operacji nadpisania prototypu reguły LLD, która jest ustawiana dla wykrytej pozycji. Ma następujące właściwości:

Właściwość	Type	Opis
history	string	Nadpisuje historię prototypu pozycji, czyli jednostkę czasu określającą, jak długo dane historii powinny być przechowywane. Akceptuje również makro użytkownika i makro LLD. Zachowanie właściwości: - *wymagane*

Trendy operacji nadpisania prototypu reguły LLD

Wartość trendów operacji nadpisania prototypu reguły LLD, która jest ustawiana dla wykrytej pozycji. Ma następujące właściwości:

Właściwość	Type	Opis
trends	string	Nadpisuje trendy prototypu pozycji, czyli jednostkę czasu określającą, jak długo dane trendów powinny być przechowywane. Akceptuje również makro użytkownika i makro LLD. Zachowanie właściwości: - *wymagane*

Ważność operacji nadpisania prototypu reguły LLD

Wartość ważności operacji nadpisania prototypu reguły LLD, która jest ustawiana dla wykrytego wyzwalacza. Ma następujące właściwości:

Właściwość	Type	Opis
severity	integer	Nadpisuje ważność prototypu wyzwalacza. Możliwe wartości: 0 - *(domyślnie)* niesklasyfikowany; 1 - informacja; 2 - ostrzeżenie; 3 - średni; 4 - wysoki; 5 - katastrofa. Zachowanie właściwości: - *wymagane*

Znacznik operacji nadpisania prototypu reguły LLD

Obiekt znacznika operacji nadpisania prototypu reguły LLD zawiera nazwę i wartość znacznika, które są ustawiane dla wykrytego obiektu. Ma następujące właściwości:

Właściwość	Type	Opis
tag	string	Nowa nazwa znacznika. Zachowanie właściwości: - *wymagane*
value	string	Nowa wartość znacznika.

Szablon operacji nadpisania prototypu reguły LLD

Obiekt szablonu operacji nadpisania prototypu reguły LLD, który jest połączony z wykrytym hostem. Ma następujące właściwości:

Właściwość	Type	Opis
templateid	ID	Nadpisuje szablon szablonów połączonych z prototypem hosta. Zachowanie właściwości: - *wymagane*

Wartość trybu inwentaryzacji operacji nadpisania prototypu reguły LLD

Wartość trybu inwentaryzacji operacji nadpisania prototypu reguły LLD, która jest ustawiana dla wykrytego hosta. Ma następujące właściwości:

Właściwość	Type	Opis
inventory_mode	integer	Nadpisuje tryb inwentaryzacji prototypu hosta. Możliwe wartości: -1 - wyłączone; 0 - *(domyślnie)* ręczne; 1 - automatyczne. Zachowanie właściwości: - *wymagane*

discoveryruleprototype.create

Opis

`object discoveryruleprototype.create(object/array lldRules)`

Ta metoda umożliwia tworzenie nowych prototypów reguł LLD.

> **Note:**
> Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Prototypy reguł LLD do utworzenia.

Oprócz standardowych właściwości prototypu reguły LLD, metoda akceptuje następujące parametry.

Parametr	Typ	Opis
filter	object	Filtr prototypu reguły LLD dla reguły LLD.
preprocessing	object/array	Opcje przetwarzania wstępnego prototypu reguły LLD.
lld_macro_paths	object/array	Opcje lld_macro_path prototypu reguły LLD.
overrides	object/array	Opcje nadpisań prototypu reguły LLD.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory utworzonych prototypów reguł LLD we właściwości `itemids`. Kolejność zwróconych identyfikatorów odpowiada kolejności przekazanych prototypów reguł LLD.

Przykłady

Tworzenie prototypu reguły LLD

Utwórz prototyp reguły LLD (Typ: Zagnieżdżony), aby wykrywać tablespace'y w instancji bazy danych.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "discoveryruleprototype.create",
    "params": {
        "name": "Discover tablespaces for {#DB}",
        "key_": "db.tablespace.discovery[{#DB}]",
        "hostid": "10084",
        "ruleid": "47251",
        "type": 23
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "47252"
        ]
    },
    "id": 1
}
```

Zobacz także

- Filtr prototypu reguły LLD
- Ścieżki makr LLD
- Wstępne przetwarzanie prototypu reguły LLD

Źródło

CDiscoveryRulePrototype::create() w *ui/include/classes/api/services/CDiscoveryRulePrototype.php*.

discoveryruleprototype.delete

Opis

`object discoveryruleprototype.delete(array lldRuleIds)`

Ta metoda umożliwia usuwanie prototypów reguł LLD.

> **Note:**
> Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji User roles.

Parametry

`(array)` ID prototypów reguł LLD do usunięcia.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory usuniętych prototypów reguł LLD we właściwości `ruleids`.

Przykłady

Usuwanie wielu prototypów reguł LLD

Usuń dwa prototypy reguł LLD.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "discoveryruleprototype.delete",
    "params": [
        "47252",
        "47253"
    ],
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "ruleids": [
            "47252",
            "47253"
        ]
    },
    "id": 1
}
```

Źródło

CDiscoveryRulePrototype::delete() w *ui/include/classes/api/services/CDiscoveryRulePrototype.php*.

discoveryruleprototype.get

Opis

`integer/array discoveryruleprototype.get(object parameters)`

Ta metoda umożliwia pobranie prototypów reguł LLD zgodnie z podanymi parametrami.

Note:
Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w Rolach użytkowników.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
discoveryids	ID/array	Zwracaj tylko prototypy reguł LLD należące do podanych reguł LLD lub prototypów reguł LLD.
itemids	ID/array	Zwracaj tylko prototypy reguł LLD o podanych identyfikatorach.
groupids	ID/array	Zwracaj tylko prototypy reguł LLD należące do hostów z podanych grup.
hostids	ID/array	Zwracaj tylko prototypy reguł LLD należące do podanych hostów.
inherited	boolean	Jeśli ustawiono `true`, zwracaj tylko prototypy reguł LLD odziedziczone z szablonu.
interfaceids	ID/array	Zwracaj tylko prototypy reguł LLD używające podanych interfejsów hosta.
monitored	boolean	Jeśli ustawiono `true`, zwracaj tylko włączone prototypy reguł LLD należące do monitorowanych hostów.
templated	boolean	Jeśli ustawiono `true`, zwracaj tylko prototypy reguł LLD należące do szablonów.
templateids	ID/array	Zwracaj tylko prototypy reguł LLD należące do podanych szablonów.
selectDiscoveryRule	query	Zwracaj właściwość `discoveryRule` z nadrzędną regułą LLD prototypu reguły LLD. Zwróci pustą odpowiedź, jeśli element nadrzędny jest prototypem reguły wykrywania.
selectDiscoveryRulePrototype	query	Zwracaj właściwość `discoveryRulePrototype` z nadrzędnym prototypem reguły LLD dla prototypu reguły LLD. Zwróci pustą odpowiedź, jeśli element nadrzędny jest regułą wykrywania (nie prototypem).
selectDiscoveryRulePrototypes	query	Zwracaj właściwość `discoveryRulePrototypes` z podrzędnymi prototypami reguł LLD należącymi do prototypu reguły LLD. Obsługuje `count`.
selectFilter	query	Zwracaj właściwość `filter` z danymi filtra używanego przez prototyp reguły LLD.
selectGraphs	query	Zwraca właściwość `graphs` z prototypami wykresów należącymi do prototypu reguły LLD. Obsługuje `count`.
selectHostPrototypes	query	Zwracaj właściwość `hostPrototypes` z prototypami hostów należącymi do prototypu reguły LLD. Obsługuje `count`.
selectHosts	query	Zwracaj właściwość `hosts` z tablicą hostów, do których należy prototyp reguły LLD.
selectItems	query	Zwracaj właściwość `items` z prototypami pozycji należącymi do prototypu reguły LLD. Obsługuje `count`.
selectTriggers	query	Zwracaj właściwość `triggers` z prototypami wyzwalaczy należącymi do prototypu reguły LLD. Obsługuje `count`.
selectLLDMacroPaths	query	Zwracaj właściwość `lld_macro_paths` z listą makr LLD i ścieżek do wartości przypisanych do każdego odpowiedniego makra.
selectPreprocessing	query	Zwracaj właściwość `preprocessing` z opcjami przetwarzania wstępnego prototypu reguły LLD.

Parametr	Typ	Opis
selectOverrides	query	Zwracaj właściwość `lld_rule_overrides` z listą filtrów nadpisywania, warunków i operacji wykonywanych na obiektach prototypów.
filter	object	Zwracaj tylko te wyniki, które dokładnie odpowiadają podanemu filtrowi. Akceptuje obiekt, w którym klucze są nazwami właściwości, a wartościami są pojedyncza wartość lub tablica wartości do dopasowania. Nie obsługuje właściwości typu danych `text` data type. Obsługuje dodatkowe właściwości: `host` - nazwa techniczna hosta, do którego należy prototyp reguły LLD.
limitSelects	integer	Ogranicza liczbę rekordów zwracanych przez podzapytania. Ma zastosowanie do następujących podzapytań: `selectItems`, `selectGraphs`, `selectTriggers`.
sortfield	string/array	Sortuj wynik według podanych właściwości. Możliwe wartości: `itemid`, `name`, `key_`, `delay`, `type`, `status`.
countOutput	boolean	Te parametry opisano w komentarzu referencyjnym.
editable	boolean	
excludeSearch	boolean	
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli został użyty parametr `countOutput`.

Przykłady

Pobieranie prototypów reguł wykrywania z hosta

Pobierz wszystkie prototypy reguł wykrywania dla określonego ID hosta.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "discoveryruleprototype.get",
    "params": {
        "hostids": "10084"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "itemid": "47253",
            "type": "23",
```

```
            "snmp_oid": "",
            "hostid": "10084",
            "name": "Odkryj przestrzenie tabel dla {#DB}",
            "key_": "db.tablespace.discovery[{#DB}]",
            "delay": "0",
            "history": "31d",
            "trends": "365d",
            "status": "0",
            "value_type": "4",
            "trapper_hosts": "",
            "units": "",
            "logtimefmt": "",
            "templateid": "0",
            "valuemapid": "0",
            "params": "",
            "ipmi_sensor": "",
            "authtype": "0",
            "username": "",
            "password": "",
            "publickey": "",
            "privatekey": "",
            "flags": "3",
            "interfaceid": "0",
            "description": "",
            "inventory_link": "0",
            "lifetime": "7d",
            "jmx_endpoint": "",
            "master_itemid": "0",
            "timeout": "",
            "url": "",
            "query_fields": [],
            "posts": "",
            "status_codes": "200",
            "follow_redirects": "1",
            "post_type": "0",
            "http_proxy": "",
            "headers": [],
            "retrieve_mode": "0",
            "request_method": "0",
            "output_format": "0",
            "ssl_cert_file": "",
            "ssl_key_file": "",
            "ssl_key_password": "",
            "verify_peer": "0",
            "verify_host": "0",
            "allow_traps": "0",
            "discover": "0",
            "uuid": "",
            "lifetime_type": "0",
            "enabled_lifetime_type": "2",
            "enabled_lifetime": "0",
            "parameters": []
        }
    ],
    "id": 1
}
```


Zobacz także

- Prototyp wykresu
- Host
- Prototyp pozycji
- Filtr prototypu reguły LLD

- Prototyp wyzwalacza

Źródło

CDiscoveryRulePrototype::get() w *ui/include/classes/api/services/CDiscoveryRulePrototype.php*.

discoveryruleprototype.update

Opis

`object discoveryruleprototype.update(object/array lldRules)`

Ta metoda umożliwia aktualizację istniejących prototypów reguł LLD.

Należy pamiętać, że aktualizacja już odkrytych prototypów jest ograniczona.

> **Note:**
> Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Właściwości prototypu reguły LLD do zaktualizowania.

Właściwość `itemid` musi być zdefiniowana dla każdego prototypu reguły LLD, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko przekazane właściwości, wszystkie pozostałe pozostaną bez zmian.

Oprócz standardowych właściwości prototypu reguły LLD, metoda akceptuje następujące parametry.

Parametr	Typ	Opis
filter	object	Filtr prototypu reguły LLD zastępujący istniejący filtr.
preprocessing	object/array	Opcje preprocessingu prototypu reguły LLD zastępujące istniejące opcje preprocessingu. Zachowanie parametru: - *tylko do odczytu* dla obiektów dziedziczonych
lld_macro_paths	object/array	Opcje lld_macro_path prototypu reguły LLD zastępujące istniejące opcje lld_macro_path. Zachowanie parametru: - *tylko do odczytu* dla obiektów dziedziczonych
overrides	object/array	Opcje nadpisań prototypu reguły LLD zastępujące istniejące opcje nadpisań. Zachowanie parametru: - *tylko do odczytu* dla obiektów dziedziczonych

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych prototypów reguł LLD we właściwości `itemids`.

Przykłady

Aktualizacja opcji preprocessing prototypu reguły LLD

Zaktualizuj prototyp reguły LLD za pomocą reguły preprocessing JSONPath. Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "discoveryruleprototype.update",
    "params": {
        "itemid": "47253",
        "preprocessing": [
            {
                "type": 12,
                "params": "$.tablespaces",
                "error_handler": 1
```

```
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "47253"
        ]
    },
    "id": 1
}
```

Źródło

CDiscoveryRulePrototype::update() w *ui/include/classes/api/services/CDiscoveryRulePrototype.php*.

Prototyp wykresu

Ta klasa jest przeznaczona do pracy z prototypami wykresów.

Odwołania do obiektów:

- Prototyp wykresu

Dostępne metody:

- graphprototype.create - utwórz nowe prototypy wykresów
- graphprototype.delete - usuń prototypy wykresów
- graphprototype.get - pobierz prototypy wykresów
- graphprototype.update - zaktualizuj prototypy wykresów

Obiekt prototypu grafu

Następujące obiekty są bezpośrednio powiązane z API `graphprototype`.

Prototyp wykresu

Obiekt prototypu wykresu ma następujące właściwości.

Właściwość	Typ	Opis
graphid	ID	ID prototypu wykresu. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji
height	integer	Wysokość prototypu wykresu w pikselach. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
name	string	Nazwa prototypu wykresu. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
width	integer	Szerokość prototypu wykresu w pikselach. Zachowanie właściwości: - *wymagane* dla operacji tworzenia

Właściwość	Typ	Opis
flags	integer	Pochodzenie prototypu wykresu. Możliwe wartości: 2 - prototyp wykresu; 6 - wykryty prototyp wykresu Zachowanie właściwości: - *tylko do odczytu*
graphtype	integer	Typ układu prototypu wykresu. Możliwe wartości: 0 - *(domyślnie)* normalny; 1 - skumulowany; 2 - kołowy; 3 - rozdzielony.
percent_left	float	Lewy percentyl. Domyślnie: 0.
percent_right	float	Prawy percentyl. Domyślnie: 0.
show_3d	integer	Czy wykryte wykresy kołowe i rozdzielone mają być wyświetlane w 3D. Możliwe wartości: 0 - *(domyślnie)* wyświetlaj w 2D; 1 - wyświetlaj w 3D.
show_legend	integer	Czy legenda ma być wyświetlana na wykrytym wykresie. Możliwe wartości: 0 - ukryj; 1 - *(domyślnie)* wyświetlaj.
show_work_period	integer	Czy czas pracy ma być wyświetlany na wykrytym wykresie. Możliwe wartości: 0 - ukryj; 1 - *(domyślnie)* wyświetlaj.
templateid	ID	ID prototypu wykresu nadrzędnego szablonu. Zachowanie właściwości: - *tylko do odczytu*
yaxismax	float	Stała maksymalna wartość osi Y.
yaxismin	float	Stała minimalna wartość osi Y.
ymax_itemid	ID	ID pozycji używanej jako maksymalna wartość osi Y. Jeśli użytkownik nie ma dostępu do określonej pozycji, wykres jest renderowany tak, jakby `ymax_type` było ustawione na ”calculated”.
ymax_type	integer	Metoda obliczania wartości maksymalnej dla osi Y. Możliwe wartości: 0 - *(domyślnie)* calculated; 1 - stała; 2 - pozycja.
ymin_itemid	ID	ID pozycji używanej jako minimalna wartość osi Y. Jeśli użytkownik nie ma dostępu do określonej pozycji, wykres jest renderowany tak, jakby `ymin_type` było ustawione na ”calculated”.
ymin_type	integer	Metoda obliczania wartości minimalnej dla osi Y. Możliwe wartości: 0 - *(domyślnie)* calculated; 1 - stała; 2 - pozycja.

Właściwość	Typ	Opis
discover	integer	Status wykrywania prototypu wykresu. Możliwe wartości: 0 - *(domyślnie)* nowe wykresy będą wykrywane; 1 - nowe wykresy nie będą wykrywane, a istniejące wykresy zostaną oznaczone jako utracone.
uuid	string	Uniwersalny unikalny identyfikator używany do łączenia importowanych prototypów wykresów z już istniejącymi. Generowany automatycznie, jeśli nie został podany. Zachowanie właściwości: - *obsługiwane*, jeśli prototyp wykresu należy do szablonu

graphprototype.create

Opis

`object graphprototype.create(object/array graphPrototypes)`

Ta metoda umożliwia tworzenie nowych prototypów wykresów.

Note:
Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Prototypy wykresów do utworzenia.

Oprócz standardowych właściwości prototypu wykresu, metoda akceptuje następujące parametry.

Parametr	Type	Opis
gitems	array	Elementy wykresu, które mają zostać utworzone dla prototypów wykresów. Elementy wykresu mogą odwoływać się zarówno do pozycji, jak i prototypów pozycji, ale musi być obecny co najmniej jeden prototyp pozycji. Zachowanie parametrów: - *wymagany*

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory utworzonych prototypów wykresów we właściwości `graphids`. Kolejność zwróconych identyfikatorów odpowiada kolejności przekazanych prototypów wykresów.

Przykłady

Tworzenie prototypu wykresu

Utwórz prototyp wykresu z dwiema pozycjami.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "graphprototype.create",
    "params": {
        "name": "Disk space usage {#FSNAME}",
        "width": 900,
        "height": 200,
        "gitems": [
            {
                "itemid": "22828",
```

```
                "color": "00AA00"
            },
            {
                "itemid": "22829",
                "color": "3333FF"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "graphids": [
            "652"
        ]
    },
    "id": 1
}
```

Zobacz także

- Pozycja wykresu

Źródło

CGraphPrototype::create() w *ui/include/classes/api/services/CGraphPrototype.php*.

graphprototype.delete

Opis

`object graphprototype.delete(array graphPrototypeIds)`

Ta metoda pozwala na usuwanie prototypów grafów.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania metody można odwołać w ustawieniach roli użytkownika. Więcej informacji można znaleźć w User roles.

Parametery

`(array)` ID prototypów wykresów do usunięcia.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory usuniętych prototypów wykresów we właściwości `graphids`.

Przykłady

Usuwanie wielu prototypów wykresów

Usuń dwa prototypy wykresów.

Żądanie:

```
{
"jsonrpc": "2.0",
"method": "graphprototype.delete",
"params": [
"652",
"653"
],
"id": 1
}
```

Odpowiedź:

```
{
"jsonrpc": "2.0",
"result": {
"graphids": [
"652",
"653"
]
},
"id": 1
}
```

Źródło

CGraphPrototype::delete() w *ui/include/classes/api/services/CGraphPrototype.php*.

graphprototype.get

Opis

`integer/array graphprototype.get(object parameters)`

Ta metoda umożliwia pobieranie prototypów wykresów zgodnie z podanymi parametrami.

Note:
Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w Rolach użytkowników.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Type	Opis
discoveryids	ID/array	Zwracaj tylko prototypy wykresów należące do podanych reguł wykrywania.
graphids	ID/array	Zwracaj tylko prototypy wykresów o podanych ID.
groupids	ID/array	Zwracaj tylko prototypy wykresów należące do hostów lub szablonów w podanych grupach hostów lub grupach szablonów.
hostids	ID/array	Zwracaj tylko prototypy wykresów należące do podanych hostów.
inherited	boolean	Jeśli ustawione na `true`, zwracaj tylko prototypy wykresów odziedziczone z szablonu.
itemids	ID/array	Zwracaj tylko prototypy wykresów zawierające podane prototypy pozycji.
templated	boolean	Jeśli ustawione na `true`, zwracaj tylko prototypy wykresów należące do szablonów.
templateids	ID/array	Zwracaj tylko prototypy wykresów należące do podanych szablonów.
selectDiscoveryData	query	Zwracaj właściwość `discoveryData` z danymi obiektu wykrywania prototypu wykresu. Obiekt wykrywania prototypu wykresu łączy wykryty prototyp wykresu z prototypem wykresu, z którego został wykryty. Ma następujące właściwości: `parent_graphid` - `(ID)` ID prototypu wykresu, z którego wykres został utworzony; `status` - `(int)` status wykrywania wykresu: 0 - *(domyślnie)* prototyp wykresu jest wykryty, 1 - prototyp wykresu nie jest już wykrywany; `ts_delete` - `(timestamp)` czas, kiedy prototyp wykresu, który nie jest już wykrywany, zostanie usunięty.
selectDiscoveryRule	query	Zwracaj właściwość `discoveryRule` z regułą LLD, do której należy prototyp wykresu.
selectDiscoveryRulePrototype	query	Zwracaj właściwość `discoveryRulePrototype` z nadrzędnym prototypem reguły LLD, do którego należy prototyp wykresu.

Parametr	Type	Opis
selectGraphItems	query	Zwracaj właściwość `gitems` z elementami wykresu używanymi w prototypie wykresu.
selectHostGroups	query	Zwracaj właściwość `hostgroups` z grupami hostów, do których należy prototyp wykresu.
selectHosts	query	Zwracaj właściwość `hosts` z hostami, do których należy prototyp wykresu.
selectItems	query	Zwracaj właściwość `items` z pozycjami i prototypami pozycji używanymi w prototypie wykresu.
selectTemplateGroups	query	Zwracaj właściwość `templategroups` z grupami szablonów, do których należy prototyp wykresu.
selectTemplates	query	Zwracaj właściwość `templates` z szablonami, do których należy prototyp wykresu.
filter	object	Zwracaj tylko te wyniki, które dokładnie odpowiadają podanemu filtrowi. Akceptuje obiekt, w którym klucze są nazwami właściwości, a wartościami są pojedyncza wartość lub tablica wartości do dopasowania. Nie obsługuje właściwości typu danych `text` data type. Obsługuje dodatkowe właściwości: `host` - techniczna nazwa hosta, do którego należy prototyp wykresu; `hostid` - ID hosta, do którego należy prototyp wykresu.
sortfield	string/array	Sortuj wynik według podanych właściwości. Możliwe wartości: `graphid`, `name`, `graphtype`, `discovered`.
countOutput	boolean	Te parametry są opisane w reference commentary.
editable	boolean	
excludeSearch	boolean	
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli został użyty parametr `countOutput`.

Przykłady

Pobieranie prototypów wykresów z reguły LLD

Pobierz wszystkie prototypy wykresów z reguły LLD.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "graphprototype.get",
    "params": {
        "output": "extend",
        "discoveryids": "27426"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "graphid": "1017",
            "name": "Wykorzystanie miejsca na dysku {#FSNAME}",
            "width": "600",
            "height": "340",
            "yaxismin": "0.0000",
            "yaxismax": "0.0000",
            "templateid": "442",
            "show_work_period": "0",
            "show_triggers": "0",
            "graphtype": "2",
            "show_legend": "1",
            "show_3d": "1",
            "percent_left": "0.0000",
            "percent_right": "0.0000",
            "ymin_type": "0",
            "ymax_type": "0",
            "ymin_itemid": "0",
            "ymax_itemid": "0",
            "flags": "2"
            "discover": "0"
        }
    ],
    "id": 1
}
```


Zobacz także

- Reguła wykrywania
- Pozycja wykresu
- Pozycja
- Host
- Grupa hostów
- Szablon
- Grupa szablonów

Źródło

CGraphPrototype::get() w *ui/include/classes/api/services/CGraphPrototype.php*.

graphprototype.update

Opis

`object graphprototype.update(object/array graphPrototypes)`

Ta metoda umożliwia aktualizację istniejących prototypów wykresów.

> **Note:**
> Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Właściwości prototypu wykresu do zaktualizowania.

Właściwość `graphid` musi być zdefiniowana dla każdego prototypu wykresu, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko przekazane właściwości, wszystkie pozostałe pozostaną bez zmian.

Oprócz standardowych właściwości prototypu wykresu, metoda akceptuje następujące parametry.

Parametr	Type	Opis
gitems	array	Pozycje wykresu służące do zastąpienia istniejących pozycji wykresu. Jeśli pozycja wykresu ma zdefiniowaną właściwość `gitemid`, zostanie zaktualizowana; w przeciwnym razie zostanie utworzona nowa pozycja wykresu.

Wartości zwracane

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych prototypów wykresów we właściwości `graphids`.

Przykłady

Zmiana rozmiaru prototypu wykresu

Zmień rozmiar prototypu wykresu na 1100 na 400 pikseli.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "graphprototype.update",
    "params": {
        "graphid": "439",
        "width": 1100,
        "height": 400
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "graphids": [
            "439"
        ]
    },
    "id": 1
}
```

Źródło

CGraphPrototype::update() w *ui/include/classes/api/services/CGraphPrototype.php*.

Prototyp wyzwalacza

Ta klasa jest przeznaczona do pracy z prototypami wyzwalaczy.

Odwołania do obiektów:

- Prototyp wyzwalacza
- Tag prototypu wyzwalacza

Dostępne metody:

- triggerprototype.create - tworzenie nowych prototypów wyzwalaczy
- triggerprototype.delete - usuwanie prototypów wyzwalaczy
- triggerprototype.get - pobieranie prototypów wyzwalaczy
- triggerprototype.update - aktualizowanie prototypów wyzwalaczy

Obiekt prototypu wyzwalacza

Następujące obiekty są bezpośrednio powiązane z API `triggerprototype`.

Prototyp wyzwalacza

Obiekt prototypu wyzwalacza ma następujące właściwości.

Właściwość	Typ	Opis
triggerid	ID	ID prototypu wyzwalacza. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji
description	string	Nazwa prototypu wyzwalacza. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
expression	string	Wyrażenie wyzwalacza. Musi zawierać co najmniej jeden prototyp pozycji. Prototypy pozycji z ustawionym `value_type` na 5 (binary) lub 6 (JSON) nie mogą być używane w wyrażeniach wyzwalaczy. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
event_name	string	Nazwa zdarzenia generowanego przez wyzwalacz.
opdata	string	Dane operacyjne.
comments	string	Dodatkowe komentarze do prototypu wyzwalacza.
priority	integer	Poziom ważności prototypu wyzwalacza. Możliwe wartości: 0 - *(domyślnie)* niesklasyfikowany; 1 - informacja; 2 - ostrzeżenie; 3 - średni; 4 - wysoki; 5 - katastrofa.
status	integer	Czy prototyp wyzwalacza jest włączony czy wyłączony. Możliwe wartości: 0 - *(domyślnie)* włączony; 1 - wyłączony.
flags	integer	Pochodzenie prototypu wyzwalacza. Możliwe wartości: 2 - prototyp wyzwalacza; 6 - wykryty prototyp wyzwalacza. Zachowanie właściwości: - *tylko do odczytu*
templateid	ID	ID nadrzędnego prototypu wyzwalacza szablonu. Zachowanie właściwości: - *tylko do odczytu*
type	integer	Czy prototyp wyzwalacza może generować wiele zdarzeń problemowych. Możliwe wartości: 0 - *(domyślnie)* nie generuj wielu zdarzeń; 1 - generuj wiele zdarzeń.
url	string	URL powiązany z prototypem wyzwalacza.
url_name	string	Etykieta dla URL powiązanego z prototypem wyzwalacza.
recovery_mode	integer	Tryb generowania zdarzenia OK. Możliwe wartości: 0 - *(domyślnie)* Wyrażenie; 1 - Wyrażenie odzyskiwania; 2 - Brak.

Właściwość	Typ	Opis
recovery_expression	string	Wyrażenie odzyskiwania wyzwalacza. Musi zawierać co najmniej jeden prototyp pozycji. Prototypy pozycji z ustawionym `value_type` na 5 (binary) lub 6 (JSON) nie mogą być używane w wyrażeniach odzyskiwania wyzwalacza.
correlation_mode	integer	Zamykanie zdarzenia OK. Możliwe wartości: 0 - *(domyślnie)* Wszystkie problemy; 1 - Wszystkie problemy, jeśli wartości tagów są zgodne.
correlation_tag	string	Tag do dopasowania.
manual_close	integer	Zezwalaj na ręczne zamknięcie. Możliwe wartości: 0 - *(domyślnie)* Nie; 1 - Tak.
discover	integer	Status wykrywania prototypu wyzwalacza. Możliwe wartości: 0 - *(domyślnie)* nowe wyzwalacze będą wykrywane; 1 - nowe wyzwalacze nie będą wykrywane, a istniejące wyzwalacze zostaną oznaczone jako utracone.
uuid	string	Uniwersalny unikalny identyfikator używany do łączenia importowanych prototypów wyzwalaczy z już istniejącymi. Generowany automatycznie, jeśli nie został podany. Zachowanie właściwości: - *obsługiwane*, jeśli prototyp wyzwalacza należy do szablonu

Tag wyzwalacza prototypu

Obiekt tagu wyzwalacza prototypu ma następujące właściwości.

Właściwość	Typ	Opis
tag	string	Nazwa tagu wyzwalacza prototypu. Zachowanie właściwości: - *wymagane*
value	string	Wartość tagu wyzwalacza prototypu. Zachowanie właściwości: - *tylko do odczytu*.
object	integer	Typ obiektu, z którego tag został odziedziczony. Możliwe wartości: 0 - szablon; 1 - host; 3 - pozycja; 4 - prototyp pozycji. Zachowanie właściwości: - *tylko do odczytu*.
objectid	ID	ID obiektu, z którego tag został odziedziczony. Zachowanie właściwości: - *tylko do odczytu*.

triggerprototype.create

Opis

`object triggerprototype.create(object/array triggerPrototypes)`

Ta metoda umożliwia tworzenie nowych prototypów wyzwalaczy.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkowników typu *Admin* i *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Prototypy wyzwalaczy do utworzenia.

Oprócz standardowych właściwości prototypu wyzwalacza metoda akceptuje następujące parametry.

Parametr	Typ	Opis
dependencies	array	Wyzwalacze i prototypy wyzwalaczy, od których zależy prototyp wyzwalacza. Wyzwalacze muszą mieć zdefiniowaną tylko właściwość `triggerid`.
tags	array	Tagi prototypu wyzwalacza.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory utworzonych prototypów wyzwalaczy we właściwości `triggerids`. Kolejność zwróconych identyfikatorów odpowiada kolejności przekazanych prototypów wyzwalaczy.

Przykłady

Tworzenie prototypu wyzwalacza

Utwórz prototyp wyzwalacza, aby wykrywać, kiedy system plików ma mniej niż 20% wolnego miejsca na dysku.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "triggerprototype.create",
    "params": {
        "description": "Wolne miejsce na dysku jest mniejsze niż 20% na woluminie {#FSNAME}",
        "expression": "last(/Zabbix server/vfs.fs.size[{#FSNAME},pfree])<20",
        "tags": [
            {
                "tag": "volume",
                "value": "{#FSNAME}"
            },
            {
                "tag": "type",
                "value": "{#FSTYPE}"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "triggerids": [
            "17372"
        ]
    },
    "id": 1
}
```

Źródło

CTriggerPrototype::create() w *ui/include/classes/api/services/CTriggerPrototype.php*.

triggerprototype.delete

Opis

`object triggerprototype.delete(array triggerPrototypeIds)`

Ta metoda pozwala na usuwanie prototypów wyzwalaczy.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania metody można odwołać w ustawieniach roli użytkownika. Więcej informacji można znaleźć w Role użytkownika.

Parametry

`(array)` ID prototypów wyzwalaczy do usunięcia.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory usuniętych prototypów wyzwalaczy we właściwości `triggerids`.

Przykłady

Usuwanie wielu prototypów wyzwalaczy

Usuń dwa prototypy wyzwalaczy.

Żądanie:

```
{
"jsonrpc": "2.0",
"method": "triggerprototype.delete",
"params": [
"12002",
"12003"
],
"id": 1
}
```

Odpowiedź:

```
{
"jsonrpc": "2.0",
"result": {
"triggerids": [
"12002",
"12003"
]
},
"id": 1
}
```

Źródło

CTriggerPrototype::delete() w *ui/include/classes/api/services/CTriggerPrototype.php*.

triggerprototype.get

Opis

`integer/array triggerprototype.get(object parameters)`

Ta metoda umożliwia pobieranie prototypów wyzwalaczy zgodnie z podanymi parametrami.

Note:
Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w Rolach użytkowników.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
active	flag	Zwracaj tylko włączone prototypy wyzwalaczy należące do monitorowanych hostów.
discoveryids	ID/array	Zwracaj tylko prototypy wyzwalaczy należące do podanych reguł LLD.
functions	string/array	Zwracaj tylko wyzwalacze używające podanych funkcji. Listę obsługiwanych funkcji można znaleźć na stronie Supported functions.
group	string	Zwracaj tylko prototypy wyzwalaczy należące do hostów lub szablonów z grup hostów lub grup szablonów o podanej nazwie.
groupids	ID/array	Zwracaj tylko prototypy wyzwalaczy należące do hostów lub szablonów z podanych grup hostów lub grup szablonów.
host	string	Zwracaj tylko prototypy wyzwalaczy należące do hostów o podanej nazwie.
hostids	ID/array	Zwracaj tylko prototypy wyzwalaczy należące do podanych hostów.
inherited	boolean	Jeśli ustawiono na `true`, zwracaj tylko prototypy wyzwalaczy dziedziczone z szablonu.
maintenance	boolean	Jeśli ustawiono na `true`, zwracaj tylko włączone prototypy wyzwalaczy należące do hostów w konserwacji.
min_severity	integer	Zwracaj tylko prototypy wyzwalaczy o ważności większej lub równej podanej ważności.
monitored	flag	Zwracaj tylko włączone prototypy wyzwalaczy należące do monitorowanych hostów i zawierające wyłącznie włączone pozycje.
templated	boolean	Jeśli ustawiono na `true`, zwracaj tylko prototypy wyzwalaczy należące do szablonów.
templateids	ID/array	Zwracaj tylko prototypy wyzwalaczy należące do podanych szablonów.
triggerids	ID/array	Zwracaj tylko prototypy wyzwalaczy o podanych identyfikatorach.
expandExpression	flag	Rozwiń funkcje i makra w wyrażeniu wyzwalacza.
selectDependencies	query	Zwracaj prototypy wyzwalaczy i wyzwalacze, od których zależy prototyp wyzwalacza, we właściwości `dependencies`.
selectDiscoveryData	query	Zwracaj właściwość `discoveryData` z danymi obiektu wykrywania prototypu wyzwalacza. Obiekt wykrywania prototypu wyzwalacza łączy wykryty prototyp wyzwalacza z prototypem wyzwalacza, z którego został wykryty. Ma on następujące właściwości: `parent_triggerid` - `(ID)` identyfikator prototypu wyzwalacza, z którego utworzono prototyp wyzwalacza; `status` - `(int)` status wykrywania prototypu wyzwalacza: 0 - *(domyślnie)* prototyp wyzwalacza jest wykryty, 1 - prototyp wyzwalacza nie jest już wykrywany; `ts_delete` - `(timestamp)` czas, kiedy prototyp wyzwalacza, który nie jest już wykrywany, zostanie usunięty; `ts_disable` - `(timestamp)` czas, kiedy prototyp wyzwalacza, który nie jest już wykrywany, zostanie wyłączony; `disable_source` - `(int)` wskaźnik określający, czy prototyp wyzwalacza został wyłączony przez regułę LLD czy ręcznie: 0 - *(domyślnie)* wyłączony automatycznie, 1 - wyłączony przez regułę LLD.
selectDiscoveryRule	query	Zwracaj regułę LLD, do której należy prototyp wyzwalacza, we właściwości `discoveryRule`.
selectDiscoveryRulePrototype	query	Zwracaj właściwość `discoveryRulePrototype` z nadrzędnym prototypem reguły LLD, do którego należy prototyp wyzwalacza.

Parametr	Typ	Opis
selectFunctions	query	Zwracaj funkcje używane w prototypie wyzwalacza we właściwości `functions`. Obiekty funkcji reprezentują funkcje używane w wyrażeniu wyzwalacza i mają następujące właściwości: `functionid` - `(ID)` identyfikator funkcji; `itemid` - `(ID)` identyfikator pozycji użytej w funkcji; `function` - `(string)` nazwa funkcji; `parameter` - `(string)` parametr przekazany do funkcji. Parametr zapytania jest zastępowany symbolem $ w zwracanym ciągu.
selectHostGroups	query	Zwracaj grupy hostów, do których należy prototyp wyzwalacza, we właściwości `hostgroups`.
selectHosts	query	Zwracaj hosty, do których należy prototyp wyzwalacza, we właściwości `hosts`.
selectInheritedTags	query	Zwracaj właściwość `inheritedTags` z tagami dziedziczonymi z szablonów, podłączonych szablonów i hostów oraz z prototypów pozycji, do których odwołują się wyrażenia wyzwalacza lub odtwarzania.
selectItems	query	Zwracaj pozycje i prototypy pozycji używane przez prototyp wyzwalacza we właściwości `items`.
selectTags	query	Zwracaj tagi prototypu wyzwalacza we właściwości `tags`.
selectTemplateGroups	query	Zwracaj grupy szablonów, do których należy prototyp wyzwalacza, we właściwości `templategroups`.
filter	object	Zwracaj tylko te wyniki, które dokładnie odpowiadają podanemu filtrowi. Akceptuje obiekt, w którym kluczami są nazwy właściwości, a wartościami są pojedyncza wartość lub tablica wartości do dopasowania. Nie obsługuje właściwości typu danych `text` data type. Obsługuje dodatkowe właściwości: `host` - techniczna nazwa hosta, do którego należy prototyp wyzwalacza; `hostid` - identyfikator hosta, do którego należy prototyp wyzwalacza.
limitSelects	integer	Ogranicza liczbę rekordów zwracanych przez podzapytania. Dotyczy następujących podzapytań: `selectHosts` - wyniki będą sortowane według `host`.
sortfield	string/array	Sortuj wynik według podanych właściwości. Możliwe wartości: `triggerid`, `description`, `status`, `priority`, `discovered`.
countOutput	boolean	Te parametry opisano w reference commentary.
editable	boolean	
excludeSearch	boolean	
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli użyto parametru `countOutput`.

Przykłady

Pobieranie prototypów wyzwalaczy z reguły LLD

Pobierz wszystkie prototypy wyzwalaczy i ich funkcje z reguły LLD.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "triggerprototype.get",
    "params": {
        "output": "extend",
        "selectFunctions": "extend",
        "discoveryids": "22450"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "triggerid": "13272",
            "expression": "{12598}<20",
            "description": "Liczba wolnych i-węzłów jest mniejsza niż 20% na woluminie {#FSNAME}",
            "url": "",
            "status": "0",
            "value": "0",
            "priority": "2",
            "lastchange": "0",
            "comments": "",
            "error": "",
            "templateid": "0",
            "type": "0",
            "state": "0",
            "flags": "2",
            "recovery_mode": "0",
            "recovery_expression": "",
            "correlation_mode": "0",
            "correlation_tag": "",
            "manual_close": "0",
            "opdata": "",
            "discover": "0",
            "event_name": "",
            "uuid": "6ce467d05e8745409a177799bed34bb3",
            "url_name": "",
            "functions": [
                {
                    "functionid": "12598",
                    "itemid": "22454",
                    "triggerid": "13272",
                    "parameter": "$",
                    "function": "last"
                }
            ]
        },
        {
            "triggerid": "13266",
            "expression": "{13500}<20",
            "description": "Wolne miejsce na dysku jest mniejsze niż 20% na woluminie {#FSNAME}",
            "url": "",
            "status": "0",
            "value": "0",
```

```
            "priority": "2",
            "lastchange": "0",
            "comments": "",
            "error": "",
            "templateid": "0",
            "type": "0",
            "state": "0",
            "flags": "2",
            "recovery_mode": "0",
            "recovery_expression": "",
            "correlation_mode": "0",
            "correlation_tag": "",
            "manual_close": "0",
            "opdata": "",
            "discover": "0",
            "event_name": "",
            "uuid": "74a1fc62bfe24b7eabe4e244c70dc384",
            "url_name": "",
            "functions": [
                {
                    "functionid": "13500",
                    "itemid": "22686",
                    "triggerid": "13266",
                    "parameter": "$",
                    "function": "last"
                }
            ]
        }
    ],
    "id": 1
}
```

Pobieranie określonego prototypu wyzwalacza z tagami

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "triggerprototype.get",
    "params": {
        "output": [
            "triggerid",
            "description"
        ],
        "selectTags": "extend",
        "triggerids": [
            "17373"
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "triggerid": "17373",
            "description": "Wolne miejsce na dysku jest mniejsze niż 20% na woluminie {#FSNAME}",
            "tags": [
                {
                    "tag": "volume",
                    "value": "{#FSNAME}"
                },
```

```
                {
                    "tag": "type",
                    "value": "{#FSTYPE}"
                }
            ]
        }
    ],
    "id": 1
}
```

Zobacz także

- Reguła wykrywania
- Pozycja
- Host
- Grupa hostów
- Grupa szablonów

Źródło

CTriggerPrototype::get() w *ui/include/classes/api/services/CTriggerPrototype.php*.

triggerprototype.update

Opis

`object triggerprototype.update(object/array triggerPrototypes)`

Ta metoda umożliwia aktualizację istniejących prototypów wyzwalaczy.

Note:
Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w rolach użytkowników.

Parametry

`(object/array)` Właściwości prototypu wyzwalacza do zaktualizowania.

Właściwość `triggerid` musi być zdefiniowana dla każdego prototypu wyzwalacza, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko przekazane właściwości, wszystkie pozostałe pozostaną bez zmian.

Oprócz standardowych właściwości prototypu wyzwalacza metoda akceptuje następujące parametry.

Parametr	Typ	Opis
dependencies	array	Wyzwalacze i prototypy wyzwalaczy, od których zależy prototyp wyzwalacza. Dla wyzwalaczy musi być zdefiniowana tylko właściwość `triggerid`.
tags	array	Tagi prototypu wyzwalacza.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych prototypów wyzwalaczy we właściwości `triggerids`.

Przykłady

Włączanie prototypu wyzwalacza

Włącz prototyp wyzwalacza, to znaczy ustaw jego status na ”0”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "triggerprototype.update",
    "params": {
        "triggerid": "13938",
```

```
        "status": 0
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "triggerids": [
            "13938"
        ]
    },
    "id": 1
}
```

Zastępowanie tagów prototypu wyzwalacza

Zastąp tagi dla jednego prototypu wyzwalacza.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "triggerprototype.update",
    "params": {
        "triggerid": "17373",
        "tags": [
            {
                "tag": "volume",
                "value": "{#FSNAME}"
            },
            {
                "tag": "type",
                "value": "{#FSTYPE}"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "triggerids": [
            "17373"
        ]
    },
    "id": 1
}
```

Źródło

CTriggerPrototype::update() w *ui/include/classes/api/services/CTriggerPrototype.php*.

Proxy

Ta klasa jest przeznaczona do pracy z proxy.

Odwołania do obiektów:

- Proxy

Dostępne metody:

- proxy.create - tworzenie nowych proxy
- proxy.delete - usuwanie proxy
- proxy.get - pobieranie proxy
- proxy.update - aktualizacja proxy

Obiekt proxy

Następujące obiekty są bezpośrednio powiązane z API `proxy`.

Proxy

Obiekt proxy ma następujące właściwości.

Właściwość	Typ	Opis
proxyid	ID	ID proxy. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji
name	string	Nazwa proxy. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
proxy_groupid	ID	ID grupy proxy. 0 - proxy nie jest przypisany do żadnej grupy proxy.
local_address	string	Adres dla aktywnych agentów. Adres IP lub nazwa DNS, z którą należy się połączyć. Zachowanie właściwości: - *wymagane*, jeśli `proxy_groupid` nie jest równe 0
local_port	string	Numer portu lokalnego proxy, z którym należy się połączyć. Obsługiwane są makra użytkownika. Domyślnie: 10051. Zachowanie właściwości: - *obsługiwane*, jeśli `proxy_groupid` nie jest równe 0
operating_mode	integer	Typ proxy. Możliwe wartości: 0 - aktywny proxy; 1 - pasywny proxy. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
description	text	Opis proxy.
lastaccess	timestamp	Czas, kiedy proxy ostatnio połączył się z serwerem. Zachowanie właściwości: - *tylko do odczytu*
address	string	Adres IP lub nazwa DNS, z którą należy się połączyć. Obsługiwane są makra użytkownika. Zachowanie właściwości: - *wymagane*, jeśli tryb działania Zabbix proxy jest pasywny

Właściwość	Typ	Opis
port	string	Numer portu, z którym należy się połączyć. Obsługiwane są makra użytkownika. Domyślnie: 10051. Zachowanie właściwości: - *obsługiwane*, jeśli tryb działania Zabbix proxy jest pasywny
allowed_addresses	string	Oddzielone przecinkami adresy IP lub nazwy DNS aktywnego Zabbix proxy.
tls_connect	integer	Połączenia do hosta. Możliwe wartości: 1 - *(domyślnie)* Bez szyfrowania; 2 - PSK; 4 - certyfikat.
tls_accept	integer	Połączenia od hosta. Możliwe wartości maski bitowej: 1 - *(domyślnie)* Bez szyfrowania; 2 - PSK; 4 - certyfikat. To pole jest maską bitową; akceptowalna jest dowolna suma możliwych wartości maski bitowej (na przykład 6 dla PSK i certyfikatu).
tls_issuer	string	Wystawca certyfikatu.
tls_subject	string	Podmiot certyfikatu.
tls_psk_identity	string	Tożsamość PSK; musi być sparowana tylko z jednym PSK (w autoregistration, hosts i proxies). Nie należy umieszczać poufnych informacji w tożsamości PSK, ponieważ jest ona wysyłana przez sieć bez szyfrowania, aby poinformować odbiorcę, którego PSK użyć. Zachowanie właściwości: - *tylko do zapisu* - *wymagane*, jeśli `tls_connect` jest ustawione na ”PSK” lub `tls_accept` zawiera bit ”PSK”
tls_psk	string	Klucz współdzielony (PSK); musi mieć co najmniej 32 cyfry szesnastkowe. Zachowanie właściwości: - *tylko do zapisu* - *wymagane*, jeśli `tls_connect` jest ustawione na ”PSK” lub `tls_accept` zawiera bit ”PSK”
custom_timeouts	integer	Czy zastąpić globalne limity czasu pozycja na poziomie proxy. Możliwe wartości: 0 - *(domyślnie)* użyj ustawień globalnych; 1 - zastąp limity czasu.
timeout_zabbix_agent	string	Na przetwarzanie nie należy poświęcać więcej niż `timeout_*` sekund. Akceptuje sekundy lub jednostkę czasu z sufiksem (np. 30s, 1m). Akceptuje również makra użytkownika. Zakres możliwych wartości: 1-600s. Domyślnie: ””. Zachowanie właściwości: - *wymagane*, jeśli `custom_timeouts` jest ustawione na 1.
timeout_simple_check		

Właściwość	Typ	Opis
timeout_snmp_agent timeout_external_check timeout_db_monitor timeout_http_agent timeout_ssh_agent timeout_telnet_agent timeout_script timeout_browser		
version	integer	Wersja proxy. Trzyczęściowy numer wersji Zabbix, gdzie dla każdej części używane są dwie cyfry dziesiętne, np. 60401 dla wersji 6.4.1, 70002 dla wersji 7.0.2 itd. 0 - Nieznana wersja proxy. Zachowanie właściwości: - *tylko do odczytu*
compatibility	integer	Wersja proxy w porównaniu z wersją Zabbix serwer. Możliwe wartości: 0 - Niezdefiniowana; 1 - Bieżąca wersja (proxy i serwer mają tę samą wersję główną); 2 - Nieaktualna wersja (wersja proxy jest starsza niż wersja serwera, ale jest częściowo obsługiwana); 3 - Nieobsługiwana wersja (wersja proxy jest starsza niż wersja poprzedniego wydania LTS serwera lub główna wersja serwera jest starsza niż główna wersja proxy). Zachowanie właściwości: - *tylko do odczytu*
state	integer	Stan proxy. Możliwe wartości: 0 - Nieznany; 1 - Offline; 2 - Online. Zachowanie właściwości: - *tylko do odczytu*

proxy.create

Opis

`object proxy.create(object/array proxies)`

Ta metoda umożliwia tworzenie nowych proxy.

Note:
Ta metoda jest dostępna tylko dla użytkownika typu *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji znajduje się w Rolach użytkowników.

Parametry

`(object/array)` Proxy do utworzenia.

Oprócz standardowych właściwości proxy, metoda akceptuje następujące parametry.

Parametr	Typ	Opis
hosts	array	Hosty, które mają być monitorowane przez proxy. Jeśli host jest już monitorowany przez inny proxy, zostanie przypisany ponownie do bieżącego proxy. Hosty muszą mieć zdefiniowaną wyłącznie właściwość `hostid`.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory utworzonych proxy we właściwości `proxyids`. Kolejność zwróconych identyfikatorów odpowiada kolejności przekazanych proxy.

Przykłady

Utwórz aktywny proxy

Utwórz aktywny proxy „Active proxy” i przypisz do niego host do monitorowania.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "proxy.create",
    "params": {
        "name": "Active proxy",
        "operating_mode": "0",
        "hosts": [
            {
                "hostid": "10279"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "proxyids": [
            "10280"
        ]
    },
    "id": 1
}
```

Utwórz pasywny proxy

Utwórz pasywny proxy „Passive proxy” i przypisz do niego dwa hosty do monitorowania.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "proxy.create",
    "params": {
        "name": "Passive proxy",
        "operating_mode": "1",
        "address": "127.0.0.1",
        "port": "10051",
        "hosts": [
            {
                "hostid": "10192"
            },
            {
                "hostid": "10139"
```

```
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "proxyids": [
            "10284"
        ]
    },
    "id": 1
}
```

Tworzenie proxy i dodawanie go do grupy proxy

Utwórz aktywny proxy „Active proxy” i dodaj go do grupy proxy o ID „1”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "proxy.create",
    "params": {
        "name": "Active proxy",
        "proxy_groupid": "1",
        "operating_mode": "0"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "proxyids": [
            "5"
        ]
    },
    "id": 1
}
```

Zobacz także

- Host
- Grupa proxy

Źródło

CProxy::create() w *ui/include/classes/api/services/CProxy.php*.

proxy.delete

Opis

`object proxy.delete(array proxies)`

Ta metoda umożliwia usuwanie proxy.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkowników typu *Super admin*. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach ról użytkowników. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(array)` ID proxy do usunięcia.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory usuniętych proxy we właściwości `proxyids`.

Przykłady

Usuń wiele proxy

Usuń dwa proxy.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "proxy.delete",
    "params": [
        "10286",
        "10285"
    ],
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "proxyids": [
            "10286",
            "10285"
        ]
    },
    "id": 1
}
```

Źródło

CProxy::delete() w *ui/include/classes/api/services/CProxy.php*.

proxy.get

Opis

`integer/array proxy.get(object parameters)`

Ta metoda umożliwia pobieranie proxy zgodnie z podanymi parametrami.

> **Note:**
> Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji znajduje się w sekcji Role użytkowników.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
proxyids	ID/array	Zwracaj tylko proxy o podanych identyfikatorach.
proxy_groupids	ID/array	Zwracaj tylko proxy należące do podanych grup proxy.
selectAssignedHosts	query	Zwracaj właściwość `assignedHosts` z hostami przypisanymi do proxy. Obsługuje `count`.

Parametr	Typ	Opis
selectHosts	query	Zwracaj właściwość `hosts` z hostami monitorowanymi przez proxy. Obsługuje `count`.
selectProxyGroup	query	Zwracaj właściwość `proxyGroup` z obiektem grupy proxy.
sortfield	string/array	Sortuj wynik według podanych właściwości. Możliwe wartości: `proxyid`, `name`, `operating_mode`.
countOutput	boolean	Te parametry opisano w komentarzu referencyjnym.
editable	boolean	
excludeSearch	boolean	
filter	object	
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli został użyty parametr `countOutput`.

Przykłady

Pobieranie wszystkich proxy

Pobierz wszystkie skonfigurowane proxy i ich interfejsy.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "proxy.get",
    "params": {
        "output": "extend"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "proxyid": "11",
            "name": "Active proxy",
            "proxy_groupid": "0",
            "local_address": "",
            "local_port": "10051",
            "operating_mode": "0",
            "description": "",
            "allowed_addresses": "",
            "address": "127.0.0.1",
            "port": "10051",
            "tls_connect": "1",
            "tls_accept": "1",
            "tls_issuer": "",
            "tls_subject": "",
            "custom_timeouts": "0",
```

```
            "timeout_zabbix_agent": "",
            "timeout_simple_check": "",
            "timeout_snmp_agent": "",
            "timeout_external_check": "",
            "timeout_db_monitor": "",
            "timeout_http_agent": "",
            "timeout_ssh_agent": "",
            "timeout_telnet_agent": "",
            "timeout_script": "",
            "last_access": "1693391880",
            "version": "70000",
            "compatibility": "1",
            "state": "1"
        },
        {
            "proxyid": "12",
            "name": "Passive proxy",
            "proxy_groupid": "1",
            "local_address": "127.0.0.1",
            "local_port": "10051",
            "operating_mode": "1",
            "description": "",
            "allowed_addresses": "",
            "address": "127.0.0.1",
            "port": "10051",
            "tls_connect": "1",
            "tls_accept": "1",
            "tls_issuer": "",
            "tls_subject": "",
            "custom_timeouts": "1",
            "timeout_zabbix_agent": "5s",
            "timeout_simple_check": "5s",
            "timeout_snmp_agent": "5s",
            "timeout_external_check": "5s",
            "timeout_db_monitor": "5s",
            "timeout_http_agent": "5s",
            "timeout_ssh_agent": "5s",
            "timeout_telnet_agent": "5s",
            "timeout_script": "5s",
            "lastaccess": "1693391875",
            "version": "60400",
            "compatibility": "2",
            "state": "2"
        }
    ],
    "id": 1
}
```


Zobacz także

- Host
- Grupa proxy

Źródło

CProxy::get() w *ui/include/classes/api/services/CProxy.php*.

proxy.update

Opis

`object proxy.update(object/array proxies)`

Ta metoda umożliwia aktualizację istniejących proxy.

Note:
Ta metoda jest dostępna tylko dla użytkowników typu *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji znajduje się w Rolach użytkowników.

Parametry

`(object/array)` Właściwości proxy do zaktualizowania.

Właściwość `proxyid` musi być zdefiniowana dla każdego proxy, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko przekazane właściwości, wszystkie pozostałe pozostaną bez zmian.

Oprócz standardowych właściwości proxy metoda akceptuje następujące parametry.

Parametr	Typ	Opis
hosts	array	Hosty do monitorowania przez proxy. Jeśli host jest już monitorowany przez inny proxy, zostanie ponownie przypisany do bieżącego proxy. Dla hostów musi być zdefiniowana tylko właściwość `hostid`.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych proxy we właściwości `proxyids`.

Przykłady

Zmień hosty monitorowane przez proxy

Zaktualizuj proxy, aby monitorował dwa podane hosty.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "proxy.update",
    "params": {
        "proxyid": "10293",
        "hosts": [
            {
                "hostid": "10294"
            },
            {
                "hostid": "10295"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "proxyids": [
            "10293"
        ]
    },
    "id": 1
}
```

Zmień status proxy

Zmień proxy na aktywny proxy i zmień jego nazwę na „Active proxy”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "proxy.update",
    "params": {
        "proxyid": "10293",
        "name": "Active proxy",
        "operating_mode": "0"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "proxyids": [
            "10293"
        ]
    },
    "id": 1
}
```

Dodawanie proxy do grupy proxy

Zaktualizuj proxy o ID „5” i dodaj go do grupy proxy o ID „1”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "proxy.create",
    "params": {
        "proxyid": "5",
        "proxy_groupid": "1",
        "local_address": "127.0.0.1"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "proxyids": [
            "5"
        ]
    },
    "id": 1
}
```

Zobacz także

- Host
- Grupa proxy

Źródło

CProxy::update() w *ui/include/classes/api/services/CProxy.php*.

Pulpit

Ta klasa jest przeznaczona do pracy z pulpitami.

Odwołania do obiektów:

- Pulpit

- Strona pulpitu
  - Widżet pulpitu
    - Pole widżetu pulpitu
- Grupa użytkowników pulpitu
- Użytkownik pulpitu

Dostępne metody:

- dashboard.create - tworzenie nowych pulpitów
- dashboard.delete - usuwanie pulpitów
- dashboard.get - pobieranie pulpitów
- dashboard.update - aktualizowanie pulpitów

Obiekt Pulpitu Nawigacyjnego

Następujące obiekty są bezpośrednio związane z API `dashboard`.

Pulpit

Obiekt pulpitu ma następujące właściwości.

Właściwość	Typ	Opis
dashboardid	ID	ID pulpitu. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji
name	string	Nazwa pulpitu. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
userid	ID	ID użytkownika będącego właścicielem pulpitu.
private	integer	Typ udostępniania pulpitu. Możliwe wartości: 0 - pulpit publiczny; 1 - *(domyślnie)* pulpit prywatny.
display_period	integer	Domyślny okres wyświetlania strony (w sekundach). Możliwe wartości: 10, 30, 60, 120, 600, 1800, 3600. Domyślnie: 30.
auto_start	integer	Automatyczne uruchamianie pokazu slajdów. Możliwe wartości: 0 - nie uruchamiaj automatycznie pokazu slajdów; 1 - *(domyślnie)* automatycznie uruchamiaj pokaz slajdów.

Strona pulpitu

Obiekt strony pulpitu ma następujące właściwości.

Właściwość	Typ	Opis
dashboard_pageid	ID	ID strony pulpitu. Zachowanie właściwości: - *tylko do odczytu*
name	string	Nazwa strony pulpitu. Domyślnie: pusty ciąg znaków.

Właściwość	Typ	Opis
display_period	integer	Okres wyświetlania strony pulpitu (w sekundach). Możliwe wartości: 0, 10, 30, 60, 120, 600, 1800, 3600. Domyślnie: 0 (zostanie użyty domyślny okres wyświetlania strony).
widgets	array	Tablica obiektów widgetu pulpitu.

Widżet pulpitu

Obiekt widżetu pulpitu ma następujące właściwości.

Właściwość	Typ	Opis
widgetid	ID	ID widżetu pulpitu. Zachowanie właściwości: - *tylko do odczytu*
type	string	Typ widżetu pulpitu. Możliwe wartości: actionlog - Dziennik działań; clock - Zegar; discovery - Status wykrywania; favgraphs - Ulubione wykresy; favmaps - Ulubione mapy; gauge - Wskaźnik; geomap - Mapa geograficzna; graph - Wykres (klasyczny); graphprototype - Prototyp wykresu; honeycomb - Plaster miodu; hostavail - Dostępność hosta; hostcard - Karta hosta; hostnavigator - Nawigator hostów; itemcard - Karta pozycji; itemhistory - Historia pozycji; itemnavigator - Nawigator pozycji; item - Wartość pozycji; map - Mapa; navtree - Drzewo nawigacji mapy; piechart - Wykres kołowy; problemhosts - Hosty z problemami; problems - Problemy; problemsbysv - Problemy według ważności; scatterplot - Wykres punktowy; slareport - Raport SLA; svggraph - Wykres; systeminfo - Informacje o systemie; tophosts - Najlepsze hosty; topitems - Najlepsze pozycje; toptriggers - Najważniejsze wyzwalacze; trigover - Przegląd wyzwalaczy; url - URL; web - Monitorowanie WWW. Zachowanie właściwości: - *wymagane*
name	string	Niestandardowa nazwa widżetu.
x	integer	Pozycja pozioma od lewej strony pulpitu. Możliwe wartości mieszczą się w zakresie od 0 do 71.

Właściwość	Typ	Opis
y	integer	Pozycja pionowa od górnej krawędzi pulpitu. Możliwe wartości mieszczą się w zakresie od 0 do 63.
width	integer	Szerokość widżetu. Możliwe wartości mieszczą się w zakresie od 1 do 72.
height	integer	Wysokość widżetu. Możliwe wartości mieszczą się w zakresie od 1 do 64.
view_mode	integer	Tryb widoku widżetu. Możliwe wartości: 0 - *(domyślnie)* domyślny widok widżetu; 1 - z ukrytym nagłówkiem;
fields	array	Tablica obiektów pola widżetu pulpitu. Zachowanie właściwości: - patrz poszczególne widżety w Pola widżetu pulpitu

Pole widżetu pulpitu

Obiekt pola widżetu pulpitu ma następujące właściwości.

Właściwość	Typ	Opis
type	integer	Typ pola widżetu. Możliwe wartości: 0 - Liczba całkowita; 1 - Ciąg znaków; 2 - Grupa hostów; 3 - Host; 4 - Pozycja; 5 - Prototyp pozycji; 6 - Wykres; 7 - Prototyp wykresu; 8 - Mapa; 9 - Usługa; 10 - SLA; 11 - Użytkownik; 12 - Akcja; 13 - Typ nośnika. Zachowanie właściwości: - *wymagane*
name	string	Nazwa pola widżetu. Możliwe wartości: patrz Pola widżetu pulpitu. Zachowanie właściwości: - *wymagane*
value	mixed	Wartość pola widżetu zależna od typu. Możliwe wartości: patrz Pola widżetu pulpitu. Zachowanie właściwości: - *wymagane*

Grupa użytkowników pulpitu

Lista uprawnień pulpitu oparta na grupach użytkowników. Ma następujące właściwości.

Właściwość	Typ	Opis
usrgrpid	ID	ID grupy użytkowników. Zachowanie właściwości: - *wymagane*
permission	integer	Typ poziomu uprawnień. Możliwe wartości: 2 - tylko do odczytu; 3 - odczyt-zapis. Zachowanie właściwości: - *wymagane*

Użytkownik pulpitu

Lista uprawnień pulpitu na podstawie użytkowników. Ma następujące właściwości.

Właściwość	Typ	Opis
userid	ID	ID użytkownika. Zachowanie właściwości: - *wymagane*
permission	integer	Typ poziomu uprawnień. Możliwe wartości: 2 - tylko do odczytu; 3 - odczyt-zapis. Zachowanie właściwości: - *wymagane*

dashboard.create

Opis

`object dashboard.create(object/array dashboards)`

Ta metoda umożliwia tworzenie nowych dashboardów.

Note:
Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w Rolach użytkowników.

Parametry

`(object/array)` Pulpity do utworzenia.

Oprócz standardowych właściwości pulpitu, metoda akceptuje następujące parametry.

Parametr	Typ	Opis
pages	array	Strony pulpitu, które mają zostać utworzone dla pulpitu. Strony pulpitu będą uporządkowane w tej samej kolejności, w jakiej zostały podane. Zachowanie parametrów: - *wymagane*
users	array	Udziały użytkownika pulpitu, które mają zostać utworzone na pulpicie.
userGroups	array	Udziały grupy użytkowników pulpitu, które mają zostać utworzone na pulpicie.

Zwracane wartości

(object) Zwraca obiekt zawierający identyfikatory utworzonych pulpitów we właściwości dashboardids. Kolejność zwróconych ID jest zgodna z kojenością przekazanych pulpitów.

Przykłady

Tworzenie pulpitu

Utwórz pulpit o nazwie „My dashboard” z jednym widżetem Problemy z tagami oraz z użyciem dwóch typów udostępniania (grupa użytkowników i użytkownik) na jednej stronie pulpitu.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "dashboard.create",
    "params": {
        "name": "My dashboard",
        "display_period": 30,
        "auto_start": 1,
        "pages": [
            {
                "widgets": [
                    {
                        "type": "problems",
                        "x": 0,
                        "y": 0,
                        "width": 36,
                        "height": 5,
                        "view_mode": 0,
                        "fields": [
                            {
                                "type": 1,
                                "name": "tags.0.tag",
                                "value": "service"
                            },
                            {
                                "type": 0,
                                "name": "tags.0.operator",
                                "value": 1
                            },
                            {
                                "type": 1,
                                "name": "tags.0.value",
                                "value": "zabbix_server"
                            }
                        ]
                    }
                ]
            }
        ],
        "userGroups": [
            {
                "usrgrpid": "7",
                "permission": 2
            }
        ],
        "users": [
            {
                "userid": "4",
                "permission": 3
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "2"
        ]
    },
    "id": 1
}
```

Zobacz także

- Strona pulpitu
- Widżet pulpitu
- Pole widżetu pulpitu
- Użytkownik pulpitu
- Grupa użytkowników pulpitu

Źródło

CDashboard::create() w *ui/include/classes/api/services/CDashboard.php*.

dashboard.delete

Opis

`object dashboard.delete(array dashboardids)`

Ta metoda umożliwia usuwanie pulpitów.

Note:
Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywołania metody można odwołać w ustawieniach roli użytkownika. Więcej informacji można znaleźć w User roles.

Parametry

`(array)` identyfikatory pulpitów do usunięcia.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory usuniętych pulpitów we właściwości `dashboardids`.

Przykłady

Usuwanie wielu pulpitów

Usuń dwa pulpity.

Żądanie:

```
{
"jsonrpc": "2.0",
"method": "dashboard.delete",
"params": [
"2",
"3"
],
"id": 1
}
```

Odpowiedź:

```
{
"jsonrpc": "2.0",
"result": {
"dashboardids": [
"2",
"3"
```

```
]
},
"id": 1
}
```

Źródło

CDashboard::delete() w *ui/include/classes/api/services/CDashboard.php*.

dashboard.get

Opis

`integer/array dashboard.get(object parameters)`

Ta metoda umożliwia pobieranie pulpitów zgodnie z podanymi parametrami.

Note:
Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w User roles.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
dashboardids	ID/array	Zwraca tylko pulpity z podanymi ID.
selectPages	query	Zwraca właściwość `pages` z prawidłowo uporządkowanymi stronami pulpitu.
selectUsers	query	Zwraca właściwość `users` z użytkownikami, którym udostępniono pulpit.
selectUserGroups	query	Zwraca właściwość `userGroups` z grupami użytkowników, którym udostępniono pulpit.
sortfield	string/array	Sortuje wynik według podanych właściwości. Możliwe wartości: `dashboardid`.
countOutput	boolean	Te parametry opisano w komentarzu referencyjnym.
editable	boolean	
excludeSearch	boolean	
filter	object	
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca jedną z opcji:

- tablica obiektów;
- ilość pobranych obiektów, jeżeli parametr `countOutput` został użyty.

Przykłady

Pobieranie pulpitu nawigacyjnego według ID

Pobierz wszystkie dane o pulpitach nawigacyjnych „1” i „2”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "dashboard.get",
    "params": {
        "output": "extend",
        "selectPages": "extend",
        "selectUsers": "extend",
        "selectUserGroups": "extend",
        "dashboardids": [
            "1",
            "2"
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "dashboardid": "1",
            "name": "Dashboard",
            "userid": "1",
            "private": "0",
            "display_period": "30",
            "auto_start": "1",
            "users": [],
            "userGroups": [],
            "pages": [
                {
                    "dashboard_pageid": "1",
                    "name": "",
                    "display_period": "0",
                    "widgets": [
                        {
                            "widgetid": "9",
                            "type": "systeminfo",
                            "name": "",
                            "x": "12",
                            "y": "8",
                            "width": "12",
                            "height": "5",
                            "view_mode": "0",
                            "fields": []
                        },
                        {
                            "widgetid": "8",
                            "type": "problemsbysv",
                            "name": "",
                            "x": "12",
                            "y": "4",
                            "width": "12",
                            "height": "4",
                            "view_mode": "0",
                            "fields": []
                        },
                        {
                            "widgetid": "7",
                            "type": "problemhosts",
                            "name": "",
                            "x": "12",
```

```
                "y": "0",
                "width": "12",
                "height": "4",
                "view_mode": "0",
                "fields": []
            },
            {
                "widgetid": "6",
                "type": "discovery",
                "name": "",
                "x": "6",
                "y": "9",
                "width": "18",
                "height": "4",
                "view_mode": "0",
                "fields": []
            },
            {
                "widgetid": "5",
                "type": "web",
                "name": "",
                "x": "0",
                "y": "9",
                "width": "18",
                "height": "4",
                "view_mode": "0",
                "fields": []
            },
            {
                "widgetid": "4",
                "type": "problems",
                "name": "",
                "x": "0",
                "y": "3",
                "width": "12",
                "height": "6",
                "view_mode": "0",
                "fields": []
            },
            {
                "widgetid": "3",
                "type": "favmaps",
                "name": "",
                "x": "8",
                "y": "0",
                "width": "12",
                "height": "3",
                "view_mode": "0",
                "fields": []
            },
            {
                "widgetid": "1",
                "type": "favgraphs",
                "name": "",
                "x": "0",
                "y": "0",
                "width": "12",
                "height": "3",
                "view_mode": "0",
                "fields": []
            }
        ]
```

```
            },
            {
                "dashboard_pageid": "2",
                "name": "",
                "display_period": "0",
                "widgets": []
            },
            {
                "dashboard_pageid": "3",
                "name": "Custom page name",
                "display_period": "60",
                "widgets": []
            }
        ]
    },
    {
        "dashboardid": "2",
        "name": "My dashboard",
        "userid": "1",
        "private": "1",
        "display_period": "60",
        "auto_start": "1",
        "users": [
            {
                "userid": "4",
                "permission": "3"
            }
        ],
        "userGroups": [
            {
                "usrgrpid": "7",
                "permission": "2"
            }
        ],
        "pages": [
            {
                "dashboard_pageid": "4",
                "name": "",
                "display_period": "0",
                "widgets": [
                    {
                        "widgetid": "10",
                        "type": "problems",
                        "name": "",
                        "x": "0",
                        "y": "0",
                        "width": "12",
                        "height": "5",
                        "view_mode": "0",
                        "fields": [
                            {
                                "type": "2",
                                "name": "groupids",
                                "value": "4"
                            }
                        ]
                    }
                ]
            }
        ]
    }
],
```

```
    "id": 1
}
```

Zobacz także

- Strona pulpitu
- Widżet pulpitu
- Pole widżetu pulpitu
- Użytkownik pulpitu
- Grupa użytkowników pulpitu

Źródło

CDashboard::get() w *ui/include/classes/api/services/CDashboard.php*.

dashboard.update

Opis

`object dashboard.update(object/array dashboards)`

Ta metoda umożliwia aktualizację istniejących pulpitów.

> **Note:**
> Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach ról użytkowników. Więcej informacji można znaleźć w User roles.

Parametry

`(object/array)` Właściwości dashboardu do zaktualizowania.

Właściwość `dashboardid` musi być zdefiniowana dla każdego dashboardu, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko przekazane właściwości, wszystkie pozostałe pozostaną bez zmian.

Oprócz standardowych właściwości dashboardu, metoda akceptuje następujące parametry.

Parametr	Typ	Opis
pages	array	Strony dashboardu, które zastąpią istniejące strony dashboardu. Strony dashboardu są aktualizowane za pomocą właściwości `dashboard_pageid`. Nowe strony dashboardu zostaną utworzone dla obiektów bez właściwości `dashboard_pageid`, a istniejące strony dashboardu zostaną usunięte, jeśli nie zostaną ponownie użyte. Strony dashboardu zostaną uporządkowane w tej samej kolejności, w jakiej zostały podane. Zaktualizowane zostaną tylko określone właściwości stron dashboardu.
users	array	Udostępnienia użytkownikom dashboardu, które zastąpią istniejące elementy.
userGroups	array	Udostępnienia grupom użytkowników dashboardu, które zastąpią istniejące elementy.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych pulpitów pod właściwością `dashboardids`.

Przykłady

Zmienianie nazwy pulpitu

Zmień nazwę pulpitu na „SQL server status”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "dashboard.update",
    "params": {
```

```
        "dashboardid": "2",
        "name": "SQL server status"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "2"
        ]
    },
    "id": 1
}
```

Aktualizowanie stron pulpitu

Zmień nazwę pierwszej strony pulpitu, zastąp widgety na drugiej stronie pulpitu i dodaj nową stronę jako trzecią. Usuń wszystkie pozostałe strony pulpitu.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "dashboard.update",
    "params": {
        "dashboardid": "2",
        "pages": [
            {
                "dashboard_pageid": 1,
                "name": "Strona o zmienionej nazwie"
            },
            {
                "dashboard_pageid": 2,
                "widgets": [
                    {
                        "type": "clock",
                        "x": 0,
                        "y": 0,
                        "width": 12,
                        "height": 3
                    }
                ]
            },
            {
                "display_period": 60
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "2"
        ]
    },
    "id": 1
}
```

Zmień właściciela pulpitu

Dostępne tylko dla administratorów i super administratorów.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "dashboard.update",
    "params": {
        "dashboardid": "2",
        "userid": "1"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "2"
        ]
    },
    "id": 1
}
```

Zobacz także

- Strona pulpitu
- Widżet pulpitu
- Pole widżetu pulpitu
- Użytkownik pulpitu
- Grupa użytkowników pulpitu

Źródło

CDashboard::update() w *ui/include/classes/api/services/CDashboard.php*.

Pola widżetu pulpitu

Ta strona zawiera linki nawigacyjne do parametrów widgetów pulpitu oraz możliwych wartości właściwości dla odpowiednich obiektów pola widgetu pulpitu.

Aby zobaczyć parametry i wartości właściwości dla każdego widgetu, użyj paska bocznego, aby przejść do strony odpowiedniego widgetu.

1 Log akcji

Opis

Te parametry oraz możliwe wartości właściwości dla odpowiednich obiektów pól widgetu umożliwiają konfigurację widgetu *Action log* w metodach `dashboard.create` i `dashboard.update`.

> **Attention:**
> Właściwości `fields` widgetu nie są walidowane podczas tworzenia ani aktualizacji pulpitu. Pozwala to użytkownikom modyfikować wbudowane widgety i tworzyć niestandardowe widgety, ale jednocześnie wprowadza ryzyko nieprawidłowego tworzenia lub aktualizowania widgetów. Aby zapewnić pomyślne utworzenie lub aktualizację widgetu *Action log*, zapoznaj się z zachowaniem parametrów opisanym w poniższych tabelach.

Parametry

Następujące parametry są obsługiwane dla widżetu *Dziennik działań*.

Parametr	type	name	value
Interwał odświeżania	0	rf_rate	0 - Bez odświeżania; 10 - 10 sekund; 30 - 30 sekund; 60 - *(domyślnie)* 1 minuta; 120 - 2 minuty; 600 - 10 minut; 900 - 15 minut.
Odbiorcy	11	userids.0	ID użytkownika. Uwaga: Aby skonfigurować wielu użytkowników, utwórz obiekt pola widżetu pulpitu dla każdego użytkownika z inkrementowanym numerem w nazwie właściwości.
Działania	12	actionids.0	ID działania. Uwaga: Aby skonfigurować wiele działań, utwórz obiekt pola widżetu pulpitu dla każdego działania z inkrementowanym numerem w nazwie właściwości.
Typy mediów	13	mediatypeids.0	ID typu mediów. Uwaga: Aby skonfigurować wiele typów mediów, utwórz obiekt pola widżetu pulpitu dla każdego typu mediów z inkrementowanym numerem w nazwie właściwości.
Status	0	statuses.0	0 - W toku; 1 - Wysłano/Wykonano; 2 - Niepowodzenie. Uwaga: Aby skonfigurować wiele wartości, utwórz obiekt pola widżetu pulpitu dla każdej wartości z inkrementowanym numerem w nazwie właściwości.
Szukany ciąg	1	message	Dowolna wartość tekstowa.
Okres czasu	1	time_period._referenc	`DASHBOARD._timeperiod` - ustaw selektor okresu czasu pulpitu jako źródło danych; `ABCDE._timeperiod` - ustaw kompatybilny widżet (z parametrem *Reference* ustawionym na "`ABCDE`") jako źródło danych. Domyślnie: `DASHBOARD._timeperiod` Alternatywnie można ustawić okres czasu tylko w parametrach *Od* i *Do*.
Od	1	time_period.from	Prawidłowy ciąg czasu w składni bezwzględnej (`YYYY-MM-DD hh:mm:ss`) lub względnej (`now`, `now/d`, `now/w-1w` itd.). Zachowanie parametru: - *obsługiwany*, jeśli *Okres czasu* nie jest ustawiony - *wymagany*, jeśli ustawiono `time_period.to`
Do	1	time_period.to	Prawidłowy ciąg czasu w składni bezwzględnej (`YYYY-MM-DD hh:mm:ss`) lub względnej (`now`, `now/d`, `now/w-1w` itd.). Zachowanie parametru: - *obsługiwany*, jeśli *Okres czasu* nie jest ustawiony - *wymagany*, jeśli ustawiono `time_period.from`
Sortuj wpisy według	0	sort_triggers	3 - Czas (rosnąco); 4 - *(domyślnie)* Czas (malejąco); 5 - Typ (rosnąco); 6 - Typ (malejąco); 7 - Status (rosnąco); 8 - Status (malejąco); 11 - Odbiorca (rosnąco); 12 - Odbiorca (malejąco).

Parametr	type	name	value
Pokaż wier-sze	0	show_lines	Możliwe wartości mieszczą się w zakresie 1-100. Domyślnie: 25.

Przykłady

Poniższe przykłady mają na celu jedynie opisanie konfiguracji obiektów pól widżetu pulpitu dla widżetu *Zegara*. Aby uzyskać więcej informacji na temat konfigurowania pulpitu nawigacyjnego, zobacz `dashboard.create`.

Konfigurowanie widżetu *Dziennik działań*

Skonfiguruj widżet *Dziennik działań*, który wyświetla 10 wpisów ze szczegółami operacji działania, posortowanych według czasu (rosnąco). Dodatkowo wyświetlaj szczegóły tylko dla tych operacji działania, które próbowały wysłać wiadomość e-mail do użytkownika „1”, ale zakończyły się niepowodzeniem.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "dashboard.create",
    "params": {
        "name": "My dashboard",
        "display_period": 30,
        "auto_start": 1,
        "pages": [
            {
                "widgets": [
                    {
                        "type": "actionlog",
                        "name": "Action log",
                        "x": 0,
                        "y": 0,
                        "width": 36,
                        "height": 5,
                        "view_mode": 0,
                        "fields": [
                            {
                                "type": 0,
                                "name": "show_lines",
                                "value": 10
                            },
                            {
                                "type": 0,
                                "name": "sort_triggers",
                                "value": 3
                            },
                            {
                                "type": 11,
                                "name": "userids.0",
                                "value": 1
                            },
                            {
                                "type": 13,
                                "name": "mediatypeids.0",
                                "value": 1
                            },
                            {
                                "type": 0,
                                "name": "statuses.0",
                                "value": 2
                            }
                        ]
                    }
```

```
                ]
            }
        ],
        "userGroups": [
            {
                "usrgrpid": 7,
                "permission": 2
            }
        ],
        "users": [
            {
                "userid": 1,
                "permission": 3
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "3"
        ]
    },
    "id": 1
}
```

Zobacz także

- Pole widżetu pulpitu
- `dashboard.create`
- `dashboard.update`

2 Zegar

Opis

Te parametry oraz możliwe wartości właściwości dla odpowiednich obiektów pól widżetu umożliwiają skonfigurowanie widżetu *Clock* w metodach `dashboard.create` i `dashboard.update`.

Attention:
Właściwości `fields` widżetu nie są walidowane podczas tworzenia ani aktualizacji pulpitu. Pozwala to użytkownikom modyfikować wbudowane widżety i tworzyć własne widżety, ale jednocześnie wprowadza ryzyko nieprawidłowego tworzenia lub aktualizowania widżetów. Aby zapewnić pomyślne utworzenie lub aktualizację widżetu *Clock*, zapoznaj się z zachowaniem parametrów opisanym w poniższych tabelach.

Parametry

Następujące parametry są obsługiwane dla widżetu *Clock*.

Parametr	type	name	value
Interwał odświeżania	0	rf_rate	0 - Bez odświeżania; 10 - 10 sekund; 30 - 30 sekund; 60 - 1 minuta; 120 - 2 minuty; 600 - 10 minut; 900 - *(domyślnie)* 15 minut.

Parametr	type	name	value
Typ czasu	0	time_type	0 - *(domyślnie)* Czas lokalny; 1 - Czas serwera; 2 - Czas hosta.
Typ zegara	0	clock_type	0 - *(domyślnie)* Analogowy; 1 - Cyfrowy.

Następujące parametry są obsługiwane, jeśli *Typ czasu* jest ustawiony na „Czas hosta”.

Parametr	type	name	value
Pozycja	4	itemid.0	ID pozycji. Zachowanie parametru: - *wymagane*

Następujące parametry są obsługiwane, jeśli *Typ zegara* jest ustawiony na „Cyfrowy”.

Parametr	type	name	value
Pokaż	0	show.0	1 - Data; 2 - *(domyślnie)* Czas; 3 - Strefa czasowa. Uwaga: Aby skonfigurować wiele wartości, utwórz obiekt pola widżetu pulpitu dla każdej wartości z inkrementowanym numerem w nazwie właściwości.

Konfiguracja zaawansowana

Następujące zaawansowane parametry konfiguracji są obsługiwane, jeśli *Typ zegara* jest ustawiony na „Cyfrowy”.

Parametr	type	name	value
Kolor tła	1	bg_color	Szesnastkowy kod koloru (np. FF0000). Domyślnie: "" (puste).

Data

Następujące zaawansowane parametry konfiguracji są obsługiwane, jeśli *Clock type* jest ustawiony na „Digital”, a *Show* jest ustawione na „Date”.

Parametr	type	name	value
Pogrubienie	0	date_bold	0 - *(domyślnie)* Wyłączone; 1 - Włączone.
Kolor	1	date_color	Szesnastkowy kod koloru (np. FF0000). Domyślnie: "" (puste).

Czas

Następujące zaawansowane parametry konfiguracji są obsługiwane, jeśli *Typ zegara* jest ustawiony na „Cyfrowy”, a *Pokaż* jest ustawiony na „Czas”.

Parametr	typ	nazwa	wartość
Pogrubienie	0	time_bold	0 - *(domyślnie)* Wyłączone; 1 - Włączone.

Parametr	typ	nazwa	wartość
Kolor	1	time_color	Kod koloru szesnastkowego (np. FF0000). Domyślnie: "" (puste).
Sekundy	0	time_sec	0 - Wyłączone; 1 - *(domyślnie)* Włączone.
Format	0	time_format	0 - *(domyślny)* 24-godzinny; 1 - 12-godzinny.

Strefa czasowa

Następujące zaawansowane parametry konfiguracyjne są obsługiwane, jeśli *Clock type* jest ustawiony na „Digital”, a *Show* jest ustawione na „Time zone”.

Parametr	type	name	value
Pogrubienie	0	tzone_bold	0 - *(domyślnie)* Wyłączone; 1 - Włączone.
Kolor	1	tzone_color	Szesnastkowy kod koloru (np. FF0000). Domyślnie: "" (puste).
Strefa czasowa	1	tzone_timezone	Prawidłowy ciąg strefy czasowej (np. Europe/Riga, system, UTC itd.). Pełną listę obsługiwanych stref czasowych można znaleźć w dokumentacji PHP. Domyślnie: local. Zachowanie parametru: - *obsługiwany*, jeśli *Time type* jest ustawiony na „Local time” lub „Server time”
Format	0	tzone_format	0 - *(domyślnie)* Krótki; 1 - Pełny. Zachowanie parametru: - *obsługiwany*, jeśli *Time type* jest ustawiony na „Local time” lub „Server time”

Przykłady

Poniższe przykłady mają na celu jedynie opisanie konfiguracji obiektów pól widżetu pulpitu dla widżetu *Zegara*. Aby uzyskać więcej informacji na temat konfigurowania pulpitu nawigacyjnego, zobacz `dashboard.create`.

Konfigurowanie widżetu *Clock*

Skonfiguruj widżet *Clock*, który wyświetla lokalną datę, godzinę i strefę czasową w dostosowanym zegarze cyfrowym.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "dashboard.create",
    "params": {
        "name": "My dashboard",
        "display_period": 30,
        "auto_start": 1,
        "pages": [
            {
                "widgets": [
                    {
                        "type": "clock",
                        "name": "Clock",
                        "x": 0,
                        "y": 0,
                        "width": 12,
```

```
                    "height": 3,
                    "view_mode": 0,
                    "fields": [
                        {
                            "type": 0,
                            "name": "clock_type",
                            "value": 1
                        },
                        {
                            "type": 0,
                            "name": "show.0",
                            "value": 1
                        },
                        {
                            "type": 0,
                            "name": "show.1",
                            "value": 2
                        },
                        {
                            "type": 0,
                            "name": "show.2",
                            "value": 3
                        },
                        {
                            "type": 1,
                            "name": "date_color",
                            "value": "E1E1E1"
                        },
                        {
                            "type": 0,
                            "name": "time_bold",
                            "value": 1
                        },
                        {
                            "type": 1,
                            "name": "tzone_color",
                            "value": "E1E1E1"
                        },
                        {
                            "type": 1,
                            "name": "tzone_timezone",
                            "value": "Europe/Riga"
                        },
                        {
                            "type": 0,
                            "name": "tzone_format",
                            "value": 1
                        }
                    ]
                }
            ]
        }
    ],
    "userGroups": [
        {
            "usrgrpid": 7,
            "permission": 2
        }
    ],
    "users": [
        {
            "userid": 1,
```

```
                "permission": 3
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "3"
        ]
    },
    "id": 1
}
```

Zobacz także

- Pole widżetu pulpitu
- `dashboard.create`
- `dashboard.update`

3 Stan wykrywania

Opis

Te parametry i możliwe wartości właściwości dla odpowiednich obiektów pól widżetów dashboard pozwalają skonfigurować widżet *Discovery status* w metodach `dashboard.create` i `dashboard.update`.

Parametry

Następujące parametry są obsługiwane dla widżetu *Status wykrywania*.

Parametr	type	name	value
Interwał odświeżania	0	rf_rate	0 - Brak odświeżania; 10 - 10 sekund; 30 - 30 sekund; 60 - *(domyślnie)* 1 minuta; 120 - 2 minuty; 600 - 10 minut; 900 - 15 minut.

Przykłady

Poniższe przykłady mają na celu jedynie opisanie konfiguracji obiektów pól widżetu pulpitu dla widżetu *Status wykrywania*. Więcej informacji na temat konfiguracji pulpitu znajduje się w `dashboard.create`.

Konfigurowanie widżetu *Discovery status*

Skonfiguruj widżet *Discovery status* z interwałem odświeżania ustawionym na 15 minut.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "dashboard.create",
    "params": {
        "name": "My dashboard",
        "display_period": 30,
        "auto_start": 1,
        "pages": [
            {
```

```
                "widgets": [
                    {
                        "type": "discovery",
                        "name": "Discovery status",
                        "x": 0,
                        "y": 0,
                        "width": 18,
                        "height": 3,
                        "view_mode": 0,
                        "fields": [
                            {
                                "type": 0,
                                "name": "rf_rate",
                                "value": 900
                            }
                        ]
                    }
                ]
            }
        ],
        "userGroups": [
            {
                "usrgrpid": 7,
                "permission": 2
            }
        ],
        "users": [
            {
                "userid": 1,
                "permission": 3
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "3"
        ]
    },
    "id": 1
}
```

Zobacz także

- Pole widżetu pulpitu
- `dashboard.create`
- `dashboard.update`

4 Ulubione wykresy

Opis

Te parametry i możliwe wartości właściwości dla odpowiednich obiektów pól widgetu dashboard pozwalają skonfigurować widget *Favorite graphs* w metodach `dashboard.create` i `dashboard.update`.

Parametry

Następujące parametry są obsługiwane dla widżetu *Favorite graphs*.

Parameter	type	name	value
Refresh interval	0	rf_rate	0 - Brak odświeżania; 10 - 10 sekund; 30 - 30 sekund; 60 - 1 minuta; 120 - 2 minuty; 600 - 10 minut; 900 - *(domyślnie)* 15 minut.

Przykłady

Poniższe przykłady mają na celu jedynie opisanie konfiguracji obiektów pól widżetu pulpitu dla widżetu *Ulubione wykresy*. Więcej informacji na temat konfigurowania pulpitu można znaleźć w `dashboard.create`.

Konfigurowanie widżetu *Ulubione wykresy*

Skonfiguruj widżet *Ulubione wykresy* z interwałem odświeżania ustawionym na 10 minut.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "dashboard.create",
    "params": {
        "name": "Mój pulpit",
        "display_period": 30,
        "auto_start": 1,
        "pages": [
            {
                "widgets": [
                    {
                        "type": "favgraphs",
                        "name": "Ulubione wykresy",
                        "x": 0,
                        "y": 0,
                        "width": 12,
                        "height": 3,
                        "view_mode": 0,
                        "fields": [
                            {
                                "type": 0,
                                "name": "rf_rate",
                                "value": 600
                            }
                        ]
                    }
                ]
            }
        ],
        "userGroups": [
            {
                "usrgrpid": 7,
                "permission": 2
            }
        ],
        "users": [
            {
                "userid": 1,
                "permission": 3
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "3"
        ]
    },
    "id": 1
}
```

Zobacz także

- Pole widżetu pulpitu
- dashboard.create
- dashboard.update

5 Ulubione mapy

Opis

Te parametry oraz możliwe wartości właściwości dla odpowiednich obiektów pól widżetu pulpitu umożliwiają skonfigurowanie widżetu *Ulubione mapy* w metodach dashboard.create i dashboard.update.

Parametry

Następujące parametry są obsługiwane dla widżetu *Ulubione mapy*.

Parametr	type	name	value
Interwał odświeżania	0	rf_rate	0 - Bez odświeżania; 10 - 10 sekund; 30 - 30 sekund; 60 - 1 minuta; 120 - 2 minuty; 600 - 10 minut; 900 - *(domyślnie)* 15 minut.

Przykłady

Poniższe przykłady mają na celu jedynie opisanie konfiguracji obiektów pól widgetu pulpitu dla widgetu *Ulubione mapy*. Więcej informacji na temat konfiguracji pulpitu znajduje się w dashboard.create.

Konfigurowanie widżetu *Ulubione mapy*

Skonfiguruj widżet *Ulubione mapy* z interwałem odświeżania ustawionym na 10 minut.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "dashboard.create",
    "params": {
        "name": "My dashboard",
        "display_period": 30,
        "auto_start": 1,
        "pages": [
            {
                "widgets": [
                    {
                        "type": "favmaps",
                        "name": "Favorite maps",
                        "x": 0,
                        "y": 0,
                        "width": 12,
```

```
                        "height": 3,
                        "view_mode": 0,
                        "fields": [
                            {
                                "type": 0,
                                "name": "rf_rate",
                                "value": 600
                            }
                        ]
                    }
                ]
            }
        ],
        "userGroups": [
            {
                "usrgrpid": 7,
                "permission": 2
            }
        ],
        "users": [
            {
                "userid": 1,
                "permission": 3
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "3"
        ]
    },
    "id": 1
}
```

Zobacz także

- Pole widżetu pulpitu
- `dashboard.create`
- `dashboard.update`

6 Wskaźnik

Opis

Te parametry oraz możliwe wartości właściwości dla odpowiednich obiektów pól widgetu umożliwiają konfigurację widgetu *Gauge* w metodach `dashboard.create` i `dashboard.update`.

Attention:
Właściwości `fields` widgetu nie są walidowane podczas tworzenia ani aktualizacji pulpitu. Pozwala to użytkownikom modyfikować wbudowane widgety i tworzyć własne widgety, ale jednocześnie wprowadza ryzyko nieprawidłowego tworzenia lub aktualizowania widgetów. Aby zapewnić pomyślne utworzenie lub zaktualizowanie widgetu *Gauge*, zapoznaj się z zachowaniem parametrów opisanym w poniższych tabelach.

Parametry

Następujące parametry są obsługiwane dla widżetu *Gauge*.

Parametr	type	name	value
Interwał odświeżania	0	rf_rate	0 - Bez odświeżania; 10 - 10 sekund; 30 - 30 sekund; 60 - *(domyślnie)* 1 minuta; 120 - 2 minuty; 600 - 10 minut; 900 - 15 minut.
Pozycja	4	itemid.0	ID pozycji. Zachowanie parametrów: - *wymagane*, jeśli *Pozycja (widżet)* nie jest ustawiona
Pozycja (widżet)	1	itemid._reference	Zamiast ID pozycji: `ABCDE._itemid` - ustawia kompatybilny widżet (z parametrem *Reference* ustawionym na "ABCDE") jako źródło danych dla pozycji. Zachowanie parametrów: - *wymagane*, jeśli *Pozycja* nie jest ustawiona
Min	1	min	Dowolna wartość liczbowa. Obsługiwane są sufiksy (np. "1d", "2w", "4K", "8G"). Domyślnie: "0".
Max	1	max	Dowolna wartość liczbowa. Obsługiwane są sufiksy (np. "1d", "2w", "4K", "8G"). Domyślnie: "100".
Łuk wartości	1	value_arc_color	Szesnastkowy kod koloru (np. `FF0000`). Domyślnie: "" (puste).
Tło łuku	1	empty_color	Szesnastkowy kod koloru (np. `FF0000`). Domyślnie: "" (puste).
Tło	1	bg_color	Szesnastkowy kod koloru (np. `FF0000`). Domyślnie: "" (puste).
Pokaż	0	show.0	1 - Opis; 2 - Wartość; 3 - Wskazówka; 4 - Skala; 5 - Łuk wartości. Uwaga: Aby skonfigurować wiele wartości, utwórz obiekt pola widżetu pulpitu dla każdej wartości z inkrementowanym numerem w nazwie właściwości. Domyślnie: 1, 2, 4, 5. Wartości „Wskazówka" i „Skala" nie są obsługiwane, jeśli jednocześnie: - nie ustawiono obiektu pola widżetu pulpitu dla *Pokaż* z wartością „Łuk wartości"; - parametr konfiguracji zaawansowanej *Pokaż łuk* jest ustawiony na „Wyłączone". Parametry konfiguracji zaawansowanej dla opcji *Pokaż* nie są obsługiwane, jeśli nie ustawiono obiektów pól widżetu pulpitu z odpowiednimi wartościami.

Parametr	type	name	value
Nadpisz host	1	override_hostid._reference	`ABCDE._hostid` - ustawia kompatybilny widżet (z parametrem *Reference* ustawionym na "`ABCDE`") jako źródło danych dla hostów; `DASHBOARD._hostid` - ustawia selektor hosta pulpitu jako źródło danych dla hostów. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.

Konfiguracja zaawansowana

Poniższe zaawansowane parametry konfiguracji są obsługiwane przez widżet *Gauge*.

Note:
Liczba w nazwie właściwości *Thresholds* (np. thresholds.0.color) odnosi się do miejsca progu na liście posortowanej rosnąco. Jeśli jednak progi zostaną skonfigurowane w innej kolejności, wartości zostaną posortowane rosnąco po zaktualizowaniu konfiguracji widżetu w frontendzie Zabbix (np. `"thresholds.0.threshold":"5"` → `"thresholds.0.threshold":"1"`; `"thresholds.1.threshold":"1"` → `"thresholds.1.threshold": "5"`).

Parametr	type	name	value
Kąt	0	angle	Możliwe wartości: 180 *(domyślnie)* lub 270.
Opis			
Opis	1	description	Dowolna wartość tekstowa, w tym makra. Obsługiwane makra: {HOST.*}, {ITEM.*}, {INVENTORY.*}, makra użytkownika. Domyślnie: {ITEM.NAME}.
Rozmiar	0	desc_size	Możliwe wartości z zakresu 1-100. Domyślnie: 15.
Pozycja pionowa	0	desc_v_pos	0 - Góra; 1 - *(domyślnie)* Dół.
Pogrubienie	0	desc_bold	0 - *(domyślnie)* Wyłączone; 1 - Włączone.
Kolor	1	desc_color	Szesnastkowy kod koloru (np. `FF0000`). Domyślnie: `""` (puste).
Wartość			
Miejsca dziesiętne	0	decimal_places	Możliwe wartości z zakresu 1-10. Domyślnie: 2.
Rozmiar	0	value_size	Możliwe wartości z zakresu 1-100. Domyślnie: 25.
Pogrubienie	0	value_bold	0 - *(domyślnie)* Wyłączone; 1 - Włączone.
Kolor	1	value_color	Szesnastkowy kod koloru (np. `FF0000`). Domyślnie: `""` (puste).
Jednostki			
Jednostki (pole wyboru)	0	units_show	0 - Wyłączone; 1 - *(domyślnie)* Włączone.
Jednostki (wartość)	1	units	Dowolna wartość tekstowa. Zachowanie parametru: - *obsługiwane*, jeśli *Jednostki* (pole wyboru) jest ustawione na "Włączone"

Parametr	type	name	value
Rozmiar	0	units_size	Możliwe wartości z zakresu 1-100. Domyślnie: 25. Zachowanie parametru: - *obsługiwane*, jeśli *Jednostki* (pole wyboru) jest ustawione na ”Włączone”
Pogrubienie	0	units_bold	0 - *(domyślnie)* Wyłączone; 1 - Włączone. Zachowanie parametru: - *obsługiwane*, jeśli *Jednostki* (pole wyboru) jest ustawione na ”Włączone”
Pozycja	0	units_pos	0 - Przed wartością; 1 - Nad wartością; 2 - *(domyślnie)* Za wartością; 3 - Pod wartością. Zachowanie parametru: - *obsługiwane*, jeśli *Jednostki* (pole wyboru) jest ustawione na ”Włączone”
Kolor	1	units_color	Ten parametr jest ignorowany, jeśli jest ustawiony na jedną z następujących jednostek związanych z czasem: unixtime, uptime, s. Szesnastkowy kod koloru (np. FF0000). Domyślnie: "" (puste).
Łuk wartości			
Rozmiar łuku	0	value_arc_size	Możliwe wartości z zakresu 1-100. Domyślnie: 20.
Wskazówka			
Kolor	1	needle_color	Szesnastkowy kod koloru (np. FF0000). Domyślnie: "" (puste). Zachowanie parametru: - *obsługiwane*, jeśli ustawiono obiekt pola widżetu pulpitu dla *Pokaż* z wartością ”Value arc” lub *Pokaż łuk* jest ustawione na ”Włączone”
Skala			
Pokaż jednostki	0	scale_show_units	0 - Wyłączone; 1 - *(domyślnie)* Włączone. Zachowanie parametru: - *obsługiwane*, jeśli *Jednostki* (pole wyboru) jest ustawione na ”Włączone” oraz ustawiono obiekt pola widżetu pulpitu dla *Pokaż* z wartością ”Value arc” lub *Pokaż łuk* jest ustawione na ”Włączone”
Rozmiar	0	scale_size	Możliwe wartości z zakresu 1-100. Domyślnie: 15. Zachowanie parametru: - *obsługiwane*, jeśli ustawiono obiekt pola widżetu pulpitu dla *Pokaż* z wartością ”Value arc” lub *Pokaż łuk* jest ustawione na ”Włączone”
Miejsca dziesiętne	0	scale_decimal_places	Możliwe wartości z zakresu 1-10. Domyślnie: 0. Zachowanie parametru: - *obsługiwane*, jeśli ustawiono obiekt pola widżetu pulpitu dla *Pokaż* z wartością ”Value arc” lub *Pokaż łuk* jest ustawione na ”Włączone”

Parametr	type	name	value
Progi			
Kolor	1	thresholds.0.color	Szesnastkowy kod koloru (np. FF0000).
Próg	1	thresholds.0.threshold	Dowolna wartość liczbowa. Obsługiwane są sufiksy (np. ”1d”, ”2w”, ”4K”, ”8G”).
Pokaż etykiety	0	th_show_labels	0 - *(domyślnie)* Wyłączone; 1 - Włączone. Zachowanie parametru: - *obsługiwane*, jeśli *Progi* są ustawione oraz ustawiono obiekt pola widżetu pulpitu dla *Pokaż* z wartością ”Value arc” lub *Pokaż łuk* jest ustawione na ”Włączone”
Pokaż łuk	0	th_show_arc	0 - *(domyślnie)* Wyłączone; 1 - Włączone. Zachowanie parametru: - *obsługiwane*, jeśli *Progi* są ustawione
Rozmiar łuku	0	th_arc_size	Możliwe wartości z zakresu 1-100. Domyślnie: 5. Zachowanie parametru: - *obsługiwane*, jeśli *Pokaż łuk* jest ustawione na ”Włączone”

Przykłady

Poniższe przykłady mają na celu jedynie opisanie konfiguracji obiektów pól widżetu pulpitu dla widżetu *Gauge*. Więcej informacji na temat konfiguracji pulpitu można znaleźć w `dashboard.create`.

Konfigurowanie widżetu *Gauge*

Skonfiguruj widżet *Gauge*, który wyświetla wartość pozycji dla pozycji „44474” (Interface enp0s3: Bits sent). Dodatkowo dostrój wizualnie widżet za pomocą wielu zaawansowanych opcji, w tym progów.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "dashboard.create",
    "params": {
        "name": "My dashboard",
        "display_period": 30,
        "auto_start": 1,
        "pages": [
            {
                "widgets": [
                    {
                        "type": "gauge",
                        "name": "Gauge",
                        "x": 0,
                        "y": 0,
                        "width": 18,
                        "height": 5,
                        "view_mode": 0,
                        "fields": [
                            {
                                "type": 4,
                                "name": "itemid.0",
                                "value": 44474
                            },
                            {
                                "type": 1,
                                "name": "min",
                                "value": "100000"
```

```
            },
            {
                "type": 1,
                "name": "max",
                "value": "1000000"
            },
            {
                "type": 0,
                "name": "show.0",
                "value": 1
            },
            {
                "type": 0,
                "name": "show.1",
                "value": 2
            },
            {
                "type": 0,
                "name": "show.2",
                "value": 3
            },
            {
                "type": 0,
                "name": "show.4",
                "value": 4
            },
            {
                "type": 0,
                "name": "show.5",
                "value": 5
            },
            {
                "type": 0,
                "name": "angle",
                "value": 270
            },
            {
                "type": 0,
                "name": "desc_size",
                "value": 10
            },
            {
                "type": 0,
                "name": "desc_bold",
                "value": 1
            },
            {
                "type": 0,
                "name": "decimal_places",
                "value": 0
            },
            {
                "type": 0,
                "name": "value_bold",
                "value": 1
            },
            {
                "type": 0,
                "name": "units_size",
                "value": 15
            },
            {
```

```
                            "type": 0,
                            "name": "units_pos",
                            "value": 3
                        },
                        {
                            "type": 1,
                            "name": "needle_color",
                            "value": "3C3C3C"
                        },
                        {
                            "type": 1,
                            "name": "thresholds.0.color",
                            "value": "FF465C"
                        },
                        {
                            "type": 1,
                            "name": "thresholds.0.threshold",
                            "value": "700000"
                        },
                        {
                            "type": 1,
                            "name": "thresholds.1.color",
                            "value": "FFD54F"
                        },
                        {
                            "type": 1,
                            "name": "thresholds.1.threshold",
                            "value": "500000"
                        },
                        {
                            "type": 1,
                            "name": "thresholds.2.color",
                            "value": "0EC9AC"
                        },
                        {
                            "type": 1,
                            "name": "thresholds.2.threshold",
                            "value": "100000"
                        },
                        {
                            "type": 0,
                            "name": "th_show_labels",
                            "value": 1
                        },
                        {
                            "type": 0,
                            "name": "th_show_arc",
                            "value": 1
                        },
                        {
                            "type": 0,
                            "name": "th_arc_size",
                            "value": 15
                        }
                    ]
                }
            ]
        }
    ],
    "userGroups": [
        {
            "usrgrpid": 7,
```

```
                "permission": 2
            }
        ],
        "users": [
            {
                "userid": 1,
                "permission": 3
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "3"
        ]
    },
    "id": 1
}
```

Zobacz także

- Pole widżetu pulpitu
- `dashboard.create`
- `dashboard.update`

7 Mapa geograficzna

Opis

Te parametry oraz możliwe wartości właściwości dla odpowiednich obiektów pól widgetu umożliwiają skonfigurowanie widgetu *Geomap* w metodach `dashboard.create` i `dashboard.update`.

Attention:
Właściwości `fields` widgetu nie są walidowane podczas tworzenia ani aktualizacji pulpitu. Pozwala to użytkownikom modyfikować wbudowane widgety i tworzyć własne widgety, ale jednocześnie wiąże się z ryzykiem nieprawidłowego tworzenia lub aktualizowania widgetów. Aby zapewnić pomyślne utworzenie lub zaktualizowanie widgetu *Geomap*, należy zapoznać się z działaniem parametrów opisanym w poniższych tabelach.

Parametry

Następujące parametry są obsługiwane dla widżetu *Geomap*.

Parametr	type	name	value
Interwał odświeżania	0	rf_rate	0 - Brak odświeżania; 10 - 10 sekund; 30 - 30 sekund; 60 - *(domyślnie)* 1 minuta; 120 - 2 minuty; 600 - 10 minut; 900 - 15 minut.

Parametr	type	name	value
Grupy hostów	2	groupids.0	ID grupy hostów. Uwaga: Aby skonfigurować wiele grup hostów, utwórz obiekt pola widżetu dashboardu dla każdej grupy hostów z inkrementowanym numerem w nazwie właściwości. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na dashboardzie szablonu.
Grupy hostów (widżet)	1	groupids._reference	Zamiast ID grupy hostów: `ABCDE._hostgroupids` - ustaw kompatybilny widżet (z parametrem *Reference* ustawionym na "`ABCDE`") jako źródło danych dla grup hostów. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na dashboardzie szablonu.
Hosty	3	hostids.0	ID hosta. Uwaga: Aby skonfigurować wiele hostów, utwórz obiekt pola widżetu dashboardu dla każdego hosta z inkrementowanym numerem w nazwie właściwości. W przypadku wielu hostów parametr *Grupy hostów* nie może być w ogóle skonfigurowany albo musi być skonfigurowany z co najmniej jedną grupą hostów, do której należą skonfigurowane hosty. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na dashboardzie szablonu.
Hosty (widżet/dashboard)	1	hostids._reference	Zamiast ID hosta: `DASHBOARD.hostids` - ustaw selektor hostów dashboardu jako źródło danych dla hostów; `ABCDE._hostids` - ustaw kompatybilny widżet (z parametrem *Reference* ustawionym na "`ABCDE`") jako źródło danych dla hostów. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na dashboardzie szablonu.
Tagi			
Typ obliczania	0	evaltype	0 - *(domyślnie)* And/Or; 2 - Or. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na dashboardzie szablonu.
Nazwa tagu	1	tags.0.tag	Dowolna wartość tekstowa. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście obliczania tagów. Zachowanie parametru: - *wymagany* przy konfigurowaniu *Tagów* Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na dashboardzie szablonu.

Parametr	type	name	value
Operator	0	tags.0.operator	0 - Zawiera; 1 - Równa się; 2 - Nie zawiera; 3 - Nie równa się; 4 - Istnieje; 5 - Nie istnieje. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście obliczania tagów. Zachowanie parametru: - *wymagany* przy konfigurowaniu *Tagów* Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na dashboardzie szablonu.
Wartość tagu	1	tags.0.value	Dowolna wartość tekstowa. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście obliczania tagów. Zachowanie parametru: - *wymagany* przy konfigurowaniu *Tagów* Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na dashboardzie szablonu.
Widok początkowy	1	default_view	Oddzielone przecinkami wartości *szerokości geograficznej*, *długości geograficznej*, *poziomu powiększenia* (*opcjonalnie*, możliwe wartości z zakresu 0-30). Przykład: `40.6892494,-74.0466891,10`.
Klastrowanie			
Tryb klastrowania	0	clustering_mode	0 - *(domyślnie)* Auto; 1 - Poziom powiększenia.
Poziom powiększenia klastrowania	0	clustering_zoom_level	Możliwe wartości z zakresu 0-30. Domyślnie: 0. Zachowanie parametru: - *obsługiwany* jeśli *Tryb klastrowania* jest ustawiony na "Poziom powiększenia"
Reference	1	reference	Dowolna wartość tekstowa składająca się z 5 znaków (np. `ABCDE` lub `JBPNL`). Ta wartość musi być unikalna w obrębie dashboardu, do którego należy widżet. Zachowanie parametru: - *wymagany*

Przykłady

Poniższe przykłady mają na celu jedynie opisanie konfiguracji obiektów pól widżetu pulpitu dla widżetu *Geomap*. Więcej informacji na temat konfiguracji pulpitu można znaleźć w `dashboard.create`.

Konfigurowanie widżetu *Geomap*

Skonfiguruj widżet *Geomap*, który wyświetla hosty z grup hostów „2" i „22" na podstawie następującej konfiguracji tagów: tag o nazwie „component" zawiera wartość „node", a tag o nazwie „location" jest równy wartości „New York". Dodatkowo ustaw początkowy widok mapy na współrzędne „40.6892494" (szerokość geograficzna), „-74.0466891" (długość geograficzna) z poziomem powiększenia „10".

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "dashboard.create",
```

```
    "params": {
        "name": "My dashboard",
        "display_period": 30,
        "auto_start": 1,
        "pages": [
            {
                "widgets": [
                    {
                        "type": "geomap",
                        "name": "Geomap",
                        "x": 0,
                        "y": 0,
                        "width": 36,
                        "height": 5,
                        "view_mode": 0,
                        "fields": [
                            {
                                "type": 2,
                                "name": "groupids.0",
                                "value": 22
                            },
                            {
                                "type": 2,
                                "name": "groupids.1",
                                "value": 2
                            },
                            {
                                "type": 1,
                                "name": "default_view",
                                "value": "40.6892494,-74.0466891,10"
                            },
                            {
                                "type": 0,
                                "name": "evaltype",
                                "value": 2
                            },
                            {
                                "type": 1,
                                "name": "tags.0.tag",
                                "value": "component"
                            },
                            {
                                "type": 0,
                                "name": "tags.0.operator",
                                "value": 0
                            },
                            {
                                "type": 1,
                                "name": "tags.0.value",
                                "value": "node"
                            },
                            {
                                "type": 1,
                                "name": "tags.1.tag",
                                "value": "location"
                            },
                            {
                                "type": 0,
                                "name": "tags.1.operator",
                                "value": 1
                            },
                            {
```

```
                                "type": 1,
                                "name": "tags.1.value",
                                "value": "New York"
                            }
                        ]
                    }
                ]
            }
        ],
        "userGroups": [
            {
                "usrgrpid": 7,
                "permission": 2
            }
        ],
        "users": [
            {
                "userid": 1,
                "permission": 3
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "3"
        ]
    },
    "id": 1
}
```

Zobacz także

- Pole widżetu pulpitu
- `dashboard.create`
- `dashboard.update`

8 Graph

Opis

Te parametry oraz możliwe wartości właściwości dla odpowiednich obiektów pól widgetu umożliwiają skonfigurowanie widgetu *Graph* w metodach `dashboard.create` i `dashboard.update`.

Attention:
Właściwości `fields` widgetu nie są walidowane podczas tworzenia ani aktualizacji pulpitu. Pozwala to użytkownikom modyfikować wbudowane widgety i tworzyć własne widgety, ale jednocześnie wprowadza ryzyko nieprawidłowego tworzenia lub aktualizowania widgetów. Aby zapewnić pomyślne utworzenie lub zaktualizowanie widgetu *Graph*, zapoznaj się z zachowaniem parametrów opisanym w poniższych tabelach.

Parametry

Dla widżetu *Graph* obsługiwane są następujące parametry.

Parametr	type	name	value
Interwał odświeżania	0	rf_rate	0 - Bez odświeżania; 10 - 10 sekund; 30 - 30 sekund; 60 - *(domyślnie)* 1 minuta; 120 - 2 minuty; 600 - 10 minut; 900 - 15 minut.
Odwołanie	1	reference	Dowolna wartość tekstowa składająca się z 5 znaków (np. `ABCDE` lub `JBPNL`). Ta wartość musi być unikalna w obrębie pulpitu, do którego należy widżet. Zachowanie parametru: - *wymagane*

Zestaw danych

Następujące parametry są obsługiwane przy konfigurowaniu *Zestawu danych*.

Note:
Pierwsza liczba w nazwie właściwości (np. ds.0.hosts.0, ds.0.items.0) oznacza konkretny zestaw danych, natomiast druga liczba, jeśli występuje, oznacza skonfigurowany host lub pozycję.

Parametr	type	name	value
Typ zestawu danych	0	ds.0.dataset_type	0 - Lista pozycji; 1 - *(domyślnie)* Wzorce pozycji.
Pozycje	4	ds.0.itemids.0	ID pozycji. Podczas konfigurowania widżetu na pulpicie szablonu należy ustawić tylko pozycje skonfigurowane w szablonie. Uwaga: Aby skonfigurować wiele pozycji, utwórz obiekt pola widżetu pulpitu dla każdej pozycji z inkrementowanym numerem w nazwie właściwości. Zachowanie parametru: - *wymagane*, jeśli *Typ zestawu danych* jest ustawiony na "Lista pozycji", a *Pozycje (widżet)* nie jest ustawione
Pozycje (widżet)	1	ds.0.itemids.0._reference	Zamiast ID pozycji: `ABCDE._itemid` - ustaw kompatybilny widżet (z parametrem *Reference* ustawionym na "`ABCDE`") jako źródło danych dla pozycji. Uwaga: Aby skonfigurować wiele widżetów, utwórz obiekt pola widżetu pulpitu dla każdego widżetu z inkrementowanym numerem w nazwie właściwości. Zachowanie parametru: - *wymagane*, jeśli *Typ zestawu danych* jest ustawiony na "Lista pozycji", a *Pozycje* nie jest ustawione
Kolor	1	ds.0.color.0	Szesnastkowy kod koloru (np. `FF0000`). Zachowanie parametru: - *wymagane*, jeśli *Typ zestawu danych* jest ustawiony na "Lista pozycji"

Parametr	type	name	value
Wzorce hostów	1	ds.0.hosts.0	Nazwa lub wzorzec hosta (np. ”Zabbix*”). Zachowanie parametru: - *wymagane*, jeśli *Typ zestawu danych* jest ustawiony na ”Wzorce pozycji” Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Wzorce pozycji	1	ds.0.items.0	Nazwa lub wzorzec pozycji (np. ”*: Number of processed *values per second”). Podczas konfigurowania widżetu na pulpicie szablonu należy ustawić tylko wzorce dla pozycji skonfigurowanych w szablonie. Zachowanie parametru: - *wymagane*, jeśli *Typ zestawu danych* jest ustawiony na ”Wzorce pozycji”
Kolor	1	ds.0.color	Szesnastkowy kod koloru (np. `FF0000`). Zachowanie parametru: - *obsługiwane*, jeśli *Typ zestawu danych* jest ustawiony na ”Wzorce pozycji”, a *Paleta kolorów* nie jest ustawiona
Paleta kolorów	0	ds.0.color_palette	Indeks palety kolorów. Możliwe wartości mieszczą się w zakresie 0-11. Domyślnie: 0. Zachowanie parametru: - *obsługiwane*, jeśli *Typ zestawu danych* jest ustawiony na ”Wzorce pozycji”, a *Kolor* nie jest ustawiony
Rysowanie	0	ds.0.type	0 - *(domyślnie)* Linia; 1 - Punkty; 2 - Schodkowy; 3 - Słupkowy.
Skumulowany	0	ds.0.stacked	0 - *(domyślnie)* Wyłączone; 1 - Włączone. Zachowanie parametru: - *obsługiwane*, jeśli *Rysowanie* jest ustawione na ”Linia”, ”Schodkowy” lub ”Słupkowy”
Szerokość	0	ds.0.width	Możliwe wartości mieszczą się w zakresie 1-10. Domyślnie: 1. Zachowanie parametru: - *obsługiwane*, jeśli *Rysowanie* jest ustawione na ”Linia” lub ”Schodkowy”
Rozmiar punktu	0	ds.0.pointsize	Możliwe wartości mieszczą się w zakresie 1-10. Domyślnie: 3. Zachowanie parametru: - *obsługiwane*, jeśli *Rysowanie* jest ustawione na ”Punkty”
Przezroczystość	0	ds.0.transparency	Możliwe wartości mieszczą się w zakresie 1-10. Domyślnie: 5.

Parametr	type	name	value
Wypełnienie	0	ds.0.fill	Możliwe wartości mieszczą się w zakresie 1-10. Domyślnie: 3. Zachowanie parametru: - *obsługiwane*, jeśli *Rysowanie* jest ustawione na ”Linia” lub ”Schodkowy”
Brakujące dane	0	ds.0.missingdatafunc	0 - *(domyślnie)* Brak; 1 - Połączone; 2 - Traktuj jako 0; 3 - Ostatnia znana wartość. Zachowanie parametru: - *obsługiwane*, jeśli *Rysowanie* jest ustawione na ”Linia” lub ”Schodkowy”
Nadpisanie hosta	1	ds.0.override_hostid	ABCDE - ustaw `ABCDE._hostid` (z parametrem ”Reference” ustawionym na ”ABCDE”) jako źródło danych dla hostów; `DASHBOARD._hostid` - ustaw selektor hosta pulpitu jako źródło danych dla hostów. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Oś Y	0	ds.0.axisy	0 - *(domyślnie)* Lewa; 1 - Prawa.
Odwróć wartości	0	ds.0.invert_values	0 - (domyślnie) Wyłączone; 1 - Włączone.
Przesunięcie czasu	1	ds.0.timeshift	Prawidłowy ciąg czasu (np. 3600, 1h itd.). Możesz używać sufiksów czasu. Dozwolone są również wartości ujemne. Domyślnie: "" (puste).
Funkcja agre-gacji	0	ds.0.aggregate_function	0 - *(domyślnie)* nieużywane; 1 - min; 2 - max; 3 - avg; 4 - count; 5 - sum; 6 - first; 7 - last.
Interwał agre-gacji	1	ds.0.aggregate_interval	Prawidłowy ciąg czasu (np. 3600, 1h itd.). Możesz używać sufiksów czasu. Domyślnie: 1h.
Agreguj	0	ds.0.aggregate_grouping	0 - *(domyślnie)* Każda pozycja; 1 - Zestaw danych. Zachowanie parametru: - *obsługiwane*, jeśli *Funkcja agregacji* jest ustawiona na ”min”, ”max”, ”avg”, ”count”, ”sum”, ”first” lub ”last”
Przybliżenie	0	ds.0.approximation	1 - min; 2 - *(domyślnie)* avg; 4 - max; 7 - all.
Etykieta zestawu danych	1	ds.0.data_set_label	Dowolna wartość tekstowa. Domyślnie: "" (puste).
Tagi pozy-cji			
Typ oceny	0	ds.0.item_tags_evaltype	0 - *(domyślnie)* And/Or; 2 - Or.

Parametr	type	name	value
Nazwa tagu	1	ds.0.item_tags.0.tag	Dowolna wartość tekstowa. Uwaga: Liczba w nazwie właściwości odnosi się do kolejności tagu na liście oceny tagów. Zachowanie parametru: - *wymagane*, jeśli konfigurowane są *Tagi pozycji*
Operator	0	ds.0.item_tags.0.operator	0 - Zawiera; 1 - Równa się; 2 - Nie zawiera; 3 - Nie równa się; 4 - Istnieje; 5 - Nie istnieje. Uwaga: Liczba w nazwie właściwości odnosi się do kolejności tagu na liście oceny tagów. Zachowanie parametru: - *wymagane*, jeśli konfigurowane są *Tagi pozycji*
Wartość tagu	1	ds.0.item_tags.0.value	Dowolna wartość tekstowa. Uwaga: Liczba w nazwie właściwości odnosi się do kolejności tagu na liście oceny tagów. Zachowanie parametru: - *wymagane*, jeśli konfigurowane są *Tagi pozycji*

Opcje wyświetlania

Następujące parametry są obsługiwane przy konfigurowaniu *Opcji wyświetlania*.

Parametr	type	name	value
Wybór danych historycznych	0	source	0 - *(domyślnie)* Auto; 1 - Historia; 2 - Trendy.
Proste wyzwalacze	0	simple_triggers	0 - *(domyślnie)* Wyłączone; 1 - Włączone.
Czas pracy	0	working_time	0 - *(domyślnie)* Wyłączone; 1 - Włączone.
Nazwy hostów w etykietach	0	show_hostnames	0 - *(domyślnie)* Auto; 1 - Pokaż; 2 - Ukryj. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Linia percentyla (lewa)			
Status	0	percentile_left	0 - *(domyślnie)* Wyłączone; 1 - Włączone. Zachowanie parametru: - *obsługiwane*, jeśli *Oś Y* (w konfiguracji *Zestawu danych*) jest ustawiona na „Lewa”

Parametr	type	name	value
Wartość	0	percentile_left_value	Możliwe wartości mieszczą się w zakresie od 1 do 100. Zachowanie parametru: - *obsługiwane*, jeśli *Oś Y* (w konfiguracji *Zestawu danych*) jest ustawiona na „Lewa”
Linia per-centyla (prawa)			
Status	0	percentile_right	0 - *(domyślnie)* Wyłączone; 1 - Włączone. Zachowanie parametru: - *obsługiwane*, jeśli *Oś Y* (w konfiguracji *Zestawu danych*) jest ustawiona na „Prawa”
Wartość	0	percentile_right_value	Możliwe wartości mieszczą się w zakresie od 1 do 100. Zachowanie parametru: - *obsługiwane*, jeśli *Oś Y* (w konfiguracji *Zestawu danych*) jest ustawiona na „Prawa”

Okres czasu

Następujące parametry są obsługiwane przy konfigurowaniu *Okresu czasu*.

Parametr	type	name	value
Okres czasu	1	time_period._referenc	`DASHBOARD._timeperiod` - ustaw selektor okresu czasu pulpitu jako źródło danych; `ABCDE._timeperiod` - ustaw kompatybilny widget (z parametrem *Reference* ustawionym na ”ABCDE”) jako źródło danych. Domyślnie: `DASHBOARD._timeperiod` Alternatywnie można ustawić okres czasu tylko w parametrach *Od* i *Do*.
Od	1	time_period.from	Prawidłowy ciąg czasu w składni czasu bezwzględnego (`YYYY-MM-DD hh:mm:ss`) lub względnego (`now`, `now/d`, `now/w-1w` itd.). Zachowanie parametru: - *obsługiwany*, jeśli *Okres czasu* nie jest ustawiony - *wymagany*, jeśli ustawiono `time_period.to`
Do	1	time_period.to	Prawidłowy ciąg czasu w składni czasu bezwzględnego (`YYYY-MM-DD hh:mm:ss`) lub względnego (`now`, `now/d`, `now/w-1w` itd.). Zachowanie parametru: - *obsługiwany*, jeśli *Okres czasu* nie jest ustawiony - *wymagany*, jeśli ustawiono `time_period.from`

Osie

Następujące parametry są obsługiwane przy konfigurowaniu *Osi*.

Parametr	type	name	value
Lewe Y	0	lefty	0 - Wyłączone; 1 - *(domyślnie)* Włączone. Zachowanie parametru: - *obsługiwane*, jeśli *Oś Y* (w konfiguracji *Zbiór danych*) jest ustawiona na „Lewa”
Prawe Y	0	righty	0 - *(domyślnie)* Wyłączone; 1 - Włączone. Zachowanie parametru: - *obsługiwane*, jeśli *Oś Y* (w konfiguracji *Zbiór danych*) jest ustawiona na „Prawa”
Skala	0	lefty_scale righty_scale	0 - *(domyślnie)* Liniowa; 1 - Logarytmiczna.
Min	1	lefty_min righty_min	Dowolna wartość liczbowa. Domyślnie: "" (puste).
Max	1	lefty_max righty_max	Dowolna wartość liczbowa. Domyślnie: "" (puste).
Jednostki (typ)	0	lefty_units righty_units	0 - *(domyślnie)* Auto; 1 - Statyczne.
Jednostki (wartość)	1	lefty_static_units righty_static_units	Dowolna wartość tekstowa. Domyślnie: "" (puste).
Oś X	0	xaxis	0 - Wyłączona; 1 - *(domyślnie)* Włączona.

Legenda

Następujące parametry są obsługiwane przy konfigurowaniu *Legendy*.

Parametr	type	name	value
Pokaż legendę	0	legend	0 - Wyłączone; 1 - *(domyślnie)* Włączone.
Wyświetl min/avg/max	0	legend_statistic	0 - *(domyślnie)* Wyłączone; 1 - Włączone. Zachowanie parametru: - *obsługiwane*, jeśli *Pokaż legendę* jest ustawione na ”Włączone”
Pokaż funkcję agregacji	0	legend_aggregation	0 - *(domyślnie)* Wyłączone; 1 - Włączone. Zachowanie parametru: - *obsługiwane*, jeśli *Pokaż legendę* jest ustawione na ”Włączone”
Wiersze	0	legend_lines_mode	0 - *(domyślnie)* Stałe; 1 - Zmienne. Zachowanie parametru: - *obsługiwane*, jeśli *Pokaż legendę* jest ustawione na ”Włączone”

Parametr	type	name	value
Liczba wierszy/ Maksymalna liczba wierszy	0	legend_lines	Możliwe wartości mieszczą się w zakresie od 1 do 10. Domyślnie: 1. Zachowanie parametru: - *obsługiwane*, jeśli *Pokaż legendę* jest ustawione na ”Włączone”
Liczba kolumn	0	legend_columns	Możliwe wartości mieszczą się w zakresie od 1 do 4. Domyślnie: 4. Zachowanie parametru: - *obsługiwane*, jeśli *Pokaż legendę* jest ustawione na ”Włączone”, a *Wyświetl min/avg/max* jest ustawione na ”Wyłączone”

Problemy

Następujące parametry są obsługiwane przy konfigurowaniu *Problemów*.

Parametr	type	name	value
Pokaż problemy	0	show_problems	0 - *(domyślnie)* Wyłączone; 1 - Włączone.
Tylko wybrane pozycje	0	graph_item_problems	0 - Wyłączone; 1 - *(domyślnie)* Włączone.
Hosty problemów	1	problemhosts.0	Nazwa hosta. Uwaga: Liczba w nazwie właściwości odnosi się do skonfigurowanego hosta. Aby skonfigurować wiele hostów, utwórz obiekt pola widżetu pulpitu dla każdego hosta z kolejnym numerem w nazwie właściwości. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Poziom ważności	0	severities.0	0 - Niesklasyfikowane; 1 - Informacja; 2 - Ostrzeżenie; 3 - Średni; 4 - Wysoki; 5 - Katastrofa. Domyślnie: puste (wszystkie włączone). Uwaga: Aby skonfigurować wiele wartości, utwórz obiekt pola widżetu pulpitu dla każdej wartości z kolejnym numerem w nazwie właściwości.
Problem	1	problem_name	Nazwa zdarzenia problemu (bez rozróżniania wielkości liter, pełna nazwa lub jej część).
Tagi problemu			
Typ oceny	0	evaltype	0 - *(domyślnie)* And/Or; 2 - Or.

Parametr	type	name	value
Nazwa tagu	1	tags.0.tag	Dowolna wartość tekstowa. Uwaga: Liczba w nazwie właściwości odnosi się do kolejności tagu na liście oceny tagów. Zachowanie parametru: - *wymagane* podczas konfigurowania *Tagów problemu*
Operator	0	tags.0.operator	0 - Zawiera; 1 - Równa się; 2 - Nie zawiera; 3 - Nie równa się; 4 - Istnieje; 5 - Nie istnieje. Uwaga: Liczba w nazwie właściwości odnosi się do kolejności tagu na liście oceny tagów. Zachowanie parametru: - *wymagane* podczas konfigurowania *Tagów problemu*
Wartość tagu	1	tags.0.value	Dowolna wartość tekstowa. Uwaga: Liczba w nazwie właściwości odnosi się do kolejności tagu na liście oceny tagów. Zachowanie parametru: - *wymagane* podczas konfigurowania *Tagów problemu*

Nadpisania

Następujące parametry są obsługiwane przy konfigurowaniu *Nadpisań*.

Note:
Pierwsza liczba w nazwie właściwości (np. or.0.hosts.0, or.0.items.0) reprezentuje konkretny zestaw danych, natomiast druga liczba, jeśli występuje, reprezentuje skonfigurowany host lub pozycję.

Parametr	type	name	value
Wzorce hostów	1	or.0.hosts.0	Nazwa lub wzorzec hosta (np. `Zabbix*`). Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu. Zachowanie parametru: - *wymagany* przy konfigurowaniu *Nadpisań*
Wzorce pozycji	1	or.0.items.0	Nazwa lub wzorzec pozycji (np. `*: Number of processed *values per second`). Podczas konfigurowania widżetu na pulpicie szablonu należy ustawić tylko wzorce dla pozycji skonfigurowanych w szablonie. Zachowanie parametru: - *wymagany* przy konfigurowaniu *Nadpisań*
Kolor bazowy	1	or.0.color	Szesnastkowy kod koloru (np. `FF0000`).
Szerokość	0	or.0.width	Możliwe wartości mieszczą się w zakresie 1-10.
Rysowanie	0	or.0.type	0 - Linia; 1 - Punkty; 2 - Schodkowy; 3 - Słupki.
Przezroczystość	0	or.0.transparency	Możliwe wartości mieszczą się w zakresie 1-10.
Wypełnienie	0	or.0.fill	Możliwe wartości mieszczą się w zakresie 1-10.
Rozmiar punktu	0	or.0.pointsize	Możliwe wartości mieszczą się w zakresie 1-10.

Parametr	type	name	value
Brakujące dane	0	or.0.missingdatafunc	0 - Brak; 1 - Połączone; 2 - Traktuj jako 0; 3 - Ostatnia znana wartość.
Oś Y	0	or.0.axisy	0 - Lewa; 1 - Prawa.
Odwróć wartości	0	or.0.invert_values	0 - (domyślnie) Wyłączone; 1 - Włączone.
Przesunięcie czasu	1	or.0.timeshift	Prawidłowy ciąg czasu (np. 3600, 1h itd.). Możesz używać sufiksów czasu. Wartości ujemne są dozwolone.

Przykłady

Poniższe przykłady mają na celu jedynie opisanie konfiguracji obiektów pól widżetu pulpitu dla widżetu *Graph*. Aby uzyskać więcej informacji na temat konfiguracji pulpitu, zobacz `dashboard.create`.

Konfigurowanie widżetu *Graph*

Skonfiguruj widżet *Graph* w następujący sposób:

- 2 zestawy danych dla łącznie 9 pozycji na 1 hoście.
- Pierwszy zestaw danych jest typu „Item list” i składa się z 3 pozycji, które są reprezentowane przez linie o różnych kolorach, ale tej samej szerokości, przezroczystości i wypełnieniu.
- Drugi zestaw danych jest typu „Item patterns”, składa się z 6 pozycji, ma skonfigurowaną agregację i jest reprezentowany przez linię z niestandardowym kolorem, szerokością, przezroczystością i wypełnieniem.
- Drugi zestaw danych ma również niestandardową etykietę zestawu danych.
- Dane na wykresie są wyświetlane dla okresu ostatnich 3 godzin.
- Problemy na wykresie są wyświetlane tylko dla skonfigurowanych pozycji.
- Wykres ma dwie osie Y, z których prawa oś Y wyświetla wartości tylko dla drugiego zestawu danych.
- Legenda wykresu wyświetla skonfigurowane pozycje w 4 wierszach, a także minimalne, maksymalne i średnie wartości zestawów danych.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "dashboard.create",
    "params": {
        "name": "My dashboard",
        "display_period": 30,
        "auto_start": 1,
        "pages": [
            {
                "widgets": [
                    {
                        "type": "svggraph",
                        "name": "Graph",
                        "x": 0,
                        "y": 0,
                        "width": 36,
                        "height": 5,
                        "view_mode": 0,
                        "fields": [
                            {
                                "type": 0,
                                "name": "ds.0.dataset_type",
                                "value": 0
                            },
                            {
                                "type": 4,
                                "name": "ds.0.itemids.0",
                                "value": 23264
                            },
                            {
```

```
            "type": 1,
            "name": "ds.0.color.0",
            "value": "FF0000"
        },
        {
            "type": 4,
            "name": "ds.0.itemids.1",
            "value": 23269
        },
        {
            "type": 1,
            "name": "ds.0.color.1",
            "value": "BF00FF"
        },
        {
            "type": 4,
            "name": "ds.0.itemids.2",
            "value": 23257
        },
        {
            "type": 1,
            "name": "ds.0.color.2",
            "value": "0040FF"
        },
        {
            "type": 0,
            "name": "ds.0.width",
            "value": 3
        },
        {
            "type": 0,
            "name": "ds.0.transparency",
            "value": 3
        },
        {
            "type": 0,
            "name": "ds.0.fill",
            "value": 1
        },
        {
            "type": 1,
            "name": "ds.1.hosts.0",
            "value": "Zabbix server"
        },
        {
            "type": 1,
            "name": "ds.1.items.0",
            "value": "*: Number of processed *values per second"
        },
        {
            "type": 1,
            "name": "ds.1.color",
            "value": "000000"
        },
        {
            "type": 0,
            "name": "ds.1.transparency",
            "value": 0
        },
        {
            "type": 0,
            "name": "ds.1.fill",
```

```
            "value": 0
        },
        {
            "type": 0,
            "name": "ds.1.axisy",
            "value": 1
        },
        {
            "type": 0,
            "name": "ds.1.aggregate_function",
            "value": 3
        },
        {
            "type": 1,
            "name": "ds.1.aggregate_interval",
            "value": "1m"
        },
        {
            "type": 0,
            "name": "ds.1.aggregate_grouping",
            "value": 1
        },
        {
            "type": 1,
            "name": "ds.1.data_set_label",
            "value": "Number of processed values per second"
        },
        {
            "type": 0,
            "name": "graph_time",
            "value": 1
        },
        {
            "type": 1,
            "name": "time_period.from",
            "value": "now-3h"
        },
        {
            "type": 1,
            "name": "time_period.to",
            "value": "now"
        },
        {
            "type": 0,
            "name": "legend_statistic",
            "value": 1
        },
        {
            "type": 0,
            "name": "legend_lines",
            "value": 4
        },
        {
            "type": 0,
            "name": "show_problems",
            "value": 1
        },
        {
            "type": 1,
            "name": "reference",
            "value": "YZABC"
        }
```

```
                        ]
                    }
                ]
            }
        ],
        "userGroups": [
            {
                "usrgrpid": 7,
                "permission": 2
            }
        ],
        "users": [
            {
                "userid": 1,
                "permission": 3
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "3"
        ]
    },
    "id": 1
}
```

Zobacz także

- Pole widżetu pulpitu
- `dashboard.create`
- `dashboard.update`

9 Graph (classic)

Opis

Te parametry oraz możliwe wartości właściwości dla odpowiednich obiektów pól widgetu umożliwiają skonfigurowanie widgetu *Graph (classic)* w metodach `dashboard.create` i `dashboard.update`.

Attention:
Właściwości `fields` widgetu nie są walidowane podczas tworzenia ani aktualizacji pulpitu. Pozwala to użytkownikom modyfikować wbudowane widgety i tworzyć własne widgety, ale jednocześnie wprowadza ryzyko nieprawidłowego tworzenia lub aktualizowania widgetów. Aby zapewnić pomyślne utworzenie lub zaktualizowanie widgetu *Graph (classic)*, zapoznaj się z zachowaniem parametrów opisanym w poniższych tabelach.

Parametry

Następujące parametry są obsługiwane dla widżetu *Wykres (klasyczny)*.

Parametr	type	name	value
Interwał odświeżania	0	rf_rate	0 - Bez odświeżania; 10 - 10 sekund; 30 - 30 sekund; 60 - *(domyślnie)* 1 minuta; 120 - 2 minuty; 600 - 10 minut; 900 - 15 minut.
Źródło	0	source_type	0 - *(domyślnie)* Wykres; 1 - Wykres prosty.
Wykres	6	graphid.0	ID wykresu. Zachowanie parametru: - *wymagany*, jeśli *Źródło* jest ustawione na "Wykres"
Wykres (widżet)	1	graphid._reference	Zamiast ID wykresu: `ABCDE._graphid` - ustaw kompatybilny widżet (z parametrem *Odwołanie* ustawionym na "ABCDE") jako źródło danych dla wykresów. Zachowanie parametru: - *wymagany*, jeśli *Źródło* jest ustawione na "Wykres prosty", a *Wykres* nie jest ustawiony
Pozycja	4	itemid.0	ID pozycji. Zachowanie parametru: - *wymagany*, jeśli *Źródło* jest ustawione na "Wykres prosty", a *Pozycja (widżet)* nie jest ustawiona
Pozycja (widżet)	1	itemid._reference	Zamiast ID pozycji: `ABCDE._itemid` - ustaw kompatybilny widżet (z parametrem *Odwołanie* ustawionym na "ABCDE") jako źródło danych dla pozycji. Zachowanie parametru: - *wymagany*, jeśli *Źródło* jest ustawione na "Wykres prosty", a *Pozycja* nie jest ustawiona
Okres czasu	1	time_period._reference	`DASHBOARD._timeperiod` - ustaw selektor okresu czasu pulpitu jako źródło danych; `ABCDE._timeperiod` - ustaw kompatybilny widżet (z parametrem *Odwołanie* ustawionym na "ABCDE") jako źródło danych. Domyślnie: `DASHBOARD._timeperiod` Alternatywnie możesz ustawić okres czasu tylko w parametrach *Od* i *Do*.
Od	1	time_period.from	Prawidłowy ciąg czasu w składni bezwzględnej (`YYYY-MM-DD hh:mm:ss`) lub względnej (`now`, `now/d`, `now/w-1w` itd.). Zachowanie parametru: - *obsługiwany*, jeśli *Okres czasu* nie jest ustawiony - *wymagany*, jeśli ustawiono `time_period.to`
Do	1	time_period.to	Prawidłowy ciąg czasu w składni bezwzględnej (`YYYY-MM-DD hh:mm:ss`) lub względnej (`now`, `now/d`, `now/w-1w` itd.). Zachowanie parametru: - *obsługiwany*, jeśli *Okres czasu* nie jest ustawiony - *wymagany*, jeśli ustawiono `time_period.from`
Pokaż legendę	0	show_legend	0 - Wyłączone; 1 - *(domyślnie)* Włączone.

Parametr	type	name	value
Nadpisz host	1	override_hostid._reference	`ABCDE._hostid` - ustaw kompatybilny widżet (z parametrem *Odwołanie* ustawionym na "ABCDE") jako źródło danych dla hostów; `DASHBOARD._hostid` - ustaw selektor hosta pulpitu jako źródło danych dla hostów. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Odwołanie	1	reference	Dowolna wartość tekstowa składająca się z 5 znaków (np. `ABCDE` lub `JBPNL`). Ta wartość musi być unikalna w obrębie pulpitu, do którego należy widżet. Zachowanie parametru: - *wymagany*

Przykłady

Poniższe przykłady mają na celu jedynie opisanie konfiguracji obiektów pól widżetu pulpitu dla widżetu *Wykres (klasyczny)*. Aby uzyskać więcej informacji na temat konfigurowania pulpitu nawigacyjnego, zobacz `dashboard.create`.

Konfigurowanie widżetu *Graph (classic)*

Skonfiguruj widżet *Graph (classic)*, który wyświetla prosty wykres dla pozycji „42269".

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "dashboard.create",
    "params": {
        "name": "My dashboard",
        "display_period": 30,
        "auto_start": 1,
        "pages": [
            {
                "widgets": [
                    {
                        "type": "graph",
                        "name": "Graph (classic)",
                        "x": 0,
                        "y": 0,
                        "width": 36,
                        "height": 5,
                        "view_mode": 0,
                        "fields": [
                            {
                                "type": 0,
                                "name": "source_type",
                                "value": 1
                            },
                            {
                                "type": 4,
                                "name": "itemid.0",
                                "value": 42269
                            },
                            {
                                "type": 1,
                                "name": "reference",
                                "value": "RSTUV"
                            }
                        ]
                    }
                ]
            }
```

```
        ],
        "userGroups": [
            {
                "usrgrpid": 7,
                "permission": 2
            }
        ],
        "users": [
            {
                "userid": 1,
                "permission": 3
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "3"
        ]
    },
    "id": 1
}
```

Zobacz także

- Pole widżetu pulpitu
- `dashboard.create`
- `dashboard.update`

10 Graph prototype

Opis

Te parametry oraz możliwe wartości właściwości dla odpowiednich obiektów pól widgetu umożliwiają skonfigurowanie widgetu *Graph prototype* w metodach `dashboard.create` i `dashboard.update`.

Attention:
Właściwości `fields` widgetu nie są walidowane podczas tworzenia ani aktualizacji dashboardu. Pozwala to użytkownikom modyfikować wbudowane widgety i tworzyć niestandardowe widgety, ale jednocześnie wprowadza ryzyko nieprawidłowego tworzenia lub aktualizowania widgetów. Aby zapewnić pomyślne utworzenie lub zaktualizowanie widgetu *Graph prototype*, zapoznaj się z zachowaniem parametrów opisanym w poniższych tabelach.

Parametry

Następujące parametry są obsługiwane dla widżetu *Prototyp wykresu*.

Parametr	type	name	value
Interwał odświeżania	0	rf_rate	0 - Bez odświeżania; 10 - 10 sekund; 30 - 30 sekund; 60 - *(domyślnie)* 1 minuta; 120 - 2 minuty; 600 - 10 minut; 900 - 15 minut.
Źródło	0	source_type	2 - *(domyślnie)* Prototyp wykresu; 3 - Prosty prototyp wykresu.

Parametr	type	name	value
Prototyp wykresu	7	graphid.0	ID prototypu wykresu. Zachowanie parametru: - *wymagany*, jeśli *Źródło* jest ustawione na ”Prototyp wykresu”
Prototyp pozycji	5	itemid.0	ID prototypu pozycji. Zachowanie parametru: - *wymagany*, jeśli *Źródło* jest ustawione na ”Prosty prototyp wykresu”
Okres czasu	1	time_period._reference	`DASHBOARD._timeperiod` - ustaw selektor okresu czasu pulpitu jako źródło danych; `ABCDE._timeperiod` - ustaw kompatybilny widżet (z parametrem *Reference* ustawionym na ”`ABCDE`”) jako źródło danych. Domyślnie: `DASHBOARD._timeperiod` Alternatywnie można ustawić okres czasu tylko w parametrach *Od* i *Do*.
Od	1	time_period.from	Prawidłowy ciąg czasu w składni bezwzględnej (`YYYY-MM-DD hh:mm:ss`) lub względnej (`now`, `now/d`, `now/w-1w` itd.). Zachowanie parametru: - *obsługiwany*, jeśli *Okres czasu* nie jest ustawiony - *wymagany*, jeśli ustawiono `time_period.to`
Do	1	time_period.to	Prawidłowy ciąg czasu w składni bezwzględnej (`YYYY-MM-DD hh:mm:ss`) lub względnej (`now`, `now/d`, `now/w-1w` itd.). Zachowanie parametru: - *obsługiwany*, jeśli *Okres czasu* nie jest ustawiony - *wymagany*, jeśli ustawiono `time_period.from`
Pokaż legendę	0	show_legend	0 - Wyłączone; 1 - *(domyślnie)* Włączone.
Nadpisz host	1	override_hostid._reference	`ABCDE._hostid` - ustaw kompatybilny widżet (z parametrem *Reference* ustawionym na ”`ABCDE`”) jako źródło danych dla hostów; `DASHBOARD._hostid` - ustaw selektor hosta pulpitu jako źródło danych dla hostów. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Kolumny	0	columns	Możliwe wartości mieszczą się w zakresie 1-24. Domyślnie: 2.
Wiersze	0	rows	Możliwe wartości mieszczą się w zakresie 1-16. Domyślnie: 1.
Reference	1	reference	Dowolna wartość tekstowa składająca się z 5 znaków (na przykład `ABCDE` lub `JBPNL`). Ta wartość musi być unikalna w obrębie pulpitu, do którego należy widżet. Zachowanie parametru: - *wymagany*

Przykłady

Poniższe przykłady mają na celu jedynie opisanie konfiguracji obiektów pól widżetu pulpitu dla widżetu *Prototyp wykresu*. Więcej informacji na temat konfiguracji pulpitu można znaleźć w `dashboard.create`.

Konfigurowanie widżetu *Graph prototype*

Skonfiguruj widżet *Graph prototype*, który wyświetla siatkę 3 wykresów (3 kolumny, 1 wiersz) utworzonych z prototypu pozycji (ID: ”42316”) przez wykrywanie niskopoziomowe.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "dashboard.create",
    "params": {
        "name": "My dashboard",
        "display_period": 30,
        "auto_start": 1,
        "pages": [
            {
                "widgets": [
                    {
                        "type": "graphprototype",
                        "name": "Graph prototype",
                        "x": 0,
                        "y": 0,
                        "width": 48,
                        "height": 5,
                        "view_mode": 0,
                        "fields": [
                            {
                                "type": 0,
                                "name": "source_type",
                                "value": 3
                            },
                            {
                                "type": 5,
                                "name": "itemid.0",
                                "value": 42316
                            },
                            {
                                "type": 0,
                                "name": "columns",
                                "value": 3
                            },
                            {
                                "type": 1,
                                "name": "reference",
                                "value": "OPQWX"
                            }
                        ]
                    }
                ]
            }
        ],
        "userGroups": [
            {
                "usrgrpid": 7,
                "permission": 2
            }
        ],
        "users": [
            {
                "userid": 1,
                "permission": 3
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "3"
        ]
    },
    "id": 1
}
```

Zobacz także

- Pole widżetu pulpitu
- `dashboard.create`
- `dashboard.update`

11 Honeycomb

Opis

Te parametry oraz możliwe wartości właściwości dla odpowiednich obiektów pól widgetu umożliwiają konfigurację widgetu *Honeycomb* w metodach `dashboard.create` i `dashboard.update`.

Attention:
Właściwości `fields` widgetu nie są walidowane podczas tworzenia ani aktualizacji dashboardu. Pozwala to użytkownikom modyfikować wbudowane widgety i tworzyć własne widgety, ale jednocześnie wprowadza ryzyko nieprawidłowego tworzenia lub aktualizowania widgetów. Aby zapewnić pomyślne utworzenie lub aktualizację widgetu *Honeycomb*, zapoznaj się z zachowaniem parametrów opisanym w poniższych tabelach.

Parametry

Następujące parametry są obsługiwane dla widżetu *Honeycomb*.

Parametr	type	name	value
Interwał odświeżania	0	rf_rate	0 - Bez odświeżania; 10 - 10 sekund; 30 - 30 sekund; 60 - *(domyślnie)* 1 minuta; 120 - 2 minuty; 600 - 10 minut; 900 - 15 minut.
Grupy hostów	2	groupids.0	ID grupy hostów. Uwaga: Aby skonfigurować wiele grup hostów, utwórz obiekt pola widżetu pulpitu dla każdej grupy hostów z numerem zwiększanym w nazwie właściwości. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Grupy hostów (Widżet)	1	groupids._reference	Zamiast ID grupy hostów: `ABCDE._hostgroupids` - ustaw zgodny widżet (z parametrem *Reference* ustawionym na "ABCDE") jako źródło danych dla grup hostów. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.

Parametr	type	name	value
Hosty	3	hostids.0	ID hosta. Uwaga: Aby skonfigurować wiele hostów, utwórz obiekt pola widżetu pulpitu dla każdego hosta z numerem zwiększanym w nazwie właściwości. W przypadku wielu hostów parametr *Grupy hostów* nie może być w ogóle skonfigurowany albo musi być skonfigurowany z co najmniej jedną grupą hostów, do której należą skonfigurowane hosty. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Hosty (Widżet/Pulpit)	1	hostids._reference	Zamiast ID hosta: `DASHBOARD.hostids` - ustaw selektor hostów pulpitu jako źródło danych dla hostów; `ABCDE._hostids` - ustaw zgodny widżet (z parametrem *Reference* ustawionym na "`ABCDE`") jako źródło danych dla hostów. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Tagi hostów			
Typ oceny	0	evaltype_host	0 - *(domyślnie)* And/Or; 2 - Or. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Nazwa tagu	1	host_tags.0.tag	Dowolna wartość tekstowa. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście oceny tagów. Zachowanie parametru: - *wymagane* przy konfigurowaniu *Tagów hostów* Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Operator	0	host_tags.0.operator	0 - Zawiera; 1 - Równa się; 2 - Nie zawiera; 3 - Nie równa się; 4 - Istnieje; 5 - Nie istnieje. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście oceny tagów. Zachowanie parametru: - *wymagane* przy konfigurowaniu *Tagów hostów* Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Wartość tagu	1	host_tags.0.value	Dowolna wartość tekstowa. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście oceny tagów. Zachowanie parametru: - *wymagane* przy konfigurowaniu *Tagów hostów* Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.

Parametr	type	name	value
Wzorce pozycji	1	items.0	Nazwa lub wzorzec pozycji. Uwaga: Aby skonfigurować wiele wzorców pozycji, utwórz obiekt pola widżetu pulpitu dla każdego wzorca pozycji z numerem zwiększanym w nazwie właściwości. Zachowanie parametru: - *wymagane*
Tagi pozycji			
Typ oceny	0	evaltype_item	0 - *(domyślnie)* And/Or; 2 - Or.
Nazwa tagu	1	item_tags.0.tag	Dowolna wartość tekstowa. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście oceny tagów. Zachowanie parametru: - *wymagane* przy konfigurowaniu *Tagów pozycji*
Operator	0	item_tags.0.operator	0 - Zawiera; 1 - Równa się; 2 - Nie zawiera; 3 - Nie równa się; 4 - Istnieje; 5 - Nie istnieje. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście oceny tagów. Zachowanie parametru: - *wymagane* przy konfigurowaniu *Tagów pozycji*
Wartość tagu	1	item_tags.0.value	Dowolna wartość tekstowa. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście oceny tagów. Zachowanie parametru: - *wymagane* przy konfigurowaniu *Tagów pozycji*
Pokaż hosty w konserwacji	0	maintenance	0 - *(domyślnie)* Wyłączone; 1 - Włączone.
Pokaż	0	show.0	1 - Etykieta podstawowa; 2 - Etykieta dodatkowa. Uwaga: Aby skonfigurować wiele wartości, utwórz obiekt pola widżetu pulpitu dla każdej wartości z numerem zwiększanym w nazwie właściwości. Domyślnie: 1, 2.
Reference	1	reference	Dowolna wartość tekstowa składająca się z 5 znaków (na przykład `ABCDE` lub `JBPNL`). Ta wartość musi być unikalna w obrębie pulpitu, do którego należy widżet. Zachowanie parametru: - *wymagane*

Konfiguracja zaawansowana

Dla widżetu *Honeycomb* obsługiwane są następujące zaawansowane parametry konfiguracji.

Note:
Liczba w nazwie właściwości *Thresholds* (np. thresholds.0.color) odnosi się do miejsca progu na liście, posortowanej rosnąco. Jeśli jednak progi zostaną skonfigurowane w innej kolejności, wartości zostaną posortowane rosnąco po zaktualizowaniu konfiguracji widżetu w frontendzie Zabbix (np. `"thresholds.0.threshold":"5"` → `"thresholds.0.threshold":"1"`; `"thresholds.1.threshold":"1"` → `"thresholds.1.threshold": "5"`).

Parametr	type	name	value
Etykieta główna			
Typ	0	primary_label_type	0 - *(domyślnie)* Tekst; 1 - Wartość.
Tekst	1	primary_label	Dowolna wartość tekstowa, w tym makra. Obsługiwane makra: {HOST.*}, {ITEM.*}, {INVENTORY.*}, makra użytkownika. Domyślnie: {HOST.NAME} Zachowanie parametru: - *obsługiwane*, jeśli *Typ* jest ustawiony na ”Tekst”
Miejsca dziesiętne	0	primary_label_decimal_places	Możliwe wartości mieszczą się w zakresie 0-6. Domyślnie: 2. Zachowanie parametru: - *obsługiwane*, jeśli *Typ* jest ustawiony na ”Wartość”
Rozmiar (typ)	0	primary_label_size_type	0 - *(domyślnie)* Auto; 1 - Niestandardowy.
Rozmiar	0	primary_label_size	Możliwe wartości mieszczą się w zakresie 1-100. Domyślnie: 20. Zachowanie parametru: - *obsługiwane*, jeśli *Rozmiar* (typ) jest ustawiony na ”Niestandardowy”
Pogrubienie	0	primary_label_bold	0 - *(domyślnie)* Wyłączone; 1 - Włączone.
Kolor	1	primary_label_color	Szesnastkowy kod koloru (np. FF0000). Domyślnie: na podstawie `theme` obiektu Settings object i obiektu User object: 1F2C33 dla ”blue-theme” lub ”hc-light”; EEEEEE dla ”dark-theme” lub ”hc-dark”.
Jednostki (pole wyboru)	0	primary_label_units_show	0 - Wyłączone; 1 - *(domyślnie)* Włączone. Zachowanie parametru: - *obsługiwane*, jeśli *Typ* jest ustawiony na ”Wartość”
Jednostki (wartość)	1	primary_label_units	Dowolna wartość tekstowa. "" (puste) Zachowanie parametru: - *obsługiwane*, jeśli *Typ* jest ustawiony na ”Wartość” i *Jednostki* (pole wyboru) są ustawione na ”Włączone”

Parametr	type	name	value
Pozycja	0	primary_label_units_pos	0 - Przed wartością; 1 - *(domyślnie)* Po wartości. Zachowanie parametru: - *obsługiwane*, jeśli *Typ* jest ustawiony na ”Wartość” i *Jednostki* (pole wyboru) są ustawione na ”Włączone” Ten parametr jest ignorowany, jeśli ustawiono jedną z następujących jednostek związanych z czasem: unixtime, uptime, s.
Etykieta dodatkowa			
Typ	0	secondary_label_type	0 - Tekst; 1 - *(domyślnie)* Wartość.
Tekst	1	secondary_label	Dowolna wartość tekstowa, w tym makra. Obsługiwane makra: {HOST.*}, {ITEM.*}, {INVENTORY.*}, makra użytkownika. Domyślnie: {{ITEM.LASTVALUE}.fmtnum(2)} Zachowanie parametru: - *obsługiwane*, jeśli *Typ* jest ustawiony na ”Tekst”
Miejsca dziesiętne	0	secondary_label_decimal_places	Możliwe wartości mieszczą się w zakresie 0-6. Domyślnie: 2. Zachowanie parametru: - *obsługiwane*, jeśli *Typ* jest ustawiony na ”Wartość”
Rozmiar (typ)	0	secondary_label_size_type	0 - *(domyślnie)* Auto; 1 - Niestandardowy.
Rozmiar	0	secondary_label_size	Możliwe wartości mieszczą się w zakresie 1-100. Domyślnie: 30. Zachowanie parametru: - *obsługiwane*, jeśli *Rozmiar* (typ) jest ustawiony na ”Niestandardowy”
Pogrubienie	0	secondary_label_bold	0 - Wyłączone; 1 - *(domyślnie)* Włączone.
Kolor	1	secondary_label_color	Szesnastkowy kod koloru (np. `FF0000`). Domyślnie: na podstawie `theme` obiektu Settings object i obiektu User object: `1F2C33` dla ”blue-theme” lub ”hc-light”; `EEEEEE` dla ”dark-theme” lub ”hc-dark”.
Jednostki (pole wyboru)	0	secondary_label_units_show	0 - Wyłączone; 1 - *(domyślnie)* Włączone. Zachowanie parametru: - *obsługiwane*, jeśli *Typ* jest ustawiony na ”Wartość”
Jednostki (wartość)	1	secondary_label_units	Dowolna wartość tekstowa. "" (puste) Zachowanie parametru: - *obsługiwane*, jeśli *Typ* jest ustawiony na ”Wartość” i *Jednostki* (pole wyboru) są ustawione na ”Włączone”

Parametr	type	name	value
Pozycja	0	secondary_label_position	0 - Przed wartością; 1 - *(domyślnie)* Po wartości. Zachowanie parametru: - *obsługiwane*, jeśli *Typ* jest ustawiony na ”Wartość” i *Jednostki* (pole wyboru) są ustawione na ”Włączone” Ten parametr jest ignorowany, jeśli ustawiono jedną z następujących jednostek związanych z czasem: unixtime, uptime, s.
Kolor tła			
Kolor tła	1	bg_color	Szesnastkowy kod koloru (np. FF0000). Domyślnie: na podstawie theme obiektu Settings object i obiektu User object: D9E7ED dla ”blue-theme”; 3D5059 dla ”dark-theme”; AAD7E9 dla ”hc-light”; 335463 dla ”hc-dark”.
Progi			
Interpolacja kolorów	0	interpolation	0 - Wyłączona; 1 - *(domyślnie)* Włączona.
Kolor	1	thresholds.0.color	Szesnastkowy kod koloru (np. FF0000).
Próg	1	thresholds.0.threshold	Dowolna wartość liczbowa. Obsługiwane są sufiksy (np. ”1d”, ”2w”, ”4K”, ”8G”).

Przykłady

Poniższe przykłady mają na celu jedynie opisanie konfiguracji obiektów pól widżetu pulpitu dla widżetu *Honeycomb*. Więcej informacji na temat konfiguracji pulpitu można znaleźć w dashboard.create.

Konfigurowanie widżetu *Honeycomb*

Skonfiguruj widżet *Honeycomb*, który wyświetla wykorzystanie procesów serwera Zabbix. Dodatkowo zmień główną etykietę komórek honeycomb i dostrój wizualnie widżet za pomocą progów.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "dashboard.create",
    "params": {
        "name": "My dashboard",
        "display_period": "30",
        "auto_start": "1",
        "pages": [
            {
                "widgets": [
                    {
                        "type": "honeycomb",
                        "name": "Honeycomb",
                        "x": "0",
                        "y": "0",
                        "width": "24",
                        "height": "5",
                        "view_mode": "0",
                        "fields": [
                            {
                                "type": 2,
                                "name": "groupids.0",
                                "value": 4
                            },
                            {
                                "type": 3,
```

```
                            "name": "hostids.0",
                            "value": 10084
                        },
                        {
                            "type": 1,
                            "name": "items.0",
                            "value": "Zabbix server: Utilization*"
                        },
                        {
                            "type": 1,
                            "name": "primary_label",
                            "value": "{ITEM.NAME}"
                        },
                        {
                            "type": 1,
                            "name": "thresholds.0.color",
                            "value": "0EC9AC"
                        },
                        {
                            "type": 1,
                            "name": "thresholds.0.threshold",
                            "value": "0"
                        },
                        {
                            "type": 1,
                            "name": "thresholds.1.color",
                            "value": "FFD54F"
                        },
                        {
                            "type": 1,
                            "name": "thresholds.1.threshold",
                            "value": "70"
                        },
                        {
                            "type": 1,
                            "name": "thresholds.2.color",
                            "value": "FF465C"
                        },
                        {
                            "type": 1,
                            "name": "thresholds.2.threshold",
                            "value": "90"
                        },
                        {
                            "type": 1,
                            "name": "reference",
                            "value": "KSTMQ"
                        }
                    ]
                }
            ]
        }
    ],
    "userGroups": [
        {
            "usrgrpid": 7,
            "permission": 2
        }
    ],
    "users": [
        {
            "userid": 1,
```

```
                "permission": 3
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "3"
        ]
    },
    "id": 1
}
```

Zobacz także

- Pole widżetu pulpitu
- `dashboard.create`
- `dashboard.update`

12 Dostępność hosta

Opis

Te parametry oraz możliwe wartości właściwości dla odpowiednich obiektów pól widżetu pulpitu umożliwiają skonfigurowanie widżetu *Dostępność hosta* w metodach `dashboard.create` i `dashboard.update`.

Parametry

Następujące parametry są obsługiwane dla widżetu *Dostępność hosta*.

Parametr	type	name	value
Interwał odświeżania	0	rf_rate	0 - Bez odświeżania; 10 - 10 sekund; 30 - 30 sekund; 60 - 1 minuta; 120 - 2 minuty; 600 - 10 minut; 900 - *(domyślnie)* 15 minut.
Grupy hostów	2	groupids.0	ID grupy hostów. Uwaga: Aby skonfigurować wiele grup hostów, utwórz obiekt pola widżetu pulpitu dla każdej grupy hostów z numerem zwiększanym w nazwie właściwości. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Grupy hostów (widżet)	1	groupids._reference	Zamiast ID grupy hostów: `ABCDE._hostgroupids` - ustaw kompatybilny widżet (z parametrem *Odwołanie* ustawionym na "`ABCDE`") jako źródło danych dla grup hostów. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.

Parametr	type	name	value
Typ interfejsu	0	interface_type.0	0 - Brak; 1 - agent Zabbix (sprawdzanie pasywne); 2 - SNMP; 3 - IPMI; 4 - JMX; 5 - agent Zabbix (sprawdzanie aktywne). Domyślnie: 1, 2, 3, 4, 5 (wszystkie włączone). Uwaga: Aby skonfigurować wiele wartości, utwórz obiekt pola widżetu pulpitu dla każdej wartości z numerem zwiększanym w nazwie właściwości.
Układ	0	layout	0 - *(domyślnie)* Poziomy; 1 - Pionowy.
Pokaż hosty w konserwacji	0	maintenance	0 - *(domyślnie)* Wyłączone; 1 - Włączone.
Pokaż tylko sumy	0	only_totals	0 - *(domyślnie)* Wyłączone; 1 - Włączone.

Przykłady

Poniższe przykłady mają na celu jedynie opisanie konfiguracji obiektów pól widżetu pulpitu dla widżetu *Dostępność hosta*. Więcej informacji na temat konfiguracji pulpitu można znaleźć w `dashboard.create`.

Konfigurowanie widżetu *Dostępność hosta*

Skonfiguruj widżet *Dostępność hosta*, który wyświetla informacje o dostępności (w układzie pionowym) dla hostów z grupy hostów „4” ze skonfigurowanymi interfejsami „Zabbix agent” i „SNMP”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "dashboard.create",
    "params": {
        "name": "My dashboard",
        "display_period": 30,
        "auto_start": 1,
        "pages": [
            {
                "widgets": [
                    {
                        "type": "hostavail",
                        "name": "Host availability",
                        "x": 0,
                        "y": 0,
                        "width": 18,
                        "height": 3,
                        "view_mode": 0,
                        "fields": [
                            {
                                "type": 2,
                                "name": "groupids.0",
                                "value": 4
                            },
                            {
                                "type": 0,
                                "name": "interface_type",
                                "value": 1
```

```
                            },
                            {
                                "type": 0,
                                "name": "interface_type",
                                "value": 2
                            },
                            {
                                "type": 0,
                                "name": "layout",
                                "value": 1
                            }
                        ]
                    }
                ]
            }
        ],
        "userGroups": [
            {
                "usrgrpid": 7,
                "permission": 2
            }
        ],
        "users": [
            {
                "userid": 1,
                "permission": 3
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "3"
        ]
    },
    "id": 1
}
```

Zobacz także

- Pole widżetu pulpitu
- `dashboard.create`
- `dashboard.update`

######13 Karta hosta {#manual-api-reference-dashboard-widget_fields-host_card}

Opis

Te parametry oraz możliwe wartości właściwości dla odpowiednich obiektów pól widgetu umożliwiają skonfigurowanie widgetu *Karta hosta* w metodach `dashboard.create` i `dashboard.update`.

Attention:
Właściwości `fields` widgetu nie są walidowane podczas tworzenia ani aktualizacji pulpitu. Pozwala to użytkownikom modyfikować wbudowane widgety i tworzyć własne widgety, ale wprowadza również ryzyko nieprawidłowego tworzenia lub aktualizowania widgetów. Aby zapewnić pomyślne utworzenie lub zaktualizowanie widgetu *Karta hosta*, zapoznaj się z zachowaniem parametrów opisanym w poniższych tabelach.

Parametry

Następujące parametry są obsługiwane dla widżetu *Karta hosta*.

Parametr	type	name	value
Interwał odświeżania	0	rf_rate	0 - Brak odświeżania; 10 - 10 sekund; 30 - 30 sekund; 60 - *(domyślnie)* 1 minuta; 120 - 2 minuty; 600 - 10 minut; 900 - 15 minut.
Host	3	hostid.0	ID hosta. Zachowanie parametrów: - *wymagane*, jeśli *Host (Widżet/Pulpit)* nie jest ustawiony Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Host (Widżet/Pulpit)	1	hostid._reference	Zamiast ID hosta: `DASHBOARD.hostid` - ustaw selektor hosta pulpitu jako źródło danych dla hosta; `ABCDE._hostid` - ustaw kompatybilny widżet (z parametrem *Reference* ustawionym na "`ABCDE`") jako źródło danych dla hosta. Zachowanie parametrów: - *wymagane*, jeśli *Host* nie jest ustawiony Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Pokaż ukryte problemy	0	show_suppressed	0 - *(domyślnie)* Wyłączone; 1 - Włączone.
Pokaż	0	sections.0	0 - Grupy hostów; 1 - Opis; 2 - Monitorowanie; 3 - Dostępność; 4 - Monitorowane przez; 5 - Szablony; 6 - Inwentarz; 7 - Tagi. Uwaga: Liczba w nazwie właściwości odnosi się do kolejności sekcji na liście sekcji. Aby skonfigurować wiele sekcji, utwórz obiekt pola widżetu pulpitu dla każdej sekcji, zwiększając numer w nazwie właściwości.

Następujące parametry są obsługiwane, jeśli *Pokaż* jest ustawione na „Inwentarz".

Parametr	type	name	value
Pola inwentarza	0	inventory.0	ID inwentarza. Uwaga: Aby skonfigurować wiele pól inwentarza, utwórz obiekt pola widżetu pulpitu dla każdego pola inwentarza, zwiększając numer w nazwie właściwości.

Przykłady

Poniższe przykłady mają na celu jedynie opisanie konfiguracji obiektów pól widżetu pulpitu dla widżetu *Host card*. Więcej informacji na temat konfiguracji pulpitu można znaleźć w `dashboard.create`.

Konfigurowanie widżetu *Host card*

Skonfiguruj widżet *Host card*, który wyświetla następujące sekcje: „Monitoring”, „Availability”, „Monitored by”, „Inventory” i „Tags”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "dashboard.create",
    "params": {
        "name": "My dashboard",
        "display_period": 30,
        "auto_start": 1,
        "pages": [
            {
                "widgets": [
                    {
                        "type": "hostcard",
                        "name": "Host card",
                        "x": 0,
                        "y": 0,
                        "width": 14,
                        "height": 7,
                        "view_mode": 0,
                        "fields": [
                            {
                                "type": 3,
                                "name": "hostid.0",
                                "value": 10084
                            },
                            {
                                "type": 0,
                                "name": "show_suppressed",
                                "value": 1
                            },
                            {
                                "type": 0,
                                "name": "sections.0",
                                "value": 2
                            },
                            {
                                "type": 0,
                                "name": "sections.1",
                                "value": 3
                            },
                            {
                                "type": 0,
                                "name": "sections.2",
                                "value": 4
                            },
                            {
                                "type": 0,
                                "name": "sections.3",
                                "value": 6
                            },
                            {
                                "type": 0,
                                "name": "sections.4",
                                "value": 7
                            },
                            {
                                "type": 0,
                                "name": "inventory.0",
                                "value": 25
                            },
                            {
```

```
                                "type": 0,
                                "name": "inventory.1",
                                "value": 26
                            }
                        ]
                    }
                ]
            }
        ],
        "userGroups": [
            {
                "usrgrpid": 7,
                "permission": 2
            }
        ],
        "users": [
            {
                "userid": 1,
                "permission": 3
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "3"
        ]
    },
    "id": 1
}
```

Zobacz także

- Pole widżetu pulpitu
- `dashboard.create`
- `dashboard.update`

14 Nawigator hostów

Opis

Te parametry oraz możliwe wartości właściwości dla odpowiednich obiektów pól widgetu umożliwiają skonfigurowanie widgetu *Host navigator* w metodach `dashboard.create` i `dashboard.update`.

Attention:
Właściwości `fields` widgetu nie są walidowane podczas tworzenia ani aktualizacji dashboardu. Pozwala to użytkownikom modyfikować wbudowane widgety i tworzyć własne widgety, ale jednocześnie wprowadza ryzyko nieprawidłowego tworzenia lub aktualizowania widgetów. Aby zapewnić pomyślne utworzenie lub zaktualizowanie widgetu *Host navigator*, zapoznaj się z zachowaniem parametrów opisanym w poniższych tabelach.

Parametry

Poniższe parametry są obsługiwane dla widżetu *Nawigator hostów*.

Parametr	type	name	value
Interwał odświeżania	0	rf_rate	0 - Brak odświeżania; 10 - 10 sekund; 30 - 30 sekund; 60 - *(domyślnie)* 1 minuta; 120 - 2 minuty; 600 - 10 minut; 900 - 15 minut.
Grupy hostów	2	groupids.0	ID grupy hostów. Uwaga: Aby skonfigurować wiele grup hostów, utwórz obiekt pola widżetu pulpitu dla każdej grupy hostów z inkrementowanym numerem w nazwie właściwości. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Grupy hostów (widżet)	1	groupids._reference	Zamiast ID grupy hostów: `ABCDE._hostgroupids` - ustaw kompatybilny widżet (z parametrem *Reference* ustawionym na "`ABCDE`") jako źródło danych dla grup hostów. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Wzorce hostów	1	hosts.0	Nazwa lub wzorzec hosta. Uwaga: Aby skonfigurować wiele wzorców hostów, utwórz obiekt pola widżetu pulpitu dla każdego wzorca hosta z inkrementowanym numerem w nazwie właściwości. W przypadku wielu wzorców hostów parametr *Grupy hostów* nie może być w ogóle skonfigurowany albo musi być skonfigurowany z co najmniej jedną grupą hostów, do której należą hosty pasujące do skonfigurowanych wzorców hostów. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Status hosta	0	status	-1 - *(domyślnie)* Dowolny; 0 - Włączony; 1 - Wyłączony. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Tagi hosta			
Typ oceny	0	host_tags_evaltype	0 - *(domyślnie)* I/Lub; 2 - Lub. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Nazwa tagu	1	host_tags.0.tag	Dowolna wartość tekstowa. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście oceny tagów. Zachowanie parametru: - *wymagane* przy konfigurowaniu *Tagów hosta* Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.

Parametr	type	name	value
Operator	0	host_tags.0.operator	0 - Zawiera; 1 - Równa się; 2 - Nie zawiera; 3 - Nie równa się; 4 - Istnieje; 5 - Nie istnieje. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście oceny tagów. Zachowanie parametru: - *wymagane* przy konfigurowaniu *Tagów hosta* Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Wartość tagu	1	host_tags.0.value	Dowolna wartość tekstowa. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście oceny tagów. Zachowanie parametru: - *wymagane* przy konfigurowaniu *Tagów hosta* Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Poziom ważności	0	severities.0	0 - Niesklasyfikowane; 1 - Informacja; 2 - Ostrzeżenie; 3 - Średni; 4 - Wysoki; 5 - Katastrofa. Domyślnie: puste (wszystkie włączone). Uwaga: Aby skonfigurować wiele wartości, utwórz obiekt pola widżetu pulpitu dla każdej wartości z inkrementowanym numerem w nazwie właściwości.
Pokaż hosty w konserwacji	0	maintenance	0 - *(domyślnie)* Wyłączone; 1 - Włączone.
Pokaż problemy	0	show_problems	0 - Wszystkie; 1 - *(domyślnie)* Nieukryte; 2 - Brak.
Grupuj według			
Atrybut	0	group_by.0.attribute	0 - Grupa hostów; 1 - Wartość tagu; 2 - Poziom ważności. Uwaga: Numer w nazwie właściwości odnosi się do kolejności atrybutu na liście atrybutów grupowania. Zachowanie parametru: - *wymagane* przy konfigurowaniu *Grupuj według*

Parametr	type	name	value
Wartość	1	group_by.0.tag_name	Dowolna wartość tekstowa. Uwaga: Numer w nazwie właściwości odnosi się do atrybutu grupowania ustawionego w parametrze *Atrybut*. Zachowanie parametru: - *wymagane* przy konfigurowaniu *Grupuj według*, gdy *Atrybut* jest ustawiony na "Wartość tagu"
Limit hostów	0	show_lines	Możliwe wartości mieszczą się w zakresie 1-9999. Domyślnie: 100. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Reference	1	reference	Dowolna wartość tekstowa składająca się z 5 znaków (np. `ABCDE` lub `JBPNL`). Ta wartość musi być unikalna w obrębie pulpitu, do którego należy widżet. Zachowanie parametru: - *wymagane*

Przykłady

Poniższe przykłady mają na celu jedynie opisanie konfiguracji obiektów pól widgetu pulpitu dla widgetu *Host navigator*. Więcej informacji na temat konfiguracji pulpitu można znaleźć w `dashboard.create`.

Konfigurowanie widżetu *Host navigator*

Skonfiguruj widżet *Host navigator*, który wyświetla hosty pogrupowane według ich grupy hostów, a następnie według wartości tagu „city".

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "dashboard.create",
    "params": {
        "name": "My dashboard",
        "display_period": "30",
        "auto_start": "1",
        "pages": [
            {
                "widgets": [
                    {
                        "type": "hostnavigator",
                        "name": "Host navigator",
                        "x": "0",
                        "y": "0",
                        "width": "12",
                        "height": "5",
                        "view_mode": "0",
                        "fields": [
                            {
                                "type": 2,
                                "name": "groupids.0",
                                "value": 2
                            },
                            {
                                "type": 2,
                                "name": "groupids.1",
                                "value": 4
                            },
                            {
```

```
                                "type": 0,
                                "name": "group_by.0.attribute",
                                "value": 0
                            },
                            {
                                "type": 0,
                                "name": "group_by.1.attribute",
                                "value": 1
                            },
                            {
                                "type": 1,
                                "name": "group_by.1.tag_name",
                                "value": "city"
                            },
                            {
                                "type": 1,
                                "name": "reference",
                                "value": "SWKLB"
                            }
                        ]
                    }
                ]
            }
        ],
        "userGroups": [
            {
                "usrgrpid": 7,
                "permission": 2
            }
        ],
        "users": [
            {
                "userid": 1,
                "permission": 3
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "3"
        ]
    },
    "id": 1
}
```

Zobacz także

- Pole widżetu pulpitu
- `dashboard.create`
- `dashboard.update`

15 Karta pozycji

Opis

Te parametry oraz możliwe wartości właściwości dla odpowiednich obiektów pól widgetu umożliwiają konfigurację widgetu *Item*

card w metodach `dashboard.create` i `dashboard.update`.

Attention:
Właściwości `fields` widgetu nie są walidowane podczas tworzenia ani aktualizacji pulpitu. Pozwala to użytkownikom modyfikować wbudowane widgety i tworzyć własne widgety, ale jednocześnie wprowadza ryzyko nieprawidłowego tworzenia lub aktualizowania widgetów. Aby zapewnić pomyślne utworzenie lub zaktualizowanie widgetu *Item card*, zapoznaj się z zachowaniem parametrów opisanym w poniższych tabelach.

Parametry

Następujące parametry są obsługiwane dla widżetu *Karta pozycji*.

Parametr	type	name	value
Interwał odświeżania	0	rf_rate	0 - Bez odświeżania; 10 - 10 sekund; 30 - 30 sekund; 60 - *(domyślnie)* 1 minuta; 120 - 2 minuty; 600 - 10 minut; 900 - 15 minut.
Pozycja	4	itemid.0	ID pozycji. Zachowanie parametrów: - *wymagane*, jeśli *Pozycja (widżet)* nie jest ustawiona
Pozycja (widżet)	1	itemid._reference	Zamiast ID pozycji: `ABCDE._itemid` - ustaw kompatybilny widżet (z parametrem *Odwołanie* ustawionym na "`ABCDE`") jako źródło danych dla pozycji. Zachowanie parametrów: - *wymagane*, jeśli *Pozycja* nie jest ustawiona
Pokaż	0	sections.0	0 - Opis; 1 - Tekst błędu; 2 - Metryki; 3 - Najnowsze dane; 4 - Typ informacji; 5 - Wyzwalacze; 6 - Interfejs hosta; 7 - Typ; 8 - Inwentarz hosta; 9 - Tagi. Uwaga: Liczba w nazwie właściwości odnosi się do kolejności sekcji na liście sekcji. Aby skonfigurować wiele sekcji, utwórz obiekt pola widżetu pulpitu dla każdej sekcji z kolejnym numerem zwiększonym w nazwie właściwości.
Nadpisz host	1	override_hostid._reference	`ABCDE._hostid` - ustaw kompatybilny widżet (z parametrem *Odwołanie* ustawionym na "`ABCDE`") jako źródło danych dla hostów; `DASHBOARD._hostid` - ustaw selektor hosta pulpitu jako źródło danych dla hostów. Domyślnie: "" (puste) Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.

Sparkline

Następujące parametry są obsługiwane, jeśli opcja *Pokaż* jest ustawiona na „Najnowsze dane".

Parametr	type	name	value
Szerokość	0	sparkline.width	Możliwe wartości mieszczą się w zakresie 0-10. Domyślnie: 1.
Wypełnienie	0	sparkline.fill	Możliwe wartości mieszczą się w zakresie 0-10. Domyślnie: 3.
Kolor	1	sparkline.color	Szesnastkowy kod koloru (np. FF0000). Domyślnie: 42A5F5.
Okres czasu	1	sparkline.time_period.from	DASHBOARD._timeperiod — ustaw selektor okresu czasu pulpitu jako źródło danych; ABCDE._timeperiod — ustaw zgodny widget (z parametrem reference równym ABCDE) jako źródło danych. Domyślnie: "" (puste) Alternatywnie można ustawić okres czasu tylko w parametrach *Od* i *Do*.
Od	1	sparkline.time_period.from	Prawidłowy ciąg czasu w składni bezwzględnej (YYYY-MM-DD hh:mm:ss) lub względnej (now, now/d, now/w-1w itd.). Domyślnie: now-1h. Zachowanie parametru: - *obsługiwany*, jeśli *Okres czasu* nie jest ustawiony - *wymagany*, jeśli ustawiono sparkline.time_period.to
Do	1	sparkline.time_period.to	Prawidłowy ciąg czasu w składni bezwzględnej (YYYY-MM-DD hh:mm:ss) lub względnej (now, now/d, now/w-1w itd.). Domyślnie: now. Zachowanie parametru: - *obsługiwany*, jeśli *Okres czasu* nie jest ustawiony - *wymagany*, jeśli ustawiono time_period.to
Dane historyczne	0	sparkline.history	0 — *(domyślnie)* Auto; 1 — Historia; 2 — Trendy.

Przykłady

Poniższe przykłady mają na celu jedynie opisanie konfiguracji obiektów pól widżetu pulpitu dla widżetu *Karta pozycji*. Więcej informacji na temat konfiguracji pulpitu można znaleźć w dashboard.create.

Konfigurowanie widżetu *Karta pozycji*

Skonfiguruj widżet *Karta pozycji*, który wyświetla następujące sekcje: „Opis”, „Najnowsze dane”, „Wyzwalacze” i „Tagi”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "dashboard.create",
    "params": {
        "name": "My dashboard",
        "display_period": 30,
        "auto_start": 1,
        "pages": [
            {
                "widgets": [
                    {
                        "type": "itemcard",
                        "name": "Item card",
```

```
                        "x": 0,
                        "y": 0,
                        "width": 14,
                        "height": 7,
                        "view_mode": 0,
                        "fields": [
                            {
                                "type": 4,
                                "name": "itemid.0",
                                "value": 42257
                            },
                            {
                                "type": 0,
                                "name": "sections.0",
                                "value": 0
                            },
                            {
                                "type": 0,
                                "name": "sections.1",
                                "value": 3
                            },
                            {
                                "type": 0,
                                "name": "sections.2",
                                "value": 5
                            },
                            {
                                "type": 0,
                                "name": "sections.3",
                                "value": 9
                            }
                        ]
                    }
                ]
            }
        ],
        "userGroups": [
            {
                "usrgrpid": 7,
                "permission": 2
            }
        ],
        "users": [
            {
                "userid": 1,
                "permission": 3
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "3"
        ]
    },
    "id": 1
}
```

Zobacz także

- Pole widżetu pulpitu
- `dashboard.create`
- `dashboard.update`

16 Historia pozycji

Opis

Te parametry oraz możliwe wartości właściwości dla odpowiednich obiektów pól widgetu umożliwiają skonfigurowanie widgetu *Historia pozycji* w metodach `dashboard.create` i `dashboard.update`.

Attention:
Właściwości `fields` widgetu nie są walidowane podczas tworzenia ani aktualizacji pulpitu. Pozwala to użytkownikom modyfikować wbudowane widgety i tworzyć własne widgety, ale jednocześnie wprowadza ryzyko nieprawidłowego tworzenia lub aktualizowania widgetów. Aby zapewnić pomyślne utworzenie lub zaktualizowanie widgetu *Historia pozycji*, zapoznaj się z zachowaniem parametrów opisanym w poniższych tabelach.

Parametry

Następujące parametry są obsługiwane dla widżetu *Historia pozycji*.

Parametr	type	name	value
Interwał odświeżania	0	rf_rate	0 - Bez odświeżania; 10 - 10 sekund; 30 - 30 sekund; 60 - *(domyślnie)* 1 minuta; 120 - 2 minuty; 600 - 10 minut; 900 - 15 minut.
Układ	0	layout	0 - *(domyślnie)* Poziomy; 1 - Pionowy.
Kolumny (zobacz poniżej)			
Pokaż wiersze	0	show_lines	Możliwe wartości mieszczą się w zakresie 1-100. Domyślnie: 25.
Nadpisz host	1	override_hostid._reference	`ABCDE._hostid` - ustaw kompatybilny widżet (z parametrem *Reference* ustawionym na "`ABCDE`") jako źródło danych dla hostów; `DASHBOARD._hostid` - ustaw selektor hosta jako źródło danych dla hostów. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Konfiguracja zaawansowana (zobacz poniżej)			
Reference	1	reference	Dowolna wartość tekstowa składająca się z 5 znaków (na przykład `ABCDE` lub `JBPNL`). Ta wartość musi być unikalna w obrębie pulpitu, do którego należy widżet. Zachowanie parametru: - *wymagany*

Kolumny

Kolumny mają wspólne parametry oraz dodatkowe parametry zależne od konfiguracji parametru *Pozycja*.

Note:
Dla wszystkich parametrów związanych z kolumnami liczba w nazwie właściwości (np. columns.0.name) odnosi się do kolumny, dla której parametr jest skonfigurowany.

Następujące parametry są obsługiwane dla wszystkich kolumn.

Parametr	type	name	value
Nazwa	1	columns.0.name	Dowolna wartość tekstowa. Zachowanie parametru: - *wymagane*
Pozycja	4	columns.0.itemid	ID pozycji. Podczas konfigurowania widżetu na pulpicie szablonu należy ustawić tylko pozycje skonfigurowane w szablonie. Zachowanie parametru: - *wymagane*
Kolor bazowy	1	columns.0.base_color	Szesnastkowy kod koloru (np. FF0000). Domyślnie: "" (puste).

Następujące parametry kolumn są obsługiwane, jeśli skonfigurowana *pozycja* jest pozycją typu numerycznego.

Parametr	type	name	value
Wyświetlanie	0	columns.0.display	1 - *(domyślnie)* Bez zmian; 2 - Pasek; 3 - Wskaźniki.
Min	1	columns.0.min	Dowolna wartość liczbowa. Zachowanie parametru: - *obsługiwane*, jeśli *Wyświetlanie* jest ustawione na „Pasek” lub „Wskaźniki”
Max	1	columns.0.max	Dowolna wartość liczbowa. Zachowanie parametru: - *obsługiwane*, jeśli *Wyświetlanie* jest ustawione na „Pasek” lub „Wskaźniki”
Progi			
Kolor	1	columns.0.thresholds.color	Szesnastkowy kod koloru (np. FF0000).
Próg	1	columns.0.thresholds.threshold	Dowolna wartość liczbowa. Sufiksy (np. „1d”, „2w”, „4K”, „8G”) są obsługiwane.
Dane historyczne	0	columns.0.history	0 - *(domyślnie)* Auto; 1 - Historia; 2 - Trendy.

Następujące parametry kolumn są obsługiwane, jeśli skonfigurowana *pozycja* jest pozycją typu znakowego, tekstowego lub log.

Parametr	type	name	value
Wyróżnienia			
Wyróżnienie	1	columns.0.highlights.color	Szesnastkowy kod koloru (np. FF0000).
Próg	1	columns.0.highlights.pattern	Dowolne wyrażenie regularne.
Wyświetlanie	0	columns.0.display	1 - *(domyślnie)* Bez zmian; 4 - HTML; 5 - Pojedyncza linia.

Parametr	type	name	value
Pojedyncza linia	0	columns.0.max_length	Możliwe wartości mieszczą się w zakresie 1-500. Domyślnie: 100. Zachowanie parametru: - *obsługiwane*, jeśli *Wyświetlanie* jest ustawione na „Pojedyncza linia”
Użyj czcionki o stałej szerokości	0	columns.0.monospace_font	0 - *(domyślnie)* Użyj domyślnej czcionki; 1 - Użyj czcionki o stałej szerokości.
Wyświetl czas lokalny	0	columns.0.local_time	0 - *(domyślnie)* Wyświetl znacznik czasu; 1 - Wyświetl czas lokalny. Zachowanie parametru: - *obsługiwane*, jeśli *pozycja* jest ustawiona jako pozycja typu log, a *Pokaż znacznik czasu* jest ustawione na „Włączone”

Następujące parametry kolumn są obsługiwane, jeśli skonfigurowana *pozycja* jest pozycją typu binarnego.

Parametr	type	nazwa	wartość
Pokaż miniaturę	1	columns.0.show_thumbnail	0 - *(domyślnie)* Wyłączone; 1 - Włączone.

Konfiguracja zaawansowana

Poniższe zaawansowane parametry konfiguracji są obsługiwane przez widżet *Historia pozycji*.

Parametr	type	name	value
Nowe wartości	0	sortorder	0 - *(domyślnie)* U góry; 1 - Na dole.
Pokaż znacznik czasu	0	show_timestamp	0 - *(domyślnie)* Wyłączone; 1 - Włączone.
Pokaż nagłówek kolumny	0	show_column_header	0 - Wył.; 1 - Poziomo; 2 - *(domyślnie)* Pionowo.
Okres czasu	1	time_period._reference	`DASHBOARD._timeperiod` - ustaw selektor okresu czasu pulpitu jako źródło danych; `ABCDE._timeperiod` - ustaw kompatybilny widżet (z parametrem *Reference* ustawionym na ”`ABCDE`”) jako źródło danych. Domyślnie: `DASHBOARD._timeperiod` Alternatywnie można ustawić okres czasu tylko w parametrach *Od* i *Do*.
Od	1	time_period.from	Prawidłowy ciąg czasu w składni bezwzględnej (`YYYY-MM-DD hh:mm:ss`) lub względnej (`now`, `now/d`, `now/w-1w` itd.). Zachowanie parametru: - *obsługiwany*, jeśli *Okres czasu* nie jest ustawiony - *wymagany*, jeśli ustawiono `time_period.to`

Parametr	type	name	value
Do	1	time_period.to	Prawidłowy ciąg czasu w składni bezwzględnej (`YYYY-MM-DD hh:mm:ss`) lub względnej (`now`, `now/d`, `now/w-1w` itd.). Zachowanie parametru: - *obsługiwany*, jeśli *Okres czasu* nie jest ustawiony - *wymagany*, jeśli ustawiono `time_period.from`

Przykłady

Poniższe przykłady mają na celu jedynie opisanie konfiguracji obiektów pól widżetu pulpitu dla widżetu *Item history*. Więcej informacji na temat konfiguracji pulpitu można znaleźć w `dashboard.create`.

Konfigurowanie widżetu *Historia pozycji*

Skonfiguruj widżet *Historia pozycji*, który wyświetla najnowsze dane dla dwóch numerycznych pozycji „42269” i „42270”. Dodatkowo skonfiguruj kolumny pozycji tak, aby były wyświetlane pionowo, z nazwami kolumn wyświetlanymi poziomo; ogranicz widok do 15 wierszy danych i uwzględnij osobną kolumnę znacznika czasu.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "dashboard.create",
    "params": {
        "name": "My dashboard",
        "display_period": 30,
        "auto_start": 1,
        "pages": [
            {
                "widgets": [
                    {
                        "type": "itemhistory",
                        "name": "Item history",
                        "x": "0",
                        "y": "0",
                        "width": "18",
                        "height": "6",
                        "view_mode": "0",
                        "fields": [
                            {
                                "type": "0",
                                "name": "layout",
                                "value": "1"
                            },
                            {
                                "type": "1",
                                "name": "columns.0.name",
                                "value": "CPU utilization"
                            },
                            {
                                "type": "4",
                                "name": "columns.0.itemid",
                                "value": "42269"
                            },
                            {
                                "type": "1",
                                "name": "columns.1.name",
                                "value": "Memory utilization"
                            },
                            {
                                "type": "4",
                                "name": "columns.1.itemid",
                                "value": "42270"
```

```
                            },
                            {
                                "type": "0",
                                "name": "show_lines",
                                "value": "15"
                            },
                            {
                                "type": "0",
                                "name": "show_timestamp",
                                "value": "1"
                            },
                            {
                                "type": "0",
                                "name": "show_column_header",
                                "value": "1"
                            },
                            {
                                "type": "1",
                                "name": "reference",
                                "value": "KIVKD"
                            }
                        ]
                    }
                ]
            }
        ],
        "userGroups": [
            {
                "usrgrpid": 7,
                "permission": 2
            }
        ],
        "users": [
            {
                "userid": 1,
                "permission": 3
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "3"
        ]
    },
    "id": 1
}
```

Zobacz także

- Pole widżetu pulpitu
- `dashboard.create`
- `dashboard.update`

17 Nawigator pozycji

Opis

Te parametry oraz możliwe wartości właściwości dla odpowiednich obiektów pól widgetu umożliwiają skonfigurowanie widgetu *Item navigator* w metodach `dashboard.create` i `dashboard.update`.

Attention:
Właściwości `fields` widgetu nie są walidowane podczas tworzenia ani aktualizacji pulpitu. Pozwala to użytkownikom modyfikować wbudowane widgety i tworzyć własne widgety, ale jednocześnie wprowadza ryzyko nieprawidłowego tworzenia lub aktualizowania widgetów. Aby zapewnić pomyślne utworzenie lub zaktualizowanie widgetu *Item navigator*, zapoznaj się z zachowaniem parametrów opisanym w poniższych tabelach.

Parametry

Następujące parametry są obsługiwane dla widżetu *Nawigator pozycji*.

Parametr	type	name	value
Interwał odświeżania	0	rf_rate	0 - Bez odświeżania; 10 - 10 sekund; 30 - 30 sekund; 60 - *(domyślnie)* 1 minuta; 120 - 2 minuty; 600 - 10 minut; 900 - 15 minut.
Grupy hostów	2	groupids.0	ID grupy hostów. Uwaga: Aby skonfigurować wiele grup hostów, utwórz obiekt pola widżetu pulpitu dla każdej grupy hostów z inkrementowanym numerem w nazwie właściwości. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Grupy hostów (Widżet)	1	groupids._reference	Zamiast ID grupy hostów: `ABCDE._hostgroupids` - ustaw kompatybilny widżet (z parametrem *Reference* ustawionym na "ABCDE") jako źródło danych dla grup hostów. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Hosty	3	hostids.0	ID hosta. Uwaga: Aby skonfigurować wiele hostów, utwórz obiekt pola widżetu pulpitu dla każdego hosta z inkrementowanym numerem w nazwie właściwości. W przypadku wielu hostów parametr *Grupy hostów* nie może być w ogóle skonfigurowany albo musi być skonfigurowany z co najmniej jedną grupą hostów, do której należą skonfigurowane hosty. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Hosty (Widżet/Pulpit)	1	hostids._reference	Zamiast ID hosta: `DASHBOARD.hostid` - ustaw selektor hosta pulpitu jako źródło danych dla hostów; `ABCDE._hostid` - ustaw kompatybilny widżet (z parametrem *Reference* ustawionym na "ABCDE") jako źródło danych dla hostów. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Tagi hosta			
Typ oceny	0	host_tags_evaltype	0 - *(domyślnie)* I/Lub; 2 - Lub. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.

Parametr	type	name	value
Nazwa tagu	1	host_tags.0.tag	Dowolna wartość tekstowa. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście oceny tagów. Zachowanie parametru: - *wymagane* przy konfigurowaniu *Tagów hosta* Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Operator	0	host_tags.0.operator	0 - Zawiera; 1 - Równa się; 2 - Nie zawiera; 3 - Nie równa się; 4 - Istnieje; 5 - Nie istnieje. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście oceny tagów. Zachowanie parametru: - *wymagane* przy konfigurowaniu *Tagów hosta* Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Wartość tagu	1	host_tags.0.value	Dowolna wartość tekstowa. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście oceny tagów. Zachowanie parametru: - *wymagane* przy konfigurowaniu *Tagów hosta* Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Wzorce pozycji	1	items.0	Nazwa lub wzorzec pozycji. Uwaga: Aby skonfigurować wiele wzorców pozycji, utwórz obiekt pola widżetu pulpitu dla każdego wzorca pozycji z inkrementowanym numerem w nazwie właściwości.
Tagi pozycji			
Typ oceny	0	item_tags_evaltype	0 - *(domyślnie)* I/Lub; 2 - Lub.
Nazwa tagu	1	item_tags.0.tag	Dowolna wartość tekstowa. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście oceny tagów. Zachowanie parametru: - *wymagane* przy konfigurowaniu *Tagów pozycji*

Parametr	type	name	value
Operator	0	item_tags.0.operator	0 - Zawiera; 1 - Równa się; 2 - Nie zawiera; 3 - Nie równa się; 4 - Istnieje; 5 - Nie istnieje. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście oceny tagów. Zachowanie parametru: - *wymagane* przy konfigurowaniu *Tagów pozycji*
Wartość tagu	1	item_tags.0.value	Dowolna wartość tekstowa. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście oceny tagów. Zachowanie parametru: - *wymagane* przy konfigurowaniu *Tagów pozycji*
Stan	0	state	-1 - *(domyślnie)* Wszystkie; 0 - Normalny; 1 - Nieobsługiwane.
Pokaż problemy	0	show_problems	0 - Wszystkie; 1 - *(domyślnie)* Nieutłumione; 2 - Brak.
Grupuj według			
Atrybut	0	group_by.0.attribute	0 - Grupa hostów; 1 - Nazwa hosta; 2 - Wartość tagu hosta; 3 - Wartość tagu pozycji. Uwaga: Numer w nazwie właściwości odnosi się do kolejności atrybutu na liście atrybutów grupowania. Zachowanie parametru: - *wymagane* przy konfigurowaniu *Grupuj według*
Wartość	1	group_by.0.tag_name	Dowolna wartość tekstowa. Uwaga: Numer w nazwie właściwości odnosi się do atrybutu grupowania ustawionego w parametrze *Atrybut*. Zachowanie parametru: - *wymagane* przy konfigurowaniu *Grupuj według*, gdy *Atrybut* jest ustawiony na ”Wartość tagu hosta” lub ”Wartość tagu pozycji”
Limit pozycji	0	show_lines	Możliwe wartości mieszczą się w zakresie 1-9999. Domyślnie: 100.
Reference	1	reference	Dowolna wartość tekstowa składająca się z 5 znaków (np. `ABCDE` lub `JBPNL`). Ta wartość musi być unikalna w obrębie pulpitu, do którego należy widżet. Zachowanie parametru: - *wymagane*

Przykłady

Poniższe przykłady mają na celu jedynie opisanie konfiguracji obiektów pól widżetu pulpitu dla widżetu *Item navigator*. Więcej informacji na temat konfiguracji pulpitu można znaleźć w `dashboard.create`.

Konfigurowanie widżetu *Nawigator pozycji*

Skonfiguruj widżet *Nawigator pozycji*, który wyświetla do 1000 pozycji pogrupowanych według ich hosta, a następnie według wartości tagu pozycji „component”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "dashboard.create",
    "params": {
        "name": "My dashboard",
        "display_period": "30",
        "auto_start": "1",
        "pages": [
            {
                "widgets": [
                    {
                        "type": "itemnavigator",
                        "name": "Item navigator",
                        "x": "0",
                        "y": "0",
                        "width": "12",
                        "height": "5",
                        "view_mode": "0",
                        "fields": [
                            {
                                "type": 0,
                                "name": "group_by.0.attribute",
                                "value": 0
                            },
                            {
                                "type": 0,
                                "name": "group_by.1.attribute",
                                "value": 3
                            },
                            {
                                "type": 1,
                                "name": "group_by.1.tag_name",
                                "value": "component"
                            },
                            {
                                "type": 0,
                                "name": "show_lines",
                                "value": 1000
                            },
                            {
                                "type": 1,
                                "name": "reference",
                                "value": "DFNLK"
                            }
                        ]
                    }
                ]
            }
        ],
        "userGroups": [
            {
                "usrgrpid": 7,
                "permission": 2
            }
        ],
        "users": [
            {
                "userid": 1,
                "permission": 3
```

```
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "3"
        ]
    },
    "id": 1
}
```

Zobacz także

- Pole widżetu pulpitu
- `dashboard.create`
- `dashboard.update`

18 Wartość pozycji

Opis

Te parametry oraz możliwe wartości właściwości dla odpowiednich obiektów pól widgetu umożliwiają skonfigurowanie widgetu *Wartość pozycji* w metodach `dashboard.create` i `dashboard.update`.

Attention:
Właściwości `fields` widgetu nie są walidowane podczas tworzenia ani aktualizacji pulpitu. Pozwala to użytkownikom modyfikować wbudowane widgety i tworzyć własne widgety, ale jednocześnie wprowadza ryzyko nieprawidłowego tworzenia lub aktualizowania widgetów. Aby zapewnić pomyślne utworzenie lub zaktualizowanie widgetu *Wartość pozycji*, zapoznaj się z zachowaniem parametrów opisanym w poniższych tabelach.

Parametry

Następujące parametry są obsługiwane dla widżetu *Wartość pozycji*.

Parametr	type	name	value
Interwał odświeżania	0	rf_rate	0 - Brak odświeżania; 10 - 10 sekund; 30 - 30 sekund; 60 - *(domyślnie)* 1 minuta; 120 - 2 minuty; 600 - 10 minut; 900 - 15 minut.
Pozycja	4	itemid.0	ID pozycji. Zachowanie parametrów: - *wymagane*, jeśli *Pozycja (widżet)* nie jest ustawiona
Pozycja (widżet)	1	itemid._reference	Zamiast ID pozycji: `ABCDE._itemid` - ustaw kompatybilny widżet (z parametrem *Odwołanie* ustawionym na "ABCDE") jako źródło danych dla pozycji. Zachowanie parametrów: - *wymagane*, jeśli *Pozycja* nie jest ustawiona

Parametr	type	name	value
Pokaż	0	show.0	1 - Opis; 2 - Wartość; 3 - Czas; 4 - Wskaźnik zmiany; 5 - Wykres przebiegu. Domyślnie: 1, 2, 3, 4. Uwaga: Aby skonfigurować wiele wartości, utwórz obiekt pola widżetu pulpitu dla każdej wartości z inkrementowanym numerem w nazwie właściwości.
Nadpisz host	1	override_hostid._reference	`ABCDE._hostid` - ustaw kompatybilny widżet (z parametrem *Odwołanie* ustawionym na "ABCDE") jako źródło danych dla hostów; `DASHBOARD._hostid` - ustaw selektor hosta pulpitu jako źródło danych dla hostów. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.

Zaawansowana konfiguracja

Dla widżetu *Wartość pozycji* obsługiwane są następujące zaawansowane parametry konfiguracji.

Note:
Liczba w nazwie właściwości *Thresholds* (na przykład thresholds.0.color) odnosi się do miejsca progu na liście posortowanej rosnąco. Jeśli jednak progi zostaną skonfigurowane w innej kolejności, wartości zostaną posortowane rosnąco po zaktualizowaniu konfiguracji widżetu w frontend Zabbix (na przykład `"thresholds.0.threshold":"5"` → `"thresholds.0.threshold":"1"`; `"thresholds.1.threshold":"1"` → `"thresholds.1.threshold": "5"`).

Parameter	type	name	value
Kolor tła	1	bg_color	Szesnastkowy kod koloru (na przykład `FF0000`). Domyślnie: `""` (puste).
Progi			
Kolor	1	thresholds.0.color	Szesnastkowy kod koloru (na przykład `FF0000`).
Próg	1	thresholds.0.threshold	Dowolna wartość tekstowa.
Funkcja agregacji	0	aggregate_function	0 - *(domyślnie)* nieużywana; 1 - min; 2 - max; 3 - avg; 4 - count; 5 - sum; 6 - first; 7 - last.
Okres czasu	1	time_period._reference	`DASHBOARD._timeperiod` - ustaw selektor okresu czasu pulpitu jako źródło danych; `ABCDE._timeperiod` - ustaw kompatybilny widżet (z parametrem `reference` równym `ABCDE`) jako źródło danych. Domyślnie: `DASHBOARD._timeperiod` Alternatywnie można ustawić okres czasu tylko w parametrach *Od* i *Do*. Zachowanie parametru: - *obsługiwany*, jeśli *Funkcja agregacji* jest ustawiona na "min", "max", "avg", "count", "sum", "first", "last"

Parameter	type	name	value
Od	1	time_period.from	Prawidłowy ciąg czasu w składni bezwzględnej (`YYYY-MM-DD hh:mm:ss`) lub względnej (`now`, `now/d`, `now/w-1w` itd.). Zachowanie parametru: - *obsługiwany*, jeśli *Okres czasu* nie jest ustawiony, a *Funkcja agregacji* jest ustawiona na ”min”, ”max”, ”avg”, ”count”, ”sum”, ”first”, ”last” - *wymagany*, jeśli ustawiono `time_period.to`
Do	1	time_period.to	Prawidłowy ciąg czasu w składni bezwzględnej (`YYYY-MM-DD hh:mm:ss`) lub względnej (`now`, `now/d`, `now/w-1w` itd.). Zachowanie parametru: - *obsługiwany*, jeśli *Okres czasu* nie jest ustawiony, a *Funkcja agregacji* jest ustawiona na ”min”, ”max”, ”avg”, ”count”, ”sum”, ”first”, ”last” - *wymagany*, jeśli ustawiono `time_period.from`
Dane historyczne	0	history	0 - *(domyślnie)* Auto; 1 - Historia; 2 - Trendy.

Opis

Następujące zaawansowane parametry konfiguracji są obsługiwane, jeśli opcja *Pokaż* jest ustawiona na „Opis”.

Parametr	type	name	value
Opis	1	description	Dowolna wartość tekstowa, w tym makra. Obsługiwane makra: {HOST.*}, {ITEM.*}, {INVENTORY.*}, makra użytkownika. Domyślnie: {ITEM.NAME}.
Pozycja pozioma	0	desc_h_pos	0 - Lewo; 1 - *(domyślnie)* Środek; 2 - Prawo. Dwa lub więcej elementów (Opis, Wartość, Czas) nie może współdzielić tej samej *Pozycji poziomej* i *Pozycji pionowej*.
Pozycja pionowa	0	desc_v_pos	0 - Góra; 1 - Środek; 2 - *(domyślnie)* Dół. Dwa lub więcej elementów (Opis, Wartość, Czas) nie może współdzielić tej samej *Pozycji poziomej* i *Pozycji pionowej*.
Rozmiar	0	desc_size	Możliwe wartości mieszczą się w zakresie 1-100. Domyślnie: 15.
Pogrubienie	0	desc_bold	0 - *(domyślnie)* Wyłączone; 1 - Włączone.
Kolor	1	desc_color	Szesnastkowy kod koloru (np. `FF0000`). Domyślnie: `""` (puste).

Wartość

Następujące zaawansowane parametry konfiguracji są obsługiwane, jeśli dla opcji *Pokaż* ustawiono wartość „Wartość”.

Parametr	type	name	value
Miejsca dziesiętne			

Parametr	type	name	value
Miejsca dziesiętne	0	decimal_places	Możliwe wartości mieszczą się w zakresie 1-10. Domyślnie: 2.
Rozmiar	0	decimal_size	Możliwe wartości mieszczą się w zakresie 1-100. Domyślnie: 35.
Pozycja			
Pozycja pozioma	0	value_h_pos	0 - Lewo; 1 - *(domyślnie)* Środek; 2 - Prawo. Dwa lub więcej elementów (Opis, Wartość, Czas) nie może mieć tej samej *Pozycji poziomej* i *Pozycji pionowej*.
Pozycja pionowa	0	value_v_pos	0 - Góra; 1 - *(domyślnie)* Środek; 2 - Dół. Dwa lub więcej elementów (Opis, Wartość, Czas) nie może mieć tej samej *Pozycji poziomej* i *Pozycji pionowej*.
Rozmiar	0	value_size	Możliwe wartości mieszczą się w zakresie 1-100. Domyślnie: 45.
Pogrubienie	0	value_bold	0 - Wyłączone; 1 - *(domyślnie)* Włączone.
Kolor	1	value_color	Szesnastkowy kod koloru (np. FF0000). Domyślnie: "" (puste).
Jednostki			
Jednostki (pole wyboru)	0	units_show	0 - Wyłączone; 1 - *(domyślnie)* Włączone.
Jednostki (wartość)	1	units	Dowolna wartość tekstowa.
Pozycja	0	units_pos	0 - Przed wartością; 1 - Nad wartością; 2 - *(domyślnie)* Za wartością; 3 - Pod wartością.
Rozmiar	0	units_size	Możliwe wartości mieszczą się w zakresie 1-100. Domyślnie: 35.
Pogrubienie	0	units_bold	0 - Wyłączone; 1 - *(domyślnie)* Włączone.
Kolor	1	units_color	Szesnastkowy kod koloru (np. FF0000). Domyślnie: "" (puste).

Czas

Następujące zaawansowane parametry konfiguracji są obsługiwane, jeśli opcja *Pokaż* jest ustawiona na „Czas”.

Parametr	type	name	value
Pozycja pozioma	0	time_h_pos	0 - Lewo; 1 - *(domyślnie)* Środek; 2 - Prawo. Dwa lub więcej elementów (Opis, Wartość, Czas) nie mogą współdzielić tej samej *Pozycji poziomej* i *Pozycji pionowej*.

Parametr	type	name	value
Pozycja pionowa	0	time_v_pos	0 - *(domyślnie)* Góra; 1 - Środek; 2 - Dół. Dwa lub więcej elementów (Opis, Wartość, Czas) nie mogą współdzielić tej samej *Pozycji poziomej* i *Pozycji pionowej*.
Rozmiar	0	time_size	Możliwe wartości mieszczą się w zakresie 1-100. Domyślnie: 15.
Pogrubienie	0	time_bold	0 - *(domyślnie)* Wyłączone; 1 - Włączone.
Kolor	1	time_color	Szesnastkowy kod koloru (np. FF0000). Domyślnie: "" (puste).

Wskaźnik zmiany

Następujące zaawansowane parametry konfiguracji są obsługiwane, jeśli dla opcji *Pokaż* ustawiono wartość „Wskaźnik zmiany”.

Parametr	type	name	value
Kolor wskaźnika zmiany ↑	1	up_color	Szesnastkowy kod koloru (np. FF0000). Domyślnie: "" (puste).
Kolor wskaźnika zmiany ↓	1	down_color	Szesnastkowy kod koloru (np. FF0000). Domyślnie: "" (puste).
Kolor wskaźnika zmiany ↕	1	updown_color	Szesnastkowy kod koloru (np. FF0000). Domyślnie: "" (puste).

Sparkline

Następujące zaawansowane parametry konfiguracji są obsługiwane, jeśli opcja *Pokaż* jest ustawiona na „Sparkline”.

Parametr	type	name	value
Szerokość	0	sparkline.width	Możliwe wartości mieszczą się w zakresie 0-10. Domyślnie: 1.
Wypełnienie	0	sparkline.fill	Możliwe wartości mieszczą się w zakresie 0-10. Domyślnie: 3.
Kolor	1	sparkline.color	Szesnastkowy kod koloru (np. FF0000). Domyślnie: 42A5F5.
Okres czasu	1	sparkline.time_period.from	DASHBOARD._timeperiod — ustaw selektor okresu czasu pulpitu jako źródło danych; ABCDE._timeperiod — ustaw kompatybilny widget (z parametrem reference równym ABCDE) jako źródło danych. Domyślnie: DASHBOARD._timeperiod Alternatywnie można ustawić okres czasu tylko w parametrach *Od* i *Do*.
Od	1	sparkline.time_period.from	Prawidłowy ciąg czasu w składni czasu bezwzględnego (YYYY-MM-DD hh:mm:ss) lub względnego (now, now/d, now/w-1w itd.). Zachowanie parametru: - *wymagany*, jeśli ustawiono sparkline.time_period.to

Parametr	type	name	value
Do	1	sparkline.time_period.to	Prawidłowy ciąg czasu w składni czasu bezwzględnego (`YYYY-MM-DD hh:mm:ss`) lub względnego (`now`, `now/d`, `now/w-1w` itd.). Zachowanie parametru: - *wymagany*, jeśli ustawiono `sparkline.time_period.from`
Dane historyczne	0	sparkline.history	0 — *(domyślnie)* Auto; 1 — Historia; 2 — Trendy.

Przykłady

Poniższe przykłady mają na celu jedynie opisanie konfiguracji obiektów pól widżetu pulpitu dla widżetu *Wartość pozycji*. Więcej informacji na temat konfiguracji pulpitu można znaleźć w `dashboard.create`.

Konfigurowanie widżetu *Wartość pozycji*

Skonfiguruj widżet *Wartość pozycji*, który wyświetla wartość pozycji dla pozycji „42266” (dostępność agenta Zabbix). Dodatkowo dostosuj wizualnie widżet za pomocą wielu zaawansowanych opcji, w tym dynamicznego koloru tła, który zmienia się w zależności od stanu dostępności agenta Zabbix.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "dashboard.create",
    "params": {
        "name": "My dashboard",
        "display_period": 30,
        "auto_start": 1,
        "pages": [
            {
                "widgets": [
                    {
                        "type": "item",
                        "name": "Item value",
                        "x": 0,
                        "y": 0,
                        "width": 12,
                        "height": 3,
                        "view_mode": 0,
                        "fields": [
                            {
                                "type": 4,
                                "name": "itemid.0",
                                "value": 42266
                            },
                            {
                                "type": 0,
                                "name": "show.0",
                                "value": 1
                            },
                            {
                                "type": 0,
                                "name": "show.1",
                                "value": 2
                            },
                            {
                                "type": 0,
                                "name": "show.2",
                                "value": 3
                            },
```

```
                {
                    "type": 1,
                    "name": "description",
                    "value": "Agent status"
                },
                {
                    "type": 0,
                    "name": "desc_h_pos",
                    "value": 0
                },
                {
                    "type": 0,
                    "name": "desc_v_pos",
                    "value": 0
                },
                {
                    "type": 0,
                    "name": "desc_bold",
                    "value": 1
                },
                {
                    "type": 1,
                    "name": "desc_color",
                    "value": "F06291"
                },
                {
                    "type": 0,
                    "name": "value_h_pos",
                    "value": 0
                },
                {
                    "type": 0,
                    "name": "value_size",
                    "value": 25
                },
                {
                    "type": 1,
                    "name": "value_color",
                    "value": "FFFF00"
                },
                {
                    "type": 0,
                    "name": "units_show",
                    "value": 0
                },
                {
                    "type": 0,
                    "name": "time_h_pos",
                    "value": 2
                },
                {
                    "type": 0,
                    "name": "time_v_pos",
                    "value": 2
                },
                {
                    "type": 0,
                    "name": "time_size",
                    "value": 10
                },
                {
                    "type": 0,
```

```
                                "name": "time_bold",
                                "value": 1
                            },
                            {
                                "type": 1,
                                "name": "time_color",
                                "value": "9FA8DA"
                            },
                            {
                                "type": 1,
                                "name": "thresholds.0.color",
                                "value": "E1E1E1"
                            },
                            {
                                "type": 1,
                                "name": "thresholds.0.threshold",
                                "value": "0"
                            },
                            {
                                "type": 1,
                                "name": "thresholds.1.color",
                                "value": "D1C4E9"
                            },
                            {
                                "type": 1,
                                "name": "thresholds.1.threshold",
                                "value": "1"
                            }
                        ]
                    }
                ]
            }
        ],
        "userGroups": [
            {
                "usrgrpid": 7,
                "permission": 2
            }
        ],
        "users": [
            {
                "userid": 1,
                "permission": 3
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "3"
        ]
    },
    "id": 1
}
```

Zobacz także

- Pole widżetu pulpitu

- `dashboard.create`
- `dashboard.update`

19 Mapa

Opis

Te parametry oraz możliwe wartości właściwości dla odpowiednich obiektów pól widgetu umożliwiają skonfigurowanie widgetu *Map* w metodach `dashboard.create` i `dashboard.update`.

Attention:
Właściwości `fields` widgetu nie są walidowane podczas tworzenia ani aktualizacji dashboardu. Pozwala to użytkownikom modyfikować wbudowane widgety i tworzyć własne widgety, ale jednocześnie wprowadza ryzyko nieprawidłowego tworzenia lub aktualizowania widgetów. Aby zapewnić pomyślne utworzenie lub aktualizację widgetu *Map*, zapoznaj się z zachowaniem parametrów opisanym w poniższych tabelach.

Parametry

Następujące parametry są obsługiwane dla widżetu *Mapa*.

Parametr	type	name	value
Interwał odświeżania	0	rf_rate	0 - Bez odświeżania; 10 - 10 sekund; 30 - 30 sekund; 60 - 1 minuta; 120 - 2 minuty; 600 - 10 minut; 900 - *(domyślnie)* 15 minut.
Mapa	8	sysmapid.0	ID mapy. Zachowanie parametru: - *wymagany*, jeśli *Mapa (widżet)* nie jest ustawiona
Mapa (widżet)	1	sysmapid._reference	`ABCDE._mapid` - ustawia widżet *Drzewo nawigacji map* (z parametrem *Odwołanie* ustawionym na "ABCDE") jako źródło danych dla map. Zachowanie parametru: - *wymagany*, jeśli *Mapa* nie jest ustawiona
Odwołanie	1	reference	Dowolna wartość tekstowa składająca się z 5 znaków (np. `ABCDE` lub `JBPNL`). Ta wartość musi być unikalna w obrębie pulpitu, do którego należy widżet. Zachowanie parametru: - *wymagany*

Przykłady

Poniższe przykłady mają na celu jedynie opisanie konfiguracji obiektów pól widżetu pulpitu dla widżetu *Mapa*. Więcej informacji na temat konfiguracji pulpitu można znaleźć w `dashboard.create`.

Konfigurowanie widżetu *Mapa*

Skonfiguruj widżet *Mapa*, który wyświetla mapę „1".

Żądanie:

```
{
"jsonrpc": "2.0",
"metoda": "dashboard.create",
"parametry": {
"nazwa": "Mój pulpit",
"okres_wyświetlania": 30,
"automatyczny_start": 1,
```

```
"strony": [
{
"widżety": [
{
"typ": "mapa",
"nazwa": "Mapa",
"x": 0,
"y": 0,
"szerokość": 54,
"wysokość": 5,
"tryb_widoku": 0,
"pola": [
{
"typ": 8,
"nazwa": "sysmapid.0",
"wartość": 1
}
]
}
]
}
],
"grupy_użytkowników": [
{
"usrgrpid": 7,
"permission": 2
}
],
"users": [
{
"userid": 1,
"permission": 3
}
]
},
"id": 1
}
```

Odpowiedź:

```
{
"jsonrpc": "2.0",
"result": {
"dashboardids": [
"3"
]
},
"id": 1
}
```

Konfigurowanie połączonego widżetu *Mapa*

Skonfiguruj widżet *Mapa* połączony z widżetem *Drzewo nawigacji mapy*.

Żądanie:

```
{
"jsonrpc": "2.0",
"metoda": "dashboard.create",
"parametry": {
"nazwa": "Mój pulpit",
"okres_wyświetlania": 30,
"automatyczny_start": 1,
"strony": [
{
```

```
"widżety": [
{
"typ": "mapa",
"nazwa": "Mapa",
"x": 0,
"y": 5,
"szerokość": 54,
"wysokość": 5,
"tryb_widoku": 0,
"pola": [
{
"typ": 1,
"nazwa": "sysmapid._reference",
"wartość": "ABCDE._mapid"
}
]
},
{
"typ": „navtree”,
„name”: „Drzewo nawigacji mapy”,
„x”: 0,
„y”: 0,
„width”: 18,
„height”: 5,
„view_mode”: 0,
„fields”: [
{
„type”: 1,
„name”: „navtree.1.name”,
„value”: „Element A”
},
{
„type”: 1,
„name”: „navtree.2.name”,
„value”: „Element B”
},
{
„type”: 1,
„name”: „navtree.3.name”,
„value”: „Element C”
},
{
„type”: 1,
„name”: „navtree.4.name”,
„value”: „Element A1”
},
{
„type”: 1,
„name”: „navtree.5.name”,
„wartość”: „Element A2”
},
{
„typ”: 1,
„nazwa”: „navtree.6.name”,
„wartość”: „Element B1”
},
{
„typ”: 1,
„nazwa”: „navtree.7.name”,
„wartość”: „Element B2”
},
{
```

```
„typ": 0,
„nazwa": „navtree.4.parent",
„wartość": 1
},
{
„typ": 0,
„nazwa": „navtree.5.parent",
„wartość": 1
},
{
„typ": 0,
„nazwa": „navtree.6.parent",
„wartość": 2
},
{
„typ": 0,
„nazwa": „navtree.7.parent",
„wartość": 2
},
{
"typ": 0,
"nazwa": "navtree.1.order",
"wartość": 1
},
{
"typ": 0,
"nazwa": "navtree.2.order",
"wartość": 2
},
{
"typ": 0,
"nazwa": "navtree.3.order",
"wartość": 3
},
{
"typ": 0,
"nazwa": "navtree.4.order",
"wartość": 1
},
{
"typ": 0,
"nazwa": "navtree.5.order",
"wartość": 2
},
{
"typ": 0,
"nazwa": "navtree.6.order",
"wartość": 1
},
{
"typ": 0,
"nazwa": "navtree.7.order",
"wartość": 2
},
{
"type": 8,
"name": "navtree.6.sysmapid",
"value": 1
},
{
"type": 1,
"name": "reference",
```

```
"value": "ABCDE"
}
]
}
]
}
],
"userGroups": [
{
"usrgrpid": 7,
"permission": 2
}
],
"users": [
{
"userid": 1,
"permission": 3
}
]
},
"id": 1
}
```

Odpowiedź:

```
{
"jsonrpc": "2.0",
"result": {
"dashboardids": [
"3"
]
},
"id": 1
}
```

Zobacz także

- Pole widżetu pulpitu
- `dashboard.create`
- `dashboard.update`
- Drzewo nawigacyjne mapy

20 Drzewo nawigacji mapy

Opis

Te parametry oraz możliwe wartości właściwości dla odpowiednich obiektów pól widgetu umożliwiają skonfigurowanie widgetu *Drzewo nawigacji map* w metodach `dashboard.create` i `dashboard.update`.

Attention:
Właściwości `fields` widgetu nie są walidowane podczas tworzenia ani aktualizacji pulpitu. Pozwala to użytkownikom modyfikować wbudowane widgety i tworzyć własne widgety, ale jednocześnie wprowadza ryzyko nieprawidłowego tworzenia lub aktualizowania widgetów. Aby zapewnić pomyślne utworzenie lub zaktualizowanie widgetu *Drzewo nawigacji map*, zapoznaj się z zachowaniem parametrów opisanym w poniższych tabelach.

Parametry

Następujące parametry są obsługiwane dla widżetu *Drzewo nawigacji map*.

Parametr	type	name	value
Interwał odświeżania	0	rf_rate	0 - Brak odświeżania; 10 - 10 sekund; 30 - 30 sekund; 60 - 1 minuta; 120 - 2 minuty; 600 - 10 minut; 900 - *(domyślnie)* 15 minut.
Pokaż niedostępne mapy	1	show_unavailable	0 - *(domyślnie)* Wyłączone; 1 - Włączone.
Odwołanie	1	reference	Dowolna wartość tekstowa składająca się z 5 znaków (np. `ABCDE` lub `JBPNL`). Ta wartość musi być unikalna w obrębie pulpitu, do którego należy widżet. Zachowanie parametrów: - *wymagane*

Następujące parametry są obsługiwane przy konfigurowaniu elementów drzewa nawigacji map.

Parametr	type	name	value
Nazwa	1	navtree.1.name	Dowolna wartość tekstowa. Uwaga: Liczba w nazwie właściwości określa numer elementu.
Powiązana mapa	8	navtree.1.sysmapid	ID mapy. Uwaga: Liczba w nazwie właściwości odnosi się do elementu, z którym mapa jest powiązana.
Parametry tworzenia hierarchii elementów	0	navtree.1.parent	Numer elementu nadrzędnego. Uwaga: Liczba w nazwie właściwości odnosi się do elementu podrzędnego. Wartość właściwości odnosi się do elementu nadrzędnego.
	0	navtree.1.order	Pozycja elementu w drzewie nawigacji map. Uwaga: Liczba w nazwie właściwości odnosi się do numeru elementu. Wartość właściwości odnosi się do pozycji elementu w drzewie nawigacji map. Pozycja elementu nadrzędnego jest określana w obrębie całego drzewa nawigacji map. Pozycja elementu podrzędnego jest określana w obrębie elementu nadrzędnego.

Przykłady

Poniższe przykłady mają na celu jedynie opisanie konfiguracji obiektów pól widżetu pulpitu dla widżetu *Drzewo nawigacji map*. Więcej informacji na temat konfiguracji pulpitu można znaleźć w `dashboard.create`.

Konfigurowanie widżetu *Map navigation tree*

Skonfiguruj widżet *Map navigation tree*, który wyświetla następujące drzewo nawigacji map:

- Element A
  - Element A1
  - Element A2
- Element B
  - Element B1 (zawiera podlinkowaną mapę „1”, którą można wyświetlić w podlinkowanym widżecie *Map widget*)
  - Element B2
- Element C

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "dashboard.create",
    "params": {
```

```
        "name": "My dashboard",
        "display_period": 30,
        "auto_start": 1,
        "pages": [
            {
                "widgets": [
                    {
                        "type": "navtree",
                        "name": "Map navigation tree",
                        "x": 0,
                        "y": 0,
                        "width": 18,
                        "height": 5,
                        "view_mode": 0,
                        "fields": [
                            {
                                "type": 1,
                                "name": "navtree.1.name",
                                "value": "Element A"
                            },
                            {
                                "type": 1,
                                "name": "navtree.2.name",
                                "value": "Element B"
                            },
                            {
                                "type": 1,
                                "name": "navtree.3.name",
                                "value": "Element C"
                            },
                            {
                                "type": 1,
                                "name": "navtree.4.name",
                                "value": "Element A1"
                            },
                            {
                                "type": 1,
                                "name": "navtree.5.name",
                                "value": "Element A2"
                            },
                            {
                                "type": 1,
                                "name": "navtree.6.name",
                                "value": "Element B1"
                            },
                            {
                                "type": 1,
                                "name": "navtree.7.name",
                                "value": "Element B2"
                            },
                            {
                                "type": 0,
                                "name": "navtree.4.parent",
                                "value": 1
                            },
                            {
                                "type": 0,
                                "name": "navtree.5.parent",
                                "value": 1
                            },
                            {
                                "type": 0,
```

```
                            "name": "navtree.6.parent",
                            "value": 2
                        },
                        {
                            "type": 0,
                            "name": "navtree.7.parent",
                            "value": 2
                        },
                        {
                            "type": 0,
                            "name": "navtree.1.order",
                            "value": 1
                        },
                        {
                            "type": 0,
                            "name": "navtree.2.order",
                            "value": 2
                        },
                        {
                            "type": 0,
                            "name": "navtree.3.order",
                            "value": 3
                        },
                        {
                            "type": 0,
                            "name": "navtree.4.order",
                            "value": 1
                        },
                        {
                            "type": 0,
                            "name": "navtree.5.order",
                            "value": 2
                        },
                        {
                            "type": 0,
                            "name": "navtree.6.order",
                            "value": 1
                        },
                        {
                            "type": 0,
                            "name": "navtree.7.order",
                            "value": 2
                        },
                        {
                            "type": 8,
                            "name": "navtree.6.sysmapid",
                            "value": 1
                        },
                        {
                            "type": 1,
                            "name": "reference",
                            "value": "HJQXF"
                        }
                    ]
                }
            ]
        }
    ],
    "userGroups": [
        {
            "usrgrpid": 7,
            "permission": 2
```

```
            }
        ],
        "users": [
            {
                "userid": 1,
                "permission": 3
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "3"
        ]
    },
    "id": 1
}
```

Zobacz także

- Pole widżetu pulpitu
- `dashboard.create`
- `dashboard.update`
- Mapy

21 Wykres kołowy

Opis

Te parametry oraz możliwe wartości właściwości dla odpowiednich obiektów pól widgetu umożliwiają skonfigurowanie widgetu *Pie chart* w metodach `dashboard.create` i `dashboard.update`.

Attention:
Właściwości `fields` widgetu nie są walidowane podczas tworzenia ani aktualizacji pulpitu. Pozwala to użytkownikom modyfikować wbudowane widgety i tworzyć własne widgety, ale jednocześnie wprowadza ryzyko nieprawidłowego tworzenia lub aktualizowania widgetów. Aby zapewnić pomyślne utworzenie lub zaktualizowanie widgetu *Pie chart*, zapoznaj się z zachowaniem parametrów opisanym w poniższych tabelach.

Parametry

Następujące parametry są obsługiwane dla widżetu *Wykres kołowy*.

Parametr	type	name	value
Interwał odświeżania	0	rf_rate	0 - Bez odświeżania; 10 - 10 sekund; 30 - 30 sekund; 60 - *(domyślnie)* 1 minuta; 120 - 2 minuty; 600 - 10 minut; 900 - 15 minut.

Zestaw danych

Następujące parametry są obsługiwane przy konfigurowaniu *Zestawu danych*.

Note:
Pierwsza liczba w nazwie właściwości (np. ds.0.hosts.0, ds.0.items.0) oznacza konkretny zestaw danych, natomiast druga liczba, jeśli występuje, oznacza skonfigurowany host lub pozycję.

Parametr	type	name	value
Typ zestawu danych	0	ds.0.dataset_type	0 - Lista pozycji; 1 - *(domyślnie)* Wzorce pozycji.
Pozycje	4	ds.0.itemids.0	ID pozycji. Podczas konfigurowania widżetu na pulpicie szablonu należy ustawić tylko pozycje skonfigurowane w szablonie. Uwaga: Aby skonfigurować wiele pozycji, utwórz obiekt pola widżetu pulpitu dla każdej pozycji z inkrementowanym numerem w nazwie właściwości. Zachowanie parametru: - *wymagane*, jeśli *Typ zestawu danych* jest ustawiony na ”Lista pozycji”, a *Pozycje (Widżet)* nie są ustawione
Pozycje (Widżet)	1	ds.0.itemids.0._reference	Zamiast ID pozycji: `ABCDE._itemid` - ustaw kompatybilny widżet (z parametrem *Reference* ustawionym na ”ABCDE”) jako źródło danych dla pozycji. Uwaga: Aby skonfigurować wiele widżetów, utwórz obiekt pola widżetu pulpitu dla każdego widżetu z inkrementowanym numerem w nazwie właściwości. Zachowanie parametru: - *wymagane*, jeśli *Typ zestawu danych* jest ustawiony na ”Lista pozycji”, a *Pozycje* nie są ustawione
Kolor	1	ds.0.color.0	Szesnastkowy kod koloru (np. `FF0000`). Zachowanie parametru: - *wymagane*, jeśli *Typ zestawu danych* jest ustawiony na ”Lista pozycji”
Typ pozycji	0	ds.0.type.0	0 - *(domyślnie)* Normalny; 1 - Suma. Wartość ”Suma” można ustawić tylko dla jednej pozycji na całym wykresie. Zachowanie parametru: - *obsługiwane*, jeśli *Typ zestawu danych* jest ustawiony na ”Lista pozycji”
Wzorce hostów	1	ds.0.hosts.0	Nazwa lub wzorzec hosta (np. ”Zabbix*”). Zachowanie parametru: - *wymagane*, jeśli *Typ zestawu danych* jest ustawiony na ”Wzorce pozycji” Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Wzorce pozycji	1	ds.0.items.0	Nazwa lub wzorzec pozycji (np. ”*: Number of processed *values per second”). Podczas konfigurowania widżetu na pulpicie szablonu należy ustawić tylko wzorce dla pozycji skonfigurowanych w szablonie. Zachowanie parametru: - *wymagane*, jeśli *Typ zestawu danych* jest ustawiony na ”Wzorce pozycji”

Parametr	type	name	value
Kolor	1	ds.0.color	Szesnastkowy kod koloru (np. FF0000). Zachowanie parametru: - *obsługiwane*, jeśli *Typ zestawu danych* jest ustawiony na ”Wzorce pozycji”, a *Paleta kolorów* nie jest ustawiona
Paleta kolorów	0	ds.0.color_palette	Indeks palety kolorów. Możliwe wartości mieszczą się w zakresie 0-11. Domyślnie: 0. Zachowanie parametru: - *obsługiwane*, jeśli *Typ zestawu danych* jest ustawiony na ”Wzorce pozycji”, a *Kolor* nie jest ustawiony
Funkcja agregacji	0	ds.0.aggregate_function	1 - min; 2 - max; 3 - avg; 4 - count; 5 - sum; 6 - first; 7 - *(domyślnie)* last.
Agregacja zestawu danych	0	ds.0.dataset_aggregation	0 - *(domyślnie)* brak; 1 - min; 2 - max; 3 - avg; 4 - count; 5 - sum. Zachowanie parametru: - *obsługiwane*, jeśli *Typ pozycji* jest ustawiony na ”Suma”
Etykieta zestawu danych	1	ds.0.data_set_label	Dowolna wartość tekstowa. Domyślnie: "" (puste).
Tagi pozycji			
Typ oceny	0	ds.0.item_tags_evaltype	0 - *(domyślnie)* And/Or; 2 - Or.
Nazwa tagu	1	ds.0.item_tags.0.tag	Dowolna wartość tekstowa. Uwaga: Liczba w nazwie właściwości odnosi się do kolejności tagu na liście oceny tagów. Zachowanie parametru: - *wymagane* przy konfigurowaniu *Tagów pozycji*
Operator	0	ds.0.item_tags.0.operator	0 - Zawiera; 1 - Równe; 2 - Nie zawiera; 3 - Nie równa się; 4 - Istnieje; 5 - Nie istnieje. Uwaga: Liczba w nazwie właściwości odnosi się do kolejności tagu na liście oceny tagów. Zachowanie parametru: - *wymagane* przy konfigurowaniu *Tagów pozycji*

Parametr	type	name	value
Wartość tagu	1	ds.0.item_tags.0.value	Dowolna wartość tekstowa. Uwaga: Liczba w nazwie właściwości odnosi się do kolejności tagu na liście oceny tagów. Zachowanie parametru: - *wymagane* przy konfigurowaniu *Tagów pozycji*

Opcje wyświetlania

Następujące parametry są obsługiwane przy konfigurowaniu *opcji wyświetlania*.

Parameter	type	name	value
Wybór danych historycznych	0	source	0 - *(domyślnie)* Auto; 1 - Historia; 2 - Trendy.
Rysuj	0	draw_type	0 - *(domyślnie)* Wykres kołowy; 1 - Pierścień.
Szerokość	0	width	20 - 20% promienia; 30 - 30% promienia; 40 - 40% promienia; 50 - *(domyślnie)* 50% promienia. Zachowanie parametru: - *obsługiwane*, jeśli *Rysuj* jest ustawione na ”Pierścień”
Szerokość obramowania	0	stroke	Możliwe wartości mieszczą się w zakresie 0-10. Domyślnie: 0. Zachowanie parametru: - *obsługiwane*, jeśli *Rysuj* jest ustawione na ”Pierścień”
Pokaż wartość całkowitą	0	total_show	0 - *(domyślnie)* Wyłączone; 1 - Włączone. Zachowanie parametru: - *obsługiwane*, jeśli *Rysuj* jest ustawione na ”Pierścień”
Rozmiar	0	value_size_type	0 - *(domyślnie)* Auto; 1 - Niestandardowy. Zachowanie parametru: - *obsługiwane*, jeśli *Pokaż wartość całkowitą* jest ustawione na ”Włączone”
Rozmiar (wartość dla rozmiaru niestandardowego)	0	value_size	Możliwe wartości mieszczą się w zakresie 1-100. Domyślnie: 20. Zachowanie parametru: - *obsługiwane*, jeśli *Pokaż wartość całkowitą* jest ustawione na ”Włączone”
Miejsca dziesiętne	0	decimal_places	Możliwe wartości mieszczą się w zakresie 0-6. Domyślnie: 2. Zachowanie parametru: - *obsługiwane*, jeśli *Pokaż wartość całkowitą* jest ustawione na ”Włączone”

Parameter	type	name	value
Jednostki (pole wyboru)	0	units_show	0 - *(domyślnie)* Wyłączone; 1 - Włączone. Zachowanie parametru: - *obsługiwane*, jeśli *Pokaż wartość całkowitą* jest ustawione na ”Włączone”
Jednostki (wartość)	1	units	Dowolna wartość tekstowa. Zachowanie parametru: - *obsługiwane*, jeśli *Jednostki* (pole wyboru) jest ustawione na ”Włączone”
Pogrubienie	0	value_bold	0 - *(domyślnie)* Wyłączone; 1 - Włączone. Zachowanie parametru: - *obsługiwane*, jeśli *Pokaż wartość całkowitą* jest ustawione na ”Włączone”
Kolor	1	value_color	Szesnastkowy kod koloru (np. FF0000). Zachowanie parametru: - *obsługiwane*, jeśli *Pokaż wartość całkowitą* jest ustawione na ”Włączone”
Odstęp między sek-torami	0	space	Możliwe wartości mieszczą się w zakresie 0-10. Domyślnie: 1.
Scal sek-tory mniejsze niż N% (pole wyboru)	0	merge	0 - *(domyślnie)* Wyłączone; 1 - Włączone.
Scal sek-tory mniejsze niż N% (wartość)	0	merge_percent	Możliwe wartości mieszczą się w zakresie 1-10. Domyślnie: 1. Zachowanie parametru: - *obsługiwane*, jeśli *Scal sektory mniejsze niż N%* (pole wyboru) jest ustawione na ”Włączone”
Scal sek-tory mniejsze niż N% (kolor)	1	merge_color	Szesnastkowy kod koloru (np. FF0000). Zachowanie parametru: - *obsługiwane*, jeśli *Scal sektory mniejsze niż N%* (pole wyboru) jest ustawione na ”Włączone”

Okres czasu

Następujące parametry są obsługiwane przy konfigurowaniu *Okresu czasu*.

Parametr	type	name	value
Okres czasu	1	time_period._referenda	`DASHBOARD._timeperiod` - ustaw selektor okresu czasu pulpitu jako źródło danych; `ABCDE._timeperiod` - ustaw kompatybilny widget (z parametrem *Reference* ustawionym na "ABCDE") jako źródło danych. Domyślnie: `DASHBOARD._timeperiod` Alternatywnie możesz ustawić okres czasu tylko w parametrach *Od* i *Do*.
Od	1	time_period.from	Prawidłowy ciąg czasu w składni czasu bezwzględnego (`YYYY-MM-DD hh:mm:ss`) lub względnego (`now`, `now/d`, `now/w-1w` itd.). Zachowanie parametru: - *obsługiwany*, jeśli *Okres czasu* nie jest ustawiony - *wymagany*, jeśli ustawiono `time_period.to`
Do	1	time_period.to	Prawidłowy ciąg czasu w składni czasu bezwzględnego (`YYYY-MM-DD hh:mm:ss`) lub względnego (`now`, `now/d`, `now/w-1w` itd.). Zachowanie parametru: - *obsługiwany*, jeśli *Okres czasu* nie jest ustawiony - *wymagany*, jeśli ustawiono `time_period.from`

Legenda

Następujące parametry są obsługiwane przy konfigurowaniu *Legendy*.

Parametr	type	name	value
Pokaż legendę	0	legend	0 - Wyłączone; 1 - *(domyślnie)* Włączone.
Pokaż wartość	0	legend_value	0 - *(domyślnie)* Wyłączone; 1 - Włączone. Zachowanie parametru: - *obsługiwane*, jeśli *Pokaż legendę* jest ustawione na "Włączone"
Pokaż funkcję agregacji	0	legend_aggregation	0 - *(domyślnie)* Wyłączone; 1 - Włączone. Zachowanie parametru: - *obsługiwane*, jeśli *Pokaż legendę* jest ustawione na "Włączone"
Wiersze	0	legend_lines_mode	0 - *(domyślnie)* Stałe; 1 - Zmienne. Zachowanie parametru: - *obsługiwane*, jeśli *Pokaż legendę* jest ustawione na "Włączone"
Liczba wierszy/ Maksymalna liczba wierszy	0	legend_lines	Możliwe wartości mieszczą się w zakresie od 1 do 10. Domyślnie: 1. Zachowanie parametru: - *obsługiwane*, jeśli *Pokaż legendę* jest ustawione na "Włączone"
Liczba kolumn	0	legend_columns	Możliwe wartości mieszczą się w zakresie od 1 do 4. Domyślnie: 4. Zachowanie parametru: - *obsługiwane*, jeśli *Pokaż wartość* jest ustawione na "Włączone"

Przykłady

Poniższe przykłady mają na celu jedynie opisanie konfiguracji obiektów pól widżetu pulpitu dla widżetu *Pie chart*. Więcej informacji na temat konfiguracji pulpitu znajduje się w `dashboard.create`.

Konfigurowanie widżetu *Pie chart*

Skonfiguruj widżet *Pie chart* w następujący sposób:

- 2 zestawy danych dla łącznie 9 pozycji na 1 hoście.
- Pierwszy zestaw danych jest typu ”Item list” i składa się z 3 pozycji, z których wszystkie mają typ ”Normal” i są reprezentowane różnymi kolorami.
- Drugi zestaw danych jest typu ”Item patterns”, składa się z 6 pozycji, ma skonfigurowaną agregację dla każdej pozycji i jest reprezentowany przez niestandardowy kolor.
- Drugi zestaw danych ma również niestandardową etykietę zestawu danych.
- Dane na wykresie kołowym są wyświetlane jako wykres pierścieniowy z niestandardową szerokością oraz wartością całkowitą z jednostkami w środku.
- Dane na wykresie kołowym są wyświetlane i agregowane dla niestandardowego okresu czasu obejmującego ostatnie 3 godziny.
- Legenda wykresu kołowego wyświetla skonfigurowane pozycje w 4 wierszach.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "dashboard.create",
    "params": {
        "name": "My dashboard",
        "display_period": 30,
        "auto_start": 1,
        "pages": [
            {
                "widgets": [
                    {
                        "type": "piechart",
                        "name": "Pie chart",
                        "x": 0,
                        "y": 0,
                        "width": 24,
                        "height": 5,
                        "view_mode": 0,
                        "fields": [
                            {
                                "type": 0,
                                "name": "ds.0.dataset_type",
                                "value": 0
                            },
                            {
                                "type": 4,
                                "name": "ds.0.itemids.0",
                                "value": 23264
                            },
                            {
                                "type": 1,
                                "name": "ds.0.color.0",
                                "value": "FF0000"
                            },
                            {
                                "type": 0,
                                "name": "ds.0.type.0",
                                "value": 0
                            },
                            {
                                "type": 4,
                                "name": "ds.0.itemids.1",
                                "value": 23269
                            },
```

```
                    {
                        "type": 1,
                        "name": "ds.0.color.1",
                        "value": "BF00FF"
                    },
                    {
                      "type": 0,
                      "name": "ds.0.type.1",
                      "value": 0
                    },
                    {
                        "type": 4,
                        "name": "ds.0.itemids.2",
                        "value": 23257
                    },
                    {
                        "type": 1,
                        "name": "ds.0.color.2",
                        "value": "0040FF"
                    },
                    {
                      "type": 0,
                      "name": "ds.0.type.2",
                      "value": 0
                    },
                    {
                        "type": 1,
                        "name": "ds.1.hosts.0",
                        "value": "Zabbix server"
                    },
                    {
                        "type": 1,
                        "name": "ds.1.items.0",
                        "value": "*: Number of processed *values per second"
                    },
                    {
                        "type": 1,
                        "name": "ds.1.color",
                        "value": "000000"
                    },
                    {
                        "type": 0,
                        "name": "ds.1.aggregate_function",
                        "value": 3
                    },
                    {
                        "type": 1,
                        "name": "ds.1.data_set_label",
                        "value": "Number of processed values per second"
                    },
                    {
                        "type": 0,
                        "name": "draw_type",
                        "value": 1
                    },
                    {
                        "type": 0,
                        "name": "width",
                        "value": 30
                    },
                    {
                        "type": 0,
```

```
                                "name": "total_show",
                                "value": 1
                            },
                            {
                                "type": 0,
                                "name": "units_show",
                                "value": 1
                            },
                            {
                                "type": 0,
                                "name": "graph_time",
                                "value": 1
                            },
                            {
                                "type": 1,
                                "name": "time_period.from",
                                "value": "now-3h"
                            },
                            {
                                "type": 1,
                                "name": "time_period.to",
                                "value": "now"
                            },
                            {
                                "type": 0,
                                "name": "legend_lines",
                                "value": 4
                            }
                        ]
                    }
                ]
            }
        ],
        "userGroups": [
            {
                "usrgrpid": 7,
                "permission": 2
            }
        ],
        "users": [
            {
                "userid": 1,
                "permission": 3
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "3"
        ]
    },
    "id": 1
}
```

Zobacz także

- Pole widżetu pulpitu

- `dashboard.create`
- `dashboard.update`

22 Hosty z problemami

Opis

Te parametry oraz możliwe wartości właściwości dla odpowiednich obiektów pól widgetu umożliwiają skonfigurowanie widgetu *Hosty z problemami* w metodach `dashboard.create` i `dashboard.update`.

Attention:
Właściwości `fields` widgetu nie są walidowane podczas tworzenia ani aktualizacji pulpitu. Pozwala to użytkownikom modyfikować wbudowane widgety i tworzyć własne widgety, ale jednocześnie wprowadza ryzyko nieprawidłowego tworzenia lub aktualizowania widgetów. Aby zapewnić pomyślne utworzenie lub zaktualizowanie widgetu *Hosty z problemami*, zapoznaj się z zachowaniem parametrów opisanym w poniższych tabelach.

Parametry

Następujące parametry są obsługiwane dla widżetu *Hosty z problemami*.

Parametr	type	name	value
Interwał odświeżania	0	rf_rate	0 - Brak odświeżania; 10 - 10 sekund; 30 - 30 sekund; 60 - *(domyślnie)* 1 minuta; 120 - 2 minuty; 600 - 10 minut; 900 - 15 minut.
Grupy hostów	2	groupids.0	ID grupy hostów. Uwaga: Aby skonfigurować wiele grup hostów, utwórz obiekt pola widżetu pulpitu dla każdej grupy hostów z numerem zwiększanym w nazwie właściwości. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Grupy hostów (Widżet)	1	groupids._reference	Zamiast ID grupy hostów: `ABCDE._hostgroupids` - ustaw kompatybilny widżet (z parametrem *Reference* ustawionym na "ABCDE") jako źródło danych dla grup hostów. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Wyklucz grupy hostów	2	exclude_groupids.0	ID grupy hostów. Uwaga: Aby wykluczyć wiele grup hostów, utwórz obiekt pola widżetu pulpitu dla każdej grupy hostów z numerem zwiększanym w nazwie właściwości. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Hosty	3	hostids.0	ID hosta. Uwaga: Aby skonfigurować wiele hostów, utwórz obiekt pola widżetu pulpitu dla każdego hosta z numerem zwiększanym w nazwie właściwości. W przypadku wielu hostów parametr *Grupy hostów* nie może być w ogóle skonfigurowany albo musi być skonfigurowany z co najmniej jedną grupą hostów, do której należą skonfigurowane hosty. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.

Parametr	type	name	value
Hosty (Widżet/Pulpit)	1	hostids._reference	Zamiast ID hosta: `DASHBOARD.hostids` - ustaw selektor hostów pulpitu jako źródło danych dla hostów; `ABCDE._hostids` - ustaw kompatybilny widżet (z parametrem *Reference* ustawionym na "`ABCDE`") jako źródło danych dla hostów. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Problem	1	problem	Nazwa zdarzenia problemu (bez rozróżniania wielkości liter, pełna nazwa lub jej część).
Istotność	0	severities.0	0 - Niesklasyfikowane; 1 - Informacja; 2 - Ostrzeżenie; 3 - Średni; 4 - Wysoki; 5 - Katastrofa. Domyślnie: puste (wszystkie włączone). Uwaga: Aby skonfigurować wiele wartości, utwórz obiekt pola widżetu pulpitu dla każdej wartości z numerem zwiększanym w nazwie właściwości.
Tagi problemu			
Typ oceny	0	evaltype	0 - *(domyślnie)* And/Or; 2 - Or.
Nazwa tagu	1	tags.0.tag	Dowolna wartość tekstowa. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście oceny tagów. Zachowanie parametru: - *wymagane* podczas konfigurowania *Tagów problemu*
Operator	0	tags.0.operator	0 - Zawiera; 1 - Równa się; 2 - Nie zawiera; 3 - Nie równa się; 4 - Istnieje; 5 - Nie istnieje. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście oceny tagów. Zachowanie parametru: - *wymagane* podczas konfigurowania *Tagów problemu*
Wartość tagu	1	tags.0.value	Dowolna wartość tekstowa. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście oceny tagów. Zachowanie parametru: - *wymagane* podczas konfigurowania *Tagów problemu*
Pokaż wycisżone problemy	0	show_suppressed	0 - *(domyślnie)* Wyłączone; 1 - Włączone.

Parametr	type	name	value
Ukryj grupy bez problemów	0	hide_empty_groups	0 - *(domyślnie)* Wyłączone; 1 - Włączone. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Wyświetlanie problemów	0	ext_ack	0 - *(domyślnie)* Wszystkie; 1 - Tylko niepotwierdzone; 2 - Rozdzielone.
Reference	1	reference	Dowolna wartość tekstowa składająca się z 5 znaków (np. `ABCDE` lub `JBPNL`). Ta wartość musi być unikalna w obrębie pulpitu, do którego należy widżet. Zachowanie parametru: - *wymagane*

Przykłady

Poniższe przykłady mają na celu jedynie opisanie konfiguracji obiektów pól widżetu pulpitu dla widżetu *Problem hosts*. Więcej informacji na temat konfiguracji pulpitu można znaleźć w `dashboard.create`.

Konfigurowanie widżetu *Problem hosts*

Skonfiguruj widżet *Problem hosts*, który wyświetla hosty z grup hostów „2” i „4”, mające problemy z nazwą zawierającą ciąg „CPU” oraz o następujących poziomach ważności: „Warning”, „Average”, „High”, „Disaster”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "dashboard.create",
    "params": {
        "name": "My dashboard",
        "display_period": 30,
        "auto_start": 1,
        "pages": [
            {
                "widgets": [
                    {
                        "type": "problemhosts",
                        "name": "Problem hosts",
                        "x": 0,
                        "y": 0,
                        "width": 36,
                        "height": 5,
                        "view_mode": 0,
                        "fields": [
                            {
                                "type": 2,
                                "name": "groupids.0",
                                "value": 2
                            },
                            {
                                "type": 2,
                                "name": "groupids.1",
                                "value": 4
                            },
                            {
                                "type": 1,
                                "name": "problem",
                                "value": "cpu"
                            },
                            {
                                "type": 0,
```

```
                                "name": "severities.0",
                                "value": 2
                            },
                            {
                                "type": 0,
                                "name": "severities.1",
                                "value": 3
                            },
                            {
                                "type": 0,
                                "name": "severities.2",
                                "value": 4
                            },
                            {
                                "type": 0,
                                "name": "severities.3",
                                "value": 5
                            }
                        ]
                    }
                ]
            }
        ],
        "userGroups": [
            {
                "usrgrpid": 7,
                "permission": 2
            }
        ],
        "users": [
            {
                "userid": 1,
                "permission": 3
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "3"
        ]
    },
    "id": 1
}
```

Zobacz także

- Pole widżetu pulpitu
- `dashboard.create`
- `dashboard.update`

23 Problemy

Opis

Te parametry oraz możliwe wartości właściwości dla odpowiednich obiektów pól widgetu umożliwiają skonfigurowanie widgetu *Problems* w metodach `dashboard.create` i `dashboard.update`.

Attention:
Właściwości `fields` widgetu nie są walidowane podczas tworzenia ani aktualizacji dashboardu. Pozwala to użytkownikom modyfikować wbudowane widgety i tworzyć własne widgety, ale jednocześnie wprowadza ryzyko nieprawidłowego tworzenia lub aktualizowania widgetów. Aby zapewnić pomyślne utworzenie lub aktualizację widgetu *Problems*, zapoznaj się z zachowaniem parametrów opisanym w poniższych tabelach.

Parametry

Następujące parametry są obsługiwane dla widżetu *Problemy*.

Parametr	type	name	value
Interwał odświeżania	0	rf_rate	0 - Brak odświeżania; 10 - 10 sekund; 30 - 30 sekund; 60 - *(domyślnie)* 1 minuta; 120 - 2 minuty; 600 - 10 minut; 900 - 15 minut.
Pokaż	0	show	1 - *(domyślnie)* Ostatnie problemy; 2 - Historia; 3 - Problemy.
Grupy hostów	2	groupids.0	ID grupy hostów. Uwaga: Aby skonfigurować wiele grup hostów, utwórz obiekt pola widżetu pulpitu dla każdej grupy hostów z numerem zwiększanym w nazwie właściwości. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Grupy hostów (Widżet)	1	groupids._reference	Zamiast ID grupy hostów: `ABCDE._hostgroupids` - ustaw kompatybilny widżet (z parametrem *Reference* ustawionym na "`ABCDE`") jako źródło danych dla grup hostów. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Wyklucz grupy hostów	2	exclude_groupids.0	ID grupy hostów. Uwaga: Aby wykluczyć wiele grup hostów, utwórz obiekt pola widżetu pulpitu dla każdej grupy hostów z numerem zwiększanym w nazwie właściwości. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Hosty	3	hostids.0	ID hosta. Uwaga: Aby skonfigurować wiele hostów, utwórz obiekt pola widżetu pulpitu dla każdego hosta z numerem zwiększanym w nazwie właściwości. W przypadku wielu hostów parametr *Grupy hostów* nie może być w ogóle skonfigurowany albo musi być skonfigurowany z co najmniej jedną grupą hostów, do której należą skonfigurowane hosty. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.

Parametr	type	name	value
Hosty (Widżet/Pulpit)	1	hostids._reference	Zamiast ID hosta: `DASHBOARD.hostids` - ustaw selektor hostów pulpitu jako źródło danych dla hostów; `ABCDE._hostids` - ustaw kompatybilny widżet (z parametrem *Reference* ustawionym na "`ABCDE`") jako źródło danych dla hostów. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Problem	1	problem	Nazwa zdarzenia problemu (bez rozróżniania wielkości liter, pełna nazwa lub jej część).
Poziom ważności	0	severities.0	0 - Niesklasyfikowane; 1 - Informacja; 2 - Ostrzeżenie; 3 - Średni; 4 - Wysoki; 5 - Katastrofa. Domyślnie: puste (wszystkie włączone). Uwaga: Aby skonfigurować wiele wartości, utwórz obiekt pola widżetu pulpitu dla każdej wartości z numerem zwiększanym w nazwie właściwości.
Tagi problemu			
Typ oceny	0	evaltype	0 - *(domyślnie)* I/Lub; 2 - Lub.
Nazwa tagu	1	tags.0.tag	Dowolna wartość tekstowa. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście oceny tagów. Zachowanie parametru: - *wymagany* przy konfigurowaniu *Tagów problemu*
Operator	0	tags.0.operator	0 - Zawiera; 1 - Równa się; 2 - Nie zawiera; 3 - Nie równa się; 4 - Istnieje; 5 - Nie istnieje. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście oceny tagów. Zachowanie parametru: - *wymagany* przy konfigurowaniu *Tagów problemu*
Wartość tagu	1	tags.0.value	Dowolna wartość tekstowa. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście oceny tagów. Zachowanie parametru: - *wymagany* przy konfigurowaniu *Tagów problemu*
Pokaż tagi	0	show_tags	0 - *(domyślnie)* Brak; 1 - 1; 2 - 2; 3 - 3.

Parametr	type	name	value
Nazwa tagu (format)	0	tag_name_format	0 - *(domyślnie)* Pełna; 1 - Skrócona; 2 - Brak. Zachowanie parametru: - *obsługiwany* jeśli *Pokaż tagi* jest ustawione na ”1”, ”2” lub ”3”
Priorytet wyświetlania tagów	1	tag_priority	Lista tagów oddzielonych przecinkami. Zachowanie parametru: - *obsługiwany* jeśli *Pokaż tagi* jest ustawione na ”1”, ”2” lub ”3”
Pokaż dane operacyjne	0	show_opdata	0 - *(domyślnie)* Brak; 1 - Osobno; 2 - Z nazwą problemu.
Pokaż wyciszone problemy	0	show_suppressed	0 - *(domyślnie)* Wyłączone; 1 - Włączone.
Status potwierdzenia	0	acknowledgement_status	0 - *(domyślnie)* wszystkie; 1 - Niepotwierdzone; 2 - Potwierdzone.
Przeze mnie	0	acknowledged_by_me	0 - *(domyślnie)* Wyłączone; 1 - Włączone.
Sortuj wpisy według	0	sort_triggers	1 - Poziom ważności (malejąco); 2 - Host (rosnąco); 3 - Czas (rosnąco); 4 - *(domyślnie)* Czas (malejąco); 13 - Poziom ważności (rosnąco); 14 - Host (malejąco); 15 - Problem (rosnąco); 16 - Problem (malejąco). Dla wszystkich wartości, z wyjątkiem ”Czas (malejąco)” i ”Czas (rosnąco)”, parametr *Pokaż oś czasu* musi być ustawiony na ”Wyłączone”. Wartości ”Host (rosnąco)” i ”Host (malejąco)” nie są obsługiwane podczas konfigurowania widżetu na pulpicie szablonu.
Pokaż oś czasu	0	show_timeline	0 - Wyłączone; 1 - *(domyślnie)* Włączone. Zachowanie parametru: - *obsługiwany* jeśli *Sortuj wpisy według* jest ustawione na ”Czas (malejąco)” lub ”Czas (rosnąco)”
Podświetl cały wiersz	0	highlight_row	0 - *(domyślnie)* Wyłączone; 1 - Włączone. Ten parametr nie jest obsługiwany w motywach o wysokim kontraście.
Pokaż wiersze	0	show_lines	Możliwe wartości mieszczą się w zakresie 1-100. Domyślnie: 25.

Parametr	type	name	value
Reference	1	reference	Dowolna wartość tekstowa składająca się z 5 znaków (np. ABCDE lub JBPNL). Ta wartość musi być unikalna w obrębie pulpitu, do którego należy widżet. Zachowanie parametru: - *wymagany*

Przykłady

Poniższe przykłady mają na celu jedynie opisanie konfiguracji obiektów pól widżetu pulpitu dla widżetu *Problemy*. Więcej informacji na temat konfiguracji pulpitu można znaleźć w `dashboard.create`.

Konfigurowanie widżetu *Problemy*

Skonfiguruj widżet *Problemy*, który wyświetla problemy dla grupy hostów „4”, spełniające następujące warunki:

- Problemy, które mają znacznik o nazwie „scope”, zawierający wartości „performance” lub „availability”, albo „capacity”.
- Problemy o następujących poziomach ważności: „Warning”, „Average”, „High”, „Disaster”.

Dodatkowo skonfiguruj widżet tak, aby wyświetlał znaczniki i dane operacyjne.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "dashboard.create",
    "params": {
        "name": "My dashboard",
        "display_period": 30,
        "auto_start": 1,
        "pages": [
            {
                "widgets": [
                    {
                        "type": "problems",
                        "name": "Problems",
                        "x": 0,
                        "y": 0,
                        "width": 36,
                        "height": 5,
                        "view_mode": 0,
                        "fields": [
                            {
                                "type": 2,
                                "name": "groupids.0",
                                "value": 4
                            },
                            {
                                "type": 1,
                                "name": "tags.0.tag",
                                "value": "scope"
                            },
                            {
                                "type": 0,
                                "name": "tags.0.operator",
                                "value": 0
                            },
                            {
                                "type": 1,
                                "name": "tags.0.value",
                                "value": "performance"
                            },
                            {
                                "type": 1,
```

```
                        "name": "tags.1.tag",
                        "value": "scope"
                    },
                    {
                        "type": 0,
                        "name": "tags.1.operator",
                        "value": 0
                    },
                    {
                        "type": 1,
                        "name": "tags.1.value",
                        "value": "availability"
                    },
                    {
                        "type": 1,
                        "name": "tags.2.tag",
                        "value": "scope"
                    },
                    {
                        "type": 0,
                        "name": "tags.2.operator",
                        "value": 0
                    },
                    {
                        "type": 1,
                        "name": "tags.2.value",
                        "value": "capacity"
                    },
                    {
                        "type": 0,
                        "name": "severities.0",
                        "value": 2
                    },
                    {
                        "type": 0,
                        "name": "severities.1",
                        "value": 3
                    },
                    {
                        "type": 0,
                        "name": "severities.2",
                        "value": 4
                    },
                    {
                        "type": 0,
                        "name": "severities.3",
                        "value": 5
                    },
                    {
                        "type": 0,
                        "name": "show_tags",
                        "value": 1
                    },
                    {
                        "type": 0,
                        "name": "show_opdata",
                        "value": 1
                    }
                ]
            }
        ]
    }
```

```
        ],
        "userGroups": [
            {
                "usrgrpid": 7,
                "permission": 2
            }
        ],
        "users": [
            {
                "userid": 1,
                "permission": 3
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "3"
        ]
    },
    "id": 1
}
```

Zobacz także

- Pole widżetu pulpitu
- `dashboard.create`
- `dashboard.update`

24 Problemy według ważności

Opis

Te parametry oraz możliwe wartości właściwości dla odpowiednich obiektów pól widgetu umożliwiają konfigurację widgetu *Problemy według ważności* w metodach `dashboard.create` i `dashboard.update`.

Attention:
Właściwości `fields` widgetu nie są walidowane podczas tworzenia ani aktualizacji pulpitu. Pozwala to użytkownikom modyfikować wbudowane widgety i tworzyć własne widgety, ale jednocześnie wprowadza ryzyko nieprawidłowego tworzenia lub aktualizowania widgetów. Aby zapewnić pomyślne utworzenie lub aktualizację widgetu *Problemy według ważności*, zapoznaj się z zachowaniem parametrów opisanym w poniższych tabelach.

Parametry

Następujące parametry są obsługiwane dla widżetu *Problemy według ważności*.

Parametr	type	name	value
Interwał odświeżania	0	rf_rate	0 - Bez odświeżania; 10 - 10 sekund; 30 - 30 sekund; 60 - *(domyślnie)* 1 minuta; 120 - 2 minuty; 600 - 10 minut; 900 - 15 minut.

Parametr	type	name	value
Grupy hostów	2	groupids.0	ID grupy hostów. Uwaga: Aby skonfigurować wiele grup hostów, utwórz obiekt pola widżetu pulpitu dla każdej grupy hostów z numerem zwiększanym w nazwie właściwości. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Grupy hostów (Widżet)	1	groupids._reference	Zamiast ID grupy hostów: `ABCDE._hostgroupids` - ustaw kompatybilny widżet (z parametrem *Reference* ustawionym na "ABCDE") jako źródło danych dla grup hostów. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Wyklucz grupy hostów	2	exclude_groupids.0	ID grupy hostów. Uwaga: Aby wykluczyć wiele grup hostów, utwórz obiekt pola widżetu pulpitu dla każdej grupy hostów z numerem zwiększanym w nazwie właściwości. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Hosty	3	hostids.0	ID hosta. Uwaga: Aby skonfigurować wiele hostów, utwórz obiekt pola widżetu pulpitu dla każdego hosta z numerem zwiększanym w nazwie właściwości. W przypadku wielu hostów parametr *Grupy hostów* nie może być w ogóle skonfigurowany albo musi być skonfigurowany z co najmniej jedną grupą hostów, do której należą skonfigurowane hosty. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Hosty (Widżet/Pulpit)	1	hostids._reference	Zamiast ID hosta: `DASHBOARD.hostids` - ustaw selektor hosta pulpitu jako źródło danych dla hostów; `ABCDE._hostids` - ustaw kompatybilny widżet (z parametrem *Reference* ustawionym na "ABCDE") jako źródło danych dla hostów. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Problem	1	problem	Nazwa zdarzenia problemu (bez rozróżniania wielkości liter, pełna nazwa lub jej część).
Ważność	0	severities.0	0 - Niesklasyfikowane; 1 - Informacja; 2 - Ostrzeżenie; 3 - Średnia; 4 - Wysoka; 5 - Katastrofa. Domyślnie: puste (wszystkie włączone). Uwaga: Aby skonfigurować wiele wartości, utwórz obiekt pola widżetu pulpitu dla każdej wartości z numerem zwiększanym w nazwie właściwości.
Tagi problemu			
Typ obliczania	0	evaltype	0 - *(domyślnie)* I/Lub; 2 - Lub.

Parametr	type	name	value
Nazwa tagu	1	tags.0.tag	Dowolna wartość tekstowa. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście obliczania tagów. Zachowanie parametru: - *wymagane* przy konfigurowaniu *Tagów problemu*
Operator	0	tags.0.operator	0 - Zawiera; 1 - Równa się; 2 - Nie zawiera; 3 - Nie równa się; 4 - Istnieje; 5 - Nie istnieje. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście obliczania tagów. Zachowanie parametru: - *wymagane* przy konfigurowaniu *Tagów problemu*
Wartość tagu	1	tags.0.value	Dowolna wartość tekstowa. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście obliczania tagów. Zachowanie parametru: - *wymagane* przy konfigurowaniu *Tagów problemu*
Pokaż	0	show_type	0 - *(domyślnie)* Grupy hostów; 1 - Sumy. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu, a domyślnie jest ustawiony na ”Sumy”.
Układ	0	layout	0 - *(domyślnie)* Poziomy; 1 - Pionowy. Zachowanie parametru: - *obsługiwane* jeśli *Pokaż* jest ustawione na ”Sumy”
Pokaż dane operacyjne	0	show_opdata	0 - *(domyślnie)* Brak; 1 - Osobno; 2 - Z nazwą problemu.
Pokaż ukryte problemy	0	show_suppressed	0 - *(domyślnie)* Wyłączone; 1 - Włączone.
Ukryj grupy bez problemów	0	hide_empty_groups	0 - *(domyślnie)* Wyłączone; 1 - Włączone. Zachowanie parametru: - *obsługiwane* jeśli *Pokaż* jest ustawione na ”Grupy hostów” Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Wyświetlanie problemów	0	ext_ack	0 - *(domyślnie)* Wszystkie; 1 - Tylko niepotwierdzone; 2 - Rozdzielone.
Pokaż oś czasu	0	show_timeline	0 - Wyłączone; 1 - *(domyślnie)* Włączone.

Parametr	type	name	value
Reference	1	reference	Dowolna wartość tekstowa składająca się z 5 znaków (np. `ABCDE` lub `JBPNL`). Ta wartość musi być unikalna w obrębie pulpitu, do którego należy widżet. Zachowanie parametru: - *wymagane*

Przykłady

Poniższe przykłady mają na celu jedynie opisanie konfiguracji obiektów pól widżetu pulpitu dla widżetu *Problemy według ważności*. Więcej informacji na temat konfiguracji pulpitu można znaleźć w `dashboard.create`.

Konfigurowanie widżetu *Problemy według ważności*

Skonfiguruj widżet *Problemy według ważności*, który wyświetla łączną liczbę problemów dla wszystkich grup hostów.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "dashboard.create",
    "params": {
        "name": "My dashboard",
        "display_period": 30,
        "auto_start": 1,
        "pages": [
            {
                "widgets": [
                    {
                        "type": "problemsbysv",
                        "name": "Problems by severity",
                        "x": 0,
                        "y": 0,
                        "width": 36,
                        "height": 5,
                        "view_mode": 0,
                        "fields": [
                            {
                                "type": 0,
                                "name": "show_type",
                                "value": 1
                            }
                        ]
                    }
                ]
            }
        ],
        "userGroups": [
            {
                "usrgrpid": 7,
                "permission": 2
            }
        ],
        "users": [
            {
                "userid": 1,
                "permission": 3
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "3"
        ]
    },
    "id": 1
}
```

Zobacz także

- Pole widżetu pulpitu
- `dashboard.create`
- `dashboard.update`

25 Wykres punktowy

Opis

Te parametry oraz możliwe wartości właściwości dla odpowiednich obiektów pól widgetu umożliwiają skonfigurowanie widgetu *Scatter plot* w metodach `dashboard.create` i `dashboard.update`.

Attention:
Właściwości `fields` widgetu nie są walidowane podczas tworzenia ani aktualizacji dashboardu. Pozwala to użytkownikom modyfikować wbudowane widgety oraz tworzyć własne widgety, ale jednocześnie wprowadza ryzyko nieprawidłowego tworzenia lub aktualizowania widgetów. Aby zapewnić pomyślne utworzenie lub zaktualizowanie widgetu *Scatter plot*, zapoznaj się z zachowaniem parametrów opisanym w poniższych tabelach.

Parametry

Następujące parametry są obsługiwane dla widżetu *Scatter plot*.

Parametr	type	nazwa	wartość
Interwał odświeżania	0	rf_rate	0 - Brak odświeżania; 10 - 10 sekund; 30 - 30 sekund; 60 - *(domyślnie)* 1 minuta; 120 - 2 minuty; 600 - 10 minut; 900 - 15 minut.
Odwołanie	1	reference	Dowolna wartość tekstowa składająca się z 5 znaków (np. `ABCDE` lub `JBPNL`). Ta wartość musi być unikalna w obrębie dashboardu, do którego należy widżet. Zachowanie parametru: - *wymagane*

Zestaw danych

Następujące parametry są obsługiwane przy konfigurowaniu *Zestawu danych*.

Note:
Pierwsza liczba w nazwie właściwości (np. ds.0.hosts.0, ds.0.items.0) oznacza konkretny zestaw danych, natomiast druga liczba, jeśli występuje, oznacza skonfigurowany host lub pozycję.

Parametr	type	name	value
Typ zestawu danych	0	ds.0.dataset_type	0 - Lista pozycji; 1 - *(domyślnie)* Wzorce pozycji.

Parametr	type	name	value
Zestaw danych: Lista pozycji			
Kolor	1	ds.0.color.0	Szesnastkowy kod koloru (np. `FF0000`). Zachowanie parametru: - *wymagany*, jeśli *Typ zestawu danych* jest ustawiony na ”Lista pozycji”
Oś X	4	ds.0.x_axis_itemids.0	ID pozycji. Podczas konfigurowania widżetu na pulpicie szablonu należy ustawić tylko pozycje skonfigurowane w szablonie. Uwaga: Aby skonfigurować wiele pozycji, utwórz obiekt pola widżetu pulpitu dla każdej pozycji z inkrementowanym numerem w nazwie właściwości. Zachowanie parametru: - *wymagany*, jeśli *Typ zestawu danych* jest ustawiony na ”Lista pozycji”, a *Oś X (Widżet)* nie jest ustawiona
Oś X (Widżet)	1	ds.0.x_axis_itemids.0._reference	Zamiast ID pozycji: `ABCDE._itemid` - ustaw kompatybilny widżet (z parametrem *Reference* ustawionym na ”`ABCDE`”) jako źródło danych dla pozycji. Uwaga: Aby skonfigurować wiele widżetów, utwórz obiekt pola widżetu pulpitu dla każdego widżetu z inkrementowanym numerem w nazwie właściwości. Zachowanie parametru: - *wymagany*, jeśli *Typ zestawu danych* jest ustawiony na ”Lista pozycji”, a *Oś X* nie jest ustawiona
Oś Y	4	ds.0.y_axis_itemids.0	ID pozycji. Podczas konfigurowania widżetu na pulpicie szablonu należy ustawić tylko pozycje skonfigurowane w szablonie. Uwaga: Aby skonfigurować wiele pozycji, utwórz obiekt pola widżetu pulpitu dla każdej pozycji z inkrementowanym numerem w nazwie właściwości. Zachowanie parametru: - *wymagany*, jeśli *Typ zestawu danych* jest ustawiony na ”Lista pozycji”, a *Oś Y (Widżet)* nie jest ustawiona
Oś Y (Widżet)	1	ds.0.y_axis_itemids.0._reference	Zamiast ID pozycji: `ABCDE._itemid` - ustaw kompatybilny widżet (z parametrem *Reference* ustawionym na ”`ABCDE`”) jako źródło danych dla pozycji. Uwaga: Aby skonfigurować wiele widżetów, utwórz obiekt pola widżetu pulpitu dla każdego widżetu z inkrementowanym numerem w nazwie właściwości. Zachowanie parametru: - *wymagany*, jeśli *Typ zestawu danych* jest ustawiony na ”Lista pozycji”, a *Oś Y* nie jest ustawiona

Parametr	type	name	value
Nadpisz host	1	ds.0.override_hostid.ABCDE_hostid	`ABCDE._hostid`- ustaw kompatybilny widżet (z parametrem "Reference" ustawionym na "ABCDE") jako źródło danych dla hostów; `DASHBOARD._hostid` - ustaw selektor hosta pulpitu jako źródło danych dla hostów. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Zestaw danych: Wzorce pozycji			
Kolor	1	ds.0.color	Szesnastkowy kod koloru (np. `FF0000`). Zachowanie parametru: - *obsługiwany*, jeśli *Typ zestawu danych* jest ustawiony na "Wzorce pozycji", a *Paleta kolorów* nie jest ustawiona
Paleta kolorów	0	ds.0.color_palette	Indeks palety kolorów. Możliwy zakres wartości: 0-11. Domyślnie: 0. Zachowanie parametru: - *obsługiwany*, jeśli *Typ zestawu danych* jest ustawiony na "Wzorce pozycji", a *Kolor* nie jest ustawiony
Wzorce hostów	1	ds.0.hosts.0	Nazwa lub wzorzec hosta (np. "Zabbix*"). Zachowanie parametru: - *wymagany*, jeśli *Typ zestawu danych* jest ustawiony na "Wzorce pozycji" Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Wzorce pozycji osi X	1	ds.0.x_axis_items.0	Nazwa lub wzorzec pozycji (np. "*: Number of processed *values per second"). Podczas konfigurowania widżetu na pulpicie szablonu należy ustawić tylko wzorce dla pozycji skonfigurowanych w szablonie. Zachowanie parametru: - *wymagany*, jeśli *Typ zestawu danych* jest ustawiony na "Wzorce pozycji"
Wzorce pozycji osi Y	1	ds.0.y_axis_items.0	Nazwa lub wzorzec pozycji (np. "*: Number of processed *values per second"). Podczas konfigurowania widżetu na pulpicie szablonu należy ustawić tylko wzorce dla pozycji skonfigurowanych w szablonie. Zachowanie parametru: - *wymagany*, jeśli *Typ zestawu danych* jest ustawiony na "Wzorce pozycji"
Grupy hostów	2	groupids.0	ID grupy hostów. Uwaga: Aby skonfigurować wiele grup hostów, utwórz obiekt pola widżetu pulpitu dla każdej grupy hostów z inkrementowanym numerem w nazwie właściwości. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.

Parametr	type	name	value
Grupy hostów (Widżet)	1	groupids._reference	Zamiast ID grupy hostów: `ABCDE._hostgroupids` - ustaw kompatybilny widżet (z parametrem *Reference* ustawionym na "`ABCDE`") jako źródło danych dla grup hostów. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Nadpisz host	1	ds.0.override_hostid._reference	`ABCDE._hostid`- ustaw kompatybilny widżet (z parametrem "Reference" ustawionym na "`ABCDE`") jako źródło danych dla hostów; `DASHBOARD._hostid` - ustaw selektor hosta pulpitu jako źródło danych dla hostów. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Tagi hosta			
Typ oceny	0	evaltype_host	0 - *(domyślnie)* And/Or; 2 - Or. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Nazwa tagu	1	host_tags.0.tag	Dowolna wartość tekstowa. Uwaga: Liczba w nazwie właściwości odnosi się do kolejności tagu na liście oceny tagów. Zachowanie parametru: - *wymagany* przy konfigurowaniu *Tagów hosta* Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Operator	0	host_tags.0.operator	0 - Zawiera; 1 - Równa się; 2 - Nie zawiera; 3 - Nie równa się; 4 - Istnieje; 5 - Nie istnieje. Uwaga: Liczba w nazwie właściwości odnosi się do kolejności tagu na liście oceny tagów. Zachowanie parametru: - *wymagany* przy konfigurowaniu *Tagów hosta* Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Wartość tagu	1	host_tags.0.value	Dowolna wartość tekstowa. Uwaga: Liczba w nazwie właściwości odnosi się do kolejności tagu na liście oceny tagów. Zachowanie parametru: - *wymagany* przy konfigurowaniu *Tagów hosta* Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.

Parametr	type	name	value
Znacznik	0	ds.0.marker	0 - *(domyślnie)* Elipsa; 1 - Kwadrat; 2 - Trójkąt; 3 - Romb; 4 - Gwiazda; 5 - Krzyżyk.
Rozmiar znacznika	0	ds.0.marker_size	0 - *(domyślnie)* Mały (6px); 1 - Średni (9px); 2 - Duży (15px).
Przesunięcie czasu	1	ds.0.timeshift	Prawidłowy ciąg czasu (np. 3600, 1h itd.). Możesz używać sufiksów czasu. Dozwolone są również wartości ujemne. Domyślnie: "" (puste).
Interwał agregacji	1	ds.0.aggregate_interval	Prawidłowy ciąg czasu (np. 3600, 1h itd.). Możesz używać sufiksów czasu. Domyślnie: 15m.
Funkcja agregacji	0	ds.0.aggregate_function	0 - nieużywane; 1 - min; 2 - max; 3 - *(domyślnie)* avg; 4 - count; 5 - sum; 6 - first; 7 - last.

Opcje wyświetlania

Następujące parametry są obsługiwane przy konfigurowaniu *Opcji wyświetlania*.

Parametr	type	name	value
Wybór danych historycznych	0	source	0 - *(domyślnie)* Auto; 1 - Historia; 2 - Trendy.
Nazwy hostów na etykietach	0	show_hostnames	0 - *(domyślnie)* Auto; 1 - Pokaż; 2 - Ukryj. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na dashboardzie szablonu.

Okres czasu

Następujące parametry są obsługiwane przy konfigurowaniu *Okresu czasu*.

Parametr	type	name	value
Okres czasu	1	time_period._reference	DASHBOARD._timeperiod — ustaw selektor okresu czasu pulpitu jako źródło danych; ABCDE._timeperiod — ustaw kompatybilny widget (z parametrem *Reference* ustawionym na "ABCDE") jako źródło danych. Domyślnie: DASHBOARD._timeperiod Alternatywnie można ustawić okres czasu tylko w parametrach *Od* i *Do*.

Parametr	type	name	value
Od	1	time_period.from	Prawidłowy ciąg czasu w składni bezwzględnej (`YYYY-MM-DD hh:mm:ss`) lub względnej (`now`, `now/d`, `now/w-1w` itd.). Zachowanie parametru: - *obsługiwany*, jeśli *Okres czasu* nie jest ustawiony - *wymagany*, jeśli ustawiono `time_period.to`
Do	1	time_period.to	Prawidłowy ciąg czasu w składni bezwzględnej (`YYYY-MM-DD hh:mm:ss`) lub względnej (`now`, `now/d`, `now/w-1w` itd.). Zachowanie parametru: - *obsługiwany*, jeśli *Okres czasu* nie jest ustawiony - *wymagany*, jeśli ustawiono `time_period.from`

Osie

Następujące parametry są obsługiwane do konfiguracji *Osi*.

Parametr	type	name	value
Oś X	0	x_axis	0 - Wyłączona; 1 - *(domyślnie)* Włączona.
Oś Y	0	y_axis	0 - *(domyślnie)* Wyłączona; 1 - Włączona.
Min	1	x_axis_min	Dowolna wartość liczbowa. Domyślnie: "" (puste).
		y_axis_min	
Max	1	x_axis_max	Dowolna wartość liczbowa. Domyślnie: "" (puste).
		y_axis_max	
Jednostki (typ)	0	x_axis_units	0 - *(domyślnie)* Automatycznie; 1 - Statyczne.
		y_axis_units	
Jednostki (wartość)	1	x_axis_static_units	Dowolna wartość tekstowa. Domyślnie: "" (puste).
		y_axis_static_units	

Legenda

Następujące parametry są obsługiwane przy konfigurowaniu *Legendy*.

Parametr	type	name	value
Pokaż legendę	0	legend	0 - Wyłączone; 1 - *(domyślnie)* Włączone.
Pokaż funkcję agregacji	0	legend_aggregation	0 - *(domyślnie)* Wyłączone; 1 - Włączone. Zachowanie parametru: - *obsługiwane*, jeśli *Pokaż legendę* jest ustawione na „Włączone”
Wiersze	0	legend_lines_mode	0 - *(domyślnie)* Stałe; 1 - Zmienne. Zachowanie parametru: - *obsługiwane*, jeśli *Pokaż legendę* jest ustawione na „Włączone”

Parametr	type	name	value
Liczba wierszy/ Maksymalna liczba wierszy	0	legend_lines	Możliwe wartości z zakresu: 1-10. Domyślnie: 1. Zachowanie parametru: - *obsługiwane*, jeśli *Pokaż legendę* jest ustawione na „Włączone”
Liczba kolumn	0	legend_columns	Możliwe wartości z zakresu: 1-4. Domyślnie: 4. Zachowanie parametru: - *obsługiwane*, jeśli *Pokaż legendę* jest ustawione na „Włączone”

Progi

Następujące parametry są obsługiwane do konfigurowania *Progów*.

Note:
Liczba w nazwie właściwości *Thresholds* (np. thresholds.0.color) odnosi się do miejsca progu na liście, posortowanej rosnąco. Jeśli jednak progi są skonfigurowane w innej kolejności, wartości zostaną posortowane rosnąco po zaktualizowaniu konfiguracji widżetu w frontendzie Zabbix (np. `"thresholds.0.threshold":"5"` → `"thresholds.0.threshold":"1"`; `"thresholds.1.threshold":"1"` → `"thresholds.1.threshold": "5"`).

Parametr	type	name	value
Interpolacja kolorów	0	interpolation	0 - *(domyślnie)* Wyłączona; 1 - Włączona.
Kolor	1	thresholds.0.color	Szesnastkowy kod koloru (np. FF0000).
Oś X	1	thresholds.0.x_axis_threshold	Dowolna wartość liczbowa. Obsługiwane są sufiksy (np. ”1d”, ”2w”, ”4K”, ”8G”).
Oś Y	1	thresholds.0.y_axis_threshold	Dowolna wartość liczbowa. Obsługiwane są sufiksy (np. ”1d”, ”2w”, ”4K”, ”8G”).

Przykłady

Poniższe przykłady mają na celu jedynie opisanie konfiguracji obiektów pól widgetu pulpitu dla widgetu *Scatter plot*. Więcej informacji na temat konfiguracji pulpitu można znaleźć w `dashboard.create`.

Konfigurowanie widżetu *Scatter plot*

Skonfiguruj widżet *Scatter plot* w następujący sposób:

- 5 zestawów danych typu „Wzorce pozycji”, każdy z domyślną agregacją (avg, 15m) i różnymi znacznikami.
- Legenda wyświetla skonfigurowane pozycje w jednym wierszu i dwóch kolumnach.
- Progi są skonfigurowane tak, aby kolor znacznika zmieniał się na czerwony, gdy jego wartość osiągnie 80 na dowolnej osi.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "dashboard.create",
    "params": {
        "name": "My dashboard",
        "display_period": 30,
        "auto_start": 1,
        "pages": [
            {
                "widgets": [
                    {
                        "type": "scatterplot",
                        "name": "Scatter plot",
                        "x": 0,
                        "y": 0,
```

```
                "width": 36,
                "height": 5,
                "view_mode": 0,
                "fields": [
                    {
                        "type": 1,
                        "name": "ds.0.color",
                        "value": "0C5A87"
                    },
                    {
                        "type": 1,
                        "name": "ds.0.hosts.0",
                        "value": "de-frankfurt*"
                    },
                    {
                        "type": 1,
                        "name": "ds.0.x_axis_items.0",
                        "value": "Memory utilization"
                    },
                    {
                        "type": 1,
                        "name": "ds.0.y_axis_items.0",
                        "value": "CPU utilization"
                    },
                    {
                        "type": 0,
                        "name": "ds.0.marker",
                        "value": 0
                    },
                    {
                        "type": 0,
                        "name": "ds.0.marker_size",
                        "value": 1
                    },
                    {
                        "type": 1,
                        "name": "ds.1.color",
                        "value": "66B0D9"
                    },
                    {
                        "type": 1,
                        "name": "ds.1.hosts.0",
                        "value": "fr-paris*"
                    },
                    {
                        "type": 1,
                        "name": "ds.1.x_axis_items.0",
                        "value": "Memory utilization"
                    },
                    {
                        "type": 1,
                        "name": "ds.1.y_axis_items.0",
                        "value": "CPU utilization"
                    },
                    {
                        "type": 0,
                        "name": "ds.1.marker",
                        "value": 1
                    },
                    {
                        "type": 0,
                        "name": "ds.1.marker_size",
```

```
            "value": 1
        },
        {
            "type": 1,
            "name": "ds.2.color",
            "value": "0A466A"
        },
        {
            "type": 1,
            "name": "ds.2.hosts.0",
            "value": "lv-riga*"
        },
        {
            "type": 1,
            "name": "ds.2.x_axis_items.0",
            "value": "Memory utilization"
        },
        {
            "type": 1,
            "name": "ds.2.y_axis_items.0",
            "value": "CPU utilization"
        },
        {
            "type": 0,
            "name": "ds.2.marker",
            "value": 2
        },
        {
            "type": 0,
            "name": "ds.2.marker_size",
            "value": 1
        },
        {
            "type": 1,
            "name": "ds.3.color",
            "value": "3394C3"
        },
        {
            "type": 1,
            "name": "ds.3.hosts.0",
            "value": "pl-warsaw*"
        },
        {
            "type": 1,
            "name": "ds.3.x_axis_items.0",
            "value": "Memory utilization"
        },
        {
            "type": 1,
            "name": "ds.3.y_axis_items.0",
            "value": "CPU utilization"
        },
        {
            "type": 0,
            "name": "ds.3.marker",
            "value": 3
        },
        {
            "type": 0,
            "name": "ds.3.marker_size",
            "value": 1
        },
```

```
                {
                    "type": 1,
                    "name": "ds.4.color",
                    "value": "1492C8"
                },
                {
                    "type": 1,
                    "name": "ds.4.hosts.0",
                    "value": "se-stockholm*"
                },
                {
                    "type": 1,
                    "name": "ds.4.x_axis_items.0",
                    "value": "Memory utilization"
                },
                {
                    "type": 1,
                    "name": "ds.4.y_axis_items.0",
                    "value": "CPU utilization"
                },
                {
                    "type": 0,
                    "name": "ds.4.marker",
                    "value": 4
                },
                {
                    "type": 0,
                    "name": "ds.4.marker_size",
                    "value": 1
                },
                {
                    "type": 0,
                    "name": "legend_columns",
                    "value": 2
                },
                {
                    "type": 0,
                    "name": "interpolation",
                    "value": 1
                },
                {
                    "type": 1,
                    "name": "thresholds.0.color",
                    "value": "D40000"
                },
                {
                    "type": 1,
                    "name": "thresholds.0.x_axis_threshold",
                    "value": "80"
                },
                {
                    "type": 1,
                    "name": "thresholds.0.y_axis_threshold",
                    "value": ""
                },
                {
                    "type": 1,
                    "name": "thresholds.1.color",
                    "value": "D40000"
                },
                {
                    "type": 1,
```

```
                                "name": "thresholds.1.x_axis_threshold",
                                "value": ""
                            },
                            {
                                "type": 1,
                                "name": "thresholds.1.y_axis_threshold",
                                "value": "80"
                            },
                            {
                                "type": 1,
                                "name": "reference",
                                "value": "JQISY"
                            }
                        ]
                    }
                ]
            }
        ],
        "userGroups": [
            {
                "usrgrpid": 7,
                "permission": 2
            }
        ],
        "users": [
            {
                "userid": 1,
                "permission": 3
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "3"
        ]
    },
    "id": 1
}
```

Zobacz także

- Pole widżetu pulpitu
- `dashboard.create`
- `dashboard.update`

26 Raport SLA

Opis

Te parametry oraz możliwe wartości właściwości dla odpowiednich obiektów pól widgetu umożliwiają konfigurację widgetu *Raport SLA* w metodach `dashboard.create` i `dashboard.update`.

Attention:
Właściwości `fields` widgetu nie są walidowane podczas tworzenia ani aktualizacji pulpitu. Pozwala to użytkownikom modyfikować wbudowane widgety i tworzyć własne widgety, ale jednocześnie wprowadza ryzyko nieprawidłowego tworzenia lub aktualizowania widgetów. Aby zapewnić pomyślne utworzenie lub aktualizację widgetu *Raport SLA*, zapoznaj się z zachowaniem parametrów opisanym w poniższych tabelach.

Parametry

Następujące parametry są obsługiwane dla widżetu *Raport SLA*.

Parametr	type	name	value
Interwał odświeżania	0	rf_rate	0 - *(domyślnie)* Bez odświeżania; 10 - 10 sekund; 30 - 30 sekund; 60 - 1 minuta; 120 - 2 minuty; 600 - 10 minut; 900 - 15 minut.
SLA	10	slaid.0	ID SLA. Zachowanie parametrów: - *wymagane*
Usługa	9	serviceid.0	ID usługi.
Pokaż okresy	0	show_periods	Możliwe wartości mieszczą się w zakresie 1-100. Domyślnie: 20.
Od	1	date_from	Prawidłowy ciąg daty w formacie `YYYY-MM-DD`. Obsługiwane są daty względne z modyfikatorami `d`, `w`, `M`, `y` (np. `now`, `now/d`, `now/w-1w` itd.).
Do	1	date_to	Prawidłowy ciąg daty w formacie `YYYY-MM-DD`. Obsługiwane są daty względne z modyfikatorami `d`, `w`, `M`, `y` (np. `now`, `now/d`, `now/w-1w` itd.).

Przykłady

Poniższe przykłady mają na celu jedynie opisanie konfiguracji obiektów pól widgetu pulpitu dla widgetu *Raport SLA*. Więcej informacji na temat konfiguracji pulpitu można znaleźć w `dashboard.create`.

Konfigurowanie widżetu *Raport SLA*

Skonfiguruj widżet *Raport SLA*, który wyświetla raport SLA dla usługi SLA „4”, usługi „2”, za okres ostatnich 30 dni.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "dashboard.create",
    "params": {
        "name": "My dashboard",
        "display_period": 30,
        "auto_start": 1,
        "pages": [
            {
                "widgets": [
                    {
                        "type": "slareport",
                        "name": "SLA report",
                        "x": 0,
                        "y": 0,
                        "width": 36,
                        "height": 5,
                        "view_mode": 0,
                        "fields": [
                            {
```

```
                                "type": 10,
                                "name": "slaid.0",
                                "value": 4
                            },
                            {
                                "type": 9,
                                "name": "serviceid.0",
                                "value": 2
                            },
                            {
                                "type": 1,
                                "name": "date_from",
                                "value": "now-30d"
                            },
                            {
                                "type": 1,
                                "name": "date_to",
                                "value": "now"
                            }
                        ]
                    }
                ]
            }
        ],
        "userGroups": [
            {
                "usrgrpid": 7,
                "permission": 2
            }
        ],
        "users": [
            {
                "userid": 1,
                "permission": 3
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "3"
        ]
    },
    "id": 1
}
```

Zobacz także

- Pole widżetu pulpitu
- `dashboard.create`
- `dashboard.update`

27 Informacje o systemie

Opis

Te parametry oraz możliwe wartości właściwości dla odpowiednich obiektów pól widgetu umożliwiają konfigurację widgetu *Infor-*

macje o systemie w metodach `dashboard.create` i `dashboard.update`.

Attention:
Właściwości `fields` widgetu nie są walidowane podczas tworzenia ani aktualizacji pulpitu. Pozwala to użytkownikom modyfikować wbudowane widgety i tworzyć własne widgety, ale jednocześnie wprowadza ryzyko nieprawidłowego tworzenia lub aktualizowania widgetów. Aby zapewnić pomyślne utworzenie lub zaktualizowanie widgetu *Informacje o systemie*, zapoznaj się z zachowaniem parametrów opisanym w poniższych tabelach.

Parametry

Następujące parametry są obsługiwane dla widżetu *Informacje o systemie*.

Parametr	type	name	value
Interwał odświeżania	0	rf_rate	0 - Bez odświeżania; 10 - 10 sekund; 30 - 30 sekund; 60 - 1 minuta; 120 - 2 minuty; 600 - 10 minut; 900 - *(domyślnie)* 15 minut.
Pokaż	0	info_type	0 - *(domyślnie)* Statystyki systemu; 1 - Węzły wysokiej dostępności.
Pokaż szczegóły sprawdzania aktualizacji oprogramowania	0	show_software_update_check_details	0 - *(domyślnie)* Wyłączone; 1 - Włączone. Zachowanie parametru: - *obsługiwany*, jeśli `AllowSoftwareUpdateCheck` w konfiguracji serwera Zabbix jest włączony i *Pokaż* jest ustawione na „Statystyki systemu”

Przykłady

Poniższe przykłady mają na celu jedynie opisanie konfiguracji obiektów pól widżetu pulpitu dla widżetu *Informacje o systemie*. Więcej informacji na temat konfiguracji pulpitu można znaleźć w `dashboard.create`.

Konfigurowanie widżetu *Informacje o systemie*

Skonfiguruj widżet *Informacje o systemie*, który wyświetla statystyki systemowe z interwałem odświeżania wynoszącym 10 minut oraz z włączonym sprawdzaniem aktualizacji oprogramowania.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "dashboard.create",
    "params": {
        "name": "My dashboard",
        "display_period": 30,
        "auto_start": 1,
        "pages": [
            {
                "widgets": [
                    {
                        "type": "systeminfo",
                        "name": "System information",
                        "x": 0,
                        "y": 0,
                        "width": 36,
                        "height": 5,
                        "view_mode": 0,
                        "fields": [
                            {
                                "type": 0,
                                "name": "rf_rate",
```

```
                                "value": 600
                            },
                            {
                                "type": 0,
                                "name": "show_software_update_check_details",
                                "value": 1
                            }
                        ]
                    }
                ]
            }
        ],
        "userGroups": [
            {
                "usrgrpid": 7,
                "permission": 2
            }
        ],
        "users": [
            {
                "userid": 1,
                "permission": 3
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "3"
        ]
    },
    "id": 1
}
```

Zobacz także

- Pole widżetu pulpitu
- `dashboard.create`
- `dashboard.update`

28 Najważniejsze hosty

Opis

Te parametry oraz możliwe wartości właściwości dla odpowiednich obiektów pól widgetu umożliwiają konfigurację widgetu *Top hosts* w metodach `dashboard.create` i `dashboard.update`.

> **Attention:**
> Właściwości `fields` widgetu nie są walidowane podczas tworzenia ani aktualizacji pulpitu. Pozwala to użytkownikom modyfikować wbudowane widgety i tworzyć własne widgety, ale jednocześnie wprowadza ryzyko nieprawidłowego tworzenia lub aktualizowania widgetów. Aby zapewnić pomyślne utworzenie lub aktualizację widgetu *Top hosts*, zapoznaj się z zachowaniem parametrów opisanym w poniższych tabelach.

Parametry

Dla widżetu *Top hosts* obsługiwane są następujące parametry.

Parametr	type	name	value
Interwał odświeżania	0	rf_rate	0 - Bez odświeżania; 10 - 10 sekund; 30 - 30 sekund; 60 - *(domyślnie)* 1 minuta; 120 - 2 minuty; 600 - 10 minut; 900 - 15 minut.
Grupy hostów	2	groupids.0	ID grupy hostów. Uwaga: Aby skonfigurować wiele grup hostów, utwórz obiekt pola widżetu pulpitu dla każdej grupy hostów z numerem zwiększanym w nazwie właściwości. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Grupy hostów (widżet)	1	groupids._reference	Zamiast ID grupy hostów: `ABCDE._hostgroupids` - ustaw kompatybilny widżet (z parametrem *Reference* ustawionym na "`ABCDE`") jako źródło danych dla grup hostów. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Hosty	3	hostids.0	ID hosta. Uwaga: Aby skonfigurować wiele hostów, utwórz obiekt pola widżetu pulpitu dla każdego hosta z numerem zwiększanym w nazwie właściwości. W przypadku wielu hostów parametr *Grupy hostów* nie może być w ogóle skonfigurowany albo musi być skonfigurowany z co najmniej jedną grupą hostów, do której należą skonfigurowane hosty. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Hosty (widżet/pulpit)	1	hostids._reference	Zamiast ID hosta: `DASHBOARD.hostids` - ustaw selektor hostów pulpitu jako źródło danych dla hostów; `ABCDE._hostids` - ustaw kompatybilny widżet (z parametrem *Reference* ustawionym na "`ABCDE`") jako źródło danych dla hostów. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Tagi hosta			
Typ obliczania	0	evaltype	0 - *(domyślnie)* And/Or; 2 - Or. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Nazwa tagu	1	tags.0.tag	Dowolna wartość tekstowa. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście obliczania tagów. Zachowanie parametru: - *wymagane* podczas konfigurowania *Tagów hosta* Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.

Parametr	type	name	value
Operator	0	tags.0.operator	0 - Zawiera; 1 - Równa się; 2 - Nie zawiera; 3 - Nie równa się; 4 - Istnieje; 5 - Nie istnieje. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście obliczania tagów. Zachowanie parametru: - *wymagane* podczas konfigurowania *Tagów hosta* Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Wartość tagu	1	tags.0.value	Dowolna wartość tekstowa. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście obliczania tagów. Zachowanie parametru: - *wymagane* podczas konfigurowania *Tagów hosta* Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Pokaż hosty w konserwacji	0	maintenance	0 - *(domyślnie)* Wyłączone; 1 - Włączone.
Kolumny (zobacz poniżej)			
Sortuj według	0	column	Wartość liczbowa kolumny z skonfigurowanych kolumn.
Kolejność	0	order	2 - *(domyślnie)* Top N; 3 - Bottom N.
Limit hostów	0	show_lines	Możliwe wartości mieszczą się w zakresie 1-1000. Domyślnie: 10. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.

Kolumny

Kolumny posiadają wspólne parametry oraz dodatkowe parametry w zależności od konfiguracji parametru *Data*.

Note:
Dla wszystkich parametrów związanych z kolumnami, liczba w nazwie właściwości (np. columns.name.0) odnosi się do kolumny, dla której parametr jest skonfigurowany.

Następujące parametry są obsługiwane dla wszystkich kolumn.

Parametr	type	name	value
Nazwa	1	columns.0.name	Dowolna wartość tekstowa. Zachowanie parametru: - *wymagany*

Parametr	type	name	value
Dane	0	columns.0.data	1 - Wartość pozycji; 2 - Nazwa hosta; 3 - Tekst. Zachowanie parametru: - *wymagany*
Kolor bazowy	1	columns.0.base_color	Szesnastkowy kod koloru (np. FF0000). Zachowanie parametru: - *wymagany*

Wartość pozycji

Następujące parametry są obsługiwane, jeśli *Dane* są ustawione na „Wartość pozycji”.

Note:
Pierwsza liczba w nazwie właściwości *Thresholds* (na przykład columnsthresholds.0.color.0) odnosi się do kolumny, dla której skonfigurowano progi, natomiast druga liczba odnosi się do pozycji progu na liście posortowanej rosnąco. Jeśli jednak progi zostaną skonfigurowane w innej kolejności, wartości zostaną posortowane rosnąco po zaktualizowaniu konfiguracji widżetu w frontend Zabbix (na przykład `"threshold.0.threshold":"5"` → `"threshold.0.threshold":"1"`; `"threshold.1.threshold":"1"` → `"threshold.1.threshold": "5"`).

Parametr	type	name	value
Pozycja	1	columns.0.item	Prawidłowa nazwa pozycji. Podczas konfigurowania widżetu na pulpicie szablonu należy ustawiać tylko pozycje skonfigurowane w szablonie.
Wyświetlaj wartość pozycji jako	0	columns.0.display_value_as	0 - *(domyślnie)* Numerycznie; 1 - Tekst; 2 - Binarnie.
Wyświetlanie	0	columns.0.display	1 - *(domyślnie)* Bez zmian; 2 - Pasek; 3 - Wskaźniki; 6 - Wykres iskrowy. Zachowanie parametru: - *obsługiwane*, jeśli *Wyświetlaj wartość pozycji jako* jest ustawione na „Numerycznie”
Min	1	columns.0.min	Dowolna wartość liczbowa. Zachowanie parametru: - *obsługiwane*, jeśli *Wyświetlaj wartość pozycji jako* jest ustawione na „Numerycznie”, a *Wyświetlanie* jest ustawione na „Pasek” lub „Wskaźniki”
Max	1	columns.0.max	Dowolna wartość liczbowa. Zachowanie parametru: - *obsługiwane*, jeśli *Wyświetlaj wartość pozycji jako* jest ustawione na „Numerycznie”, a *Wyświetlanie* jest ustawione na „Pasek” lub „Wskaźniki”
Miejsca dziesiętne	0	columns.0.decimal_places	Możliwe wartości mieszczą się w zakresie 0-10. Domyślnie: 2. Zachowanie parametru: - *obsługiwane*, jeśli *Wyświetlaj wartość pozycji jako* jest ustawione na „Numerycznie”

Parametr	type	name	value
Wykres iskrowy			
Szerokość	0	columns.0.sparkline.width	Możliwe wartości mieszczą się w zakresie 0-10. Domyślnie: 1. Zachowanie parametru: - *obsługiwane*, jeśli *Wyświetlaj wartość pozycji jako* jest ustawione na „Numerycznie”, a *Wyświetlanie* jest ustawione na „Wykres iskrowy”
Wypełnienie	0	columns.0.sparkline.fill	Możliwe wartości mieszczą się w zakresie 0-10. Domyślnie: 3. Zachowanie parametru: - *obsługiwane*, jeśli *Wyświetlaj wartość pozycji jako* jest ustawione na „Numerycznie”, a *Wyświetlanie* jest ustawione na „Wykres iskrowy”
Kolor	1	columns.0.sparkline.color	Szesnastkowy kod koloru (na przykład `FF0000`). Domyślnie: `42A5F5`. Zachowanie parametru: - *obsługiwane*, jeśli *Wyświetlaj wartość pozycji jako* jest ustawione na „Numerycznie”, a *Wyświetlanie* jest ustawione na „Wykres iskrowy”
Okres czasu	1	columns.0.sparkline.time_period.from columns.0.sparkline.time_period.to	`DASHBOARD._timeperiod` — ustaw selektor okresu czasu pulpitu jako źródło danych; `ABCDE._timeperiod` — ustaw kompatybilny widżet (z parametrem `reference` równym `ABCDE`) jako źródło danych. Domyślnie: `DASHBOARD._timeperiod` Alternatywnie można ustawić okres czasu tylko w parametrach *Od* i *Do*. Zachowanie parametru: - *obsługiwane*, jeśli *Wyświetlaj wartość pozycji jako* jest ustawione na „Numerycznie”, a *Wyświetlanie* jest ustawione na „Wykres iskrowy”
Od	1	columns.0.sparkline.time_period.from	Początkowy punkt czasu w składni bezwzględnej (`YYYY-MM-DD hh:mm:ss`) lub względnej (`now`, `now/d`, `now/w-1w` itd.). Zachowanie parametru: - *obsługiwane*, jeśli *Wyświetlaj wartość pozycji jako* jest ustawione na „Numerycznie”, a *Wyświetlanie* jest ustawione na „Wykres iskrowy” - *wymagane*, jeśli ustawiono `columns.0.sparkline.time_period.to`
Do	1	columns.0.sparkline.time_period.to	Końcowy punkt czasu w składni bezwzględnej (`YYYY-MM-DD hh:mm:ss`) lub względnej (`now`, `now/d`, `now/w-1w` itd.). Zachowanie parametru: - *obsługiwane*, jeśli *Wyświetlaj wartość pozycji jako* jest ustawione na „Numerycznie”, a *Wyświetlanie* jest ustawione na „Wykres iskrowy” - *wymagane*, jeśli ustawiono `columns.0.sparkline.time_period.from`
Dane historyczne	0	columns.0.sparkline.history	0 - *(domyślnie)* Auto; 1 - Historia; 2 - Trendy. Zachowanie parametru: - *obsługiwane*, jeśli *Wyświetlaj wartość pozycji jako* jest ustawione na „Numerycznie”, a *Wyświetlanie* jest ustawione na „Wykres iskrowy”
Progi			

Parametr	type	name	value
Kolor	1	columnsthresholds.0.color.0	Szesnastkowy kod koloru (na przykład `FF0000`). Zachowanie parametru: - *obsługiwane*, jeśli *Wyświetlaj wartość pozycji jako* jest ustawione na „Numerycznie”
Próg	1	columnsthresholds.0.threshold.0	Dowolna wartość tekstowa. Zachowanie parametru: - *obsługiwane*, jeśli *Wyświetlaj wartość pozycji jako* jest ustawione na „Numerycznie”
Wyróżnienia			
Kolor	1	columns.0.highlights.0.color	Szesnastkowy kod koloru (na przykład `FF0000`). Zachowanie parametru: - *obsługiwane*, jeśli *Wyświetlaj wartość pozycji jako* jest ustawione na „Tekst”
Wzorzec	1	columns.0.highlights.0.pattern	Dowolna wartość tekstowa. Zachowanie parametru: - *obsługiwane*, jeśli *Wyświetlaj wartość pozycji jako* jest ustawione na „Tekst”
Pokaż miniaturę	0	columns.0.show_thumbnail	0 - *(domyślnie)* Wyłączone; 1 - Włączone. Zachowanie parametru: - *obsługiwane*, jeśli *Wyświetlaj wartość pozycji jako* jest ustawione na „Binarnie”
Funkcja agregacji	0	columns.0.aggregate_function	0 - *(domyślnie)* nieużywana; 1 - min; 2 - max; 3 - avg; 4 - count; 5 - sum; 6 - first; 7 - last.
Okres czasu	1	columns.0.time_period.reference	`DASHBOARD._timeperiod` — ustaw selektor okresu czasu pulpitu jako źródło danych; `ABCDE._timeperiod` — ustaw kompatybilny widżet (z parametrem `reference` równym `ABCDE`) jako źródło danych. Domyślnie: `DASHBOARD._timeperiod` Alternatywnie można ustawić okres czasu tylko w parametrach *Od* i *Do*. Zachowanie parametru: - *obsługiwane*, jeśli *Funkcja agregacji* jest ustawiona na „min”, „max”, „avg”, „count”, „sum”, „first”, „last”
Od	1	columns.0.time_period.from	Prawidłowy ciąg czasu w składni bezwzględnej (`YYYY-MM-DD hh:mm:ss`) lub względnej (`now`, `now/d`, `now/w-1w` itd.). Zachowanie parametru: - *obsługiwane*, jeśli *Okres czasu* nie jest ustawiony, a *Funkcja agregacji* jest ustawiona na „min”, „max”, „avg”, „count”, „sum”, „first”, „last” - *wymagane*, jeśli ustawiono `columns.0.time_period.to`

Parametr	type	name	value
Do	1	columns.0.time_period.to	Prawidłowy ciąg czasu w składni bezwzględnej (`YYYY-MM-DD hh:mm:ss`) lub względnej (`now`, `now/d`, `now/w-1w` itd.). Zachowanie parametru: - *obsługiwane*, jeśli *Okres czasu* nie jest ustawiony, a *Funkcja agregacji* jest ustawiona na „min”, „max”, „avg”, „count”, „sum”, „first”, „last” - *wymagane*, jeśli ustawiono `columns.0.time_period.from`
Dane historyczne	0	columns.0.history	0 - *(domyślnie)* Auto; 1 - Historia; 2 - Trendy. Zachowanie parametru: - *obsługiwane*, jeśli *Wyświetlaj wartość pozycji jako* jest ustawione na „Numerycznie”
Reference	1	reference	Dowolna wartość tekstowa składająca się z 5 znaków (na przykład `ABCDE` lub `JBPNL`). Ta wartość musi być unikalna w obrębie pulpitu, do którego należy widżet. Zachowanie parametru: - *wymagane*

Tekst

Następujące parametry są obsługiwane, jeśli *Dane* są ustawione na ”Tekst”.

Parametr	typ	nazwa	wartość
Tekst	1	columns.0.text	Dowolna wartość tekstowa, w tym makra. Obsługiwane makra: {HOST.*}, {INVENTORY.*}. Zachowanie parametru: - *wymagane*, jeśli *Dane* są ustawione na „Tekst”

Przykłady

Poniższe przykłady mają na celu jedynie opisanie konfiguracji obiektów pól widżetu pulpitu dla widżetu *Top hosts*. Więcej informacji na temat konfiguracji pulpitu można znaleźć w `dashboard.create`.

Konfigurowanie widżetu *Top hosts*

Skonfiguruj widżet *Top hosts*, który wyświetla hosty o najwyższym wykorzystaniu CPU w grupie hostów „4”. Dodatkowo skonfiguruj następujące niestandardowe kolumny: „Nazwa hosta”, „Wykorzystanie CPU w %”, „Średnia 1m”, „Średnia 5m”, „Średnia 15m”, „Procesy”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "dashboard.create",
    "params": {
        "name": "My dashboard",
        "display_period": 30,
        "auto_start": 1,
        "pages": [
            {
                "widgets": [
                    {
                        "type": "tophosts",
                        "name": "Top hosts",
                        "x": 0,
                        "y": 0,
```

```
                "width": 36,
                "height": 5,
                "view_mode": 0,
                "fields": [
                    {
                        "type": 2,
                        "name": "groupids.0",
                        "value": 4
                    },
                    {
                        "type": 1,
                        "name": "columns.0.name",
                        "value": "Host"
                    },
                    {
                        "type": 0,
                        "name": "columns.0.data",
                        "value": 2
                    },
                    {
                        "type": 1,
                        "name": "columns.0.base_color",
                        "value": "FFFFFF"
                    },
                    {
                        "type": 1,
                        "name": "columns.1.name",
                        "value": "CPU utilization in %"
                    },
                    {
                        "type": 0,
                        "name": "columns.1.data",
                        "value": 1
                    },
                    {
                        "type": 1,
                        "name": "columns.1.base_color",
                        "value": "4CAF50"
                    },
                    {
                        "type": 1,
                        "name": "columns.1.item",
                        "value": "CPU utilization"
                    },
                    {
                        "type": 0,
                        "name": "columns.1.display",
                        "value": 3
                    },
                    {
                        "type": 1,
                        "name": "columns.1.min",
                        "value": "0"
                    },
                    {
                        "type": 1,
                        "name": "columns.1.max",
                        "value": "100"
                    },
                    {
                        "type": 1,
                        "name": "columnsthresholds.1.color.0",
```

```
            "value": "FFFF00"
        },
        {
            "type": 1,
            "name": "columnsthresholds.1.threshold.0",
            "value": "50"
        },
        {
            "type": 1,
            "name": "columnsthresholds.1.color.1",
            "value": "FF8000"
        },
        {
            "type": 1,
            "name": "columnsthresholds.1.threshold.1",
            "value": "80"
        },
        {
            "type": 1,
            "name": "columnsthresholds.1.color.2",
            "value": "FF4000"
        },
        {
            "type": 1,
            "name": "columnsthresholds.1.threshold.2",
            "value": "90"
        },
        {
            "type": 1,
            "name": "columns.2.name",
            "value": "1m avg"
        },
        {
            "type": 0,
            "name": "columns.2.data",
            "value": 1
        },
        {
            "type": 1,
            "name": "columns.2.base_color",
            "value": "FFFFFF"
        },
        {
            "type": 1,
            "name": "columns.2.item",
            "value": "Load average (1m avg)"
        },
        {
            "type": 1,
            "name": "columns.3.name",
            "value": "5m avg"
        },
        {
            "type": 0,
            "name": "columns.3.data",
            "value": 1
        },
        {
            "type": 1,
            "name": "columns.3.base_color",
            "value": "FFFFFF"
        },
```

```
                        {
                            "type": 1,
                            "name": "columns.3.item",
                            "value": "Load average (5m avg)"
                        },
                        {
                            "type": 1,
                            "name": "columns.4.name",
                            "value": "15m avg"
                        },
                        {
                            "type": 0,
                            "name": "columns.4.data",
                            "value": 1
                        },
                        {
                            "type": 1,
                            "name": "columns.4.base_color",
                            "value": "FFFFFF"
                        },
                        {
                            "type": 1,
                            "name": "columns.4.item",
                            "value": "Load average (15m avg)"
                        },
                        {
                            "type": 1,
                            "name": "columns.5.name",
                            "value": "Processes"
                        },
                        {
                            "type": 0,
                            "name": "columns.5.data",
                            "value": 1
                        },
                        {
                            "type": 1,
                            "name": "columns.5.base_color",
                            "value": "FFFFFF"
                        },
                        {
                            "type": 1,
                            "name": "columns.5.item",
                            "value": "Number of processes"
                        },
                        {
                            "type": 0,
                            "name": "columns.5.decimal_places",
                            "value": 0
                        },
                        {
                            "type": 0,
                            "name": "column",
                            "value": 1
                        }
                    ]
                }
            ]
        }
    ],
    "userGroups": [
        {
```

```
                "usrgrpid": 7,
                "permission": 2
            }
        ],
        "users": [
            {
                "userid": 1,
                "permission": 3
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "3"
        ]
    },
    "id": 1
}
```

Zobacz także

- Pole widżetu pulpitu
- `dashboard.create`
- `dashboard.update`

29 Najważniejsze pozycje

Opis

Te parametry oraz możliwe wartości właściwości dla odpowiednich obiektów pól widgetu umożliwiają skonfigurowanie widgetu *Top items* w metodach `dashboard.create` i `dashboard.update`.

Attention:
Właściwości `fields` widgetu nie są walidowane podczas tworzenia ani aktualizacji pulpitu. Pozwala to użytkownikom modyfikować wbudowane widgety i tworzyć własne widgety, ale jednocześnie wprowadza ryzyko nieprawidłowego tworzenia lub aktualizowania widgetów. Aby zapewnić pomyślne utworzenie lub aktualizację widgetu *Top items*, zapoznaj się z zachowaniem parametrów opisanym w poniższych tabelach.

Parametry

Następujące parametry są obsługiwane dla widżetu *Top items*.

Parametr	type	name	value
Interwał odświeżania	0	rf_rate	0 - Bez odświeżania; 10 - 10 sekund; 30 - 30 sekund; 60 - *(domyślnie)* 1 minuta; 120 - 2 minuty; 600 - 10 minut; 900 - 15 minut.

Parametr	type	name	value
Grupy hostów	2	groupids.0	ID grupy hostów. Uwaga: Aby skonfigurować wiele grup hostów, utwórz obiekt pola widżetu pulpitu dla każdej grupy hostów z numerem zwiększanym w nazwie właściwości. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Grupy hostów (widżet)	1	groupids._reference	Zamiast ID grupy hostów: `ABCDE._hostgroupids` - ustaw kompatybilny widżet (z parametrem *Reference* ustawionym na "`ABCDE`") jako źródło danych dla grup hostów. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Hosty	3	hostids.0	ID hosta. Uwaga: Aby skonfigurować wiele hostów, utwórz obiekt pola widżetu pulpitu dla każdego hosta z numerem zwiększanym w nazwie właściwości. W przypadku wielu hostów parametr *Grupy hostów* nie może być w ogóle skonfigurowany albo musi być skonfigurowany z co najmniej jedną grupą hostów, do której należą skonfigurowane hosty. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Hosty (widżet/pulpit)	1	hostids._reference	Zamiast ID hosta: `DASHBOARD.hostids` - ustaw selektor hostów pulpitu jako źródło danych dla hostów; `ABCDE._hostids` - ustaw kompatybilny widżet (z parametrem *Reference* ustawionym na "`ABCDE`") jako źródło danych dla hostów. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Tagi hostów			
Typ obliczania	0	host_tags_evaltype	0 - *(domyślnie)* And/Or; 2 - Or. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Nazwa tagu	1	host_tags.0.tag	Dowolna wartość tekstowa. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście obliczania tagów. Zachowanie parametru: - *wymagane* przy konfigurowaniu *Tagów hostów* Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.

Parametr	type	name	value
Operator	0	host_tags.0.operator	0 - Zawiera; 1 - Równa się; 2 - Nie zawiera; 3 - Nie równa się; 4 - Istnieje; 5 - Nie istnieje. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście obliczania tagów. Zachowanie parametru: - *wymagane* przy konfigurowaniu *Tagów hostów* Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Wartość tagu	1	host_tags.0.value	Dowolna wartość tekstowa. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście obliczania tagów. Zachowanie parametru: - *wymagane* przy konfigurowaniu *Tagów hostów* Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Układ	0	layout	0 - *(domyślnie)* Poziomy; 1 - Pionowy.
Pokaż problemy	0	show_problems	0 - Wszystkie; 1 - *(domyślnie)* Nieukryte; 2 - Brak.
Pozycje (zobacz poniżej)			

Zaawansowana konfiguracja

Poniższe zaawansowane parametry konfiguracji są obsługiwane przez widżet *Top items*.

Parametr	type	name	value
Porządkowanie hostów			
Sortuj według	0	host_ordering_order_by	0 - *(domyślnie)* Nazwa hosta; 3 - Wartość pozycji.
Wzorce pozycji	1	host_ordering_item.0	Nazwa lub wzorzec pozycji (np. ”*: Number of processed *values per second”). Uwaga: Aby skonfigurować wiele wzorców pozycji, utwórz obiekt pola widżetu pulpitu dla każdego wzorca pozycji z inkrementowanym numerem w nazwie właściwości. Podczas konfigurowania widżetu na pulpicie szablonu należy ustawić tylko wzorce dla pozycji skonfigurowanych w szablonie. Zachowanie parametru: - *wymagane*, jeśli *Sortuj według* jest ustawione na ”Wartość pozycji”
Kolejność	0	host_ordering_order	2 - *(domyślnie)* Górne N; 3 - Dolne N.
Limit	0	host_ordering_limit	Możliwe wartości mieszczą się w zakresie od 1 do 100. Domyślnie: 10.

Parametr	type	name	value
Porządkowanie pozycji			
Sortuj według	0	item_ordering_order_by	1 - Host; 2 - Nazwa pozycji; 3 - *(domyślnie)* Wartość pozycji.
Wzorce hostów	1	item_ordering_host.0	Nazwa lub wzorzec hosta. Uwaga: Aby skonfigurować wiele wzorców hostów, utwórz obiekt pola widżetu pulpitu dla każdego wzorca hosta z inkrementowanym numerem w nazwie właściwości. Zachowanie parametru: - *wymagane*, jeśli *Sortuj według* jest ustawione na "Host"
Kolejność	0	item_ordering_order	2 - *(domyślnie)* Górne N; 3 - Dolne N.
Limit	0	item_ordering_limit	Możliwe wartości mieszczą się w zakresie od 1 do 100. Domyślnie: 10.

Kolumny

Note:
Pierwsza liczba w nazwie właściwości (np. columns.0.items.0, columns.0.item_tags_evaltype) oznacza konkretną kolumnę, natomiast druga liczba, jeśli występuje, oznacza skonfigurowaną encję (np. wzorzec pozycji, znacznik).

Parametr	type	name	value
Wzorce pozycji	1	columns.0.items.0	Nazwa lub wzorzec pozycji (np. "*: Number of processed *values per second"). Uwaga: Aby skonfigurować wiele wzorców pozycji, utwórz obiekt pola widżetu pulpitu dla każdego wzorca pozycji z inkrementowaną drugą liczbą w nazwie właściwości. Podczas konfigurowania widżetu na pulpicie szablonu należy ustawić tylko wzorce dla pozycji skonfigurowanych w szablonie. Zachowanie parametrów: - *wymagane*
Znaczniki pozycji			
Typ oceny	0	columns.0.item_tags_evaltype	1 - *(domyślnie)* And/Or; 2 - Or.
Nazwa znacznika	1	columns.0.item_tags.0.tag	Dowolna wartość tekstowa. Uwaga: Druga liczba w nazwie właściwości odnosi się do kolejności znacznika na liście oceny znaczników. Zachowanie parametrów: - *wymagane* przy konfigurowaniu *Znaczników pozycji*

Parametr	type	name	value
Operator	0	columns.0.item_tags.0.operator	**0** - Zawiera; 1 - Równe; 2 - Nie zawiera; 3 - Nie równa się; 4 - Istnieje; 5 - Nie istnieje. Uwaga: Druga liczba w nazwie właściwości odnosi się do kolejności znacznika na liście oceny znaczników. Zachowanie parametrów: - *wymagane* przy konfigurowaniu *Znaczników pozycji*
Wartość znacznika	1	columns.0.item_tags.0.value	Dowolna wartość tekstowa. Uwaga: Druga liczba w nazwie właściwości odnosi się do kolejności znacznika na liście oceny znaczników. Zachowanie parametrów: - *wymagane* przy konfigurowaniu *Znaczników pozycji*
Kolor bazowy	1	columns.0.base_color	Szesnastkowy kod koloru (np. FF0000).
Wyświetl wartość jako	0	columns.0.display_value_as	1 - *(domyślnie)* Numerycznie; 2 - Tekst.
Wyświetlanie	0	columns.0.display	1 - *(domyślnie)* Bez zmian; 2 - Pasek; 3 - Wskaźniki; 6 - Sparkline.
Min	1	columns.0.min	Dowolna wartość liczbowa. Obsługiwane są sufiksy (np. ”1d”, ”2w”, ”4K”, ”8G”). Zachowanie parametrów: - *obsługiwane* jeśli *Wyświetl wartość jako* jest ustawione na ”Numerycznie”, a *Wyświetlanie* jest ustawione na ”Pasek” lub ”Wskaźniki”
Max	1	columns.0.max	Dowolna wartość liczbowa. Obsługiwane są sufiksy (np. ”1d”, ”2w”, ”4K”, ”8G”). Zachowanie parametrów: - *obsługiwane* jeśli *Wyświetl wartość jako* jest ustawione na ”Numerycznie”, a *Wyświetlanie* jest ustawione na ”Pasek” lub ”Wskaźniki”
Sparkline			
Szerokość	0	columns.0.sparkline.width	Możliwe wartości mieszczą się w zakresie 0-10. Domyślnie: 1. Zachowanie parametrów: - *obsługiwane* jeśli *Wyświetlanie* jest ustawione na ”Sparkline”
Wypełnienie	0	columns.0.sparkline.fill	Możliwe wartości mieszczą się w zakresie 0-10. Domyślnie: 3. Zachowanie parametrów: - *obsługiwane* jeśli *Wyświetlanie* jest ustawione na ”Sparkline”
Kolor	1	columns.0.sparkline.color	Szesnastkowy kod koloru (np. FF0000). Domyślnie: 42A5F5. Zachowanie parametrów: - *obsługiwane* jeśli *Wyświetlanie* jest ustawione na ”Sparkline”

Parametr	type	name	value
Okres czasu	1	columns.0.sparkline.time_period.from	`DASHBOARD._timeperiod` - ustaw selektor okresu czasu pulpitu jako źródło danych; `ABCDE._timeperiod` - ustaw kompatybilny widżet (z parametrem `reference` równym `ABCDE`) jako źródło danych. Domyślnie: `DASHBOARD._timeperiod` Alternatywnie można ustawić okres czasu tylko w parametrach *Od* i *Do*. Zachowanie parametrów: - *obsługiwane* jeśli *Wyświetlanie* jest ustawione na ”Sparkline”
Od	1	columns.0.sparkline.time_period.from	Prawidłowy ciąg czasu w składni bezwzględnej (`YYYY-MM-DD hh:mm:ss`) lub względnej (`now`, `now/d`, `now/w-1w` itd.). Zachowanie parametrów: - *obsługiwane* jeśli *Wyświetlanie* jest ustawione na ”Sparkline” - *wymagane* jeśli ustawiono `columns.0.sparkline.time_period.to`
Do	1	columns.0.sparkline.time_period.to	Prawidłowy ciąg czasu w składni bezwzględnej (`YYYY-MM-DD hh:mm:ss`) lub względnej (`now`, `now/d`, `now/w-1w` itd.). Zachowanie parametrów: - *obsługiwane* jeśli *Wyświetlanie* jest ustawione na ”Sparkline” - *wymagane* jeśli ustawiono `columns.0.sparkline.time_period.from`
Dane historyczne	0	columns.0.sparkline.history	0 - *(domyślnie)* Auto; 1 - Historia; 2 - Trendy. Zachowanie parametrów: - *obsługiwane* jeśli *Wyświetlanie* jest ustawione na ”Sparkline”
Progi			
Kolor	1	columns.0.thresholds.color	Szesnastkowy kod koloru (np. `FF0000`). Zachowanie parametrów: - *obsługiwane* jeśli *Wyświetl wartość jako* jest ustawione na ”Numerycznie”
Próg	1	columns.0.thresholds.threshold	Dowolna wartość liczbowa. Obsługiwane są sufiksy (np. ”1d”, ”2w”, ”4K”, ”8G”). Zachowanie parametrów: - *obsługiwane* jeśli *Wyświetl wartość jako* jest ustawione na ”Numerycznie”
Wyróżnienia			
Wyróżnienie	1	columns.0.highlights.color	Szesnastkowy kod koloru (np. `FF0000`). Zachowanie parametrów: - *obsługiwane* jeśli *Wyświetl wartość jako* jest ustawione na ”Tekst”
Próg	1	columns.0.highlights.pattern	Dowolne wyrażenie regularne. Zachowanie parametrów: - *obsługiwane* jeśli *Wyświetl wartość jako* jest ustawione na ”Tekst”
Miejsca dziesiętne	0	columns.0.decimal_places	Możliwe wartości mieszczą się w zakresie 0-10. Domyślnie: 2.
Konfiguracja zaawansowana			

Parametr	type	name	value
Funkcja agregacji	0	columns.0.aggregate_function	Jeśli *Wyświetl wartość jako* jest ustawione na ”Numerycznie”: 0 - *(domyślnie)* nieużywane; 1 - min; 2 - max; 3 - avg; 4 - count; 5 - sum; 6 - first; 7 - last. Jeśli *Wyświetl wartość jako* jest ustawione na ”Tekst”: 0 - *(domyślnie)* nieużywane; 4 - count; 6 - first; 7 - last.
Okres czasu	1	columns.0.time_period.from	DASHBOARD._timeperiod - ustaw selektor okresu czasu pulpitu jako źródło danych; ABCDE._timeperiod - ustaw kompatybilny widżet (z parametrem reference równym ABCDE) jako źródło danych. Domyślnie: DASHBOARD._timeperiod Alternatywnie można ustawić okres czasu tylko w parametrach *Od* i *Do*. Zachowanie parametrów: - *obsługiwane* jeśli *Funkcja agregacji* jest ustawiona na ”min”, ”max”, ”avg”, ”count”, ”sum”, ”first”, ”last”
Od	1	columns.0.time_period.from	Prawidłowy ciąg czasu w składni bezwzględnej (YYYY-MM-DD hh:mm:ss) lub względnej (now, now/d, now/w-1w itd.). Zachowanie parametrów: - *obsługiwane* jeśli *Okres czasu* nie jest ustawiony, a *Funkcja agregacji* jest ustawiona na ”min”, ”max”, ”avg”, ”count”, ”sum”, ”first”, ”last” - *wymagane* jeśli ustawiono columns.0.time_period.to
Do	1	columns.0.time_period.to	Prawidłowy ciąg czasu w składni bezwzględnej (YYYY-MM-DD hh:mm:ss) lub względnej (now, now/d, now/w-1w itd.). Zachowanie parametrów: - *obsługiwane* jeśli *Okres czasu* nie jest ustawiony, a *Funkcja agregacji* jest ustawiona na ”min”, ”max”, ”avg”, ”count”, ”sum”, ”first”, ”last” - *wymagane* jeśli ustawiono columns.0.time_period.from
Dane historyczne	0	columns.0.history	0 - *(domyślnie)* Auto; 1 - Historia; 2 - Trendy. Zachowanie parametrów: - *obsługiwane* jeśli *Wyświetl wartość jako* jest ustawione na ”Numerycznie”
Agreguj	0	columns.0.aggregate_columns	0 - *(domyślnie)* Każda pozycja 1 - Łącznie. Zachowanie parametrów: - *obsługiwane* jeśli *Wyświetl wartość jako* jest ustawione na ”Numerycznie”, a *Wyświetlanie* jest ustawione na ”Bez zmian”, ”Pasek” lub ”Wskaźniki”.

Parametr	type	name	value
Funkcja agregacji łączonej	0	columns.0.column_aggregate_function	1 - min; 2 - max; 3 - avg; 4 - count; 5 - sum *(domyślnie)*. Zachowanie parametrów: - *wymagane* przy konfigurowaniu *Agreguj*.
Nazwa kolumny łączonej	1	columns.0.combined_column_name	Dowolna wartość tekstowa. Zachowanie parametrów: - *wymagane* przy konfigurowaniu *Agreguj*.

Przykłady

Poniższe przykłady mają na celu jedynie opisanie konfiguracji obiektów pól widgetu pulpitu dla widgetu *Top items*. Więcej informacji na temat konfiguracji pulpitu można znaleźć w `dashboard.create`.

Konfigurowanie widżetu *Top items*

Skonfiguruj widżet *Top items*, który wyświetla dane dla hosta „10084” i tylko dla pozycji, dla których tag o nazwie „component” zawiera wartość „cpu”. Dodatkowo wyświetl dane z hostami umieszczonymi u góry i użyj kolorowego paska wskaźnika do reprezentacji komórek.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "dashboard.create",
    "params": {
        "name": "My dashboard",
        "display_period": 30,
        "auto_start": 1,
        "pages": [
            {
                "widgets": [
                    {
                        "type": "topitems",
                        "name": "Top items",
                        "x": 0,
                        "y": 0,
                        "width": 36,
                        "height": 5,
                        "view_mode": 0,
                        "fields": [
                            {
                                "type": 3,
                                "name": "hostids.0",
                                "value": 10084
                            },
                            {
                                "type": 1,
                                "name": "columns.0.items.0",
                                "value": "*"
                            },
                            {
                                "type": 1,
                                "name": "columns.0.item_tags.0.tag",
                                "value": "component"
                            },
                            {
                                "type": 0,
                                "name": "columns.0.item_tags.0.operator",
```

```
                                "value": 0
                            },
                            {
                                "type": 1,
                                "name": "columns.0.item_tags.0.value",
                                "value": "cpu"
                            },
                            {
                                "type": 0,
                                "name": "columns.0.display",
                                "value": 2
                            },
                            {
                                "type": 0,
                                "name": "layout",
                                "value": 1
                            }
                        ]
                    }
                ]
            }
        ],
        "userGroups": [
            {
                "usrgrpid": 7,
                "permission": 2
            }
        ],
        "users": [
            {
                "userid": 1,
                "permission": 3
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "3"
        ]
    },
    "id": 1
}
```

Zobacz także

- Pole widżetu pulpitu
- `dashboard.create`
- `dashboard.update`

30 najważniejszych wyzwalaczy

Opis

Te parametry oraz możliwe wartości właściwości dla odpowiednich obiektów pól widgetu umożliwiają skonfigurowanie widgetu *Top triggers* w metodach `dashboard.create` i `dashboard.update`.

Attention:
Właściwości `fields` widgetu nie są walidowane podczas tworzenia ani aktualizacji dashboardu. Pozwala to użytkownikom modyfikować wbudowane widgety i tworzyć własne widgety, ale jednocześnie wprowadza ryzyko nieprawidłowego tworzenia lub aktualizowania widgetów. Aby zapewnić pomyślne utworzenie lub zaktualizowanie widgetu *Top triggers*, zapoznaj się z zachowaniem parametrów opisanym w poniższych tabelach.

Parametry

Następujące parametry są obsługiwane dla widżetu *Top triggers*.

Parametr	type	name	value
Interwał odświeżania	0	rf_rate	0 - *(domyślnie)* Bez odświeżania; 10 - 10 sekund; 30 - 30 sekund; 60 - 1 minuta; 120 - 2 minuty; 600 - 10 minut; 900 - 15 minut.
Grupy hostów	2	groupids.0	ID grupy hostów. Uwaga: Aby skonfigurować wiele grup hostów, utwórz obiekt pola widżetu pulpitu dla każdej grupy hostów z inkrementowanym numerem w nazwie właściwości. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Hosty	3	hostids.0	ID hosta. Uwaga: Aby skonfigurować wiele hostów, utwórz obiekt pola widżetu pulpitu dla każdego hosta z inkrementowanym numerem w nazwie właściwości. W przypadku wielu hostów parametr *Grupy hostów* nie może być w ogóle skonfigurowany albo musi być skonfigurowany z co najmniej jedną grupą hostów, do której należą skonfigurowane hosty. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Problem	1	problem	Nazwa zdarzenia problemu (bez rozróżniania wielkości liter, pełna nazwa lub jej część).
Poziom ważności	0	severities.0	Poziomy ważności wyzwalacza. 0 - Niesklasyfikowane; 1 - Informacja; 2 - Ostrzeżenie; 3 - Średni; 4 - Wysoki; 5 - Katastrofa. Domyślnie: puste (wszystkie włączone). Uwaga: Aby skonfigurować wiele wartości, utwórz obiekt pola widżetu pulpitu dla każdej wartości z inkrementowanym numerem w nazwie właściwości.
Tagi problemu			
Typ oceny	0	evaltype	0 - *(domyślnie)* And/Or; 2 - Or.

Parametr	type	name	value
Nazwa tagu	1	tags.0.tag	Dowolna wartość tekstowa. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście oceny tagów. Zachowanie parametru: - *wymagane* podczas konfigurowania *Tagów problemu*
Operator	0	tags.0.operator	0 - Zawiera; 1 - Równa się; 2 - Nie zawiera; 3 - Nie równa się; 4 - Istnieje; 5 - Nie istnieje. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście oceny tagów. Zachowanie parametru: - *wymagane* podczas konfigurowania *Tagów problemu*
Wartość tagu	1	tags.0.value	Dowolna wartość tekstowa. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście oceny tagów. Zachowanie parametru: - *wymagane* podczas konfigurowania *Tagów problemu*
Okres czasu	1	time_period._reference	`DASHBOARD._timeperiod` - ustaw selektor okresu czasu pulpitu jako źródło danych; `ABCDE._timeperiod` - ustaw kompatybilny widżet (z parametrem *Reference* ustawionym na "`ABCDE`") jako źródło danych. Domyślnie: `DASHBOARD._timeperiod` Alternatywnie możesz ustawić okres czasu tylko w parametrach *Od* i *Do*.
Od	1	time_period.from	Prawidłowy ciąg czasu w składni czasu bezwzględnego (`YYYY-MM-DD hh:mm:ss`) lub względnego (`now`, `now/d`, `now/w-1w` itd.). Zachowanie parametru: - *obsługiwane* jeśli *Okres czasu* nie jest ustawiony - *wymagane* jeśli ustawiono `time_period.to`
Do	1	time_period.to	Prawidłowy ciąg czasu w składni czasu bezwzględnego (`YYYY-MM-DD hh:mm:ss`) lub względnego (`now`, `now/d`, `now/w-1w` itd.). Zachowanie parametru: - *obsługiwane* jeśli *Okres czasu* nie jest ustawiony - *wymagane* jeśli ustawiono `time_period.from`
Limit wyzwalaczy	0	show_lines	Możliwe wartości mieszczą się w zakresie 1-100. Domyślnie: 10.

Przykłady

Poniższe przykłady mają na celu jedynie opisanie konfiguracji obiektów pól widżetu pulpitu dla widżetu *Top triggers*. Więcej informacji na temat konfiguracji pulpitu można znaleźć w `dashboard.create`.

Konfigurowanie widżetu *Top triggers*

Skonfiguruj widżet *Top triggers*, który wyświetla 5 najważniejszych wyzwalaczy dla grupy hostów „4" wraz z liczbą wszystkich problemów dla każdego wyzwalacza. Widżet wyświetla tylko wyzwalacze o poziomach ważności „Warning", „Average", „High" lub

„Disaster” oraz problemy, które mają tag o nazwie „scope”, zawierający wartości „performance”, „availability” lub „capacity”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "dashboard.create",
    "params": {
        "name": "My dashboard",
        "display_period": 30,
        "auto_start": 1,
        "pages": [
            {
                "widgets": [
                    {
                        "type": "toptriggers",
                        "name": "Top triggers",
                        "x": 0,
                        "y": 0,
                        "width": 36,
                        "height": 5,
                        "view_mode": 0,
                        "fields": [
                            {
                                "type": 2,
                                "name": "groupids.0",
                                "value": 4
                            },
                            {
                                "type": 0,
                                "name": "severities.0",
                                "value": 2
                            },
                            {
                                "type": 0,
                                "name": "severities.1",
                                "value": 3
                            },
                            {
                                "type": 0,
                                "name": "severities.2",
                                "value": 4
                            },
                            {
                                "type": 0,
                                "name": "severities.3",
                                "value": 5
                            },
                            {
                                "type": 1,
                                "name": "tags.0.tag",
                                "value": "scope"
                            },
                            {
                                "type": 0,
                                "name": "tags.0.operator",
                                "value": 0
                            },
                            {
                                "type": 1,
                                "name": "tags.0.value",
                                "value": "performance"
                            },
                            {
```

```
                                "type": 1,
                                "name": "tags.1.tag",
                                "value": "scope"
                            },
                            {
                                "type": 0,
                                "name": "tags.1.operator",
                                "value": 0
                            },
                            {
                                "type": 1,
                                "name": "tags.1.value",
                                "value": "availability"
                            },
                            {
                                "type": 1,
                                "name": "tags.2.tag",
                                "value": "scope"
                            },
                            {
                                "type": 0,
                                "name": "tags.2.operator",
                                "value": 0
                            },
                            {
                                "type": 1,
                                "name": "tags.2.value",
                                "value": "capacity"
                            },
                            {
                                "type": 0,
                                "name": "show_lines",
                                "value": 5
                            }
                        ]
                    }
                ]
            }
        ],
        "userGroups": [
            {
                "usrgrpid": 7,
                "permission": 2
            }
        ],
        "users": [
            {
                "userid": 1,
                "permission": 3
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "3"
        ]
```

```
    },
    "id": 1
}
```

Zobacz także

- Pole widżetu pulpitu
- `dashboard.create`
- `dashboard.update`

31 Przegląd wyzwalaczy

Opis

Te parametry oraz możliwe wartości właściwości dla odpowiednich obiektów pól widgetu umożliwiają konfigurację widgetu *Przegląd wyzwalaczy* w metodach `dashboard.create` i `dashboard.update`.

Attention:
Właściwości `fields` widgetu nie są walidowane podczas tworzenia ani aktualizacji dashboardu. Pozwala to użytkownikom modyfikować wbudowane widgety i tworzyć własne widgety, ale jednocześnie wprowadza ryzyko nieprawidłowego tworzenia lub aktualizowania widgetów. Aby zapewnić pomyślne utworzenie lub zaktualizowanie widgetu *Przegląd wyzwalaczy*, zapoznaj się z zachowaniem parametrów opisanym w poniższych tabelach.

Parametry

Następujące parametry są obsługiwane dla widżetu *Przegląd wyzwalaczy*.

Parametr	type	name	value
Interwał odświeżania	0	rf_rate	0 - Bez odświeżania; 10 - 10 sekund; 30 - 30 sekund; 60 - *(domyślnie)* 1 minuta; 120 - 2 minuty; 600 - 10 minut; 900 - 15 minut.
Pokaż	0	show	1 - *(domyślnie)* Ostatnie problemy; 2 - Dowolne; 3 - Problemy.
Grupy hostów	2	groupids.0	ID grupy hostów. Uwaga: Aby skonfigurować wiele grup hostów, utwórz obiekt pola widżetu pulpitu dla każdej grupy hostów z inkrementowanym numerem w nazwie właściwości. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Grupy hostów (Widżet)	1	groupids._reference	Zamiast ID grupy hostów: `ABCDE._hostgroupids` - ustaw kompatybilny widżet (z parametrem *Reference* ustawionym na "ABCDE") jako źródło danych dla grup hostów. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.

Parametr	type	name	value
Hosty	3	hostids.0	ID hosta. Uwaga: Aby skonfigurować wiele hostów, utwórz obiekt pola widżetu pulpitu dla każdego hosta z inkrementowanym numerem w nazwie właściwości. W przypadku wielu hostów parametr *Grupy hostów* nie może być w ogóle skonfigurowany albo musi być skonfigurowany z co najmniej jedną grupą hostów, do której należą skonfigurowane hosty. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Hosty (Widżet/Pulpit)	1	hostids._reference	Zamiast ID hosta: `DASHBOARD.hostids` - ustaw selektor hostów pulpitu jako źródło danych dla hostów; `ABCDE._hostids` - ustaw kompatybilny widżet (z parametrem *Reference* ustawionym na "`ABCDE`") jako źródło danych dla hostów. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Tagi problemów			
Typ oceny	0	evaltype	0 - *(domyślnie)* I/Lub; 2 - Lub.
Nazwa tagu	1	tags.0.tag	Dowolna wartość tekstowa. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście oceny tagów. Zachowanie parametru: - *wymagane* podczas konfigurowania *Tagów problemów*
Operator	0	tags.0.operator	0 - Zawiera; 1 - Równa się; 2 - Nie zawiera; 3 - Nie równa się; 4 - Istnieje; 5 - Nie istnieje. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście oceny tagów. Zachowanie parametru: - *wymagane* podczas konfigurowania *Tagów problemów*
Wartość tagu	1	tags.0.value	Dowolna wartość tekstowa. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście oceny tagów. Zachowanie parametru: - *wymagane* podczas konfigurowania *Tagów problemów*
Pokaż wycisz. problemy	0	show_suppressed	0 - *(domyślnie)* Wyłączone; 1 - Włączone.
Układ	0	layout	0 - *(domyślnie)* Poziomy; 1 - Pionowy.

Przykłady

Poniższe przykłady mają na celu jedynie opisanie konfiguracji obiektów pól widżetu pulpitu dla widżetu *Przegląd wyzwalaczy*.

Więcej informacji na temat konfiguracji pulpitu można znaleźć w `dashboard.create`.

Konfigurowanie widżetu *Przegląd wyzwalaczy*

Skonfiguruj widżet *Przegląd wyzwalaczy*, który wyświetla stany wyzwalaczy dla wszystkich grup hostów mających wyzwalacze z tagiem o nazwie „scope” i zawierającym wartość „availability”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "dashboard.create",
    "params": {
        "name": "My dashboard",
        "display_period": 30,
        "auto_start": 1,
        "pages": [
            {
                "widgets": [
                    {
                        "type": "trigover",
                        "name": "Trigger overview",
                        "x": 0,
                        "y": 0,
                        "width": 36,
                        "height": 5,
                        "view_mode": 0,
                        "fields": [
                            {
                                "type": 1,
                                "name": "tags.0.tag",
                                "value": "scope"
                            },
                            {
                                "type": 0,
                                "name": "tags.0.operator",
                                "value": 0
                            },
                            {
                                "type": 1,
                                "name": "tags.0.value",
                                "value": "availability"
                            }
                        ]
                    }
                ]
            }
        ],
        "userGroups": [
            {
                "usrgrpid": 7,
                "permission": 2
            }
        ],
        "users": [
            {
                "userid": 1,
                "permission": 3
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "3"
        ]
    },
    "id": 1
}
```

Zobacz także

- Pole widżetu pulpitu
- `dashboard.create`
- `dashboard.update`

32 URL

Opis

Te parametry oraz możliwe wartości właściwości dla odpowiednich obiektów pól widgetu umożliwiają skonfigurowanie widgetu *URL* w metodach `dashboard.create` i `dashboard.update`.

Attention:
Właściwości `fields` widgetu nie są walidowane podczas tworzenia ani aktualizacji pulpitu. Pozwala to użytkownikom modyfikować wbudowane widgety i tworzyć własne widgety, ale jednocześnie wprowadza ryzyko nieprawidłowego tworzenia lub aktualizowania widgetów. Aby zapewnić pomyślne utworzenie lub aktualizację widgetu *URL*, zapoznaj się z zachowaniem parametrów opisanym w poniższych tabelach.

Parametry

Następujące parametry są obsługiwane dla widżetu *URL*.

Parametr	type	name	value
Interwał odświeżania	0	rf_rate	0 - *(domyślnie)* Bez odświeżania; 10 - 10 sekund; 30 - 30 sekund; 60 - 1 minuta; 120 - 2 minuty; 600 - 10 minut; 900 - 15 minut.
URL	1	url	Prawidłowy ciąg URL. Zachowanie parametru: - *wymagany*
Nadpisz host	1	override_hostid._reference	`ABCDE._hostid` - ustaw kompatybilny widżet (z parametrem *Reference* ustawionym na "ABCDE") jako źródło danych dla hostów; `DASHBOARD._hostid` - ustaw selektor hosta jako źródło danych dla hostów. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.

Przykłady

Poniższe przykłady mają na celu jedynie opisanie konfiguracji obiektów pól widżetu pulpitu dla widżetu *URL*. Więcej informacji na temat konfiguracji pulpitu można znaleźć w `dashboard.create`.

Konfigurowanie widżetu *URL*

Skonfiguruj widżet *URL*, który wyświetla stronę główną podręcznika Zabbix.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "dashboard.create",
    "params": {
        "name": "My dashboard",
        "display_period": 30,
        "auto_start": 1,
        "pages": [
            {
                "widgets": [
                    {
                        "type": "url",
                        "name": "URL",
                        "x": 0,
                        "y": 0,
                        "width": 36,
                        "height": 5,
                        "view_mode": 0,
                        "fields": [
                            {
                                "type": 1,
                                "name": "url",
                                "value": "https://www.zabbix.com/documentation/8.0/en"
                            }
                        ]
                    }
                ]
            }
        ],
        "userGroups": [
            {
                "usrgrpid": 7,
                "permission": 2
            }
        ],
        "users": [
            {
                "userid": 1,
                "permission": 3
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "3"
        ]
    },
    "id": 1
}
```

Zobacz także

- Pole widżetu pulpitu
- dashboard.create
- dashboard.update

33 Monitorowanie WWW

Opis

Te parametry oraz możliwe wartości właściwości dla odpowiednich obiektów pól widgetu umożliwiają skonfigurowanie widgetu *Monitorowanie WWW* w metodach `dashboard.create` i `dashboard.update`.

Attention:
Właściwości `fields` widgetu nie są walidowane podczas tworzenia ani aktualizacji dashboardu. Pozwala to użytkownikom modyfikować wbudowane widgety i tworzyć niestandardowe widgety, ale jednocześnie wprowadza ryzyko nieprawidłowego tworzenia lub aktualizowania widgetów. Aby zapewnić pomyślne utworzenie lub aktualizację widgetu *Monitorowanie WWW*, zapoznaj się z zachowaniem parametrów opisanym w poniższych tabelach.

Parametry

Następujące parametry są obsługiwane dla widżetu *Monitorowanie WWW*.

Parametr	type	name	value
Interwał odświeżania	0	rf_rate	0 - Bez odświeżania; 10 - 10 sekund; 30 - 30 sekund; 60 - *(domyślnie)* 1 minuta; 120 - 2 minuty; 600 - 10 minut; 900 - 15 minut.
Grupy hostów	2	groupids.0	ID grupy hostów. Uwaga: Aby skonfigurować wiele grup hostów, utwórz obiekt pola widżetu pulpitu dla każdej grupy hostów z inkrementowanym numerem w nazwie właściwości. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Grupy hostów (Widżet)	1	groupids._reference	Zamiast ID grupy hostów: `ABCDE._hostgroupids` - ustaw kompatybilny widżet (z parametrem *Reference* ustawionym na "ABCDE") jako źródło danych dla grup hostów. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Wyklucz grupy hostów	2	exclude_groupids.0	ID grupy hostów. Uwaga: Aby wykluczyć wiele grup hostów, utwórz obiekt pola widżetu pulpitu dla każdej grupy hostów z inkrementowanym numerem w nazwie właściwości. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Hosty	3	hostids.0	ID hosta. Uwaga: Aby skonfigurować wiele hostów, utwórz obiekt pola widżetu pulpitu dla każdego hosta z inkrementowanym numerem w nazwie właściwości. W przypadku wielu hostów parametr *Grupy hostów* nie może być w ogóle skonfigurowany albo musi być skonfigurowany z co najmniej jedną grupą hostów, do której należą skonfigurowane hosty. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.

Parametr	type	name	value
Hosty (Widżet/Pulpit)	1	hostids._reference	Zamiast ID hosta: `DASHBOARD.hostids` - ustaw selektor hostów pulpitu jako źródło danych dla hostów; `ABCDE._hostids` - ustaw kompatybilny widżet (z parametrem *Reference* ustawionym na "`ABCDE`") jako źródło danych dla hostów. Ten parametr nie jest obsługiwany podczas konfigurowania widżetu na pulpicie szablonu.
Tagi scenariusza			
Typ obliczania	0	evaltype	0 - *(domyślnie)* And/Or; 2 - Or.
Nazwa tagu	1	tags.0.tag	Dowolna wartość tekstowa. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście obliczania tagów. Zachowanie parametru: - *wymagane* przy konfigurowaniu *Tagów scenariusza*
Operator	0	tags.0.operator	0 - Zawiera; 1 - Równa się; 2 - Nie zawiera; 3 - Nie równa się; 4 - Istnieje; 5 - Nie istnieje. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście obliczania tagów. Zachowanie parametru: - *wymagane* przy konfigurowaniu *Tagów scenariusza*
Wartość tagu	1	tags.0.value	Dowolna wartość tekstowa. Uwaga: Numer w nazwie właściwości odnosi się do kolejności tagu na liście obliczania tagów. Zachowanie parametru: - *wymagane* przy konfigurowaniu *Tagów scenariusza*
Pokaż hosty w utrzymaniu	0	maintenance	0 - Wyłączone; 1 - *(domyślnie)* Włączone.
Reference	1	reference	Dowolna wartość tekstowa składająca się z 5 znaków (np. `ABCDE` lub `JBPNL`). Ta wartość musi być unikalna w obrębie pulpitu, do którego należy widżet. Zachowanie parametru: - *wymagane*

Przykłady

Poniższe przykłady mają na celu jedynie opisanie konfiguracji obiektów pól widżetu pulpitu dla widżetu *Web monitoring*. Więcej informacji na temat konfiguracji pulpitu można znaleźć w `dashboard.create`.

Konfigurowanie widżetu *Web monitoring*

Skonfiguruj widżet *Web monitoring*, który wyświetla podsumowanie statusu aktywnych scenariuszy monitorowania WWW dla grupy hostów „4".

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "dashboard.create",
    "params": {
        "name": "My dashboard",
        "display_period": 30,
        "auto_start": 1,
        "pages": [
            {
                "widgets": [
                    {
                        "type": "web",
                        "name": "Web monitoring",
                        "x": 0,
                        "y": 0,
                        "width": 18,
                        "height": 3,
                        "view_mode": 0,
                        "fields": [
                            {
                                "type": 2,
                                "name": "groupids.0",
                                "value": 4
                            }
                        ]
                    }
                ]
            }
        ],
        "userGroups": [
            {
                "usrgrpid": 7,
                "permission": 2
            }
        ],
        "users": [
            {
                "userid": 1,
                "permission": 3
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "3"
        ]
    },
    "id": 1
}
```

Zobacz także

- Pole widżetu pulpitu
- dashboard.create
- dashboard.update

Pulpit szablonu

Ta klasa została zaprojektowana do pracy z pulpitami szablonów.

Odwołania do obiektów:

- Pulpit szablonu
- Strona pulpitu szablonu
  - Widget pulpitu szablonu
    - Pole widgetu pulpitu szablonu

Dostępne metody:

- templatedashboard.create - utwórz nowe pulpity szablonów
- templatedashboard.delete - usuń pulpity szablonów
- templatedashboard.get - pobierz pulpity szablonów
- templatedashboard.update - zaktualizuj pulpity szablonów

Obiekt pulpitu nawigacyjnego szablonu

Następujące obiekty są bezpośrednio powiązane z API `templateashboard`.

Pulpit szablonu

Obiekt pulpitu szablonu ma następujące właściwości.

Właściwość	Typ	Opis
dashboardid	ID	ID pulpitu szablonu. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji
name	string	Nazwa pulpitu szablonu. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
templateid	ID	ID szablonu, do którego należy pulpit. Zachowanie właściwości: - *stałe* - *wymagane* dla operacji tworzenia
display_period	integer	Domyślny okres wyświetlania strony (w sekundach). Możliwe wartości: 10, 30, 60, 120, 600, 1800, 3600. Domyślnie: 30.
auto_start	integer	Automatyczne uruchamianie pokazu slajdów. Możliwe wartości: 0 - nie uruchamiaj automatycznie pokazu slajdów; 1 - *(domyślnie)* uruchamiaj automatycznie pokaz slajdów.
uuid	string	Uniwersalny unikalny identyfikator używany do łączenia importowanych pulpitów szablonów z już istniejącymi. Generowany automatycznie, jeśli nie został podany.

Strona pulpitu szablonu

Obiekt strony pulpitu szablonu ma następujące właściwości.

Właściwość	Typ	Opis
dashboard_pageid	ID	ID strony pulpitu. Zachowanie właściwości: - *tylko do odczytu*
name	string	Nazwa strony pulpitu. Domyślnie: pusty ciąg.
display_period	integer	Okres wyświetlania strony pulpitu (w sekundach). Możliwe wartości: 0, 10, 30, 60, 120, 600, 1800, 3600. Domyślnie: 0 (zostanie użyty domyślny okres wyświetlania strony).
widgets	array	Tablica obiektów widgetu pulpitu szablonu.

Widżet pulpitu szablonu

Obiekt widżetu pulpitu szablonu ma następujące właściwości.

Właściwość	Typ	Opis
widgetid	ID	ID widżetu pulpitu. Zachowanie właściwości: - *tylko do odczytu*

Właściwość	Typ	Opis
type	string	Typ widżetu pulpitu. Możliwe wartości: actionlog - Dziennik akcji; clock - Zegar; discovery - Status wykrywania; favgraphs - Ulubione wykresy; favmaps - Ulubione mapy; gauge - Wskaźnik; graph - Wykres (klasyczny); graphprototype - Prototyp wykresu; honeycomb - Honeycomb; hostavail - Dostępność hosta; hostcard - Karta hosta; hostnavigator - Nawigator hostów; itemcard - Karta pozycji; itemnavigator - Nawigator pozycji; item - Wartość pozycji; map - Mapa; navtree - Drzewo nawigacji map; piechart - Wykres kołowy; plaintext - Zwykły tekst; problemhosts - Hosty z problemami; problems - Problemy; problemsbysv - Problemy według ważności; scatterplot - Wykres punktowy; slareport - Raport SLA; svggraph - Wykres; systeminfo - Informacje o systemie; tophosts - Najlepsze hosty; topitems - Najlepsze pozycje; toptriggers - Najważniejsze wyzwalacze; trigover - Przegląd wyzwalaczy; url - URL; web - Monitorowanie WWW. Zachowanie właściwości: - *wymagane*
name	string	Niestandardowa nazwa widżetu.
x	integer	Pozycja pozioma od lewej strony pulpitu. Możliwe wartości mieszczą się w zakresie od 0 do 71.
y	integer	Pozycja pionowa od górnej krawędzi pulpitu. Możliwe wartości mieszczą się w zakresie od 0 do 63.
width	integer	Szerokość widżetu. Możliwe wartości mieszczą się w zakresie od 1 do 72.
height	integer	Wysokość widżetu. Możliwe wartości mieszczą się w zakresie od 1 do 64.
view_mode	integer	Tryb widoku widżetu. Możliwe wartości: 0 - *(domyślnie)* domyślny widok widżetu; 1 - z ukrytym nagłówkiem;
fields	array	Tablica obiektów pola widżetu pulpitu szablonu.

Pole widgetu pulpitu szablonu

Obiekt pola widgetu pulpitu szablonu ma następujące właściwości.

Właściwość	Typ	Opis
type	integer	Typ pola widgetu. Możliwe wartości: 0 - Integer; 1 - String; 4 - Pozycja; 5 - Prototyp pozycji; 6 - Wykres; 7 - Prototyp wykresu; 8 - Mapa; 9 - Usługa; 10 - SLA; 11 - Użytkownik; 12 - Akcja; 13 - Typ nośnika. Zachowanie właściwości: - *wymagane*
name	string	Nazwa pola widgetu. Możliwe wartości: patrz Pola widgetu pulpitu. Należy pamiętać, że niektóre parametry związane z hostem (np. *Grupy hostów*, *Wyklucz grupy hostów* i *Hosty* w widżecie *Problemy*, *Grupy hostów* w widżecie *Dostępność hostów* itd.) nie są dostępne podczas konfigurowania widgetu na pulpicie szablonu. Wynika to z tego, że pulpity szablonów wyświetlają dane tylko z hosta, do którego szablon jest podłączony. Zachowanie właściwości: - *wymagane*
value	mixed	Wartość pola widgetu zależna od typu. Możliwe wartości: patrz Pola widgetu pulpitu. Należy pamiętać, że niektóre parametry związane z hostem (np. *Grupy hostów*, *Wyklucz grupy hostów* i *Hosty* w widżecie *Problemy*, *Grupy hostów* w widżecie *Dostępność hostów* itd.) nie są dostępne podczas konfigurowania widgetu na pulpicie szablonu. Wynika to z tego, że pulpity szablonów wyświetlają dane tylko z hosta, do którego szablon jest podłączony. Zachowanie właściwości: - *wymagane*

templatedashboard.create

Opis

`object templatedashboard.create(object/array templateDashboards)`

Ta metoda umożliwia tworzenie nowych pulpitów szablonów.

> **Note:**
> Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach ról użytkowników. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Pulpity szablonu do utworzenia.

Oprócz standardowych właściwości pulpitu szablonu, metoda akceptuje następujące parametry.

Parametr	Type	Opis
pages	array	Strony pulpitu szablonu, które mają zostać utworzone dla pulpitu. Strony pulpitu będą uporządkowane w tej samej kolejności, w jakiej zostały podane. Zachowanie parametru: - *wymagany*

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory utworzonych pulpitów nawigacyjnych szablonu we właściwości `dashboardids`. Kolejność zwróconych identyfikatorów odpowiada kolejności przekazanych pulpitów nawigacyjnych szablonu.

Przykłady

Tworzenie dashboardu szablonu

Utwórz dashboard szablonu o nazwie „Graphs” z jednym widżetem Graph na pojedynczej stronie dashboardu.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "templatedashboard.create",
    "params": {
        "templateid": "10318",
        "name": "Graphs",
        "pages": [
            {
                "widgets": [
                    {
                        "type": "graph",
                        "x": 0,
                        "y": 0,
                        "width": 12,
                        "height": 5,
                        "view_mode": 0,
                        "fields": [
                            {
                                "type": 6,
                                "name": "graphid",
                                "value": "1123"
                            }
                        ]
                    }
                ]

            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "32"
        ]
    },
    "id": 1
}
```

Zobacz także

- Strona pulpitu szablonu
- Widżet pulpitu szablonu
- Pole widżetu pulpitu szablonu

Źródło

CTemplateDashboard::create() w *ui/include/classes/api/services/CTemplateDashboard.php*.

templatedashboard.delete

Opis

`object templatedashboard.delete(array templateDashboardIds)`

Ta metoda umożliwia usuwanie szablonów pulpitów.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkowników typu *Admin* i *Super admin*. Uprawnienia do wywołania metody można odwołać w ustawieniach roli użytkownika. Więcej informacji można znaleźć w User roles.

Parametry

`(array)` ID pulpitów szablonu do usunięcia.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory usuniętych pulpitów szablonu we właściwości `dashboardids`.

Przykłady

Usuwanie wielu pulpitów szablonów

Usuń dwa pulpity szablonów.

Żądanie:

```
{
"jsonrpc": "2.0",
"method": "templateashboard.delete",
"params": [
"45",
"46"
],
"id": 1
}
```

Odpowiedź:

```
{
"jsonrpc": "2.0",
"result": {
"dashboardids": [
"45",
"46"
]
},
"id": 1
}
```

Źródło

CTemplateDashboard::delete() w *ui/include/classes/api/services/CTemplateDashboard.php*.

templatedashboard.get

Opis

`integer/array templatedashboard.get(object parameters)`

Ta metoda umożliwia pobieranie pulpitów szablonów zgodnie z podanymi parametrami.

Note:
Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
dashboardids	ID/array	Zwraca tylko dashboardy szablonów o podanych identyfikatorach.
templateids	ID/array	Zwraca tylko dashboardy szablonów należące do podanych szablonów.
selectPages	query	Zwraca właściwość `pages` ze stronami dashboardu szablonu, w poprawnej kolejności.
sortfield	string/array	Sortuje wynik według podanych właściwości. Możliwe wartości: `dashboardid`, `name`.
countOutput	boolean	Te parametry są opisane w komentarzu referencyjnym.
editable	boolean	
excludeSearch	boolean	
filter	object	
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli został użyty parametr `countOutput`.

Przykłady

Pobieranie pulpitów szablonu

Pobierz wszystkie pulpity szablonu z widgetami dla określonego szablonu.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "templatedashboard.get",
    "params": {
        "output": "extend",
        "selectPages": "extend",
        "templateids": "10001"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "dashboardid": "23",
            "name": "Docker overview",
            "templateid": "10001",
```

```
            "display_period": "30",
            "auto_start": "1",
            "uuid": "6dfcbe0bc5ad400ea9c1c2dd7649282f",
            "pages": [
                {
                    "dashboard_pageid": "1",
                    "name": "",
                    "display_period": "0",
                    "widgets": [
                        {
                            "widgetid": "220",
                            "type": "graph",
                            "name": "",
                            "x": "0",
                            "y": "0",
                            "width": "36",
                            "height": "5",
                            "view_mode": "0",
                            "fields": [
                                {
                                    "type": "6",
                                    "name": "graphid",
                                    "value": "1125"
                                }
                            ]
                        },
                        {
                            "widgetid": "221",
                            "type": "graph",
                            "name": "",
                            "x": "12",
                            "y": "0",
                            "width": "36",
                            "height": "5",
                            "view_mode": "0",
                            "fields": [
                                {
                                    "type": "6",
                                    "name": "graphid",
                                    "value": "1129"
                                }
                            ]
                        },
                        {
                            "widgetid": "222",
                            "type": "graph",
                            "name": "",
                            "x": "0",
                            "y": "5",
                            "width": "36",
                            "height": "5",
                            "view_mode": "0",
                            "fields": [
                                {
                                    "type": "6",
                                    "name": "graphid",
                                    "value": "1128"
                                }
                            ]
                        },
                        {
                            "widgetid": "223",
```

```
                            "type": "graph",
                            "name": "",
                            "x": "12",
                            "y": "5",
                            "width": "36",
                            "height": "5",
                            "view_mode": "0",
                            "fields": [
                                {
                                    "type": "6",
                                    "name": "graphid",
                                    "value": "1126"
                                }
                            ]
                        },
                        {
                            "widgetid": "224",
                            "type": "graph",
                            "name": "",
                            "x": "0",
                            "y": "10",
                            "width": "36",
                            "height": "5",
                            "view_mode": "0",
                            "fields": [
                                {
                                    "type": "6",
                                    "name": "graphid",
                                    "value": "1127"
                                }
                            ]
                        }
                    ]
                }
            ]
        }
    ],
    "id": 1
}
```


Zobacz także

- Strona pulpitu szablonu
- Widżet pulpitu szablonu
- Pole widżetu pulpitu szablonu

Źródło

CTemplateDashboard::get() w *ui/include/classes/api/services/CTemplateDashboard.php*.

templatedashboard.update

Opis

`object templatedashboard.update(object/array templateDashboards)`

Ta metoda umożliwia aktualizację istniejących dashboardów szablonów.

> **Note:**
> Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Właściwości pulpitu nawigacyjnego szablonu do zaktualizowania.

Właściwość dashboardid musi być określona dla każdego pulpitu nawigacyjnego, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko określone właściwości.

Oprócz standardowych właściwości pulpitu nawigacyjnego szablonu, metoda akceptuje następujące parametry.

Parametr	Typ	Opis
pages	array	Strony pulpitu nawigacyjnego szablonu, które zastąpią istniejące strony pulpitu nawigacyjnego. Strony pulpitu nawigacyjnego są aktualizowane za pomocą właściwości dashboard_pageid. Nowe strony pulpitu nawigacyjnego zostaną utworzone dla obiektów bez właściwości dashboard_pageid, a istniejące strony pulpitu nawigacyjnego zostaną usunięte, jeśli nie zostaną ponownie użyte. Strony pulpitu nawigacyjnego zostaną uporządkowane w tej samej kolejności, w jakiej zostały określone. Zaktualizowane zostaną tylko określone właściwości stron pulpitu nawigacyjnego. Dla właściwości pages wymagany jest co najmniej jeden obiekt strony pulpitu nawigacyjnego.

Wartości zwracane

(object) Zwraca obiekt zawierający identyfikatory zaktualizowanych pulpitów szablonu we właściwości dashboardids.

Przykłady

Zmiana nazwy dashboardu szablonu

Zmień nazwę dashboardu szablonu na „Performance graphs”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "templatedashboard.update",
    "params": {
        "dashboardid": "23",
        "name": "Performance graphs"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "23"
        ]
    },
    "id": 1
}
```

Aktualizowanie stron pulpitu nawigacyjnego szablonu

Zmień nazwę pierwszej strony pulpitu nawigacyjnego, zastąp widgety na drugiej stronie pulpitu nawigacyjnego i dodaj nową stronę jako trzecią. Usuń wszystkie pozostałe strony pulpitu nawigacyjnego.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "templatedashboard.update",
    "params": {
        "dashboardid": "2",
        "pages": [
            {
                "dashboard_pageid": 1,
```

```
                "name": "Renamed Page"
            },
            {
                "dashboard_pageid": 2,
                "widgets": [
                    {
                        "type": "clock",
                        "x": 0,
                        "y": 0,
                        "width": 12,
                        "height": 3
                    }
                ]
            },
            {
                "display_period": 60
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "2"
        ]
    },
    "id": 1
}
```

Zobacz także

- Widżet pulpitu szablonu
- Pole widżetu pulpitu szablonu

Źródło

CTemplateDashboard::update() w *ui/include/classes/api/services/CTemplateDashboard.php*.

Raport

Ta klasa jest przeznaczona do pracy z zaplanowanymi raportami.

Odwołania do obiektów:

- Report
- Users
- User groups

Dostępne metody:

- report.create - tworzenie nowych zaplanowanych raportów
- report.delete - usuwanie zaplanowanych raportów
- report.get - pobieranie zaplanowanych raportów
- report.update - aktualizowanie zaplanowanych raportów

Obiekt raportu

Następujące obiekty są bezpośrednio powiązane z API `report`.

Raport

Obiekt raportu ma następujące właściwości:

Właściwość	Typ	Opis
reportid	ID	ID raportu. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji
userid	ID	ID użytkownika, który utworzył raport. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
name	string	Unikalna nazwa raportu. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
dashboardid	ID	ID pulpitu, na podstawie którego tworzony jest raport. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
period	integer	Okres, za który raport zostanie przygotowany. Możliwe wartości: 0 - *(domyślnie)* poprzedni dzień; 1 - poprzedni tydzień; 2 - poprzedni miesiąc; 3 - poprzedni rok.
cycle	integer	Harmonogram powtarzania okresu. Możliwe wartości: 0 - *(domyślnie)* codziennie; 1 - co tydzień; 2 - co miesiąc; 3 - co rok.
start_time	integer	Pora dnia, w sekundach, o której raport zostanie przygotowany do wysłania. Domyślnie: 0.
weekdays	integer	Dni tygodnia do wysyłania raportu. Możliwe wartości bitmapy: 1 - poniedziałek; 2 - wtorek; 4 - środa; 8 - czwartek; 16 - piątek; 32 - sobota; 64 - niedziela. To pole jest maską bitową; akceptowana jest dowolna suma możliwych wartości bitmapy (na przykład 21 dla poniedziałku, środy i piątku). Domyślnie: 0. Zachowanie właściwości: - *wymagane*, jeśli `cycle` jest ustawione na ”weekly”.
active_since	string	Data rozpoczęcia. Możliwe wartości: pusty ciąg - *(domyślnie)* nie określono (zapisywane jako 0); określona data w formacie YYYY-MM-DD (zapisywana jako znacznik czasu początku dnia (00:00:00)).

Właściwość	Typ	Opis
active_till	string	Data zakończenia. Możliwe wartości: pusty ciąg - *(domyślnie)* nie określono (zapisywane jako 0); określona data w formacie YYYY-MM-DD (zapisywana jako znacznik czasu końca dnia (23:59:59)).
subject	string	Temat wiadomości raportu.
message	string	Treść wiadomości raportu.
status	integer	Czy raport jest włączony, czy wyłączony. Możliwe wartości: 0 - Wyłączony; 1 - *(domyślnie)* Włączony.
description	text	Opis raportu.
state	integer	Stan raportu. Możliwe wartości: 0 - *(domyślnie)* raport nie został jeszcze przetworzony; 1 - raport został wygenerowany i pomyślnie wysłany do wszystkich odbiorców; 2 - generowanie raportu nie powiodło się; ”info” zawiera informacje o błędzie; 3 - raport został wygenerowany, ale wysyłka do części (lub wszystkich) odbiorców nie powiodła się; ”info” zawiera informacje o błędzie. Zachowanie właściwości: - *tylko do odczytu*
lastsent	timestamp	Znacznik czasu Unix ostatniego pomyślnie wysłanego raportu. Zachowanie właściwości: - *tylko do odczytu*
info	string	Opis błędu lub dodatkowe informacje. Zachowanie właściwości: - *tylko do odczytu*

Użytkownicy

Obiekt users ma następujące właściwości:

Właściwość	Typ	Opis
userid	ID	ID użytkownika, do którego ma zostać wysłany raport. Zachowanie właściwości: - *wymagane*
access_userid	ID	ID użytkownika, w imieniu którego raport zostanie wygenerowany. 0 - *(domyślnie)* Wygeneruj raport przez odbiorcę.
exclude	integer	Czy wykluczyć użytkownika z listy mailingowej. Możliwe wartości: 0 - *(domyślnie)* Uwzględnij; 1 - Wyklucz.

Grupy użytkowników

Obiekt grup użytkowników ma następujące właściwości:

Właściwość	Typ	Opis
usrgrpid	ID	ID grupy użytkowników, do której ma zostać wysłany raport. Zachowanie właściwości: - *wymagane*
access_userid	ID	ID użytkownika, w imieniu którego zostanie wygenerowany raport. 0 - *(domyślnie)* Wygeneruj raport przez odbiorcę.

report.create

Opis

`object report.create(object/array reports)`

Ta metoda umożliwia tworzenie nowych zaplanowanych raportów.

Note:
Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Zaplanowane raporty do utworzenia.

Oprócz standardowych właściwości zaplanowanego raportu, metoda akceptuje następujące parametry.

Parametr	Type	Opis
users	object/array	Użytkownicy, do których ma zostać wysłany raport. Zachowanie parametrów: - *wymagane*, jeśli `user_groups` nie jest ustawione
user_groups	object/array	Grupy użytkowników, do których ma zostać wysłany raport. Zachowanie parametrów: - *wymagane*, jeśli `users` nie jest ustawione

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory utworzonych zaplanowanych raportów we właściwości `reportids`. Kolejność zwróconych identyfikatorów odpowiada kolejności przekazanych zaplanowanych raportów.

Przykłady

Tworzenie zaplanowanego raportu

Utwórz raport tygodniowy, który będzie przygotowywany za poprzedni tydzień w każdy poniedziałek-piątek o 12:00 od 2021-04-01 do 2021-08-31.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "report.create",
    "params": {
        "userid": "1",
        "name": "Raport tygodniowy",
        "dashboardid": "1",
        "period": "1",
        "cycle": "1",
        "start_time": "43200",
        "weekdays": "31",
        "active_since": "2021-04-01",
        "active_till": "2021-08-31",
```

```
        "subject": "Raport tygodniowy",
        "message": "Tekst towarzyszący raportowi",
        "status": "1",
        "description": "Opis raportu",
        "users": [
            {
                "userid": "1",
                "access_userid": "1",
                "exclude": "0"
            },
            {
                "userid": "2",
                "access_userid": "0",
                "exclude": "1"
            }
        ],
        "user_groups": [
            {
                "usrgrpid": "7",
                "access_userid": "0"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "reportids": [
            "1"
        ]
    },
    "id": 1
}
```

Zobacz także

- Użytkownicy
- Grupy użytkowników

Źródło

CReport::create() w *ui/include/classes/api/services/CReport.php*.

report.delete

Opis

`object report.delete(array reportids)`

Ta metoda umożliwia usuwanie zaplanowanych raportów.

Note:
Ta metoda jest dostępna tylko dla użytkowników typu *Admin* i *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(array)` ID raportów okresowych do usunięcia.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory usuniętych zaplanowanych raportów we właściwości `reportids`.

Przykłady

Usuwanie wielu zaplanowanych raportów

Usuń dwa zaplanowane raporty.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "report.delete",
    "params": [
        "1",
        "2"
    ],
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "reportids": [
            "1",
            "2"
        ]
    },
    "id": 1
}
```

Źródło

CReport::delete() w *ui/include/classes/api/services/CReport.php*.

report.get

Opis

`integer/array report.get(object parameters)`

Ta metoda umożliwia pobieranie zaplanowanych raportów zgodnie z podanymi parametrami.

Note:
Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w Rolach użytkowników.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
reportids	ID/array	Zwraca tylko zaplanowane raporty o podanych identyfikatorach raportów.
expired	boolean	Jeśli ustawiono na `true`, zwraca tylko wygasłe zaplanowane raporty.
selectUsers	query	Zwraca właściwość `users` zawierającą użytkowników, do których skonfigurowano wysyłanie raportu.
selectUserGroups	query	Zwraca właściwość `user_groups` zawierającą grupy użytkowników, do których skonfigurowano wysyłanie raportu.
sortfield	string/array	Sortuje wynik według podanych właściwości. Możliwe wartości: `reportid`, `name`, `status`.
countOutput	boolean	Te parametry opisano w komentarzu referencyjnym.
excludeSearch	boolean	
filter	object	

Parametr	Typ	Opis
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli został użyty parametr `countOutput`.

Przykłady

Pobieranie danych raportu

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "report.get",
    "params": [
        "output": "extend",
        "selectUsers": "extend",
        "selectUserGroups": "extend",
        "reportids": ["1", "2"]
    ],
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "reportid": "1",
            "userid": "1",
            "name": "Weekly report",
            "dashboardid": "1",
            "period": "1",
            "cycle": "1",
            "start_time": "43200",
            "weekdays": "31",
            "active_since": "2021-04-01",
            "active_till": "2021-08-31",
            "subject": "Weekly report",
            "message": "Report accompanying text",
            "status": "1",
            "description": "Report description",
            "state": "1",
            "lastsent": "1613563219",
            "info": "",
            "users": [
                {
                    "userid": "1",
                    "access_userid": "1",
                    "exclude": "0"
                },
                {
```

```
                    "userid": "2",
                    "access_userid": "0",
                    "exclude": "1"
                }
            ],
            "user_groups": [
                {
                    "usrgrpid": "7",
                    "access_userid": "0"
                }
            ]
        },
        {
            "reportid": "2",
            "userid": "1",
            "name": "Monthly report",
            "dashboardid": "2",
            "period": "2",
            "cycle": "2",
            "start_time": "0",
            "weekdays": "0",
            "active_since": "2021-05-01",
            "active_till": "",
            "subject": "Monthly report",
            "message": "Report accompanying text",
            "status": "1",
            "description": "",
            "state": "0",
            "lastsent": "0",
            "info": "",
            "users": [
                {
                    "userid": "1",
                    "access_userid": "1",
                    "exclude": "0"
                }
            ],
            "user_groups": []
        }
    ],
    "id": 1
}
```


Zobacz także

- Użytkownicy
- Grupy użytkowników

Źródło

CReport::get() w *ui/include/classes/api/services/CReport.php*.

report.update

Opis

`object report.update(object/array reports)`

Ta metoda umożliwia aktualizację istniejących zaplanowanych raportów.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkowników typu *Admin* i *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Właściwości zaplanowanego raportu do zaktualizowania.

Właściwość `reportid` musi być zdefiniowana dla każdego zaplanowanego raportu, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko przekazane właściwości, wszystkie pozostałe pozostaną bez zmian.

Oprócz standardowych właściwości zaplanowanego raportu metoda akceptuje następujące parametry.

Parametr	Typ	Opis
users	object/array	Użytkownicy, którzy mają zastąpić bieżących użytkowników przypisanych do zaplanowanego raportu. Zachowanie parametru: - *wymagany*, jeśli `user_groups` nie jest ustawione
user_groups	object/array	Grupy użytkowników, które mają zastąpić bieżące grupy użytkowników przypisane do zaplanowanego raportu. Zachowanie parametru: - *wymagany*, jeśli `users` nie jest ustawione

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych zaplanowanych raportów we właściwości `reportids`.

Przykłady

Wyłączanie zaplanowanego raportu

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "report.update",
    "params": {
        "reportid": "1",
        "status": "0"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "reportids": [
            "1"
        ]
    },
    "id": 1
}
```

Zobacz także

- Użytkownicy
- Grupy użytkowników

Źródło

CReport::update() w *ui/include/classes/api/services/CReport.php*.

Reguła LLD

Ta klasa jest przeznaczona do pracy z regułami wykrywania niskiego poziomu.

Odwołania do obiektów:

- Reguła LLD

    - Nagłówek HTTP
    - Pole zapytania HTTP
- Filtr reguły LLD
    - Warunek filtra reguły LLD
- Ścieżka makra LLD
- Przetwarzanie wstępne reguły LLD
- Nadpisania reguły LLD
    - Filtr nadpisania reguły LLD
        * Warunek filtra nadpisania reguły LLD
    - Operacja nadpisania reguły LLD
        * Status operacji nadpisania reguły LLD
        * Wykrywanie operacji nadpisania reguły LLD
        * Okres operacji nadpisania reguły LLD
        * Historia operacji nadpisania reguły LLD
        * Trendy operacji nadpisania reguły LLD
        * Poziom ważności operacji nadpisania reguły LLD
        * Tag operacji nadpisania reguły LLD
        * Szablon operacji nadpisania reguły LLD
        * Inwentaryzacja operacji nadpisania reguły LLD

Dostępne metody:

- discoveryrule.create - utwórz nowe reguły LLD
- discoveryrule.delete - usuń reguły LLD
- discoveryrule.get - pobierz reguły LLD
- discoveryrule.update - zaktualizuj reguły LLD

Obiekt reguły LLD (Low Level Discovery)

Następujące obiekty są bezpośrednio powiązane z API `discoveryrule`.

Reguła LLD

Obiekt reguły wykrywania niskiego poziomu ma następujące właściwości.

Właściwość	Typ	Opis
itemid	ID	ID reguły LLD. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji
delay	string	Interwał aktualizacji reguły LLD. Akceptuje sekundy lub jednostkę czasu z sufiksem (np. 30s, 1m, 2h, 1d) oraz opcjonalnie jeden lub więcej niestandardowych interwałów, wszystkie oddzielone średnikami. Niestandardowe interwały mogą być kombinacją interwałów elastycznych i harmonogramowanych. Akceptuje makra użytkownika. Jeśli są używane, wartość musi być pojedynczym makrem. Wiele makr lub makra zmieszane z tekstem nie są obsługiwane. Interwały elastyczne mogą być zapisane jako dwa makra oddzielone ukośnikiem (np. `{$FLEX_INTERVAL}/{$FLEX_PERIOD}`). Przykład: `1h;wd1-5h9-18;{$Macro1}/1-7,00:00-24:00;0/6-7,12:00-24:00;{$Macr` Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”Zabbix agent” (0), ”Simple check” (3), ”Zabbix internal” (5), ”External check” (10), ”Database monitor” (11), ”IPMI agent” (12), ”SSH agent” (13), ”TELNET agent” (14), ”JMX agent” (16), ”HTTP agent” (19), ”SNMP agent” (20), ”Script” (21), ”Browser” (22), lub jeśli `type` jest ustawione na ”Zabbix agent (active)” (7) i `key_` nie zawiera ”mqtt.get”

Właściwość	Typ	Opis
hostid	ID	ID hosta, do którego należy reguła LLD. Zachowanie właściwości: - *stałe* - *wymagane* dla operacji tworzenia
flags	integer	Pochodzenie reguły wykrywania. Możliwe wartości: 1 - reguła wykrywania niskiego poziomu; 5 - reguła wykrywania niskiego poziomu przekonwertowana z prototypu. Zachowanie właściwości: - *tylko do odczytu*
interfaceid	ID	ID interfejsu hosta reguły LLD. Zachowanie właściwości: - *wymagane*, jeśli reguła LLD należy do hosta i `type` jest ustawione na ”Zabbix agent”, ”IPMI agent”, ”JMX agent” lub ”SNMP agent” - *obsługiwane*, jeśli reguła LLD należy do hosta i `type` jest ustawione na ”Simple check”, ”External check”, ”SSH agent”, ”TELNET agent” lub ”HTTP agent”
key_	string	Klucz reguły LLD. Zachowanie właściwości: - *wymagane* dla operacji tworzenia - *tylko do odczytu* dla obiektów dziedziczonych
name	string	Nazwa reguły LLD. Zachowanie właściwości: - *wymagane* dla operacji tworzenia - *tylko do odczytu* dla obiektów dziedziczonych
type	integer	Typ reguły LLD. Możliwe wartości: 0 - Zabbix agent; 2 - Zabbix trapper; 3 - Simple check; 5 - Zabbix internal; 7 - Zabbix agent (active); 10 - External check; 11 - Database monitor; 12 - IPMI agent; 13 - SSH agent; 14 - TELNET agent; 16 - JMX agent; 18 - pozycja zależna; 19 - HTTP agent; 20 - SNMP agent; 21 - Script; 22 - Browser; 23 - Zagnieżdżony. Ten typ jest dozwolony tylko wtedy, gdy nadrzędna reguła jest szablonem (zakłada się, że jest podłączony do prototypu hosta podczas wykrywania) lub wykrytym hostem (który ma regułę LLD w swoim korzeniu). Zachowanie właściwości: - *wymagane* dla operacji tworzenia - *tylko do odczytu* dla obiektów dziedziczonych

Właściwość	Typ	Opis
url	string	Ciąg URL. Obsługuje makra użytkownika, {HOST.IP}, {HOST.CONN}, {HOST.DNS}, {HOST.HOST}, {HOST.NAME}, {HOST.PORT}, {ITEM.ID}, {ITEM.KEY}. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych
allow_traps	integer	Pozwala wypełniać wartość podobnie jak w pozycji trapper. Możliwe wartości: 0 - *(domyślnie)* Nie zezwalaj na przyjmowanie danych przychodzących; 1 - Zezwalaj na przyjmowanie danych przychodzących. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent”
authtype	integer	Metoda uwierzytelniania. Możliwe wartości, jeśli `type` jest ustawione na ”SSH agent”: 0 - *(domyślnie)* hasło; 1 - klucz publiczny. Możliwe wartości, jeśli `type` jest ustawione na ”HTTP agent”: 0 - *(domyślnie)* brak; 1 - basic; 2 - NTLM; 3 - Kerberos; 4 - Digest. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”SSH agent” lub ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych (jeśli `type` jest ustawione na ”HTTP agent”)
description	string	Opis reguły LLD.
error	string	Tekst błędu, jeśli występują problemy z aktualizacją wartości reguły LLD. Zachowanie właściwości: - *tylko do odczytu*
follow_redirects	integer	Podążanie za przekierowaniami odpowiedzi podczas odpytywania danych. Możliwe wartości: 0 - Nie podążaj za przekierowaniami; 1 - *(domyślnie)* Podążaj za przekierowaniami. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych
headers	array	Tablica nagłówków, które zostaną wysłane podczas wykonywania żądania HTTP. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych
http_proxy	string	Ciąg połączenia proxy HTTP(S). Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych

Właściwość	Typ	Opis
ipmi_sensor	string	Czujnik IPMI. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”IPMI agent” i `key_` nie jest ustawione na ”ipmi.get” - *obsługiwane*, jeśli `type` jest ustawione na ”IPMI agent” - *tylko do odczytu* dla obiektów dziedziczonych
jmx_endpoint	string	Niestandardowy ciąg połączenia JMX agent. Domyślnie: service:jmx:rmi:///jndi/rmi://{HOST.CONN}:{HOST.PORT}/jmxrmi Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”JMX agent”
lifetime	string	Okres czasu, po którym pozycje, które nie są już wykrywane, zostaną usunięte. Akceptuje sekundy, jednostkę czasu z sufiksem lub makro użytkownika. Domyślnie: `7d`.
lifetime_type	integer	Scenariusz usuwania utraconych zasobów LLD. Możliwe wartości: 0 - *(domyślnie)* Usuń po osiągnięciu progu lifetime; 1 - Nie usuwaj; 2 - Usuń natychmiast.
enabled_lifetime	string	Okres czasu, po którym pozycje, które nie są już wykrywane, zostaną wyłączone. Akceptuje sekundy, jednostkę czasu z sufiksem lub makro użytkownika. Domyślnie: `0`.
enabled_lifetime_type	integer	Scenariusz wyłączania utraconych zasobów LLD. Możliwe wartości: 0 - Wyłącz po osiągnięciu progu lifetime; 1 - Nie wyłączaj; 2 - *(domyślnie)* Wyłącz natychmiast.
master_itemid	ID	ID pozycji nadrzędnej. Reguła wykrywania nie może być pozycją nadrzędną dla innej reguły wykrywania. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”Dependent item” - *tylko do odczytu* dla obiektów dziedziczonych
output_format	integer	Czy odpowiedź powinna zostać przekonwertowana do JSON. Możliwe wartości: 0 - *(domyślnie)* Przechowuj surowe dane; 1 - Konwertuj do JSON. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych

Właściwość	Typ	Opis
params	string	Dodatkowe parametry zależne od typu reguły LLD: - wykonywany skrypt dla reguł LLD SSH i Telnet; - zapytanie SQL dla reguł LLD monitora bazy danych; - formuła dla obliczanych reguł LLD; - skrypt dla reguł LLD typu script i browser. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”Database monitor”, ”SSH agent”, ”TELNET agent”, ”Script” lub ”Browser” - *tylko do odczytu* dla obiektów dziedziczonych (jeśli `type` jest ustawione na ”Script” lub ”Browser”)
parameters	object/array	Dodatkowe parametry, jeśli `type` jest ustawione na ”Script” lub ”Browser”. Tablica obiektów z właściwościami `name` i `value`, gdzie `name` musi być unikalne. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”Script” lub ”Browser” - *tylko do odczytu* dla obiektów dziedziczonych
password	string	Hasło do uwierzytelniania. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”JMX agent” i `username` jest ustawione - *obsługiwane*, jeśli `type` jest ustawione na ”Simple check”, ”Database monitor”, ”SSH agent”, ”TELNET agent” lub ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych (jeśli `type` jest ustawione na ”HTTP agent”)
post_type	integer	Typ treści danych POST przechowywanych we właściwości `posts`. Możliwe wartości: 0 - *(domyślnie)* Surowe dane; 2 - Dane JSON; 3 - Dane XML. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych
posts	string	Dane treści żądania HTTP(S). Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”HTTP agent” i `post_type` jest ustawione na ”JSON data” lub ”XML data” - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” i `post_type` jest ustawione na ”Raw data” - *tylko do odczytu* dla obiektów dziedziczonych
privatekey	string	Nazwa pliku klucza prywatnego. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”SSH agent” i `authtype` jest ustawione na ”public key”
publickey	string	Nazwa pliku klucza publicznego. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”SSH agent” i `authtype` jest ustawione na ”public key”
query_fields	array	Tablica pól zapytania, które zostaną wysłane podczas wykonywania żądania HTTP. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych

Właściwość	Typ	Opis
request_method	integer	Typ metody żądania. Możliwe wartości: 0 - *(domyślnie)* GET; 1 - POST; 2 - PUT; 3 - HEAD. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych
retrieve_mode	integer	Która część odpowiedzi powinna zostać zapisana. Możliwe wartości, jeśli `request_method` jest ustawione na ”GET”, ”POST” lub ”PUT”: 0 - *(domyślnie)* Treść; 1 - Nagłówki; 2 - Zostaną zapisane zarówno treść, jak i nagłówki. Możliwe wartości, jeśli `request_method` jest ustawione na ”HEAD”: 1 - Nagłówki. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych
snmp_oid	string	OID SNMP. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”SNMP agent” - *tylko do odczytu* dla obiektów dziedziczonych
ssl_cert_file	string	Ścieżka do pliku publicznego klucza SSL. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych
ssl_key_file	string	Ścieżka do pliku prywatnego klucza SSL. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych
ssl_key_password	string	Hasło do pliku klucza SSL. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych
state	integer	Stan reguły LLD. Możliwe wartości: 0 - *(domyślnie)* normalny; 1 - nieobsługiwane. Zachowanie właściwości: - *tylko do odczytu*
status	integer	Status reguły LLD. Możliwe wartości: 0 - *(domyślnie)* włączona reguła LLD; 1 - wyłączona reguła LLD.

Właściwość	Typ	Opis
status_codes	string	Zakresy wymaganych kodów statusu HTTP, oddzielone przecinkami. Obsługuje również makra użytkownika jako część listy rozdzielanej przecinkami. Przykład: 200,200-{$M},{$M},200-400 Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych
templateid	ID	ID nadrzędnej reguły LLD szablonu. Zachowanie właściwości: - *tylko do odczytu*
timeout	string	Limit czasu żądania odpytywania danych pozycji. Akceptuje sekundy lub jednostkę czasu z sufiksem (np. 30s, 1m). Akceptuje również makra użytkownika. Zakres możliwych wartości: 1-600s. Domyślnie: ”” - użyj ustawień proxy/globalnych. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”Zabbix agent” (0), ”Simple check” (3) i `key_` nie zaczyna się od ”`vmware.`” ani ”`icmpping`”, ”Zabbix agent (active)” (7), ”External check” (10), ”Database monitor” (11), ”SSH agent” (13), ”TELNET agent” (14), ”HTTP agent” (19), ”SNMP agent” (20) i `snmp_oid` zaczyna się od ”`walk[`” lub ”`get[`”, ”Script” (21), ”Browser” (22) - *tylko do odczytu* dla obiektów dziedziczonych
trapper_hosts	string	Dozwolone hosty. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”Zabbix trapper”, lub jeśli `type` jest ustawione na ”HTTP agent” i `allow_traps` jest ustawione na ”Allow to accept incoming data”
username	string	Nazwa użytkownika do uwierzytelniania. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”SSH agent”, ”TELNET agent”, lub jeśli `type` jest ustawione na ”JMX agent” i `password` jest ustawione - *obsługiwane*, jeśli `type` jest ustawione na ”Simple check”, ”Database monitor” lub ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych (jeśli `type` jest ustawione na ”HTTP agent”)
uuid	string	Uniwersalny unikalny identyfikator, używany do łączenia importowanych reguł LLD z już istniejącymi. Generowany automatycznie, jeśli nie został podany. Zachowanie właściwości: - *obsługiwane*, jeśli reguła LLD należy do szablonu
verify_host	integer	Czy weryfikować, że nazwa hosta dla połączenia odpowiada nazwie w certyfikacie hosta. Możliwe wartości: 0 - *(domyślnie)* Nie weryfikuj; 1 - Weryfikuj. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych

Właściwość	Typ	Opis
verify_peer	integer	Czy weryfikować, że certyfikat hosta jest autentyczny. Możliwe wartości: 0 - *(domyślnie)* Nie weryfikuj; 1 - Weryfikuj. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”HTTP agent” - *tylko do odczytu* dla obiektów dziedziczonych

Nagłówek HTTP

Obiekt nagłówka ma następujące właściwości:

Właściwość	Typ	Opis
name	string	Nazwa nagłówka HTTP. Zachowanie właściwości: - *wymagane*
value	string	Wartość nagłówka. Zachowanie właściwości: - *wymagane*

Pole zapytania HTTP

Obiekt pola zapytania definiuje nazwę i wartość używane do określenia parametru URL. Ma następujące właściwości:

Właściwość	Typ	Opis
name	string	Nazwa parametru. Zachowanie właściwości: - *wymagane*
value	string	Wartość parametru. Zachowanie właściwości: - *wymagane*

Filtr reguły LLD

Obiekt filtra reguły LLD definiuje zestaw warunków, które mogą być używane do filtrowania wykrytych obiektów. Ma następujące właściwości:

Właściwość	Typ	Opis
conditions	object/array	Zestaw warunków filtra używanych do filtrowania wyników. Warunki zostaną posortowane zgodnie z kolejnością ich występowania w formule. Zachowanie właściwości: - *wymagane*

Właściwość	Typ	Opis
evaltype	integer	Metoda oceny warunków filtra. Możliwe wartości: 0 - And/Or; 1 - And; 2 - Or; 3 - Wyrażenie niestandardowe. Zachowanie właściwości: - *wymagane*
eval_formula	string	Wygenerowane wyrażenie, które będzie używane do oceny warunków filtra. Wyrażenie zawiera identyfikatory odnoszące się do określonych warunków filtra przez ich `formulaid`. Wartość `eval_formula` jest równa wartości `formula` dla filtrów z wyrażeniem niestandardowym. Zachowanie właściwości: - *tylko do odczytu*
formula	string	Wyrażenie zdefiniowane przez użytkownika, używane do oceny warunków filtrów z wyrażeniem niestandardowym. Wyrażenie musi zawierać identyfikatory odnoszące się do określonych warunków filtra przez ich `formulaid`. Identyfikatory użyte w wyrażeniu muszą dokładnie odpowiadać tym zdefiniowanym w warunkach filtra: żaden warunek nie może pozostać nieużyty ani pominięty. Zachowanie właściwości: - *wymagane*, jeśli `evaltype` jest ustawione na „custom expression”

Warunek filtra reguły LLD

Obiekt warunku filtra reguły LLD definiuje oddzielne sprawdzenie wykonywane na wartości makra LLD. Ma następujące właściwości:

Właściwość	Type	Opis
macro	string	Makro LLD, na którym ma zostać wykonane sprawdzenie. Property behavior: - *required*
value	string	Wartość do porównania. Property behavior: - *required* jeśli `operator` jest ustawiony na „matches regular expression” lub „does not match regular expression”
formulaid	string	Dowolny unikalny identyfikator używany do odwoływania się do warunku z niestandardowego wyrażenia. Może zawierać wyłącznie wielkie litery. Identyfikator musi zostać zdefiniowany przez użytkownika podczas modyfikowania warunków filtra, ale zostanie wygenerowany ponownie przy późniejszym ich pobieraniu. Property behavior: - *required* jeśli `evaltype` obiektu LLD rule filter object jest ustawiony na „custom expression”
operator	integer	Operator warunku. Możliwe wartości: 8 - *(domyślnie)* pasuje do wyrażenia regularnego; 9 - nie pasuje do wyrażenia regularnego; 12 - istnieje; 13 - nie istnieje.

Note:
Aby lepiej zrozumieć, jak używać filtrów z różnymi typami wyrażeń, zobacz przykłady na stronach metod discoveryrule.get i discoveryrule.create.

Ścieżka makra LLD

Ścieżka makra LLD ma następujące właściwości:

Właściwość	Type	Opis
lld_macro	string	Makro LLD. Zachowanie właściwości: - *wymagane*
path	string	Selektor wartości, która zostanie przypisana do odpowiadającego jej makra. Zachowanie właściwości: - *wymagane*

Wstępne przetwarzanie reguły LLD

Obiekt wstępnego przetwarzania reguły LLD ma następujące właściwości.

Właściwość	Typ	Opis
type	integer	Typ opcji wstępnego przetwarzania. Możliwe wartości: 5 - Wyrażenie regularne; 11 - XML XPath; 12 - JSONPath; 14 - Pasuje do wyrażenia regularnego; 15 - Nie pasuje do wyrażenia regularnego; 16 - Sprawdź błąd w JSON; 17 - Sprawdź błąd w XML; 20 - Odrzuć niezmienione z heartbeat; 21 - JavaScript; 23 - Prometheus do JSON; 24 - CSV do JSON; 25 - Zamień; 27 - XML do JSON; 28 - Wartość SNMP walk; 29 - SNMP walk do JSON; 30 - Wartość SNMP get. Zachowanie właściwości: - *wymagane*
params	string	Dodatkowe parametry używane przez opcję wstępnego przetwarzania. Wiele parametrów jest rozdzielanych znakiem nowej linii (\n). Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”Wyrażenie regularne” (5), ”XML XPath” (11), ”JSONPath” (12), ”Pasuje do wyrażenia regularnego” (14), ”Nie pasuje do wyrażenia regularnego” (15), ”Sprawdź błąd w JSON” (16), ”Sprawdź błąd w XML” (17), ”Odrzuć niezmienione z heartbeat” (20), ”JavaScript” (21), ”Prometheus do JSON” (23), ”CSV do JSON” (24), ”Zamień” (25), ”Wartość SNMP walk” (28), ”SNMP walk do JSON” (29) lub ”Wartość SNMP get” (30)

Właściwość	Typ	Opis
error_handler	integer	Typ akcji używany w przypadku niepowodzenia kroku wstępnego przetwarzania. Możliwe wartości: 0 - Komunikat o błędzie jest ustawiany przez Zabbix server; 1 - Odrzuć wartość; 2 - Ustaw własną wartość; 3 - Ustaw własny komunikat o błędzie. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”Wyrażenie regularne” (5), ”XML XPath” (11), ”JSONPath” (12), ”Pasuje do wyrażenia regularnego” (14), ”Nie pasuje do wyrażenia regularnego” (15), ”Sprawdź błąd w JSON” (16), ”Sprawdź błąd w XML” (17), ”Prometheus do JSON” (23), ”CSV do JSON” (24), ”XML do JSON” (27), ”Wartość SNMP walk” (28), ”SNMP walk do JSON” (29) lub ”Wartość SNMP get” (30)
error_handler_params	string	Parametry obsługi błędów. Zachowanie właściwości: - *wymagane*, jeśli `error_handler` jest ustawione na ”Ustaw własną wartość” lub ”Ustaw własny komunikat o błędzie”

Dla każdego typu wstępnego przetwarzania obsługiwane są następujące parametry i mechanizmy obsługi błędów.

Typ wstępnego przetwarzania	Nazwa	Parametr 1	Parametr 2	Parametr 3	Obsługiwane mechanizmy obsługi błędów
5	Wyrażenie regularne	wzorzec[1]	wynik[2]		0, 1, 2, 3
11	XML XPath	ścieżka[3]			0, 1, 2, 3
12	JSONPath	ścieżka[3]			0, 1, 2, 3
14	Pasuje do wyrażenia regularnego	wzorzec[1]			0, 1, 2, 3
15	Nie pasuje do wyrażenia regularnego	wzorzec[1]			0, 1, 2, 3
16	Sprawdź błąd w JSON	ścieżka[3]			0, 1, 2, 3
17	Sprawdź błąd w XML	ścieżka[3]			0, 1, 2, 3
20	Odrzuć niezmienione z heartbeat	sekundy[4, 5]			
21	JavaScript	skrypt[2]			

Typ wstępnego przetwarzania	Nazwa	Parametr 1	Parametr 2	Parametr 3	Obsługiwane mechanizmy obsługi błędów
23	Prometheus do JSON	wzorzec[5, 6]			0, 1, 2, 3
24	CSV do JSON	znak[2]	znak[2]	0,1	0, 1, 2, 3
25	Zamień	szukany ciąg[2]	zamiennik[2]		
27	XML do JSON				0, 1, 2, 3
28	Wartość SNMP walk	OID[2]	Format: 0 - Bez zmian 1 - UTF-8 z Hex-STRING 2 - MAC z Hex-STRING 3 - Integer z BITS		0, 1, 2, 3
29	SNMP walk do JSON[7]	Nazwa pola[2]	Prefiks OID[2]	Format: 0 - Bez zmian 1 - UTF-8 z Hex-STRING 2 - MAC z Hex-STRING 3 - Integer z BITS	0, 1, 2, 3
30	Wartość SNMP get	Format: 1 - UTF-8 z Hex-STRING 2 - MAC z Hex-STRING 3 - Integer z BITS			0, 1, 2, 3

[1] wyrażenie regularne
[2] ciąg znaków
[3] JSONPath lub XML XPath
[4] dodatnia liczba całkowita (z obsługą sufiksów czasu, np. 30s, 1m, 2h, 1d)
[5] makro użytkownika
[6] Wzorzec Prometheus zgodny ze składnią: `<metric name>{<label name>="<label value>", ...} == <value>`. Każdy składnik wzorca Prometheus (metryka, nazwa etykiety, wartość etykiety i wartość metryki) może być makrem użytkownika.
[7] Obsługuje wiele rekordów ”Nazwa pola,Prefiks OID,Format”, rozdzielonych znakiem nowej linii.

Nadpisania reguł LLD

Obiekt nadpisań reguł LLD definiuje zestaw reguł (filtrów, warunków i operacji), które są używane do nadpisywania właściwości różnych obiektów prototypów. Ma następujące właściwości:

Właściwość	Type	Opis
name	string	Unikalna nazwa nadpisania. Zachowanie właściwości: - *wymagane*
step	integer	Unikalny numer kolejności nadpisania. Zachowanie właściwości: - *wymagane*

Właściwość	Type	Opis
stop	integer	Zatrzymaj przetwarzanie kolejnych nadpisań, jeśli wystąpi dopasowanie. Możliwe wartości: 0 - *(domyślnie)* nie zatrzymuj przetwarzania nadpisań; 1 - zatrzymaj przetwarzanie nadpisań, jeśli filtr pasuje.
filter	object	Filtr nadpisania.
operations	object/array	Operacje nadpisania.

Filtr nadpisania reguły LLD

Obiekt filtra nadpisania reguły LLD definiuje zestaw warunków, które po dopasowaniu do wykrytego obiektu powodują zastosowanie nadpisania. Ma następujące właściwości:

Właściwość	Typ	Opis
conditions	object/array	Zestaw warunków filtra nadpisania używanych do dopasowywania wykrytych obiektów. Warunki zostaną posortowane zgodnie z kolejnością ich umieszczenia w formule. Zachowanie właściwości: - *wymagane*
evaltype	integer	Metoda oceny warunków filtra nadpisania. Możliwe wartości: 0 - And/Or; 1 - And; 2 - Or; 3 - Wyrażenie niestandardowe. Zachowanie właściwości: - *wymagane*
eval_formula	string	Wygenerowane wyrażenie, które będzie używane do oceny warunków filtra nadpisania. Wyrażenie zawiera identyfikatory odwołujące się do określonych warunków filtra nadpisania za pomocą ich `formulaid`. Wartość `eval_formula` jest równa wartości `formula` dla filtrów z wyrażeniem niestandardowym. Zachowanie właściwości: - *tylko do odczytu*
formula	string	Wyrażenie zdefiniowane przez użytkownika, używane do oceny warunków filtrów nadpisania z wyrażeniem niestandardowym. Wyrażenie musi zawierać identyfikatory odwołujące się do określonych warunków filtra nadpisania za pomocą ich `formulaid`. Identyfikatory użyte w wyrażeniu muszą dokładnie odpowiadać tym zdefiniowanym w warunkach filtra nadpisania: żaden warunek nie może pozostać nieużyty ani pominięty. Zachowanie właściwości: - *wymagane*, jeśli `evaltype` jest ustawione na „wyrażenie niestandardowe”

Warunek filtra nadpisania reguły LLD

Obiekt warunku filtra nadpisania reguły LLD definiuje oddzielne sprawdzenie wykonywane na wartości makra LLD. Ma następujące właściwości:

Właściwość	Type	Opis
macro	string	Makro LLD, dla którego ma zostać wykonane sprawdzenie. Zachowanie właściwości: - *wymagane*
value	string	Wartość do porównania. Zachowanie właściwości: - *wymagane*, jeśli `operator` jest ustawiony na „pasuje do wyrażenia regularnego” lub „nie pasuje do wyrażenia regularnego”
formulaid	string	Dowolny unikalny identyfikator używany do odwoływania się do warunku z niestandardowego wyrażenia. Może zawierać wyłącznie wielkie litery. Identyfikator musi zostać zdefiniowany przez użytkownika podczas modyfikowania warunków filtra, ale zostanie wygenerowany ponownie przy późniejszym żądaniu tych warunków. Zachowanie właściwości: - *wymagane*, jeśli `evaltype` obiektu filtra nadpisania reguły LLD jest ustawiony na „wyrażenie niestandardowe”
operator	integer	Operator warunku. Możliwe wartości: 8 - *(domyślnie)* pasuje do wyrażenia regularnego; 9 - nie pasuje do wyrażenia regularnego; 12 - istnieje; 13 - nie istnieje.

Operacja nadpisania reguły LLD

Operacja nadpisania reguły LLD to połączenie warunków i działań wykonywanych na obiekcie prototypu. Ma następujące właściwości:

Właściwość	Type	Opis
operationobject	integer	Typ wykrytego obiektu, dla którego ma zostać wykonane działanie. Możliwe wartości: 0 - Prototyp pozycji; 1 - Prototyp wyzwalacza; 2 - Prototyp wykresu; 3 - Prototyp hosta; 4 - Prototyp wykrywania. Zachowanie właściwości: - *wymagane*
operator	integer	Operator warunku nadpisania. Możliwe wartości: 0 - *(domyślnie)* równa się; 1 - nie równa się; 2 - zawiera; 3 - nie zawiera; 8 - pasuje; 9 - nie pasuje.
value	string	Wzorzec do dopasowania do nazwy prototypu pozycji, wyzwalacza, wykresu lub hosta, zależnie od wybranego obiektu.
opstatus	object	Obiekt statusu operacji nadpisania dla obiektów prototypu pozycji, wyzwalacza i hosta.
opdiscover	object	Obiekt statusu wykrywania operacji nadpisania (wszystkie typy obiektów).
opperiod	object	Obiekt okresu operacji nadpisania (interwału aktualizacji) dla obiektu prototypu pozycji.
ophistory	object	Obiekt historii operacji nadpisania dla obiektu prototypu pozycji.

Właściwość	Type	Opis
optrends	object	Obiekt trendów operacji nadpisania dla obiektu prototypu pozycji.
opseverity	object	Obiekt ważności operacji nadpisania dla obiektu prototypu wyzwalacza.
optag	object/array	Obiekt tagu operacji nadpisania dla obiektów prototypu wyzwalacza i hosta.
optemplate	object/array	Obiekt szablonu operacji nadpisania dla obiektu prototypu hosta.
opinventory	object	Obiekt inwentaryzacji operacji nadpisania dla obiektu prototypu hosta.

Status operacji nadpisania reguły LLD

Status operacji nadpisania reguły LLD ustawiany dla wykrytego obiektu. Ma następujące właściwości:

Właściwość	Typ	Opis
status	integer	Nadpisuje status wybranego obiektu. Możliwe wartości: 0 - Utwórz włączony; 1 - Utwórz wyłączony. Zachowanie właściwości: - *wymagane*

Operacja nadpisania reguły LLD: discover

Status discover operacji nadpisania reguły LLD, który jest ustawiany dla wykrytego obiektu. Ma następujące właściwości:

Właściwość	Typ	Opis
discover	integer	Nadpisuje status discover dla wybranego obiektu. Możliwe wartości: 0 - Tak, kontynuuj wykrywanie obiektów; 1 - Nie, nowe obiekty nie będą wykrywane, a istniejące zostaną oznaczone jako utracone. Zachowanie właściwości: - *wymagane*

Okres operacji nadpisania reguły LLD

Okres operacji nadpisania reguły LLD jest wartością interwału aktualizacji ustawianą dla odkrytej pozycji. Ma następujące właściwości:

Właściwość	Type	Opis
delay	string	Nadpisuje interwał aktualizacji prototypu pozycji. Akceptuje sekundy lub jednostkę czasu z sufiksem (np. 30s, 1m, 2h, 1d) oraz opcjonalnie jeden lub więcej interwałów niestandardowych, wszystkie oddzielone średnikami. Interwały niestandardowe mogą stanowić mieszankę interwałów elastycznych i harmonogramowanych. Akceptuje makra użytkownika lub makra LLD. Jeśli są używane, wartość musi być pojedynczym makrem. Wiele makr lub makra zmieszane z tekstem nie są obsługiwane. Interwały elastyczne mogą być zapisane jako dwa makra oddzielone ukośnikiem (np. `{$FLEX_INTERVAL}/{$FLEX_PERIOD}`). Przykład: `1h;wd1-5h9-18;{$Macro1}/1-7,00:00-24:00;0/6-7,12:00-24:00;{$Macr` Zachowanie właściwości: *- required*

Historia operacji nadpisania reguły LLD

Wartość historii operacji nadpisania reguły LLD, która jest ustawiana dla wykrytej pozycji. Ma następujące właściwości:

Właściwość	Type	Opis
history	string	Nadpisuje historię prototypu pozycji, czyli jednostkę czasu określającą, jak długo dane historyczne powinny być przechowywane. Akceptuje również makro użytkownika i makro LLD. Zachowanie właściwości: *- wymagane*

Trendy operacji nadpisania reguły LLD

Wartość trendów operacji nadpisania reguły LLD, która jest ustawiana dla wykrytej pozycji. Ma następujące właściwości:

Właściwość	Type	Opis
trends	string	Nadpisuje trendy prototypu pozycji, czyli jednostkę czasu określającą, jak długo dane trendów mają być przechowywane. Akceptuje również makro użytkownika i makro LLD. Zachowanie właściwości: *- required*

Ważność operacji nadpisania reguły LLD

Wartość ważności operacji nadpisania reguły LLD, która jest ustawiana dla odkrytego wyzwalacza. Ma następujące właściwości:

Właściwość	Typ	Opis
severity	integer	Nadpisuje ważność prototypu wyzwalacza. Możliwe wartości: 0 - *(domyślnie)* niesklasyfikowany; 1 - informacja; 2 - ostrzeżenie; 3 - średni; 4 - wysoki; 5 - katastrofa. Zachowanie właściwości: - *wymagane*

Znacznik operacji nadpisania reguły LLD

Obiekt znacznika operacji nadpisania reguły LLD zawiera nazwę i wartość znacznika ustawiane dla wykrytego obiektu. Ma następujące właściwości:

Właściwość	Type	Opis
tag	string	Nowa nazwa znacznika. Zachowanie właściwości: - *wymagane*
value	string	Nowa wartość znacznika.

Szablon operacji przesłaniania reguły LLD

Obiekt szablonu operacji przesłaniania reguły LLD, który jest powiązany z wykrytym hostem. Ma następujące właściwości:

Właściwość	Type	Opis
templateid	ID	Przesłania szablon powiązanych szablonów prototypu hosta. Zachowanie właściwości: - *wymagane*

Wartość trybu inwentaryzacji operacji nadpisania reguły LLD

Wartość trybu inwentaryzacji operacji nadpisania reguły LLD, która jest ustawiana dla wykrytego hosta. Ma następujące właściwości:

Właściwość	Typ	Opis
inventory_mode	integer	Nadpisuje tryb inwentaryzacji prototypu hosta. Możliwe wartości: -1 - wyłączony; 0 - *(domyślnie)* ręczny; 1 - automatyczny. Zachowanie właściwości: - *wymagane*

discoveryrule.create

Opis

`object discoveryrule.create(object/array lldRules)`

Ta metoda umożliwia tworzenie nowych reguł LLD.

Note:
Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji znajduje się w sekcji Role użytkowników.

Parametry

`(object/array)` Reguły LLD do utworzenia.

Oprócz standardowych właściwości reguły LLD, metoda akceptuje następujące parametry.

Parametr	Type	Opis
filter	object	Filtr reguły LLD dla reguły LLD.
preprocessing	object/array	Opcje przetwarzania wstępnego reguły LLD.
lld_macro_paths	object/array	Opcje lld_macro_path reguły LLD.
overrides	object/array	Opcje nadpisań reguły LLD.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory utworzonych reguł LLD we właściwości `itemids`. Kolejność zwróconych identyfikatorów ID jest zgodna z kolejnością przekazanych reguł LLD.

Przykłady

Tworzenie reguły LLD

Utwórz regułę LLD agenta Zabbix, aby wykrywać zamontowane systemy plików. Wykryte pozycje będą aktualizowane co 30 sekund.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "discoveryrule.create",
    "params": {
        "name": "Mounted filesystem discovery",
        "key_": "vfs.fs.discovery",
        "hostid": "10197",
        "type": 0,
        "interfaceid": "112",
        "delay": "30s"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "27665"
        ]
    },
    "id": 1
}
```

Używanie filtra

Utwórz regułę LLD z zestawem warunków, według których będą filtrowane wyniki. Warunki zostaną zgrupowane przy użyciu operatora logicznego „and”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "discoveryrule.create",
    "params": {
        "name": "Filtered LLD rule",
```

```
        "key_": "lld",
        "hostid": "10116",
        "type": 0,
        "interfaceid": "13",
        "delay": "30s",
        "filter": {
            "evaltype": 1,
            "conditions": [
                {
                    "macro": "{#MACRO1}",
                    "value": "@regex1"
                },
                {
                    "macro": "{#MACRO2}",
                    "value": "@regex2",
                    "operator": "9"
                },
                {
                    "macro": "{#MACRO3}",
                    "value": "",
                    "operator": "12"
                },
                {
                    "macro": "{#MACRO4}",
                    "value": "",
                    "operator": "13"
                }
            ]
        }
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "27665"
        ]
    },
    "id": 1
}
```

Tworzenie reguły LLD ze ścieżkami makr

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "discoveryrule.create",
    "params": {
        "name": "Reguła LLD ze ścieżkami makr LLD",
        "key_": "lld",
        "hostid": "10116",
        "type": 0,
        "interfaceid": "13",
        "delay": "30s",
        "lld_macro_paths": [
            {
                "lld_macro": "{#MACRO1}",
                "path": "$.path.1"
            },
            {
```

```
                "lld_macro": "{#MACRO2}",
                "path": "$.path.2"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "27665"
        ]
    },
    "id": 1
}
```

Użycie niestandardowego filtra wyrażeń

Utwórz regułę LLD z filtrem, który będzie używać niestandardowego wyrażenia do oceny warunków. Reguła LLD ma wykrywać tylko obiekty, których wartość makra "{#MACRO1}" pasuje jednocześnie do obu wyrażeń regularnych "regex1" i "regex2", a wartość "{#MACRO2}" pasuje do "regex3" lub "regex4". Identyfikatory formuł "A", "B", "C" i "D" zostały wybrane arbitralnie.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "discoveryrule.create",
    "params": {
        "name": "Filtered LLD rule",
        "key_": "lld",
        "hostid": "10116",
        "type": 0,
        "interfaceid": "13",
        "delay": "30s",
        "filter": {
            "evaltype": 3,
            "formula": "(A and B) and (C or D)",
            "conditions": [
                {
                    "macro": "{#MACRO1}",
                    "value": "@regex1",
                    "formulaid": "A"
                },
                {
                    "macro": "{#MACRO1}",
                    "value": "@regex2",
                    "formulaid": "B"
                },
                {
                    "macro": "{#MACRO2}",
                    "value": "@regex3",
                    "formulaid": "C"
                },
                {
                    "macro": "{#MACRO2}",
                    "value": "@regex4",
                    "formulaid": "D"
                }
            ]
        }
    },
```

```
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "27665"
        ]
    },
    "id": 1
}
```

Używanie niestandardowych pól zapytania i nagłówków

Utwórz regułę LLD z niestandardowymi polami zapytania i nagłówkami.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "discoveryrule.create",
    "params": {
        "hostid": "10257",
        "interfaceid": "5",
        "type": 19,
        "name": "API HTTP agent",
        "key_": "api_discovery_rule",
        "delay": "5s",
        "url": "http://127.0.0.1?discoverer.php",
        "query_fields": [
            {
                "name": "mode",
                "value": "json"
            },
            {
                "name": "elements",
                "value": "2"
            }
        ],
        "headers": [
            {
                "name": "X-Type",
                "value": "api"
            },
            {
                "name": "Authorization",
                "value": "Bearer mF_A.B5f-2.1JcM"
            }
        ],
        "allow_traps": 1,
        "trapper_hosts": "127.0.0.1"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "28336"
        ]
```

```
    },
    "id": 1
}
```

Tworzenie reguły LLD z preprocessingiem

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "discoveryrule.create",
    "params": {
        "name": "Reguła wykrywania z preprocessingiem",
        "key_": "lld.with.preprocessing",
        "hostid": "10001",
        "ruleid": "27665",
        "type": 0,
        "delay": "60s",
        "interfaceid": "1155",
        "preprocessing": [
            {
                "type": 20,
                "params": "20",
                "error_handler": 0,
                "error_handler_params": ""
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "44211"
        ]
    },
    "id": 1
}
```

Tworzenie reguły LLD z nadpisaniami

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "discoveryrule.create",
    "params": {
        "name": "Discover database host",
        "key_": "lld.with.overrides",
        "hostid": "10001",
        "type": 0,
        "delay": "60s",
        "interfaceid": "1155",
        "overrides": [
            {
                "name": "Discover MySQL host",
                "step": "1",
                "stop": "1",
                "filter": {
                    "evaltype": "2",
                    "conditions": [
                        {
```

```
                    "macro": "{#UNIT.NAME}",
                    "operator": "8",
                    "value": "^mysqld\\.service$"
                },
                {
                    "macro": "{#UNIT.NAME}",
                    "operator": "8",
                    "value": "^mariadb\\.service$"
                }
            ]
        },
        "operations": [
            {
                "operationobject": "3",
                "operator": "2",
                "value": "Database host",
                "opstatus": {
                    "status": "0"
                },
                "optemplate": [
                    {
                        "templateid": "10170"
                    }
                ],
                "optag": [
                    {
                        "tag": "database",
                        "value": "mysql"
                    }
                ]
            }
        ]
    },
    {
        "name": "Discover PostgreSQL host",
        "step": "2",
        "stop": "1",
        "filter": {
            "evaltype": "0",
            "conditions": [
                {
                    "macro": "{#UNIT.NAME}",
                    "operator": "8",
                    "value": "^postgresql\\.service$"
                }
            ]
        },
        "operations": [
            {
                "operationobject": "3",
                "operator": "2",
                "value": "Database host",
                "opstatus": {
                    "status": "0"
                },
                "optemplate": [
                    {
                        "templateid": "10263"
                    }
                ],
                "optag": [
                    {
```

```
                                "tag": "database",
                                "value": "postgresql"
                            }
                        ]
                    }
                ]
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "30980"
        ]
    },
    "id": 1
}
```

Utwórz regułę LLD skryptu

Utwórz proste zbieranie danych za pomocą reguły LLD skryptu.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "discoveryrule.create",
    "params": {
        "name": "Script example",
        "key_": "custom.script.lldrule",
        "hostid": "12345",
        "type": 21,
        "params": "var request = new HttpRequest();\nreturn request.post(\"https://postman-echo.com/post\"
        "parameters": [{
            "name": "host",
            "value": "{HOST.CONN}"
        }],
        "timeout": "6s",
        "delay": "30s"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "23865"
        ]
    },
    "id": 1
}
```

Utwórz regułę LLD z określonym okresem czasu wyłączania i bez usuwania

Utwórz regułę LLD z niestandardowym okresem czasu wyłączania encji po tym, jak nie jest już wykrywana, z ustawieniem, że nigdy nie zostanie usunięta.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "discoveryrule.create",
    "params": {
        "name": "lld disable after 1h",
        "key_": "lld.disable",
        "hostid": "10001",
        "type": 2,
        "lifetime_type": 1,
        "enabled_lifetime_type": 0,
        "enabled_lifetime": "1h"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "46864"
        ]
    },
    "id": 1
}
```

Zobacz także

- Filtr reguły LLD
- Ścieżki makr LLD
- Wstępne przetwarzanie reguły LLD

Źródło

CDiscoveryRule::create() w *ui/include/classes/api/services/CDiscoveryRule.php*.

discoveryrule.delete

Opis

`object discoveryrule.delete(array lldRuleIds)`

Ta metoda pozwala na usuwanie reguł LLD.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkowników typu *Admin* i *Super admin*. Uprawnienia do wywołania metody można odwołać w ustawieniach roli użytkownika. Więcej informacji można znaleźć w User roles.

Parametry

`(array)` Identyfikatory IDs reguł LLD do usunięcia.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory usuniętych reguł LLD we właściwości `ruleids`.

Przykłady

Usuwanie wielu reguł LLD

Usuń dwie reguły LLD.

Żądanie:

```
{
"jsonrpc": "2.0",
"method": "discoveryrule.delete",
"params": [
```

```
"27665",
"27668"
],
"id": 1
}
```

Odpowiedź:

```
{
"jsonrpc": "2.0",
"result": {
"ruleids": [
"27665",
"27668"
]
},
"id": 1
}
```

Źródło

CDiscoveryRule::delete() w *ui/include/classes/api/services/CDiscoveryRule.php*.

discoveryrule.get

Opis

`integer/array discoveryrule.get(object parameters)`

Ta metoda umożliwia pobranie reguł LLD zgodnie z podanymi parametrami.

Note:
Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji User roles.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
itemids	ID/array	Zwraca tylko reguły LLD o podanych identyfikatorach.
groupids	ID/array	Zwraca tylko reguły LLD należące do hostów z podanych grup.
hostids	ID/array	Zwraca tylko reguły LLD należące do podanych hostów.
inherited	boolean	Jeśli ustawiono `true`, zwraca tylko reguły LLD odziedziczone z szablonu.
interfaceids	ID/array	Zwraca tylko reguły LLD używające podanych interfejsów hosta.
monitored	boolean	Jeśli ustawiono `true`, zwraca tylko włączone reguły LLD należące do monitorowanych hostów.
templated	boolean	Jeśli ustawiono `true`, zwraca tylko reguły LLD należące do szablonów.
templateids	ID/array	Zwraca tylko reguły LLD należące do podanych szablonów.
selectDiscoveryData	query	Zwraca właściwość `discoveryData` z danymi obiektu wykrywania reguły LLD. Obiekt wykrywania reguły LLD łączy wykrytą regułę LLD z prototypem reguły LLD, z którego została wykryta.
selectDiscoveryRulePrototypes	query	Zwraca właściwość `discoveryRulePrototypes` z prototypami reguł LLD należącymi do reguły LLD. Obsługuje `count`.
selectFilter	query	Zwraca właściwość `filter` z danymi filtra używanego przez regułę LLD.
selectGraphs	query	Zwraca właściwość `graphs` z prototypami wykresów należącymi do reguły LLD. Obsługuje `count`.

Parametr	Typ	Opis
selectHostPrototypes	query	Zwraca właściwość `hostPrototypes` z prototypami hostów należącymi do reguły LLD. Obsługuje `count`.
selectHosts	query	Zwraca właściwość `hosts` z tablicą hostów, do których należy reguła LLD.
selectItems	query	Zwraca właściwość `items` z prototypami pozycji należącymi do reguły LLD. Obsługuje `count`.
selectTriggers	query	Zwraca właściwość `triggers` z prototypami wyzwalaczy należącymi do reguły LLD. Obsługuje `count`.
selectLLDMacroPaths	query	Zwraca właściwość `lld_macro_paths` z listą makr LLD i ścieżek do wartości przypisanych do każdego odpowiadającego makra.
selectPreprocessing	query	Zwraca właściwość `preprocessing` z opcjami przetwarzania wstępnego reguły LLD.
selectOverrides	query	Zwraca właściwość `lld_rule_overrides` z listą filtrów nadpisywania, warunków i operacji wykonywanych na obiektach prototypów.
filter	object	Zwraca tylko te wyniki, które dokładnie odpowiadają podanemu filtrowi. Akceptuje obiekt, w którym kluczami są nazwy właściwości, a wartościami są pojedyncza wartość lub tablica wartości do dopasowania. Nie obsługuje właściwości typu danych `text` data type. Obsługuje dodatkowe właściwości: `host` - nazwa techniczna hosta, do którego należy reguła LLD.
limitSelects	integer	Ogranicza liczbę rekordów zwracanych przez podzapytania. Dotyczy następujących podzapytań: `selectItems`, `selectGraphs`, `selectTriggers`.
sortfield	string/array	Sortuje wynik według podanych właściwości. Możliwe wartości: `itemid`, `name`, `key_`, `delay`, `type`, `status`.
countOutput	boolean	Te parametry opisano w komentarzu referencyjnym.
editable	boolean	
excludeSearch	boolean	
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów
- liczbę pobranych obiektów, jeśli został użyty parametr `countOutput`.

Przykłady

Pobieranie reguł wykrywania z hosta

Pobierz wszystkie reguły wykrywania dla określonego ID hosta.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "discoveryrule.get",
    "params": {
        "output": "extend",
        "hostids": "10202"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "itemid": "27425",
            "type": "0",
            "snmp_oid": "",
            "hostid": "10202",
            "name": "Wykrywanie interfejsów sieciowych",
            "key_": "net.if.discovery",
            "delay": "1h",
            "status": "0",
            "trapper_hosts": "",
            "templateid": "22444",
            "valuemapid": "0",
            "params": "",
            "ipmi_sensor": "",
            "authtype": "0",
            "username": "",
            "password": "",
            "publickey": "",
            "privatekey": "",
            "flags": "1",
            "interfaceid": "119",
            "description": "Wykrywanie interfejsów sieciowych zgodnie z definicją w globalnym wyrażeniu re
            "lifetime": "30d",
            "jmx_endpoint": "",
            "master_itemid": "0",
            "timeout": "",
            "url": "",
            "query_fields": [],
            "posts": "",
            "status_codes": "200",
            "follow_redirects": "1",
            "post_type": "0",
            "http_proxy": "",
            "headers": [],
            "retrieve_mode": "0",
            "request_method": "0",
            "output_format": "0",
            "ssl_cert_file": "",
            "ssl_key_file": "",
            "ssl_key_password": "",
            "verify_peer": "0",
            "verify_host": "0",
            "allow_traps": "0",
            "uuid": "",
            "lifetime_type": "0",
            "enabled_lifetime_type": "2",
            "enabled_lifetime": "0",
            "state": "0",
```

```
            "error": "",
            "parameters": []
        },
        {
            "itemid": "27426",
            "type": "0",
            "snmp_oid": "",
            "hostid": "10202",
            "name": "Wykrywanie zamontowanych systemów plików",
            "key_": "vfs.fs.discovery",
            "delay": "1h",
            "status": "0",
            "trapper_hosts": "",
            "templateid": "22450",
            "valuemapid": "0",
            "params": "",
            "ipmi_sensor": "",
            "authtype": "0",
            "username": "",
            "password": "",
            "publickey": "",
            "privatekey": "",
            "flags": "1",
            "interfaceid": "119",
            "description": "Wykrywanie systemów plików różnych typów zgodnie z definicją w globalnym wyraż
            "lifetime": "30d",
            "jmx_endpoint": "",
            "master_itemid": "0",
            "timeout": "",
            "url": "",
            "query_fields": [],
            "posts": "",
            "status_codes": "200",
            "follow_redirects": "1",
            "post_type": "0",
            "http_proxy": "",
            "headers": [],
            "retrieve_mode": "0",
            "request_method": "0",
            "output_format": "0",
            "ssl_cert_file": "",
            "ssl_key_file": "",
            "ssl_key_password": "",
            "verify_peer": "0",
            "verify_host": "0",
            "allow_traps": "0",
            "uuid": "",
            "lifetime_type": "0",
            "enabled_lifetime_type": "2",
            "enabled_lifetime": "0",
            "state": "0",
            "error": "",
            "parameters": []
        }
    ],
    "id": 1
}
```


Pobieranie warunków filtra

Pobierz nazwę reguły LLD „24681” oraz jej warunki filtra. Filtr używa typu obliczania „and”, więc właściwość `formula` jest pusta, a `eval_formula` jest generowana automatycznie.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "discoveryrule.get",
    "params": {
        "output": ["name"],
        "selectFilter": "extend",
        "itemids": ["24681"]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "itemid": "24681",
            "name": "Filtered LLD rule",
            "filter": {
                "evaltype": "1",
                "formula": "",
                "conditions": [
                    {
                        "macro": "{#MACRO1}",
                        "value": "@regex1",
                        "operator": "8",
                        "formulaid": "A"
                    },
                    {
                        "macro": "{#MACRO2}",
                        "value": "@regex2",
                        "operator": "9",
                        "formulaid": "B"
                    },
                    {
                        "macro": "{#MACRO3}",
                        "value": "",
                        "operator": "12",
                        "formulaid": "C"
                    },
                    {
                        "macro": "{#MACRO4}",
                        "value": "",
                        "operator": "13",
                        "formulaid": "D"
                    }
                ],
                "eval_formula": "A and B and C and D"
            }
        }
    ],
    "id": 1
}
```

Pobieranie reguły LLD według URL

Pobierz regułę LLD dla hosta na podstawie wartości pola URL reguły. Obsługiwane jest tylko dokładne dopasowanie ciągu URL zdefiniowanego dla reguły LLD.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "discoveryrule.get",
```

```
    "params": {
        "hostids": "10257",
        "filter": {
            "type": 19,
            "url": "http://127.0.0.1/discoverer.php"
        }
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "itemid": "28336",
            "type": "19",
            "snmp_oid": "",
            "hostid": "10257",
            "name": "API HTTP agent",
            "key_": "api_discovery_rule",
            "delay": "5s",
            "status": "0",
            "trapper_hosts": "",
            "templateid": "0",
            "valuemapid": "0",
            "params": "",
            "ipmi_sensor": "",
            "authtype": "0",
            "username": "",
            "password": "",
            "publickey": "",
            "privatekey": "",
            "flags": "1",
            "interfaceid": "5",
            "description": "",
            "lifetime": "30d",
            "jmx_endpoint": "",
            "master_itemid": "0",
            "timeout": "",
            "url": "http://127.0.0.1/discoverer.php",
            "query_fields": [
                {
                    "name": "mode",
                    "value": "json"
                },
                {
                    "name": "elements",
                    "value": "2"
                }
            ],
            "posts": "",
            "status_codes": "200",
            "follow_redirects": "1",
            "post_type": "0",
            "http_proxy": "",
            "headers": [
                {
                    "name" : "X-Type",
                    "value": "api"
                },
                {
```

```
                    "name": "Authorization",
                    "value": "Bearer mF_A.B5f-2.1JcM"
                }
            ],
            "retrieve_mode": "0",
            "request_method": "1",
            "output_format": "0",
            "ssl_cert_file": "",
            "ssl_key_file": "",
            "ssl_key_password": "",
            "verify_peer": "0",
            "verify_host": "0",
            "allow_traps": "0",
            "uuid": "",
            "lifetime_type": "0",
            "enabled_lifetime_type": "2",
            "enabled_lifetime": "0",
            "state": "0",
            "error": "",
            "parameters": []
        }
    ],
    "id": 1
}
```


Pobieranie reguły LLD z nadpisaniami

Pobierz jedną regułę LLD, która ma różne ustawienia nadpisywania.

Żądanie:


```
{
    "jsonrpc": "2.0",
    "method": "discoveryrule.get",
    "params": {
        "output": ["name"],
        "itemids": "30980",
        "selectOverrides": ["name", "step", "stop", "filter", "operations"]
    },
    "id": 1
}
```


Odpowiedź:


```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "name": "Discover database host",
            "overrides": [
                {
                    "name": "Discover MySQL host",
                    "step": "1",
                    "stop": "1",
                    "filter": {
                        "evaltype": "2",
                        "formula": "",
                        "conditions": [
                            {
                                "macro": "{#UNIT.NAME}",
                                "operator": "8",
                                "value": "^mysqld\\.service$",
                                "formulaid": "A"
                            },
                            {
```

```
                        "macro": "{#UNIT.NAME}",
                        "operator": "8",
                        "value": "^mariadb\\.service$",
                        "formulaid": "B"
                    }
                ],
                "eval_formula": "A or B"
            },
            "operations": [
                {
                    "operationobject": "3",
                    "operator": "2",
                    "value": "Database host",
                    "opstatus": {
                        "status": "0"
                    },
                    "optag": [
                        {
                            "tag": "database",
                            "value": "mysql"
                        }
                    ],
                    "optemplate": [
                        {
                            "templateid": "10170"
                        }
                    ]
                }
            ]
        },
        {
            "name": "Discover PostgreSQL host",
            "step": "2",
            "stop": "1",
            "filter": {
                "evaltype": "0",
                "formula": "",
                "conditions": [
                    {
                        "macro": "{#UNIT.NAME}",
                        "operator": "8",
                        "value": "^postgresql\\.service$",
                        "formulaid": "A"
                    }
                ],
                "eval_formula": "A"
            },
            "operations": [
                {
                    "operationobject": "3",
                    "operator": "2",
                    "value": "Database host",
                    "opstatus": {
                        "status": "0"
                    },
                    "optag": [
                        {
                            "tag": "database",
                            "value": "postgresql"
                        }
                    ],
                    "optemplate": [
```

```
                                {
                                    "templateid": "10263"
                                }
                            ]
                        }
                    ]
                }
            ]
        }
    ],
    "id": 1
}
```

Zobacz także

- Prototyp wykresu
- Host
- Prototyp pozycji
- Filtr reguły LLD
- Prototyp wyzwalacza

Źródło

CDiscoveryRule::get() w *ui/include/classes/api/services/CDiscoveryRule.php*.

discoveryrule.update

Opis

`object discoveryrule.update(object/array lldRules)`

Ta metoda umożliwia aktualizację istniejących reguł LLD.

Note:
Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w Rolach użytkowników.

Parametry

`(object/array)` Właściwości reguły LLD do zaktualizowania.

Właściwość `itemid` musi być zdefiniowana dla każdej reguły LLD, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko przekazane właściwości, wszystkie pozostałe pozostaną bez zmian.

Oprócz standardowych właściwości reguły LLD metoda akceptuje następujące parametry.

Parametr	Typ	Opis
filter	object	Filtr reguły LLD zastępujący istniejący filtr.
preprocessing	object/array	Opcje preprocessingu reguły LLD zastępujące istniejące opcje preprocessingu. Zachowanie parametru: - *tylko do odczytu* dla obiektów dziedziczonych
lld_macro_paths	object/array	Opcje lld_macro_path reguły LLD zastępujące istniejące opcje lld_macro_path. Zachowanie parametru: - *tylko do odczytu* dla obiektów dziedziczonych
overrides	object/array	Opcje nadpisań reguły LLD zastępujące istniejące opcje nadpisań. Zachowanie parametru: - *tylko do odczytu* dla obiektów dziedziczonych

Zwracane wartości

(`object`) Zwraca obiekt zawierający identyfikatory zaktualizowanych reguł LLD we właściwości `itemids`.

Przykłady

Dodawanie filtra do reguły LLD

Dodaj filtr, aby zawartość makra *{#FSTYPE}* pasowała do wyrażenia regularnego *@File systems for discovery*.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "discoveryrule.update",
    "params": {
        "itemid": "22450",
        "filter": {
            "evaltype": 1,
            "conditions": [
                {
                    "macro": "{#FSTYPE}",
                    "value": "@File systems for discovery"
                }
            ]
        }
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "22450"
        ]
    },
    "id": 1
}
```

Dodawanie ścieżek makr LLD

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "discoveryrule.update",
    "params": {
        "itemid": "22450",
        "lld_macro_paths": [
            {
                "lld_macro": "{#MACRO1}",
                "path": "$.json.path"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "22450"
        ]
    },
```

```
    "id": 1
}
```

Wyłącz przechwytywanie

Wyłącz przechwytywanie LLD dla reguły wykrywania.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "discoveryrule.update",
    "params": {
        "itemid": "28336",
        "allow_traps": 0
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "28336"
        ]
    },
    "id": 1
}
```

Aktualizowanie opcji przetwarzania wstępnego reguły LLD

Zaktualizuj regułę LLD, używając reguły przetwarzania wstępnego „JSONPath”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "discoveryrule.update",
    "params": {
        "itemid": "44211",
        "preprocessing": [
            {
                "type": 12,
                "params": "$.path.to.json",
                "error_handler": 2,
                "error_handler_params": "5"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "44211"
        ]
    },
    "id": 1
}
```

Aktualizacja skryptu reguły LLD

Zaktualizuj skrypt reguły LLD innym skryptem i usuń zbędne parametry, które były używane przez poprzedni skrypt.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "discoveryrule.update",
    "params": {
        "itemid": "23865",
        "parameters": [],
        "script": "Zabbix.log(3, 'Log test');\nreturn 1;"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "23865"
        ]
    },
    "id": 1
}
```

Aktualizacja czasu życia reguły LLD

Zaktualizuj regułę LLD, aby wyłączyć encję, która nie jest już wykrywana, po 12 godzinach i usunąć ją po 7 dniach.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "discoveryrule.update",
    "params": {
        "itemid": "46864",
        "lifetime_type": 0,
        "lifetime": "7d",
        "enabled_lifetime_type": 0,
        "enabled_lifetime": "12h"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "46864"
        ]
    },
    "id": 1
}
```

Źródło

CDiscoveryRule::update() w *ui/include/classes/api/services/CDiscoveryRule.php*.

Reguła wykrywania

Ta klasa została zaprojektowana do pracy z regułami wykrywania sieci.

Note:
To API jest przeznaczone do pracy z regułami wykrywania sieci. W przypadku reguł wykrywania niskiego poziomu zobacz API reguł LLD.

Odwołania do obiektów:

- Reguła wykrywania

Dostępne metody:

- drule.create - utwórz nowe reguły wykrywania sieci
- drule.delete - usuń reguły wykrywania sieci
- drule.get - pobierz reguły wykrywania sieci
- drule.update - zaktualizuj reguły wykrywania sieci

Obiekt reguły odkrywania

Następujące obiekty są bezpośrednio powiązane z API `drule`.

Reguła wykrywania

Obiekt reguły wykrywania definiuje regułę wykrywania sieci. Ma on następujące właściwości.

Właściwość	Typ	Opis
druleid	ID	ID reguły wykrywania. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji
iprange	string	Jeden lub kilka zakresów IP do sprawdzenia, oddzielonych przecinkami. Więcej informacji o obsługiwanych formatach zakresów IP można znaleźć w sekcji konfiguracja wykrywania sieci. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
name	string	Nazwa reguły wykrywania. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
delay	string	Interwał wykonywania reguły wykrywania. Akceptuje sekundy lub jednostkę czasu z sufiksem (np. 30s, 1m, 2h, 1d) albo makro użytkownika. Domyślnie: 1h.
proxyid	ID	ID proxy używanego do wykrywania.
status	integer	Określa, czy reguła wykrywania jest włączona. Możliwe wartości: 0 - *(domyślnie)* włączona; 1 - wyłączona.
concurrency_max	integer	Maksymalna liczba równoczesnych kontroli na regułę wykrywania. Możliwe wartości: 0 - *(domyślnie)* nieograniczona liczba kontroli; 1 - jedna kontrola; 2-999 - niestandardowa liczba kontroli.
error	string	Tekst błędu, jeśli podczas wykonywania reguły wykrywania wystąpiły jakiekolwiek problemy. Zachowanie właściwości: - *tylko do odczytu*

drule.create

Opis

`object drule.create(object/array discoveryRules)`

Ta metoda umożliwia tworzenie nowych reguł wykrywania.

> **Note:**
> Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Reguły wykrywania do utworzenia.

Oprócz standardowych właściwości reguły wykrywania, metoda akceptuje następujące parametry.

Parametr	Typ	Opis
dchecks	array	Kontrole wykrywania do utworzenia dla reguły wykrywania. Zachowanie parametru: - *wymagany*

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory utworzonych reguł wykrywania we właściwości `druleids`. Kolejność zwróconych identyfikatorów odpowiada kolejności przekazanych reguł wykrywania.

Przykłady

Utwórz regułę wykrywania

Utwórz regułę wykrywania, aby znaleźć maszyny z uruchomionym agent Zabbix w sieci lokalnej. Reguła musi używać pojedynczego sprawdzenia agent Zabbix na porcie 10050.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "drule.create",
    "params": {
        "name": "Zabbix agent discovery",
        "iprange": "192.168.1.1-255",
        "concurrency_max": "10",
        "dchecks": [
            {
                "type": "9",
                "key_": "system.uname",
                "ports": "10050",
                "uniq": "0"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "druleids": [
            "6"
        ]
    },
```

```
    "id": 1
}
```

Zobacz także

- Kontrola wykrywania

Źródło

CDRule::create() w *ui/include/classes/api/services/CDRule.php*.

drule.delete

Opis

`object drule.delete(array discoveryRuleIds)`

Ta metoda pozwala na usuwanie reguł wykrywania.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkowników typu *Admin* i *Super admin*. Uprawnienia do wywołania metody można odwołać w ustawieniach roli użytkownika. Więcej informacji można znaleźć w User roles.

Parametry

`(array)` Identyfikatory ID reguł wykrywania do usunięcia.

Wartości zwracane

`(object)` Zwraca obiekt zawierający identyfikatory usuniętych reguł wykrywania w ramach właściwości `druleids`.

Przykłady

Usuń wiele reguł wykrywania

Usuń dwie reguły wykrywania.

Żądanie:

```
{
"jsonrpc": "2.0",
"method": "drule.delete",
"params": [
"4",
"6"
],
"id": 1
}
```

Odpowiedź:

```
{
"jsonrpc": "2.0",
"result": {
"druleids": [
"4",
"6"
]
},
"id": 1
}
```

Źródło

CDRule::delete() w *ui/include/classes/api/services/CDRule.php*.

drule.get

Opis

`integer/array drule.get(object parameters)`

Ta metoda umożliwia pobranie reguł wykrywania zgodnie z podanymi parametrami.

> **Note:**
> Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji znajduje się w sekcji User roles.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
dhostids	ID/array	Zwraca tylko reguły wykrywania, które utworzyły podane wykryte hosty.
druleids	ID/array	Zwraca tylko reguły wykrywania o podanych ID.
dserviceids	ID/array	Zwraca tylko reguły wykrywania, które utworzyły podane wykryte usługi.
selectDChecks	query	Zwraca właściwość `dchecks` z kontrolami wykrywania używanymi przez regułę wykrywania. Obsługuje `count`.
selectDHosts	query	Zwraca właściwość `dhosts` z wykrytymi hostami utworzonymi przez regułę wykrywania. Obsługuje `count`.
limitSelects	integer	Ogranicza liczbę rekordów zwracanych przez podzapytania. Ma zastosowanie do następujących podzapytań: `selectDChecks` - wyniki będą sortowane według `dcheckid`; `selectDHosts` - wyniki będą sortowane według `dhostsid`.
sortfield	string/array	Sortuje wynik według podanych właściwości. Możliwe wartości: `druleid`, `name`.
countOutput	boolean	Te parametry są opisane w komentarzu referencyjnym.
editable	boolean	
excludeSearch	boolean	
filter	object	
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli został użyty parametr `countOutput`.

Przykłady

Pobierz wszystkie reguły wykrywania

Pobierz wszystkie skonfigurowane reguły wykrywania oraz kontrole wykrywania, których używają.

Żądanie:

```
{
    "jsonrpc": "2.0",
```

```
    "method": "drule.get",
    "params": {
        "output": "extend",
        "selectDChecks": "extend"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "druleid": "2",
            "proxyid": "0",
            "name": "Local network",
            "iprange": "192.168.3.1-255",
            "delay": "5s",
            "status": "0",
            "concurrency_max": "0",
            "error": "",
            "dchecks": [
                {
                    "dcheckid": "7",
                    "druleid": "2",
                    "type": "3",
                    "key_": "",
                    "snmp_community": "",
                    "ports": "21",
                    "snmpv3_securityname": "",
                    "snmpv3_securitylevel": "0",
                    "snmpv3_authpassphrase": "",
                    "snmpv3_privpassphrase": "",
                    "uniq": "0",
                    "snmpv3_authprotocol": "0",
                    "snmpv3_privprotocol": "0",
                    "snmpv3_contextname": "",
                    "host_source": "1",
                    "name_source": "0",
                    "allow_redirect": "0"
                },
                {
                    "dcheckid": "8",
                    "druleid": "2",
                    "type": "4",
                    "key_": "",
                    "snmp_community": "",
                    "ports": "80",
                    "snmpv3_securityname": "",
                    "snmpv3_securitylevel": "0",
                    "snmpv3_authpassphrase": "",
                    "snmpv3_privpassphrase": "",
                    "uniq": "0",
                    "snmpv3_authprotocol": "0",
                    "snmpv3_privprotocol": "0",
                    "snmpv3_contextname": "",
                    "host_source": "1",
                    "name_source": "0",
                    "allow_redirect": "0"
                }
            ]
        },
```

```
        {
            "druleid": "6",
            "proxyid": "0",
            "name": "Zabbix agent discovery",
            "iprange": "192.168.1.1-255",
            "delay": "1h",
            "status": "0",
            "concurrency_max": "10",
            "error": "",
            "dchecks": [
                {
                    "dcheckid": "10",
                    "druleid": "6",
                    "type": "9",
                    "key_": "system.uname",
                    "snmp_community": "",
                    "ports": "10050",
                    "snmpv3_securityname": "",
                    "snmpv3_securitylevel": "0",
                    "snmpv3_authpassphrase": "",
                    "snmpv3_privpassphrase": "",
                    "uniq": "0",
                    "snmpv3_authprotocol": "0",
                    "snmpv3_privprotocol": "0",
                    "snmpv3_contextname": "",
                    "host_source": "2",
                    "name_source": "3",
                    "allow_redirect": "0"
                }
            ]
        }
    ],
    "id": 1
}
```


Zobacz także

- Wykryty host
- Sprawdzenie wykrywania

Źródło

CDRule::get() w *ui/include/classes/api/services/CDRule.php*.

drule.update

Opis

`object drule.update(object/array discoveryRules)`

Ta metoda umożliwia aktualizację istniejących reguł wykrywania.

> **Note:**
> Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji znajduje się w sekcji Role użytkowników.

Parametry

`(object/array)` Właściwości reguły wykrywania do zaktualizowania.

Właściwość `druleid` musi być zdefiniowana dla każdej reguły wykrywania, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko przekazane właściwości, wszystkie pozostałe pozostaną bez zmian.

Oprócz standardowych właściwości reguły wykrywania, metoda akceptuje następujące parametry.

Parametr	Type	Opis
dchecks	array	Kontrole wykrywania zastępujące istniejące kontrole.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych reguł wykrywania właściwości `druleids`.

Przykłady

Zmień zakres IP reguły wykrywania

Zmień zakres IP reguły wykrywania na „192.168.2.1-255”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "drule.update",
    "params": {
        "druleid": "6",
        "iprange": "192.168.2.1-255"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "druleids": [
            "6"
        ]
    },
    "id": 1
}
```

Zobacz także

- Kontrola wykrywania

Źródło

CDRule::update() w *ui/include/classes/api/services/CDRule.php*.

Rola

Ta klasa jest przeznaczona do pracy z rolami użytkowników.

Odwołania do obiektów:

- Role
- Role rules
  - UI element
  - Service
  - Service tag
  - Module
  - Action

Dostępne metody:

- role.create - utwórz nowe role użytkowników
- role.delete - usuń role użytkowników
- role.get - pobierz role użytkowników
- role.update - zaktualizuj role użytkowników

Obiekt roli

Następujące obiekty są bezpośrednio powiązane z API `role`.

Rola

Obiekt roli ma następujące właściwości:

Właściwość	Typ	Opis
roleid	ID	ID roli. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji
name	string	Nazwa roli. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
type	integer	Typ użytkownika. Możliwe wartości: 1 - *(domyślnie)* Użytkownik; 2 - Admin; 3 - Super admin. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
readonly	integer	Czy rola jest tylko do odczytu. Możliwe wartości: 0 - *(domyślnie)* Nie; 1 - Tak. Zachowanie właściwości: - *tylko do odczytu*

Reguły roli

Obiekt reguł roli ma następujące właściwości:

Właściwość	Type	Opis
ui	array	Tablica obiektów elementu UI.
ui.default_access	integer	Określa, czy dostęp do nowych elementów UI jest włączony. Możliwe wartości: 0 - Wyłączony; 1 - *(domyślnie)* Włączony.
services.read.mode	integer	Dostęp tylko do odczytu do usług. Możliwe wartości: 0 - Dostęp tylko do odczytu do usług określonych przez właściwość `services.read.list` lub dopasowanych przez właściwość `services.read.tag`; 1 - *(domyślnie)* Dostęp tylko do odczytu do wszystkich usług.
services.read.list	array	Tablica obiektów Service. Określone usługi, w tym usługi podrzędne, otrzymają dla roli użytkownika dostęp tylko do odczytu. Dostęp tylko do odczytu nie zastąpi dostępu do odczytu i zapisu do usług. Zachowanie właściwości: - *obsługiwane*, jeśli `services.read.mode` jest ustawione na "0"

Właściwość	Type	Opis
services.read.tag	object	Tablica obiektów Service tag. Usługi dopasowane przez tag, w tym usługi podrzędne, otrzymają dla roli użytkownika dostęp tylko do odczytu. Dostęp tylko do odczytu nie zastąpi dostępu do odczytu i zapisu do usług. Zachowanie właściwości: - *obsługiwane*, jeśli `services.read.mode` jest ustawione na "0"
services.write.mode	integer	Dostęp do odczytu i zapisu do usług. Możliwe wartości: 0 - *(domyślnie)* Dostęp do odczytu i zapisu do usług określonych przez właściwość `services.write.list` lub dopasowanych przez właściwość `services.write.tag`; 1 - Dostęp do odczytu i zapisu do wszystkich usług.
services.write.list	array	Tablica obiektów Service. Określone usługi, w tym usługi podrzędne, otrzymają dla roli użytkownika dostęp do odczytu i zapisu. Dostęp do odczytu i zapisu zastąpi dostęp tylko do odczytu do usług. Zachowanie właściwości: - *obsługiwane*, jeśli `services.write.mode` jest ustawione na "0"
services.write.tag	object	Tablica obiektów Service tag. Usługi dopasowane przez tag, w tym usługi podrzędne, otrzymają dla roli użytkownika dostęp do odczytu i zapisu. Dostęp do odczytu i zapisu zastąpi dostęp tylko do odczytu do usług. Zachowanie właściwości: - *obsługiwane*, jeśli `services.write.mode` jest ustawione na "0"
modules	array	Tablica obiektów modułu.
modules.default_access	integer	Określa, czy dostęp do nowych modułów jest włączony. Możliwe wartości: 0 - Wyłączony; 1 - *(domyślnie)* Włączony.
api.access	integer	Określa, czy dostęp do API jest włączony. Możliwe wartości: 0 - Wyłączony; 1 - *(domyślnie)* Włączony.
api.mode	integer	Tryb traktowania metod API wymienionych we właściwości `api`. Możliwe wartości: 0 - *(domyślnie)* Lista zabronionych; 1 - Lista dozwolonych.
api	array	Tablica metod API.
actions	array	Tablica obiektów akcji.
actions.default_access	integer	Określa, czy dostęp do nowych akcji jest włączony. Możliwe wartości: 0 - Wyłączony; 1 - *(domyślnie)* Włączony.

Element UI

Obiekt elementu UI ma następujące właściwości:

Właściwość	Typ	Opis
name	string	Nazwa elementu UI. Możliwe wartości, jeśli type obiektu Role jest ustawiony na ”User”, ”Admin” lub ”Super admin”: `monitoring.dashboard` - *Pulpity*; `monitoring.problems` - *Monitorowanie → Problemy*; `monitoring.hosts` - *Monitorowanie → Hosty*; `monitoring.latest_data` - *Monitorowanie → Najnowsze dane*; `monitoring.maps` - *Monitorowanie → Mapy*; `services.services` - *Usługi → Usługi*; `services.sla_report` - *Usługi → Raport SLA*; `inventory.overview` - *Inwentaryzacja → Przegląd*; `inventory.hosts` - *Inwentaryzacja → Hosty*; `reports.availability_report` - *Raporty → Raport dostępności*; `reports.top_triggers` - *Raporty → 100 najważniejszych wyzwalaczy*. Możliwe wartości, jeśli type obiektu Role jest ustawiony na ”Admin” lub ”Super admin”: `monitoring.discovery` - *Monitorowanie → Wykrywanie*; `services.sla` - *Usługi → SLA*; `reports.scheduled_reports` - *Raporty → Raporty cykliczne*; `reports.notifications` - *Raporty → Powiadomienia*; `configuration.template_groups` - *Zbieranie danych → Grupy szablonów*; `configuration.host_groups` - *Zbieranie danych → Grupy hostów*; `configuration.templates` - *Zbieranie danych → Szablony*; `configuration.hosts` - *Zbieranie danych → Hosty*; `configuration.maintenance` - *Zbieranie danych → Konserwacja*; `configuration.discovery` - *Zbieranie danych → Wykrywanie*; `configuration.trigger_actions` - *Alerty → Akcje → Akcje wyzwalaczy*; `configuration.service_actions` - *Alerty → Akcje → Akcje usług*; `configuration.discovery_actions` - *Alerty → Akcje → Akcje wykrywania*; `configuration.autoregistration_actions` - *Alerty → Akcje → Akcje autorejestracji*; `configuration.internal_actions` - *Alerty → Akcje → Akcje wewnętrzne*. Możliwe wartości, jeśli type obiektu Role jest ustawiony na ”Super admin”: `reports.system_info` - *Raporty → Informacje systemowe*; `reports.audit` - *Raporty → Dziennik audytu*; `reports.action_log` - *Raporty → Dziennik akcji*; `configuration.event_correlation` - *Zbieranie danych → Korelacja zdarzeń*; `administration.media_types` - *Alerty → Typy mediów*; `administration.scripts` - *Alerty → Skrypty*; `administration.user_groups` - *Użytkownicy → Grupy użytkowników*; `administration.user_roles` - *Użytkownicy → Role użytkowników*; `administration.users` - *Użytkownicy → Użytkownicy*; `administration.api_tokens` - *Użytkownicy → Tokeny API*; `administration.authentication` - *Użytkownicy → Uwierzytelnianie*; `administration.general` - *Administracja → Ogólne*; `administration.audit_log` - *Administracja → Dziennik audytu*; `administration.housekeeping` - *Administracja → Housekeeping*; `administration.proxy_groups` - *Administracja → Grupy proxy*; `administration.proxies` - *Administracja → Proxy*; `administration.macros` - *Administracja → Makra*; `administration.queue` - *Administracja → Kolejka*.

Zachowanie właściwości:

Właściwość	Typ	Opis
status	integer	Czy dostęp do elementu UI jest włączony. Możliwe wartości: 0 - Wyłączony; 1 - *(domyślnie)* Włączony.

Usługa

Właściwość	Type	Opis
serviceid	ID	ID usługi. Property behavior: - *wymagane*

Znacznik usługi

Właściwość	Type	Opis
tag	string	Nazwa znacznika. Jeśli zostanie podany pusty ciąg znaków, znacznik usługi nie będzie używany do dopasowywania usług. Zachowanie właściwości: - *wymagane*
value	string	Wartość znacznika. Jeśli nie zostanie podana żadna wartość lub zostanie podany pusty ciąg znaków, do dopasowywania usług będzie używana tylko nazwa znacznika.

Moduł

Obiekt modułu ma następujące właściwości:

Właściwość	Typ	Opis
moduleid	ID	ID modułu. Zachowanie właściwości: - *wymagane*
status	integer	Czy dostęp do modułu jest włączony. Możliwe wartości: 0 - Wyłączony; 1 - *(domyślnie)* Włączony.

Akcja

Obiekt akcji ma następujące właściwości:

Właściwość	Typ	Opis
name	string	Nazwa akcji. Możliwe wartości, jeśli `type` obiektu Role jest ustawione na ”User”, ”Admin” lub ”Super admin”: `edit_dashboards` - Tworzenie i edycja pulpitów; `edit_maps` - Tworzenie i edycja map; `add_problem_comments` - Dodawanie komentarzy do problemów; `change_severity` - Zmiana ważności problemu; `acknowledge_problems` - Potwierdzanie problemów; `suppress_problems` - Tłumienie problemów; `close_problems` - Zamykanie problemów; `execute_scripts` - Wykonywanie skryptów; `manage_api_tokens` - Zarządzanie tokenami API; `change_problem_ranking` - Zmiana klasyfikacji problemu z przyczyny na symptom i odwrotnie; `edit_own_media` - Zezwala na tworzenie/edycję własnych mediów. Możliwe wartości, jeśli `type` obiektu Role jest ustawione na ”Admin” lub ”Super admin”: `edit_maintenance` - Tworzenie i edycja okresów konserwacji; `manage_scheduled_reports` - Zarządzanie zaplanowanymi raportami, `manage_sla` - Zarządzanie SLA. Możliwe wartości, jeśli `type` obiektu Role jest ustawione na ”User” lub ”Admin”: `invoke_execute_now` - pozwala wykonywać kontrole pozycji użytkownikom, którzy mają tylko uprawnienia do odczytu na hoście. Możliwe wartości, jeśli `type` obiektu Role jest ustawione na ”Super admin”: `edit_user_media` - Zezwala na tworzenie/edycję mediów dla użytkowników. Zachowanie właściwości: - *wymagane*
status	integer	Czy dostęp do wykonania akcji jest włączony. Możliwe wartości: 0 - Wyłączone; 1 - *(domyślnie)* Włączone.

role.create

Opis

`object role.create(object/array roles)`

Ta metoda umożliwia tworzenie nowych ról.

Note:
Ta metoda jest dostępna tylko dla typu użytkownika *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Role do utworzenia.

Oprócz standardowych właściwości roli, metoda akceptuje następujące parametry.

Parametr	Type	Opis
rules	array	Reguły roli, które mają zostać utworzone dla roli.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory utworzonych ról we właściwości `roleids`. Kolejność zwróconych identyfikatorów odpowiada kolejności przekazanych ról.

Przykłady

Tworzenie roli

Utwórz rolę typu „Użytkownik” z zablokowanym dostępem do dwóch elementów interfejsu użytkownika.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "role.create",
    "params": {
        "name": "Operator",
        "type": "1",
        "rules": {
            "ui": [
                {
                    "name": "monitoring.hosts",
                    "status": "0"
                },
                {
                    "name": "monitoring.maps",
                    "status": "0"
                }
            ]
        }
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "roleids": [
            "5"
        ]
    },
    "id": 1
}
```

Zobacz także

- Reguły roli
- Element interfejsu użytkownika
- Moduł
- Akcja

Źródło

CRole::create() w *ui/include/classes/api/services/CRole.php*.

role.delete

Opis

`object role.delete(array roleids)`

Ta metoda pozwala usunąć role.

Note:
Ta metoda jest dostępna dla użytkownika typu *Super admin*. Uprawnienia mogą zostać cofnięte w konfiguracji roli użytkownika. Więcej informacji User roles.

Parametry

`(array)` ID ról do usunięcia.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory usuniętych ról we właściwości `roleids`.

Przykłady

Usunięcie wielu ról użytkownika

Usunięcie dwóch ról użytkownika.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "role.delete",
    "params": [
        "4",
        "5"
    ],
    "auth": "3a57200802b24cda67c4e4010b50c065",
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "roleids": [
            "4",
            "5"
        ]
    },
    "id": 1
}
```

Źródło

CRole::delete() w *ui/include/classes/api/services/CRole.php*.

role.get

Opis

`integer/array role.get(object parameters)`

Ta metoda umożliwia pobieranie ról zgodnie z podanymi parametrami.

Note:
Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
roleids	ID/array	Zwracaj tylko role o podanych identyfikatorach.

Parametr	Typ	Opis
selectRules	query	Zwracaj właściwość `rules` z regułami roli.
selectUsers	query	Zwracaj właściwość `users` z użytkownikami, do których przypisana jest rola. Ograniczenia zależne od typu użytkownika opisano w `user.get`.
sortfield	string/array	Sortuj wynik według podanych właściwości. Możliwe wartości: `roleid`, `name`.
countOutput	boolean	Te parametry opisano w komentarzu referencyjnym.
editable	boolean	
excludeSearch	boolean	
filter	object	
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli został użyty parametr `countOutput`.

Przykłady

Pobieranie danych roli

Pobierz dane roli „Super admin role” oraz jej reguły dostępu.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "role.get",
    "params": {
        "output": "extend",
        "selectRules": "extend",
        "roleids": "3"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "roleid": "3",
            "name": "Super admin role",
            "type": "3",
            "readonly": "1",
            "rules": {
                "ui": [
                    {
                        "name": "monitoring.dashboard",
                        "status": "1"
                    },
                    {
                        "name": "monitoring.problems",
```

```
            "status": "1"
        },
        {
            "name": "monitoring.hosts",
            "status": "1"
        },
        {
            "name": "monitoring.latest_data",
            "status": "1"
        },
        {
            "name": "monitoring.maps",
            "status": "1"
        },
        {
            "name": "services.services",
            "status": "1"
        },
        {
            "name": "services.sla_report",
            "status": "1"
        },
        {
            "name": "inventory.overview",
            "status": "1"
        },
        {
            "name": "inventory.hosts",
            "status": "1"
        },
        {
            "name": "reports.availability_report",
            "status": "1"
        },
        {
            "name": "reports.top_triggers",
            "status": "1"
        },
        {
            "name": "monitoring.discovery",
            "status": "1"
        },
        {
            "name": "services.sla",
            "status": "1"
        },
        {
            "name": "reports.scheduled_reports",
            "status": "1"
        },
        {
            "name": "reports.notifications",
            "status": "1"
        },
        {
            "name": "configuration.template_groups",
            "status": "1"
        },
        {
            "name": "configuration.host_groups",
            "status": "1"
        },
```

```
                {
                    "name": "configuration.templates",
                    "status": "1"
                },
                {
                    "name": "configuration.hosts",
                    "status": "1"
                },
                {
                    "name": "configuration.maintenance",
                    "status": "1"
                },
                {
                    "name": "configuration.discovery",
                    "status": "1"
                },
                {
                    "name": "configuration.trigger_actions",
                    "status": "1"
                },
                {
                    "name": "configuration.service_actions",
                    "status": "1"
                },
                {
                    "name": "configuration.discovery_actions",
                    "status": "1"
                },
                {
                    "name": "configuration.autoregistration_actions",
                    "status": "1"
                },
                {
                    "name": "configuration.internal_actions",
                    "status": "1"
                },
                {
                    "name": "reports.system_info",
                    "status": "1"
                },
                {
                    "name": "reports.audit",
                    "status": "1"
                },
                {
                    "name": "reports.action_log",
                    "status": "1"
                },
                {
                    "name": "configuration.event_correlation",
                    "status": "1"
                },
                {
                    "name": "administration.media_types",
                    "status": "1"
                },
                {
                    "name": "administration.scripts",
                    "status": "1"
                },
                {
                    "name": "administration.user_groups",
```

```
                "status": "1"
            },
            {
                "name": "administration.user_roles",
                "status": "1"
            },
            {
                "name": "administration.users",
                "status": "1"
            },
            {
                "name": "administration.api_tokens",
                "status": "1"
            },
            {
                "name": "administration.authentication",
                "status": "1"
            },
            {
                "name": "administration.general",
                "status": "1"
            },
            {
                "name": "administration.audit_log",
                "status": "1"
            },
            {
                "name": "administration.housekeeping",
                "status": "1"
            },
            {
                "name": "administration.proxy_groups",
                "status": "1"
            },
            {
                "name": "administration.proxies",
                "status": "1"
            },
            {
                "name": "administration.macros",
                "status": "1"
            },
            {
                "name": "administration.queue",
                "status": "1"
            }
        ],
        "ui.default_access": "1",
        "services.read.mode": "1",
        "services.read.list": [],
        "services.read.tag": {
            "tag": "",
            "value": ""
        },
        "services.write.mode": "1",
        "services.write.list": [],
        "services.write.tag": {
            "tag": "",
            "value": ""
        },
        "modules": [
            {
```

```
            "moduleid": 1,
            "status": "1"
        },
        {
            "moduleid": 2,
            "status": "1"
        },
        {
            "moduleid": 3,
            "status": "1"
        },
        {
            "moduleid": 4,
            "status": "1"
        },
        {
            "moduleid": 5,
            "status": "1"
        },
        {
            "moduleid": 6,
            "status": "1"
        },
        {
            "moduleid": 7,
            "status": "1"
        },
        {
            "moduleid": 8,
            "status": "1"
        },
        {
            "moduleid": 9,
            "status": "1"
        },
        {
            "moduleid": 10,
            "status": "1"
        },
        {
            "moduleid": 11,
            "status": "1"
        },
        {
            "moduleid": 12,
            "status": "1"
        },
        {
            "moduleid": 13,
            "status": "1"
        },
        {
            "moduleid": 14,
            "status": "1"
        },
        {
            "moduleid": 15,
            "status": "1"
        },
        {
            "moduleid": 16,
            "status": "1"
```

```
        },
        {
            "moduleid": 17,
            "status": "1"
        },
        {
            "moduleid": 18,
            "status": "1"
        },
        {
            "moduleid": 19,
            "status": "1"
        },
        {
            "moduleid": 20,
            "status": "1"
        },
        {
            "moduleid": 21,
            "status": "1"
        },
        {
            "moduleid": 22,
            "status": "1"
        },
        {
            "moduleid": 23,
            "status": "1"
        },
        {
            "moduleid": 24,
            "status": "1"
        },
        {
            "moduleid": 25,
            "status": "1"
        },
        {
            "moduleid": 26,
            "status": "1"
        },
        {
            "moduleid": 27,
            "status": "1"
        },
        {
            "moduleid": 28,
            "status": "1"
        },
        {
            "moduleid": 29,
            "status": "1"
        },
        {
            "moduleid": 30,
            "status": "1"
        },
        {
            "moduleid": 31,
            "status": "1"
        },
        {
```

```
                    "moduleid": 32,
                    "status": "1"
                },
                {
                    "moduleid": 33,
                    "status": "1"
                }
            ],
            "modules.default_access": "1",
            "api.access": "1",
            "api.mode": "0",
            "api": [],
            "actions": [
                {
                    "name": "edit_dashboards",
                    "status": "1"
                },
                {
                    "name": "edit_maps",
                    "status": "1"
                },
                {
                    "name": "acknowledge_problems",
                    "status": "1"
                },
                {
                    "name": "suppress_problems",
                    "status": "1"
                },
                {
                    "name": "close_problems",
                    "status": "1"
                },
                {
                    "name": "change_severity",
                    "status": "1"
                },
                {
                    "name": "add_problem_comments",
                    "status": "1"
                },
                {
                    "name": "execute_scripts",
                    "status": "1"
                },
                {
                    "name": "manage_api_tokens",
                    "status": "1"
                },
                {
                    "name": "edit_maintenance",
                    "status": "1"
                },
                {
                    "name": "manage_scheduled_reports",
                    "status": "1"
                },
                {
                    "name": "manage_sla",
                    "status": "1"
                },
                {
```

```
                        "name": "invoke_execute_now",
                        "status": "1"
                    },
                    {
                        "name": "change_problem_ranking",
                        "status": "1"
                    },
                    {
                        "name": "edit_own_media",
                        "status": "1"
                    },
                    {
                        "name": "edit_user_media",
                        "status": "1"
                    }
                ],
                "actions.default_access": "1"
            }
        }
    ],
    "id": 1
}
```


Zobacz także

- Reguły roli
- Użytkownik

Źródło

CRole::get() w *ui/include/classes/api/services/CRole.php*.

role.update

Opis

`object role.update(object/array roles)`

Ta metoda umożliwia aktualizację istniejących ról.

Note:
Ta metoda jest dostępna tylko dla typu użytkownika *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Zobacz Role użytkowników , aby uzyskać więcej informacji.

Parametry

`(object/array)` Właściwości roli do zaktualizowania.

Właściwość `roleid` musi być zdefiniowana dla każdej roli, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko przekazane właściwości, wszystkie pozostałe pozostaną bez zmian.

Oprócz standardowych właściwości roli metoda akceptuje następujące parametry.

Parametr	Type	Opis
rules	array	Reguły dostępu rules do zaktualizowania dla roli.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych ról we właściwości `roleids`.

Przykłady

Wyłączanie możliwości wykonywania skryptów

Zaktualizuj rolę o ID „5”, wyłącz możliwość wykonywania skryptów.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "role.update",
    "params": [
        {
            "roleid": "5",
            "rules": {
                "actions": [
                    {
                        "name": "execute_scripts",
                        "status": "0"
                    }
                ]
            }
        }
    ],
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "roleids": [
            "5"
        ]
    },
    "id": 1
}
```

Ograniczanie dostępu do API

Zaktualizuj rolę o ID „5”, zabraniając wywoływania dowolnych metod „create”, „update” lub „delete”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "role.update",
    "params": [
        {
            "roleid": "5",
            "rules": {
                "api.access": "1",
                "api.mode": "0",
                "api": ["*.create", "*.update", "*.delete"]
            }
        }
    ],
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "roleids": [
            "5"
        ]
    },
    "id": 1
}
```

Źródło

CRole::update() w *ui/include/classes/api/services/CRole.php*.

Scenariusz WWW

Ta klasa jest przeznaczona do pracy ze scenariuszami WWW.

Odwołania do obiektów:

- Scenariusz WWW
- Krok scenariusza
  - Pole HTTP
- Tag scenariusza WWW

Dostępne metody:

- httptest.create - utwórz nowe scenariusze WWW
- httptest.delete - usuń scenariusze WWW
- httptest.get - pobierz scenariusze WWW
- httptest.update - zaktualizuj scenariusze WWW

Obiekt scenariusza internetowego

Następujące obiekty są bezpośrednio powiązane z API `webcheck`.

Scenariusz WWW

Obiekt scenariusza WWW ma następujące właściwości.

Właściwość	Typ	Opis
httptestid	ID	ID scenariusza WWW. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji
hostid	ID	ID hosta, do którego należy scenariusz WWW. Zachowanie właściwości: - *stałe* - *wymagane* dla operacji tworzenia
name	string	Nazwa scenariusza WWW. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
agent	string	Ciąg user agent, który będzie używany przez scenariusz WWW. Domyślnie: Zabbix
authentication	integer	Metoda uwierzytelniania, która będzie używana przez scenariusz WWW. Możliwe wartości: 0 - *(domyślnie)* brak; 1 - podstawowe uwierzytelnianie HTTP; 2 - uwierzytelnianie NTLM; 3 - uwierzytelnianie Kerberos; 4 - uwierzytelnianie Digest.
delay	string	Interwał wykonywania scenariusza WWW. Akceptuje sekundy lub jednostkę czasu z sufiksem (np. 30s, 1m, 2h, 1d) albo makro użytkownika. Domyślnie: 1m.
headers	array	Nagłówki HTTP, które będą wysyłane podczas wykonywania żądania.
http_password	string	Hasło używane do podstawowego uwierzytelniania HTTP, NTLM, Kerberos lub Digest.

Właściwość	Typ	Opis
http_proxy	string	Proxy, który będzie używany przez scenariusz WWW, podany jako *http://[username[:password]@]proxy.example.com[:port]*.
http_user	string	Nazwa użytkownika używana do podstawowego uwierzytelniania HTTP, NTLM, Kerberos lub Digest.
retries	integer	Liczba prób wykonania każdego kroku przez scenariusz WWW przed zgłoszeniem niepowodzenia. Domyślnie: 1.
ssl_cert_file	string	Nazwa pliku certyfikatu SSL używanego do uwierzytelniania klienta (musi być w formacie PEM).
ssl_key_file	string	Nazwa pliku klucza prywatnego SSL używanego do uwierzytelniania klienta (musi być w formacie PEM).
ssl_key_password	string	Hasło klucza prywatnego SSL.
status	integer	Określa, czy scenariusz WWW jest włączony. Możliwe wartości: 0 - *(domyślnie)* włączony; 1 - wyłączony.
templateid	ID	ID nadrzędnego scenariusza WWW szablonu. Zachowanie właściwości: - *tylko do odczytu*
variables	array	Zmienne scenariusza WWW.
verify_host	integer	Określa, czy należy sprawdzać, czy nazwa hosta dla połączenia jest zgodna z nazwą w certyfikacie hosta. Możliwe wartości: 0 - *(domyślnie)* pomiń weryfikację hosta; 1 - weryfikuj hosta.
verify_peer	integer	Określa, czy należy sprawdzać autentyczność certyfikatu hosta. Możliwe wartości: 0 - *(domyślnie)* pomiń weryfikację peer; 1 - weryfikuj peer.
uuid	string	Globalny unikalny identyfikator używany do łączenia importowanych scenariuszy WWW z już istniejącymi. Generowany automatycznie, jeśli nie został podany. Zachowanie właściwości: - *obsługiwane*, jeśli scenariusz WWW należy do szablonu

Krok scenariusza

Obiekt kroku scenariusza definiuje określone sprawdzenie scenariusza WWW. Ma następujące właściwości.

Właściwość	Typ	Opis
name	string	Nazwa kroku scenariusza. Zachowanie właściwości: - *wymagane*
no	integer	Numer sekwencyjny kroku w scenariuszu WWW. Zachowanie właściwości: - *wymagane*
url	string	Adres URL do sprawdzenia. Zachowanie właściwości: - *wymagane*

Właściwość	Typ	Opis
follow_redirects	integer	Określa, czy podążać za przekierowaniami HTTP. Możliwe wartości: 0 - nie podążaj za przekierowaniami; 1 - *(domyślnie)* podążaj za przekierowaniami.
headers	array	Nagłówki HTTP, które zostaną wysłane podczas wykonywania żądania. Nagłówki kroku scenariusza zastąpią nagłówki określone dla scenariusza WWW.
posts	string/array	Zmienne HTTP POST jako ciąg znaków (surowe dane POST) lub jako tablica pól HTTP (dane pól formularza).
required	string	Tekst, który musi występować w odpowiedzi.
retrieve_mode	integer	Część odpowiedzi HTTP, którą krok scenariusza musi pobrać. Możliwe wartości: 0 - *(domyślnie)* tylko treść; 1 - tylko nagłówki; 2 - nagłówki i treść.
status_codes	string	Zakresy wymaganych kodów statusu HTTP, oddzielone przecinkami.
timeout	string	Limit czasu żądania w sekundach. Akceptuje sekundy, jednostkę czasu z sufiksem lub makro użytkownika. Domyślnie: 15s. Maksimum: 1h. Minimum: 1s.
variables	array	Zmienne kroku scenariusza.
query_fields	array	Pola zapytania - tablica pól HTTP, które zostaną dodane do adresu URL podczas wykonywania żądania.

Pole HTTP

Obiekt pola HTTP definiuje nazwę i wartość używane do określania zmiennych scenariusza WWW, nagłówków HTTP oraz pól POST lub pól zapytania. Ma następujące właściwości.

Właściwość	Typ	Opis
name	string	Nazwa nagłówka/zmiennej/pola POST lub GET. Zachowanie właściwości: - *wymagane*
value	string	Wartość nagłówka/zmiennej/pola POST lub GET. Zachowanie właściwości: - *wymagane*

Tag scenariusza WWW

Obiekt tagu scenariusza WWW ma następujące właściwości.

Właściwość	Typ	Opis
tag	string	Nazwa tagu scenariusza WWW. Zachowanie właściwości: - *wymagane*
value	string	Wartość tagu scenariusza WWW. Zachowanie właściwości: - *tylko do odczytu*.

Właściwość	Typ	Opis
object	integer	Typ obiektu, z którego tag został odziedziczony. Możliwe wartości: 0 - szablon; 1 - host. Zachowanie właściwości: - *tylko do odczytu*.
objectid	ID	ID obiektu, z którego tag został odziedziczony. Zachowanie właściwości: - *tylko do odczytu*.

httptest.create

Opis

`object httptest.create(object/array webScenarios)`

Ta metoda umożliwia tworzenie nowych scenariuszy WWW.

Note:
Utworzenie scenariusza WWW automatycznie utworzy zestaw pozycji monitorowania WWW.

Note:
Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach ról użytkowników. Więcej informacji znajduje się w sekcji Role użytkowników.

Parametry

`(object/array)` Scenariusze web do utworzenia.

Oprócz standardowych właściwości scenariusza web, metoda akceptuje następujące parametry.

Parametr	Type	Opis
steps	array	Kroki scenariusza. Zachowanie parametru: - *wymagany*
tags	array	Tagi scenariusza web.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory utworzonych scenariuszy WWW we właściwości `httptestids`. Kolejność zwróconych identyfikatorów odpowiada kolejności przekazanych scenariuszy WWW.

Przykłady

Tworzenie scenariusza WWW

Utwórz scenariusz WWW do monitorowania strony głównej firmy. Scenariusz będzie miał dwa kroki, aby sprawdzić stronę główną oraz stronę „O nas” i upewnić się, że zwracają kod statusu HTTP 200.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "httptest.create",
    "params": {
        "name": "Homepage check",
        "hostid": "10085",
        "steps": [
            {
                "name": "Homepage",
```

```
                "url": "http://example.com",
                "status_codes": "200",
                "no": 1
            },
            {
                "name": "Homepage / About",
                "url": "http://example.com/about",
                "status_codes": "200",
                "no": 2
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "httptestids": [
            "5"
        ]
    },
    "id": 1
}
```

Zobacz także

- Krok scenariusza

Źródło

CHttpTest::create() w *ui/include/classes/api/services/CHttpTest.php*.

httptest.delete

Opis

`object httptest.delete(array webScenarioIds)`

Ta metoda umożliwia usuwanie scenariuszy sieci WWW.

Note:
Ta metoda jest dostępna tylko dla użytkowników typu *Admin* i *Super admin*. Uprawnienia do wywołania metody można odwołać w ustawieniach roli użytkownika. Więcej informacji można znaleźć w Role użytkownika.

Parametry

`(array)` ID scenariuszy sieci WWW do usunięcia.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory usuniętych scenariuszy sieci WWW we właściwości `httptestids`.

Przykłady

Usuwanie wielu scenariuszy sieci WWW

Usuń dwa scenariusze sieci WWW.

Żądanie:

```
{
"jsonrpc": "2.0",
"method": "httptest.delete",
"params": [
"2",
"3"
```

```
],
"id": 1
}
```

Odpowiedź:

```
{
"jsonrpc": "2.0",
"result": {
"httptestids": [
"2",
"3"
]
},
"id": 1
}
```

Źródło

CHttpTest::delete() w *ui/include/classes/api/services/CHttpTest.php*.

httptest.get

Opis

`integer/array httptest.get(object parameters)`

Ta metoda umożliwia pobieranie scenariuszy WWW zgodnie z podanymi parametrami.

> **Note:**
> Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji znajduje się w sekcji Role użytkowników.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
groupids	ID/array	Zwraca tylko scenariusze WWW należące do podanych grup hostów.
hostids	ID/array	Zwraca tylko scenariusze WWW należące do podanych hostów.
httptestids	ID/array	Zwraca tylko scenariusze WWW o podanych identyfikatorach.
inherited	boolean	Jeśli ustawiono na `true`, zwraca tylko scenariusze WWW odziedziczone z szablonu.
inheritedTags	boolean	Zwraca scenariusze WWW, które mają podane `tags` również w szablonie/hoście/podłączonych szablonach. Możliwe wartości: `true` - szablon/host/podłączone szablony również muszą mieć podane tagi; `false` - *(domyślnie)* tagi z szablonu/hosta/podłączonych szablonów są ignorowane.
monitored	boolean	Jeśli ustawiono na `true`, zwraca tylko włączone scenariusze WWW należące do monitorowanych hostów.
selectInheritedTags	query	Zwraca właściwość `inheritedTags` z tagami znajdującymi się w szablonie/hoście/podłączonych szablonach.
templated	boolean	Jeśli ustawiono na `true`, zwraca tylko scenariusze WWW należące do szablonów.
templateids	ID/array	Zwraca tylko scenariusze WWW należące do podanych szablonów.
expandName	flag	Rozwija makra w nazwie scenariusza WWW.
expandStepName	flag	Rozwija makra w nazwach kroków scenariusza.

Parametr	Typ	Opis
evaltype	integer	Metoda oceny tagów. Możliwe wartości: 0 - *(domyślnie)* And/Or; 2 - Or.
tags	array	Zwraca tylko scenariusze WWW z podanymi tagami. Format: `[{"tag": "<tag>", "value": "<value>", "operator": "<operator>"}, ...]`. Pusta tablica zwraca wszystkie scenariusze WWW. Możliwe wartości operatora: 0 - *(domyślnie)* Zawiera; 1 - Równe; 2 - Nie zawiera; 3 - Nie równa się; 4 - Istnieje; 5 - Nie istnieje.
selectHosts	query	Zwraca hosty, do których należy scenariusz WWW, jako tablicę we właściwości `hosts`.
selectSteps	query	Zwraca kroki scenariusza WWW we właściwości `steps`. Obsługuje `count`.
selectTags	query	Zwraca tagi scenariusza WWW we właściwości `tags`.
sortfield	string/array	Sortuje wynik według podanych właściwości. Możliwe wartości: `httptestid`, `name`.
countOutput	boolean	Te parametry opisano w komentarzu referencyjnym.
editable	boolean	
excludeSearch	boolean	
filter	object	
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli został użyty parametr `countOutput`.

Przykłady

Pobieranie scenariusza WWW

Pobierz wszystkie dane o scenariuszu WWW „9”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "httptest.get",
    "params": {
        "output": "extend",
        "selectSteps": "extend",
        "httptestids": "9"
    },
    "id": 1
}
```

Odpowiedź:


```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "httptestid": "9",
            "name": "Homepage check",
            "delay": "1m",
            "status": "0",
            "agent": "Zabbix",
            "authentication": "0",
            "http_user": "",
            "http_password": "",
            "hostid": "10084",
            "templateid": "0",
            "http_proxy": "",
            "retries": "1",
            "ssl_cert_file": "",
            "ssl_key_file": "",
            "ssl_key_password": "",
            "verify_peer": "0",
            "verify_host": "0",
            "uuid": "",
            "headers": [],
            "variables": [],
            "steps": [
                {
                    "httpstepid": "36",
                    "httptestid": "9",
                    "name": "Homepage",
                    "no": "1",
                    "url": "http://example.com",
                    "timeout": "15s",
                    "posts": "",
                    "required": "",
                    "status_codes": "200",
                    "follow_redirects": "1",
                    "retrieve_mode": "0",
                    "post_type": "1",
                    "headers": [],
                    "variables": [
                        {
                            "name":"{var}",
                            "value":"12"
                        }
                    ],
                    "query_fields": []
                },
                {
                    "httpstepid": "37",
                    "httptestid": "9",
                    "name": "Homepage / About",
                    "no": "2",
                    "url": "http://example.com/about",
                    "timeout": "15s",
                    "posts": "",
                    "required": "",
                    "status_codes": "200",
                    "follow_redirects": "1",
                    "retrieve_mode": "0",
                    "post_type": "1",
                    "headers": [],
```

```
                    "variables": [],
                    "query_fields": []
                }
            ]
        }
    ],
    "id": 1
}
```

Zobacz także

- Host
- Krok scenariusza

Źródło

CHttpTest::get() w *ui/include/classes/api/services/CHttpTest.php*.

httptest.update

Opis

`object httptest.update(object/array webScenarios)`

Ta metoda umożliwia aktualizację istniejących scenariuszy WWW.

Note:
Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach ról użytkowników. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Właściwości scenariusza WWW do zaktualizowania.

Właściwość `httptestid` musi być zdefiniowana dla każdego scenariusza WWW, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko przekazane właściwości, wszystkie pozostałe pozostaną bez zmian.

Oprócz standardowych właściwości scenariusza WWW, metoda akceptuje następujące parametry.

Parametr	Typ	Opis
steps	array	Kroki scenariusza zastępujące istniejące kroki.
tags	array	Tagi scenariusza WWW.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych scenariuszy WWW we właściwości `httptestid`.

Przykłady

Włączanie scenariusza WWW

Włącz scenariusz WWW, to znaczy ustaw jego status na „0”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "httptest.update",
    "params": {
        "httptestid": "5",
        "status": 0
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "httptestids": [
            "5"
        ]
    },
    "id": 1
}
```

Zobacz także

- Krok scenariusza

Źródło

CHttpTest::update() w *ui/include/classes/api/services/CHttpTest.php*.

Skrypt

Ta klasa jest przeznaczona do pracy ze skryptami.

Odwołania do obiektów:

- Script
  - Parametry webhooka
- Debug
  - Wpis dziennika

Dostępne metody:

- script.create - utwórz nowe skrypty
- script.delete - usuń skrypty
- script.execute - uruchom skrypty
- script.get - pobierz skrypty
- script.getscriptsbyevents - pobierz skrypty dla zdarzeń
- script.getscriptsbyhosts - pobierz skrypty dla hostów
- script.update - zaktualizuj skrypty

Obiekt skryptu

Następujące obiekty są bezpośrednio powiązane z API `script`.

Skrypt

Obiekt skryptu ma następujące właściwości.

Właściwość	Typ	Opis
scriptid	ID	ID skryptu. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji
name	string	Nazwa skryptu. Zachowanie właściwości: - *wymagane* dla operacji tworzenia

Właściwość	Typ	Opis
type	integer	Typ skryptu. Możliwe wartości, jeśli `scope` jest ustawione na ”action operation”: 0 - Script; 1 - IPMI; 2 - SSH; 3 - TELNET; 5 - Webhook. Możliwe wartości, jeśli `scope` jest ustawione na ”manual host action” lub ”manual event action”: 6 - URL. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
command	string	Polecenie do uruchomienia. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”Script”, ”IPMI”, ”SSH”, ”TELNET” lub ”Webhook”
scope	integer	Zakres skryptu. Możliwe wartości: 1 - action operation; 2 - manual host action; 4 - manual event action. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
execute_on	integer	Gdzie uruchomić skrypt. Możliwe wartości: 0 - uruchom na Zabbix agent; 1 - uruchom na Zabbix serwer. Jest to *obsługiwane* tylko wtedy, gdy wykonywanie skryptów globalnych jest włączone na Zabbix serwerze; 2 - *(domyślnie)* uruchom na Zabbix serwerze lub proxy. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”Script”
menu_path	string	Foldery oddzielone ukośnikiem, które tworzą nawigację w formie menu w frontend po kliknięciu hosta lub zdarzenia. Zachowanie właściwości: - *obsługiwane*, jeśli `scope` jest ustawione na ”manual host action” lub ”manual event action”
authtype	integer	Metoda uwierzytelniania używana dla skryptu typu SSH. Możliwe wartości: 0 - hasło; 1 - klucz publiczny. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”SSH”
username	string	Nazwa użytkownika używana do uwierzytelniania. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”SSH” lub ”TELNET”

Właściwość	Typ	Opis
password	string	Hasło używane dla skryptów SSH z uwierzytelnianiem hasłem oraz skryptów TELNET. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”SSH” i `authtype` jest ustawione na ”password”, lub `type` jest ustawione na ”TELNET”
publickey	string	Nazwa pliku klucza publicznego używanego dla skryptów SSH z uwierzytelnianiem kluczem publicznym. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”SSH” i `authtype` jest ustawione na ”public key”
privatekey	string	Nazwa pliku klucza prywatnego używanego dla skryptów SSH z uwierzytelnianiem kluczem publicznym. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”SSH” i `authtype` jest ustawione na ”public key”
port	string	Numer portu używany dla skryptów SSH i TELNET. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”SSH” lub ”TELNET”
groupid	ID	ID grupy hostów, na której można uruchomić skrypt. Jeśli ustawione na ”0”, skrypt będzie dostępny dla wszystkich grup hostów. Domyślnie: 0.
usrgrpid	ID	ID grupy użytkowników, która będzie uprawniona do uruchamiania skryptu. Jeśli ustawione na ”0”, skrypt będzie dostępny dla wszystkich grup użytkowników. Domyślnie: 0.
host_access	integer	Uprawnienia do hosta wymagane do uruchomienia skryptu. Możliwe wartości: 2 - *(domyślnie)* odczyt; 3 - zapis. Zachowanie właściwości: - *obsługiwane*, jeśli `scope` jest ustawione na ”manual host action” lub ”manual event action”
confirmation	string	Tekst wyskakującego okna potwierdzenia. Okno wyskakujące pojawi się podczas próby uruchomienia skryptu z frontend Zabbix. Zachowanie właściwości: - *obsługiwane*, jeśli `scope` jest ustawione na ”manual host action” lub ”manual event action”

Właściwość	Typ	Opis
timeout	string	Limit czasu wykonania skryptu webhook w sekundach. Obsługiwane są sufiksy czasu (np. 30s, 1m). Możliwe wartości: 1-60s. Domyślnie: 30s. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”Webhook”
parameters	array	Tablica parametrów wejściowych webhooka. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”Webhook”
description	string	Opis skryptu.
url	string	URL zdefiniowany przez użytkownika. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na ”URL”
new_window	integer	Otwórz URL w nowym oknie. Możliwe wartości: 0 - Nie; 1 - *(domyślnie)* Tak. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na ”URL”
manualinput	integer	Wskazuje, czy skrypt akceptuje dane wejściowe podane przez użytkownika. Możliwe wartości: 0 - *(domyślnie)* Wyłączone; 1 - Włączone; Zachowanie właściwości: - *obsługiwane*, jeśli `scope` jest ustawione na ”manual host action” lub ”manual event action”
manualinput_prompt	string	Tekst monitu dla ręcznego wprowadzania danych. Zachowanie właściwości: - *wymagane*, jeśli `manualinput` jest ustawione na ”Enabled”
manualinput_validator	string	Pole tekstowe używane do walidacji danych wejściowych podanych przez użytkownika. Ciąg składa się albo z wyrażenia regularnego, albo z zestawu wartości oddzielonych przecinkami. Zachowanie właściwości: - *wymagane*, jeśli `manualinput` jest ustawione na ”Enabled”
manualinput_validator_type	integer	Określa oczekiwany typ danych wejściowych użytkownika. Możliwe wartości: 0 - *(domyślnie)* String. Oznacza, że manualinput_validator ma być traktowane jako wyrażenie regularne; 1 - List. Oznacza, że manualinput_validator ma być traktowane jako lista możliwych wartości wejściowych oddzielonych przecinkami. Zachowanie właściwości: - *obsługiwane*, jeśli `manualinput` jest ustawione na ”Enabled”

Właściwość	Typ	Opis
manualinput_default_value	string	Wartość domyślna do automatycznego uzupełniania danych wejściowych użytkownika. Zachowanie właściwości: - *obsługiwane*, jeśli `manualinput_validator_type` jest ustawione na "String"

Parametry webhooka

Parametry przekazywane do skryptu webhooka podczas jego wywołania mają następujące właściwości.

Właściwość	Typ	Opis
name	string	Nazwa parametru. Zachowanie właściwości: - *wymagane*
value	string	Wartość parametru. Obsługuje makra.

Debug

Informacje debugowania wykonanego skryptu webhook. Obiekt debug ma następujące właściwości.

Właściwość	Type	Opis
logs	array	Tablica wpisów dziennika.
ms	string	Czas wykonywania skryptu w milisekundach.

Wpis dziennika

Obiekt wpisu dziennika ma następujące właściwości.

Właściwość	Typ	Opis
level	integer	Poziom dziennika.
ms	string	Czas, który upłynął w milisekundach od uruchomienia skryptu do momentu dodania wpisu dziennika.
message	string	Komunikat dziennika.

script.create

Opis

`object script.create(object/array scripts)`

Ta metoda umożliwia tworzenie nowych skryptów.

Note:
Ta metoda jest dostępna tylko dla użytkownika typu *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Skrypty do utworzenia.

Metoda akceptuje skrypty ze standardowymi właściwościami skryptu.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory utworzonych skryptów we właściwości `scriptids`. Kolejność zwróconych identyfikatorów odpowiada kolejności przekazanych skryptów.

Przykłady

Utwórz skrypt webhook

Utwórz skrypt webhook, który wysyła żądanie HTTP do zewnętrznej usługi.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "script.create",
    "params": {
        "name": "Webhook script",
        "command": "try {\n var request = new HttpRequest(),\n response,\n data;\n\n request.addHeader('Co
        "scope": 1,
        "type": 5,
        "timeout": "40s",
        "parameters": [
            {
                "name": "token",
                "value": "{$WEBHOOK.TOKEN}"
            },
            {
                "name": "host",
                "value": "{HOST.HOST}"
            },
            {
                "name": "v",
                "value": "2.2"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "scriptids": [
            "3"
        ]
    },
    "id": 1
}
```

Utwórz skrypt SSH

Utwórz skrypt SSH z uwierzytelnianiem kluczem publicznym, który może być wykonywany na hoście i ma menu kontekstowe.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "script.create",
    "params": {
        "name": "SSH script",
        "command": "my script command",
        "type": 2,
        "authtype": 1,
        "username": "John",
        "publickey": "pub.key",
        "privatekey": "priv.key",
        "password": "secret",
        "port": "12345",
        "scope": 2,
        "menu_path": "All scripts/SSH",
        "usrgrpid": "7",
        "groupid": "4"
    },
```

```
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "scriptids": [
            "5"
        ]
    },
    "id": 1
}
```

Utwórz niestandardowy skrypt

Utwórz niestandardowy skrypt, który zrestartuje serwer. Skrypt będzie wymagał uprawnień do zapisu do hosta i poprosi użytkownika o ręczne wprowadzenie danych. Po pomyślnym przesłaniu danych wejściowych skrypt wyświetli komunikat potwierdzający we frontendzie.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "script.create",
    "params": {
        "name": "Reboot server",
        "command": "reboot server {MANUALINPUT}",
        "type": 0,
        "scope": 2,
        "confirmation": "Are you sure you would like to reboot the server {MANUALINPUT}?",
        "manualinput": 1,
        "manualinput_prompt": "Which server you want to reboot?",
        "manualinput_validator": "[1-9]",
        "manualinput_validator_type": 0,
        "manualinput_default_value": "1"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "scriptids": [
            "4"
        ]
    },
    "id": 1
}
```

Utwórz skrypt typu URL

Utwórz skrypt typu URL dla zakresu host, który pozostaje w tym samym oknie i ma tekst potwierdzenia.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "script.create",
    "params": {
        "name": "URL script",
        "type": 6,
        "scope": 2,
        "url": "http://zabbix/ui/zabbix.php?action=host.edit&hostid={HOST.ID}",
        "confirmation": "Edytować host {HOST.NAME}?",
```

```
        "new_window": 0
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "scriptids": [
            "56"
        ]
    },
    "id": 1
}
```

Utwórz skrypt typu URL z ręcznym wprowadzaniem

Utwórz skrypt typu URL dla zakresu zdarzenia, który otwiera się w nowym oknie i ma ręczne wprowadzanie.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "script.create",
    "params": {
        "name": "Skrypt URL z ręcznym wprowadzaniem",
        "type": 6,
        "scope": 4,
        "url": "http://zabbix/ui/zabbix.php?action={MANUALINPUT}",
        "new_window": 1,
        "manualinput": 1,
        "manualinput_prompt": "Wybierz stronę do otwarcia:",
        "manualinput_validator": "dashboard.view,script.list,actionlog.list",
        "manualinput_validator_type": 1
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "scriptids": [
            "57"
        ]
    },
    "id": 1
}
```

Źródło

CScript::create() w *ui/include/classes/api/services/CScript.php*.

script.delete

Opis

`object script.delete(array scriptIds)`

Ta metoda umożliwia usuwanie skryptów.

Note:
Ta metoda jest dostępna tylko dla użytkownika *Super admin*. Uprawnienia do wywołania metody można cofnąć w ustawieniach roli użytkownika. Więcej informacji można znaleźć w User roles.

Parametry

`(array)` ID skryptów do usunięcia.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory usuniętych skryptów we właściwości `scriptids`.

Przykłady

Usuń wiele skryptów

Usuń dwa skrypty.

Żądanie:

```
{
"jsonrpc": "2.0",
"method": "script.delete",
"params": [
"3",
"4"
],
"id": 1
}
```

Odpowiedź:

```
{
"jsonrpc": "2.0",
"result": {
"scriptids": [
"3",
"4"
]
},
"id": 1
}
```

Źródło

CScript::delete() w *ui/include/classes/api/services/CScript.php*.

script.execute

Opis

`object script.execute(object parameters)`

Ta metoda umożliwia uruchomienie skryptu na hoście lub zdarzeniu. Z wyjątkiem skryptów typu URL. Nie są one wykonywalne.

Note:
Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji znajduje się w sekcji Role użytkowników.

Parametry

`(object)` Parametry zawierające ID skryptu do uruchomienia oraz albo ID hosta, albo ID zdarzenia i wartość manualinput.

Parametr	Type	Opis
scriptid	ID	ID skryptu do uruchomienia. Zachowanie parametru: - *wymagany*
hostid	ID	ID hosta, na którym ma zostać uruchomiony skrypt. Zachowanie parametru: - *wymagany*, jeśli `eventid` nie jest ustawione

Parametr	Type	Opis
eventid	ID	ID zdarzenia, dla którego ma zostać uruchomiony skrypt. Zachowanie parametru: - *wymagany*, jeśli `hostid` nie jest ustawione
manualinput	string	Wartość podana przez użytkownika, z którą ma zostać uruchomiony skrypt, zastępująca makro {MANUALINPUT}.

Zwracane wartości

`(object)` Zwraca wynik wykonania skryptu.

Właściwość	Type	Opis
response	string	Czy skrypt został uruchomiony pomyślnie. Możliwa wartość - `success`.
value	string	Dane wyjściowe skryptu.
debug	object	Zawiera obiekt debug, jeśli wykonywany jest skrypt webhook. Dla innych typów skryptów zawiera pusty obiekt.

Przykłady

Uruchamianie skryptu webhook

Uruchom skrypt webhook, który wysyła żądanie HTTP do zewnętrznej usługi.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "script.execute",
    "params": {
        "scriptid": "4",
        "hostid": "30079"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "response": "success",
        "value": "{\"status\":\"sent\",\"timestamp\":\"1611235391\"}",
        "debug": {
            "logs": [
                {
                    "level": 3,
                    "ms": 480,
                    "message": "[Webhook Script] HTTP status: 200."
                }
            ],
            "ms": 495
        }
    },
    "id": 1
}
```

Uruchamianie niestandardowego skryptu

Uruchom skrypt „ping” na hoście.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "script.execute",
    "params": {
        "scriptid": "1",
        "hostid": "30079"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "response": "success",
        "value": "PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.\n64 bytes from 127.0.0.1: icmp_req=1 tt
        "debug": []
    },
    "id": 1
}
```

Uruchom własny skrypt z ręcznym wprowadzaniem danych

Uruchom skrypt „ping” z poleceniem „ping -c {MANUALINPUT} {HOST.CONN}; case $? in [01]) true;; *) false;; esac” na hoście.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "script.execute",
    "params": {
        "scriptid": "7",
        "hostid": "30079",
        "manualinput": "2"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "response": "success",
        "value": "PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.\n64 bytes from 127.0.0.1: icmp_seq=1 tt
        "debug": []
    },
    "id": 1
}
```

Źródło

CScript::execute() w *ui/include/classes/api/services/CScript.php*.

script.get

Opis

`integer/array script.get(object parameters)`

Ta metoda umożliwia pobieranie skryptów zgodnie z podanymi parametrami.

Note:
Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w User roles.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
groupids	ID/array	Zwraca tylko skrypty, które mogą być uruchamiane dla podanych grup hostów.
hostids	ID/array	Zwraca tylko skrypty, które mogą być uruchamiane dla podanych hostów.
scriptids	ID/array	Zwraca tylko skrypty o podanych ID.
usrgrpids	ID/array	Zwraca tylko skrypty, które mogą być uruchamiane przez użytkowników z podanych grup użytkowników.
selectHostGroups	query	Zwraca właściwość `hostgroups` z grupami hostów, dla których skrypt może być uruchamiany.
selectHosts	query	Zwraca właściwość `hosts` z hostami, dla których skrypt może być uruchamiany.
selectActions	query	Zwraca właściwość `actions` z akcjami, z którymi skrypt jest powiązany.
sortfield	string/array	Sortuje wynik według podanych właściwości. Możliwe wartości: `scriptid`, `name`.
countOutput	boolean	Te parametry są opisane w komentarzu referencyjnym.
editable	boolean	
excludeSearch	boolean	
filter	object	
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli został użyty parametr `countOutput`.

Przykłady

Pobierz wszystkie skrypty

Pobierz wszystkie skonfigurowane skrypty.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "script.get",
    "params": {
        "output": "extend"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "scriptid": "1",
```

```
            "name": "Ping",
            "command": "/bin/ping -c 3 {HOST.CONN} 2>&1",
            "host_access": "2",
            "usrgrpid": "0",
            "groupid": "0",
            "description": "",
            "confirmation": "",
            "type": "0",
            "execute_on": "1",
            "timeout": "30s",
            "scope": "2",
            "port": "",
            "authtype": "0",
            "username": "",
            "password": "",
            "publickey": "",
            "privatekey": "",
            "menu_path": "",
            "url": "",
            "new_window": "1",
            "manualinput": "0",
            "manualinput_prompt": "",
            "manualinput_validator": "",
            "manualinput_validator_type": "0",
            "manualinput_default_value": "",
            "parameters": []
        },
        {
            "scriptid": "2",
            "name": "Traceroute",
            "command": "/usr/bin/traceroute {HOST.CONN} 2>&1",
            "host_access": "2",
            "usrgrpid": "0",
            "groupid": "0",
            "description": "",
            "confirmation": "",
            "type": "0",
            "execute_on": "1",
            "timeout": "30s",
            "scope": "2",
            "port": "",
            "authtype": "0",
            "username": "",
            "password": "",
            "publickey": "",
            "privatekey": "",
            "menu_path": "",
            "url": "",
            "new_window": "1",
            "manualinput": "0",
            "manualinput_prompt": "",
            "manualinput_validator": "",
            "manualinput_validator_type": "0",
            "manualinput_default_value": "",
            "parameters": []
        },
        {
            "scriptid": "3",
            "name": "Detect operating system",
            "command": "sudo /usr/bin/nmap -O {HOST.CONN} 2>&1",
            "host_access": "2",
            "usrgrpid": "7",
```

```
            "groupid": "0",
            "description": "",
            "confirmation": "",
            "type": "0",
            "execute_on": "1",
            "timeout": "30s",
            "scope": "2",
            "port": "",
            "authtype": "0",
            "username": "",
            "password": "",
            "publickey": "",
            "privatekey": "",
            "menu_path": "",
            "url": "",
            "new_window": "1",
            "manualinput": "0",
            "manualinput_prompt": "",
            "manualinput_validator": "",
            "manualinput_validator_type": "0",
            "manualinput_default_value": "",
            "parameters": []
        },
        {
            "scriptid": "4",
            "name": "Webhook",
            "command": "try {\n var request = new HttpRequest(),\n response,\n data;\n\n request.addHeader
            "host_access": "2",
            "usrgrpid": "7",
            "groupid": "0",
            "description": "",
            "confirmation": "",
            "type": "5",
            "execute_on": "1",
            "timeout": "30s",
            "scope": "2",
            "port": "",
            "authtype": "0",
            "username": "",
            "password": "",
            "publickey": "",
            "privatekey": "",
            "menu_path": "",
            "url": "",
            "new_window": "1",
            "manualinput": "0",
            "manualinput_prompt": "",
            "manualinput_validator": "",
            "manualinput_validator_type": "0",
            "manualinput_default_value": "",
            "parameters": [
                {
                    "name": "token",
                    "value": "{$WEBHOOK.TOKEN}"
                },
                {
                    "name": "host",
                    "value": "{HOST.HOST}"
                },
                {
                    "name": "v",
                    "value": "2.2"
```

```
                }
            ]
        },
        {
            "scriptid": "5",
            "name": "URL",
            "command": "",
            "host_access": "2",
            "usrgrpid": "0",
            "groupid": "0",
            "description": "",
            "confirmation": "Go to {HOST.NAME}?",
            "type": "6",
            "execute_on": "1",
            "timeout": "30s",
            "scope": "4",
            "port": "",
            "authtype": "0",
            "username": "",
            "password": "",
            "publickey": "",
            "privatekey": "",
            "menu_path": "",
            "url": "http://zabbix/ui/zabbix.php?action=latest.view&hostids[]={HOST.ID}",
            "new_window": "0",
            "manualinput": "0",
            "manualinput_prompt": "",
            "manualinput_validator": "",
            "manualinput_validator_type": "0",
            "manualinput_default_value": "",
            "parameters": []
        },
        {
            "scriptid": "6",
            "name": "URL with user input",
            "command": "",
            "host_access": "2",
            "usrgrpid": "0",
            "groupid": "0",
            "description": "",
            "confirmation": "Open zabbix page {MANUALINPUT}?",
            "type": "6",
            "execute_on": "1",
            "timeout": "30s",
            "scope": "2",
            "port": "",
            "authtype": "0",
            "username": "",
            "password": "",
            "publickey": "",
            "privatekey": "",
            "menu_path": "",
            "url": "http://zabbix/ui/zabbix.php?action={MANUALINPUT}",
            "new_window": "0",
            "manualinput": "1",
            "manualinput_prompt": "Select a page to open:",
            "manualinput_validator": "dashboard.view,script.list,actionlog.list",
            "manualinput_validator_type": "1",
            "parameters": []
        }
    ],
    "id": 1
```

```
}
```

Zobacz także

- Host
- Grupa hostów

Źródło

CScript::get() w *ui/include/classes/api/services/CScript.php*.

script.getscriptsbyevents

Opis

`object script.getscriptsbyevents(object parameters)`

Ta metoda umożliwia pobranie wszystkich dostępnych skryptów dla danego zdarzenia lub określonego skryptu, jeśli podano ID skryptu. Gdy podano manualinput, zastępuje makro {MANUALINPUT} określoną wartością.

> **Note:**
> Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Metoda akceptuje obiekt lub tablicę obiektów z następującymi parametrami.

Parametr	Type	Opis
eventid	ID	ID zdarzenia, dla którego mają zostać zwrócone skrypty. Musi być unikalne. Zachowanie parametrów: - *wymagany*
scriptid	ID	ID skryptu do zwrócenia.
manualinput	string	Wartość podanej przez użytkownika wartości makra {MANUALINPUT}.

Zwracane wartości

`(object)` Zwraca obiekt z identyfikatorami zdarzeń jako właściwościami oraz tablicami dostępnych skryptów jako wartościami. Jeśli podano identyfikator skryptu, skojarzona wartość jest tablicą zawierającą określony skrypt.

> **Note:**
> Metoda automatycznie rozwinie makra w tekście `confirmation`, tekście `manualinput prompt` oraz w `url`.
> Jeśli parametr manualinput zostanie podany, makro {MANUALINPUT} zostanie rozwinięte do określonej wartości.

Przykłady

Pobieranie skryptów według identyfikatorów zdarzeń

Pobierz wszystkie skrypty dostępne dla zdarzeń „632” i „614”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "script.getscriptsbyevents",
    "params": [
      {
         "eventid":  "632"
      },
      {
         "eventid":  "614"
      }
    ],
```

```
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "632": [
            {
                "scriptid": "3",
                "name": "Wykryj system operacyjny",
                "command": "sudo /usr/bin/nmap -O {HOST.CONN} 2>&1",
                "host_access": "2",
                "usrgrpid": "7",
                "groupid": "0",
                "description": "",
                "confirmation": "",
                "type": "0",
                "execute_on": "1",
                "timeout": "30s",
                "scope": "4",
                "port": "",
                "authtype": "0",
                "username": "",
                "password": "",
                "publickey": "",
                "privatekey": "",
                "menu_path": "",
                "url": "",
                "new_window": "1",
                "manualinput": "0",
                "manualinput_prompt": "",
                "manualinput_validator_type": "0",
                "manualinput_validator": "",
                "manualinput_default_value": "",
                "parameters": []
            },
            {
                "scriptid": "1",
                "name": "Ping",
                "command": "/bin/ping -c 3 {HOST.CONN} 2>&1",
                "host_access": "2",
                "usrgrpid": "0",
                "groupid": "0",
                "description": "",
                "confirmation": "",
                "type": "0",
                "execute_on": "1",
                "timeout": "30s",
                "scope": "4",
                "port": "",
                "authtype": "0",
                "username": "",
                "password": "",
                "publickey": "",
                "privatekey": "",
                "menu_path": "",
                "url": "",
                "new_window": "1",
                "manualinput": "0",
                "manualinput_prompt": "",
                "manualinput_validator_type": "0",
```

```
            "manualinput_validator": "",
            "manualinput_default_value": "",
            "parameters": []
        },
        {
            "scriptid": "4",
            "name": "Otwórz stronę Zabbix",
            "command": "",
            "host_access": "2",
            "usrgrpid": "0",
            "groupid": "0",
            "description": "",
            "confirmation": "Czy na pewno chcesz otworzyć stronę *UNKNOWN*?",
            "type": "6",
            "execute_on": "2",
            "timeout": "30s",
            "scope": "4",
            "port": "",
            "authtype": "0",
            "username": "",
            "password": "",
            "publickey": "",
            "privatekey": "",
            "menu_path": "",
            "url": "http://localhost/ui/zabbix.php?action=*UNKNOWN*",
            "new_window": "1",
            "manualinput": "1",
            "manualinput_prompt": "Strona Zabbix do otwarcia:",
            "manualinput_validator_type": "1",
            "manualinput_validator": "dashboard.view,discovery.view",
            "manualinput_default_value": "",
            "parameters": []
        },
        {
            "scriptid": "2",
            "name": "Traceroute",
            "command": "/usr/bin/traceroute {HOST.CONN} 2>&1",
            "host_access": "2",
            "usrgrpid": "0",
            "groupid": "0",
            "description": "",
            "confirmation": "",
            "type": "0",
            "execute_on": "1",
            "timeout": "30s",
            "scope": "4",
            "port": "",
            "authtype": "0",
            "username": "",
            "password": "",
            "publickey": "",
            "privatekey": "",
            "menu_path": "",
            "url": "",
            "new_window": "1",
            "manualinput": "0",
            "manualinput_prompt": "",
            "manualinput_validator_type": "0",
            "manualinput_validator": "",
            "manualinput_default_value": "",
            "parameters": []
        }
```

```
    ],
    "614": [
        {
            "scriptid": "3",
            "name": "Wykryj system operacyjny",
            "command": "sudo /usr/bin/nmap -O {HOST.CONN} 2>&1",
            "host_access": "2",
            "usrgrpid": "7",
            "groupid": "0",
            "description": "",
            "confirmation": "",
            "type": "0",
            "execute_on": "1",
            "timeout": "30s",
            "scope": "4",
            "port": "",
            "authtype": "0",
            "username": "",
            "password": "",
            "publickey": "",
            "privatekey": "",
            "menu_path": "",
            "url": "",
            "new_window": "1",
            "manualinput": "0",
            "manualinput_prompt": "",
            "manualinput_validator_type": "1",
            "manualinput_validator": "",
            "manualinput_default_value": "",
            "parameters": []
        },
        {
            "scriptid": "1",
            "name": "Ping",
            "command": "/bin/ping -c 3 {HOST.CONN} 2>&1",
            "host_access": "2",
            "usrgrpid": "0",
            "groupid": "0",
            "description": "",
            "confirmation": "",
            "type": "0",
            "execute_on": "1",
            "timeout": "30s",
            "scope": "4",
            "port": "",
            "authtype": "0",
            "username": "",
            "password": "",
            "publickey": "",
            "privatekey": "",
            "menu_path": "",
            "url": "",
            "new_window": "1",
            "manualinput": "0",
            "manualinput_prompt": "",
            "manualinput_validator_type": "0",
            "manualinput_validator": "",
            "manualinput_default_value": "",
            "parameters": []
        },
        {
            "scriptid": "4",
```

```
                "name": "Otwórz stronę Zabbix",
                "command": "",
                "host_access": "2",
                "usrgrpid": "0",
                "groupid": "0",
                "description": "",
                "confirmation": "Czy na pewno chcesz otworzyć stronę *UNKNOWN*?",
                "type": "6",
                "execute_on": "2",
                "timeout": "30s",
                "scope": "4",
                "port": "",
                "authtype": "0",
                "username": "",
                "password": "",
                "publickey": "",
                "privatekey": "",
                "menu_path": "",
                "url": "http://localhost/ui/zabbix.php?action=*UNKNOWN*",
                "new_window": "1",
                "manualinput": "1",
                "manualinput_prompt": "Strona Zabbix do otwarcia:",
                "manualinput_validator_type": "1",
                "manualinput_validator": "dashboard.view,discovery.view",
                "manualinput_default_value": "",
                "parameters": []
            },
            {
                "scriptid": "2",
                "name": "Traceroute",
                "command": "/usr/bin/traceroute {HOST.CONN} 2>&1",
                "host_access": "2",
                "usrgrpid": "0",
                "groupid": "0",
                "description": "",
                "confirmation": "",
                "type": "0",
                "execute_on": "1",
                "timeout": "30s",
                "scope": "4",
                "port": "",
                "authtype": "0",
                "username": "",
                "password": "",
                "publickey": "",
                "privatekey": "",
                "menu_path": "",
                "url": "",
                "new_window": "1",
                "manualinput": "0",
                "manualinput_prompt": "",
                "manualinput_validator_type": "0",
                "manualinput_validator": "",
                "manualinput_default_value": "",
                "parameters": []
            }
        ]
    },
    "id": 1
}
```


Pobieranie określonego skryptu z wartością manualinput.

Pobierz skrypt o ID „4” dla zdarzenia „632” z wartością manualinput „dashboard.view”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "script.getscriptsbyevents",
    "params": [
      {
        "eventid":  "632",
        "scriptid": "4",
        "manualinput": "dashboard.view"
      }
  ],
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
      "632": [
        {
          "scriptid": "4",
          "name": "Open Zabbix page",
          "command": "",
          "host_access": "2",
          "usrgrpid": "0",
          "groupid": "0",
          "description": "",
          "confirmation": "Are you sure you want to open page dashboard.view?",
          "type": "6",
          "execute_on": "2",
          "timeout": "30s",
          "scope": "4",
          "port": "",
          "authtype": "0",
          "username": "",
          "password": "",
          "publickey": "",
          "privatekey": "",
          "menu_path": "",
          "url": "http://localhost/ui/zabbix.php?action=dashboard.view",
          "new_window": "1",
          "manualinput": "1",
          "manualinput_prompt": "Zabbix page to open:",
          "manualinput_validator_type": "1",
          "manualinput_validator": "dashboard.view,discovery.view",
          "manualinput_default_value": "",
          "parameters": []
        }
      ]
    },
    "id": 1
}
```

Źródło

CScript::getScriptsByEvents() w *ui/include/classes/api/services/CScript.php*.

script.getscriptsbyhosts

Opis

`object script.getscriptsbyhosts(object parameters)`

Ta metoda umożliwia pobranie wszystkich dostępnych skryptów dla danego hosta lub określonego skryptu, jeśli podano ID skryptu. Gdy podano manualinput, zastępuje makro {MANUALINPUT} określoną wartością.

Note:
Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Metoda akceptuje obiekt lub tablicę obiektów z następującymi parametrami.

Parametr	Typ	Opis
hostid	ID	ID hosta, dla którego mają zostać zwrócone skrypty. Musi być unikalne. Zachowanie parametrów: - *wymagane*
scriptid	ID	ID skryptu do zwrócenia.
manualinput	string	Wartość makra {MANUALINPUT} podana przez użytkownika.

Zwracane wartości

`(object)` Zwraca obiekt z identyfikatorami hostów jako właściwościami oraz tablicami dostępnych skryptów jako wartościami. Jeśli podano identyfikator skryptu, skojarzona wartość jest tablicą zawierającą określony skrypt.

Note:
Metoda automatycznie rozwinie makra w tekście `confirmation`, tekście `manualinput prompt` oraz w `url`.
Jeśli parametr manualinput zostanie podany, makro {MANUALINPUT} zostanie rozwinięte do określonej wartości.

Przykłady

Pobieranie skryptów według identyfikatorów hostów

Pobierz wszystkie skrypty dostępne na hostach „30079” i „30073”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "script.getscriptsbyhosts",
    "params": [
       {
          "hostid":  "30079"
       },
       {
          "hostid":  "30073"
       }
    ],
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "30079": [
            {
                "scriptid": "3",
                "name": "Wykryj system operacyjny",
                "command": "sudo /usr/bin/nmap -O {HOST.CONN} 2>&1",
                "host_access": "2",
                "usrgrpid": "7",
                "groupid": "0",
                "description": "",
```

```
            "confirmation": "",
            "type": "0",
            "execute_on": "1",
            "timeout": "30s",
            "scope": "2",
            "port": "",
            "authtype": "0",
            "username": "",
            "password": "",
            "publickey": "",
            "privatekey": "",
            "menu_path": "",
            "url": "",
            "new_window": "1",
            "manualinput": "0",
            "manualinput_prompt": "",
            "manualinput_validator_type": "0",
            "manualinput_validator": "",
            "manualinput_default_value": "",
            "parameters": []
        },
        {
            "scriptid": "1",
            "name": "Ping",
            "command": "/bin/ping -c 3 {HOST.CONN} 2>&1",
            "host_access": "2",
            "usrgrpid": "0",
            "groupid": "0",
            "description": "",
            "confirmation": "",
            "type": "0",
            "execute_on": "1",
            "timeout": "30s",
            "scope": "2",
            "port": "",
            "authtype": "0",
            "username": "",
            "password": "",
            "publickey": "",
            "privatekey": "",
            "menu_path": "",
            "url": "",
            "new_window": "1",
            "manualinput": "0",
            "manualinput_prompt": "",
            "manualinput_validator_type": "0",
            "manualinput_validator": "",
            "manualinput_default_value": "",
            "parameters": []
        },
        {
            "scriptid": "4",
            "name": "Otwórz stronę Zabbix",
            "command": "",
            "host_access": "2",
            "usrgrpid": "0",
            "groupid": "0",
            "description": "",
            "confirmation": "Czy na pewno chcesz otworzyć stronę *UNKNOWN*?",
            "type": "6",
            "execute_on": "2",
            "timeout": "30s",
```

```
            "scope": "2",
            "port": "",
            "authtype": "0",
            "username": "",
            "password": "",
            "publickey": "",
            "privatekey": "",
            "menu_path": "",
            "url": "http://localhost/ui/zabbix.php?action=*UNKNOWN*",
            "new_window": "1",
            "manualinput": "0",
            "manualinput_prompt": "Strona Zabbix do otwarcia:",
            "manualinput_validator_type": "0",
            "manualinput_validator": "dashboard.view,discovery.view",
            "manualinput_default_value": "",
            "parameters": []
        },
        {
            "scriptid": "2",
            "name": "Traceroute",
            "command": "/usr/bin/traceroute {HOST.CONN} 2>&1",
            "host_access": "2",
            "usrgrpid": "0",
            "groupid": "0",
            "description": "",
            "confirmation": "",
            "type": "0",
            "execute_on": "1",
            "timeout": "30s",
            "scope": "2",
            "port": "",
            "authtype": "0",
            "username": "",
            "password": "",
            "publickey": "",
            "privatekey": "",
            "menu_path": "",
            "url": "",
            "new_window": "1",
            "manualinput": "0",
            "manualinput_prompt": "",
            "manualinput_validator_type": "0",
            "manualinput_validator": "",
            "manualinput_default_value": "",
            "parameters": []
        }
    ],
    "30073": [
        {
            "scriptid": "3",
            "name": "Wykryj system operacyjny",
            "command": "sudo /usr/bin/nmap -O {HOST.CONN} 2>&1",
            "host_access": "2",
            "usrgrpid": "7",
            "groupid": "0",
            "description": "",
            "confirmation": "",
            "type": "0",
            "execute_on": "1",
            "timeout": "30s",
            "scope": "2",
            "port": "",
```

```
            "authtype": "0",
            "username": "",
            "password": "",
            "publickey": "",
            "privatekey": "",
            "menu_path": "",
            "url": "",
            "new_window": "1",
            "manualinput": "0",
            "manualinput_prompt": "",
            "manualinput_validator_type": "0",
            "manualinput_validator": "",
            "manualinput_default_value": "",
            "parameters": []
        },
        {
            "scriptid": "1",
            "name": "Ping",
            "command": "/bin/ping -c 3 {HOST.CONN} 2>&1",
            "host_access": "2",
            "usrgrpid": "0",
            "groupid": "0",
            "description": "",
            "confirmation": "",
            "type": "0",
            "execute_on": "1",
            "timeout": "30s",
            "scope": "2",
            "port": "",
            "authtype": "0",
            "username": "",
            "password": "",
            "publickey": "",
            "privatekey": "",
            "menu_path": "",
            "url": "",
            "new_window": "1",
            "manualinput": "0",
            "manualinput_prompt": "",
            "manualinput_validator_type": "0",
            "manualinput_validator": "",
            "manualinput_default_value": "",
            "parameters": []
        },
        {
            "scriptid": "4",
            "name": "Otwórz stronę Zabbix",
            "command": "",
            "host_access": "2",
            "usrgrpid": "0",
            "groupid": "0",
            "description": "",
            "confirmation": "Czy na pewno chcesz otworzyć stronę *UNKNOWN*?",
            "type": "6",
            "execute_on": "2",
            "timeout": "30s",
            "scope": "2",
            "port": "",
            "authtype": "0",
            "username": "",
            "password": "",
            "publickey": "",
```

```
                "privatekey": "",
                "menu_path": "",
                "url": "http://localhost/ui/zabbix.php?action=*UNKNOWN*",
                "new_window": "1",
                "manualinput": "1",
                "manualinput_prompt": "Strona Zabbix do otwarcia:",
                "manualinput_validator_type": "1",
                "manualinput_validator": "dashboard.view,discovery.view",
                "manualinput_default_value": "",
                "parameters": []
            },
            {
                "scriptid": "2",
                "name": "Traceroute",
                "command": "/usr/bin/traceroute {HOST.CONN} 2>&1",
                "host_access": "2",
                "usrgrpid": "0",
                "groupid": "0",
                "description": "",
                "confirmation": "",
                "type": "0",
                "execute_on": "1",
                "timeout": "30s",
                "scope": "2",
                "port": "",
                "authtype": "0",
                "username": "",
                "password": "",
                "publickey": "",
                "privatekey": "",
                "menu_path": "",
                "url": "",
                "new_window": "1",
                "manualinput": "0",
                "manualinput_prompt": "",
                "manualinput_validator_type": "0",
                "manualinput_validator": "",
                "manualinput_default_value": "",
                "parameters": []
            }
        ]
    },
    "id": 1
}
```


Pobierz określony skrypt z wartością manualinput.

Pobierz skrypt o ID „4” na hoście „30079” z wartością manualinput „dashboard.view”.

Żądanie:


```
{
    "jsonrpc": "2.0",
    "method": "script.getscriptsbyhosts",
    "params": [
      {
        "hostid":  "30079",
        "scriptid": "4",
        "manualinput": "dashboard.view"
      }
  ],
    "id": 1
}
```


Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
      "30079": [
        {
          "scriptid": "4",
          "name": "Open Zabbix page",
          "command": "",
          "host_access": "2",
          "usrgrpid": "0",
          "groupid": "0",
          "description": "",
          "confirmation": "Are you sure you want to open page dashboard.view?",
          "type": "6",
          "execute_on": "2",
          "timeout": "30s",
          "scope": "2",
          "port": "",
          "authtype": "0",
          "username": "",
          "password": "",
          "publickey": "",
          "privatekey": "",
          "menu_path": "",
          "url": "http://localhost/ui/zabbix.php?action=dashboard.view",
          "new_window": "1",
          "manualinput": "1",
          "manualinput_prompt": "Zabbix page to open:",
          "manualinput_validator_type": "1",
          "manualinput_validator": "dashboard.view,discovery.view",
          "manualinput_default_value": "",
          "parameters": []
        }
      ]
    },
    "id": 1
}
```


Źródło

CScript::getScriptsByHosts() w *ui/include/classes/api/services/CScript.php*.

script.update

Opis

`object script.update(object/array scripts)`

Ta metoda umożliwia aktualizację istniejących skryptów.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkownika typu *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji User roles.

Parametry

`(object/array)` Właściwości skryptu, które mają zostać zaktualizowane.

Właściwość `scriptid` musi być zdefiniowana dla każdego skryptu, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko przekazane właściwości, wszystkie pozostałe pozostaną bez zmian. Wyjątkiem jest zmiana właściwości `type` z 5 (Webhook) na inną: właściwość `parameters` zostanie wyczyszczona.

Wartości zwracane

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych skryptów we właściwości `scriptids`.

Przykłady

Zmień polecenie skryptu

Zmień polecenie skryptu na "/bin/ping -c 10 {HOST.CONN} 2>&1".

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "script.update",
    "params": {
        "scriptid": "1",
        "command": "/bin/ping -c 10 {HOST.CONN} 2>&1"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "scriptids": [
            "1"
        ]
    },
    "id": 1
}
```

Zmień polecenie skryptu i dodaj ręczne dane wejściowe

Zmień polecenie skryptu na "/bin/ping -c {MANUALINPUT} {HOST.CONN} 2>&1".

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "script.update",
    "params": {
      "scriptid": "1",
      "command": "/bin/ping -c {MANUALINPUT} {HOST.CONN} 2>&1",
      "manualinput": "1",
      "manualinput_prompt": "Określ liczbę pakietów ICMP do wysłania za pomocą polecenia ping",
      "manualinput_validator": "^(?:[1-9]|10)$",
      "manualinput_validator_type": "0",
      "manualinput_default_value": "10"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "scriptids": [
            "1"
        ]
    },
    "id": 1
}
```

Źródło

CScript::update() w *ui/include/classes/api/services/CScript.php*.

SLA

Ta klasa została zaprojektowana do pracy z obiektami SLA (Service Level Agreement) używanymi do oceny wydajności infrastruktury IT i usług biznesowych.

Odwołania do obiektów:

- SLA
- Harmonogram SLA
- Wykluczony przestój SLA
- Tag usługi SLA

Dostępne metody:

- sla.create - tworzenie nowych SLA
- sla.delete - usuwanie SLA
- sla.get - pobieranie SLA
- sla.getsli - pobieranie danych Service Level Indicator (SLI) dla SLA
- sla.update - aktualizowanie SLA

Obiekt SLA (Service Level Agreement)

Następujące obiekty są bezpośrednio powiązane z API `sla` (Service Level Agreement).

SLA

Obiekt SLA ma następujące właściwości.

Właściwość	Typ	Opis
slaid	ID	ID SLA. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji
name	string	Nazwa SLA. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
period	integer	Okres raportowania SLA. Możliwe wartości: 0 - dziennie; 1 - tygodniowo; 2 - miesięcznie; 3 - kwartalnie; 4 - rocznie. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
slo	float	Minimalny akceptowalny cel poziomu usług (Service Level Objective, SLO) wyrażony w procentach. Jeśli wskaźnik poziomu usług (Service Level Indicator, SLI) spadnie poniżej tej wartości, SLA jest uznawane za będące w stanie problemu/niespełnienia. Możliwe wartości: 0-100 (do 4 cyfr po przecinku). Zachowanie właściwości: - *wymagane* dla operacji tworzenia
effective_date	integer	Data wejścia SLA w życie. Możliwe wartości: znacznik czasu daty w UTC.

Właściwość	Typ	Opis
timezone	string	Strefa czasowa raportowania, na przykład: `Europe/London`, `UTC`. Pełną listę obsługiwanych stref czasowych można znaleźć w dokumentacji PHP. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
status	integer	Status SLA. Możliwe wartości: 0 - *(domyślnie)* SLA wyłączone; 1 - SLA włączone.
description	string	Opis SLA.

Harmonogram SLA

Obiekt harmonogramu SLA definiuje okresy, w których połączone usługi mają działać prawidłowo. Ma następujące właściwości.

Właściwość	Type	Opis
period_from	integer	Czas rozpoczęcia cyklicznego tygodniowego okresu czasu (włącznie). Możliwe wartości: liczba sekund (licząc od niedzieli). Zachowanie właściwości: - *wymagane*
period_to	integer	Czas zakończenia cyklicznego tygodniowego okresu czasu (wyłącznie). Możliwe wartości: liczba sekund (licząc od niedzieli). Zachowanie właściwości: - *wymagane*

Wyłączony czas niedostępności SLA

Obiekt wyłączonego czasu niedostępności definiuje okresy, w których powiązana usługa lub usługi mają być planowo wyłączone z działania, bez wpływu na SLI, np. podczas planowanej konserwacji. Ma następujące właściwości.

Właściwość	Type	Opis
name	string	Nazwa wykluczonego okresu niedostępności. Zachowanie właściwości: - *wymagane*
period_from	integer	Czas rozpoczęcia wykluczonego okresu niedostępności (włącznie). Możliwe wartości: znacznik czasu. Zachowanie właściwości: - *wymagane*
period_to	integer	Czas zakończenia wykluczonego okresu niedostępności (wyłącznie). Możliwe wartości: znacznik czasu. Zachowanie właściwości: - *wymagane*

Znacznik usługi SLA

Obiekt znacznika usługi SLA łączy usługi, które mają zostać uwzględnione w obliczeniach SLA. Ma następujące właściwości.

Właściwość	Type	Opis
tag	string	Nazwa tagu usługi SLA. Zachowanie właściwości: - *wymagane*
operator	integer	Operator tagu usługi SLA. Możliwe wartości: 0 - *(domyślnie)* Równa się; 2 - Zawiera.
value	string	Wartość tagu usługi SLA.

sla.create

Opis

`object sla.create(object/array SLAs)`

Ta metoda umożliwia tworzenie nowych obiektów SLA.

Note:
Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w User roles.

Parametry

`(object/array)` Obiekty SLA do utworzenia.

Oprócz standardowych właściwości SLA, metoda akceptuje następujące parametry.

Parametr	Typ	Opis
service_tags	array	Tagi usług SLA, które mają zostać utworzone dla SLA. Zachowanie parametrów: - *wymagane*
schedule	array	Harmonogram SLA, który ma zostać utworzony dla SLA. Podanie pustego parametru będzie interpretowane jako harmonogram 24x7. Domyślnie: harmonogram 24x7.
excluded_downtimes	array	Wykluczone przestoje SLA, które mają zostać utworzone dla SLA.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory utworzonych SLA we właściwości `slaids`. Kolejność zwróconych identyfikatorów odpowiada kolejności przekazanych SLA.

Przykłady

Tworzenie SLA

Poleć utworzenie wpisu SLA dla: * śledzenia dostępności usług związanych z silnikiem SQL; * niestandardowego harmonogramu obejmującego wszystkie dni robocze, z wyłączeniem ostatniej godziny w sobotę; * daty wejścia w życie przypadającej na ostatni dzień roku 2022; * planowanego przestoju trwającego 1 godzinę i 15 minut, rozpoczynającego się o północy 4 lipca; * włączonego obliczania tygodniowego raportu SLA; * minimalnego akceptowalnego SLO na poziomie 99,9995%.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "sla.create",
    "params": [
        {
            "name": "Czas działania bazy danych",
            "slo": "99.9995",
```

```
            "period": "1",
            "timezone": "America/Toronto",
            "description": "Zapewnienie doskonałej dostępności głównych silników baz danych.",
            "effective_date": 1672444800,
            "status": 1,
            "schedule": [
                {
                    "period_from": 0,
                    "period_to": 601200
                }
            ],
            "service_tags": [
                {
                    "tag": "database",
                    "operator": "0",
                    "value": "mysql"
                },
                {
                    "tag": "database",
                    "operator": "0",
                    "value": "postgresql"
                }
            ],
            "excluded_downtimes": [
                {
                    "name": "Wdrożenie aktualizacji wersji oprogramowania",
                    "period_from": "1648760400",
                    "period_to": "1648764900"
                }
            ]
        }
    ],
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "slaids": [
            "5"
        ]
    },
    "id": 1
}
```

Źródło

CSla::create() w *ui/include/classes/api/services/CSla.php*.

sla.delete

Opis

`object sla.delete(array slaids)`

Ta metoda umożliwia usuwanie wpisów SLA.

> **Note:**
> Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji znajduje się w sekcji Role użytkowników.

Parametry

(array) ID SLA do usunięcia.

Zwracane wartości

(object) Zwraca obiekt zawierający identyfikatory usuniętych SLA we właściwości slaids.

Przykłady

Usuwanie wielu SLA

Usuń dwa wpisy SLA.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "sla.delete",
    "params": [
        "4",
        "5"
    ],
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "slaids": [
            "4",
            "5"
        ]
    },
    "id": 1
}
```

Źródło

CSla::delete() w *ui/include/classes/api/services/CSla.php*.

sla.get

Opis

integer/array sla.get(object parameters)

Metoda umożliwia pobieranie obiektów SLA zgodnie z podanymi parametrami.

Note:
Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywołania metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w User roles.

Parametry

(object) Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
slaids	ID/array	Zwraca tylko SLA o podanych identyfikatorach.
serviceids	ID/array	Zwraca tylko SLA pasujące do określonych usług.
selectSchedule	query	Zwraca właściwość schedule z harmonogramami SLA. Obsługuje count.
selectExcludedDowntimes	query	Zwraca właściwość excluded_downtimes z wykluczonymi przestojami SLA. Obsługuje count.

Parametr	Typ	Opis
selectServiceTags	query	Zwraca właściwość `service_tags` z tagami usług SLA. Obsługuje `count`.
sortfield	string/array	Sortuje wynik według podanych właściwości. Możliwe wartości: `slaid`, `name`, `period`, `slo`, `effective_date`, `timezone`, `status`, `description`.
countOutput	boolean	Te parametry są opisane w komentarzu referencyjnym.
editable	boolean	
excludeSearch	boolean	
filter	object	
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca jedną z opcji:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli parametr `countOutput` został wykorzystany.

Przykłady

Pobieranie wszystkich danych o SLA

Pobieranie danych o wszystkich SLA i ich właściwościach.

Żądanie:

```
{
"jsonrpc": "2.0",
"metoda": "sla.get",
"parametry": {
"wyjście": "rozszerz",
"selectSchedule": ["period_from", "period_to"],
"selectExcludedDowntimes": ["nazwa", "period_from", "period_to"],
"selectServiceTags": ["tag", "operator", "wartość"],
"preservekeys": prawda
},
"id": 1
}
```

Odpowiedź:

```
{
"jsonrpc": "2.0",
"wynik": {
"1": {
"slaid": "1",
"nazwa": "Czas działania bazy danych",
„period”: „1”,

slo”: „99.9995”,

effective_date”: „1672444800”,

timezone”: „America/Toronto”,

status”: „1”,
```

```
description": „Zapewnij doskonały czas sprawności głównych silników baz danych SQL.",

service_tags": [
{
„tag": „database",

„operator": „0",

„value": „mysql"
},
{
„tag": „database",

operator": „0",

„value": „postgresql"
}
],

schedule": [
{
„period_from": „0",

„period_to": „601200"
}
],

excluded_downtimes": [
{
„name": „Wdrażanie aktualizacji wersji oprogramowania",
„okres_od": „1648760400",
„okres_do": „1648764900"
}
]
}
},
„id": 1
}
```


Źródło

CSla:get() w *ui/include/classes/api/services/CSla.php*.

sla.getsli

Opis

`object sla.getsli(object parameters)`

Ta metoda umożliwia obliczenie danych wskaźnika poziomu usługi (SLI) dla umowy o gwarantowanym poziomie usług (SLA).

> **Note:**
> Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object)` Parametry zawierające identyfikator SLA, okresy raportowania oraz opcjonalnie identyfikatory usług, dla których ma zostać obliczony wskaźnik SLI.

Parametr	Typ	Opis
slaid	ID	Identyfikator SLA, dla którego mają zostać zwrócone informacje o dostępności. Zachowanie parametru: - *wymagany*
period_from	timestamp	Początkowy znacznik czasu (włącznie), dla którego ma zostać zaraportowany wskaźnik SLI. Możliwe wartości: znacznik czasu Unix.
period_to	timestamp	Końcowy znacznik czasu (włącznie), dla którego ma zostać zaraportowany wskaźnik SLI. Możliwe wartości: znacznik czasu Unix.
periods	integer	Liczba okresów do zaraportowania. Możliwe wartości: 1-100
serviceids	ID/array	Identyfikatory usług, dla których ma zostać zwrócony wskaźnik SLI.

Podział na okresy

Poniższa tabela przedstawia układ zwracanych wycinków okresów na podstawie kombinacji parametrów.

Note:
Zwracane okresy nie poprzedzają pierwszego dostępnego okresu (na podstawie daty wejścia SLA w życie) i nie wykraczają poza bieżący okres.

Parametry			Zwracane okresy
period_from	**period_to**	**periods**	
-	-	-	Ostatnie 20 okresów, w tym bieżący.
-	-	N	Ostatnie N okresów.
-	specified	-	Ostatnie 20 okresów przed `period_to`.
-	specified	N	Ostatnie N okresów przed `period_to`.
specified	-	-	Pierwsze 20 okresów zaczynając od `period_from`.
specified	-	N	Pierwsze N okresów zaczynając od `period_from`.
specified	specified	-	Do 100 okresów w określonym zakresie.
specified	specified	N	N okresów w określonym zakresie.

Zwracane wartości

`(object)` Zwraca wyniki obliczenia.

Właściwość	Type	Opis
periods	array	Lista raportowanych okresów. Każdy raportowany okres jest reprezentowany jako obiekt składający się z: - `period_from` - `(timestamp)` Początkowy znacznik czasu (włącznie) raportowanego okresu. - `period_to` - `(timestamp)` Końcowy znacznik czasu (wyłącznie) raportowanego okresu. Okresy są sortowane według `period_from`, przy czym najwcześniejsze okresy pojawiają się jako pierwsze.
serviceids	array	Lista identyfikatorów usług w raportowanych okresach. Kolejność sortowania listy nie jest określona. Nawet jeśli parametr `serviceids` został przekazany do metody `sla.getsli`.

Właściwość	Type	Opis
sli	array	Dane SLI (jako **tablica dwuwymiarowa**) dla każdego raportowanego okresu i usługi. Indeks właściwości `periods` jest używany jako **pierwszy** wymiar właściwości `sli`. Indeks właściwości `serviceids` jest używany jako **drugi** wymiar właściwości `sli`.

Dane SLI

Dane SLI zwracane dla każdego raportowanego okresu i serwisu obejmują:

Właściwość	Type	Opis
uptime	integer	Czas, przez jaki serwis znajdował się w stanie *OK* podczas zaplanowanego czasu działania, pomniejszony o wykluczone przestoje.
downtime	integer	Czas, przez jaki serwis znajdował się w stanie *not OK* podczas zaplanowanego czasu działania, pomniejszony o wykluczone przestoje.
sli	float	SLI (procent całkowitego czasu działania), na podstawie czasu działania i przestoju.
error_budget	integer	Budżet błędów (w sekundach), na podstawie SLI i SLO.
excluded_downtimes	array	Tablica wykluczonych przestojów w tym okresie raportowania. Każdy obiekt będzie zawierał następujące parametry: - `name` - (`string`) Nazwa wykluczonego przestoju. - `period_from` - (`timestamp`) Znacznik czasu rozpoczęcia (włącznie) wykluczonego przestoju. - `period_to` - (`timestamp`) Znacznik czasu zakończenia (wyłącznie) wykluczonego przestoju. Wykluczone przestoje są sortowane według `period_from`, przy czym najwcześniejsze okresy są wyświetlane jako pierwsze.

Przykłady

Obliczanie SLI dla dziennego SLA

Pobierz dane SLI dla usług o identyfikatorach „1” i „4”, które są powiązane ze SLA o identyfikatorze „1”. Pobierz dane dla jednego okresu do „1761861599” (30 paź 2025 23:59:59 GMT+0200). Ponieważ okres raportowania SLA jest dzienny, dane SLI są pobierane od „1761775200” (30 paź 2025 00:00:00 GMT+0200) do „1761861600” (31 paź 2025 00:00:00 GMT+0200).

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "sla.getsli",
    "params": {
        "slaid": "1",
        "serviceids": [
            1,
            4
        ],
        "periods": 1,
        "period_to": 1761861599
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
```

```
    "result": {
        "periods": [
            {
                "period_from": 1761775200,
                "period_to": 1761861600
            }
        ],
        "serviceids": [
            1,
            4
        ],
        "sli": [
            [
                {
                    "uptime": 43843,
                    "downtime": 0,
                    "sli": 100,
                    "error_budget": 0,
                    "excluded_downtimes": [
                        {
                            "name": "Maintenance OCT",
                            "period_from": 1761825600,
                            "period_to": 1761829200
                        }
                    ]
                },
                {
                    "uptime": 32225,
                    "downtime": 0,
                    "sli": 100,
                    "error_budget": 0,
                    "excluded_downtimes": []
                }
            ]
        ]
    },
    "id": 1
}
```


Obliczanie SLI dla miesięcznego SLA

Pobierz dane SLI o usługach o identyfikatorach „50”, „60” i „70”, które są powiązane ze SLA o identyfikatorze „5”. Pobierz dane dla trzech okresów rozpoczynających się od „1635724800” (01 lis 2021 00:00:00 UTC). Ponieważ okres raportowania SLA jest miesięczny, dane SLI są pobierane dla następujących trzech miesięcy:

- Od „1635724800” (01 lis 2021 00:00:00 UTC) do „1638316800” (01 gru 2021 00:00:00 UTC)
- Od „1638316800” (01 gru 2021 00:00:00 UTC) do „1640995200” (01 sty 2022 00:00:00 UTC)
- Od „1640995200” (01 sty 2022 00:00:00 UTC) do „1643673600” (01 lut 2022 00:00:00 UTC)

Żądanie:


```
{
    "jsonrpc": "2.0",
    "method": "sla.getsli",
    "params": {
        "slaid": "5",
        "serviceids": [
            50,
            60,
            70
        ],
        "periods": 3,
        "period_from": 1635724800
    },
    "id": 1
```

```
}
```

Odpowiedź:


```
{
    "jsonrpc": "2.0",
    "result": {
        "periods": [
            {
                "period_from": 1635724800,
                "period_to": 1638316800
            },
            {
                "period_from": 1638316800,
                "period_to": 1640995200
            },
            {
                "period_from": 1640995200,
                "period_to": 1643673600
            }
        ],
        "serviceids": [
            50,
            60,
            70
        ],
        "sli": [
            [
                {
                    "uptime": 1186212,
                    "downtime": 0,
                    "sli": 100,
                    "error_budget": 0,
                    "excluded_downtimes": [
                        {
                            "name": "Maintenance Nov 25 - Dec 01",
                            "period_from": 1637836212,
                            "period_to": 1638316800
                        }
                    ]
                },
                {
                    "uptime": 1186212,
                    "downtime": 0,
                    "sli": 100,
                    "error_budget": 0,
                    "excluded_downtimes": [
                        {
                            "name": "Maintenance Nov 25 - Dec 01",
                            "period_from": 1637836212,
                            "period_to": 1638316800
                        }
                    ]
                },
                {
                    "uptime": 1186212,
                    "downtime": 0,
                    "sli": 100,
                    "error_budget": 0,
                    "excluded_downtimes": [
                        {
                            "name": "Maintenance Nov 25 - Dec 01",
                            "period_from": 1637836212,
```

```
                    "period_to": 1638316800
                }
            ]
        }
    ],
    [
        {
            "uptime": 1147548,
            "downtime": 0,
            "sli": 100,
            "error_budget": 0,
            "excluded_downtimes": [
                {
                    "name": "Maintenance Dec 02 - Dec 10",
                    "period_from": 1638439200,
                    "period_to": 1639109652
                }
            ]
        },
        {
            "uptime": 1147548,
            "downtime": 0,
            "sli": 100,
            "error_budget": 0,
            "excluded_downtimes": [
                {
                    "name": "Maintenance Dec 02 - Dec 10",
                    "period_from": 1638439200,
                    "period_to": 1639109652
                }
            ]
        },
        {
            "uptime": 1147548,
            "downtime": 0,
            "sli": 100,
            "error_budget": 0,
            "excluded_downtimes": [
                {
                    "name": "Maintenance Dec 02 - Dec 10",
                    "period_from": 1638439200,
                    "period_to": 1639109652
                }
            ]
        }
    ],
    [
        {
            "uptime": 1674000,
            "downtime": 0,
            "sli": 100,
            "error_budget": 0,
            "excluded_downtimes": []
        },
        {
            "uptime": 1674000,
            "downtime": 0,
            "sli": 100,
            "error_budget": 0,
            "excluded_downtimes": []
        },
        {
```

```
                    "uptime": 1674000,
                    "downtime": 0,
                    "sli": 100,
                    "error_budget": 0,
                    "excluded_downtimes": []
                }
            ]
        ]
    },
    "id": 1
}
```

Źródło

CSla::getSli() w *ui/include/classes/api/services/CSla.php*

sla.update

Opis

`object sla.update(object/array slaids)`

Ta metoda umożliwia aktualizację istniejących wpisów SLA.

> **Note:**
> Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji User roles.

Parametry

`(object/array)` Właściwości SLA do zaktualizowania.

Właściwość `slaid` musi być zdefiniowana dla każdego SLA, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko przekazane właściwości, wszystkie pozostałe pozostaną bez zmian.

Oprócz standardowych właściwości SLA, metoda akceptuje następujące parametry.

Parametr	Type	Opis
service_tags	array	Tagi usług SLA zastępujące bieżące tagi usług SLA.
schedule	array	Harmonogram SLA zastępujący bieżący. Podanie pustego parametru będzie interpretowane jako harmonogram 24x7.
excluded_downtimes	array	Wykluczone przestoje SLA zastępujące bieżące.

Wartości zwracane

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych SLA we właściwości `slaids`.

Przykłady

Aktualizacja tagów usługi

Ustaw SLA o ID „5” tak, aby było obliczane w interwałach miesięcznych dla usług związanych z NoSQL, bez zmiany jego harmonogramu ani wykluczonych przestojów; ustaw SLO na 95%.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "sla.update",
    "params": [
        {
            "slaid": "5",
            "name": "NoSQL Database engines",
            "slo": "95",
            "period": 2,
```

```
            "service_tags": [
                {
                    "tag": "database",
                    "operator": "0",
                    "value": "redis"
                },
                {
                    "tag": "database",
                    "operator": "0",
                    "value": "mongodb"
                }
            ]
        }
    ],
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "slaids": [
            "5"
        ]
    },
    "id": 1
}
```

Zmiana harmonogramu SLA

Przełącz SLA o ID „5” na harmonogram 24x7.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "sla.update",
    "params": {
        "slaid": "5",
        "schedule": []
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "slaids": [
            "5"
        ]
    },
    "id": 1
}
```

Zmiana wykluczonych przestojów dla SLA

Dodaj planowany 4-godzinny przestój związany z rozbudową pamięci RAM w dniu 6 kwietnia 2022 r., zachowując jednocześnie (należy go zdefiniować ponownie) wcześniej istniejący plan aktualizacji oprogramowania z 4 lipca dla SLA o ID „5”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "sla.update",
    "params": {
```

```
        "slaid": "5",
        "excluded_downtimes": [
            {
                "name": "Software version upgrade rollout",
                "period_from": "1648760400",
                "period_to": "1648764900"
            },
            {
                "name": "RAM upgrade",
                "period_from": "1649192400",
                "period_to": "1649206800"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "slaids": [
            "5"
        ]
    },
    "id": 1
}
```

Źródło

CSla::update() w *ui/include/classes/api/services/CSla.php*.

Szablon

Ta klasa jest przeznaczona do pracy z szablonami.

Odwołania do obiektów:

- Szablon
- Tag szablonu

Dostępne metody:

- template.create - tworzenie nowych szablonów
- template.delete - usuwanie szablonów
- template.get - pobieranie szablonów
- template.massadd - dodawanie powiązanych obiektów do szablonów
- template.massremove - usuwanie powiązanych obiektów z szablonów
- template.update - aktualizowanie szablonów

Obiekt szablonu

Następujące obiekty są bezpośrednio powiązane z API `template`.

Szablon

Obiekt szablonu ma następujące właściwości.

Właściwość	Typ	Opis
templateid	ID	ID szablonu. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji

Właściwość	Typ	Opis
description	text	Opis szablonu.
host	string	Nazwa techniczna szablonu. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
name	string	Widoczna nazwa szablonu. Domyślnie: wartość właściwości `host`.
readme	text	Instrukcje konfiguracji specyficzne dla szablonu, wyświetlane w Kreatorze hosta. Obsługuje formatowanie Markdown.
uuid	string	Uniwersalny unikalny identyfikator, używany do łączenia importowanych szablonów z już istniejącymi. Generowany automatycznie, jeśli nie został podany.
vendor_name	string	Nazwa dostawcy szablonu. W przypadku operacji tworzenia zarówno `vendor_name`, jak i `vendor_version` powinny być ustawione albo pozostawione puste. W przypadku operacji aktualizacji `vendor_version` może pozostać puste, jeśli ma wartość w bazie danych.
vendor_version	string	Wersja dostawcy szablonu. W przypadku operacji tworzenia zarówno `vendor_name`, jak i `vendor_version` powinny być ustawione albo pozostawione puste. W przypadku operacji aktualizacji `vendor_name` może pozostać puste, jeśli ma wartość w bazie danych.
wizard_ready	integer	Określa, czy szablon jest dostępny do wyboru w Kreatorze hosta. Możliwe wartości: 0 - *(domyślnie)* Niedostępny. 1 - Dostępny.

Znacznik szablonu

Obiekt znacznika szablonu ma następujące właściwości.

Właściwość	Typ	Opis
tag	string	Nazwa znacznika szablonu. Zachowanie właściwości: - *wymagane*
value	string	Wartość znacznika szablonu. Zachowanie właściwości: - *tylko do odczytu*.
object	integer	Typ obiektu, z którego znacznik został odziedziczony. Możliwe wartości: 0 - szablon. Zachowanie właściwości: - *tylko do odczytu*.
objectid	ID	ID obiektu, z którego znacznik został odziedziczony. Zachowanie właściwości: - *tylko do odczytu*.

template.create

Opis

`object template.create(object/array templates)`

Ta metoda umożliwia tworzenie nowych szablonów.

> **Note:**
> Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Szablony do utworzenia.

Oprócz standardowych właściwości szablonu, metoda akceptuje następujące parametry.

Parametr	Type	Opis
groups	object/array	Grupy szablonów, do których należy dodać szablon. Grupy szablonów muszą mieć zdefiniowaną wyłącznie właściwość `groupid`. Zachowanie parametrów: - *wymagane*
tags	object/array	Tagi szablonu.
templates	object/array	Szablony, które mają zostać podlinkowane do szablonu. Szablony muszą mieć zdefiniowaną wyłącznie właściwość `templateid`.
macros	object/array	Makra użytkownika, które mają zostać utworzone dla szablonu.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory utworzonych szablonów we właściwości `templateids`. Kolejność zwróconych identyfikatorów odpowiada kolejności przekazanych szablonów.

Przykłady

Tworzenie szablonu

Utwórz szablon z tagami i podłącz dwa szablony do tego szablonu.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "template.create",
    "params": {
        "host": "Linux template",
        "groups": {
            "groupid": 1
        },
        "templates": [
            {
                "templateid": "11115"
            },
            {
                "templateid": "11116"
            }
        ],
        "tags": [
            {
                "tag": "host-name",
                "value": "{HOST.NAME}"
            }
        ]
    },
```

```
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "templateids": [
            "11117"
        ]
    },
    "id": 1
}
```

Źródło

CTemplate::create() w *ui/include/classes/api/services/CTemplate.php*.

template.delete

Opis

`object template.delete(array templateIds)`

Ta metoda umożliwia usuwanie szablonów.

Usunięcie szablonu powoduje również usunięcie wszystkich jego encji (pozycji, wyzwalaczy, wykresów itp.) ze wszystkich hostów lub szablonów, z którymi jest powiązany. Aby zachować te encje, najpierw odłącz szablon od odpowiednich hostów lub szablonów za pomocą metod `host.update`, `host.massremove`, `template.update` lub `template.massremove`.

> **Note:**
> Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji znajduje się w sekcji Role użytkowników.

Parametry

`(array)` ID szablonów do usunięcia.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory usuniętych szablonów we właściwości `templateids`.

Przykłady

Usuwanie wielu szablonów

Usuń dwa szablony.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "template.delete",
    "params": [
        "13",
        "32"
    ],
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "templateids": [
            "13",
            "32"
        ]
```

```
    },
    "id": 1
}
```

Źródło

CTemplate::delete() w *ui/include/classes/api/services/CTemplate.php*.

template.get

Opis

`integer/array template.get(object parameters)`

Ta metoda umożliwia pobieranie szablonów zgodnie z podanymi parametrami.

Note:
Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji znajduje się w sekcji Role użytkowników.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Type	Opis
templateids	ID/array	Zwracaj tylko szablony o podanych ID szablonów.
groupids	ID/array	Zwracaj tylko szablony należące do podanych grup szablonów.
parentTemplateids	ID/array	Zwracaj tylko szablony, do których podany szablon jest podłączony.
hostids	ID/array	Zwracaj tylko szablony, które są podłączone do podanych hostów/szablonów.
graphids	ID/array	Zwracaj tylko szablony zawierające podane wykresy.
itemids	ID/array	Zwracaj tylko szablony zawierające podane pozycje.
triggerids	ID/array	Zwracaj tylko szablony zawierające podane wyzwalacze.
with_items	flag	Zwracaj tylko szablony, które mają pozycje.
with_triggers	flag	Zwracaj tylko szablony, które mają wyzwalacze.
with_graphs	flag	Zwracaj tylko szablony, które mają wykresy.
with_httptests	flag	Zwracaj tylko szablony, które mają scenariusze WWW.
evaltype	integer	Metoda oceny tagów. Możliwe wartości: 0 - *(domyślnie)* And/Or; 2 - Or.
tags	object/array	Zwracaj tylko szablony z podanymi tagami. Format: `[{"tag": "<tag>", "value": "<value>", "operator": "<operator>"}, ...]`. Pusta tablica zwraca wszystkie szablony. Możliwe wartości operatora: 0 - *(domyślnie)* Zawiera; 1 - Równa się; 2 - Nie zawiera; 3 - Nie równa się; 4 - Istnieje; 5 - Nie istnieje.
inheritedTags	boolean	Zwracaj szablony, które mają podane `tags` również w podłączonych szablonach. Możliwe wartości: `true` - podłączone szablony również muszą mieć podane tagi; `false` - *(domyślnie)* tagi z podłączonych szablonów są ignorowane.
selectInheritedTags	query	Zwracaj właściwość `inheritedTags` z tagami znajdującymi się na podłączonych szablonach.

Parametr	Type	Opis
selectTags	query	Zwracaj tagi szablonu we właściwości `tags`.
selectDiscoveryRules	query	Zwracaj właściwość `discoveryRules` z regułami LLD szablonu. Obsługuje `count`.
selectHosts	query	Zwracaj hosty podłączone do szablonu we właściwości `hosts`. Obsługuje `count`.
selectTemplateGroups	query	Zwracaj grupy szablonów, do których należy szablon, we właściwości `templategroups`.
selectTemplates	query	Zwracaj szablony, do których podany szablon jest podłączony, we właściwości `templates`. Obsługuje `count`.
selectParentTemplates	query	Zwracaj szablony, które są podłączone do podanego szablonu, we właściwości `parentTemplates`. Obsługuje `count`.
selectHttpTests	query	Zwracaj scenariusze WWW z szablonu we właściwości `httpTests`. Obsługuje `count`.
selectItems	query	Zwracaj pozycje z szablonu we właściwości `items`. Obsługuje `count`.
selectTriggers	query	Zwracaj wyzwalacze z szablonu we właściwości `triggers`. Obsługuje `count`.
selectGraphs	query	Zwracaj wykresy z szablonu we właściwości `graphs`. Obsługuje `count`.
selectMacros	query	Zwracaj makra z szablonu we właściwości `macros`.
selectDashboards	query	Zwracaj pulpity z szablonu we właściwości `dashboards`. Obsługuje `count`.
selectValueMaps	query	Zwracaj właściwość `valuemaps` z mapami wartości szablonu.
limitSelects	integer	Ogranicza liczbę rekordów zwracanych przez podzapytania. Dotyczy następujących podzapytań: `selectTemplates` - wyniki będą sortowane według `name`; `selectHosts` - sortowane według `host`; `selectParentTemplates` - sortowane według `host`; `selectItems` - sortowane według `name`; `selectDiscoveryRules` - sortowane według `name`; `selectTriggers` - sortowane według `description`; `selectGraphs` - sortowane według `name`; `selectDashboards` - sortowane według `name`.
sortfield	string/array	Sortuj wynik według podanych właściwości. Możliwe wartości: `hostid`, `host`, `name`, `status`.
countOutput	boolean	Te parametry są opisane w komentarzu referencyjnym.
editable	boolean	
excludeSearch	boolean	
filter	object	
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Parametr	Type	Opis
selectDiscoveries	query	Zwracaj mechanizmy wykrywania niskiego poziomu z szablonu we właściwości `discoveries`. Obsługuje `count`. To zapytanie jest **przestarzałe**; użyj zamiast tego `selectDiscoveryRules`.

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli został użyty parametr `countOutput`.

Przykłady

Pobieranie szablonów według nazwy

Pobierz wszystkie dane o dwóch szablonach o nazwach „Linux by Zabbix agent” i „Windows by Zabbix agent”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "template.get",
    "params": {
        "output": "extend",
        "filter": {
            "host": [
                "Linux by Zabbix agent",
                "Windows by Zabbix agent"
            ]
        }
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "proxyid": "0",
            "host": "Linux by Zabbix agent",
            "status": "3",
            "ipmi_authtype": "-1",
            "ipmi_privilege": "2",
            "ipmi_username": "",
            "ipmi_password": "",
            "maintenanceid": "0",
            "maintenance_status": "0",
            "maintenance_type": "0",
            "maintenance_from": "0",
            "name": "Linux by Zabbix agent",
            "flags": "0",
            "templateid": "10001",
            "description": "To jest oficjalny szablon Linux. Wymaga Zabbix agent 8.0 lub nowszego.\r\n\r\n
            "tls_connect": "1",
            "tls_accept": "1",
            "tls_issuer": "",
            "tls_subject": "",
            "tls_psk_identity": "",
            "tls_psk": "",
```

```
            "custom_interfaces": "0",
            "uuid": "f8f7908280354f2abeed07dc788c3747",
            "vendor_name": "Zabbix",
            "vendor_version": "8.0-2",
            "proxy_groupid": "0",
            "monitored_by": "0",
            "wizard_ready": "1",
            "readme": "## Przegląd\r\n\r\nTo jest oficjalny szablon Linux. Wymaga Zabbix agent 8.0 lub now
        },
        {
            "proxyid": "0",
            "host": "Windows by Zabbix agent",
            "status": "3",
            "ipmi_authtype": "-1",
            "ipmi_privilege": "2",
            "ipmi_username": "",
            "ipmi_password": "",
            "maintenanceid": "0",
            "maintenance_status": "0",
            "maintenance_type": "0",
            "maintenance_from": "0",
            "name": "Windows by Zabbix agent",
            "flags": "0",
            "templateid": "10081",
            "description": "To jest oficjalny szablon Windows. Wymaga Zabbix agent 8.0 lub nowszego.\r\n\r
            "tls_connect": "1",
            "tls_accept": "1",
            "tls_issuer": "",
            "tls_subject": "",
            "tls_psk_identity": "",
            "tls_psk": "",
            "custom_interfaces": "0",
            "uuid": "13b06904a6bf41cbb795e3193d896340",
            "vendor_name": "Zabbix",
            "vendor_version": "8.0-2",
            "proxy_groupid": "0",
            "monitored_by": "0",
            "wizard_ready": "1",
            "readme": "## Przegląd\r\n\r\nTo jest oficjalny szablon Windows. Wymaga Zabbix agent 8.0 lub n
        }
    ],
    "id": 1
}
```


Pobieranie grup szablonów

Pobierz grupy szablonów, do których należy szablon „Linux by Zabbix agent”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "template.get",
    "params": {
        "output": ["hostid"],
        "selectTemplateGroups": "extend",
        "filter": {
            "host": [
                "Linux by Zabbix agent"
            ]
        }
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "templateid": "10001",
            "templategroups": [
                {
                    "groupid": "10",
                    "name": "Templates/Operating systems",
                    "uuid": "846977d1dfed4968bc5f8bdb363285bc"
                }
            ]
        }
    ],
    "id": 1
}
```

Pobieranie hostów według szablonu

Pobierz hosty, które mają podłączony szablon „10001” (*Linux by Zabbix agent*).

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "template.get",
    "params": {
        "output": "templateid",
        "templateids": "10001",
        "selectHosts": ["hostid", "name"]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "templateid": "10001",
            "hosts": [
                {
                    "hostid": "10084",
                    "name": "Zabbix server"
                },
                {
                    "hostid": "10603",
                    "name": "Host 1"
                },
                {
                    "hostid": "10604",
                    "name": "Host 2"
                }
            ]
        }
    ],
    "id": 1
}
```

Wyszukiwanie według tagów szablonu

Pobierz szablony, które mają tag „host-name” równy „{HOST.NAME}”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "template.get",
    "params": {
        "output": ["hostid"],
        "selectTags": "extend",
        "evaltype": 0,
        "tags": [
            {
                "tag": "host-name",
                "value": "{HOST.NAME}",
                "operator": 1
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "templateid": "10402",
            "tags": [
                {
                    "tag": "host-name",
                    "value": "{HOST.NAME}"
                }
            ]
        }
    ],
    "id": 1
}
```

Zobacz także

- Grupa szablonów
- Szablon
- Makro użytkownika
- Interfejs hosta

Źródło

CTemplate::get() w *ui/include/classes/api/services/CTemplate.php*.

template.massadd

Opis

`object template.massadd(object parameters)`

Ta metoda umożliwia jednoczesne dodanie wielu powiązanych obiektów do podanych szablonów.

> **Note:**
> Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach ról użytkowników. Więcej informacji znajduje się w sekcji Role użytkowników.

Parametry

`(object)` Parametry zawierające identyfikatory szablonów do zaktualizowania oraz obiekty do dodania do szablonów.

Metoda akceptuje następujące parametry.

Parametr	Type	Opis
templates	object/array	Szablony do zaktualizowania. Szablony muszą mieć zdefiniowaną tylko właściwość `templateid`. Zachowanie parametrów: - *wymagane*
groups	object/array	Grupy szablonów do dodania do podanych szablonów. Grupy szablonów muszą mieć zdefiniowaną tylko właściwość `groupid`.
macros	object/array	Makra użytkownika do utworzenia dla podanych szablonów.
templates_link	object/array	Szablony do podlinkowania do podanych szablonów. Szablony muszą mieć zdefiniowaną tylko właściwość `templateid`.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych szablonów we właściwości `templateids`.

Przykłady

Powiąż grupę z szablonami

Dodaj grupę szablonów „2” do dwóch szablonów.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "template.massadd",
    "params": {
        "templates": [
            {
                "templateid": "10085"
            },
            {
                "templateid": "10086"
            }
        ],
        "groups": [
            {
                "groupid": "2"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "templateids": [
            "10085",
            "10086"
        ]
    },
    "id": 1
}
```

Podłącz dwa szablony do szablonu

Podłącz szablony „10106” i „10104” do szablonu „10073”.

Request:

```
{
    "jsonrpc": "2.0",
    "method": "template.massadd",
    "params": {
        "templates": [
            {
                "templateid": "10073"
            }
        ],
        "templates_link": [
            {
                "templateid": "10106"
            },
            {
                "templateid": "10104"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "templateids": [
            "10073"
        ]
    },
    "id": 1
}
```

Zobacz także

- template.update
- Host
- Grupa szablonów
- Makro użytkownika

Źródło

CTemplate::massAdd() w *ui/include/classes/api/services/CTemplate.php*.

template.massremove

Opis

`object template.massremove(object parameters)`

Ta metoda umożliwia usunięcie powiązanych obiektów z wielu szablonów.

Note:
Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji znajduje się w sekcji User roles.

Parametry

`(object)` Parametry zawierające identyfikatory szablonów do zaktualizowania oraz obiekty, które powinny zostać usunięte.

Parametr	Typ	Opis
templateids	ID/array	Identyfikatory szablonów, które mają zostać zaktualizowane. Zachowanie parametru: - *wymagany*

Parametr	Typ	Opis
groupids	ID/array	Identyfikatory grup szablonów, z których należy usunąć podane szablony.
macros	string/array	Identyfikatory makr użytkownika, które mają zostać usunięte z podanych szablonów.
templateids_clear	ID/array	Identyfikatory szablonów, które mają zostać odłączone i wyczyszczone z podanych szablonów (nadrzędnych).
templateids_link	ID/array	Identyfikatory szablonów, które mają zostać odłączone od podanych szablonów (nadrzędnych).

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych szablonów we właściwości `templateids`.

Przykłady

Usuwanie szablonów z grupy

Usuń dwa szablony z grupy „2”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "template.massremove",
    "params": {
        "templateids": [
            "10085",
            "10086"
        ],
        "groupids": "2"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "templateids": [
            "10085",
            "10086"
        ]
    },
    "id": 1
}
```

Odłączanie szablonów od hosta

Odłącz szablony „10106” i „10104” od szablonu „10085”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "template.massremove",
    "params": {
        "templateids": "10085",
        "templateids_link": [
            "10106",
            "10104"
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "templateids": [
            "10085"
        ]
    },
    "id": 1
}
```

Zobacz także

- template.update
- Makro użytkownika

Źródło

CTemplate::massRemove() w *ui/include/classes/api/services/CTemplate.php*.

template.update

Opis

`object template.update(object/array templates)`

Ta metoda umożliwia aktualizację istniejących szablonów.

Note:
Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Właściwości szablonu do zaktualizowania.

Właściwość `templateid` musi być zdefiniowana dla każdego szablonu, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko podane właściwości, wszystkie pozostałe pozostaną bez zmian.

Oprócz standardowych właściwości szablonu metoda akceptuje następujące parametry.

Parametr	Typ	Opis
groups	object/array	Grupy szablonów zastępujące bieżące grupy szablonów, do których należą szablony. Dla grup szablonów musi być zdefiniowana tylko właściwość `groupid`.
tags	object/array	Tagi szablonu zastępujące bieżące tagi szablonu.
macros	object/array	Makra użytkownika zastępujące bieżące makra użytkownika w podanych szablonach.
templates	object/array	Szablony zastępujące aktualnie podlinkowane szablony. Szablony, które nie zostaną przekazane, zostaną jedynie odlinkowane. Dla szablonów musi być zdefiniowana tylko właściwość `templateid`.
templates_clear	object/array	Szablony do odlinkowania i wyczyszczenia z podanych szablonów. Dla szablonów musi być zdefiniowana tylko właściwość `templateid`.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych szablonów we właściwości `templateids`.

Przykłady

Zmiana standardowych właściwości szablonu

Zmień nazwę techniczną szablonu na „Linux by Zabbix agent Custom”, nazwę widoczną na „My template” oraz zaktualizuj opis szablonu.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "template.update",
    "params": {
        "templateid": "10086",
        "host": "Linux by Zabbix agent Custom",
        "name": "My template",
        "description": "This is a custom Linux template."
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "templateids": [
            "10086"
        ]
    },
    "id": 1
}
```

Aktualizowanie grup szablonów

Zastąp wszystkie grupy szablonów dla danego szablonu inną grupą.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "template.update",
    "params": {
        "templateid": "10086",
        "groups": [
            {
                "groupid": "24"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "templateids": [
            "10086"
        ]
    },
    "id": 1
}
```

Aktualizowanie wielu grup szablonów

Zastąp wszystkie grupy szablonów dla wielu szablonów innymi grupami.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "template.update",
    "params": [
        {
```

```
            "templateid": "10086",
            "groups": [
                {
                    "groupid": "24"
                }
            ]
        },
        {
            "templateid": "10087",
            "groups": [
                {
                    "groupid": "1"
                },
                {
                    "groupid": "12"
                }
            ]
        },
        {
            "templateid": "10088",
            "groups": [
                {
                    "groupid": "1"
                },
                {
                    "groupid": "12"
                }
            ]
        }
    ],
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "templateids": [
            "10086",
            "10087",
            "10088"
        ]
    },
    "id": 1
}
```

Aktualizowanie tagów szablonu

Zastąp wszystkie tagi szablonu innym tagiem.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "template.update",
    "params": {
        "templateid": "10086",
        "tags": [
            {
                "tag": "host-name",
                "value": "{HOST.NAME}"
            }
        ]
    },
```

```
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "templateids": [
            "10086"
        ]
    },
    "id": 1
}
```

Aktualizowanie makr szablonu

Zastąp wszystkie makra szablonu innymi.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "template.update",
    "params": {
        "templateid": "10086",
        "macros": [
            {
                "macro": "{$MY_MACRO}",
                "value": "new_value"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "templateids": [
            "10086"
        ]
    },
    "id": 1
}
```

Aktualizowanie wielu makr szablonu

Zastąp wszystkie makra użytkownika podanym makrem użytkownika w wielu szablonach.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "template.update",
    "params": [
            {
                "templateid": "10087",
                "macros": [
                    {
                        "macro": "{$AGENT.TIMEOUT}",
                        "value": "5m",
                        "description": "Limit czasu, po którym agent jest uznawany za niedostępny. Działa
                    }
                ]
            },
```

```
            {
                "templateid": "10088",
                "macros": [
                    {
                        "macro": "{$AGENT.TIMEOUT}",
                        "value": "5m",
                        "description": "Limit czasu, po którym agent jest uznawany za niedostępny. Działa
                    }
                ]
            }
        ],
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "templateids": [
            "10087",
            "10088"
        ]
    },
    "id": 1
}
```

Aktualizacja podłączonych szablonów szablonu

Odłącz (bez czyszczenia) wszystkie szablony od podanego szablonu i podłącz do niego inny.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "template.update",
    "params": {
        "templateid": "10086",
        "templates": [
            {
                "templateid": "10001"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "templateids": [
            "10086"
        ]
    },
    "id": 1
}
```

Czyszczenie wielu podłączonych szablonów szablonu

Odłącz i wyczyść określony podłączony szablon z podanych szablonów.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "template.update",
```

```
    "params": [
        {
            "templateid": "10087",
            "templates_clear": [
                {
                    "templateid": "10001"
                }
            ]
        },
        {
            "templateid": "10088",
            "templates_clear": [
                {
                    "templateid": "10001"
                }
            ]
        }
    ],
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "templateids": [
            "10087",
            "10088"
        ]
    },
    "id": 1
}
```

Źródło

CTemplate::update() w *ui/include/classes/api/services/CTemplate.php*.

Token

Ta klasa jest przeznaczona do pracy z tokenami.

Odwołania do obiektów:

- Token

Dostępne metody:

- token.create - tworzenie nowych tokenów
- token.delete - usuwanie tokenów
- token.get - pobieranie tokenów
- token.update - aktualizowanie tokenów
- token.generate - generowanie tokenów

Obiekt tokena

Następujące obiekty są bezpośrednio powiązane z API `token`.

Token

Obiekt tokenu ma następujące właściwości.

Właściwość	Typ	Opis
tokenid	ID	ID tokenu. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji
name	string	Nazwa tokenu. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
description	text	Opis tokenu.
userid	ID	ID użytkownika, do którego przypisano token. Domyślnie: *bieżący użytkownik*. Zachowanie właściwości: - *stałe*
lastaccess	timestamp	Data i godzina ostatniego uwierzytelnienia tokenu. ”0”, jeśli token nigdy nie został uwierzytelniony. Zachowanie właściwości: - *tylko do odczytu*
status	integer	Status tokenu. Możliwe wartości: 0 - *(domyślnie)* token włączony; 1 - token wyłączony.
expires_at	timestamp	Data i godzina wygaśnięcia tokenu. ”0” dla tokenów, które nigdy nie wygasają.
created_at	timestamp	Data i godzina utworzenia tokenu. Zachowanie właściwości: - *tylko do odczytu*
creator_userid	ID	ID użytkownika, który utworzył token. Zachowanie właściwości: - *tylko do odczytu*

token.create

Opis

`object token.create(object/array tokens)`

Ta metoda umożliwia tworzenie nowych tokenów.

Note:
Uprawnienie *Manage API tokens* permission jest wymagane, aby rola użytkownika mogła zarządzać tokenami innych użytkowników.

Attention:
Token utworzony tą metodą musi również zostać wygenerowany, zanim będzie można go użyć.

Parametry

`(object/array)` Tokeny do utworzenia.

Metoda akceptuje tokeny ze standardowymi właściwościami tokenu.

Zwracane wartości

(object) Zwraca obiekt zawierający identyfikatory utworzonych tokenów we właściwości tokenids. Kolejność zwróconych identyfikatorów odpowiada kolejności przekazanych tokenów.

Przykłady

Utwórz token

Utwórz włączony token, który nigdy nie wygasa i uwierzytelnia użytkownika o ID 2.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "token.create",
    "params": {
        "name": "Your token",
        "userid": "2"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "tokenids": [
            "188"
        ]
    },
    "id": 1
}
```

Utwórz wyłączony token, który wygasa 21 stycznia 2021 roku. Ten token będzie uwierzytelniał bieżącego użytkownika.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "token.create",
    "params": {
        "name": "Your token",
        "status": "1",
        "expires_at": "1611238072"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "tokenids": [
            "189"
        ]
    },
    "id": 1
}
```

Źródło

CToken::create() w *ui/include/classes/api/services/CToken.php*.

token.delete

Opis

`object token.delete(array tokenids)`

Ta metoda umożliwia usuwanie tokenów.

> **Note:**
> Uprawnienie *Zarządzanie Tokenami API* permission jest wymagane dla roli użytkownika, aby zarządzać tokenami dla innych użytkowników.

Parametry

`(array)` ID tokenów do usunięcia.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory usuniętych tokenów we właściwości `tokenids`.

Przykłady

Usuń wiele tokenów

Usuń dwa tokeny.

Żądanie:

```
{
"jsonrpc": "2.0",
"method": "token.delete",
"params": [
"188",
"192"
],
"id": 1
}
```

Odpowiedź:

```
{
"jsonrpc": "2.0",
"result": {
"tokenids": [
"188",
"192"
]
},
"id": 1
}
```

Źródło

CToken::delete() w *ui/include/classes/api/services/CToken.php*.

token.generate

Opis

`object token.generate(array tokenids)`

Ta metoda umożliwia generowanie tokenów.

> **Note:**
> Uprawnienie *Manage API tokens* permission jest wymagane, aby rola użytkownika mogła zarządzać tokenami innych użytkowników.

> **Attention:**
> Token może zostać wygenerowany tą metodą tylko wtedy, gdy został utworzony.

Parametry

`(array)` ID tokenów do wygenerowania.

Zwracane wartości

`(array)` Zwraca tablicę obiektów zawierających identyfikator wygenerowanego tokenu we właściwości `tokenid` oraz wygenerowany ciąg autoryzacyjny we właściwości `token`.

Właściwość	Type	Opis
tokenid	ID	Identyfikator tokenu.
token	string	Wygenerowany ciąg autoryzacyjny dla tego tokenu.

Przykłady

Wygeneruj wiele tokenów

Wygeneruj dwa tokeny.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "token.generate",
    "params": [
        "1",
        "2"
    ],
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "tokenid": "1",
            "token": "bbcfce79a2d95037502f7e9a534906d3466c9a1484beb6ea0f4e7be28e8b8ce2"
        },
        {
            "tokenid": "2",
            "token": "fa1258a83d518eabd87698a96bd7f07e5a6ae8aeb8463cae33d50b91dd21bd6d"
        }
    ],
    "id": 1
}
```

Źródło

CToken::generate() w *ui/include/classes/api/services/CToken.php*.

token.get

Opis

`integer/array token.get(object parameters)`

Ta metoda umożliwia pobieranie tokenów zgodnie z podanymi parametrami.

> **Note:**
> Tylko użytkownik typu *Super admin* może wyświetlać tokeny innych użytkowników.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
tokenids	ID/array	Zwracaj tylko tokeny o podanych identyfikatorach.
userids	ID/array	Zwracaj tylko tokeny utworzone dla podanych użytkowników.

Parametr	Typ	Opis
token	string	Zwracaj tylko tokeny utworzone dla podanego *tokenu uwierzytelniającego*.
valid_at	timestamp	Zwracaj tylko tokeny, które są ważne (nie wygasły) w podanej dacie i czasie.
expired_at	timestamp	Zwracaj tylko tokeny, które są wygasłe (nieważne) w podanej dacie i czasie.
sortfield	string/array	Sortuj wynik według podanych właściwości. Możliwe wartości: `tokenid`, `name`, `lastaccess`, `status`, `expires_at`, `created_at`.
countOutput	boolean	Te parametry są opisane w komentarzu referencyjnym.
excludeSearch	boolean	
filter	object	
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli został użyty parametr `countOutput`.

Przykłady

Pobieranie tokena

Pobierz wszystkie dane tokena o ID „2”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "token.get",
    "params": {
        "output": "extend",
        "tokenids": "2"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "tokenid": "1",
            "name": "The Token",
            "description": "",
            "userid": "1",
            "lastaccess": "0",
            "status": "0",
            "expires_at": "1609406220",
            "created_at": "1611239454",
            "creator_userid": "1"
        }
    ],
```

```
    "id": 1
}
```

Źródło

CToken::get() w *ui/include/classes/api/services/CToken.php*.

token.update

Opis

`object token.update(object/array tokens)`

Ta metoda umożliwia aktualizację istniejących tokenów.

> **Note:**
> Uprawnienie *Manage API tokens* permission jest wymagane, aby rola użytkownika mogła zarządzać tokenami innych użytkowników.

Parametry

`(object/array)` Właściwości tokenów do zaktualizowania.

Właściwość `tokenid` musi być zdefiniowana dla każdego tokenu, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko przekazane właściwości, wszystkie pozostałe pozostaną bez zmian.

Metoda akceptuje tokeny ze standardowymi właściwościami tokenu.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych tokenów we właściwości `tokenids`.

Przykłady

Usuń datę wygaśnięcia tokena

Usuń datę wygaśnięcia z tokena.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "token.update",
    "params": {
        "tokenid": "2",
        "expires_at": "0"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "tokenids": [
            "2"
        ]
    },
    "id": 1
}
```

Źródło

CToken::update() w *ui/include/classes/api/services/CToken.php*.

Trend

Ta klasa została zaprojektowana do pracy z danymi trendów.

Odwołania do obiektów:

- Trend zmiennoprzecinkowy
- Trend całkowitoliczbowy

Dostępne metody:

- trend.get — pobieranie trendów

Obiekt trendu

Następujące obiekty są bezpośrednio powiązane z API `trend`.

Note:
Obiekty trendów różnią się w zależności od typu informacji elementu. Są tworzone przez serwer Zabbix i nie mogą być modyfikowane za pośrednictwem API.

Trend float

Obiekt trendu float ma następujące właściwości.

Właściwość	Typ	Opis
clock	timestamp	Znacznik czasu godziny, dla której obliczono wartość. Na przykład znacznik czasu „04:00:00” oznacza wartości obliczone dla okresu „04:00:00-04:59:59”.
itemid	ID	ID powiązanej pozycji.
num	integer	Liczba wartości, które były dostępne dla danej godziny.
value_min	float	Minimalna wartość godzinowa.
value_avg	float	Średnia wartość godzinowa.
value_max	float	Maksymalna wartość godzinowa.

Trend całkowitoliczbowy

Obiekt trendu całkowitoliczbowego ma następujące właściwości.

Właściwość	Typ	Opis
clock	timestamp	Znacznik czasu godziny, dla której obliczono wartość. Na przykład znacznik czasu „04:00:00” oznacza wartości obliczone dla okresu „04:00:00-04:59:59”.
itemid	ID	ID powiązanej pozycji.
num	integer	Liczba wartości, które były dostępne dla danej godziny.
value_min	integer	Minimalna wartość godzinowa.
value_avg	integer	Średnia wartość godzinowa.
value_max	integer	Maksymalna wartość godzinowa.

trend.get

Opis

`integer/array trend.get(object parameters)`

Ta metoda umożliwia pobieranie danych trendów zgodnie z podanymi parametrami.

Note:
Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w Rolach użytkowników.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Type	Opis
itemids	ID/array	Zwracaj tylko trendy dla podanych identyfikatorów pozycji.
time_from	timestamp	Zwracaj tylko wartości, które zostały zebrane po podanym czasie lub o podanym czasie.
time_till	timestamp	Zwracaj tylko wartości, które zostały zebrane przed podanym czasem lub o podanym czasie.
countOutput	boolean	Policz liczbę pobranych obiektów.
limit	integer	Ogranicz liczbę pobranych obiektów.
output	query	Ustaw właściwości obiektu trendu, które mają zostać zwrócone.

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli został użyty parametr `countOutput`.

Przykłady

Pobieranie danych trendów pozycji

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "trend.get",
    "params": {
        "output": [
            "itemid",
            "clock",
            "num",
            "value_min",
            "value_avg",
            "value_max"
        ],
        "itemids": [
            "23715"
        ],
        "limit": "1"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "itemid": "23715",
            "clock": "1446199200",
            "num": "60",
            "value_min": "0.165",
            "value_avg": "0.2168",
            "value_max": "0.35"
        }
    ],
    "id": 1
}
```

Źródło

CTrend::get() w *ui/include/classes/api/services/CTrend.php*.

Typ nośnika

Ta klasa jest przeznaczona do pracy z typami nośników.

Odwołania do obiektów:

- Typ nośnika
  - Parametry webhooka
  - Parametry skryptu
- Szablon wiadomości

Dostępne metody:

- mediatype.create - utwórz nowe typy nośników
- mediatype.delete - usuń typy nośników
- mediatype.get - pobierz typy nośników
- mediatype.update - zaktualizuj typy nośników

Obiekt typu mediów

Następujące obiekty są bezpośrednio powiązane z API `mediatype`.

Typ nośnika

Obiekt typu nośnika ma następujące właściwości.

Property	Type	Description
mediatypeid	ID	ID typu nośnika. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji
name	string	Nazwa typu nośnika. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
type	integer	Transport używany przez typ nośnika. Możliwe wartości: 0 - E-mail; 1 - Skrypt; 2 - SMS; 4 - Webhook.
exec_path	string	Zachowanie właściwości: - *wymagane* dla operacji tworzenia Nazwa pliku skryptu (np. notification.sh), który znajduje się w katalogu określonym w parametrze konfiguracji serwera AlertScriptsPath.
gsm_modem	string	Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na „Script” Nazwa urządzenia szeregowego modemu GSM.
passwd	string	Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na „SMS” Hasło uwierzytelniające. Zachowanie właściwości: - *obsługiwane*, jeśli `smtp_authentication` jest ustawione na „Normal password”

Property	Type	Description
provider	integer	Dostawca poczty e-mail. Możliwe wartości: 0 - *(domyślnie)* Generic SMTP; 1 - Gmail; 2 - Gmail relay; 3 - Office365; 4 - Office365 relay.
smtp_email	string	Adres e-mail, z którego będą wysyłane powiadomienia. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na „Email”
smtp_helo	string	SMTP HELO. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na „Email”
smtp_server	string	Serwer SMTP. Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na „Email”
smtp_port	integer	Port serwera SMTP, z którym ma zostać nawiązane połączenie. Domyślnie: 25. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na „Email”
smtp_security	integer	Poziom zabezpieczeń połączenia SMTP, który ma być używany. Możliwe wartości: 0 - *(domyślnie)* Brak; 1 - STARTTLS; 2 - SSL/TLS. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na „Email”
smtp_verify_host	integer	Weryfikacja hosta SSL dla SMTP. Możliwe wartości: 0 - *(domyślnie)* Nie; 1 - Tak. Zachowanie właściwości: - *obsługiwane*, jeśli `smtp_security` jest ustawione na „STARTTLS” lub „SSL/TLS”
smtp_verify_peer	integer	Weryfikacja peera SSL dla SMTP. Możliwe wartości: 0 - *(domyślnie)* Nie; 1 - Tak. Zachowanie właściwości: - *obsługiwane*, jeśli `smtp_security` jest ustawione na „STARTTLS” lub „SSL/TLS”

Property	Type	Description
smtp_authentication	integer	Metoda uwierzytelniania SMTP, która ma być używana. Możliwe wartości: 0 - *(domyślnie)* Brak; 1 - Normal password; 2 - OAuth token. Uwierzytelnianie OAuth nie jest dozwolone dla dostawcy poczty e-mail *Office365 relay*. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na „Email”
redirection_url	string	Adres URL frontendu Zabbix, na który nastąpi przekierowanie zwrotne po autoryzacji OAuth. Domyślnie: Wartość właściwości ustawień API `url` z częścią `zabbix.php?action=oauth.authorize` Zachowanie właściwości: - *wymagane*, jeśli `smtp_authentication` jest ustawione na „OAuth token”
client_id	string	Identyfikator klienta zarejestrowany na serwerze autoryzacji OAuth. Zachowanie właściwości: - *wymagane*, jeśli `smtp_authentication` jest ustawione na „OAuth token”
client_secret	string	Sekret klienta zarejestrowany na serwerze autoryzacji OAuth. Dostępny tylko dla użytkownika typu Super Admin. Zachowanie właściwości: - *wymagane*, jeśli `smtp_authentication` jest ustawione na „OAuth token”
authorization_url	string	Adres URL OAuth wraz z parametrami, służący do uzyskania tokenów dostępu i odświeżania. Zachowanie właściwości: - *wymagane*, jeśli `smtp_authentication` jest ustawione na „OAuth token”
token_url	string	Adres URL OAuth służący do wymiany tokenu autoryzacyjnego na tokeny dostępu i odświeżania. Ten adres URL jest również używany przez serwer do odświeżania nieważnego tokenu dostępu. Zachowanie właściwości: - *wymagane*, jeśli `smtp_authentication` jest ustawione na „OAuth token”
tokens_status	integer	Maska bitowa stanu tokenów. Możliwe wartości: 0 - (domyślnie) Oba tokeny zawierają nieprawidłową wartość 1 - Token dostępu zawiera prawidłową wartość 2 - Token odświeżania zawiera prawidłową wartość 3 - Oba tokeny zawierają prawidłową wartość. Zachowanie właściwości: - *obsługiwane*, jeśli `smtp_authentication` jest ustawione na „OAuth token”
access_token	string	Wartość tokenu dostępu OAuth. Zachowanie właściwości: - *wymagane*, jeśli `smtp_authentication` jest ustawione na „OAuth token”

Property	Type	Description
access_token_updated	timestamp	Znacznik czasu ostatniej modyfikacji `access_token` wykonanej przez serwer podczas odświeżania przy użyciu `refresh_token` lub przez API przy zmianach tokenu. Zachowanie właściwości: - *obsługiwane*, jeśli `smtp_authentication` jest ustawione na „OAuth token”
access_expires_in	integer	Czas w sekundach, po którym `access_token` stanie się nieaktualny i będzie wymagał wysłania żądania do `refresh_url`. Jest ustawiany przez serwer Zabbix podczas odświeżania `access_token` lub przez API przy zmianach tokenu. Znacznik czasu jest obliczany przez dodanie wartości `access_token_updated`. Zachowanie właściwości: - *obsługiwane*, jeśli `smtp_authentication` jest ustawione na „OAuth token”
refresh_token	string	Wartość tokenu odświeżania OAuth. Zachowanie właściwości: - *wymagane*, jeśli `smtp_authentication` jest ustawione na „OAuth token”
status	integer	Czy typ nośnika jest włączony. Możliwe wartości: 0 - *(domyślnie)* Włączony; 1 - Wyłączony.
username	string	Nazwa użytkownika. Zachowanie właściwości: - *obsługiwane*, jeśli `smtp_authentication` jest ustawione na „Normal password”
maxsessions	integer	Maksymalna liczba alertów, które mogą być przetwarzane równolegle. Możliwe wartości, jeśli `type` jest ustawione na „SMS”: 1. Możliwe wartości, jeśli `type` jest ustawione na „Email”, „Script” lub „Webhook”: 0-100. Domyślnie: 1.
maxattempts	integer	Maksymalna liczba prób wysłania alertu. Możliwe wartości: 1-100. Domyślnie: 3.
attempt_interval	string	Interwał między kolejnymi próbami ponowienia. Akceptuje sekundy oraz jednostkę czasu z sufiksem. Możliwe wartości: 0-1h. Domyślnie: 10s.
message_format	integer	Format wiadomości. Możliwe wartości: 0 - Zwykły tekst; 1 - *(domyślnie)* HTML. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na „Email”

Property	Type	Description
script	text	Treść skryptu webhook (JavaScript). Zachowanie właściwości: - *wymagane*, jeśli `type` jest ustawione na „Webhook”
timeout	string	Limit czasu skryptu webhook. Akceptuje sekundy oraz jednostkę czasu z sufiksem. Możliwe wartości: 1-60s. Domyślnie: 30s. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na „Webhook”
process_tags	integer	Przetwarzaj wartości właściwości JSON w odpowiedzi skryptu webhook jako tagi. Tagi te są dodawane do wszystkich istniejących tagów problemu. Możliwe wartości: 0 - *(domyślnie)* Ignoruj odpowiedź skryptu webhook; 1 - Przetwarzaj odpowiedź skryptu webhook jako tagi. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na „Webhook”
show_event_menu	integer	Uwzględnij wpis w menu zdarzenia, który prowadzi do niestandardowego adresu URL. Dodaje również właściwość `urls` do danych wyjściowych problem.get i event.get. Możliwe wartości: 0 - *(domyślnie)* Nie uwzględniaj wpisu menu zdarzenia ani właściwości `urls`; 1 - Uwzględnij wpis menu zdarzenia i właściwość `urls`. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na „Webhook”
event_menu_url	string	Adres URL używany we wpisie menu zdarzenia oraz we właściwości `urls` zwracanej przez problem.get i event.get. Zachowanie właściwości: - *obsługiwane*, jeśli `show_event_menu` jest ustawione na „Include event menu entry and `urls` property”
event_menu_name	string	Nazwa używana dla wpisu menu zdarzenia oraz we właściwości `urls` zwracanej przez problem.get i event.get. Zachowanie właściwości: - *obsługiwane*, jeśli `show_event_menu` jest ustawione na „Include event menu entry and `urls` property”
parameters	array	Parametry webhooka lub skryptu. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na „Webhook” lub „Script”
description	text	Opis typu nośnika.

Parametry webhooka

Parametry webhooka mają następujące właściwości.

Właściwość	Type	Opis
name	string	Nazwa parametru. Zachowanie właściwości: - *wymagane*
value	string	Wartość parametru, obsługuje makra. Obsługiwane makra są opisane na stronie Supported macros.

Parametry skryptu

Parametry skryptu mają następujące właściwości.

Właściwość	Type	Opis
sortorder	integer	Kolejność, w jakiej wartości parametrów będą przekazywane do skryptu jako argumenty wiersza poleceń, zaczynając od 0 jako pierwszego argumentu. Zachowanie właściwości: - *wymagane*
value	string	Wartość parametru, obsługuje makra. Obsługiwane makra są opisane na stronie Supported macros.

Szablon wiadomości

Obiekt szablonu wiadomości definiuje szablon, który będzie używany jako domyślna wiadomość dla operacji akcji wysyłających powiadomienie. Ma on następujące właściwości.

Właściwość	Type	Opis
eventsource	integer	Źródło zdarzenia. Możliwe wartości: 0 - Wyzwalacze; 1 - Wykrywanie; 2 - Autorejestracja; 3 - Wewnętrzne; 4 - Usługi. Property behavior: - *required*
recovery	integer	Tryb operacji. Możliwe wartości: 0 - Operacje; 1 - Operacje odzyskiwania; 2 - Operacje aktualizacji. Property behavior: - *required*
subject	string	Temat wiadomości.
message	string	Treść wiadomości.

mediatype.create

Opis

`object mediatype.create(object/array mediaTypes)`

Ta metoda umożliwia tworzenie nowych typów mediów.

Note:
Ta metoda jest dostępna tylko dla użytkownika typu *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Typy mediów do utworzenia.

Oprócz standardowych właściwości typu mediów metoda akceptuje następujące parametry.

Parametr	Type	Opis
message_templates	array	Szablony wiadomości, które mają zostać utworzone dla typu mediów.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory utworzonych typów mediów we właściwości `mediatypeids`. Kolejność zwracanych identyfikatorów odpowiada kolejności przekazanych typów mediów.

Przykłady

Tworzenie typu nośnika e-mail

Utwórz nowy typ nośnika e-mail z niestandardowym portem SMTP i szablonami wiadomości.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "mediatype.create",
    "params": {
        "type": "0",
        "name": "Email",
        "smtp_server": "mail.example.com",
        "smtp_helo": "example.com",
        "smtp_email": "zabbix@example.com",
        "smtp_port": "587",
        "message_format": "1",
        "message_templates": [
            {
                "eventsource": "0",
                "recovery": "0",
                "subject": "Problem: {EVENT.NAME}",
                "message": "Problem \"{EVENT.NAME}\" na hoście \"{HOST.NAME}\" rozpoczął się o {EVENT.TIME
            },
            {
                "eventsource": "0",
                "recovery": "1",
                "subject": "Rozwiązano w {EVENT.DURATION}: {EVENT.NAME}",
                "message": "Problem \"{EVENT.NAME}\" na hoście \"{HOST.NAME}\" został rozwiązany o {EVENT.
            },
            {
                "eventsource": "0",
                "recovery": "2",
                "subject": "Zaktualizowany problem w {EVENT.AGE}: {EVENT.NAME}",
                "message": "{USER.FULLNAME} wykonał(a) akcję {EVENT.UPDATE.ACTION} dla problemu \"{EVENT.N
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
```

```
        "mediatypeids": [
            "7"
        ]
    },
    "id": 1
}
```

Tworzenie typu nośnika skryptu

Utwórz nowy typ nośnika skryptu z niestandardową wartością liczby prób oraz interwału między nimi.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "mediatype.create",
    "params": {
        "type": "1",
        "name": "Push notifications",
        "exec_path": "push-notification.sh",
        "maxattempts": "5",
        "attempt_interval": "11s",
        "parameters": [
            {
                "sortorder": "0",
                "value": "{ALERT.SENDTO}"
            },
            {
                "sortorder": "1",
                "value": "{ALERT.SUBJECT}"
            },
            {
                "sortorder": "2",
                "value": "{ALERT.MESSAGE}"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "mediatypeids": [
            "8"
        ]
    },
    "id": 1
}
```

Tworzenie typu nośnika webhook

Utwórz nowy typ nośnika webhook.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "mediatype.create",
    "params": {
        "type": "4",
        "name": "Webhook",
        "script": "var Webhook = {\r\n    token: null,\r\n    to: null,\r\n    subject: null,\r\n    messa
        "parameters": [
            {
```

```
                "name": "Message",
                "value": "{ALERT.MESSAGE}"
            },
            {
                "name": "Subject",
                "value": "{ALERT.SUBJECT}"
            },
            {
                "name": "To",
                "value": "{ALERT.SENDTO}"
            },
            {
                "name": "Token",
                "value": "<Token>"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "mediatypeids": [
            "9"
        ]
    },
    "id": 1
}
```

Źródło

CMediaType::create() w *ui/include/classes/api/services/CMediaType.php*.

mediatype.delete

Opis

`object mediatype.delete(array mediaTypeIds)`

Ta metoda pozwala na usuwanie typów mediów.

> **Note:**
> Ta metoda jest dostępna tylko dla typu użytkownika *Super admin*. Uprawnienia do wywołania metody można cofnąć w ustawieniach roli użytkownika. Więcej informacji można znaleźć w User roles.

Parametry

`(array)` ID typów mediów do usunięcia.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory usuniętych typów mediów we właściwości `mediatypeids`.

Przykłady

Usuwanie wielu typów mediów

Usuń dwa typy mediów.

Żądanie:

```
{
"jsonrpc": "2.0",
"method": "mediatype.delete",
"params": [
```

```
"3",
"5"
],
"id": 1
}
```

Odpowiedź:

```
{
"jsonrpc": "2.0",
"result": {
"mediatypeids": [
"3",
"5"
]
},
"id": 1
}
```

Źródło

CMediaType::delete() w *ui/include/classes/api/services/CMediaType.php*.

mediatype.get

Opis

`integer/array mediatype.get(object parameters)`

Ta metoda umożliwia pobieranie typów mediów zgodnie z podanymi parametrami.

Note:
Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji User roles.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Note:
Podczas żądania informacji o typach mediów powiązanych z użytkownikiem, użytkownicy typu *Admin* i *User* mogą pobierać dane tylko o własnym użytkowniku. Przykład znajduje się w sekcji Pobieranie typów mediów jako *Admin*.

Parametr	Typ	Opis
mediatypeids	ID/array	Zwracaj tylko typy mediów o podanych ID.
mediaids	ID/array	Zwracaj tylko typy mediów używane przez podane media.
userids	ID/array	Zwracaj tylko typy mediów używane przez podanych użytkowników.
selectActions	query	Zwracaj właściwość `actions` z akcjami używającymi typu mediów.
selectMessageTemplates	query	Zwracaj właściwość `message_templates` z tablicą komunikatów typu mediów. Zachowanie parametru: - *obsługiwane* dla użytkowników typu *Super admin*
selectUsers	query	Zwracaj właściwość `users` z użytkownikami używającymi typu mediów. Ograniczenia zależne od typu użytkownika opisano w `user.get`.
sortfield	string/array	Sortuj wynik według podanych właściwości. Możliwe wartości: `mediatypeid`.

Parametr	Typ	Opis
filter	object	Zwracaj tylko te wyniki, które dokładnie odpowiadają podanemu filtrowi. Akceptuje obiekt, w którym klucze są nazwami właściwości, a wartościami są pojedyncza wartość lub tablica wartości do dopasowania. Nie obsługuje właściwości typu danych `text` data type. Możliwe właściwości obiektu typu mediów dla użytkowników typu *Admin* i *User*: `mediatypeid`, `name`, `type`, `status`, `maxattempts`.
output	query	Właściwości obiektu typu mediów, które mają zostać zwrócone. Użytkownicy typu *Admin* i *User* mogą pobierać tylko następujące właściwości: `mediatypeid`, `name`, `type`, `status`, `maxattempts`, `description`. Przykład znajduje się w sekcji Pobieranie typów mediów jako *Admin*. Domyślnie: `extend`.
search	object	Zwracaj wyniki pasujące do podanego wzorca (bez rozróżniania wielkości liter). Akceptuje obiekt, w którym klucze są nazwami właściwości, a wartościami są ciągi znaków do wyszukania. Jeśli nie podano dodatkowych opcji, zostanie wykonane wyszukiwanie `LIKE "%…%"`. Obsługuje tylko właściwości typu danych `string` i `text` data type. Możliwe właściwości obiektu typu mediów dla użytkowników typu *Admin* i *User*: `name`, `description`.
countOutput	boolean	Te parametry opisano w komentarzu referencyjnym.
editable	boolean	
excludeSearch	boolean	
limit	integer	
preservekeys	boolean	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli został użyty parametr `countOutput`.

Przykłady

Pobieranie typów mediów

Pobierz wszystkie skonfigurowane typy mediów. Poniższy przykład zwraca dwa typy mediów:

- typ mediów e-mail;
- typ mediów SMS.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "mediatype.get",
    "params": {
        "output": "extend",
        "selectMessageTemplates": "extend"
```

```
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "mediatypeid": "1",
            "type": "0",
            "name": "Email",
            "smtp_server": "mail.example.com",
            "smtp_helo": "example.com",
            "smtp_email": "zabbix@example.com",
            "exec_path": "",
            "gsm_modem": "",
            "username": "",
            "passwd": "",
            "status": "0",
            "smtp_port": "25",
            "smtp_security": "0",
            "smtp_verify_peer": "0",
            "smtp_verify_host": "0",
            "smtp_authentication": "0",
            "maxsessions": "1",
            "maxattempts": "3",
            "attempt_interval": "10s",
            "message_format": "0",
            "script": "",
            "timeout": "30s",
            "process_tags": "0",
            "show_event_menu": "1",
            "event_menu_url": "",
            "event_menu_name": "",
            "description": "",
            "provider": "0",
            "message_templates": [
                {
                    "eventsource": "0",
                    "recovery": "0",
                    "subject": "Problem: {EVENT.NAME}",
                    "message": "Problem rozpoczął się o {EVENT.TIME} dnia {EVENT.DATE}\r\nNazwa problemu:
                },
                {
                    "eventsource": "0",
                    "recovery": "1",
                    "subject": "Rozwiązano: {EVENT.NAME}",
                    "message": "Problem został rozwiązany o {EVENT.RECOVERY.TIME} dnia {EVENT.RECOVERY.DAT
                },
                {
                    "eventsource": "0",
                    "recovery": "2",
                    "subject": "Zaktualizowany problem: {EVENT.NAME}",
                    "message": "{USER.FULLNAME} wykonał(a) akcję {EVENT.UPDATE.ACTION} dla problemu dnia {
                },
                {
                    "eventsource": "1",
                    "recovery": "0",
                    "subject": "Wykrywanie: {DISCOVERY.DEVICE.STATUS} {DISCOVERY.DEVICE.IPADDRESS}",
                    "message": "Reguła wykrywania: {DISCOVERY.RULE.NAME}\r\n\r\nIP urządzenia: {DISCOVERY.
                },
```

```
            {
                "eventsource": "2",
                "recovery": "0",
                "subject": "Autorejestracja: {HOST.HOST}",
                "message": "Nazwa hosta: {HOST.HOST}\r\nIP hosta: {HOST.IP}\r\nPort agenta: {HOST.PORT
            }
        ],
        "parameters": []
    },
    {
        "mediatypeid": "3",
        "type": "2",
        "name": "SMS",
        "smtp_server": "",
        "smtp_helo": "",
        "smtp_email": "",
        "exec_path": "",
        "gsm_modem": "/dev/ttyS0",
        "username": "",
        "passwd": "",
        "status": "0",
        "smtp_port": "25",
        "smtp_security": "0",
        "smtp_verify_peer": "0",
        "smtp_verify_host": "0",
        "smtp_authentication": "0",
        "maxsessions": "1",
        "maxattempts": "3",
        "attempt_interval": "10s",
        "message_format": "1",
        "script": "",
        "timeout": "30s",
        "process_tags": "0",
        "show_event_menu": "1",
        "event_menu_url": "",
        "event_menu_name": "",
        "description": "",
        "provider": "0",
        "message_templates": [
            {
                "eventsource": "0",
                "recovery": "0",
                "subject": "",
                "message": "{EVENT.SEVERITY}: {EVENT.NAME}\r\nHost: {HOST.NAME}\r\n{EVENT.DATE} {EVENT
            },
            {
                "eventsource": "0",
                "recovery": "1",
                "subject": "",
                "message": "ROZWIĄZANO: {EVENT.NAME}\r\nHost: {HOST.NAME}\r\n{EVENT.DATE} {EVENT.TIME}
            },
            {
                "eventsource": "0",
                "recovery": "2",
                "subject": "",
                "message": "{USER.FULLNAME} wykonał(a) akcję {EVENT.UPDATE.ACTION} dla problemu dnia {
            },
            {
                "eventsource": "1",
                "recovery": "0",
                "subject": "",
                "message": "Wykrywanie: {DISCOVERY.DEVICE.STATUS} {DISCOVERY.DEVICE.IPADDRESS}"
```

```
                },
                {
                    "eventsource": "2",
                    "recovery": "0",
                    "subject": "",
                    "message": "Autorejestracja: {HOST.HOST}\r\nIP hosta: {HOST.IP}\r\nPort agenta: {HOST.
                }
            ],
            "parameters": []
        }
    ],
    "id": 1
}
```

Pobieranie typów mediów jako *Admin*

Jako użytkownik typu *Admin* pobierz wszystkie typy mediów, które są włączone, wraz z użytkownikami korzystającymi z tych typów mediów. Poniższy przykład zwraca dwa typy mediów:

- typ mediów e-mail z jednym użytkownikiem (tylko własny użytkownik użytkownika typu *Admin*);
- typ mediów SMS bez użytkowników.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "mediatype.get",
    "params": {
        "output": "extend",
        "filter": {
            "status": 0
        },
        "selectUsers": "extend"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "mediatypeid": "1",
            "type": "0",
            "name": "Email",
            "status": "0",
            "description": "",
            "maxattempts": "3",
            "users": [
                {
                    "userid": "3",
                    "username": "database-admin",
                    "name": "John",
                    "surname": "Doe",
                    "url": "",
                    "autologin": "0",
                    "autologout": "0",
                    "lang": "default",
                    "refresh": "30s",
                    "theme": "default",
                    "attempt_failed": "0",
                    "attempt_ip": "",
                    "attempt_clock": "0",
                    "rows_per_page": "50",
                    "timezone": "default",
```

```
                    "roleid": "2",
                    "provisioned": "0"
                }
            ]
        },
        {
            "mediatypeid": "3",
            "type": "2",
            "name": "SMS",
            "status": "0",
            "description": "",
            "maxattempts": "3",
            "users": []
        }
    ],
    "id": 1
}
```

Pobieranie typów nośników skryptu i webhooka

Poniższy przykład zwraca trzy typy nośników:

- typ nośnika skryptu z parametrami;
- typ nośnika skryptu bez parametrów;
- typ nośnika webhooka z parametrami.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "mediatype.get",
    "params": {
        "output": ["mediatypeid", "name", "parameters"],
        "filter": {
            "type": [1, 4]
        }
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "mediatypeid": "10",
            "name": "Script with parameters",
            "parameters": [
                {
                    "sortorder": "0",
                    "value": "{ALERT.SENDTO}"
                },
                {
                    "sortorder": "1",
                    "value": "{EVENT.NAME}"
                },
                {
                    "sortorder": "2",
                    "value": "{ALERT.MESSAGE}"
                },
                {
                    "sortorder": "3",
                    "value": "Zabbix alert"
                }
            ]
```

```
        },
        {
            "mediatypeid": "13",
            "name": "Script without parameters",
            "parameters": []
        },
        {
            "mediatypeid": "11",
            "name": "Webhook",
            "parameters": [
                {
                    "name": "alert_message",
                    "value": "{ALERT.MESSAGE}"
                },
                {
                    "name": "event_update_message",
                    "value": "{EVENT.UPDATE.MESSAGE}"
                },
                {
                    "name": "host_name",
                    "value": "{HOST.NAME}"
                },
                {
                    "name": "trigger_description",
                    "value": "{TRIGGER.DESCRIPTION}"
                },
                {
                    "name": "trigger_id",
                    "value": "{TRIGGER.ID}"
                },
                {
                    "name": "alert_source",
                    "value": "Zabbix"
                }
            ]
        }
    ],
    "id": 1
}
```

Zobacz także

- Użytkownik

Źródło

CMediaType::get() w *ui/include/classes/api/services/CMediaType.php*.

mediatype.update

Opis

`object mediatype.update(object/array mediaTypes)`

Ta metoda umożliwia aktualizację istniejących typów mediów.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkownika typu *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Właściwości typu mediów do zaktualizowania.

Właściwość `mediatypeid` musi być zdefiniowana dla każdego typu mediów, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko przekazane właściwości, wszystkie pozostałe pozostaną bez zmian.

Oprócz standardowych właściwości typu mediów, metoda akceptuje następujące parametry.

Parametr	Typ	Opis
message_templates	array	Szablony wiadomości zastępujące bieżące szablony wiadomości.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych typów mediów we właściwości `mediatypeids`.

Przykłady

Włączanie typu mediów

Włącz typ mediów, czyli ustaw jego status na ”0”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "mediatype.update",
    "params": {
        "mediatypeid": "6",
        "status": "0"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "mediatypeids": [
            "6"
        ]
    },
    "id": 1
}
```

Źródło

CMediaType::update() w *ui/include/classes/api/services/CMediaType.php*.

Ustawienia

Ta klasa została zaprojektowana do pracy z typowymi ustawieniami administracyjnymi.

Odwołania do obiektu:

- Settings

Dostępne metody:

- settings.get - pobieranie ustawień
- settings.update - aktualizacja ustawień

Obiekt ustawień

Następujące obiekty są bezpośrednio powiązane z API `settings`.

Ustawienia

Obiekt ustawień ma następujące właściwości.

Właściwość	Typ	Opis
default_lang	string	Domyślny język systemu. Domyślnie: `en_US`.
default_timezone	string	Domyślna strefa czasowa systemu. Domyślnie: `system` - domyślna strefa systemowa. Pełną listę obsługiwanych stref czasowych można znaleźć w dokumentacji PHP.
default_theme	string	Domyślny motyw. Możliwe wartości: `blue-theme` - *(domyślnie)* Niebieski; `dark-theme` - Ciemny; `hc-light` - Jasny o wysokim kontraście; `hc-dark` - Ciemny o wysokim kontraście.
search_limit	integer	Limit wyników wyszukiwania i filtrowania. Domyślnie: 1000.
max_overview_table_size	integer	Maksymalna liczba kolumn i wierszy w widgetach pulpitu Przegląd danych i Przegląd wyzwalaczy. Domyślnie: 50.
max_in_table	integer	Maksymalna liczba elementów wyświetlanych wewnątrz komórki tabeli. Domyślnie: 50.
server_check_interval	integer	Wyświetlaj ostrzeżenie, jeśli serwer Zabbix jest niedostępny. Możliwe wartości: 0 - Nie wyświetlaj ostrzeżenia; 10 - *(domyślnie)* Wyświetlaj ostrzeżenie.
work_period	string	Czas pracy. Domyślnie: 1-5,09:00-18:00.
show_technical_errors	integer	Wyświetlaj błędy techniczne (PHP/SQL) użytkownikom niebędącym Super adminami oraz użytkownikom, którzy nie należą do grup użytkowników z włączonym trybem debugowania. Możliwe wartości: 0 - *(domyślnie)* Nie wyświetlaj błędów technicznych; 1 - Wyświetlaj błędy techniczne.
history_period	string	Maksymalny okres wyświetlania danych historycznych w widgetach pulpitu Najnowsze dane, Web i Przegląd danych. Akceptuje sekundy oraz jednostkę czasu z sufiksem. Domyślnie: 24h.
period_default	string	Domyślny okres filtra czasu. Akceptuje sekundy oraz jednostkę czasu z sufiksem, z obsługą miesięcy i lat (30s, 1m, 2h, 1d, 1M, 1y). Domyślnie: 1h.
max_period	string	Maksymalny okres dla filtra czasu. Akceptuje sekundy oraz jednostkę czasu z sufiksem, z obsługą miesięcy i lat (30s, 1m, 2h, 1d, 1M, 1y). Domyślnie: 2y.
severity_color_0	string	Kolor ważności „Niesklasyfikowane” jako szesnastkowy kod koloru. Domyślnie: 97AAB3.
severity_color_1	string	Kolor ważności „Informacja” jako szesnastkowy kod koloru. Domyślnie: 7499FF.

Właściwość	Typ	Opis
severity_color_2	string	Kolor ważności „Ostrzeżenie” jako szesnastkowy kod koloru. Domyślnie: FFC859.
severity_color_3	string	Kolor ważności „Średni” jako szesnastkowy kod koloru. Domyślnie: FFA059.
severity_color_4	string	Kolor ważności „Wysoki” jako szesnastkowy kod koloru. Domyślnie: E97659.
severity_color_5	string	Kolor ważności „Katastrofa” jako szesnastkowy kod koloru. Domyślnie: E45959.
severity_name_0	string	Nazwa dla ważności „Niesklasyfikowane”. Domyślnie: Niesklasyfikowane.
severity_name_1	string	Nazwa dla ważności „Informacja”. Domyślnie: Informacja.
severity_name_2	string	Nazwa dla ważności „Ostrzeżenie”. Domyślnie: Ostrzeżenie.
severity_name_3	string	Nazwa dla ważności „Średni”. Domyślnie: Średni.
severity_name_4	string	Nazwa dla ważności „Wysoki”. Domyślnie: Wysoki.
severity_name_5	string	Nazwa dla ważności „Katastrofa”. Domyślnie: Katastrofa.
custom_color	integer	Używaj niestandardowych kolorów statusu zdarzeń. Możliwe wartości: 0 - *(domyślnie)* Nie używaj niestandardowych kolorów statusu zdarzeń; 1 - Używaj niestandardowych kolorów statusu zdarzeń.
ok_period	string	Okres wyświetlania wyzwalaczy OK. Akceptuje sekundy oraz jednostkę czasu z sufiksem. Domyślnie: 5m.
blink_period	string	Okres migania przy zmianie stanu wyzwalacza. Akceptuje sekundy oraz jednostkę czasu z sufiksem. Domyślnie: 2m.
problem_unack_color	string	Kolor niepotwierdzonych zdarzeń PROBLEM jako szesnastkowy kod koloru. Domyślnie: CC0000.
problem_ack_color	string	Kolor potwierdzonych zdarzeń PROBLEM jako szesnastkowy kod koloru. Domyślnie: CC0000.
ok_unack_color	string	Kolor niepotwierdzonych zdarzeń RESOLVED jako szesnastkowy kod koloru. Domyślnie: 009900.
ok_ack_color	string	Kolor potwierdzonych zdarzeń RESOLVED jako szesnastkowy kod koloru. Domyślnie: 009900.

Właściwość	Typ	Opis
problem_unack_style	integer	Miganie dla niepotwierdzonych zdarzeń PROBLEM. Możliwe wartości: 0 - Nie pokazuj migania; 1 - *(domyślnie)* Pokazuj miganie.
problem_ack_style	integer	Miganie dla potwierdzonych zdarzeń PROBLEM. Możliwe wartości: 0 - Nie pokazuj migania; 1 - *(domyślnie)* Pokazuj miganie.
ok_unack_style	integer	Miganie dla niepotwierdzonych zdarzeń RESOLVED. Możliwe wartości: 0 - Nie pokazuj migania; 1 - *(domyślnie)* Pokazuj miganie.
ok_ack_style	integer	Miganie dla potwierdzonych zdarzeń RESOLVED. Możliwe wartości: 0 - Nie pokazuj migania; 1 - *(domyślnie)* Pokazuj miganie.
url	string	Adres URL frontendu.
discovery_groupid	ID	ID grupy hostów, do której będą automatycznie dodawane wykryte hosty.
default_inventory_mode	integer	Domyślny tryb inwentaryzacji hosta. Możliwe wartości: -1 - *(domyślnie)* Wyłączony; 0 - Ręczny; 1 - Automatyczny.
alert_usrgrpid	ID	ID grupy użytkowników, do której będzie wysyłany komunikat alarmowy o niedostępności bazy danych. Jeśli ustawiono „0”, komunikat alarmowy nie zostanie wysłany.
snmptrap_logging	integer	Rejestruj niedopasowane pułapki SNMP. Możliwe wartości: 0 - Nie rejestruj niedopasowanych pułapek SNMP; 1 - *(domyślnie)* Rejestruj niedopasowane pułapki SNMP.
login_attempts	integer	Liczba nieudanych prób logowania, po której formularz logowania zostanie zablokowany. Domyślnie: 5.
login_block	string	Przedział czasu, przez który formularz logowania będzie zablokowany, jeśli liczba nieudanych prób logowania przekroczy wartość zdefiniowaną w polu login_attempts. Akceptuje sekundy oraz jednostkę czasu z sufiksem. Domyślnie: 30s.
validate_uri_schemes	integer	Weryfikuj schematy URI. Możliwe wartości: 0 - Nie weryfikuj; 1 - *(domyślnie)* Weryfikuj.
uri_valid_schemes	string	Prawidłowe schematy URI. Domyślnie: http,https,ftp,file,mailto,tel,ssh.
x_frame_options	string	Nagłówek HTTP X-Frame-Options. Domyślnie: SAMEORIGIN.

Właściwość	Typ	Opis
iframe_sandboxing_enabled	integer	Używaj sandboxingu iframe. Możliwe wartości: 0 - Nie używaj; 1 - *(domyślnie)* Używaj.
iframe_sandboxing_exceptions	string	Wyjątki sandboxingu iframe.
connect_timeout	string	Limit czasu połączenia z serwerem Zabbix. Zakres możliwych wartości: 1-30s. Domyślnie: 3s. Zachowanie właściwości: - *required*
socket_timeout	string	Domyślny limit czasu sieciowego. Zakres możliwych wartości: 1-300s. Domyślnie: 3s. Zachowanie właściwości: - *required*
media_type_test_timeout	string	Sieciowy limit czasu dla testu typu nośnika. Zakres możliwych wartości: 1-300s. Domyślnie: 65s. Zachowanie właściwości: - *required*
item_test_timeout	string	Sieciowy limit czasu dla testów pozycji. Zakres możliwych wartości: 1-600s. Domyślnie: 60s. Zachowanie właściwości: - *required*
script_timeout	string	Sieciowy limit czasu wykonania skryptu. Zakres możliwych wartości: 1-300s. Domyślnie: 60s. Zachowanie właściwości: - *required*
report_test_timeout	string	Sieciowy limit czasu dla testu zaplanowanego raportu. Zakres możliwych wartości: 1-300s. Domyślnie: 60s. Zachowanie właściwości: - *required*
auditlog_enabled	integer	Czy włączyć rejestrowanie audytu. Możliwe wartości: 0 - Wyłącz; 1 - *(domyślnie)* Włącz.

Właściwość	Typ	Opis
auditlog_mode	integer	Czy włączyć rejestrowanie audytu działań wykrywania niskiego poziomu, wykrywania sieci i autorejestracji wykonywanych przez serwer (użytkownik systemowy). Możliwe wartości: 0 - Wyłącz; 1 - *(domyślnie)* Włącz.
ha_failover_delay	string	Opóźnienie przełączenia awaryjnego w sekundach. Domyślnie: 1m. Zachowanie właściwości: - *read-only*
geomaps_tile_provider	string	Dostawca kafelków mapy geograficznej. Możliwe wartości: `OpenStreetMap.Mapnik` - *(domyślnie)* OpenStreetMap Mapnik; `OpenTopoMap` - OpenTopoMap; `Stamen.TonerLite` - Stamen Toner Lite; `Stamen.Terrain` - Stamen Terrain; `USGS.USTopo` - USGS US Topo; `USGS.USImagery` - USGS US Imagery. Obsługuje pusty ciąg znaków w celu określenia niestandardowych wartości `geomaps_tile_url`, `geomaps_max_zoom` i `geomaps_attribution`.
geomaps_tile_url	string	URL kafelków mapy geograficznej. Zachowanie właściwości: - *supported* jeśli `geomaps_tile_provider` jest ustawione na pusty ciąg znaków
geomaps_max_zoom	integer	Maksymalny poziom powiększenia mapy geograficznej. Możliwe wartości: 0-30. Zachowanie właściwości: - *supported* jeśli `geomaps_tile_provider` jest ustawione na pusty ciąg znaków
geomaps_attribution	string	Tekst atrybucji mapy geograficznej. Zachowanie właściwości: - *supported* jeśli `geomaps_tile_provider` jest ustawione na pusty ciąg znaków
vault_provider	integer	Dostawca Vault. Możliwe wartości: 0 - *(domyślnie)* HashiCorp Vault; 1 - CyberArk Vault.
proxy_secrets_provider	integer	Rozwiązuj wartości makr sekretów przez: Możliwe wartości: 0 - *(domyślnie)* tylko serwer; 1 - serwer i proxy niezależnie.

Właściwość	Typ	Opis
timeout_zabbix_agent	string	Na przetwarzanie poświęcaj nie więcej niż `timeout_*` sekund. Akceptuje sekundy lub jednostkę czasu z sufiksem (np. 30s, 1m). Akceptuje również makra użytkownika. Zakres możliwych wartości: 1-600s. Domyślnie: 3s. Domyślnie dla `timeout_browser`: 60s. Zachowanie właściwości: *- required*
timeout_simple_check		
timeout_snmp_agent		
timeout_external_check		
timeout_db_monitor		
timeout_http_agent		
timeout_ssh_agent		
timeout_telnet_agent		
timeout_script		
timeout_browser		

settings.get

Opis

`object settings.get(object parameters)`

Ta metoda umożliwia pobranie obiektu ustawień zgodnie z podanymi parametrami.

> **Note:**
> Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w Rolach użytkowników.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje tylko jeden parametr.

Parametr	Typ	Opis
output	query	Ten parametr jest opisany w komentarzu referencyjnym.

Zwracane wartości

`(object)` Zwraca obiekt ustawień.

Przykłady

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "settings.get",
    "params": {
        "output": "extend"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "default_theme": "blue-theme",
        "search_limit": "1000",
        "max_in_table": "50",
        "server_check_interval": "10",
        "work_period": "1-5,09:00-18:00",
        "show_technical_errors": "0",
        "history_period": "24h",
        "period_default": "1h",
        "max_period": "2y",
        "severity_color_0": "97AAB3",
        "severity_color_1": "7499FF",
        "severity_color_2": "FFC859",
        "severity_color_3": "FFA059",
        "severity_color_4": "E97659",
        "severity_color_5": "E45959",
        "severity_name_0": "Not classified",
        "severity_name_1": "Information",
        "severity_name_2": "Warning",
        "severity_name_3": "Average",
        "severity_name_4": "High",
        "severity_name_5": "Disaster",
        "custom_color": "0",
        "ok_period": "5m",
        "blink_period": "2m",
        "problem_unack_color": "CC0000",
        "problem_ack_color": "CC0000",
        "ok_unack_color": "009900",
        "ok_ack_color": "009900",
        "problem_unack_style": "1",
        "problem_ack_style": "1",
        "ok_unack_style": "1",
        "ok_ack_style": "1",
        "discovery_groupid": "5",
        "default_inventory_mode": "-1",
        "alert_usrgrpid": "7",
        "snmptrap_logging": "1",
        "default_lang": "en_US",
        "default_timezone": "system",
        "login_attempts": "5",
        "login_block": "30s",
        "validate_uri_schemes": "1",
        "uri_valid_schemes": "http,https,ftp,file,mailto,tel,ssh",
        "x_frame_options": "SAMEORIGIN",
        "iframe_sandboxing_enabled": "1",
        "iframe_sandboxing_exceptions": "",
        "max_overview_table_size": "50",
        "connect_timeout": "3s",
        "socket_timeout": "3s",
        "media_type_test_timeout": "65s",
        "script_timeout": "60s",
        "item_test_timeout": "60s",
        "url": "",
        "report_test_timeout": "60s",
        "auditlog_enabled": "1",
        "auditlog_mode": "1",
        "ha_failover_delay": "1m",
        "geomaps_tile_provider": "OpenStreetMap.Mapnik",
        "geomaps_tile_url": "",
        "geomaps_max_zoom": "0",
```

```
        "geomaps_attribution": "",
        "vault_provider": "0",
        "timeout_zabbix_agent": "3s",
        "timeout_simple_check": "3s",
        "timeout_snmp_agent": "3s",
        "timeout_external_check": "3s",
        "timeout_db_monitor": "3s",
        "timeout_http_agent": "3s",
        "timeout_ssh_agent": "3s",
        "timeout_telnet_agent": "3s",
        "timeout_script": "3s"
    },
    "id": 1
}
```

Źródło

CSettings::get() w *ui/include/classes/api/services/CSettings.php*.

settings.update

Opis

`object settings.update(object settings)`

Ta metoda umożliwia aktualizację istniejących wspólnych ustawień.

Note:
Ta metoda jest dostępna tylko dla użytkowników typu *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object)` Właściwości ustawień do zaktualizowania.

Zwracane wartości

`(array)` Zwraca tablicę z nazwami zaktualizowanych parametrów.

Przykłady

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "settings.update",
    "params": {
        "login_attempts": "1",
        "login_block": "1m"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        "login_attempts",
        "login_block"
    ],
    "id": 1
}
```

Źródło

CSettings::update() w *ui/include/classes/api/services/CSettings.php*.

Usługa

Ta klasa jest przeznaczona do pracy z usługami biznesowymi/infrastruktury IT.

Odwołania do obiektów:

- Usługa
- Reguła statusu
- Tag usługi
- Alarm usługi
- Tag problemu

Dostępne metody:

- service.create - utwórz nowe usługi
- service.delete - usuń usługi
- service.get - pobierz usługi
- service.update - zaktualizuj usługi

Obiekt usługi

Następujące obiekty są bezpośrednio powiązane z API `usługi`.

Usługa

Obiekt usługi ma następujące właściwości.

Właściwość	Typ	Opis
serviceid	ID	ID usługi. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji
algorithm	integer	Reguła obliczania statusu. Ma zastosowanie tylko wtedy, gdy istnieją usługi podrzędne. Możliwe wartości: 0 - ustaw status na OK; 1 - najbardziej krytyczny, jeśli wszystkie elementy podrzędne mają problemy; 2 - najbardziej krytyczny spośród usług podrzędnych. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
name	string	Nazwa usługi. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
sortorder	integer	Pozycja usługi używana do sortowania. Możliwe wartości: 0-999. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
weight	integer	Waga usługi. Możliwe wartości: 0-1000000. Domyślnie: 0.

Właściwość	Typ	Opis
propagation_rule	integer	Reguła propagacji statusu. Możliwe wartości: 0 - *(domyślnie)* propaguj status usługi bez zmian; 1 - zwiększ propagowany status o podaną wartość `propagation_value` (o 1 do 5 poziomów ważności); 2 - zmniejsz propagowany status o podaną wartość `propagation_value` (o 1 do 5 poziomów ważności); 3 - ignoruj tę usługę - status w ogóle nie jest propagowany do usługi nadrzędnej; 4 - ustaw stały status usługi przy użyciu podanej wartości `propagation_value`. Zachowanie właściwości: - *wymagane*, jeśli ustawiono `propagation_value`
propagation_value	integer	Wartość propagacji statusu. Możliwe wartości, jeśli `propagation_rule` jest ustawione na „0” lub „3”: 0 - Niesklasyfikowane. Możliwe wartości, jeśli `propagation_rule` jest ustawione na „1” lub „2”: 1 - Informacja; 2 - Ostrzeżenie; 3 - Średni; 4 - Wysoki; 5 - Katastrofa. Możliwe wartości, jeśli `propagation_rule` jest ustawione na „4”: -1 - OK; 0 - Niesklasyfikowane; 1 - Informacja; 2 - Ostrzeżenie; 3 - Średni; 4 - Wysoki; 5 - Katastrofa. Zachowanie właściwości: - *wymagane*, jeśli ustawiono `propagation_rule`
status	integer	Określa, czy usługa jest w stanie OK, czy w stanie problemu. Jeśli usługa jest w stanie problemu, `status` jest równy jednej z następujących wartości: - ważności najbardziej krytycznego problemu; - najwyższemu statusowi usługi podrzędnej będącej w stanie problemu. Jeśli usługa jest w stanie OK, `status` jest równy: -1. Zachowanie właściwości: - *tylko do odczytu*
description	string	Opis usługi.
uuid	string	Uniwersalny unikalny identyfikator używany do łączenia importowanych usług z już istniejącymi. Generowany automatycznie, jeśli nie został podany.
created_at	integer	Znacznik czasu Unix określający moment utworzenia usługi.

Właściwość	Typ	Opis
readonly	integer	Dostęp do usługi. Możliwe wartości: 0 - Odczyt i zapis; 1 - Tylko do odczytu. Zachowanie właściwości: - *tylko do odczytu*

Reguła statusu

Obiekt reguły statusu ma następujące właściwości.

Właściwość	Typ	Opis
type	integer	Warunek ustawienia statusu (Nowy status). Możliwe wartości: 0 - jeśli co najmniej (N) usług podrzędnych ma status (Status) lub wyższy; 1 - jeśli co najmniej (N%) usług podrzędnych ma status (Status) lub wyższy; 2 - jeśli mniej niż (N) usług podrzędnych ma status (Status) lub niższy; 3 - jeśli mniej niż (N%) usług podrzędnych ma status (Status) lub niższy; 4 - jeśli waga usług podrzędnych o statusie (Status) lub wyższym wynosi co najmniej (W); 5 - jeśli waga usług podrzędnych o statusie (Status) lub wyższym wynosi co najmniej (N%); 6 - jeśli waga usług podrzędnych o statusie (Status) lub niższym jest mniejsza niż (W); 7 - jeśli waga usług podrzędnych o statusie (Status) lub niższym jest mniejsza niż (N%). Gdzie: - N (W) to `limit_value`; - (Status) to `limit_status`; - (Nowy status) to `new_status`. Zachowanie właściwości: - *wymagane*
limit_value	integer	Wartość graniczna. Możliwe wartości: - dla N i W: 1-100000; - dla N%: 1-100. Zachowanie właściwości: - *wymagane*

Właściwość	Typ	Opis
limit_status	integer	Status graniczny. Możliwe wartości: -1 - OK; 0 - Niesklasyfikowany; 1 - Informacja; 2 - Ostrzeżenie; 3 - Średni; 4 - Wysoki; 5 - Katastrofa. Zachowanie właściwości: - *wymagane*
new_status	integer	Wartość nowego statusu. Możliwe wartości: 0 - Niesklasyfikowany; 1 - Informacja; 2 - Ostrzeżenie; 3 - Średni; 4 - Wysoki; 5 - Katastrofa. Zachowanie właściwości: - *wymagane*

Znacznik usługi

Obiekt znacznika usługi ma następujące właściwości.

Właściwość	Type	Opis
tag	string	Nazwa znacznika usługi. Zachowanie właściwości: - *wymagane*
value	string	Wartość znacznika usługi.

Alarm usługi

Note:
Alarmów usługi nie można bezpośrednio tworzyć, aktualizować ani usuwać za pomocą Zabbix API.

Obiekty alarmu usługi reprezentują zmianę stanu usługi. Mają następujące właściwości.

Właściwość	Typ	Opis
clock	timestamp	Czas wystąpienia zmiany stanu usługi.
value	integer	Status usługi. Listę możliwych wartości można znaleźć we właściwości `status` usługi.

Znacznik problemu

Znaczniki problemów umożliwiają powiązanie usług ze zdarzeniami problemów. Obiekt znacznika problemu ma następujące właściwości.

Właściwość	Typ	Opis
tag	string	Nazwa znacznika problemu. Zachowanie właściwości: - *wymagane*
operator	integer	Warunek mapowania operator. Możliwe wartości: 0 - *(domyślnie)* Równa się; 2 - Zawiera.
value	string	Wartość znacznika problemu.

service.create

Opis

`object service.create(object/array services)`

Ta metoda umożliwia tworzenie nowych usług.

> **Note:**
> Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` usługi do utworzenia.

Oprócz standardowych właściwości usługi, metoda akceptuje następujące parametry.

Parametr	Typ	Opis
children	array	Podrzędne usługi, które mają zostać powiązane z usługą. Podrzędne usługi muszą mieć zdefiniowaną tylko właściwość `serviceid`.
parents	array	Nadrzędne usługi, które mają zostać powiązane z usługą. Nadrzędne usługi muszą mieć zdefiniowaną tylko właściwość `serviceid`.
tags	array	Tagi usługi, które mają zostać utworzone dla usługi.
problem_tags	array	Tagi problemów, które mają zostać utworzone dla usługi.
status_rules	array	Reguły statusu, które mają zostać utworzone dla usługi.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory utworzonych usług we właściwości `serviceids`. Kolejność zwróconych identyfikatorów odpowiada kolejności przekazanych usług.

Przykłady

Tworzenie usługi

Utwórz usługę, która zostanie przełączona w stan problemu, jeśli co najmniej jedno dziecko ma problem.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "service.create",
    "params": {
        "name": "Server 1",
        "algorithm": 1,
        "sortorder": 1
    },
```

```
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "serviceids": [
            "5"
        ]
    },
    "id": 1
}
```

Źródło

CService::create() w *ui/include/classes/api/services/CService.php*.

service.delete

Opis

`object service.delete(array serviceIds)`

Ta metoda umożliwia usuwanie usług.

Note:
Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach ról użytkowników. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(array)` ID usług do usunięcia.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory usuniętych usług we właściwości `serviceids`.

Przykłady

Usuwanie wielu usług

Usuń dwie usługi.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "service.delete",
    "params": [
        "4",
        "5"
    ],
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "serviceids": [
            "4",
            "5"
        ]
    },
    "id": 1
}
```

Źródło

CService::delete() w *ui/include/classes/api/services/CService.php*.

service.get

Opis

`integer/array service.get(object parameters)`

Ta metoda umożliwia pobieranie usług zgodnie z podanymi parametrami.

> **Note:**
> Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji User roles.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
serviceids	ID/array	Zwracaj tylko usługi o podanych identyfikatorach.
parentids	ID/array	Zwracaj tylko usługi, które są powiązane z podanymi usługami nadrzędnymi.
deep_parentids	flag	Zwracaj wszystkie bezpośrednie i pośrednie usługi podrzędne. Używane razem z `parentids`.
childids	ID/array	Zwracaj tylko usługi, które są powiązane z podanymi usługami podrzędnymi.
evaltype	integer	Metoda oceny tagów. Możliwe wartości: 0 - *(domyślnie)* And/Or; 2 - Or.
tags	object/array	Zwracaj tylko usługi z podanymi tagami. Format: `[{"tag": "<tag>", "value": "<value>", "operator": "<operator>"}, ...]`. Pusta tablica zwraca wszystkie usługi. Możliwe wartości operator: 0 - *(domyślnie)* Zawiera; 1 - Równa się; 2 - Nie zawiera; 3 - Nie równa się; 4 - Istnieje; 5 - Nie istnieje.
problem_tags	object/array	Zwracaj tylko usługi z podanymi tagami problemów. Format: `[{"tag": "<tag>", "value": "<value>", "operator": "<operator>"}, ...]`. Pusta tablica zwraca wszystkie usługi. Możliwe wartości operator: 0 - *(domyślnie)* Zawiera; 1 - Równa się; 2 - Nie zawiera; 3 - Nie równa się; 4 - Istnieje; 5 - Nie istnieje.
without_problem_tags	flag	Zwracaj tylko usługi bez tagów problemów.
slaids	ID/array	Zwracaj tylko usługi, które są powiązane z określonymi SLA.
selectChildren	query	Zwracaj właściwość `children` z usługami podrzędnymi. Obsługuje `count`.

Parametr	Typ	Opis
selectParents	query	Zwracaj właściwość `parents` z usługami nadrzędnymi. Obsługuje `count`.
selectTags	query	Zwracaj właściwość `tags` z tagami usług. Obsługuje `count`.
selectProblemEvents	query	Zwracaj właściwość `problem_events` z tablicą obiektów zdarzeń problemów. Obiekt zdarzenia problemu ma następujące właściwości: `eventid` - `(ID)` ID zdarzenia; `severity` - `(string)` Bieżący poziom ważności zdarzenia; `name` - `(string)` Nazwa rozwiązanego zdarzenia. Obsługuje `count`.
selectProblemTags	query	Zwracaj właściwość `problem_tags` z tagami problemów. Obsługuje `count`.
selectStatusRules	query	Zwracaj właściwość `status_rules` z regułami statusu. Obsługuje `count`.
selectStatusTimeline	object/array	Zwracaj właściwość `status_timeline` zawierającą zmiany stanu usługi dla podanych okresów. Format `[{"period_from": "<period_from>", "period_to": "<period_to>"}, ...]` - gdzie `period_from` jest datą początkową (włącznie; znacznik czasu integer), a `period_to` jest datą końcową (wyłącznie; znacznik czasu integer) dla interesującego Cię okresu. Zwraca tablicę wpisów zawierających właściwość `start_value` oraz tablicę `alarms` dla zmian stanu w określonych okresach.
sortfield	string/array	Sortuj wynik według podanych właściwości. Możliwe wartości: `serviceid`, `name`, `status`, `sortorder`, `created_at`.
countOutput	boolean	Te parametry są opisane w komentarzu referencyjnym.
editable	boolean	
excludeSearch	boolean	
filter	object	
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli został użyty parametr `countOutput`.

Przykłady

Pobieranie wszystkich usług

Pobierz wszystkie dane o wszystkich usługach i ich zależnościach.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "service.get",
    "params": {
        "output": "extend",
        "selectChildren": "extend",
        "selectParents": ["serviceid", "name"]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "serviceid": "1",
            "name": "Zabbix cluster",
            "status": "-1",
            "algorithm": "2",
            "sortorder": "0",
            "weight": "0",
            "propagation_rule": "0",
            "propagation_value": "0",
            "description": "",
            "uuid": "8d77bd91b62347e4b79382912eb5df95",
            "created_at": "1761742392",
            "readonly": false,
            "parents": [],
            "children": [
                {
                    "serviceid": "2",
                    "name": "Zabbix server node 1",
                    "status": "-1",
                    "algorithm": "2",
                    "sortorder": "0",
                    "weight": "0",
                    "propagation_rule": "0",
                    "propagation_value": "0",
                    "description": "",
                    "uuid": "195911d26d7f4e218d6217079bcd5929",
                    "created_at": "1761742623",
                    "readonly": false
                },
                {
                    "serviceid": "3",
                    "name": "Zabbix server node 2",
                    "status": "-1",
                    "algorithm": "2",
                    "sortorder": "0",
                    "weight": "0",
                    "propagation_rule": "0",
                    "propagation_value": "0",
                    "description": "",
                    "uuid": "9fc659a30fe244f690dff25fc2a9db5c",
                    "created_at": "1761742654",
                    "readonly": false
                }
            ]
        },
        {
            "serviceid": "2",
```

```
            "name": "Zabbix server node 1",
            "status": "-1",
            "algorithm": "2",
            "sortorder": "0",
            "weight": "0",
            "propagation_rule": "0",
            "propagation_value": "0",
            "description": "",
            "uuid": "195911d26d7f4e218d6217079bcd5929",
            "created_at": "1761742623",
            "readonly": false,
            "parents": [
                {
                    "serviceid": "1",
                    "name": "Zabbix cluster"
                }
            ],
            "children": []
        },
        {
            "serviceid": "3",
            "name": "Zabbix server node 2",
            "status": "-1",
            "algorithm": "2",
            "sortorder": "0",
            "weight": "0",
            "propagation_rule": "0",
            "propagation_value": "0",
            "description": "",
            "uuid": "9fc659a30fe244f690dff25fc2a9db5c",
            "created_at": "1761742654",
            "readonly": false,
            "parents": [
                {
                    "serviceid": "1",
                    "name": "Zabbix cluster"
                }
            ],
            "children": []
        }
    ],
    "id": 1
}
```


Źródło

CService::get() w *ui/include/classes/api/services/CService.php*.

service.update

Opis

`object service.update(object/array services)`

Ta metoda umożliwia aktualizację istniejących usług.

> **Note:**
> Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` właściwości usługi do zaktualizowania.

Właściwość `serviceid` musi być zdefiniowana dla każdej usługi, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko przekazane właściwości, wszystkie pozostałe pozostaną bez zmian.

Oprócz standardowych właściwości usługi, metoda akceptuje następujące parametry.

Parametr	Type	Opis
children	array	Podrzędne usługi, które zastąpią bieżące usługi podrzędne. Usługi podrzędne muszą mieć zdefiniowaną wyłącznie właściwość `serviceid`.
parents	array	Nadrzędne usługi, które zastąpią bieżące usługi nadrzędne. Usługi nadrzędne muszą mieć zdefiniowaną wyłącznie właściwość `serviceid`.
tags	array	Tagi usługi, które zastąpią bieżące tagi usługi.
problem_tags	array	Tagi problemów, które zastąpią bieżące tagi problemów.
status_rules	array	Reguły statusu, które zastąpią bieżące reguły statusu.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych usług we właściwości `serviceids`.

Przykłady

Ustawianie usługi nadrzędnej dla usługi

Ustaw usługę o ID „3” jako usługę nadrzędną dla usługi o ID „5”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "service.update",
    "params": {
        "serviceid": "5",
        "parents": [
            {
                "serviceid": "3"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "serviceids": [
            "5"
        ]
    },
    "id": 1
}
```

Dodawanie zaplanowanego przestoju

Dodaj przestój dla usługi o ID „4”, zaplanowany co tydzień od poniedziałku 22:00 do wtorku 10:00.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "service.update",
    "params": {
        "serviceid": "4",
        "times": [
```

```
            {
                "type": "1",
                "ts_from": "165600",
                "ts_to": "201600"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "serviceids": [
            "4"
        ]
    },
    "id": 1
}
```

Źródło

CService::update() w *ui/include/classes/api/services/CService.php*.

Uwierzytelnianie

Ta klasa została zaprojektowana do pracy z ustawieniami uwierzytelniania.

Odwołania do obiektów:

- Authentication

Dostępne metody:

- authentication.get - pobieranie ustawień uwierzytelniania
- authentication.update - aktualizowanie ustawień uwierzytelniania

Obiekt uwierzytelniania

Następujące obiekty są bezpośrednio powiązane z API `authentication`.

Uwierzytelnianie

Obiekt uwierzytelniania ma następujące właściwości.

Właściwość	Typ	Opis
authentication_type	integer	Domyślne uwierzytelnianie. Możliwe wartości: 0 - *(domyślnie)* Wewnętrzne; 1 - LDAP.
http_auth_enabled	integer	Uwierzytelnianie HTTP. Możliwe wartości: 0 - *(domyślnie)* Wyłączone; 1 - Włączone. Zachowanie właściwości: - *obsługiwane*, jeśli `$ALLOW_HTTP_AUTH` jest włączone w pliku konfiguracyjnym frontend (*zabbix.conf.php*).

Właściwość	Typ	Opis
http_login_form	integer	Domyślny formularz logowania. Możliwe wartości: 0 - *(domyślnie)* Formularz logowania Zabbix; 1 - Formularz logowania HTTP. Zachowanie właściwości: - *obsługiwane*, jeśli `$ALLOW_HTTP_AUTH` jest włączone w pliku konfiguracyjnym frontend (*zabbix.conf.php*).
http_strip_domains	string	Nazwa domeny do usunięcia. Zachowanie właściwości: - *obsługiwane*, jeśli `$ALLOW_HTTP_AUTH` jest włączone w pliku konfiguracyjnym frontend (*zabbix.conf.php*).
http_case_sensitive	integer	Logowanie HTTP z rozróżnianiem wielkości liter. Możliwe wartości: 0 - Wyłączone; 1 - *(domyślnie)* Włączone. Zachowanie właściwości: - *obsługiwane*, jeśli `$ALLOW_HTTP_AUTH` jest włączone w pliku konfiguracyjnym frontend (*zabbix.conf.php*).
ldap_auth_enabled	integer	Uwierzytelnianie LDAP. Możliwe wartości: 0 - *(domyślnie)* Wyłączone; 1 - Włączone.
ldap_case_sensitive	integer	Logowanie LDAP z rozróżnianiem wielkości liter. Możliwe wartości: 0 - Wyłączone; 1 - *(domyślnie)* Włączone.
ldap_userdirectoryid	ID	ID domyślnego katalogu użytkowników dla uwierzytelniania LDAP. Używane dla grup użytkowników z `gui_access` ustawionym na LDAP lub Domyślne systemowe. Zachowanie właściwości: - *wymagane*, jeśli `ldap_auth_enabled` jest ustawione na ”Enabled”
saml_auth_enabled	integer	Uwierzytelnianie SAML. Możliwe wartości: 0 - *(domyślnie)* Wyłączone; 1 - Włączone.
saml_case_sensitive	integer	Logowanie SAML z rozróżnianiem wielkości liter. Możliwe wartości: 0 - Wyłączone; 1 - *(domyślnie)* Włączone.
passwd_min_length	integer	Wymagana minimalna długość hasła. Możliwe wartości mieszczą się w zakresie od 1 do 70. Domyślnie: 8.

Właściwość	Typ	Opis
passwd_check_rules	integer	Reguły sprawdzania hasła. Możliwe wartości bitmapy: 0 - Sprawdź długość hasła; 1 - Sprawdź, czy hasło zawiera wielkie i małe litery alfabetu łacińskiego; 2 - Sprawdź, czy hasło zawiera cyfry; 4 - Sprawdź, czy hasło zawiera znaki specjalne; 8 - *(domyślnie)* Sprawdź, czy hasło nie znajduje się na liście powszechnie używanych haseł oraz nie zawiera pochodnych słowa ”Zabbix” ani imienia, nazwiska lub nazwy użytkownika. To pole jest maską bitową; akceptowana jest dowolna suma możliwych wartości bitmapy (na przykład 15, aby sprawdzać wszystkie reguły).
ldap_jit_status	integer	Status aprowizacji LDAP. Możliwe wartości: 0 - Wyłączona dla skonfigurowanych dostawców tożsamości LDAP; 1 - Włączona dla skonfigurowanych dostawców tożsamości LDAP.
saml_jit_status	integer	Status aprowizacji SAML. Możliwe wartości: 0 - Wyłączona dla skonfigurowanych dostawców tożsamości SAML; 1 - Włączona dla skonfigurowanych dostawców tożsamości SAML.
jit_provision_interval	string	Przedział czasu między żądaniami aprowizacji JIT dla zalogowanego użytkownika. Akceptuje sekundy oraz jednostkę czasu z sufiksem, z obsługą miesięcy i lat (3600s,60m,1h,1d,1M,1y). Wartość minimalna: 1h. Domyślnie: 1h. Dostępne tylko dla aprowizacji LDAP.
disabled_usrgrpid	ID	ID grupy użytkowników, do której ma zostać przypisany wycofany z aprowizacji użytkownik. Grupa użytkowników musi być wyłączona i nie może zostać włączona ani usunięta, gdy jest skonfigurowana. Zachowanie właściwości: - *wymagane*, jeśli `ldap_jit_status` jest ustawione na ”Enabled for configured LDAP IdPs” lub `saml_jit_status` jest ustawione na ”Enabled for configured SAML IdPs”
mfa_status	integer	Uwierzytelnianie wieloskładnikowe. Możliwe wartości: 0 - Wyłączone (dla wszystkich skonfigurowanych metod MFA); 1 - Włączone (dla wszystkich skonfigurowanych metod MFA).
mfaid	ID	Domyślna metoda MFA dla grup użytkowników z włączonym MFA. Zachowanie właściwości: - *wymagane*, jeśli `mfa_status` jest ustawione na ”Enabled”

authentication.get

Opis

`object authentication.get(object parameters)`

Ta metoda umożliwia pobranie obiektu uwierzytelniania zgodnie z podanymi parametrami.

Note:
Ta metoda jest dostępna tylko dla użytkownika typu *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w Rolach użytkowników.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje tylko jeden parametr.

Parametr	Type	Opis
output	query	Ten parametr jest opisany w komentarzu referencyjnym.

Zwracane wartości

`(object)` Zwraca obiekt uwierzytelniania.

Przykłady

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "authentication.get",
    "params": {
        "output": "extend"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "authentication_type": "0",
        "http_auth_enabled": "0",
        "http_login_form": "0",
        "http_strip_domains": "",
        "http_case_sensitive": "1",
        "ldap_auth_enabled": "0",
        "ldap_case_sensitive": "1",
        "ldap_userdirectoryid": "0",
        "saml_auth_enabled": "0",
        "saml_case_sensitive": "0",
        "passwd_min_length": "8",
        "passwd_check_rules": "15",
        "jit_provision_interval": "1h",
        "saml_jit_status": "0",
        "ldap_jit_status": "0",
        "disabled_usrgrpid": "9",
        "mfa_status": "0",
        "mfaid": "0"
    },
    "id": 1
}
```

Źródło

CAuthentication::get() w *ui/include/classes/api/services/CAuthentication.php*.

authentication.update

Opis

`object authentication.update(object authentication)`

Ta metoda umożliwia aktualizację istniejących ustawień uwierzytelniania.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkownika typu *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object)` Właściwości uwierzytelniania, które mają zostać zaktualizowane.

Zwracane wartości

`(array)` Zwraca tablicę z nazwami zaktualizowanych parametrów.

Przykłady

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "authentication.update",
    "params": {
        "http_auth_enabled": 1,
        "http_case_sensitive": 0,
        "http_login_form": 1
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        "http_auth_enabled",
        "http_case_sensitive",
        "http_login_form"
    ],
    "id": 1
}
```

Źródło

CAuthentication::update() w *ui/include/classes/api/services/CAuthentication.php*.

Użytkownik

Ta klasa została zaprojektowana do pracy z użytkownikami.

Odwołania do obiektów:

- Użytkownik
- Media

Dostępne metody:

- user.checkauthentication - sprawdzanie i przedłużanie sesji użytkownika
- user.create - tworzenie nowych użytkowników
- user.delete - usuwanie użytkowników
- user.get - pobieranie użytkowników
- user.login - logowanie do API
- user.logout - wylogowanie z API
- user.provision - provisionowanie użytkowników LDAP
- user.resettotp - resetowanie sekretów TOTP użytkownika
- user.unblock - odblokowywanie użytkowników
- user.update - aktualizowanie użytkowników

Obiekt użytkownika

Następujące obiekty są bezpośrednio powiązane z API `user`.

Użytkownik

Obiekt użytkownika ma następujące właściwości.

Właściwość	Typ	Opis
userid	ID	ID użytkownika. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji
username	string	Nazwa użytkownika. Zachowanie właściwości: - *wymagane* dla operacji tworzenia - *tylko do odczytu* dla udostępnionych użytkowników, jeśli użytkownik jest powiązany z katalogiem użytkowników (`userdirectoryid` jest ustawione na prawidłową wartość różną od ”0”), a status provisioningu katalogu użytkowników jest włączony (`provision_status` obiektu User directory object jest ustawiony na ”1”), oraz status uwierzytelniania dla całego provisioningu LDAP lub SAML jest włączony (`ldap_jit_status` obiektu Authentication object jest ustawiony na ”Enabled for configured LDAP IdPs” lub `saml_jit_status` obiektu Authentication object jest ustawiony na ”Enabled for configured SAML IdPs”)
passwd	string	Hasło użytkownika. Wartość tego parametru może być pustym ciągiem, jeśli użytkownik jest powiązany z katalogiem użytkowników. Zachowanie właściwości: - *tylko do zapisu*
roleid	ID	ID roli użytkownika. Należy pamiętać, że użytkownicy bez roli mogą logować się do Zabbix wyłącznie przy użyciu uwierzytelniania LDAP lub SAML, pod warunkiem że ich informacje LDAP/SAML odpowiadają mapowaniom grup użytkowników skonfigurowanym w Zabbix.
attempt_clock	timestamp	Czas ostatniej nieudanej próby logowania. Zachowanie właściwości: - *tylko do odczytu*
attempt_failed	integer	Liczba ostatnich nieudanych prób logowania. Zachowanie właściwości: - *tylko do odczytu*
attempt_ip	string	Adres IP, z którego pochodziła ostatnia nieudana próba logowania. Zachowanie właściwości: - *tylko do odczytu*
autologin	integer	Czy włączyć automatyczne logowanie. Możliwe wartości: 0 - *(domyślnie)* automatyczne logowanie wyłączone; 1 - automatyczne logowanie włączone.
autologout	string	Czas życia sesji użytkownika. Akceptuje sekundy oraz jednostkę czasu z sufiksem. Jeśli ustawione na 0s, sesja nigdy nie wygaśnie. Domyślnie: 15m.

Właściwość	Typ	Opis
lang	string	Kod języka użytkownika, na przykład `en_US`. Domyślnie: `default` - domyślny systemowy.
name	string	Imię użytkownika.
provisioned	integer	Czy użytkownik został udostępniony. Możliwe wartości: 0 - nieudostępniony; 1 - udostępniony. Zachowanie właściwości: - *tylko do odczytu*
refresh	string	Okres automatycznego odświeżania. Akceptuje sekundy lub jednostkę czasu z sufiksem (np. 30s, 90s, 1m, 1h). Domyślnie: 30s.
rows_per_page	integer	Liczba wierszy obiektów wyświetlanych na stronę. Domyślnie: 50.
surname	string	Nazwisko użytkownika.
theme	string	Motyw użytkownika. Możliwe wartości: `default` - *(domyślnie)* domyślny systemowy; `blue-theme` - Niebieski; `dark-theme` - Ciemny.
ts_provisioned	timestamp	Czas wykonania ostatniej operacji provisioningu. Zachowanie właściwości: - *tylko do odczytu* - *obsługiwane* dla użytkowników typu *Super admin*
url	string	URL strony, na którą użytkownik ma zostać przekierowany po zalogowaniu.
userdirectoryid	ID	ID katalogu użytkowników, z którym użytkownik jest powiązany. Używane do provisioningu (tworzenia lub aktualizacji), a także do logowania użytkownika powiązanego z katalogiem użytkowników. W operacjach logowania wartość tej właściwości ma priorytet nad właściwością `userdirectoryid` grup użytkowników, do których należy użytkownik. Domyślnie: 0. Zachowanie właściwości: - *tylko do odczytu* - *obsługiwane* dla użytkowników typu *Super admin*
timezone	string	Strefa czasowa użytkownika, na przykład `Europe/London`, `UTC`. Domyślnie: `default` - domyślna systemowa. Pełną listę obsługiwanych stref czasowych można znaleźć w dokumentacji PHP.

Media

Obiekt media ma następujące właściwości.

Property	Type	Description
mediaid	ID	ID media użytkownika. Zachowanie właściwości: - *tylko do odczytu*
mediatypeid	ID	ID typu mediów używanego przez media użytkownika. Zachowanie właściwości: - *wymagane*
sendto	string/array	Adres, nazwa użytkownika lub inny identyfikator odbiorcy. Jeśli `type` typu mediów jest ustawiony na „Email”, wartości są reprezentowane jako tablica. Dla innych typów mediów wartość jest reprezentowana jako ciąg znaków. Zachowanie właściwości: - *wymagane*
active	integer	Określa, czy media są włączone. Możliwe wartości: 0 - *(domyślnie)* włączone; 1 - wyłączone.
severity	integer	Poziomy ważności wyzwalaczy, dla których mają być wysyłane powiadomienia. Możliwe wartości bitmapy: 1 - Niesklasyfikowane; 2 - Informacja; 4 - Ostrzeżenie; 8 - Średni; 16 - Wysoki; 32 - Katastrofa. To pole jest maską bitową; akceptowalna jest dowolna suma możliwych wartości bitmapy (na przykład 48 dla Średni, Wysoki i Katastrofa). Domyślnie: 63.
period	string	Czas, w którym mogą być wysyłane powiadomienia, określony jako okres czasu lub makra użytkownika oddzielone średnikiem. Domyślnie: 1-7,00:00-24:00.
provisioned	integer	Określa, czy użytkownik został provisioned. Możliwe wartości: 0 - nieprovisioned; 1 - provisioned.
userdirectory_mediaid	ID	ID mapowania mediów katalogu użytkowników dla provisioned media. Zachowanie właściwości: - *tylko do odczytu* - *obsługiwane* dla użytkowników typu *Super admin*

user.checkAuthentication

Opis

`object user.checkAuthentication`

Ta metoda sprawdza i przedłuża sesję użytkownika.

Attention:
Wywołanie metody `user.checkAuthentication` z użyciem parametru `sessionid` domyślnie przedłuża sesję użytkownika.

Parametry

Metoda akceptuje następujące parametry.

Parametr	Typ	Opis
extend	boolean	Czy przedłużyć sesję użytkownika. Wartość domyślna: ”true”. Ustawienie wartości na ”false” pozwala sprawdzić sesję użytkownika bez jej przedłużania.
sessionid	string	Zachowanie parametru: - *obsługiwane* jeśli ustawiono `sessionid` Token uwierzytelniania użytkownika.
token	string	Zachowanie parametru: - *wymagane* jeśli `token` nie jest ustawiony Token API użytkownika. Zachowanie parametru: - *wymagane* jeśli `sessionid` nie jest ustawiony

Zwracane wartości

`(object)` Zwraca obiekt zawierający informacje o użytkowniku.

Oprócz standardowych właściwości użytkownika zwracane są następujące informacje.

Właściwość	Type	Opis
auth_type	integer	Domyślne uwierzytelnianie dla użytkownika. Listę możliwych wartości można znaleźć we właściwości `authentication_type` obiektu Authentication object.
debug_mode	integer	Określa, czy tryb debugowania jest włączony czy wyłączony dla użytkownika. Listę możliwych wartości można znaleźć we właściwości `debug_mode` obiektu User group object.
deprovisioned	boolean	Określa, czy użytkownik należy do grupy wycofanych użytkowników.
gui_access	string	Metoda uwierzytelniania użytkownika do frontend. Listę możliwych wartości można znaleźć we właściwości `gui_access` obiektu User group object.
secret	string	Losowy ciąg 32 znaków. Jest generowany podczas logowania użytkownika. Właściwość `secret` nie jest zwracana, jeśli sesja użytkownika jest sprawdzana przy użyciu tokena API.
sessionid	string	Token uwierzytelniający, który musi być używany w kolejnych żądaniach API. Właściwość `sessionid` nie jest zwracana, jeśli sesja użytkownika jest sprawdzana przy użyciu tokena API.
type	integer	Typ użytkownika. Listę możliwych wartości można znaleźć we właściwości `type` obiektu Role object.

Właściwość	Type	Opis
userip	string	Adres IP użytkownika.

Przykłady

Sprawdzenie uwierzytelnienia przy użyciu tokenu uwierzytelniającego

Sprawdź i przedłuż sesję użytkownika przy użyciu tokenu uwierzytelniającego użytkownika oraz zwróć dodatkowe informacje o użytkowniku.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "user.checkAuthentication",
    "params": {
        "sessionid": "673b8ba11562a35da902c66cf5c23fa2"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "userid": "1",
        "username": "Admin",
        "name": "Zabbix",
        "surname": "Administrator",
        "url": "",
        "autologin": "1",
        "autologout": "0",
        "lang": "ru_RU",
        "refresh": "0",
        "theme": "default",
        "attempt_failed": "0",
        "attempt_ip": "127.0.0.1",
        "attempt_clock": "1355919038",
        "rows_per_page": "50",
        "timezone": "Europe/Riga",
        "roleid": "3",
        "userdirectoryid": "0",
        "ts_provisioned": "0",
        "type": 3,
        "userip": "127.0.0.1",
        "debug_mode": 0,
        "gui_access": "0",
        "deprovisioned": false,
        "auth_type": 0,
        "sessionid": "673b8ba11562a35da902c66cf5c23fa2",
        "secret": "0e329b933e46984e49a5c1051ecd0751"
    },
    "id": 1
}
```

Sprawdzenie uwierzytelnienia przy użyciu tokena API

Sprawdź sesję użytkownika przy użyciu tokena API użytkownika i zwróć dodatkowe informacje o użytkowniku.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "user.checkAuthentication",
    "params": {
```

```
        "token": "00aff470e07c12d707e50d98cfe39edef9e6ec349c14728dbdfbc8ddc5ea3eae"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "userid": "1",
        "username": "Admin",
        "name": "Zabbix",
        "surname": "Administrator",
        "url": "",
        "autologin": "1",
        "autologout": "0",
        "lang": "ru_RU",
        "refresh": "0",
        "theme": "default",
        "attempt_failed": "0",
        "attempt_ip": "127.0.0.1",
        "attempt_clock": "1355919338",
        "rows_per_page": "50",
        "timezone": "Europe/Riga",
        "roleid": "3",
        "userdirectoryid": "0",
        "ts_provisioned": "0",
        "debug_mode": 0,
        "deprovisioned": false,
        "gui_access": "1",
        "mfaid": 0,
        "auth_type": 0,
        "type": 3,
        "userip": "127.0.0.1"
    },
    "id": 1
}
```

Źródło

CUser::checkAuthentication() w *ui/include/classes/api/services/CUser.php*.

user.create

Opis

`object user.create(object/array users)`

Ta metoda umożliwia tworzenie nowych użytkowników.

Note:
Ta metoda jest dostępna wyłącznie dla typu użytkownika *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Note:
Siła hasła użytkownika jest weryfikowana zgodnie z regułami polityki haseł zdefiniowanymi przez Authentication API. Więcej informacji można znaleźć w sekcji Authentication API.

Parametry

`(object/array)` Użytkownicy do utworzenia.

Oprócz standardowych właściwości użytkownika metoda akceptuje następujące parametry.

Parametr	Type	Opis
usrgrps	array	Grupy użytkowników, do których użytkownik ma zostać dodany. Grupy użytkowników muszą mieć zdefiniowaną tylko właściwość `usrgrpid`.
medias	array	Media użytkownika, które mają zostać utworzone.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory utworzonych użytkowników we właściwości `userids`. Kolejność zwróconych identyfikatorów odpowiada kolejności przekazanych użytkowników.

Przykłady

Tworzenie użytkownika

Utwórz nowego użytkownika, dodaj go do grupy użytkowników i utwórz dla niego nowe media.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "user.create",
    "params": {
        "username": "John",
        "passwd": "Doe123",
        "roleid": "5",
        "usrgrps": [
            {
                "usrgrpid": "7"
            }
        ],
        "medias": [
            {
                "mediatypeid": "1",
                "sendto": [
                    "support@company.com"
                ],
                "active": 0,
                "severity": 63,
                "period": "1-7,00:00-24:00"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "userids": [
            "12"
        ]
    },
    "id": 1
}
```

Zobacz także

- Uwierzytelnianie
- Media
- Grupa użytkowników
- Rola

Źródło

CUser::create() w *ui/include/classes/api/services/CUser.php*.

user.delete

Opis

`object user.delete(array users)`

Ta metoda umożliwia usuwanie użytkowników.

> **Note:**
> Ta metoda jest dostępna tylko dla typu użytkownika *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji znajduje się w sekcji Role użytkowników.

Parametry

`(array)` ID użytkowników do usunięcia.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory usuniętych użytkowników w we właściwości `userids`.

Przykłady

Usunięcie wielu użytkowników

Usunięcie dwóch użytkowników

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "user.delete",
    "params": [
        "1",
        "5"
    ],
    "auth": "3a57200802b24cda67c4e4010b50c065",
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "userids": [
            "1",
            "5"
        ]
    },
    "id": 1
}
```

Źródło

CUser::delete() w *ui/include/classes/api/services/CUser.php*.

user.get

Opis

`integer/array user.get(object parameters)`

Ta metoda umożliwia pobieranie użytkowników zgodnie z podanymi parametrami.

Note:
Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Note:
Podczas żądania informacji o mediach użytkownika, uprawnieniach lub roli, użytkownicy typu *Admin* i *User* mogą pobierać dane tylko o swoim własnym użytkowniku. Przykład znajduje się w sekcji Pobieranie użytkowników jako *Admin*.

Parametr	Typ	Opis
mediaids	ID/array	Zwracaj tylko użytkowników, którzy używają podanych mediów.
mediatypeids	ID/array	Zwracaj tylko użytkowników, którzy używają podanych typów mediów.
userids	ID/array	Zwracaj tylko użytkowników o podanych ID.
usrgrpids	ID/array	Zwracaj tylko użytkowników należących do podanych grup użytkowników.
getAccess	flag	Dodaje dodatkowe informacje o uprawnieniach użytkownika. Dodaje następujące właściwości dla każdego użytkownika: `gui_access` - `(integer)` metoda uwierzytelniania użytkownika we frontendzie. Listę możliwych wartości można znaleźć we właściwości `gui_access` obiektu grupy użytkowników. `debug_mode` - `(integer)` wskazuje, czy debugowanie jest włączone dla użytkownika. Możliwe wartości: 0 - debugowanie wyłączone, 1 - debugowanie włączone. `users_status` - `(integer)` wskazuje, czy użytkownik jest wyłączony. Możliwe wartości: 0 - użytkownik włączony, 1 - użytkownik wyłączony.
selectMedias	query	Zwracaj media używane przez użytkownika we właściwości `medias`.
selectMediatypes	query	Zwracaj typy mediów używane przez użytkownika we właściwości `mediatypes`. Zobacz `mediatype.get`, aby poznać ograniczenia zależne od typu użytkownika.
selectUsrgrps	query	Zwracaj grupy użytkowników, do których należy użytkownik, we właściwości `usrgrps`. Zobacz `usergroup.get`, aby poznać ograniczenia zależne od typu użytkownika.
selectRole	query	Zwracaj rolę użytkownika we właściwości `role`.
filter	object	Zwracaj tylko te wyniki, które dokładnie odpowiadają podanemu filtrowi. Akceptuje obiekt, w którym kluczami są nazwy właściwości, a wartościami są pojedyncza wartość lub tablica wartości do dopasowania. Nie obsługuje właściwości typu danych `text` data type. Możliwe właściwości obiektu User dla użytkowników typu *Admin* i *User* podczas żądania danych o użytkownikach z ich grupy użytkowników: `userid`, `name`, `surname`, `username`.

Parametr	Typ	Opis
output	query	Właściwości obiektu User, które mają zostać zwrócone. Użytkownicy typu *Admin* i *User* mogą pobierać tylko następujące właściwości: - Dla własnego użytkownika: `userid`, `attempt_clock`, `attempt_failed`, `attempt_ip`, `autologin`, `autologout`, `lang`, `name`, `provisioned`, `refresh`, `roleid`, `rows_per_page`, `surname`, `theme`, `timezone`, `url`, `username`. - Dla użytkowników z ich grupy użytkowników: `userid`, `name`, `surname`, `username`. Domyślnie: `extend`.
search	object	Zwracaj wyniki pasujące do podanego wzorca (bez rozróżniania wielkości liter). Akceptuje obiekt, w którym kluczami są nazwy właściwości, a wartościami są ciągi znaków do wyszukania. Jeśli nie podano dodatkowych opcji, zostanie wykonane wyszukiwanie `LIKE "%…%"`. Obsługuje tylko właściwości typu danych `string` i `text` data type. Możliwe właściwości obiektu User dla użytkowników typu *Admin* i *User* podczas żądania danych o użytkownikach z ich grupy użytkowników: `name`, `surname`, `username`.
sortfield	string/array	Sortuj wynik według podanych właściwości. Możliwe wartości: `userid`, `username`.
countOutput	boolean	Te parametry są opisane w komentarzu referencyjnym.
editable	boolean	
excludeSearch	boolean	
limit	integer	
preservekeys	boolean	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli został użyty parametr `countOutput`.

Przykłady

Pobieranie użytkowników

Pobierz wszystkich skonfigurowanych użytkowników.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "user.get",
    "params": {
        "output": "extend"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
```

```
    "result": [
        {
            "userid": "1",
            "username": "Admin",
            "name": "Zabbix",
            "surname": "Administrator",
            "url": "",
            "autologin": "1",
            "autologout": "0",
            "lang": "en_US",
            "refresh": "0s",
            "theme": "default",
            "attempt_failed": "0",
            "attempt_ip": "",
            "attempt_clock": "0",
            "rows_per_page": "50",
            "timezone": "default",
            "roleid": "3",
            "userdirectoryid": "0",
            "ts_provisioned": "0"
        },
        {
            "userid": "2",
            "username": "guest",
            "name": "",
            "surname": "",
            "url": "",
            "autologin": "0",
            "autologout": "15m",
            "lang": "default",
            "refresh": "30s",
            "theme": "default",
            "attempt_failed": "0",
            "attempt_ip": "",
            "attempt_clock": "0",
            "rows_per_page": "50",
            "timezone": "default",
            "roleid": "4",
            "userdirectoryid": "0",
            "ts_provisioned": "0"
        },
        {
            "userid": "3",
            "username": "user",
            "name": "Zabbix",
            "surname": "User",
            "url": "",
            "autologin": "0",
            "autologout": "0",
            "lang": "ru_RU",
            "refresh": "15s",
            "theme": "dark-theme",
            "attempt_failed": "0",
            "attempt_ip": "",
            "attempt_clock": "0",
            "rows_per_page": "100",
            "timezone": "default",
            "roleid": "1",
            "userdirectoryid": "0",
            "ts_provisioned": "0"
        }
    ],
```

```
    "id": 1
}
```

Pobieranie użytkowników jako *Admin*

Jako użytkownik typu *Admin* pobierz szczegółowe dane o własnym użytkowniku oraz ograniczone dane użytkowników z własnej grupy użytkowników.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "user.get",
    "params": {
        "output": "extend",
        "getAccess": true,
        "selectMedias": "extend",
        "selectMediatypes": "extend",
        "selectUsrgrps": "extend",
        "selectRole": "extend"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "userid": "1",
            "username": "Admin",
            "name": "Zabbix",
            "surname": "Administrator",
            "usrgrps": [
                {
                    "usrgrpid": "7",
                    "name": "Zabbix administrators",
                    "gui_access": "0",
                    "users_status": "0",
                    "debug_mode": "0",
                    "mfa_status": "0"
                }
            ]
        },
        {
            "userid": "3",
            "username": "database-admin",
            "name": "John",
            "surname": "Doe",
            "url": "",
            "autologin": "0",
            "autologout": "0",
            "lang": "default",
            "refresh": "30s",
            "theme": "default",
            "attempt_failed": "0",
            "attempt_ip": "",
            "attempt_clock": "0",
            "rows_per_page": "50",
            "timezone": "default",
            "roleid": "2",
            "provisioned": "0",
            "gui_access": "0",
            "debug_mode": "0",
```

```
            "users_status": "0",
            "usrgrps": [
                {
                    "usrgrpid": "7",
                    "name": "Zabbix administrators",
                    "gui_access": "0",
                    "users_status": "0",
                    "debug_mode": "0",
                    "mfa_status": "0"
                }
            ],
            "medias": [
                {
                    "mediaid": "2",
                    "mediatypeid": "1",
                    "sendto": [
                        "john.doe@example.com"
                    ],
                    "active": "0",
                    "severity": "63",
                    "period": "1-7,00:00-24:00",
                    "provisioned": 0
                }
            ],
            "mediatypes": [
                {
                    "mediatypeid": "1",
                    "type": "0",
                    "name": "Email",
                    "status": "0",
                    "description": "",
                    "maxattempts": "3"
                }
            ],
            "role": {
                "roleid": "2",
                "name": "Admin role",
                "type": "2",
                "readonly": "0"
            }
        }
    ],
    "id": 1
}
```

Pobieranie danych użytkownika

Pobierz dane użytkownika o ID „12”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "user.get",
    "params": {
        "output": ["userid", "username"],
        "selectRole": "extend",
        "userids": "12"
    },
    "id": 1
}
```

Odpowiedź:

```
{
  "jsonrpc": "2.0",
  "result": [
      {
          "userid": "12",
          "username": "John",
          "role": {
              "roleid": "5",
              "name": "Operator",
              "type": "1",
              "readonly": "0"
          }
      }
  ],
  "id": 1
}
```


Zobacz także

- Media
- Typ nośnika
- Grupa użytkowników
- Rola

Źródło

CUser::get() w *ui/include/classes/api/services/CUser.php*.

user.login

Opis

`string/object user.login(object parameters)`

Ta metoda umożliwia zalogowanie się do API i wygenerowanie tokenu uwierzytelniającego.

Warning:
Podczas korzystania z tej metody należy również wykonać user.logout, aby zapobiec generowaniu dużej liczby rekordów otwartych sesji.

Attention:
Ta metoda jest dostępna tylko dla nieuwierzytelnionych użytkowników, którzy nie należą do żadnej grupy użytkowników z włączonym uwierzytelnianiem wieloskładnikowym.

Parametry

`(object)` Parametry zawierające nazwę użytkownika i hasło.

Metoda akceptuje następujące parametry.

Parametr	Typ	Opis
password	string	Hasło użytkownika. Zachowanie parametru: - *wymagany*
username	string	Nazwa użytkownika. Zachowanie parametru: - *wymagany*
userData	flag	Zwraca informacje o uwierzytelnionym użytkowniku.

Zwracane wartości

(string/object) Jeśli używany jest parametr userData, zwracany jest obiekt zawierający informacje o uwierzytelnionym użytkowniku.

Oprócz standardowych właściwości użytkownika zwracane są następujące informacje:

Właściwość	Typ	Opis
auth_type	integer	Domyślna metoda uwierzytelniania dla użytkownika. Listę możliwych wartości można znaleźć we właściwości authentication_type obiektu Authentication object.
debug_mode	integer	Określa, czy tryb debugowania jest włączony czy wyłączony dla użytkownika. Listę możliwych wartości można znaleźć we właściwości debug_mode obiektu User group object.
deprovisioned	boolean	Określa, czy użytkownik należy do grupy wycofanych użytkowników.
gui_access	string	Metoda uwierzytelniania użytkownika do frontendu. Listę możliwych wartości można znaleźć we właściwości gui_access obiektu User group object.
mfaid	integer	ID metody MFA, która ma być używana dla użytkownika podczas logowania. Zwraca "0", jeśli MFA jest globalnie wyłączone lub wyłączone dla wszystkich grup użytkowników, do których należy użytkownik.
secret	string	Losowy ciąg 32 znaków. Jest generowany podczas logowania użytkownika.
sessionid	string	Token uwierzytelniający, który musi być używany w kolejnych żądaniach API.
type	integer	Typ użytkownika. Listę możliwych wartości można znaleźć we właściwości type obiektu Role object.
userip	string	Adres IP użytkownika.

Note:
Jeśli użytkownik został pomyślnie uwierzytelniony po jednej lub większej liczbie nieudanych prób, metoda zwróci bieżące wartości właściwości attempt_clock, attempt_failed i attempt_ip, a następnie je zresetuje.

Jeśli parametr userData nie jest używany, metoda zwraca token uwierzytelniający wymagany do uwierzytelniania.

Przykłady

Uwierzytelnianie użytkownika

Uwierzytelnij użytkownika.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "user.login",
    "params": {
        "username": "Admin",
        "password": "zabbix"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": "0424bd59b807674191e7d77572075f33",
```

```
    "id": 1
}
```

Żądanie informacji o uwierzytelnionym użytkowniku

Uwierzytelnij i zwróć dodatkowe informacje o użytkowniku.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "user.login",
    "params": {
        "username": "Admin",
        "password": "zabbix",
        "userData": true
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "userid": "1",
        "username": "Admin",
        "name": "Zabbix",
        "surname": "Administrator",
        "url": "",
        "autologin": "1",
        "autologout": "0",
        "lang": "ru_RU",
        "refresh": "0",
        "theme": "default",
        "attempt_failed": "0",
        "attempt_ip": "127.0.0.1",
        "attempt_clock": "1355919038",
        "rows_per_page": "50",
        "timezone": "Europe/Riga",
        "roleid": "3",
        "userdirectoryid": "0",
        "type": 3,
        "userip": "127.0.0.1",
        "debug_mode": 0,
        "gui_access": "0",
        "mfaid": "1",
        "deprovisioned": false,
        "auth_type": 0,
        "sessionid": "5b56eee8be445e98f0bd42b435736e42",
        "secret": "cd0ba923319741c6586f3d866423a8f4"
    },
    "id": 1
}
```

Zobacz także

- user.logout

Źródło

CUser::login() w *ui/include/classes/api/services/CUser.php*.

user.logout

Opis

`string/object user.logout(array)`

Ta metoda umożliwia wylogowanie z API i unieważnia bieżący token uwierzytelniający.

> **Note:**
> Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(array)` Metoda akceptuje pustą tablicę.

Zwracane wartości

`(boolean)` Zwraca `true`, jeśli użytkownik został pomyślnie wylogowany.

Przykłady

Wylogowanie

Wyloguj się z API.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "user.logout",
    "params": [],
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": true,
    "id": 1
}
```

Zobacz także

- user.login

Źródło

CUser::login() w *ui/include/classes/api/services/CUser.php*.

user.provision

Opis

`object user.provision(object/array users)`

Ta metoda umożliwia provisionowanie użytkowników LDAP.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkownika typu *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji znajduje się w Rolach użytkowników.

Parametry

`(array)` ID użytkowników do provisioningu.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory provisioned users we właściwości `userids`.

Przykłady

Provisionowanie wielu użytkowników

Provisionuj dwóch użytkowników.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "user.provision",
    "params": [
        "1",
        "5"
    ],
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "userids": [
            "1",
            "5"
        ]
    },
    "id": 1
}
```

Źródło

CUser::provision() w *ui/include/classes/api/services/CUser.php*.

user.resettotp

Opis

`object user.resettotp(object/array users)`

Ta metoda umożliwia resetowanie sekretów TOTP użytkowników.

> **Note:**
> Ta metoda jest dostępna tylko dla typu użytkownika *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(array)` ID użytkowników, dla których należy zresetować sekrety TOTP.

> **Note:**
> Sesje użytkowników dla wskazanych użytkowników również zostaną usunięte (z wyjątkiem użytkownika wysyłającego żądanie).

Wartości zwracane

`(object)` Zwraca obiekt zawierający identyfikatory użytkowników, dla których sekrety TOTP zostały zresetowane, we właściwości `userids`.

Przykłady

Resetowanie sekretów TOTP dla wielu użytkowników

Zresetuj sekrety TOTP dla dwóch użytkowników.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "user.resettotp",
    "params": [
        "1",
        "5"
```

```
    ],
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "userids": [
            "1",
            "5"
        ]
    },
    "id": 1
}
```

Zobacz także

- Obiekt MFA

Źródło

CUser::resettotp() w *ui/include/classes/api/services/CUser.php*.

user.unblock

Opis

`object user.unblock(array userids)`

Ta metoda umożliwia odblokowanie użytkowników.

> **Note:**
> Ta metoda jest dostępna tylko dla typu użytkownika *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(array)` ID użytkowników do odblokowania.

Wartości zwracane

`(object)` Zwraca obiekt zawierający identyfikatory odblokowanych użytkowników we właściwości `userids`.

Przykłady

Odblokowywanie wielu użytkowników

Odblokuj dwóch użytkowników.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "user.unblock",
    "params": [
        "1",
        "5"
    ],
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "userids": [
            "1",
```

```
            "5"
        ]
    },
    "id": 1
}
```

Źródło

CUser::unblock() w *ui/include/classes/api/services/CUser.php*.

user.update

Opis

`object user.update(object/array users)`

Ta metoda umożliwia aktualizację istniejących użytkowników.

Note:
Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Note:
Siła hasła użytkownika jest weryfikowana zgodnie z regułami polityki haseł zdefiniowanymi przez Authentication API. Więcej informacji można znaleźć w sekcji Authentication API.

Parametry

`(object/array)` Właściwości użytkownika do zaktualizowania.

Właściwość `userid` musi być zdefiniowana dla każdego użytkownika, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko przekazane właściwości, wszystkie pozostałe pozostaną bez zmian.

Oprócz standardowych właściwości użytkownika metoda akceptuje następujące parametry.

Parametr	Typ	Opis
current_passwd	string	Bieżące hasło użytkownika. Wartość tego parametru może być pustym ciągiem znaków, jeśli użytkownik jest powiązany z katalogiem użytkowników. Zachowanie parametru: - *tylko do zapisu* - *wymagany*, jeśli `passwd` obiektu User object jest ustawione i użytkownik zmienia własne hasło
usrgrps	array	Grupy użytkowników zastępujące istniejące grupy użytkownika. Dla grup użytkowników musi być zdefiniowana tylko właściwość `usrgrpid`.
medias	array	Media użytkownika zastępujące istniejące, nieudostępnione media. Udostępnione media można pominąć podczas aktualizacji mediów.

Wartości zwracane

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych użytkowników we właściwości `userids`.

Przykłady

Zmiana nazwy użytkownika

Zmień nazwę użytkownika na John Doe.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "user.update",
    "params": {
        "userid": "1",
        "name": "John",
        "surname": "Doe"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "userids": [
            "1"
        ]
    },
    "id": 1
}
```

Zmiana roli użytkownika

Zmień rolę użytkownika.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "user.update",
    "params": {
        "userid": "12",
        "roleid": "6"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "userids": [
            "12"
        ]
    },
    "id": 1
}
```

Zobacz także

- Uwierzytelnianie

Źródło

CUser::update() w *ui/include/classes/api/services/CUser.php*.

Wykres

Ta klasa jest przeznaczona do pracy z wykresami.

Odniesienia do obiektów:

- Wykres

Dostępne metody:

- graph.create - tworzenie nowego wykresu
- graph.delete - usuwanie wykresu
- graph.get - pobieranie wykresu
- graph.update - aktualizacja wykresu

Obiekt Graph

Następujące obiekty są bezpośrednio powiązane z API `graph`.

Wykres

Obiekt wykresu ma następujące właściwości.

Właściwość	Typ	Opis
graphid	ID	ID wykresu. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji
height	integer	Wysokość wykresu w pikselach. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
name	string	Nazwa wykresu. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
width	integer	Szerokość wykresu w pikselach. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
flags	integer	Pochodzenie wykresu. Możliwe wartości: 0 - *(domyślnie)* zwykły wykres; 4 - wykres przekonwertowany z prototypu. Zachowanie właściwości: - *tylko do odczytu*
graphtype	integer	Typ układu wykresu. Możliwe wartości: 0 - *(domyślnie)* normalny; 1 - skumulowany; 2 - kołowy; 3 - rozstrzelony.
percent_left	float	Lewy percentyl. Domyślnie: 0.
percent_right	float	Prawy percentyl. Domyślnie: 0.
show_3d	integer	Czy wykresy kołowe i rozstrzelone mają być wyświetlane w 3D. Możliwe wartości: 0 - *(domyślnie)* wyświetlaj w 2D; 1 - wyświetlaj w 3D.
show_legend	integer	Czy wyświetlać legendę na wykresie. Możliwe wartości: 0 - ukryj; 1 - *(domyślnie)* wyświetlaj.

Właściwość	Typ	Opis
show_work_period	integer	Czy wyświetlać czas pracy na wykresie. Możliwe wartości: 0 - ukryj; 1 - *(domyślnie)* wyświetlaj.
show_triggers	integer	Czy wyświetlać linię wyzwalacza na wykresie. Możliwe wartości: 0 - ukryj; 1 - *(domyślnie)* wyświetlaj.
templateid	ID	ID wykresu nadrzędnego szablonu. Zachowanie właściwości: - *tylko do odczytu*
yaxismax	float	Stała maksymalna wartość osi Y. Domyślnie: 100.
yaxismin	float	Stała minimalna wartość osi Y. Domyślnie: 0.
ymax_itemid	ID	ID pozycji używanej jako maksymalna wartość osi Y. Jeśli użytkownik nie ma dostępu do określonej pozycji, wykres jest renderowany tak, jakby `ymax_type` było ustawione na „calculated”.
ymax_type	integer	Metoda obliczania wartości maksymalnej dla osi Y. Możliwe wartości: 0 - *(domyślnie)* calculated; 1 - stała; 2 - pozycja.
ymin_itemid	ID	ID pozycji używanej jako minimalna wartość osi Y. Jeśli użytkownik nie ma dostępu do określonej pozycji, wykres jest renderowany tak, jakby `ymin_type` było ustawione na „calculated”.
ymin_type	integer	Metoda obliczania wartości minimalnej dla osi Y. Możliwe wartości: 0 - *(domyślnie)* calculated; 1 - stała; 2 - pozycja.
uuid	string	Uniwersalny unikalny identyfikator używany do łączenia importowanych wykresów z już istniejącymi. Generowany automatycznie, jeśli nie został podany. Zachowanie właściwości: - *obsługiwane*, jeśli wykres należy do szablonu

graph.create

Opis

`object graph.create(object/array graphs)`

Ta metoda umożliwia tworzenie nowych wykresów.

Note:
Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji User roles.

Parametry

(object/array) Wykresy do utworzenia.

Oprócz standardowych właściwości wykresu, metoda akceptuje następujące parametry.

Parametr	Type	Opis
gitems	array	Pozycje wykresu, które mają zostać utworzone dla wykresu. Zachowanie parametru: - *wymagane*

Zwracane wartości

(object) Zwraca obiekt zawierający identyfikatory utworzonych wykresów we właściwości graphids. Kolejność zwróconych identyfikatorów odpowiada kolejności przekazanych wykresów.

Przykłady

Tworzenie wykresu

Utwórz wykres z dwiema pozycjami.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "graph.create",
    "params": {
        "name": "MySQL bandwidth",
        "width": 900,
        "height": 200,
        "gitems": [
            {
                "itemid": "22828",
                "color": "00AA00"
            },
            {
                "itemid": "22829",
                "color": "3333FF"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "graphids": [
            "652"
        ]
    },
    "id": 1
}
```

Zobacz także

- Pozycja wykresu

Źródło

CGraph::create() w *ui/include/classes/api/services/CGraph.php*.

graph.delete

Opis

`object graph.delete(array graphIds)`

Ta metoda umożliwia usuwanie grafów.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania metody można odwołać w ustawieniach roli użytkownika. Więcej informacji można znaleźć w User roles.

Parametry

`(array)` ID wykresów do usunięcia.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory usuniętych wykresów we właściwości `graphids`.

Przykłady

Usuwanie wielu wykresów

Usunięcie dwóch wykresów.

Request:

```
{
    "jsonrpc": "2.0",
    "method": "graph.delete",
    "params": [
        "652",
        "653"
    ],
    "auth": "3a57200802b24cda67c4e4010b50c065",
    "id": 1
}
```

Response:

```
{
    "jsonrpc": "2.0",
    "result": {
        "graphids": [
            "652",
            "653"
        ]
    },
    "id": 1
}
```

Źródło

CGraph::delete() w *ui/include/classes/api/services/CGraph.php*.

graph.get

Opis

`integer/array graph.get(object parameters)`

Ta metoda umożliwia pobieranie wykresów zgodnie z podanymi parametrami.

> **Note:**
> Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w User roles.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
graphids	ID/array	Zwracaj tylko wykresy o podanych ID.
groupids	ID/array	Zwracaj tylko wykresy należące do hostów lub szablonów w podanych grupach hostów lub grupach szablonów.
templateids	ID/array	Zwracaj tylko wykresy należące do podanych szablonów.
hostids	ID/array	Zwracaj tylko wykresy należące do podanych hostów.
itemids	ID/array	Zwracaj tylko wykresy zawierające podane pozycje.
templated	boolean	Jeśli ustawiono `true`, zwracaj tylko wykresy należące do szablonów.
inherited	boolean	Jeśli ustawiono `true`, zwracaj tylko wykresy odziedziczone z szablonu.
expandName	flag	Rozwiń makra w nazwie wykresu.
selectDiscoveryData	query	Zwróć właściwość `discoveryData` z danymi obiektu wykrywania wykresu. Obiekt wykrywania wykresu łączy wykryty wykres z prototypem wykresu, z którego został wykryty. Ma następujące właściwości: `parent_graphid` - `(ID)` ID prototypu wykresu, z którego wykres został utworzony; `status` - `(int)` status wykrywania wykresu: 0 - *(domyślnie)* wykres jest wykryty, 1 - wykres nie jest już wykryty; `ts_delete` - `(timestamp)` czas, kiedy wykres, który nie jest już wykrywany, zostanie usunięty.
selectDiscoveryRule	query	Zwróć właściwość `discoveryRule` z regułą wykrywania niskiego poziomu, która utworzyła wykres.
selectHostGroups	query	Zwróć właściwość `hostgroups` z grupami hostów, do których należy wykres.
selectTemplateGroups	query	Zwróć właściwość `templategroups` z grupami szablonów, do których należy wykres.
selectTemplates	query	Zwróć właściwość `templates` z szablonami, do których należy wykres.
selectHosts	query	Zwróć właściwość `hosts` z hostami, do których należy wykres.
selectItems	query	Zwróć właściwość `items` z pozycjami użytymi na wykresie.
selectGraphItems	query	Zwróć właściwość `gitems` z pozycjami użytymi na wykresie.
filter	object	Zwracaj tylko te wyniki, które dokładnie odpowiadają podanemu filtrowi. Akceptuje obiekt, w którym klucze są nazwami właściwości, a wartościami są pojedyncza wartość lub tablica wartości do dopasowania. Nie obsługuje właściwości typu danych `text` data type. Obsługuje dodatkowe właściwości: `host` - techniczna nazwa hosta, do którego należy wykres; `hostid` - ID hosta, do którego należy wykres.
sortfield	string/array	Sortuj wynik według podanych właściwości. Możliwe wartości: `graphid`, `name`, `graphtype`.
countOutput	boolean	Te parametry opisano w komentarzu referencyjnym.
editable	boolean	
excludeSearch	boolean	
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Parametr	Typ	Opis
selectGraphDiscovery	query	Zwróć właściwość `graphDiscovery` z obiektem wykrywania wykresu. Obiekty wykrywania wykresu łączą wykres z prototypem wykresu, z którego został utworzony. To zapytanie jest **przestarzałe**; użyj zamiast tego `selectDiscoveryData`.

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli został użyty parametr `countOutput`.

Przykłady

Pobieranie wykresów z hostów

Pobierz wszystkie wykresy z hosta „10107” i posortuj je według nazwy.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "graph.get",
    "params": {
        "output": "extend",
        "hostids": 10107,
        "sortfield": "name"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "graphid": "612",
            "name": "CPU jumps",
            "width": "900",
            "height": "200",
            "yaxismin": "0",
            "yaxismax": "100",
            "templateid": "439",
            "show_work_period": "1",
            "show_triggers": "1",
            "graphtype": "0",
            "show_legend": "1",
            "show_3d": "0",
            "percent_left": "0",
            "percent_right": "0",
            "ymin_type": "0",
            "ymax_type": "0",
            "ymin_itemid": "0",
            "ymax_itemid": "0",
            "flags": "0"
        },
        {
            "graphid": "613",
            "name": "CPU load",
            "width": "900",
            "height": "200",
            "yaxismin": "0",
```

```
            "yaxismax": "100",
            "templateid": "433",
            "show_work_period": "1",
            "show_triggers": "1",
            "graphtype": "0",
            "show_legend": "1",
            "show_3d": "0",
            "percent_left": "0",
            "percent_right": "0",
            "ymin_type": "1",
            "ymax_type": "0",
            "ymin_itemid": "0",
            "ymax_itemid": "0",
            "flags": "0"
        },
        {
            "graphid": "614",
            "name": "CPU utilization",
            "width": "900",
            "height": "200",
            "yaxismin": "0",
            "yaxismax": "100",
            "templateid": "387",
            "show_work_period": "1",
            "show_triggers": "0",
            "graphtype": "1",
            "show_legend": "1",
            "show_3d": "0",
            "percent_left": "0",
            "percent_right": "0",
            "ymin_type": "1",
            "ymax_type": "1",
            "ymin_itemid": "0",
            "ymax_itemid": "0",
            "flags": "0"
        },
        {
            "graphid": "645",
            "name": "Disk space usage /",
            "width": "600",
            "height": "340",
            "yaxismin": "0",
            "yaxismax": "0",
            "templateid": "0",
            "show_work_period": "0",
            "show_triggers": "0",
            "graphtype": "2",
            "show_legend": "1",
            "show_3d": "1",
            "percent_left": "0",
            "percent_right": "0",
            "ymin_type": "0",
            "ymax_type": "0",
            "ymin_itemid": "0",
            "ymax_itemid": "0",
            "flags": "4"
        }
    ],
    "id": 1
}
```


Zobacz także

- Reguła wykrywania
- Pozycja wykresu
- Pozycja
- Host
- Grupa hostów
- Szablon
- Grupa szablonów

Źródło

CGraph::get() w *ui/include/classes/api/services/CGraph.php*.

graph.update

Opis

`object graph.update(object/array graphs)`

Ta metoda służy do aktualizacji istniejących wykresów.

> **Note:**
> Ta metoda jest dostępna dla użytkowników typu *Admin* i *Super admin*. Uprawnienia mogą zostać zostać cofnięte w konfiguracji roli użytkownika. Więcej informacji Rola użytkownika

Parametry

`(object/array)` Właściwości wykresu do zaktualizowania.

Właściwość `graphid` musi być zdefiniowana dla każdego wykresu, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko przekazane właściwości, wszystkie pozostałe pozostaną bez zmian.

Oprócz standardowych właściwości wykresu metoda akceptuje następujące parametry.

Parametr	Typ	Opis
gitems	array	Pozycje wykresu służące do zastąpienia istniejących pozycji wykresu. Jeśli pozycja wykresu ma zdefiniowaną właściwość `gitemid`, zostanie zaktualizowana; w przeciwnym razie zostanie utworzona nowa pozycja wykresu.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych wykresów we właściwości `graphids`.

Przykłady

Ustawianie maksimum skali Y

Ustaw maksimum skali Y na stałą wartość 100.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "graph.update",
    "params": {
        "graphid": "439",
        "ymax_type": 1,
        "yaxismax": 100
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "graphids": [
```

```
            "439"
        ]
    },
    "id": 1
}
```

Źródło

CGraph::update() w *ui/include/classes/api/services/CGraph.php*.

Wykryta usługa

Ta klasa została zaprojektowana do pracy z wykrytymi usługami.

Odwołania do obiektów:

- Wykryta usługa

Dostępne metody:

- dservice.get - pobieranie wykrytych usług

Obiekt odkrywania usługi

Następujące obiekty są bezpośrednio powiązane z API `dservice`.

Wykryta usługa

Note:
Wykryte usługi są tworzone przez serwer Zabbix i nie mogą być modyfikowane za pomocą API.

Obiekt wykrytej usługi zawiera informacje o usłudze wykrytej przez regułę wykrywania sieci na hoście. Ma następujące właściwości.

Właściwość	Typ	Opis
dserviceid	ID	ID wykrytej usługi.
dcheckid	ID	ID kontroli wykrywania użytej do wykrycia usługi.
dhostid	ID	ID wykrytego hosta, na którym działa usługa.
dns	string	DNS hosta, na którym działa usługa.
ip	string	Adres IP hosta, na którym działa usługa.
lastdown	timestamp	Czas, kiedy wykryta usługa ostatnio przestała działać.
lastup	timestamp	Czas, kiedy wykryta usługa ostatnio zaczęła działać.
port	integer	Numer portu usługi.
status	integer	Status usługi. Możliwe wartości: 0 - usługa działa; 1 - usługa nie działa.
value	string	Wartość zwrócona przez usługę podczas wykonywania kontroli wykrywania agent, SNMPv1, SNMPv2 lub SNMPv3.

dservice.get

Opis

`integer/array dservice.get(object parameters)`

Ta metoda umożliwia pobranie wykrytych usług zgodnie z podanymi parametrami.

Note:
Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji User roles.

Parametry

(object) Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
dserviceids	ID/array	Zwraca tylko wykryte usługi o podanych identyfikatorach.
dhostids	ID/array	Zwraca tylko wykryte usługi należące do podanych wykrytych hostów.
dcheckids	ID/array	Zwraca tylko wykryte usługi, które zostały wykryte przez podane kontrole wykrywania.
druleids	ID/array	Zwraca tylko wykryte usługi, które zostały wykryte przez podane reguły wykrywania.
selectDRules	query	Zwraca właściwość `drules` zawierającą tablicę reguł wykrywania, które wykryły usługę.
selectDHosts	query	Zwraca właściwość `dhosts` zawierającą tablicę wykrytych hostów, do których należy usługa.
selectHosts	query	Zwraca właściwość `hosts` zawierającą hosty z tym samym adresem IP i proxy co usługa. Obsługuje `count`.
limitSelects	integer	Ogranicza liczbę rekordów zwracanych przez podzapytania. Dotyczy następujących podzapytań: `selectHosts` - wynik zostanie posortowany według `hostid`.
sortfield	string/array	Sortuje wynik według podanych właściwości. Możliwe wartości: `dserviceid`, `dhostid`, `ip`.
countOutput	boolean	Te parametry są opisane w komentarzu referencyjnym.
editable	boolean	
excludeSearch	boolean	
filter	object	
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

(integer/array) Zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli został użyty parametr `countOutput`.

Przykłady

Pobieranie usług wykrytych na hoście

Pobierz wszystkie wykryte usługi znalezione na wykrytym hoście „11”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "dservice.get",
    "params": {
        "output": "extend",
        "dhostids": "11"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "dserviceid": "12",
            "dhostid": "11",
            "value": "",
            "port": "80",
            "status": "1",
            "lastup": "0",
            "lastdown": "1348650607",
            "dcheckid": "5",
            "ip": "192.168.1.134",
            "dns": "john.local"
        },
        {
            "dserviceid": "13",
            "dhostid": "11",
            "value": "",
            "port": "21",
            "status": "1",
            "lastup": "0",
            "lastdown": "1348650610",
            "dcheckid": "6",
            "ip": "192.168.1.134",
            "dns": "john.local"
        }
    ],
    "id": 1
}
```


Zobacz także

- Wykryty host
- Kontrola wykrywania
- Host

Źródło

CDService::get() w *ui/include/classes/api/services/CDService.php*.

Wykryty host

Ta klasa została zaprojektowana do pracy z wykrytymi hostami.

Odwołania do obiektów:

- Wykryty host

Dostępne metody:

- dhost.get - pobieranie wykrytych hostów

Obiekt odkrywania hosta

Następujące obiekty są bezpośrednio powiązane z API `dhost`.

Wykryty host

> **Note:**
> Wykryte hosty są tworzone przez serwer Zabbix i nie mogą być modyfikowane za pośrednictwem API.

Obiekt wykrytego hosta zawiera informacje o hoście wykrytym przez regułę wykrywania sieci. Ma następujące właściwości.

Właściwość	Typ	Opis
dhostid	ID	ID wykrytego hosta.
druleid	ID	ID reguły wykrywania, która wykryła host.
lastdown	timestamp	Czas, kiedy wykryty host ostatnio przestał być dostępny.
lastup	timestamp	Czas, kiedy wykryty host ostatnio stał się dostępny.
status	integer	Czy wykryty host jest dostępny, czy niedostępny. Host jest dostępny, jeśli ma co najmniej jedną aktywną wykrytą usługę. Możliwe wartości: 0 - host dostępny; 1 - host niedostępny.

dhost.get

Opis

`integer/array dhost.get(object parameters)`

Ta metoda umożliwia pobieranie wykrytych hostów zgodnie z podanymi parametrami.

Note:
Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
dhostids	ID/array	Zwraca tylko wykryte hosty o podanych identyfikatorach.
druleids	ID/array	Zwraca tylko wykryte hosty, które zostały utworzone przez podane reguły wykrywania.
dserviceids	ID/array	Zwraca tylko wykryte hosty, na których działają podane usługi.
selectDRules	query	Zwraca właściwość `drules` zawierającą tablicę reguł wykrywania, które wykryły host.
selectDServices	query	Zwraca właściwość `dservices` zawierającą wykryte usługi działające na hoście. Obsługuje `count`.
limitSelects	integer	Ogranicza liczbę rekordów zwracanych przez podzapytania. Ma zastosowanie do następujących podzapytań: `selectDServices` - wyniki zostaną posortowane według `dserviceid`.
sortfield	string/array	Sortuje wynik według podanych właściwości. Możliwe wartości: `dhostid`, `druleid`.
countOutput	boolean	Te parametry są opisane w komentarzu referencyjnym.
editable	boolean	
excludeSearch	boolean	
filter	object	
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca jedną z opcji:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli parametr `countOutput` został wykorzystany.

Przykłady

Pobierz odkryte hosty według reguły wykrywania

Pobierz wszystkie hosty i odkryte usługi, które uruchamiają, które zostały wykryte przez regułę wykrywania „4”.

Zapytanie:

```
{
  "jsonrpc": "2.0",
  "method": "dhost.get",
  "params": {
    "output": "extend",
    "selectDServices": "extend",
    "druleids": "4"
  },
  "id": 1
}
```

Odpowiedź:

```
{
  "jsonrpc": "2.0",
  "result": [
    {
      "dservices": [
        {
          "dserviceid": "1",
          "dhostid": "1",
          "type": "4",
          "key_": "",
          "value": "",
          "port": "80",
          "status": "0",
          "lastup": "1337697227",
          "lastdown": "0",
          "dcheckid": "5",
          "ip": "192.168.1.1",
          "dns": "station.company.lan"
        }
      ],
      "dhostid": "1",
      "druleid": "4",
      "status": "0",
      "lastup": "1337697227",
      "lastdown": "0"
    },
    {
      "dservices": [
        {
          "dserviceid": "2",
          "dhostid": "2",
          "type": "4",
          "key_": "",
          "value": "",
          "port": "80",
          "status": "0",
          "lastup": "1337697234",
          "lastdown": "0",
          "dcheckid": "5",
```

```
          "ip": "192.168.1.4",
          "dns": "john.company.lan"
        }
      ],
      "dhostid": "2",
      "druleid": "4",
      "status": "0",
      "lastup": "1337697234",
      "lastdown": "0"
    },
    {
      "dservices": [
        {
          "dserviceid": "3",
          "dhostid": "3",
          "type": "4",
          "key_": "",
          "value": "",
          "port": "80",
          "status": "0",
          "lastup": "1337697234",
          "lastdown": "0",
          "dcheckid": "5",
          "ip": "192.168.1.26",
          "dns": "printer.company.lan"
        }
      ],
      "dhostid": "3",
      "druleid": "4",
      "status": "0",
      "lastup": "1337697234",
      "lastdown": "0"
    },
    {
      "dservices": [
        {
          "dserviceid": "4",
          "dhostid": "4",
          "type": "4",
          "key_": "",
          "value": "",
          "port": "80",
          "status": "0",
          "lastup": "1337697234",
          "lastdown": "0",
          "dcheckid": "5",
          "ip": "192.168.1.7",
          "dns": "mail.company.lan"
        }
      ],
      "dhostid": "4",
      "druleid": "4",
      "status": "0",
      "lastup": "1337697234",
      "lastdown": "0"
    }
  ],
  "id": 1
}
```


Zobacz także

- Wykryta usługa

- Reguła wykrywania

Źródło

CDHost::get() w *ui/include/classes/api/services/CDHost.php*.

Wyrażenie regularne

Ta klasa jest przeznaczona do pracy z globalnymi wyrażeniami regularnymi.

Odwołania do obiektów:

- Wyrażenie regularne
- Wyrażenia

Dostępne metody:

- regexp.create - tworzenie nowych wyrażeń regularnych
- regexp.delete - usuwanie wyrażeń regularnych
- regexp.get - pobieranie wyrażeń regularnych
- regexp.update - aktualizowanie wyrażeń regularnych

Obiekt wyrażenia regularnego

Następujące obiekty są bezpośrednio powiązane z API `regexp`.

Wyrażenie regularne

Globalny obiekt wyrażenia regularnego ma następujące właściwości.

Właściwość	Typ	Opis
regexpid	ID	ID wyrażenia regularnego. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji
name	string	Nazwa wyrażenia regularnego. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
test_string	string	Ciąg testowy.

Wyrażenia

Obiekt expressions ma następujące właściwości.

Właściwość	Typ	Opis
expression	string	Wyrażenie regularne. Zachowanie właściwości: - *wymagane*
expression_type	integer	Typ wyrażenia regularnego. Możliwe wartości: 0 - Zawiera ciąg znaków; 1 - Zawiera dowolny ciąg znaków; 2 - Nie zawiera ciągu znaków; 3 - Wynik to TRUE; 4 - Wynik to FALSE. Zachowanie właściwości: - *wymagane*

Właściwość	Typ	Opis
exp_delimiter	string	Separator wyrażenia. Wartość domyślna: ",". Możliwe wartości: "," lub ".", lub "/". Zachowanie właściwości: - *obsługiwane* jeśli `expression_type` jest ustawione na „Zawiera dowolny ciąg znaków”
case_sensitive	integer	Rozróżnianie wielkości liter. Wartość domyślna: 0. Możliwe wartości: 0 - Bez rozróżniania wielkości liter; 1 - Z rozróżnianiem wielkości liter.

regexp.create

Opis

`object regexp.create(object/array regularExpressions)`

Ta metoda umożliwia tworzenie nowych globalnych wyrażeń regularnych.

Note:
Ta metoda jest dostępna tylko dla użytkowników typu *Super admin*. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Wyrażenia regularne do utworzenia.

Oprócz standardowych właściwości metoda akceptuje następujące parametry.

Parametr	Typ	Opis
expressions	array	Opcje wyrażeń. Zachowanie parametru: - *wymagany*

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory utworzonych wyrażeń regularnych we właściwości `regexpids`.

Przykłady

Tworzenie nowego globalnego wyrażenia regularnego.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "regexp.create",
    "params": {
      "name": "Urządzenia pamięci masowej do wykrywania SNMP",
      "test_string": "/boot",
      "expressions": [
        {
          "expression": "^(Physical memory|Virtual memory|Memory buffers|Cached memory|Swap space)$",
          "expression_type": "4",
          "case_sensitive": "1"
        }
```

```
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "regexpids": [
            "16"
        ]
    },
    "id": 1
}
```

Źródło

CRegexp::create() w *ui/include/classes/api/services/CRegexp.php*.

regexp.delete

Opis

`object regexp.delete(array regexpids)`

Ta metoda umożliwia usuwanie globalnych wyrażeń regularnych.

Note:
Ta metoda jest dostępna tylko dla użytkowników typu *Super admin*. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(array)` ID wyrażeń regularnych do usunięcia.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory usuniętych wyrażeń regularnych we właściwości `regexpids`.

Przykłady

Usuwanie wielu globalnych wyrażeń regularnych.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "regexp.delete",
    "params": [
        "16",
        "17"
    ],
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "regexpids": [
            "16",
            "17"
        ]
    },
    "id": 1
}
```

Źródło

CRegexp::delete() w *ui/include/classes/api/services/CRegexp.php*.

regexp.get

Opis

`integer/array regexp.get(object parameters)`

Ta metoda umożliwia pobieranie globalnych wyrażeń regularnych zgodnie z podanymi parametrami.

Note:
Ta metoda jest dostępna tylko dla *Super Admin*. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w User roles.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
regexpids	ID/array	Zwraca tylko wyrażenia regularne o podanych identyfikatorach.
selectExpressions	query	Zwraca właściwość `expressions`.
sortfield	string/array	Sortuje wynik według podanych właściwości. Możliwe wartości: `regexpid`, `name`.
countOutput	boolean	Te parametry opisano w komentarzu referencyjnym.
editable	boolean	
excludeSearch	boolean	
filter	object	
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli został użyty parametr `countOutput`.

Przykłady

Pobieranie globalnych wyrażeń regularnych.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "regexp.get",
    "params": {
        "output": ["regexpid", "name"],
        "selectExpressions": ["expression", "expression_type"],
        "regexpids": [1, 2],
        "preservekeys": true
    },
    "id": 1
}
```

Odpowiedź:


```
{
  "jsonrpc": "2.0",
  "result": {
    "1": {
      "regexpid": "1",
      "name": "File systems for discovery",
      "expressions": [
        {
          "expression": "^(btrfs|ext2|ext3|ext4|reiser|xfs|ffs|ufs|jfs|jfs2|vxfs|hfs|apfs|refs|ntfs|fat32|
          "expression_type": "3"
        }
      ]
    },
    "2": {
      "regexpid": "2",
      "name": "Network interfaces for discovery",
      "expressions": [
        {
          "expression": "^Software Loopback Interface",
          "expression_type": "4"
        },
        {
          "expression": "^(In)?[Ll]oop[Bb]ack[0-9._]*$",
          "expression_type": "4"
        },
        {
          "expression": "^NULL[0-9.]*$",
          "expression_type": "4"
        },
        {
          "expression": "^[Ll]o[0-9.]*$",
          "expression_type": "4"
        },
        {
          "expression": "^[Ss]ystem$",
          "expression_type": "4"
        },
        {
          "expression": "^Nu[0-9.]*$",
          "expression_type": "4"
        }
      ]
    }
  },
  "id": 1
}
```


Źródło

CRegexp::get() w *ui/include/classes/api/services/CRegexp.php*.

regexp.update

Opis

`object regexp.update(object/array regularExpressions)`

Ta metoda umożliwia aktualizację istniejących globalnych wyrażeń regularnych.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkowników typu *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Właściwości wyrażenia regularnego do zaktualizowania.

Właściwość `regexpid` musi być zdefiniowana dla każdego obiektu, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko przekazane właściwości, wszystkie pozostałe pozostaną bez zmian.

Oprócz właściwości standardowych metoda akceptuje następujące parametry.

Parametr	Type	Opis
expressions	array	Opcje wyrażeń.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych wyrażeń regularnych we właściwości `regexpids`.

Przykłady

Aktualizacja globalnego wyrażenia regularnego dla wykrywania systemów plików.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "regexp.update",
    "params": {
      "regexpid": "1",
      "name": "Systemy plików do wykrywania",
      "test_string": "",
      "expressions": [
        {
          "expression": "^(btrfs|ext2|ext3|ext4|reiser|xfs|ffs|ufs|jfs|jfs2|vxfs|hfs|apfs|refs|zfs)$",
          "expression_type": "3",
          "exp_delimiter": ",",
          "case_sensitive": "0"
        },
        {
          "expression": "^(ntfs|fat32|fat16)$",
          "expression_type": "3",
          "exp_delimiter": ",",
          "case_sensitive": "0"
        }
      ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "regexpids": [
            "1"
        ]
    },
    "id": 1
}
```

Źródło

CRegexp::update() w *ui/include/classes/api/services/CRegexp.php*.

Wyzwalacz

Ta klasa jest przeznaczona do pracy z wyzwalaczami.

Odwołania do obiektów:

- Wyzwalacz
- Tag wyzwalacza

Dostępne metody:

- trigger.create - tworzenie nowych wyzwalaczy
- trigger.delete - usuwanie wyzwalaczy
- trigger.get - pobieranie wyzwalaczy
- trigger.update - aktualizacja wyzwalaczy

Obiekt wyzwalacza

Następujące obiekty są bezpośrednio powiązane z API `trigger`.

Wyzwalacz

Obiekt wyzwalacza ma następujące właściwości.

Właściwość	Typ	Opis
triggerid	ID	ID wyzwalacza. Zachowanie właściwości: - *tylko do odczytu* - *wymagane* dla operacji aktualizacji
description	string	Nazwa wyzwalacza. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
expression	string	Wyrażenie wyzwalacza. Pozycje z ustawionym `value_type` na 5 (binary) lub 6 (JSON) nie mogą być używane w wyrażeniach wyzwalacza. Zachowanie właściwości: - *wymagane* dla operacji tworzenia
event_name	string	Nazwa zdarzenia generowanego przez wyzwalacz.
opdata	string	Dane operacyjne.
comments	string	Dodatkowy opis wyzwalacza.
error	string	Tekst błędu, jeśli wystąpiły jakiekolwiek problemy podczas aktualizacji stanu wyzwalacza. Zachowanie właściwości: - *tylko do odczytu*
flags	integer	Pochodzenie wyzwalacza. Możliwe wartości: 0 - *(domyślnie)* zwykły wyzwalacz; 4 - wyzwalacz przekonwertowany z prototypu. Zachowanie właściwości: - *tylko do odczytu*
lastchange	timestamp	Czas ostatniej zmiany stanu wyzwalacza. Zachowanie właściwości: - *tylko do odczytu*
priority	integer	Poziom ważności wyzwalacza. Możliwe wartości: 0 - *(domyślnie)* niesklasyfikowany; 1 - informacja; 2 - ostrzeżenie; 3 - średni; 4 - wysoki; 5 - katastrofa.

Właściwość	Typ	Opis
state	integer	Stan wyrażenia wyzwalacza. Możliwe wartości: 0 - *(domyślnie)* stan wyzwalacza jest aktualny; 1 - bieżący stan wyzwalacza jest nieznany. Zachowanie właściwości: - *tylko do odczytu*
status	integer	Czy wyzwalacz jest włączony czy wyłączony. Możliwe wartości: 0 - *(domyślnie)* włączony; 1 - wyłączony.
templateid	ID	ID nadrzędnego wyzwalacza szablonu. Zachowanie właściwości: - *tylko do odczytu*
type	integer	Czy wyzwalacz może generować wiele zdarzeń problemu. Możliwe wartości: 0 - *(domyślnie)* nie generuj wielu zdarzeń; 1 - generuj wiele zdarzeń.
url	string	URL powiązany z wyzwalaczem.
url_name	string	Etykieta dla URL powiązanego z wyzwalaczem.
value	integer	Czy wyzwalacz jest w stanie OK czy problemu. Możliwe wartości: 0 - *(domyślnie)* OK; 1 - problem. Zachowanie właściwości: - *tylko do odczytu*
recovery_mode	integer	Tryb generowania zdarzenia OK. Możliwe wartości: 0 - *(domyślnie)* Wyrażenie; 1 - Wyrażenie odzyskiwania; 2 - Brak.
recovery_expression	string	Wyrażenie odzyskiwania wyzwalacza. Pozycje z ustawionym `value_type` na 5 (binary) lub 6 (JSON) nie mogą być używane w wyrażeniach odzyskiwania wyzwalacza.
correlation_mode	integer	Zamykanie zdarzeń OK. Możliwe wartości: 0 - *(domyślnie)* Wszystkie problemy; 1 - Wszystkie problemy, jeśli wartości tagów są zgodne.
correlation_tag	string	Tag do dopasowania.
manual_close	integer	Zezwalaj na ręczne zamknięcie. Możliwe wartości: 0 - *(domyślnie)* Nie; 1 - Tak.
uuid	string	Uniwersalny unikalny identyfikator, używany do łączenia importowanych wyzwalaczy z już istniejącymi. Generowany automatycznie, jeśli nie został podany. Zachowanie właściwości: - *obsługiwane* jeśli wyzwalacz należy do szablonu

Tag wyzwalacza

Obiekt tagu wyzwalacza ma następujące właściwości.

Właściwość	Typ	Opis
tag	string	Nazwa tagu wyzwalacza. Zachowanie właściwości: - *wymagane*
value	string	Wartość tagu wyzwalacza. Zachowanie właściwości: - *tylko do odczytu*.
object	integer	Typ obiektu, z którego tag został odziedziczony. Możliwe wartości: 0 - szablon; 1 - host; 3 - pozycja. Zachowanie właściwości: - *tylko do odczytu*.
objectid	ID	ID obiektu, z którego tag został odziedziczony. Zachowanie właściwości: - *tylko do odczytu*.
automatic	integer	Typ tagu wyzwalacza: Możliwe wartości: 0 - *(domyślnie)* tag utworzony przez użytkownika; 1 - tag utworzony przez LLD;Zachowanie właściwości: - *tylko do odczytu*.

trigger.create

Opis

`object trigger.create(object/array triggers)`

Ta metoda umożliwia tworzenie nowych wyzwalaczy.

Note:
Ta metoda jest dostępna tylko dla typów użytkowników *Admin* i *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Wyzwalacze do utworzenia.

Oprócz standardowych właściwości wyzwalacza metoda akceptuje następujące parametry.

Parametr	Typ	Opis
dependencies	array	Wyzwalacze, od których zależy wyzwalacz. Wyzwalacze muszą mieć zdefiniowaną tylko właściwość `triggerid`.
tags	array	Tagi wyzwalacza.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory utworzonych wyzwalaczy we właściwości `triggerids`. Kolejność zwróconych identyfikatorów odpowiada kolejności przekazanych wyzwalaczy.

Przykłady

Tworzenie wyzwalacza

Utwórz dwa wyzwalacze, z których każdy zależy od jednego innego wyzwalacza.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "trigger.create",
    "params": [
        {
            "description": "Obciążenie procesora jest zbyt wysokie na {HOST.NAME}",
            "expression": "last(/Linux server/system.cpu.load[percpu,avg1])>5",
            "dependencies": [
                {
                    "triggerid": "17367"
                }
            ]
        },
        {
            "description": "Usługa została zatrzymana",
            "expression": "length(last(/Linux server/log[/var/log/system,Service .* has stopped]))<>0",
            "dependencies": [
                {
                    "triggerid": "17368"
                }
            ],
            "tags": [
                {
                    "tag": "service",
                    "value": "{{ITEM.VALUE}.regsub(\"Service (.*) has stopped\", \"\\1\")}"
                },
                {
                    "tag": "error",
                    "value": ""
                }
            ]
        }
    ],
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "triggerids": [
            "17369",
            "17370"
        ]
    },
    "id": 1
}
```

Źródło

CTrigger::create() w *ui/include/classes/api/services/CTrigger.php*.

trigger.delete

Opis

`object trigger.delete(array triggerIds)`

Ta metoda umożliwia usuwanie wyzwalaczy.

Note:
Ta metoda jest dostępna tylko dla użytkowników typu *Admin* i *Super admin*. Uprawnienia do wywołania metody można odwołać w ustawieniach roli użytkownika. Więcej informacji można znaleźć w User roles.

Parametry

`(array)` ID wyzwalaczy do usunięcia.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory usuniętych wyzwalaczy we właściwości `triggerids`.

Przykłady

Usuń wiele wyzwalaczy

Usuń dwa wyzwalacze.

Żądanie:

```
{
"jsonrpc": "2.0",
"method": "trigger.delete",
"params": [
"12002",
"12003"
],
"id": 1
}
```

Odpowiedź:

```
{
"jsonrpc": "2.0",
"result": {
"triggerids": [
"12002",
"12003"
]
},
"id": 1
}
```

Źródło

CTrigger::delete() w *ui/include/classes/api/services/CTrigger.php*.

trigger.get

Opis

`integer/array trigger.get(object parameters)`

Ta metoda umożliwia pobieranie wyzwalaczy zgodnie z podanymi parametrami.

Note:
Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w User roles.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
triggerids	ID/array	Zwraca tylko wyzwalacze o podanych ID.
groupids	ID/array	Zwraca tylko wyzwalacze należące do hostów lub szablonów z podanych grup hostów lub grup szablonów.

Parametr	Typ	Opis
templateids	ID/array	Zwraca tylko wyzwalacze należące do podanych szablonów.
hostids	ID/array	Zwraca tylko wyzwalacze należące do podanych hostów.
itemids	ID/array	Zwraca tylko wyzwalacze zawierające podane pozycje.
functions	string/array	Zwraca tylko wyzwalacze używające podanych funkcji. Listę obsługiwanych funkcji można znaleźć na stronie supported function.
group	string	Zwraca tylko wyzwalacze należące do hostów lub szablonów z grupy hostów lub grupy szablonów o podanej nazwie.
host	string	Zwraca tylko wyzwalacze należące do hosta o podanej nazwie technicznej.
inherited	boolean	Jeśli ustawiono na `true`, zwraca tylko wyzwalacze dziedziczone z szablonu.
templated	boolean	Jeśli ustawiono na `true`, zwraca tylko wyzwalacze należące do szablonów.
dependent	boolean	Jeśli ustawiono na `true`, zwraca tylko wyzwalacze mające zależności. Jeśli ustawiono na `false`, zwraca tylko wyzwalacze, które nie mają zależności.
monitored	flag	Zwraca tylko włączone wyzwalacze należące do monitorowanych hostów i zawierające wyłącznie włączone pozycje.
active	flag	Zwraca tylko włączone wyzwalacze należące do monitorowanych hostów.
maintenance	boolean	Jeśli ustawiono na `true`, zwraca tylko włączone wyzwalacze należące do hostów w konserwacji.
withUnacknowledgedEvents	flag	Zwraca tylko wyzwalacze mające niepotwierdzone zdarzenia.
withAcknowledgedEvents	flag	Zwraca tylko wyzwalacze, dla których wszystkie zdarzenia są potwierdzone.
withLastEventUnacknowledged	flag	Zwraca tylko wyzwalacze, których ostatnie zdarzenie jest niepotwierdzone.
skipDependent	flag	Pomija wyzwalacze w stanie problemu, które są zależne od innych wyzwalaczy. Należy pamiętać, że inne wyzwalacze są ignorowane, jeśli są wyłączone, mają wyłączone pozycje lub hosty pozycji są wyłączone.
lastChangeSince	timestamp	Zwraca tylko wyzwalacze, które zmieniły swój stan po podanym czasie.
lastChangeTill	timestamp	Zwraca tylko wyzwalacze, które zmieniły swój stan przed podanym czasem.
only_true	flag	Zwraca tylko wyzwalacze, które ostatnio były w stanie problemu.
min_severity	integer	Zwraca tylko wyzwalacze o ważności większej lub równej podanej ważności.
evaltype	integer	Metoda oceny tagów. Możliwe wartości: 0 - *(domyślnie)* And/Or; 2 - Or.
tags	array	Zwraca tylko wyzwalacze z podanymi tagami. Format: `[{"tag": "<tag>", "value": "<value>", "operator": "<operator>"}, ...]`. Pusta tablica zwraca wszystkie wyzwalacze. Możliwe wartości operator: 0 - *(domyślnie)* Zawiera; 1 - Równa się; 2 - Nie zawiera; 3 - Nie równa się; 4 - Istnieje; 5 - Nie istnieje.
expandComment	flag	Rozwija makra w opisie wyzwalacza.
expandDescription	flag	Rozwija makra w nazwie wyzwalacza.
expandExpression	flag	Rozwija funkcje i makra w wyrażeniu wyzwalacza.
selectHostGroups	query	Zwraca grupy hostów, do których należy wyzwalacz, we właściwości `hostgroups`.
selectHosts	query	Zwraca hosty, do których należy wyzwalacz, we właściwości `hosts`.

Parametr	Typ	Opis
selectItems	query	Zwraca pozycje zawarte w wyzwalaczu we właściwości `items`.
selectFunctions	query	Zwraca funkcje użyte w wyzwalaczu we właściwości `functions`. Obiekty funkcji reprezentują funkcje użyte w wyrażeniu wyzwalacza i mają następujące właściwości: `functionid` - `(ID)` ID funkcji; `itemid` - `(ID)` ID pozycji użytej w funkcji; `function` - `(string)` nazwa funkcji; `parameter` - `(string)` parametr przekazany do funkcji. Parametr zapytania jest zastępowany symbolem $ w zwracanym ciągu.
selectDependencies	query	Zwraca wyzwalacze, od których zależy dany wyzwalacz, we właściwości `dependencies`.
selectDiscoveryData	query	Zwraca właściwość `discoveryData` z danymi obiektu wykrywania wyzwalacza. Obiekt wykrywania wyzwalacza łączy wykryty wyzwalacz z prototypem wyzwalacza, z którego został wykryty. Ma następujące właściwości: `parent_triggerid` - `(ID)` ID prototypu wyzwalacza, z którego utworzono wyzwalacz; `status` - `(int)` status wykrywania wyzwalacza: 0 - *(domyślnie)* wyzwalacz jest wykryty, 1 - wyzwalacz nie jest już wykrywany; `ts_delete` - `(timestamp)` czas, kiedy wyzwalacz, który nie jest już wykrywany, zostanie usunięty; `ts_disable` - `(timestamp)` czas, kiedy wyzwalacz, który nie jest już wykrywany, zostanie wyłączony; `disable_source` - `(int)` wskaźnik określający, czy wyzwalacz został wyłączony przez regułę LLD, czy ręcznie: 0 - *(domyślnie)* wyłączony automatycznie, 1 - wyłączony przez regułę LLD.
selectDiscoveryRule	query	Zwraca regułę wykrywania niskiego poziomu, która utworzyła wyzwalacz, we właściwości `discoveryRule`.
selectLastEvent	query	Zwraca ostatnie istotne zdarzenie wyzwalacza we właściwości `lastEvent`.
selectTags	query	Zwraca tagi wyzwalacza we właściwości `tags`.
inheritedTags	boolean	Zwraca wyzwalacze, które mają podane `tags` również w szablonie/hoście/podłączonych szablonach. Możliwe wartości: `true` - szablon/host/podłączone szablony również muszą mieć podane tagi; `false` - *(domyślnie)* tagi z szablonu/hosta/podłączonych szablonów są ignorowane.
selectInheritedTags	query	Zwraca właściwość `inheritedTags` z tagami dziedziczonymi z szablonów, podłączonych szablonów i hostów oraz z pozycji, do których odwołują się wyrażenia wyzwalacza lub odzyskiwania.
selectTemplateGroups	query	Zwraca grupy szablonów, do których należy wyzwalacz, we właściwości `templategroups`.
filter	object	Zwraca tylko te wyniki, które dokładnie odpowiadają podanemu filtrowi. Akceptuje obiekt, w którym kluczami są nazwy właściwości, a wartościami są pojedyncza wartość lub tablica wartości do dopasowania. Nie obsługuje właściwości typu danych `text` data type. Obsługuje dodatkowe właściwości: `host` - nazwa techniczna hosta, do którego należy wyzwalacz; `hostid` - ID hosta, do którego należy wyzwalacz.

Parametr	Typ	Opis
limitSelects	integer	Ogranicza liczbę rekordów zwracanych przez podzapytania. Dotyczy następujących podzapytań: `selectHosts` - wyniki będą sortowane według `host`.
sortfield	string/array	Sortuje wynik według podanych właściwości. Możliwe wartości: `triggerid`, `description`, `status`, `priority`, `lastchange`, `hostname`.
countOutput	boolean	Te parametry są opisane w reference commentary.
editable	boolean	
excludeSearch	boolean	
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	
selectTriggerDiscovery	query	Zwraca obiekt wykrywania wyzwalacza we właściwości `triggerDiscovery`. Obiekty wykrywania wyzwalacza łączą wyzwalacz z prototypem wyzwalacza, z którego został utworzony. To zapytanie jest **przestarzałe**; zamiast niego użyj `selectDiscoveryData`.

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli został użyty parametr `countOutput`.

Przykłady

Pobieranie danych według ID wyzwalacza

Pobierz wszystkie dane oraz funkcje używane w wyzwalaczu „14062”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "trigger.get",
    "params": {
        "triggerids": "14062",
        "output": "extend",
        "selectFunctions": "extend"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "triggerid": "14062",
            "expression": "{13513}<10m",
            "description": "{HOST.NAME} has been restarted (uptime < 10m)",
            "url": "",
            "status": "0",
            "value": "0",
            "priority": "2",
```

```
            "lastchange": "0",
            "comments": "The host uptime is less than 10 minutes",
            "error": "",
            "templateid": "10016",
            "type": "0",
            "state": "0",
            "flags": "0",
            "recovery_mode": "0",
            "recovery_expression": "",
            "correlation_mode": "0",
            "correlation_tag": "",
            "manual_close": "0",
            "opdata": "",
            "event_name": "",
            "uuid": "",
            "url_name": "",
            "functions": [
                {
                    "functionid": "13513",
                    "itemid": "24350",
                    "triggerid": "14062",
                    "parameter": "$",
                    "function": "last"
                }
            ]
        }
    ],
    "id": 1
}
```

Pobieranie wyzwalaczy w stanie problemu

Pobierz identyfikator, nazwę i ważność wszystkich wyzwalaczy w stanie problemu i posortuj je według ważności malejąco.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "trigger.get",
    "params": {
        "output": [
            "triggerid",
            "description",
            "priority"
        ],
        "filter": {
            "value": 1
        },
        "sortfield": "priority",
        "sortorder": "DESC"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "triggerid": "13907",
            "description": "Procesy samomonitorowania Zabbix zajęte w mniej niż 100%",
            "priority": "4"
        },
        {
```

```
            "triggerid": "13824",
            "description": "Procesy discoverera Zabbix zajęte w więcej niż 75%",
            "priority": "3"
        }
    ],
    "id": 1
}
```

Pobieranie określonego wyzwalacza z tagami

Pobierz określony wyzwalacz z tagami.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "trigger.get",
    "params": {
        "output": [
            "triggerid",
            "description"
        ],
        "selectTags": "extend",
        "triggerids": [
            "17578"
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "triggerid": "17370",
            "description": "Service status",
            "tags": [
                {
                    "tag": "service",
                    "value": "{{ITEM.VALUE}.regsub(\"Service (.*) has stopped\", \"\\1\")}",
                    "automatic": "1"
                },
                {
                    "tag": "error",
                    "value": "",
                    "automatic": "1"
                }
            ]
        }
    ],
    "id": 1
}
```

Zobacz także

- Reguła wykrywania
- Pozycja
- Host
- Grupa hostów
- Grupa szablonów

Źródło

CTrigger::get() w *ui/include/classes/api/services/CTrigger.php*.

trigger.update

Opis

`object trigger.update(object/array triggers)`

Ta metoda umożliwia aktualizację istniejących wyzwalaczy.

> **Note:**
> Ta metoda jest dostępna tylko dla użytkowników typu *Admin* i *Super admin*. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach ról użytkowników. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Właściwości wyzwalacza do zaktualizowania.

Właściwość `triggerid` musi być zdefiniowana dla każdego wyzwalacza, wszystkie pozostałe właściwości są opcjonalne. Zaktualizowane zostaną tylko przekazane właściwości, wszystkie pozostałe pozostaną bez zmian.

Oprócz standardowych właściwości wyzwalacza metoda akceptuje następujące parametry.

Parametr	Type	Opis
dependencies	array	Wyzwalacze, od których zależy wyzwalacz. W wyzwalaczach musi być zdefiniowana tylko właściwość `triggerid`.
tags	array	Tagi wyzwalacza.

Wartości zwracane

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych wyzwalaczy we właściwości `triggerids`.

Przykłady

Włączanie wyzwalacza

Włącz wyzwalacz, czyli ustaw jego status na „0”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "trigger.update",
    "params": {
        "triggerid": "13938",
        "status": 0
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "triggerids": [
            "13938"
        ]
    },
    "id": 1
}
```

Zastępowanie tagów wyzwalacza

Zastąp tagi dla wyzwalacza.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "trigger.update",
    "params": {
        "triggerid": "13938",
        "tags": [
            {
                "tag": "service",
                "value": "{{ITEM.VALUE}.regsub(\"Service (.*) has stopped\", \"\\1\")}"
            },
            {
                "tag": "error",
                "value": ""
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "triggerids": [
            "13938"
        ]
    },
    "id": 1
}
```

Zastępowanie zależności

Zastąp zależności dla wyzwalacza.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "trigger.update",
    "params": {
        "triggerid": "22713",
        "dependencies": [
            {
                "triggerid": "22712"
            },
            {
                "triggerid": "22772"
            }
        ]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "triggerids": [
            "22713"
        ]
    },
    "id": 1
}
```

Źródło

CTrigger::update() w *ui/include/classes/api/services/CTrigger.php*.

Węzeł wysokiej dostępności

Ta klasa została zaprojektowana do pracy z węzłami serwera, które są częścią klastra wysokiej dostępności lub samodzielnej instancji serwera.

Odwołania do obiektów:

- Węzeł wysokiej dostępności

Dostępne metody:

- hanode.get - pobieranie węzłów

Obiekt węzła wysokiej dostępności

Poniższy obiekt jest powiązany z działaniem klastra wysokiej dostępności serwerów Zabbix.

Węzeł wysokiej dostępności

Note:
Węzły są tworzone przez serwer Zabbix i nie mogą być modyfikowane przez API.

Obiekt węzła wysokiej dostępności ma następujące właściwości.

Właściwość	Typ	Opis
ha_nodeid	ID	ID węzła.
name	string	Nazwa przypisana do węzła przy użyciu parametru konfiguracyjnego HANodeName w pliku zabbix_server.conf. Puste dla serwera działającego w trybie samodzielnym.
address	string	Nazwa IP lub DNS, z której łączy się węzeł.
port	integer	Port, na którym działa węzeł.
lastaccess	integer	Czas heartbeat, czyli czas ostatniej aktualizacji z węzła. Znacznik czasu UTC.
status	integer	Stan węzła. Możliwe wartości: 0 - zapasowy; 1 - zatrzymany ręcznie; 2 - niedostępny; 3 - aktywny.

hanode.get

Opis

`integer/array hanode.get(object parameters)`

Ta metoda umożliwia pobranie listy węzłów klastra wysokiej dostępności zgodnie z podanymi parametrami.

Note:
Ta metoda jest dostępna tylko dla użytkowników typu *Super admin*. Więcej informacji można znaleźć w sekcji User roles.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
ha_nodeids	ID/array	Zwraca tylko węzły o podanych identyfikatorach węzłów.
filter	object	Zwraca tylko te wyniki, które dokładnie odpowiadają podanemu filtrowi. Akceptuje obiekt, w którym kluczami są nazwy właściwości, a wartościami są pojedyncza wartość lub tablica wartości do dopasowania. Obsługiwane właściwości: `name`, `address`, `status`.
sortfield	string/array	Sortuje wynik według podanych właściwości. Możliwe wartości: `name`, `lastaccess`, `status`.
countOutput	flag	Te parametry opisano w komentarzu referencyjnym.
limit	integer	
output	query	
preservekeys	boolean	
sortorder	string/array	

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów;
- liczbę pobranych obiektów, jeśli został użyty parametr `countOutput`.

Przykłady

Pobierz listę węzłów uporządkowaną według statusu

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "hanode.get",
    "params": {
        "preservekeys": true,
        "sortfield": "status",
        "sortorder": "DESC"
    },
    "id": 1
}
```

Odpowiedź:

```
{
  "jsonrpc": "2.0",
  "result": {
    "ckuo7i1nw000h0sajj3l3hh8u": {
      "ha_nodeid": "ckuo7i1nw000h0sajj3l3hh8u",
      "name": "node-active",
      "address": "192.168.1.13",
      "port": "10051",
      "lastaccess": "1635335704",
      "status": "3"
    },
    "ckuo7i1nw000e0sajwfttc1mp": {
      "ha_nodeid": "ckuo7i1nw000e0sajwfttc1mp",
      "name": "node6",
      "address": "192.168.1.10",
      "port": "10053",
      "lastaccess": "1635332902",
      "status": "2"
    },
    "ckuo7i1nv000c0sajz85xcrtt": {
      "ha_nodeid": "ckuo7i1nv000c0sajz85xcrtt",
```

```
      "name": "node4",
      "address": "192.168.1.8",
      "port": "10052",
      "lastaccess": "1635334214",
      "status": "1"
    },
    "ckuo7i1nv000a0saj1fcdkeu4": {
      "ha_nodeid": "ckuo7i1nv000a0saj1fcdkeu4",
      "name": "node2",
      "address": "192.168.1.6",
      "port": "10051",
      "lastaccess": "1635335705",
      "status": "0"
    }
  },
  "id": 1
}
```

Pobierz listę określonych węzłów według ich identyfikatorów

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "hanode.get",
    "params": {
        "ha_nodeids": ["ckuo7i1nw000e0sajwfttc1mp", "ckuo7i1nv000c0sajz85xcrtt"]
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "ha_nodeid": "ckuo7i1nv000c0sajz85xcrtt",
            "name": "node4",
            "address": "192.168.1.8",
            "port": "10052",
            "lastaccess": "1635334214",
            "status": "1"
        },
        {
            "ha_nodeid": "ckuo7i1nw000e0sajwfttc1mp",
            "name": "node6",
            "address": "192.168.1.10",
            "port": "10053",
            "lastaccess": "1635332902",
            "status": "2"
        }
    ],
    "id": 1
}
```

Pobierz listę zatrzymanych węzłów

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "hanode.get",
    "params": {
        "output": ["ha_nodeid", "address", "port"],
        "filter": {
```

```
            "status": 1
        }
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "ha_nodeid": "ckuo7i1nw000g0sajjsjre7e3",
            "address": "192.168.1.12",
            "port": "10051"
        },
        {
            "ha_nodeid": "ckuo7i1nv000c0sajz85xcrtt",
            "address": "192.168.1.8",
            "port": "10052"
        },
        {
            "ha_nodeid": "ckuo7i1nv000d0sajd95y1b6x",
            "address": "192.168.1.9",
            "port": "10053"
        }
    ],
    "id": 1
}
```

Pobierz liczbę węzłów zapasowych

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "hanode.get",
    "params": {
        "countOutput": true,
        "filter": {
            "status": 0
        }
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": "3",
    "id": 1
}
```

Sprawdzenie statusu węzłów pod określonymi adresami IP

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "hanode.get",
    "params": {
        "output": ["name", "status"],
        "filter": {
            "address": ["192.168.1.7", "192.168.1.13"]
        }
    },
```

```
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "name": "node3",
            "status": "0"
        },
        {
            "name": "node-active",
            "status": "3"
        }
    ],
    "id": 1
}
```

Źródło

CHaNode::get() w *ui/include/classes/api/services/CHaNode.php*.

Zadanie

Ta klasa jest przeznaczona do pracy z zadaniami (takimi jak sprawdzanie pozycji lub reguł wykrywania niskiego poziomu bez przeładowania konfiguracji).

Odwołania do obiektów:

- Task
  - Obiekt żądania „Wykonaj teraz”
  - Obiekt żądania „Odśwież konfigurację proxy”
  - Obiekt żądania „Informacje diagnostyczne”
    * Obiekt żądania statystyk
    * Obiekt wyniku statystyk

Dostępne metody:

- task.create - utwórz nowe zadania
- task.get - pobierz zadania

Obiekt task

Następujące obiekty są bezpośrednio powiązane z API `task`.

Task

Obiekt task ma następujące właściwości:

Property	Type	Description
taskid	ID	ID zadania. Zachowanie właściwości: *- tylko do odczytu*

Property	Type	Description
type	integer	Typ zadania. Możliwe wartości: 1 - Informacje diagnostyczne; 2 - Odśwież konfigurację proxy; 6 - Wykonaj teraz. Użytkownicy typu *Admin* i *User* mogą tworzyć tylko zadania „Wykonaj teraz”. Zwróć uwagę, że `task.get` zawsze zwraca „7” (Podsumowanie wykonania zadania). Zachowanie właściwości: - *wymagane*
status	integer	Status zadania. Możliwe wartości: 1 - nowe zadanie; 2 - zadanie w toku; 3 - zadanie ukończone; 4 - zadanie wygasło. Zachowanie właściwości: - *tylko do odczytu*
clock	timestamp	Czas utworzenia zadania. Zachowanie właściwości: - *tylko do odczytu*
ttl	integer	Czas w sekundach, po którym zadanie wygasa. Zachowanie właściwości: - *tylko do odczytu*
proxyid	ID	ID proxy, dla którego zbierane są statystyki informacji diagnostycznych. Zachowanie właściwości: - *obsługiwane*, jeśli `type` jest ustawione na „Informacje diagnostyczne” lub „Odśwież konfigurację proxy”
request	object	Obiekt żądania zadania zgodnie z typem zadania: Obiekt zadania „Wykonaj teraz” jest opisany szczegółowo poniżej; Obiekt zadania „Odśwież konfigurację proxy” jest opisany szczegółowo poniżej; Obiekt zadania „Informacje diagnostyczne” jest opisany szczegółowo poniżej. Zachowanie właściwości: - *wymagane*
result	object	Obiekt wyniku zadania informacji diagnostycznych. Może zawierać NULL, jeśli wynik nie jest jeszcze gotowy. Obiekt wyniku jest opisany szczegółowo poniżej. Zachowanie właściwości: - *tylko do odczytu*

Obiekt żądania „Execute now”

Obiekt żądania zadania „Execute now” ma następujące właściwości.

Właściwość	Typ	Opis
itemid	ID	ID pozycji i reguł wykrywania niskiego poziomu. Użytkownicy typu *Admin* i *User* mogą wykonać „Execute now” dla pozycji na hostach, do których mają uprawnienie odczytu i zapisu (*read-write*) albo uprawnienie *read* oraz włączoną akcję `invoke_execute_now` action dla swojej roli. To samo dotyczy użytkowników typu *Admin* w przypadku reguł wykrywania niskiego poziomu (LLD).

Obiekt żądania „Refresh proxy configuration”

Obiekt żądania zadania „Refresh proxy configuration” ma następujące właściwości.

Właściwość	Type	Opis
proxyids	array	ID proxy.

Obiekt żądania „Diagnostic information”

Obiekt żądania zadania informacji diagnostycznych ma następujące właściwości. Obiekt żądania statystyk dla wszystkich typów właściwości jest opisany szczegółowo poniżej.

Właściwość	Typ	Opis
historycache	object	Żądanie statystyk pamięci podręcznej historii. Dostępne na serwer i proxy.
valuecache	object	Żądanie statystyk pamięci podręcznej pozycji. Dostępne na serwer.
preprocessing	object	Żądanie statystyk menedżera przetwarzania wstępnego. Dostępne na serwer i proxy.
alerting	object	Żądanie statystyk menedżera alertów. Dostępne na serwer.
lld	object	Żądanie statystyk menedżera LLD. Dostępne na serwer.

Obiekt żądania statystyk

Obiekt żądania statystyk służy do określenia, jaki typ informacji powinien być zbierany o wewnętrznych procesach serwera/proxy. Ma on następujące właściwości.

Właściwość	Typ	Opis
stats	query	Właściwości obiektu statystyk, które mają zostać zwrócone. Lista dostępnych pól dla każdego typu statystyk informacji diagnostycznych jest opisana szczegółowo poniżej. Domyślnie: `extend` zwróci wszystkie dostępne pola statystyk.
top	object	Obiekt służący do sortowania i ograniczania zwracanych wartości statystyk. Lista dostępnych pól dla każdego typu statystyk informacji diagnostycznych jest opisana szczegółowo poniżej. Przykład: { “source.alerts”: 10 }

Lista pól statystyk dostępnych dla każdego typu żądania informacji diagnostycznych

Dla każdej właściwości typu żądania informacji diagnostycznych można żądać następujących pól statystyk.

Typ diagnostyczny	Dostępne pola	Opis
historycache	items	Liczba elementów w pamięci podręcznej.
	values	Liczba wartości w pamięci podręcznej.

Typ diagnostyczny	Dostępne pola	Opis
	memory	Statystyki pamięci współdzielonej (wolne miejsce, liczba używanych fragmentów, liczba wolnych fragmentów, maksymalny rozmiar wolnego fragmentu).
	memory.data	Statystyki pamięci współdzielonej pamięci podręcznej danych historii.
	memory.index	Statystyki pamięci współdzielonej pamięci podręcznej indeksu historii.
valuecache	items	Liczba elementów w pamięci podręcznej.
	values	Liczba wartości w pamięci podręcznej.
	memory	Statystyki pamięci współdzielonej (wolne miejsce, liczba używanych fragmentów, liczba wolnych fragmentów, maksymalny rozmiar wolnego fragmentu).
	mode	Tryb pamięci podręcznej wartości.
preprocessing	values	Liczba wartości w kolejce.
	preproc.values	Liczba wartości w kolejce z krokami przetwarzania wstępnego.
alerting	alerts	Liczba alertów w kolejce.
lld	rules	Liczba reguł w kolejce.
	values	Liczba wartości w kolejce.

Lista pól sortowania dostępnych dla każdego typu żądania informacji diagnostycznych

Następujące pola statystyczne mogą być używane do sortowania i ograniczania żądanych informacji.

Typ diagnostyczny	Dostępne pola	Typ
historycache	values	integer
valuecache	values	integer
	request.values	integer
preprocessing	values	integer
alerting	media.alerts	integer
	source.alerts	integer
lld	values	integer

Obiekt wyniku statystyk

Obiekt wyniku statystyk jest pobierany w polu `result` obiektu zadania.

Właściwość	Typ	Opis
status	integer	Status wyniku zadania. Możliwe wartości: -1 - podczas wykonywania zadania wystąpił błąd; 0 - wynik zadania został utworzony. Zachowanie właściwości: *- tylko do odczytu*
data	string/object	Wyniki zgodne z obiektem żądania statystyk dla określonego zadania informacji diagnostycznych. Zawiera ciąg komunikatu o błędzie, jeśli podczas wykonywania zadania wystąpił błąd.

task.create

Opis

`object task.create(object/array tasks)`

Ta metoda umożliwia tworzenie zadań.

Note:
Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywołania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w User roles.

Parametry

`(object/array)` Zadanie do utworzenia.

Metoda akceptuje zadania ze standardowymi właściwościami zadania.

Należy pamiętać, że zadania „Wykonaj teraz” można tworzyć tylko dla następujących typów pozycji/reguł wykrywania:

- agent Zabbix (pasywny)
- Proste sprawdzenie
- agent SNMP (v1/v2/v3)
- Wewnętrzny Zabbix
- Sprawdzenie zewnętrzne
- Monitor bazy danych
- agent HTTP
- agent IPMI
- agent SSH
- agent TELNET
- agent JMX
- Obliczana
- Zależna pozycja
- Skrypt
- Przeglądarka

Jeśli pozycja/reguła wykrywania jest typu „Zależna pozycja”, to jej pozycja nadrzędna również musi być jednym z powyższych typów.

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory utworzonych zadań we właściwości `taskids`. Jedno zadanie jest tworzone dla każdej pozycji i reguły wykrywania niskiego poziomu. Kolejność zwróconych identyfikatorów odpowiada kolejności przekazanych `itemids`.

Przykłady

Tworzenie zadania

Utwórz zadanie „Wykonaj teraz” dla pozycji i reguły wykrywania niskiego poziomu.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "task.create",
    "params": [
        {
            "type": 6,
            "request": {
                "itemid": "10092"
            }
        },
        {
            "type": 6,
            "request": {
                "itemid": "10093"
            }
        }
    ],
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "taskids": [
            "1",
            "2"
        ]
```

```
    },
    "id": 1
}
```

Utwórz zadanie „Odśwież konfigurację proxy” dla dwóch proxy.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "task.create",
    "params": [
        {
            "type": 2,
            "request": {
                "proxyids": ["10459", "10460"]
            }
        }
    ],
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "taskids": [
            "1"
        ]
    },
    "id": 1
}
```

Utwórz zadanie „Informacje diagnostyczne”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "task.create",
    "params": [
        {
            "type": 1,
            "request": {
                "alerting": {
                    "stats": [
                        "alerts"
                    ],
                    "top": {
                        "media.alerts": 10
                    }
                },
                "lld": {
                    "stats": "extend",
                    "top": {
                        "values": 5
                    }
                }
            },
            "proxyid": 0
        }
    ],
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "taskids": [
            "3"
        ]
    },
    "id": 1
}
```

Zobacz także

- Task
- Obiekt żądania „Wykonaj teraz”
- Obiekt żądania „Odśwież konfigurację proxy”
- Obiekt żądania „Informacje diagnostyczne”

Źródło

CTask::create() w *ui/include/classes/api/services/CTask.php*.

task.get

Opis

`integer/array task.get(object parameters)`

Ta metoda umożliwia pobieranie zadań zgodnie z podanymi parametrami.

Note:
Ta metoda jest dostępna tylko dla użytkownika typu *Super admin*. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
taskids	ID/array	Zwraca tylko zadania o podanych identyfikatorach.
output	query	Te parametry są opisane w komentarzu referencyjnym.
preservekeys	boolean	

Zwrócone wartości

`(integer/array)` Zwraca tablicę obiektów.

Przykłady

Pobierz zadanie według ID

Pobierz wszystkie dane dotyczące zadania o ID „1”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "task.get",
    "params": {
        "output": "extend",
        "taskids": "1"
    },
    "id": 1
}
```

Odpowiedź:


```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "taskid": "1",
            "type": "7",
            "status": "3",
            "clock": "1601039076",
            "ttl": "3600",
            "proxyid": null,
            "request": {
                "alerting": {
                    "stats": [
                        "alerts"
                    ],
                    "top": {
                        "media.alerts": 10
                    }
                },
                "lld": {
                    "stats": "extend",
                    "top": {
                        "values": 5
                    }
                }
            },
            "result": {
                "data": {
                    "alerting": {
                        "alerts": 0,
                        "top": {
                            "media.alerts": []
                        },
                        "time": 0.000663
                    },
                    "lld": {
                        "rules": 0,
                        "values": 0,
                        "top": {
                            "values": []
                        },
                        "time": 0.000442
                    }
                },
                "status": "0"
            }
        }
    ],
    "id": 1
}
```


Zobacz także

- Task
- Obiekt żądania „Wykonaj teraz”
- Obiekt żądania „Odśwież konfigurację proxy”
- Obiekt żądania „Informacje diagnostyczne”

Źródło

CTask::get() w *ui/include/classes/api/services/CTask.php*.

Zdarzenie

Ta klasa jest przeznaczona do pracy ze zdarzeniami.

Odwołania do obiektów:

- Event
- Tag zdarzenia
- URL typu nośnika

Dostępne metody:

- event.get - pobierz zdarzenia
- event.acknowledge - potwierdź zdarzenia

Obiekt zdarzenia

Następujące obiekty są bezpośrednio powiązane z API `event`.

Zdarzenie

Note:
Zdarzenia są tworzone przez serwer Zabbix i nie mogą być modyfikowane przez API.

Obiekt zdarzenia ma następujące właściwości.

Właściwość	Typ	Opis
eventid	ID	ID zdarzenia.
source	integer	Typ zdarzenia. Możliwe wartości: 0 - zdarzenie utworzone przez wyzwalacz; 1 - zdarzenie utworzone przez regułę wykrywania; 2 - zdarzenie utworzone przez aktywną autorejestrację agenta; 3 - zdarzenie wewnętrzne; 4 - zdarzenie utworzone przy aktualizacji stanu usługi.
object	integer	Typ obiektu powiązanego ze zdarzeniem. Możliwe wartości, jeśli `source` jest ustawione na „zdarzenie utworzone przez wyzwalacz”: 0 - wyzwalacz. Możliwe wartości, jeśli `source` jest ustawione na „zdarzenie utworzone przez regułę wykrywania”: 1 - wykryty host; 2 - wykryta usługa. Możliwe wartości, jeśli `source` jest ustawione na „zdarzenie utworzone przez aktywną autorejestrację agenta”: 3 - host z autorejestracji. Możliwe wartości, jeśli `source` jest ustawione na „zdarzenie wewnętrzne”: 0 - wyzwalacz; 4 - pozycja; 5 - reguła LLD. Możliwe wartości, jeśli `source` jest ustawione na „zdarzenie utworzone przy aktualizacji stanu usługi”: 6 - usługa.
objectid	ID	ID powiązanego obiektu.
acknowledged	integer	Czy zdarzenie zostało potwierdzone.
clock	timestamp	Czas utworzenia zdarzenia.
ns	integer	Nanosekundy w momencie utworzenia zdarzenia.

Właściwość	Typ	Opis
name	string	Rozwinięta nazwa zdarzenia.
value	integer	Stan powiązanego obiektu. Możliwe wartości, jeśli `source` jest ustawione na „zdarzenie utworzone przez wyzwalacz” lub „zdarzenie utworzone przy aktualizacji stanu usługi”: 0 - OK; 1 - problem. Możliwe wartości, jeśli `source` jest ustawione na „zdarzenie utworzone przez regułę wykrywania”: 0 - host lub usługa działa; 1 - host lub usługa nie działa; 2 - host lub usługa wykryte; 3 - host lub usługa utracone. Możliwe wartości, jeśli `source` jest ustawione na „zdarzenie wewnętrzne”: 0 - stan „normalny”; 1 - stan „nieznany” lub „niewspierany”. Zachowanie właściwości: - *obsługiwane* jeśli `source` jest ustawione na „zdarzenie utworzone przez wyzwalacz”, „zdarzenie utworzone przez regułę wykrywania”, „zdarzenie wewnętrzne” lub „zdarzenie utworzone przy aktualizacji stanu usługi”
severity	integer	Bieżący poziom ważności zdarzenia. Możliwe wartości: 0 - niesklasyfikowane; 1 - informacja; 2 - ostrzeżenie; 3 - średni; 4 - wysoki; 5 - katastrofa.
r_eventid	ID	ID zdarzenia odzyskania.
c_eventid	ID	ID zdarzenia użytego do nadpisania (zamknięcia) bieżącego zdarzenia zgodnie z globalną regułą korelacji. Zobacz `correlationid`, aby zidentyfikować dokładną regułę korelacji. Ten parametr jest zdefiniowany tylko wtedy, gdy zdarzenie zostało zamknięte przez globalną regułę korelacji.
cause_eventid	ID	ID zdarzenia przyczyny.
correlationid	ID	ID reguły korelacji, która spowodowała zamknięcie problemu. Ten parametr jest zdefiniowany tylko wtedy, gdy zdarzenie zostało zamknięte przez globalną regułę korelacji.
userid	ID	ID użytkownika, który zamknął zdarzenie (jeśli zdarzenie zostało zamknięte ręcznie).
suppressed	integer	Czy zdarzenie jest wyciszone. Możliwe wartości: 0 - zdarzenie jest w stanie normalnym; 1 - zdarzenie jest wyciszone.
opdata	string	Dane operacyjne z rozwiniętymi makrami.
urls	array	Aktywne adresy URL typu nośnika.

Znacznik zdarzenia

Obiekt znacznika zdarzenia ma następujące właściwości.

Właściwość	Type	Opis
tag	string	Nazwa znacznika zdarzenia.
value	string	Wartość znacznika zdarzenia.

URL typu nośnika

Obiekt URL typu nośnika ma następujące właściwości.

Właściwość	Typ	Opis
name	string	Nazwa URL zdefiniowanego dla typu nośnika.
url	string	Wartość URL zdefiniowana dla typu nośnika.

Wyniki będą zawierać wpisy tylko dla aktywnych typów nośników z włączonym wpisem menu zdarzenia. Makra użyte we właściwościach zostaną rozwinięte, ale jeśli jedna z właściwości zawiera nierozwinięte makro, obie właściwości zostaną wykluczone z wyników. Obsługiwane makra opisano w sekcji *Obsługiwane makra*.

event.acknowledge

Opis

`object event.acknowledge(object/array parameters)`

Ta metoda umożliwia aktualizację zdarzeń. Można wykonać następujące działania aktualizacyjne:

- Zamknięcie zdarzenia. Jeśli zdarzenie jest już rozwiązane, to działanie zostanie pominięte.
- Potwierdzenie zdarzenia. Jeśli zdarzenie jest już potwierdzone, to działanie zostanie pominięte.
- Cofnięcie potwierdzenia zdarzenia. Jeśli zdarzenie nie jest potwierdzone, to działanie zostanie pominięte.
- Dodanie wiadomości.
- Zmiana ważności zdarzenia. Jeśli zdarzenie ma już tę samą ważność, to działanie zostanie pominięte.
- Wyciszenie zdarzenia. Jeśli zdarzenie jest już wyciszone, to działanie zostanie pominięte.
- Wyłączenie wyciszenia zdarzenia. Jeśli zdarzenie nie jest wyciszone, to działanie zostanie pominięte.
- Zmiana rangi zdarzenia na przyczynę. Jeśli zdarzenie ma już rangę przyczyny, to działanie zostanie pominięte.
- Zmiana rangi zdarzenia na symptom. Jeśli zdarzenie ma już rangę symptomu, to działanie zostanie pominięte.

Attention:
Aktualizować można tylko zdarzenia wyzwalaczy.
Aktualizować można tylko zdarzenia problemów.
Aby zamknąć zdarzenie lub zmienić jego ważność, wymagane są uprawnienia odczytu/zapisu do wyzwalacza.
Aby zamknąć zdarzenie, w wyzwalaczu musi być dozwolone ręczne zamykanie.

Note:
Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywoływania tej metody mogą zostać odebrane w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object/array)` Parametry zawierające identyfikatory zdarzeń oraz operacje aktualizacji, które należy wykonać.

Parametr	Type	Opis
eventids	ID/array	Identyfikatory zdarzeń, które mają zostać potwierdzone. Zachowanie parametru: - *wymagany*

Parametr	Type	Opis
action	integer	Działanie(a) aktualizacji zdarzenia. Możliwe wartości bitmapy: 1 - zamknij problem; 2 - potwierdź zdarzenie; 4 - dodaj wiadomość; 8 - zmień ważność; 16 - cofnij potwierdzenie zdarzenia; 32 - wycisz zdarzenie; 64 - wyłącz wyciszenie zdarzenia; 128 - zmień rangę zdarzenia na przyczynę; 256 - zmień rangę zdarzenia na symptom. To pole jest maską bitową; akceptowana jest dowolna suma możliwych wartości bitmapy (na przykład 34 dla potwierdzenia i wyciszenia zdarzenia). Zachowanie parametru: - *wymagany*
cause_eventid	ID	Identyfikator zdarzenia będącego przyczyną. Zachowanie parametru: - *wymagany*, jeśli `action` zawiera bit „change event rank to symptom”
message	string	Treść wiadomości. Zachowanie parametru: - *wymagany*, jeśli `action` zawiera bit „add message”
severity	integer	Nowa ważność dla zdarzeń. Możliwe wartości: 0 - niesklasyfikowane; 1 - informacja; 2 - ostrzeżenie; 3 - średni; 4 - wysoki; 5 - katastrofa. Zachowanie parametru: - *wymagany*, jeśli `action` zawiera bit „change severity”
suppress_until	integer	Znacznik czasu Unix, do którego zdarzenie ma być wyciszone. Jeśli ustawiono wartość „0”, wyciszenie będzie bezterminowe. Zachowanie parametru: - *wymagany*, jeśli `action` zawiera bit „suppress event”

Zwracane wartości

`(object)` Zwraca obiekt zawierający identyfikatory zaktualizowanych zdarzeń we właściwości `eventids`.

Przykłady

Potwierdzanie zdarzenia

Potwierdź pojedyncze zdarzenie i pozostaw wiadomość.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "event.acknowledge",
    "params": {
        "eventids": "20427",
        "action": 6,
```

```
        "message": "Problem rozwiązany."
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "eventids": [
            "20427"
        ]
    },
    "id": 1
}
```

Zmiana ważności zdarzenia

Zmień ważność wielu zdarzeń i pozostaw wiadomość.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "event.acknowledge",
    "params": {
        "eventids": ["20427", "20428"],
        "action": 12,
        "message": "Maintenance required to fix it.",
        "severity": 4
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "eventids": [
            "20427",
            "20428"
        ]
    },
    "id": 1
}
```

Źródło

CEvent::acknowledge() w *ui/include/classes/api/services/CEvent.php*.

event.get

Opis

`integer/array event.get(object parameters)`

Ta metoda umożliwia pobieranie zdarzeń zgodnie z podanymi parametrami.

Attention:
Ta metoda może zwracać zdarzenia usuniętej encji, jeśli zdarzenia te nie zostały jeszcze usunięte przez housekeeper.

Note:
Ta metoda jest dostępna dla użytkowników dowolnego typu. Uprawnienia do wywoływania tej metody mogą zostać cofnięte w ustawieniach roli użytkownika. Więcej informacji można znaleźć w sekcji Role użytkowników.

Parametry

`(object)` Parametry definiujące żądane dane wyjściowe.

Metoda obsługuje następujące parametry.

Parametr	Typ	Opis
eventids	ID/array	Zwracaj tylko zdarzenia o podanych ID.
groupids	ID/array	Zwracaj tylko zdarzenia utworzone przez obiekty należące do podanych grup hostów.
hostids	ID/array	Zwracaj tylko zdarzenia utworzone przez obiekty należące do podanych hostów.
objectids	ID/array	Zwracaj tylko zdarzenia utworzone przez podane obiekty.
source	integer	Zwracaj tylko zdarzenia o podanym typie. Listę obsługiwanych typów zdarzeń można znaleźć na stronie obiektu event. Domyślnie: 0 - zdarzenia wyzwalaczy.
object	integer	Zwracaj tylko zdarzenia utworzone przez obiekty podanego typu. Listę obsługiwanych typów obiektów można znaleźć na stronie obiektu event. Domyślnie: 0 - wyzwalacz.
acknowledged	boolean	Jeśli ustawiono `true`, zwracaj tylko potwierdzone zdarzenia.
action	integer	Zwracaj tylko zdarzenia, dla których wykonano podane akcje aktualizacji zdarzenia. W przypadku wielu akcji użyj sumy dowolnych akceptowalnych wartości bitmapy jako maski bitowej (na przykład 34 dla potwierdzenia i wyciszenia zdarzenia).
action_userids	ID/array	Zwracaj tylko zdarzenia z podanymi ID użytkowników, którzy wykonali akcje aktualizacji zdarzenia.
suppressed	boolean	Jeśli ustawiono `true`, zwracaj tylko wyciszone zdarzenia.
symptom	boolean	Jeśli ustawiono `true`, zwracaj tylko zdarzenia symptomów.
severities	integer/array	Zwracaj tylko zdarzenia o podanych poziomach ważności zdarzeń. Ma zastosowanie tylko wtedy, gdy object to wyzwalacz.
trigger_severities	integer/array	Zwracaj tylko zdarzenia o podanych poziomach ważności wyzwalaczy. Ma zastosowanie tylko wtedy, gdy object to wyzwalacz.
evaltype	integer	Metoda oceny tagów. Możliwe wartości: 0 - *(domyślnie)* And/Or; 2 - Or.
tags	array	Zwracaj tylko zdarzenia z podanymi tagami. Format: `[{"tag": "<tag>", "value": "<value>", "operator": "<operator>"}, ...]`. Pusta tablica zwraca wszystkie zdarzenia. Możliwe wartości operatora: 0 - *(domyślnie)* Zawiera; 1 - Równa się; 2 - Nie zawiera; 3 - Nie równa się; 4 - Istnieje; 5 - Nie istnieje.
eventid_from	string	Zwracaj tylko zdarzenia o ID większym lub równym podanemu ID.
eventid_till	string	Zwracaj tylko zdarzenia o ID mniejszym lub równym podanemu ID.
time_from	timestamp	Zwracaj tylko zdarzenia utworzone o podanym czasie lub później.
time_till	timestamp	Zwracaj tylko zdarzenia utworzone o podanym czasie lub wcześniej.
problem_time_from	timestamp	Zwraca tylko zdarzenia, które były w stanie problemu od `problem_time_from`, niezależnie od ich bieżącego statusu. Ma zastosowanie tylko wtedy, gdy source jest zdarzeniem wyzwalacza, a object jest wyzwalaczem. Ten parametr jest wymagany, jeśli określono `problem_time_till`.

Parametr	Typ	Opis
problem_time_till	timestamp	Zwraca tylko zdarzenia, które były w stanie problemu do `problem_time_till`, niezależnie od ich bieżącego statusu. Ma zastosowanie tylko wtedy, gdy source jest zdarzeniem wyzwalacza, a object jest wyzwalaczem. Ten parametr jest wymagany, jeśli określono `problem_time_from`.
value	integer/array	Zwracaj tylko zdarzenia o podanych wartościach.
selectAcknowledges	query	Zwracaj właściwość `acknowledges` z aktualizacjami zdarzenia. Aktualizacje zdarzenia są sortowane w odwrotnej kolejności chronologicznej. Obiekt aktualizacji zdarzenia ma następujące właściwości: `acknowledgeid` - `(ID)` ID potwierdzenia; `userid` - `(ID)` ID użytkownika, który zaktualizował zdarzenie; `clock` - `(timestamp)` czas aktualizacji zdarzenia; `message` - `(string)` treść wiadomości; `action` - `(integer)` wykonana akcja aktualizacji, zobacz `event.acknowledge`; `old_severity` - `(integer)` ważność zdarzenia przed tą akcją aktualizacji; `new_severity` - `(integer)` ważność zdarzenia po tej akcji aktualizacji; `suppress_until` - `(timestamp)` czas, do którego zdarzenie będzie wyciszone; `taskid` - `(ID)` ID zadania, jeśli bieżące zdarzenie przechodzi zmianę rangi; `username` - `(string)` nazwa użytkownika, który zaktualizował zdarzenie; `name` - `(string)` imię użytkownika, który zaktualizował zdarzenie; `surname` - `(string)` nazwisko użytkownika, który zaktualizował zdarzenie. Obsługuje `count`.
selectAlerts	query	Zwracaj właściwość `alerts` z alertami wygenerowanymi przez zdarzenie. Alerty są sortowane w odwrotnej kolejności chronologicznej.
selectHosts	query	Zwracaj właściwość `hosts` z hostami zawierającymi obiekt, który utworzył zdarzenie. Obsługiwane tylko dla zdarzeń wygenerowanych przez wyzwalacze, pozycje lub reguły LLD.
selectRelatedObject	query	Zwracaj właściwość `relatedObject` z obiektem, który utworzył zdarzenie. Typ zwracanego obiektu zależy od typu zdarzenia.
selectSuppressionData	query	Zwracaj właściwość `suppression_data` z listą aktywnych okresów utrzymaniowych i ręcznych wyciszeń: `maintenanceid` - `(ID)` ID okresu utrzymaniowego; `userid` - `(ID)` ID użytkownika, który wyciszył zdarzenie; `suppress_until` - `(integer)` czas, do którego zdarzenie jest wyciszone.
selectTags	query	Zwracaj właściwość `tags` z tagami zdarzenia.
filter	object	Zwracaj tylko te wyniki, które dokładnie odpowiadają podanemu filtrowi. Akceptuje obiekt, w którym klucze są nazwami właściwości, a wartości są pojedynczą wartością lub tablicą wartości do dopasowania. Nie obsługuje właściwości typu danych `text` data type.
sortfield	string/array	Sortuj wynik według podanych właściwości. Możliwe wartości: `eventid`, `objectid`, `clock`. Możliwe wartości przy użyciu razem z `groupBy`: `objectid`. Możliwe wartości przy użyciu razem z `countOutput` i `groupBy`: `objectid`, `rowscount`.

Parametr	Typ	Opis
groupBy	string/array	Grupuj wyniki według podanych właściwości. Określone właściwości zostaną zwrócone w wynikach. Możliwe wartości: `objectid`.
countOutput	boolean	Te parametry opisano w komentarzu referencyjnym.
editable	boolean	
excludeSearch	boolean	
limit	integer	
output	query	
preservekeys	boolean	
search	object	
searchByAny	boolean	
searchWildcardsEnabled	boolean	
sortorder	string/array	
startSearch	boolean	

Zwracane wartości

`(integer/array)` Zwraca:

- tablicę obiektów
- liczbę pobranych obiektów, jeśli użyto parametru `countOutput`, ale nie użyto parametru `groupBy`
- tablicę obiektów z wynikami agregacji, jeśli użyto parametru `groupBy`

Przykłady

Pobieranie zdarzeń wyzwalacza

Pobierz najnowsze zdarzenia z wyzwalacza „22395”.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "event.get",
    "params": {
        "output": "extend",
        "selectAcknowledges": "extend",
        "selectSuppressionData": "extend",
        "selectTags": "extend",
        "objectids": "22395",
        "sortfield": ["clock", "eventid"],
        "sortorder": "DESC"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "eventid": "20",
            "source": "0",
            "object": "0",
            "objectid": "22395",
            "clock": "1728658089",
            "value": "0",
            "acknowledged": "0",
            "ns": "461809482",
            "name": "Średnie obciążenie jest zbyt wysokie (obciążenie na CPU powyżej 1.5 przez 5 min)",
            "severity": "0",
            "r_eventid": "0",
            "c_eventid": "0",
```

```
            "correlationid": "0",
            "userid": "0",
            "cause_eventid": "0",
            "acknowledges": [],
            "opdata": "Średnie obciążenia(1m 5m 15m): (1.6328 3.0522 2.2515), liczba CPU: 2",
            "suppression_data": [],
            "suppressed": "0",
            "tags": [
                {
                    "tag": "scope",
                    "value": "capacity"
                },
                {
                    "tag": "scope",
                    "value": "performance"
                },
                {
                    "tag": "component",
                    "value": "cpu"
                },
                {
                    "tag": "class",
                    "value": "os"
                },
                {
                    "tag": "target",
                    "value": "linux"
                }
            ],
            "urls": []
        },
        {
            "eventid": "4",
            "source": "0",
            "object": "0",
            "objectid": "22395",
            "clock": "1728657737",
            "value": "1",
            "acknowledged": "1",
            "ns": "460759366",
            "name": "Średnie obciążenie jest zbyt wysokie (obciążenie na CPU powyżej 1.5 przez 5 min)",
            "severity": "3",
            "r_eventid": "20",
            "c_eventid": "0",
            "correlationid": "0",
            "userid": "0",
            "cause_eventid": "0",
            "acknowledges": [
                {
                    "acknowledgeid": "1",
                    "userid": "1",
                    "clock": "1728657938",
                    "message": "Środowisko testowe. Proszę zignorować ten alert.",
                    "action": "38",
                    "old_severity": "0",
                    "new_severity": "0",
                    "suppress_until": "1728744338",
                    "taskid": "0",
                    "username": "Admin",
                    "name": "Zabbix",
                    "surname": "Administrator"
                }
```

```
            ],
            "opdata": "Średnie obciążenia(1m 5m 15m): (1.6328 3.0522 2.2515), liczba CPU: 2",
            "suppression_data": [
                {
                    "maintenanceid": "0",
                    "suppress_until": "1728744338",
                    "userid": "1"
                }
            ],
            "suppressed": "1",
            "tags": [
                {
                    "tag": "scope",
                    "value": "capacity"
                },
                {
                    "tag": "scope",
                    "value": "performance"
                },
                {
                    "tag": "component",
                    "value": "cpu"
                },
                {
                    "tag": "class",
                    "value": "os"
                },
                {
                    "tag": "target",
                    "value": "linux"
                }
            ],
            "urls": []
        }
    ],
    "id": 1
}
```


Pobieranie zdarzeń według przedziału czasu

Pobierz wszystkie zdarzenia utworzone między 17 a 18 października 2012 roku, w odwrotnej kolejności chronologicznej.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "event.get",
    "params": {
        "output": "extend",
        "time_from": "1350432000",
        "time_till": "1350518400",
        "sortfield": ["clock", "eventid"],
        "sortorder": "DESC"
    },
    "id": 1
}
```

Odpowiedź:


```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "eventid": "20617",
            "source": "0",
```

```
            "object": "0",
            "objectid": "14282",
            "clock": "1350477816",
            "value": "1",
            "acknowledged": "0",
            "ns": "0",
            "name": "Mniej niż 25% wolnego miejsca w pamięci podręcznej historii",
            "severity": "3",
            "r_eventid": "0",
            "c_eventid": "0",
            "correlationid": "0",
            "userid": "0",
            "cause_eventid": "0",
            "opdata": "",
            "suppressed": "0",
            "urls": []
        },
        {
            "eventid": "20616",
            "source": "0",
            "object": "0",
            "objectid": "14281",
            "clock": "1350477814",
            "value": "0",
            "acknowledged": "0",
            "ns": "0",
            "name": "Procesy Zabbix trapper są zajęte w ponad 75%",
            "severity": "0",
            "r_eventid": "0",
            "c_eventid": "0",
            "correlationid": "0",
            "userid": "0",
            "cause_eventid": "0",
            "opdata": "",
            "suppressed": "0",
            "urls": []
        },
        {
            "eventid": "20615",
            "source": "0",
            "object": "0",
            "objectid": "14281",
            "clock": "1350477541",
            "value": "1",
            "acknowledged": "0",
            "ns": "0",
            "name": "Procesy Zabbix trapper są zajęte w ponad 75%",
            "severity": "3",
            "r_eventid": "20616",
            "c_eventid": "0",
            "correlationid": "0",
            "userid": "0",
            "cause_eventid": "0",
            "opdata": "",
            "suppressed": "0",
            "urls": []
        }
    ],
    "id": 1
}
```


Pobieranie zdarzeń potwierdzonych przez określonego użytkownika

Pobieranie zdarzeń potwierdzonych przez użytkownika o ID=10

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "event.get",
    "params": {
        "output": "extend",
        "action": 2,
        "action_userids": [10],
        "selectAcknowledges": ["userid", "action"],
        "sortfield": ["eventid"],
        "sortorder": "DESC"
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "eventid": "503",
            "source": "0",
            "object": "0",
            "objectid": "23162",
            "clock": "1747212236",
            "value": "1",
            "acknowledged": "1",
            "ns": "413470863",
            "name": "Number of installed packages has been changed",
            "severity": "2",
            "r_eventid": "0",
            "c_eventid": "0",
            "correlationid": "0",
            "userid": "0",
            "cause_eventid": "0",
            "acknowledges": [
                {
                    "userid": "10",
                    "action": "2"
                }
            ],
            "opdata": "",
            "suppressed": "0",
            "urls": []
        }
    ],
    "id": 1
}
```

Pobieranie najważniejszych wyzwalaczy według liczby zdarzeń problemowych

Pobierz 5 najważniejszych wyzwalaczy o poziomach ważności „Warning”, „Average”, „High” lub „Disaster” wraz z liczbą zdarzeń problemowych w określonym przedziale czasu.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "event.get",
    "params": {
        "countOutput": true,
        "groupBy": "objectid",
        "source": 0,
```

```
        "object": 0,
        "value": 1,
        "time_from": 1672531200,
        "time_till": 1677628800,
        "trigger_severities": [2, 3, 4, 5],
        "sortfield": ["rowscount"],
        "sortorder": "DESC",
        "limit": 5
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "objectid": "232124",
            "rowscount": "27"
        },
        {
            "objectid": "29055",
            "rowscount": "23"
        },
        {
            "objectid": "253731",
            "rowscount": "18"
        },
        {
            "objectid": "254062",
            "rowscount": "11"
        },
        {
            "objectid": "23216",
            "rowscount": "7"
        }
    ],
    "id": 1
}
```

Zobacz także

- Alert
- Pozycja
- Host
- Reguła LLD
- Usługa
- Wyzwalacz

Źródło

CEvent::get() w *ui/include/classes/api/services/CEvent.php*.

Dodatek 1. Komentarz referencyjny

Notacja Typy danych

API Zabbix obsługuje następujące typy danych jako dane wejściowe:

Type	Description
ID	Unikalny identyfikator używany do odwoływania się do encji.

Type	Description
boolean	Wartość logiczna (`true` lub `false`).
flag	Wartość uznawana za `true`, jeśli została przekazana i nie jest równa `null`; w przeciwnym razie wartość jest uznawana za `false`.
integer	Liczba całkowita.
float	Liczba zmiennoprzecinkowa.
string	Ciąg tekstowy.
text	Dłuższy ciąg tekstowy.
timestamp	Znacznik czasu Unix.
array	Uporządkowana sekwencja wartości (zwykła tablica).
object	Tablica asocjacyjna.
query	Wartość definiująca dane, które mają zostać zwrócone. Wartość może być zdefiniowana jako tablica nazw właściwości (aby zwrócić tylko określone właściwości) lub jako jedna ze wstępnie zdefiniowanych wartości: `extend` - zwraca wszystkie właściwości obiektu; `count` - zwraca liczbę pobranych rekordów, obsługiwane tylko przez niektóre podwybory.

Attention:
API Zabbix zawsze zwraca wartości wyłącznie jako ciągi znaków lub tablice.

Zachowanie właściwości

Niektóre właściwości obiektu są oznaczone krótkimi etykietami opisującymi ich zachowanie. Używane są następujące etykiety:

- ***tylko do odczytu*** - wartość właściwości jest ustawiana automatycznie i nie może być definiowana ani zmieniana przez użytkownika, nawet w niektórych szczególnych warunkach (np. *tylko do odczytu* dla obiektów dziedziczonych lub obiektów wykrytych);
- ***tylko do zapisu*** - wartość właściwości może zostać ustawiona, ale później nie można uzyskać do niej dostępu;
- ***stała*** - wartość właściwości może zostać ustawiona podczas tworzenia obiektu, ale później nie może być zmieniona;
- ***obsługiwana*** - ustawienie wartości właściwości nie jest wymagane, ale jest dozwolone w niektórych szczególnych warunkach (np. *obsługiwana*, jeśli `type` jest ustawione na ”Simple check”, ”External check”, ”SSH agent”, ”TELNET agent” lub ”HTTP agent”); należy jednak pamiętać, że właściwości oznaczone jako *obsługiwana* mogą nadal być ustawiane na swoje wartości domyślne niezależnie od warunków;
- ***wymagana*** - ustawienie wartości właściwości jest wymagane dla wszystkich operacji (z wyjątkiem operacji pobierania) lub w niektórych szczególnych warunkach (np. *wymagana* dla operacji tworzenia; *wymagana*, jeśli `operationtype` jest ustawione na ”global script”, a `opcommand_hst` nie jest ustawione).

Note:
W przypadku operacji aktualizacji właściwość jest uznawana za „ustawioną”, gdy zostanie ustawiona podczas operacji aktualizacji.

Właściwości, które nie są oznaczone etykietami, są opcjonalne.

Zachowanie parametrów

Niektóre parametry operacji są oznaczone krótkimi etykietami opisującymi ich zachowanie dla danej operacji. Używane są następujące etykiety:

- ***tylko do odczytu*** - wartość parametru jest ustawiana automatycznie i nie może być definiowana ani zmieniana przez użytkownika, nawet w niektórych szczególnych warunkach (np. *tylko do odczytu* dla obiektów dziedziczonych lub obiektów wykrytych);
- ***tylko do zapisu*** - wartość parametru może zostać ustawiona, ale później nie można uzyskać do niej dostępu;
- ***obsługiwany*** - ustawienie wartości parametru nie jest wymagane, ale jest dozwolone w niektórych szczególnych warunkach (np. *obsługiwany*, jeśli `operating_mode` obiektu Proxy jest ustawiony na ”passive proxy”); należy jednak pamiętać, że parametry oznaczone jako *obsługiwany* nadal mogą być ustawiane na wartości domyślne niezależnie od warunków;
- ***wymagany*** - wartość parametru musi zostać ustawiona.

Parametry, które nie są oznaczone etykietami, są opcjonalne.

Zastrzeżona wartość ID ”0” Zastrzeżona wartość ID ”0” może być używana do filtrowania elementów i usuwania obiektów , do których istnieją odniesienia. Na przykład, aby usunąć odwołanie do proxy z hosta , proxyid powinno być ustawione na 0 (”proxyid”: ”0”) lub aby filtrować hosty monitorowane przez opcję serwera proxyids powinno być ustawione na 0 (”proxyids”: ”0”).

Wspólne parametry metod "get" Następujące parametry są obsługiwane przez wszystkie metody `get`:

Parametr	Typ	Opis
countOutput	boolean	Zwraca liczbę rekordów w wyniku zamiast rzeczywistych danych.
editable	boolean	Jeśli ustawiono na `true`, zwraca tylko obiekty, do których użytkownik ma uprawnienia zapisu. Domyślnie: `false`.
excludeSearch	boolean	Zwraca wyniki, które nie pasują do kryteriów podanych w parametrze `search`.
filter	object	Zwraca tylko te wyniki, które dokładnie odpowiadają podanemu filtrowi. Akceptuje obiekt, w którym kluczami są nazwy właściwości (np. właściwości obiektu Host w `host.get`, właściwości obiektu Item w `item.get` itd.), a wartościami są pojedyncza wartość lub tablica wartości do dopasowania. Nie obsługuje właściwości typu danych `text` data type. Należy pamiętać, że niektóre metody mają specyficzną funkcjonalność dla tego parametru, opisaną na stronie danej metody (np. parametr `filter` w host.get obsługuje również właściwości interfejsu hosta).
limit	integer	Ogranicza liczbę zwracanych rekordów.
output	query	Właściwości obiektu, które mają zostać zwrócone. Należy pamiętać, że identyfikator obiektu (tj. `hostid`, `itemid` itd.) jest zawsze uwzględniany w odpowiedzi, nawet jeśli nie został określony w parametrze `output`. Domyślnie: `extend`.
preservekeys	boolean	Używa identyfikatorów jako kluczy w wynikowej tablicy.
search	object	Zwraca wyniki pasujące do podanego wzorca (bez rozróżniania wielkości liter). Akceptuje obiekt, w którym kluczami są nazwy właściwości (np. właściwości obiektu Host w `host.get`, właściwości obiektu Item w `item.get` itd.), a wartościami są ciągi znaków do wyszukania. Jeśli nie podano dodatkowych opcji, zostanie wykonane wyszukiwanie `LIKE "%…%"`. Obsługuje tylko właściwości typu danych `string` i `text` data type. Należy pamiętać, że niektóre metody mają specyficzną funkcjonalność dla tego parametru, opisaną na stronie danej metody (np. parametr `search` w host.get obsługuje również właściwości interfejsu hosta).
searchByAny	boolean	Jeśli ustawiono na `true`, zwraca wyniki pasujące do dowolnego z kryteriów podanych w parametrze `filter` lub `search`, zamiast do wszystkich. Domyślnie: `false`.
searchWildcardsEnabled	boolean	Jeśli ustawiono na `true`, włącza użycie znaku "*" jako znaku wieloznacznego w parametrze `search`. Domyślnie: `false`.
sortfield	string/array	Sortuje wynik według podanych właściwości. Listę właściwości, które mogą być używane do sortowania, można znaleźć w opisie konkretnej metody API get. Makra nie są rozwijane przed sortowaniem. Jeśli nie podano wartości, dane zostaną zwrócone bez sortowania.
sortorder	string/array	Kolejność sortowania. Jeśli przekazano tablicę, każda wartość zostanie dopasowana do odpowiadającej jej właściwości podanej w parametrze `sortfield`. Możliwe wartości: `ASC` - *(domyślnie)* rosnąco; `DESC` - malejąco.
startSearch	boolean	Parametr `search` będzie porównywał początek pól, czyli zamiast tego wykona wyszukiwanie `LIKE "…%"`. Ignorowane, jeśli `searchWildcardsEnabled` jest ustawione na `true`.

Flagi pochodzenia encji Metody get zwracają właściwość `flags` dla encji powiązanych z wykrywaniem niskopoziomowym (reguła LLD/prototyp reguły LLD, pozycja/prototyp pozycji itd.). Ta właściwość jest przydatna do określenia, czy encja została wykryta, czy nie, ponieważ możliwości edycji wykrytych encji są ograniczone.

Właściwość `flags` zwraca wynik oparty na kombinacji (operacja „+") tych wartości:

Value	Description
0	Encja bazowa (pozycja, wyzwalacz, wykres, host)
1	Reguła wykrywania niskopoziomowego
2	Dowolny prototyp (prototyp pozycji, prototyp wyzwalacza, prototyp reguły LLD itd.)
4	Wykryta encja (wykryta pozycja, wyzwalacz, wykres, host, reguła LLD)

Łączna wartość zwracana przez właściwość `flags` może być następująca:

Value	Combination of	Description
0	0	Zwykła encja (pozycja, wyzwalacz, wykres, host).
2	2	Prototyp encji (prototyp pozycji, prototyp wyzwalacza itd.).
6	2+4	Wykryta pozycja, wyzwalacz, wykres, host (utworzone z prototypu).
1	1	Reguła wykrywania niskopoziomowego.
3	1+2	Prototyp reguły wykrywania niskopoziomowego.
5	1+4	Wykryta reguła wykrywania niskopoziomowego (utworzona z prototypu).
7	1+2+4	Wykryty prototyp reguły wykrywania niskopoziomowego.

Przykłady Sprawdzenie uprawnień użytkownika

Czy użytkownik ma uprawnienia do zapisu do hostów, których nazwy zaczynają się od "MySQL" lub "Linux" ?

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "host.get",
    "params": {
        "countOutput": true,
        "search": {
            "host": ["MySQL", "Linux"]
        },
        "editable": true,
        "startSearch": true,
        "searchByAny": true
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": "0",
    "id": 1
}
```

Note:
Wynik zero oznacza brak hostów z uprawnieniami do odczytu/zapisu.

Zliczanie niedopasowań

Policz liczbę hostów, których nazwy nie zawierają podciągu "ubuntu"

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "host.get",
```

```
    "params": {
        "countOutput": true,
        "search": {
            "host": "ubuntu"
        },
        "excludeSearch": true
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": "44",
    "id": 1
}
```

Wyszukiwanie hostów przy użyciu symboli wieloznacznych

Znajdź hosty, których nazwa zawiera słowo „server” i które mają porty interfejsów „10050” lub „10071”. Posortuj wynik według nazwy hosta malejąco i ogranicz go do 5 hostów.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "host.get",
    "params": {
        "output": ["hostid", "host"],
        "selectInterfaces": ["port"],
        "filter": {
            "port": ["10050", "10071"]
        },
        "search": {
            "host": "*server*"
        },
        "searchWildcardsEnabled": true,
        "searchByAny": true,
        "sortfield": "host",
        "sortorder": "DESC",
        "limit": 5
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "hostid": "50003",
            "host": "WebServer-Tomcat02",
            "interfaces": [
                {
                    "port": "10071"
                }
            ]
        },
        {
            "hostid": "50005",
            "host": "WebServer-Tomcat01",
            "interfaces": [
                {
                    "port": "10071"
```

```
                }
            ]
        },
        {
            "hostid": "50004",
            "host": "WebServer-Nginx",
            "interfaces": [
                {
                    "port": "10071"
                }
            ]
        },
        {
            "hostid": "99032",
            "host": "MySQL server 01",
            "interfaces": [
                {
                    "port": "10050"
                }
            ]
        },
        {
            "hostid": "99061",
            "host": "Linux server 01",
            "interfaces": [
                {
                    "port": "10050"
                }
            ]
        }
    ],
    "id": 1
}
```

Wyszukiwanie hostów przy użyciu symboli wieloznacznych z parametrem ”preservekeys”

Jeśli dodasz parametr ”preservekeys” do poprzedniego żądania, wynik zostanie zwrócony jako tablica asocjacyjna, gdzie kluczami są identyfikatory obiektów.

Żądanie:

```
{
    "jsonrpc": "2.0",
    "method": "host.get",
    "params": {
        "output": ["hostid", "host"],
        "selectInterfaces": ["port"],
        "filter": {
            "port": ["10050", "10071"]
        },
        "search": {
            "host": "*server*"
        },
        "searchWildcardsEnabled": true,
        "searchByAny": true,
        "sortfield": "host",
        "sortorder": "DESC",
        "limit": 5,
        "preservekeys": true
    },
    "id": 1
}
```

Odpowiedź:

```
{
    "jsonrpc": "2.0",
    "result": {
        "50003": {
            "hostid": "50003",
            "host": "WebServer-Tomcat02",
            "interfaces": [
                {
                    "port": "10071"
                }
            ]
        },
        "50005": {
            "hostid": "50005",
            "host": "WebServer-Tomcat01",
            "interfaces": [
                {
                    "port": "10071"
                }
            ]
        },
        "50004": {
            "hostid": "50004",
            "host": "WebServer-Nginx",
            "interfaces": [
                {
                    "port": "10071"
                }
            ]
        },
        "99032": {
            "hostid": "99032",
            "host": "MySQL server 01",
            "interfaces": [
                {
                    "port": "10050"
                }
            ]
        },
        "99061": {
            "hostid": "99061",
            "host": "Linux server 01",
            "interfaces": [
                {
                    "port": "10050"
                }
            ]
        }
    },
    "id": 1
}
```


Załącznik 2. Zmiany od 7.4 do 8.0

Zmiany powodujące niezgodność historia

ZBXNEXT-10069 Dodano nowy parametr `maxValueSize` do metody history.get. Jeśli żądasz danych dla pozycji z wartością binarną (`history=5`), ustaw `maxValueSize` na `null`; w przeciwnym razie `history.get` zwróci wartość pozycji obciętą do 64 KiB.

host

ZBXNEXT-10387 `host.massupdate`: Usunięto metodę. Zamiast niej użyj `host.update`.

hostgroup

ZBXNEXT-10387 `hostgroup.massupdate`: Metoda usunięta. Zamiast niej użyj `hostgroup.update`, `hostgroup.massadd` lub `hostgroup.massremove`.

hostinterface

ZBXNEXT-10387 `hostinterface.replacehostinterfaces`: Usunięto metodę. Zamiast niej użyj `hostinterface.update`, `hostinterface.massadd` lub `hostinterface.massremove`.

szablon

ZBXNEXT-10387 `template.massupdate`: Usunięto metodę. Zamiast niej użyj `template.update`, `template.massadd` lub `template_massremove`.

templategroup

ZBXNEXT-10387 `templategroup.massupdate`: Usunięto metodę. Zamiast niej użyj `templategroup.update`, `templategroup.massadd` lub `templategroup.massremove`.

Inne zmiany i poprawki błędów konektor

ZBXNEXT-10069 Dodano nową wartość `item_value_type` (64 - JSON) do obiektu connector.

pulpit

ZBXNEXT-4769 Dodano nowe pole widgetu pulpitu `show_hostnames` do widgetu graph.
ZBXNEXT-9546 Dodano nowe pola widgetu pulpitu `ds.0.item_tags_evaltype`, `ds.0.item_tags.0.tag`, `ds.0.item_tags.0.operato` oraz `ds.0.item_tags.0.value` do widgetów svggraph i piechart.
ZBXNEXT-10158 Dodano nowe pola widgetu pulpitu `columns.0.aggregate_columns`, `columns.0.combined_column_name` oraz `columns.0.column_aggregate_function` do widgetu topitems.
ZBXNEXT-9424, ZBXNEXT-4769 Dodano nowy typ widgetu pulpitu scatterplot.
ZBXNEXT-8160 Dodano nowe pola widgetu pulpitu `clustering_mode` oraz `clustering_zoom_level` do widgetu geomap.
ZBXNEXT-943 Dodano nowe pole widgetu pulpitu `ds.0.invert_values` do widgetu graph.

templatedashboard

ZBXNEXT-9424 Dodano nowy typ widgetu pulpitu szablonu scatterplot.

historia

ZBXNEXT-10069 Dodano nową wartość `history` (6 - JSON) do metody history.get.
ZBXNEXT-10069 Dodano nowy obiekt `JSON history`.

hostprototype

ZBXNEXT-9546 Dodano nowy parametr `selectInheritedTags` do metody hostprototype.get.

httptest

ZBXNEXT-9546 Dodano nowe parametry `inheritedTags` i `selectInheritedTags` do metody httptest.get.

pozycja

ZBXNEXT-10069 Dodano nową wartość `value_type` (6 - JSON) do obiektu item.
ZBXNEXT-9546 Dodano nowe parametry `inheritedTags` i `selectInheritedTags` do metody item.get.

itemprototype

ZBXNEXT-10069 Dodano nową wartość `value_type` (6 - JSON) do obiektu itemprototype.
ZBXNEXT-9546 Dodano nowy parametr `selectInheritedTags` do metody itemprototype.get.

szablon

ZBXNEXT-9546 Dodano nowe parametry `inheritedTags` i `selectInheritedTags` do metody template.get.

wyzwalacz

ZBXNEXT-9546 Dodano nowe parametry `inheritedTags` i `selectInheritedTags` do metody trigger.get.

triggerprototype

ZBXNEXT-9546 Dodano nowy parametr `selectInheritedTags` do metody triggerprototype.get.

triggertag

ZBXNEXT-5467 Dodano właściwość `automatic` do obiektu tagu wyzwalacza.

userdirectory

ZBXNEXT-9834 Dodano właściwości `idp_certificate`, `sp_private_key`, `sp_certificate`, `idp_certificate_hash`, `sp_private_key_hash` oraz `sp_certificate_hash` do obiektu katalog użytkowników.

Załącznik 3. Zmiany w wersji 8.0

8.0.1 Ta wersja nie została jeszcze wydana.

19 Rozszerzenia

Przegląd Chociaż Zabbix oferuje wiele funkcji, zawsze istnieje miejsce na dodatkową funkcjonalność. Rozszerzenia są wygodnym sposobem modyfikowania i zwiększania możliwości monitorowania w Zabbix bez zmiany jego kodu źródłowego.

Możesz rozszerzyć funkcjonalność Zabbix, korzystając albo z wbudowanych opcji rozszerzeń (pozycje trapper, parametry użytkownika itp.), albo używając lub tworząc własne rozszerzenia (moduły ładowalne, wtyczki itp.).

Ta sekcja zawiera przegląd wraz z odwołaniami do wszystkich opcji rozszerzania Zabbix.

Zbieranie danych za pomocą niestandardowych poleceń Pozycje trapper

Pozycje trapper to pozycje, które przyjmują dane przychodzące zamiast je odpytywać. Pozycje trapper są przydatne do wysyłania określonych danych do serwera lub proxy Zabbix, na przykład okresowych danych o dostępności i wydajności w przypadku długotrwale działających skryptów użytkownika. Wysyłanie danych do serwera lub proxy Zabbix jest możliwe przy użyciu narzędzia Zabbix sender lub protokołu Zabbix sender. Wysyłanie danych do serwera Zabbix jest również możliwe przy użyciu metody API `history.push`.

Kontrole zewnętrzne

Kontrola zewnętrzna to pozycja służąca do wykonywania kontroli przez uruchomienie pliku wykonywalnego, na przykład skryptu powłoki lub pliku binarnego.

Kontrole zewnętrzne są wykonywane przez serwer Zabbix lub proxy (gdy host jest monitorowany przez proxy) i nie wymagają uruchomionego agenta na monitorowanym hoście.

Parametry użytkownika

Parametr użytkownika to polecenie zdefiniowane przez użytkownika (powiązane z kluczem zdefiniowanym przez użytkownika), które po wykonaniu może pobrać dane potrzebne z hosta, na którym działa agent Zabbix. Parametry użytkownika są przydatne do konfigurowania pozycji agenta lub agenta 2, które nie są predefiniowane w Zabbix.

Pozycje `system.run[]` Zabbix agent

`system.run[]` Zabbix agent item to pozycja dla polecenia zdefiniowanego przez użytkownika (powiązana ze wstępnie zdefiniowanym kluczem `system.run[]`, na przykład `system.run[myscript.sh]`), które może być wykonywane na hoście, na którym działa Zabbix agent.

Uwaga: pozycje `system.run[]` są domyślnie wyłączone i, jeśli są używane, muszą zostać włączone (dozwolone) oraz zdefiniowane w pliku konfiguracyjnym Zabbix agent lub agent 2 (parametr konfiguracyjny `AllowKey`).

> **Attention:**
> Polecenia zdefiniowane przez użytkownika w pozycjach, takich jak sprawdzenia zewnętrzne, parametry użytkownika i pozycje agenta Zabbix `system.run[]`, są wykonywane przez użytkownika systemu operacyjnego używanego do uruchamiania komponentów Zabbix. Aby wykonać te polecenia, ten użytkownik musi mieć niezbędne uprawnienia.

Pozycje HTTP agent

HTTP agent to pozycja służąca do wykonywania żądań danych przez HTTP/HTTPS. Pozycje HTTP agent są przydatne do wysyłania żądań do punktów końcowych HTTP w celu pobierania danych z usług takich jak *Elasticsearch* i *OpenWeatherMap*, sprawdzania stanu API Zabbix lub stanu serwera WWW Apache albo Nginx itp. Pozycje HTTP agent (z włączonym trapowaniem) mogą również działać jako pozycje trapper.

Pozycje skryptowe

Pozycja skryptowa to pozycja służąca do wykonywania zdefiniowanego przez użytkownika kodu JavaScript, który pobiera dane przez HTTP/HTTPS. Pozycje skryptowe są przydatne, gdy funkcjonalność zapewniana przez pozycje agenta HTTP nie jest wystarczająca. Na przykład w wymagających scenariuszach zbierania danych, które wymagają wielu kroków lub złożonej logiki, pozycję skryptową można skonfigurować tak, aby wykonała wywołanie HTTP, następnie przetworzyła otrzymane dane, a potem przekazała przekształconą wartość do drugiego wywołania HTTP.

> **Note:**
> Pozycje HTTP agent oraz pozycje skryptowe są obsługiwane przez serwer Zabbix i proxy i nie wymagają uruchomionego agenta na monitorowanym hoście.

Zaawansowane rozszerzenia Moduły ładowalne

Moduły ładowalne, napisane w C, są wszechstronną i wydajnościowo zoptymalizowaną opcją rozszerzania funkcjonalności komponentów Zabbix (serwer, proxy, agent) na platformach UNIX. Moduł ładowalny jest zasadniczo biblioteką współdzieloną używaną przez demon Zabbix i ładowaną podczas uruchamiania. Biblioteka powinna zawierać określone funkcje, aby proces Zabbix mógł wykryć, że plik jest rzeczywiście modułem, który może załadować i z którym może pracować.

Moduły ładowalne mają szereg zalet, w tym możliwość dodawania nowych metryk lub implementowania dowolnej innej logiki (na przykład eksportu danych historii Zabbix), wysoką wydajność oraz możliwość tworzenia, używania i udostępniania zapewnianej przez nie funkcjonalności. Przyczynia się to do bezproblemowego utrzymania i pomaga łatwiej dostarczać nową funkcjonalność niezależnie od bazowego kodu Zabbix.

Moduły ładowalne są szczególnie przydatne w złożonych środowiskach monitorowania. Podczas monitorowania systemów wbudowanych, przy dużej liczbie monitorowanych parametrów lub przy użyciu ciężkich skryptów ze złożoną logiką albo długim czasem uruchamiania, rozszerzenia takie jak parametry użytkownika, pozycje agenta Zabbix `system.run[]` oraz kontrole zewnętrzne będą miały wpływ na wydajność. Moduły ładowalne oferują sposób rozszerzania funkcjonalności Zabbix bez poświęcania wydajności.

Wtyczki

Wtyczki rozszerzają możliwości monitorowania Zabbix agent 2. Napisane w języku programowania Go, stanowią alternatywę dla modułów ładowalnych (napisanych w C).

Wtyczka to pakiet Go, który definiuje strukturę i implementuje jeden lub kilka interfejsów wtyczek (*Exporter*, *Collector*, *Configurator*, *Runner*, *Watcher*). Obsługiwane są dwa typy wtyczek Zabbix agent 2:

- Wbudowane wtyczki (obsługiwane od Zabbix 4.4.0)
- Wtyczki ładowalne (obsługiwane od Zabbix 6.0.0)

Zobacz listę wtyczek dostarczanych przez Zabbix.

Instrukcje i samouczki dotyczące tworzenia własnych wtyczek można znaleźć w Developer center.

Dostosowywanie alertów Webhooki

Webhook to typ mediów w Zabbix, który umożliwia rozszerzenie możliwości alertowania Zabbix na zewnętrzne oprogramowanie, takie jak systemy helpdesk, czaty lub komunikatory. Podobnie jak pozycje skryptowe, webhooki są przydatne do wykonywania wywołań HTTP przy użyciu niestandardowego kodu JavaScript, na przykład do wysyłania powiadomień do różnych platform, takich jak Microsoft Teams, Discord i Jira. Możliwe jest również zwrócenie pewnych danych (na przykład o utworzonych zgłoszeniach helpdesk), które są następnie wyświetlane w Zabbix.

Istniejące webhooki są dostępne w repozytorium Git Zabbix. Informacje dotyczące tworzenia niestandardowych webhooków można znaleźć w dokumencie Wytyczne dotyczące tworzenia webhooków.

Skrypty alertów

Skrypt alertu to typ mediów w Zabbix, który umożliwia utworzenie alternatywnego sposobu (skryptu) obsługi alertów Zabbix. Skrypty alertów są przydatne, jeśli istniejące typy mediów do wysyłania alertów w Zabbix nie spełniają Twoich oczekiwań.

Dostosowanie frontendu Własne motywy

Można zmienić wygląd wizualny frontendu Zabbix, używając własnych motywów. Zobacz instrukcje dotyczące tworzenia i stosowania własnych motywów.

Moduły frontend

Moduły frontend zapewniają możliwość rozszerzenia funkcjonalności frontend Zabbix przez dodawanie modułów innych firm lub tworzenie własnych. Za pomocą modułów frontend można dodawać nowe pozycje menu, odpowiadające im widoki, akcje itp.

Skrypty globalne Skrypt globalny to zdefiniowany przez użytkownika zestaw poleceń, które mogą być wykonywane na monitorowanym celu (przez interpreter powłoki (/bin/sh)), w zależności od skonfigurowanego zakresu i uprawnień użytkownika. Skrypty globalne można skonfigurować dla następujących działań:

- Operacja akcji
- Ręczne działanie na hoście
- Ręczne działanie na zdarzeniu

Skrypty globalne są przydatne w wielu przypadkach. Na przykład, jeśli są skonfigurowane dla operacji akcji lub ręcznych działań na hoście, można używać skryptów globalnych do automatycznego lub ręcznego wykonywania zdalnych poleceń, takich jak ponowne uruchamianie aplikacji (serwera WWW, middleware, CRM itp.) lub zwalnianie miejsca na dysku (usuwanie starszych plików, czyszczenie `/tmp` itp.). Inny przykład: jeśli są skonfigurowane dla ręcznych działań na zdarzeniach, można używać skryptów globalnych do zarządzania zgłoszeniami problemów w systemach zewnętrznych.

Skrypty globalne mogą być wykonywane przez serwer Zabbix, proxy lub agent.

Attention:
Polecenia zdefiniowane przez użytkownika są wykonywane z poziomu użytkownika systemu operacyjnego używanego do uruchamiania komponentów Zabbix. Aby wykonać te polecenia, ten użytkownik musi mieć niezbędne uprawnienia.

Zabbix API Zabbix API to API oparte na HTTP, będące częścią frontend Zabbix. Za pomocą Zabbix API można wykonywać następujące operacje:

- Programowo pobierać i modyfikować konfigurację Zabbix.
- Importować i eksportować konfigurację Zabbix.
- Uzyskiwać dostęp do danych historycznych i trendów Zabbix.
- Konfigurować aplikacje do współpracy z Zabbix.
- Integrować Zabbix z oprogramowaniem firm trzecich.
- Automatyzować rutynowe zadania.

Zabbix API składa się z wielu metod, które są umownie pogrupowane w oddzielne API. Każda metoda wykonuje określone zadanie. Informacje o dostępnych metodach, a także przegląd funkcji udostępnianych przez Zabbix API, można znaleźć w referencji metod Zabbix API.

1 Moduły ładowalne

Przegląd

Moduły ładowalne oferują rozwiązanie nastawione na wydajność do rozszerzania funkcjonalności Zabbix.

Funkcjonalność Zabbix można rozszerzać na wiele sposobów, na przykład za pomocą parametrów użytkownika, kontroli zewnętrznych oraz pozycji agenta Zabbix system.run. Rozwiązania te działają bardzo dobrze, ale mają jedną istotną wadę, a mianowicie fork(). Zabbix musi utworzyć nowy proces za każdym razem, gdy obsługuje metrykę użytkownika, co nie jest korzystne dla wydajności. Zwykle nie stanowi to dużego problemu, jednak może być poważnym wyzwaniem podczas monitorowania systemów wbudowanych, przy dużej liczbie monitorowanych parametrów lub w przypadku ciężkich skryptów ze złożoną logiką albo długim czasem uruchamiania.

Obsługa modułów ładowalnych umożliwia rozszerzanie agenta Zabbix, serwera i proxy bez poświęcania wydajności.

Moduł ładowalny jest zasadniczo biblioteką współdzieloną używaną przez demon Zabbix i ładowaną podczas uruchamiania. Biblioteka powinna zawierać określone funkcje, aby proces Zabbix mógł wykryć, że plik jest rzeczywiście modułem, który można załadować i z którym można pracować.

Moduły ładowalne mają szereg zalet. Bardzo ważne są wysoka wydajność i możliwość implementacji dowolnej logiki, ale być może najważniejszą zaletą jest możliwość tworzenia, używania i udostępniania modułów Zabbix. Przyczynia się to do bezproblemowego utrzymania i ułatwia dostarczanie nowej funkcjonalności w prostszy sposób oraz niezależnie od bazowego kodu Zabbix.

Licencjonowanie modułów i ich dystrybucja w postaci binarnej są regulowane licencją AGPL-3.0 (moduły są linkowane z Zabbix w czasie działania i używają nagłówków Zabbix; cały kod Zabbix jest objęty licencją AGPL-3.0 od wersji Zabbix 7.0). Zabbix nie gwarantuje zgodności binarnej.

Stabilność API modułów jest gwarantowana w trakcie jednego cyklu wydania Zabbix LTS (Long Term Support). Stabilność API Zabbix nie jest gwarantowana (technicznie możliwe jest wywoływanie wewnętrznych funkcji Zabbix z modułu, ale nie ma gwarancji, że takie moduły będą działać).

API modułu

Aby biblioteka współdzielona była traktowana jako moduł Zabbix, powinna implementować i eksportować kilka funkcji. Obecnie w API modułu Zabbix istnieje sześć funkcji, z których tylko jedna jest obowiązkowa, a pozostałe pięć jest opcjonalnych.

Wymagany interfejs

Jedyną obowiązkową funkcją jest **zbx_module_api_version()**:

```
int zbx_module_api_version(void);
```

Ta funkcja powinna zwracać wersję API zaimplementowaną przez ten moduł, a aby moduł mógł zostać załadowany, wersja ta musi być zgodna z wersją API modułu obsługiwaną przez Zabbix. Wersja API modułu obsługiwana przez Zabbix to ZBX_MODULE_API_VERSION. Dlatego funkcja ta powinna zwracać tę stałą. Stara stała ZBX_MODULE_API_VERSION_ONE, używana wcześniej do tego celu, jest obecnie zdefiniowana jako równa ZBX_MODULE_API_VERSION w celu zachowania zgodności ze źródłami, jednak jej użycie nie jest zalecane.

Interfejs opcjonalny

Funkcjami opcjonalnymi są **zbx_module_init()**, **zbx_module_item_list()**, **zbx_module_item_timeout()**, **zbx_module_history_write_cbs** oraz **zbx_module_uninit()**:

```
int zbx_module_init(void);
```

Ta funkcja powinna wykonać niezbędną inicjalizację modułu (jeśli jest wymagana). W przypadku powodzenia powinna zwrócić ZBX_MODULE_OK. W przeciwnym razie powinna zwrócić ZBX_MODULE_FAIL. W tym ostatnim przypadku Zabbix nie uruchomi się.

```
ZBX_METRIC  *zbx_module_item_list(void);
```

Ta funkcja powinna zwrócić listę pozycji obsługiwanych przez moduł. Każda pozycja jest zdefiniowana w strukturze ZBX_METRIC; szczegóły znajdują się w sekcji poniżej. Lista jest zakończona strukturą ZBX_METRIC, w której pole ”key” ma wartość NULL.

```
void    zbx_module_item_timeout(int timeout);
```

Jeśli moduł eksportuje **zbx_module_item_list()**, to ta funkcja jest używana przez Zabbix do określenia ustawień timeout z pliku konfiguracyjnego Zabbix, których powinny przestrzegać kontrole pozycji zaimplementowane przez moduł. Tutaj parametr ”timeout” jest podawany w sekundach.

```
ZBX_HISTORY_WRITE_CBS   zbx_module_history_write_cbs(void);
```

Ta funkcja powinna zwrócić funkcje callback, których Zabbix server będzie używać do eksportowania historii różnych typów danych. Funkcje callback są udostępniane jako pola struktury ZBX_HISTORY_WRITE_CBS; pola mogą mieć wartość NULL, jeśli moduł nie jest zainteresowany historią określonego typu.

```
int zbx_module_uninit(void);
```

Ta funkcja powinna wykonać niezbędną deinicjalizację (jeśli jest wymagana), taką jak zwalnianie przydzielonych zasobów, zamykanie deskryptorów plików itp.

Wszystkie funkcje są wywoływane jednokrotnie podczas uruchamiania Zabbix, gdy moduł jest ładowany, z wyjątkiem zbx_module_uninit(), która jest wywoływana jednokrotnie podczas zamykania Zabbix, gdy moduł jest wyładowywany.

Definiowanie pozycji

Każda pozycja jest definiowana w strukturze ZBX_METRIC:

```
typedef struct
{
    char        *key;
    unsigned    flags;
    int     (*function)();
    char        *test_param;
}
ZBX_METRIC;
```

Tutaj **key** to klucz pozycji (np. ”dummy.random”), **flags** to albo CF_HAVEPARAMS, albo 0 (w zależności od tego, czy pozycja przyjmuje parametry), **function** to funkcja C implementująca pozycję (np. ”zbx_module_dummy_random”), a **test_param** to lista parametrów używana, gdy agent Zabbix jest uruchamiany z flagą ”-p” (np. ”1,1000”; może mieć wartość NULL). Przykładowa definicja może wyglądać następująco:

```
static ZBX_METRIC keys[] =
{
    { "dummy.random", CF_HAVEPARAMS, zbx_module_dummy_random, "1,1000" },
```

```
    { NULL }
}
```

Każda funkcja implementująca pozycję powinna przyjmować dwa parametry wskaźnikowe: pierwszy typu AGENT_REQUEST, a drugi typu AGENT_RESULT:

```
int zbx_module_dummy_random(AGENT_REQUEST *request, AGENT_RESULT *result)
{
    ...

    SET_UI64_RESULT(result, from + rand() % (to - from + 1));

    return SYSINFO_RET_OK;
}
```

Funkcje te powinny zwracać SYSINFO_RET_OK, jeśli wartość pozycji została pomyślnie pobrana. W przeciwnym razie powinny zwracać SYSINFO_RET_FAIL. Szczegółowe informacje o tym, jak pobierać informacje z AGENT_REQUEST i jak ustawiać informacje w AGENT_RESULT, można znaleźć w przykładzie modułu "dummy" poniżej.

Udostępnianie callbacków eksportu historii

Attention:
Eksport historii przez moduł nie jest już obsługiwany przez Zabbix proxy.

Moduł może określać funkcje do eksportu danych historii według typu: numeryczne (float), numeryczne (unsigned), znakowe, tekstowe i log:

```
typedef struct
{
    void    (*history_float_cb)(const ZBX_HISTORY_FLOAT *history, int history_num);
    void    (*history_integer_cb)(const ZBX_HISTORY_INTEGER *history, int history_num);
    void    (*history_string_cb)(const ZBX_HISTORY_STRING *history, int history_num);
    void    (*history_text_cb)(const ZBX_HISTORY_TEXT *history, int history_num);
    void    (*history_log_cb)(const ZBX_HISTORY_LOG *history, int history_num);
}
ZBX_HISTORY_WRITE_CBS;
```

Każda z nich powinna przyjmować jako argumenty tablicę "history" złożoną z "history_num" elementów. W zależności od typu eksportowanych danych historii, "history" jest odpowiednio tablicą następujących struktur:

```
typedef struct
{
    zbx_uint64_t    itemid;
    int     clock;
    int     ns;
    double      value;
}
ZBX_HISTORY_FLOAT;

typedef struct
{
    zbx_uint64_t    itemid;
    int     clock;
    int     ns;
    zbx_uint64_t    value;
}
ZBX_HISTORY_INTEGER;

typedef struct
{
    zbx_uint64_t    itemid;
    int     clock;
    int     ns;
    const char  *value;
}
```

```
ZBX_HISTORY_STRING;

typedef struct
{
    zbx_uint64_t    itemid;
    int     clock;
    int     ns;
    const char  *value;
}
ZBX_HISTORY_TEXT;

typedef struct
{
    zbx_uint64_t    itemid;
    int     clock;
    int     ns;
    const char  *value;
    const char  *source;
    int     timestamp;
    int     logeventid;
    int     severity;
}
ZBX_HISTORY_LOG;
```

Callbacki będą używane przez procesy synchronizacji historii Zabbix serwer na końcu procedury synchronizacji historii, po zapisaniu danych do bazy danych Zabbix i zachowaniu ich w pamięci podręcznej wartości.

Attention:
W przypadku błędu wewnętrznego w module eksportu historii zaleca się, aby moduł był napisany w taki sposób, by nie blokował całego monitoringu do czasu odzyskania sprawności, lecz zamiast tego odrzucał dane i pozwalał Zabbix serwer kontynuować działanie.

Budowanie modułów

Moduły są obecnie przeznaczone do budowania wewnątrz drzewa źródeł Zabbix, ponieważ API modułów zależy od niektórych struktur danych zdefiniowanych w nagłówkach Zabbix.

Najważniejszym nagłówkiem dla ładowalnych modułów jest **include/module.h**, który definiuje te struktury danych. Inne niezbędne nagłówki systemowe, które pomagają **include/module.h** działać poprawnie, to **stdlib.h** i **stdint.h**.

Mając te informacje na uwadze, wszystko jest gotowe do zbudowania modułu. Moduł powinien dołączać **stdlib.h**, **stdint.h** i **module.h**, a skrypt budowania powinien zapewnić, że pliki te znajdują się w ścieżce dołączania. Szczegóły można znaleźć w przykładzie modułu „dummy" poniżej.

Innym przydatnym nagłówkiem jest **include/zbxcommon.h**, który definiuje funkcję **zabbix_log()**, której można używać do celów rejestrowania i debugowania.

Parametry konfiguracji

Zabbix agent, serwer i proxy obsługują dwa parametry do pracy z modułami:

- LoadModulePath – pełna ścieżka do lokalizacji ładowalnych modułów
- LoadModule – moduł(y) do załadowania podczas uruchamiania. Moduły muszą znajdować się w katalogu określonym przez LoadModulePath lub ścieżka musi poprzedzać nazwę modułu. Jeśli poprzedzająca ścieżka jest bezwzględna (zaczyna się od '/'), wtedy LoadModulePath jest ignorowany. Dozwolone jest uwzględnienie wielu parametrów LoadModule.

Na przykład, aby rozszerzyć Zabbix agent, możemy dodać następujące parametry:

```
LoadModulePath=/usr/local/lib/zabbix/agent/
LoadModule=mariadb.so
LoadModule=apache.so
LoadModule=kernel.so
LoadModule=/usr/local/lib/zabbix/dummy.so
```

Podczas uruchamiania agent załaduje moduły mariadb.so, apache.so i kernel.so z katalogu /usr/local/lib/zabbix/agent, natomiast dummy.so zostanie załadowany z /usr/local/lib/zabbix. Agent nie uruchomi się, jeśli moduł będzie brakował, w przypadku nieprawidłowych uprawnień lub jeśli biblioteka współdzielona nie jest modułem Zabbix.

Konfiguracja frontendu

Ładowalne moduły są obsługiwane przez Zabbix agent, serwer i proxy. Dlatego typ pozycji w Zabbix frontend zależy od miejsca załadowania modułu. Jeśli moduł jest załadowany do agent, typ pozycji powinien być ustawiony na „Zabbix agent" lub „Zabbix agent (active)". Jeśli moduł jest załadowany do serwera lub proxy, typ pozycji powinien być ustawiony na „Simple check".

Eksport historii za pośrednictwem modułów Zabbix nie wymaga żadnej konfiguracji frontendu. Jeśli moduł zostanie pomyślnie załadowany przez serwer i udostępnia funkcję **zbx_module_history_write_cbs()**, która zwraca co najmniej jedną funkcję callback różną od NULL, eksport historii zostanie włączony automatycznie.

Moduł dummy

Zabbix zawiera przykładowy moduł napisany w języku C. Moduł znajduje się w katalogu src/modules/dummy:

```
alex@alex:~trunk/src/modules/dummy$ ls -l
-rw-rw-r-- 1 alex alex 9019 Apr 24 17:54 dummy.c
-rw-rw-r-- 1 alex alex   67 Apr 24 17:54 Makefile
-rw-rw-r-- 1 alex alex  245 Apr 24 17:54 README
```

Moduł jest dobrze udokumentowany i może być używany jako szablon dla własnych modułów.

Po uruchomieniu ./configure w katalogu głównym drzewa źródeł Zabbix, zgodnie z opisem powyżej, wystarczy uruchomić **make**, aby zbudować **dummy.so**.

```
/*
** Zabbix
** Copyright (C) 2001-2020 Zabbix SIA
**
** This program is free software; you can redistribute it and/or modify
** it under the terms of the GNU General Public License as published by
** the Free Software Foundation; either version 2 of the License, or
** (at your option) any later version.
**
** This program is distributed in the hope that it will be useful,
** but WITHOUT ANY WARRANTY; without even the implied warranty of
** MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
** GNU General Public License for more details.
**
** You should have received a copy of the GNU General Public License
** along with this program; if not, write to the Free Software
** Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA  02110-1301, USA.
**/

###include <stdlib.h>
###include <string.h>
###include <time.h>
###include <stdint.h>

###include "module.h"

/* the variable keeps timeout setting for item processing */
static int  item_timeout = 0;

/* module SHOULD define internal functions as static and use a naming pattern different from Zabbix intern
/* symbols (zbx_*) and loadable module API functions (zbx_module_*) to avoid conflicts
static int  dummy_ping(AGENT_REQUEST *request, AGENT_RESULT *result);
static int  dummy_echo(AGENT_REQUEST *request, AGENT_RESULT *result);
static int  dummy_random(AGENT_REQUEST *request, AGENT_RESULT *result);

static ZBX_METRIC keys[] =
/*  KEY         FLAG        FUNCTION    TEST PARAMETERS */
{
    {"dummy.ping",      0,      dummy_ping, NULL},
    {"dummy.echo",      CF_HAVEPARAMS,  dummy_echo, "a message"},
    {"dummy.random",    CF_HAVEPARAMS,  dummy_random,   "1,1000"},
    {NULL}
};
```

```c
/******************************************************************************
 *                                                                            *
 * Function: zbx_module_api_version                                           *
 *                                                                            *
 * Purpose: returns version number of the module interface                    *
 *                                                                            *
 * Return value: ZBX_MODULE_API_VERSION - version of module.h module is       *
 *               compiled with, in order to load module successfully Zabbix   *
 *               MUST be compiled with the same version of this header file   *
 *                                                                            *
 ******************************************************************************/
int zbx_module_api_version(void)
{
    return ZBX_MODULE_API_VERSION;
}

/******************************************************************************
 *                                                                            *
 * Function: zbx_module_item_timeout                                          *
 *                                                                            *
 * Purpose: set timeout value for processing of items                         *
 *                                                                            *
 * Parameters: timeout - timeout in seconds, 0 - no timeout set               *
 *                                                                            *
 ******************************************************************************/
void    zbx_module_item_timeout(int timeout)
{
    item_timeout = timeout;
}

/******************************************************************************
 *                                                                            *
 * Function: zbx_module_item_list                                             *
 *                                                                            *
 * Purpose: returns list of item keys supported by the module                 *
 *                                                                            *
 * Return value: list of item keys                                            *
 *                                                                            *
 ******************************************************************************/
ZBX_METRIC  *zbx_module_item_list(void)
{
    return keys;
}

static int  dummy_ping(AGENT_REQUEST *request, AGENT_RESULT *result)
{
    SET_UI64_RESULT(result, 1);

    return SYSINFO_RET_OK;
}

static int  dummy_echo(AGENT_REQUEST *request, AGENT_RESULT *result)
{
    char    *param;

    if (1 != request->nparam)
    {
        /* set optional error message */
        SET_MSG_RESULT(result, strdup("Invalid number of parameters."));
        return SYSINFO_RET_FAIL;
    }
```

```
    param = get_rparam(request, 0);

    SET_STR_RESULT(result, strdup(param));

    return SYSINFO_RET_OK;
}

/******************************************************************************
 *                                                                            *
 * Function: dummy_random                                                     *
 *                                                                            *
 * Purpose: a main entry point for processing of an item                      *
 *                                                                            *
 * Parameters: request - structure that contains item key and parameters      *
 *              request->key - item key without parameters                    *
 *              request->nparam - number of parameters                        *
 *              request->params[N-1] - pointers to item key parameters        *
 *              request->types[N-1] - item key parameters types:              *
 *                  REQUEST_PARAMETER_TYPE_UNDEFINED (key parameter is empty) *
 *                  REQUEST_PARAMETER_TYPE_ARRAY (array)                      *
 *                  REQUEST_PARAMETER_TYPE_STRING (quoted or unquoted string) *
 *                                                                            *
 *             result - structure that will contain result                    *
 *                                                                            *
 * Return value: SYSINFO_RET_FAIL - function failed, item will be marked      *
 *                                  as not supported by zabbix                *
 *               SYSINFO_RET_OK - success                                     *
 *                                                                            *
 * Comment: get_rparam(request, N-1) can be used to get a pointer to the Nth  *
 *          parameter starting from 0 (first parameter). Make sure it exists  *
 *          by checking value of request->nparam.                             *
 *          In the same manner get_rparam_type(request, N-1) can be used to   *
 *          get a parameter type.                                             *
 *                                                                            *
 ******************************************************************************/
static int  dummy_random(AGENT_REQUEST *request, AGENT_RESULT *result)
{
    char    *param1, *param2;
    int from, to;

    if (2 != request->nparam)
    {
        /* set optional error message */
        SET_MSG_RESULT(result, strdup("Invalid number of parameters."));
        return SYSINFO_RET_FAIL;
    }

    param1 = get_rparam(request, 0);
    param2 = get_rparam(request, 1);

    /* there is no strict validation of parameters and types for simplicity sake */
    from = atoi(param1);
    to = atoi(param2);

    if (from > to)
    {
        SET_MSG_RESULT(result, strdup("Invalid range specified."));
        return SYSINFO_RET_FAIL;
    }

    SET_UI64_RESULT(result, from + rand() % (to - from + 1));
```

```
    return SYSINFO_RET_OK;
}

/******************************************************************************
 *                                                                            *
 * Function: zbx_module_init                                                  *
 *                                                                            *
 * Purpose: the function is called on agent startup                           *
 *          It should be used to call any initialization routines             *
 *                                                                            *
 * Return value: ZBX_MODULE_OK - success                                      *
 *               ZBX_MODULE_FAIL - module initialization failed               *
 *                                                                            *
 * Comment: the module won't be loaded in case of ZBX_MODULE_FAIL             *
 *                                                                            *
 ******************************************************************************/
int zbx_module_init(void)
{
    /* initialization for dummy.random */
    srand(time(NULL));

    return ZBX_MODULE_OK;
}

/******************************************************************************
 *                                                                            *
 * Function: zbx_module_uninit                                                *
 *                                                                            *
 * Purpose: the function is called on agent shutdown                          *
 *          It should be used to cleanup used resources if there are any      *
 *                                                                            *
 * Return value: ZBX_MODULE_OK - success                                      *
 *               ZBX_MODULE_FAIL - function failed                            *
 *                                                                            *
 ******************************************************************************/
int zbx_module_uninit(void)
{
    return ZBX_MODULE_OK;
}

/******************************************************************************
 *                                                                            *
 * Functions: dummy_history_float_cb                                          *
 *            dummy_history_integer_cb                                        *
 *            dummy_history_string_cb                                         *
 *            dummy_history_text_cb                                           *
 *            dummy_history_log_cb                                            *
 *                                                                            *
 * Purpose: callback functions for storing historical data of types float,    *
 *          integer, string, text and log respectively in external storage    *
 *                                                                            *
 * Parameters: history     - array of historical data                         *
 *             history_num - number of elements in history array              *
 *                                                                            *
 ******************************************************************************/
static void dummy_history_float_cb(const ZBX_HISTORY_FLOAT *history, int history_num)
{
    int i;

    for (i = 0; i < history_num; i++)
    {
        /* do something with history[i].itemid, history[i].clock, history[i].ns, history[i].value, ... */
```

```
    }
}

static void dummy_history_integer_cb(const ZBX_HISTORY_INTEGER *history, int history_num)
{
    int i;

    for (i = 0; i < history_num; i++)
    {
        /* do something with history[i].itemid, history[i].clock, history[i].ns, history[i].value, ... */
    }
}

static void dummy_history_string_cb(const ZBX_HISTORY_STRING *history, int history_num)
{
    int i;

    for (i = 0; i < history_num; i++)
    {
        /* do something with history[i].itemid, history[i].clock, history[i].ns, history[i].value, ... */
    }
}

static void dummy_history_text_cb(const ZBX_HISTORY_TEXT *history, int history_num)
{
    int i;

    for (i = 0; i < history_num; i++)
    {
        /* do something with history[i].itemid, history[i].clock, history[i].ns, history[i].value, ... */
    }
}

static void dummy_history_log_cb(const ZBX_HISTORY_LOG *history, int history_num)
{
    int i;

    for (i = 0; i < history_num; i++)
    {
        /* do something with history[i].itemid, history[i].clock, history[i].ns, history[i].value, ... */
    }
}

/******************************************************************************
 *                                                                            *
 * Function: zbx_module_history_write_cbs                                     *
 *                                                                            *
 * Purpose: returns a set of module functions Zabbix will call to export      *
 *          different types of historical data                                *
 *                                                                            *
 * Return value: structure with callback function pointers (can be NULL if    *
 *               module is not interested in data of certain types)           *
 *                                                                            *
 ******************************************************************************/
ZBX_HISTORY_WRITE_CBS   zbx_module_history_write_cbs(void)
{
    static ZBX_HISTORY_WRITE_CBS    dummy_callbacks =
    {
        dummy_history_float_cb,
        dummy_history_integer_cb,
        dummy_history_string_cb,
        dummy_history_text_cb,
```

```
        dummy_history_log_cb,
    };

    return dummy_callbacks;
}
```

Moduł eksportuje trzy nowe pozycje:

- `dummy.ping` — zawsze zwraca „1”
- `dummy.echo[param1]` — zwraca pierwszy parametr bez zmian, na przykład `dummy.echo[ABC]` zwróci ABC
- `dummy.random[param1, param2]` — zwraca liczbę losową z zakresu param1-param2, na przykład `dummy.random[1,1000000]`

Ograniczenia

Obsługa modułów ładowalnych jest zaimplementowana wyłącznie dla platformy Unix. Oznacza to, że nie działa ona dla agentów Windows.

W niektórych przypadkach moduł może wymagać odczytu parametrów konfiguracyjnych związanych z modułem z pliku *zabbix_agentd.conf*. Obecnie nie jest to obsługiwane. Jeśli potrzebujesz, aby Twój moduł korzystał z parametrów konfiguracyjnych, prawdopodobnie powinieneś zaimplementować analizę pliku konfiguracyjnego specyficznego dla modułu.

3 Moduły frontend

Przegląd

Możliwe jest rozszerzenie funkcjonalności frontend Zabbix przez dodanie modułów firm trzecich lub tworzenie własnych modułów bez konieczności zmiany kodu źródłowego Zabbix.

Należy pamiętać, że kod modułu będzie uruchamiany z takimi samymi uprawnieniami jak kod źródłowy Zabbix. Oznacza to, że:

- moduły firm trzecich mogą być szkodliwe. Musisz ufać modułom, które instalujesz;
- błędy w kodzie modułu firmy trzeciej mogą spowodować awarię frontend. Jeśli tak się stanie, po prostu usuń kod modułu z frontend. Gdy tylko ponownie załadujesz frontend Zabbix, zobaczysz informację, że niektóre moduły są nieobecne. Przejdź do Administracja modułami (w *Administracja* → *Ogólne* → *Moduły*) i kliknij ponownie *Skanuj katalog*, aby usunąć nieistniejące moduły z bazy danych.

Instalacja

Zawsze należy przeczytać instrukcję instalacji dla konkretnego modułu. Zaleca się instalowanie nowych modułów pojedynczo, aby łatwo wychwycić błędy.

Tuż przed instalacją modułu:

- Upewnij się, że moduł został pobrany z zaufanego źródła. Instalacja szkodliwego kodu może prowadzić do konsekwencji, takich jak utrata danych
- Różne wersje tego samego modułu (to samo ID) mogą być zainstalowane równolegle, ale jednocześnie może być włączona tylko jedna wersja

Kroki instalacji modułu:

- Rozpakuj moduł we własnym folderze w katalogu `modules` Zabbix frontend
- Upewnij się, że folder modułu zawiera co najmniej plik manifest.json
- Przejdź do Administracja modułami i kliknij przycisk *Scan directory*
- Nowy moduł pojawi się na liście wraz ze swoją wersją, autorem, opisem i statusem
- Włącz moduł, klikając jego status

Rozwiązywanie problemów:

Problem	Rozwiązanie
Moduł nie pojawił się na liście	Jeśli moduł nie pojawił się na liście, upewnij się, że plik manifest.json istnieje w modules/your-module/. Jeśli nie, moduł mógł zostać rozpakowany do niewłaściwego katalogu. Jeśli plik istnieje, moduł może nie być zgodny z używaną wersją Zabbix. Sprawdź również, czy użytkownik serwera WWW ma co najmniej uprawnienia odczytu i przeszukiwania (`r-x`) do folderu modułu oraz wszystkich podkatalogów, a także uprawnienia odczytu (`r--`) do wszystkich znajdujących się w nim plików.

Problem	Rozwiązanie
Frontend uległ awarii	Kod modułu nie jest zgodny z bieżącą wersją Zabbix lub konfiguracją serwera. Usuń pliki modułu i ponownie załaduj frontend. Zobaczysz powiadomienie, że niektóre moduły są nieobecne. Przejdź do Administracja modułami i ponownie kliknij *Scan directory*, aby usunąć z bazy danych nieistniejące moduły.
Pojawia się komunikat o błędzie dotyczący identycznej przestrzeni nazw, ID lub akcji	Nowy moduł próbował zarejestrować przestrzeń nazw, ID lub akcje, które są już zarejestrowane przez inne włączone moduły. Wyłącz moduł powodujący konflikt (wspomniany w komunikacie o błędzie) przed włączeniem nowego modułu.
Pojawiają się techniczne komunikaty o błędach	Zgłoś błędy deweloperowi modułu.

Tworzenie modułów

Aby uzyskać informacje o tworzeniu niestandardowych modułów, zobacz Developer center.

20 Aneksy

Aby uzyskać dostęp do treści w sekcji Aneksy, skorzystaj z panelu bocznego.

1 Instalacja i konfiguracja

Skorzystaj z paska bocznego, aby uzyskać dostęp do treści w tej sekcji.

1 Tworzenie bazy danych

Przegląd

Baza danych Zabbix musi zostać utworzona podczas instalacji serwera lub proxy Zabbix.

Ta sekcja zawiera instrukcje dotyczące tworzenia bazy danych Zabbix. Dla każdej obsługiwanej bazy danych dostępny jest osobny zestaw instrukcji.

Note:
Aby zwiększyć bezpieczeństwo bazy danych przez utworzenie ról/użytkowników bazy danych z minimalnymi uprawnieniami, zobacz najlepsze praktyki tworzenia bazy danych dla każdej obsługiwanej bazy danych:

- MySQL/MariaDB
- PostgreSQL/TimescaleDB

Aby skonfigurować bezpieczne połączenia TLS, zobacz Bezpieczne połączenie z bazą danych.

UTF-8 jest jedynym kodowaniem obsługiwanym przez Zabbix. Wiadomo, że działa bez żadnych luk bezpieczeństwa. Użytkownicy powinni mieć świadomość, że w przypadku używania niektórych innych kodowań istnieją znane problemy bezpieczeństwa. Informacje o przełączeniu na UTF-8 można znaleźć w sekcji Naprawa zestawu znaków i porównywania bazy danych Zabbix. Zobacz także Ograniczenia filtrowania przy użyciu porównań utf8mb4.

Note:
Jeśli instalujesz z repozytorium Git Zabbix, przed przejściem do kolejnych kroków musisz uruchomić następujące polecenie:

 `make dbschema`

MySQL/MariaDB

Zestawy znaków utf8 (znane także jako utf8mb3) oraz utf8mb4 są obsługiwane (odpowiednio z porównywaniem utf8_bin i utf8mb4_bin), aby serwer/proxy Zabbix działał poprawnie z bazą danych MySQL. W przypadku nowych instalacji zaleca się użycie utf8mb4.

Deterministyczne wyzwalacze muszą zostać utworzone podczas importu schematu. W MySQL i MariaDB wymaga to ustawienia `GLOBAL log_bin_trust_function_creators = 1`, jeśli logowanie binarne jest włączone, nie ma uprawnień superusera, a `log_bin_trust_function_creators = 1` nie jest ustawione w pliku konfiguracyjnym MySQL.

Jeśli instalujesz zabbix z **pakietów**, przejdź do instrukcji dla swojej platformy.

Jeśli instalujesz Zabbix ze źródeł:

- Utwórz i skonfiguruj bazę danych oraz użytkownika.

```
mysql -uroot -p<password>

mysql> create database zabbix character set utf8mb4 collate utf8mb4_bin;
mysql> create user 'zabbix'@'localhost' identified by '<password>';
mysql> grant all privileges on zabbix.* to 'zabbix'@'localhost';
mysql> SET GLOBAL log_bin_trust_function_creators = 1;
mysql> quit;
```

- Zaimportuj dane do bazy danych i ustaw zestaw znaków utf8mb4 jako domyślny (zakładając, że znajdujesz się w katalogu głównym źródeł Zabbix). W przypadku bazy danych proxy Zabbix należy zaimportować tylko `schema.sql` (bez images.sql ani data.sql).

```
cd database/mysql
mysql -uzabbix -p<password> zabbix < schema.sql
#### zatrzymaj się tutaj, jeśli tworzysz bazę danych dla proxy Zabbix
mysql -uzabbix -p<password> zabbix < images.sql
mysql -uzabbix -p<password> --default-character-set=utf8mb4 zabbix < data.sql
```

Po pomyślnym zaimportowaniu schematu `log_bin_trust_function_creators` można wyłączyć:

```
mysql -uroot -p<password>

mysql> SET GLOBAL log_bin_trust_function_creators = 0;
mysql> quit;
```

PostgreSQL

Musisz mieć użytkownika bazy danych z uprawnieniami do tworzenia obiektów bazy danych.

Jeśli instalujesz zabbix z **pakietów**, przejdź do instrukcji dla swojej platformy.

Jeśli instalujesz Zabbix ze źródeł:

- Utwórz użytkownika bazy danych.

Poniższe polecenie powłoki utworzy użytkownika `zabbix`. Po wyświetleniu monitu podaj hasło i powtórz je (uwaga: najpierw możesz zostać poproszony o hasło sudo):

```
sudo -u postgres createuser --pwprompt zabbix
```

- Utwórz bazę danych.

Poniższe polecenie powłoki utworzy bazę danych `zabbix` (ostatni parametr), a wcześniej utworzony użytkownik będzie jej właścicielem (`-O zabbix`).

```
sudo -u postgres createdb -O zabbix -E Unicode -T template0 zabbix
```

- Zaimportuj początkowy schemat i dane (zakładając, że jesteś w katalogu głównym źródeł Zabbix). Dla bazy danych proxy Zabbix należy zaimportować tylko `schema.sql` (bez images.sql ani data.sql).

```
cd database/postgresql
cat schema.sql | sudo -u zabbix psql zabbix
#### zatrzymaj się tutaj, jeśli tworzysz bazę danych dla proxy Zabbix
cat images.sql | sudo -u zabbix psql zabbix
cat data.sql | sudo -u zabbix psql zabbix
```

Attention:
Powyższe polecenia podano jako przykład, który będzie działał w większości instalacji GNU/Linux. Możesz użyć innych poleceń w zależności od konfiguracji systemu/bazy danych, na przykład:

 `psql -U <username>`

 Jeśli masz jakiekolwiek problemy z konfiguracją bazy danych, skonsultuj się z administratorem bazy danych.

TimescaleDB

Instrukcje dotyczące tworzenia i konfiguracji TimescaleDB znajdują się w osobnej sekcji.

SQLite

Używanie SQLite jest obsługiwane tylko dla **Zabbix proxy**!

Baza danych zostanie utworzona automatycznie, jeśli nie istnieje.

Wróć do sekcji instalacji.

2 Naprawa zestawu znaków i porównywania napisów bazy danych Zabbix

MySQL/MariaDB

Historycznie MySQL i jego pochodne używały „utf8” jako aliasu dla utf8mb3 — własnej 3-bajtowej implementacji standardu UTF8 w MySQL, który jest 4-bajtowy. Począwszy od MySQL 8.0.28 i MariaDB 10.6.1, zestaw znaków „utf8mb3” jest przestarzały i w pewnym momencie jego obsługa zostanie usunięta, podczas gdy „utf8” stanie się odniesieniem do „utf8mb4”. Od Zabbix 6.0 obsługiwany jest „utf8mb4”. Aby uniknąć problemów w przyszłości, zdecydowanie zaleca się używanie „utf8mb4”. Kolejną zaletą przejścia na „utf8mb4” jest obsługa dodatkowych znaków Unicode.

> **Warning:**
> Ponieważ wersje wcześniejsze niż Zabbix 6.0 nie obsługują utf8mb4, przed wykonaniem konwersji do utf8mb4 należy najpierw zaktualizować serwer Zabbix i schemat bazy danych do wersji 6.0.x lub nowszej.

1. Sprawdź zestaw znaków i porównywanie bazy danych.

Na przykład:

```
mysql> SELECT @@character_set_database, @@collation_database;
+--------------------------+----------------------+
| @@character_set_database | @@collation_database |
+--------------------------+----------------------+
| latin2                   | latin2 _general_ci   |
+--------------------------+----------------------+
```

Lub:

```
mysql> SELECT @@character_set_database, @@collation_database;
+--------------------------+----------------------+
| @@character_set_database | @@collation_database |
+--------------------------+----------------------+
| utf8                     | utf8_bin             |
+--------------------------+----------------------+
```

Jak widać, zestaw znaków nie jest tutaj ustawiony na „utf8mb4”, a porównywanie nie jest ustawione na „utf8mb4_bin”, więc należy to poprawić.

2. Zatrzymaj Zabbix.

3. Utwórz kopię zapasową bazy danych!

4. Popraw zestaw znaków i porównywanie na poziomie bazy danych:

```
alter database <your DB name> character set utf8mb4 collate utf8mb4_bin;
```

Poprawione wartości:

```
mysql> SELECT @@character_set_database, @@collation_database;
+--------------------------+----------------------+
| @@character_set_database | @@collation_database |
+--------------------------+----------------------+
| utf8mb4                  | utf8mb4_bin          |
+--------------------------+----------------------+
```

5. Załaduj skrypt w celu poprawienia zestawu znaków i porównywania na poziomie tabel i kolumn:

```
mysql <your DB name> < utf8mb4_convert.sql
```

6. Wykonaj skrypt:

```
                SET @ZABBIX_DATABASE = '<your DB name>';
If MariaDB →    set innodb_strict_mode = OFF;
                CALL zbx_convert_utf8();
If MariaDB →    set innodb_strict_mode = ON;
                drop procedure zbx_convert_utf8;
```

Należy pamiętać, że „utf8mb4” może zużywać nieco więcej miejsca na dysku.

7. Jeśli nie wystąpiły błędy, możesz utworzyć kopię zapasową poprawionej bazy danych.

8. Uruchom Zabbix.

3 Database upgrade to primary keys

Przegląd

Ta sekcja zawiera instrukcje dotyczące ręcznej aktualizacji tabel w istniejących instalacjach do kluczy głównych.

Aktualizacja do kluczy głównych optymalizuje sposób indeksowania danych i uzyskiwania do nich dostępu, co może przyspieszyć zapytania i zaoszczędzić miejsce. Poprawia także zarządzanie danymi i synchronizację w środowiskach klastrowych, pomagając w skalowaniu i zapewniając niezawodność systemu nawet w przypadku awarii niektórych serwerów.

Attention:
Instrukcje podane na tej stronie są przeznaczone dla zaawansowanych użytkowników i mogą wymagać dostosowania do konkretnej konfiguracji. Aktualizacja do kluczy głównych może być czasochłonna i zasobochłonna. Upewnij się, że dostępna jest wystarczająca ilość wolnego miejsca na dysku; w zależności od rozmiaru bazy danych i przechowywanych danych proces może wymagać nawet 2,5 razy więcej miejsca niż obecnie zajmują tabele historii.

Klucze główne są używane we wszystkich tabelach w nowych instalacjach od Zabbix 6.0.

Nie ma automatycznej aktualizacji bazy danych do kluczy głównych; jednak istniejące instalacje można zaktualizować ręcznie **po** aktualizacji serwera Zabbix do wersji 6.0 lub nowszej.

Attention:
Od Zabbix 7.0 aktualizacja tabel do kluczy głównych obejmuje również aktualizację tabel do używania typów danych double precision.

 Jeśli używasz Zabbix 7.0 (lub nowszego), tabele już korzystają z typu double precision. Jednak instrukcje na tej stronie nadal można zastosować, aby zaktualizować tabele do kluczy głównych bez wpływu na tabele, które już używają typu double precision.

 Jeśli używasz Zabbix 6.4 (lub wcześniejszego), rozważ najpierw aktualizację tabel do typu double precision. Więcej informacji można znaleźć w sekcji Upgrading to numeric values of extended range w dokumentacji Zabbix 7.0.

Dostępne są instrukcje dla:

- MySQL
- PostgreSQL
- TimescaleDB

Ważne uwagi

Aby przeprowadzić aktualizację bazy danych:

1. Zatrzymaj serwer Zabbix.

Zdecydowanie zaleca się zatrzymanie serwera Zabbix na czas aktualizacji. Jeśli jednak jest to absolutnie konieczne, możesz przeprowadzić aktualizację, gdy serwer działa (dotyczy tylko MySQL, MariaDB oraz PostgreSQL bez TimescaleDB).

2. Wykonaj kopię zapasową bazy danych.
3. Zainstaluj najnowszy pakiet zabbix-sql-scripts zgodny z używaną wersją Zabbix (np. dla RHEL: `dnf install zabbix-sql-scripts`).
4. Uruchom skrypty dla swojej bazy danych.
5. Uruchom serwer Zabbix.

Warning:
Uruchom skrypty tylko dla bazy danych serwera. proxy nie odniesie korzyści z tej aktualizacji.

Jeśli baza danych używa partycji, skontaktuj się z administratorem DB lub pomocą techniczną Zabbix.

Pliki CSV można usunąć po pomyślnej aktualizacji do kluczy głównych.

Opcjonalnie frontend Zabbix można przełączyć w tryb konserwacji.

MySQL

Eksport i import muszą być wykonywane w tmux/screen, aby zapewnić, że sesja nie zostanie przerwana.

Zobacz także: Ważne uwagi

MySQL 8.4+ z mysqlsh

Ta metoda może być używana z działającym serwerem Zabbix, jednak zaleca się zatrzymanie serwera na czas aktualizacji. MySQL Shell (*mysqlsh*) musi być zainstalowany i mieć możliwość połączenia z bazą danych.

- Zaloguj się do konsoli MySQL jako root (zalecane) lub jako dowolny użytkownik z uprawnieniami FILE.
- Uruchom MySQL z włączoną zmienną local_infile.
- Zmień nazwy starych tabel i utwórz nowe tabele, uruchamiając `history_upgrade_prepare.sql`.

```
mysql -uzabbix -p<password> zabbix < /usr/share/zabbix/sql-scripts/mysql/option-patches/history_upgrade_pr
```

- Wyeksportuj i zaimportuj dane.

Połącz się przez mysqlsh. W przypadku używania połączenia przez socket może być wymagane podanie ścieżki.

```
sudo mysqlsh -uroot -S /run/mysqld/mysqld.sock --no-password -Dzabbix
```

Przełącz się do trybu JavaScript, używając:

```
\js
```

Następnie uruchom poniższy kod (CSVPATH można zmienić w razie potrzeby):

```
CSVPATH="/var/lib/mysql-files";

util.exportTable("history_old", CSVPATH + "/history.csv", { dialect: "csv" });
util.importTable(CSVPATH + "/history.csv", {"dialect": "csv", "table": "history" });

util.exportTable("history_uint_old", CSVPATH + "/history_uint.csv", { dialect: "csv" });
util.importTable(CSVPATH + "/history_uint.csv", {"dialect": "csv", "table": "history_uint" });

util.exportTable("history_str_old", CSVPATH + "/history_str.csv", { dialect: "csv" });
util.importTable(CSVPATH + "/history_str.csv", {"dialect": "csv", "table": "history_str" });

util.exportTable("history_log_old", CSVPATH + "/history_log.csv", { dialect: "csv" });
util.importTable(CSVPATH + "/history_log.csv", {"dialect": "csv", "table": "history_log" });

util.exportTable("history_text_old", CSVPATH + "/history_text.csv", { dialect: "csv" });
util.importTable(CSVPATH + "/history_text.csv", {"dialect": "csv", "table": "history_text" });
```

Jeśli otrzymasz komunikat „JavaScript is not supported”, oznacza to, że Twoja instalacja MySQL Shell nie ma obsługi JS. W takim przypadku zainstaluj oficjalny pakiet MySQL Shell od Oracle (lub zbuduj go ze źródeł), aby tryb JavaScript był dostępny.

- Postępuj zgodnie z instrukcjami po migracji, aby usunąć stare tabele.

MariaDB/MySQL 8.4+ bez mysqlsh

Ta metoda aktualizacji zajmuje więcej czasu i powinna być używana tylko wtedy, gdy aktualizacja z użyciem *mysqlsh* nie jest możliwa.

Aktualizacja tabel

- Zaloguj się do konsoli MySQL jako root (zalecane) lub dowolny użytkownik z uprawnieniami FILE.
- Jeśli przeprowadzasz migrację przy działającym serwer Zabbix, uruchom MySQL z włączoną zmienną local_infile.
- Zmień nazwy starych tabel i utwórz nowe tabele, uruchamiając `history_upgrade_prepare.sql`:

```
mysql -uzabbix -p<password> zabbix < /usr/share/zabbix/sql-scripts/mysql/option-patches/history_upgrade_pr
```

Migracja przy zatrzymanym serwerze

Przed migracją danych należy wyłączyć `max_execution_time` (w MySQL) lub `max_statement_time` (w MariaDB), aby uniknąć przekroczenia limitu czasu podczas migracji.

Dla MySQL:

```
SET @@max_execution_time=0;
```

Dla MariaDB:

```
SET @@max_statement_time=0;
```

```
INSERT IGNORE INTO history SELECT * FROM history_old;
INSERT IGNORE INTO history_uint SELECT * FROM history_uint_old;
INSERT IGNORE INTO history_str SELECT * FROM history_str_old;
INSERT IGNORE INTO history_log SELECT * FROM history_log_old;
INSERT IGNORE INTO history_text SELECT * FROM history_text_old;
```

Aby usunąć stare tabele, postępuj zgodnie z instrukcjami po migracji.

Migracja przy działającym serwerze

Sprawdź, dla których ścieżek włączono import/eksport:

```
mysql> SELECT @@secure_file_priv;
+-----------------------+
| @@secure_file_priv    |
+-----------------------+
| /var/lib/mysql-files/ |
+-----------------------+
```

Jeśli wartość *secure_file_priv* jest ścieżką do katalogu, eksport/import będzie wykonywany dla plików w tym katalogu. W takim przypadku odpowiednio zmień ścieżki do plików w zapytaniach lub ustaw wartość *secure_file_priv* na pusty ciąg na czas aktualizacji.

Jeśli wartość *secure_file_priv* jest pusta, eksport/import może być wykonywany z dowolnej lokalizacji.

Jeśli wartość *secure_file_priv* ma wartość NULL, ustaw ją na ścieżkę zawierającą wyeksportowane dane tabeli (`'/var/lib/mysql-files/'` w powyższym przykładzie).

Więcej informacji można znaleźć w dokumentacji MySQL lub dokumentacji MariaDB.

Przed eksportem danych należy wyłączyć `max_execution_time` (w MySQL) lub `max_statement_time` (w MariaDB), aby uniknąć przekroczenia limitu czasu podczas eksportu.

Dla MySQL:

```
SET @@max_execution_time=0;
```

Dla MariaDB:

```
SET @@max_statement_time=0;
```

```
SELECT * INTO OUTFILE '/var/lib/mysql-files/history.csv' FIELDS TERMINATED BY ',' ESCAPED BY '"' LINES TER
LOAD DATA INFILE '/var/lib/mysql-files/history.csv' IGNORE INTO TABLE history FIELDS TERMINATED BY ',' ESC

SELECT * INTO OUTFILE '/var/lib/mysql-files/history_uint.csv' FIELDS TERMINATED BY ',' ESCAPED BY '"' LINE
LOAD DATA INFILE '/var/lib/mysql-files/history_uint.csv' IGNORE INTO TABLE history_uint FIELDS TERMINATED

SELECT * INTO OUTFILE '/var/lib/mysql-files/history_str.csv' FIELDS TERMINATED BY ',' ESCAPED BY '"' LINES
LOAD DATA INFILE '/var/lib/mysql-files/history_str.csv' IGNORE INTO TABLE history_str FIELDS TERMINATED BY

SELECT * INTO OUTFILE '/var/lib/mysql-files/history_log.csv' FIELDS TERMINATED BY ',' ESCAPED BY '"' LINES
LOAD DATA INFILE '/var/lib/mysql-files/history_log.csv' IGNORE INTO TABLE history_log FIELDS TERMINATED BY

SELECT * INTO OUTFILE '/var/lib/mysql-files/history_text.csv' FIELDS TERMINATED BY ',' ESCAPED BY '"' LINE
LOAD DATA INFILE '/var/lib/mysql-files/history_text.csv' IGNORE INTO TABLE history_text FIELDS TERMINATED
```

Aby usunąć stare tabele, postępuj zgodnie z instrukcjami po migracji.

PostgreSQL

Eksport i import należy wykonać w tmux/screen, aby mieć pewność, że sesja nie zostanie przerwana. W przypadku instalacji z TimescaleDB pomiń tę sekcję i przejdź do PostgreSQL + TimescaleDB.

Zobacz także: Ważne uwagi

Aktualizacja tabel

- Zmień nazwy tabel za pomocą `history_upgrade_prepare.sql`:

```
sudo -u zabbix psql zabbix < /usr/share/zabbix/sql-scripts/postgresql/option-patches/history_upgrade_prepa
```

Migracja przy zatrzymanym serwerze

- Wyeksportuj bieżące dane historyczne, zaimportuj je do tabeli tymczasowej, a następnie wstaw dane do nowych tabel, ignorując duplikaty:

```
INSERT INTO history SELECT * FROM history_old ON CONFLICT (itemid,clock,ns) DO NOTHING;

INSERT INTO history_uint SELECT * FROM history_uint_old ON CONFLICT (itemid,clock,ns) DO NOTHING;

INSERT INTO history_str SELECT * FROM history_str_old ON CONFLICT (itemid,clock,ns) DO NOTHING;

INSERT INTO history_log SELECT * FROM history_log_old ON CONFLICT (itemid,clock,ns) DO NOTHING;

INSERT INTO history_text SELECT * FROM history_text_old ON CONFLICT (itemid,clock,ns) DO NOTHING;
```

Zobacz wskazówki dotyczące poprawy wydajności operacji INSERT: PostgreSQL: Bulk Loading Huge Amounts of Data, Checkpoint Distance and Amount of WAL.

- Postępuj zgodnie z instrukcjami po migracji, aby usunąć stare tabele.

Migracja przy działającym serwerze

- Wyeksportuj bieżącą historię, zaimportuj ją do tabeli tymczasowej, a następnie wstaw dane do nowych tabel, ignorując duplikaty:

```
\copy history_old TO '/tmp/history.csv' DELIMITER ',' CSV
CREATE TEMP TABLE temp_history (
    itemid                  bigint                                  NOT NULL,
    clock                   integer         DEFAULT '0'             NOT NULL,
    value                   DOUBLE PRECISION DEFAULT '0.0000'        NOT NULL,
    ns                      integer         DEFAULT '0'             NOT NULL
);
\copy temp_history FROM '/tmp/history.csv' DELIMITER ',' CSV
INSERT INTO history SELECT * FROM temp_history ON CONFLICT (itemid,clock,ns) DO NOTHING;

\copy history_uint_old TO '/tmp/history_uint.csv' DELIMITER ',' CSV
CREATE TEMP TABLE temp_history_uint (
    itemid                  bigint                                  NOT NULL,
    clock                   integer         DEFAULT '0'             NOT NULL,
    value                   numeric(20)     DEFAULT '0'             NOT NULL,
    ns                      integer         DEFAULT '0'             NOT NULL
);
\copy temp_history_uint FROM '/tmp/history_uint.csv' DELIMITER ',' CSV
INSERT INTO history_uint SELECT * FROM temp_history_uint ON CONFLICT (itemid,clock,ns) DO NOTHING;

\copy history_str_old TO '/tmp/history_str.csv' DELIMITER ',' CSV
CREATE TEMP TABLE temp_history_str (
    itemid                  bigint                                  NOT NULL,
    clock                   integer         DEFAULT '0'             NOT NULL,
    value                   varchar(255)    DEFAULT ''              NOT NULL,
    ns                      integer         DEFAULT '0'             NOT NULL
);
\copy temp_history_str FROM '/tmp/history_str.csv' DELIMITER ',' CSV
INSERT INTO history_str (itemid,clock,value,ns) SELECT * FROM temp_history_str ON CONFLICT (itemid,clock,n

\copy history_log_old TO '/tmp/history_log.csv' DELIMITER ',' CSV
CREATE TEMP TABLE temp_history_log (
    itemid                  bigint                                  NOT NULL,
    clock                   integer         DEFAULT '0'             NOT NULL,
    timestamp               integer         DEFAULT '0'             NOT NULL,
    source                  varchar(64)     DEFAULT ''              NOT NULL,
    severity                integer         DEFAULT '0'             NOT NULL,
    value                   text            DEFAULT ''              NOT NULL,
    logeventid              integer         DEFAULT '0'             NOT NULL,
    ns                      integer         DEFAULT '0'             NOT NULL
);
\copy temp_history_log FROM '/tmp/history_log.csv' DELIMITER ',' CSV
INSERT INTO history_log SELECT * FROM temp_history_log ON CONFLICT (itemid,clock,ns) DO NOTHING;
```

```
\copy history_text_old TO '/tmp/history_text.csv' DELIMITER ',' CSV
CREATE TEMP TABLE temp_history_text (
    itemid                  bigint                                  NOT NULL,
    clock                   integer         DEFAULT '0'             NOT NULL,
    value                   text            DEFAULT ''              NOT NULL,
    ns                      integer         DEFAULT '0'             NOT NULL
);
\copy temp_history_text FROM '/tmp/history_text.csv' DELIMITER ',' CSV
INSERT INTO history_text SELECT * FROM temp_history_text ON CONFLICT (itemid,clock,ns) DO NOTHING;
```

- Aby usunąć stare tabele, postępuj zgodnie z instrukcjami po migracji.

PostgreSQL + TimescaleDB

Eksport i import muszą być wykonywane w tmux/screen, aby zapewnić, że sesja nie zostanie przerwana. serwer Zabbix powinien być wyłączony podczas aktualizacji.

Zobacz także: Ważne uwagi

- Zmień nazwy tabel za pomocą `history_upgrade_prepare.sql`.
  - Jeśli kompresja jest włączona (w domyślnej instalacji), uruchom skrypt z `/usr/share/zabbix/sql-scripts/postgresql/tim`

    ```
    cat /usr/share/zabbix/sql-scripts/postgresql/timescaledb/option-patches/with-compression/history_
    ```

  - Jeśli kompresja jest wyłączona, uruchom skrypt z `/usr/share/zabbix/sql-scripts/postgresql/timescaledb/option-p`

    ```
    cat /usr/share/zabbix/sql-scripts/postgresql/timescaledb/option-patches/without-compression/histo
    ```

- Uruchom skrypty migracji hypertable TimescaleDB zgodnie z ustawieniami kompresji:
  - Jeśli kompresja jest włączona (w domyślnej instalacji), uruchom skrypty z `/usr/share/zabbix/sql-scripts/postgresql/ti`

    ```
    cat /usr/share/zabbix/sql-scripts/postgresql/timescaledb/option-patches/with-compression/history_
    cat /usr/share/zabbix/sql-scripts/postgresql/timescaledb/option-patches/with-compression/history_
    cat /usr/share/zabbix/sql-scripts/postgresql/timescaledb/option-patches/with-compression/history_
    cat /usr/share/zabbix/sql-scripts/postgresql/timescaledb/option-patches/with-compression/history_
    cat /usr/share/zabbix/sql-scripts/postgresql/timescaledb/option-patches/with-compression/history_
    cat /usr/share/zabbix/sql-scripts/postgresql/timescaledb/option-patches/with-compression/trends_u
    ```

  - Jeśli kompresja jest wyłączona, uruchom skrypty z `/usr/share/zabbix/sql-scripts/postgresql/timescaledb/option-`

    ```
    cat /usr/share/zabbix/sql-scripts/postgresql/timescaledb/option-patches/without-compression/histo
    cat /usr/share/zabbix/sql-scripts/postgresql/timescaledb/option-patches/without-compression/histo
    cat /usr/share/zabbix/sql-scripts/postgresql/timescaledb/option-patches/without-compression/histo
    cat /usr/share/zabbix/sql-scripts/postgresql/timescaledb/option-patches/without-compression/histo
    cat /usr/share/zabbix/sql-scripts/postgresql/timescaledb/option-patches/without-compression/histo
    cat /usr/share/zabbix/sql-scripts/postgresql/timescaledb/option-patches/without-compression/trend
    ```

Zobacz także: Wskazówki dotyczące poprawy wydajności INSERT.

- Postępuj zgodnie z instrukcjami po migracji, aby usunąć stare tabele.

Po migracji

Dla wszystkich baz danych, po zakończeniu migracji wykonaj następujące czynności:

- Zweryfikuj, że wszystko działa zgodnie z oczekiwaniami.
- Usuń stare tabele:

```
DROP TABLE history_old;
DROP TABLE history_uint_old;
DROP TABLE history_str_old;
DROP TABLE history_log_old;
DROP TABLE history_text_old;
```

- W przypadku TimescaleDB usuń również następującą starą tabelę:

```
DROP TABLE trends_old;
```

Zobacz także

- Przygotowanie tabeli auditlog do partycjonowania

4 Przygotowanie tabeli auditlog do partycjonowania

Przegląd

Niektóre bazy danych (na przykład MySQL) wymagają, aby kolumna partycjonowania była częścią unikalnego ograniczenia tabeli. Dlatego, aby partycjonować tabelę `auditlog` według czasu, klucz główny musi zostać zmieniony z `auditid` na klucz złożony `auditid` + `clock`.

Ta sekcja zawiera instrukcje dotyczące zmiany klucza głównego tabeli `auditlog`.

Attention:
Instrukcje podane na tej stronie są przeznaczone dla zaawansowanych użytkowników. Należy pamiętać, że instrukcje te mogą wymagać dostosowania do konkretnej konfiguracji. Zmiana klucza głównego może być również niezgodna z przyszłymi poprawkami aktualizacyjnymi, dlatego może być konieczna ręczna obsługa przyszłych aktualizacji.

 Zmiana klucza głównego może być operacją wymagającą dużych zasobów i zająć dużo czasu, w zależności od rozmiaru tabeli `auditlog`. Zaleca się zatrzymanie serwera Zabbix i przełączenie frontend Zabbix w tryb konserwacji na czas wprowadzania zmiany. Jeśli jednak jest to absolutnie konieczne, istnieje sposób na zmianę klucza głównego bez przestoju (patrz poniżej).

Partycjonowanie tabeli `auditlog` może poprawić na przykład housekeeping w dużych środowiskach. Chociaż housekeeping Zabbix obecnie nie może korzystać z tabel partycjonowanych (z wyjątkiem TimescaleDB), można wyłączyć housekeeping Zabbix i usuwać partycje za pomocą skryptów.

Od Zabbix 7.0 tabela `auditlog` dla TimescaleDB została przekształcona w hypertable, co pozwala housekeeperowi usuwać dane całymi chunkami. Aby zaktualizować istniejącą tabelę `auditlog` do hypertable, zobacz Upgrading TimescaleDB schema.

MySQL

Ważne uwagi dotyczące przebudowy indeksów

MySQL automatycznie przebudowuje indeksy dla klucza głównego podczas operacji `ALTER TABLE`. Jednak zdecydowanie zaleca się również ręczną przebudowę indeksów za pomocą instrukcji `OPTIMIZE TABLE`, aby zapewnić optymalną wydajność bazy danych.

Przebudowa indeksów może tymczasowo wymagać nawet tyle dodatkowego miejsca na dysku, ile zajmuje sama tabela. Aby uzyskać bieżący rozmiar danych i indeksów, można wykonać następujące instrukcje:

```
ANALYZE TABLE auditlog;
SHOW TABLE STATUS LIKE 'auditlog';
```

Jeśli dostępne miejsce na dysku jest problemem, postępuj zgodnie z instrukcjami Zmiana klucza głównego bez przestoju. Dostępne są również inne opcje:

- Zwiększenie parametru MySQL `sort_buffer_size` może pomóc zmniejszyć zużycie miejsca na dysku podczas ręcznej przebudowy indeksów. Należy jednak pamiętać, że modyfikacja tej zmiennej może wpłynąć na ogólne zużycie pamięci przez bazę danych.
- Rozważ zwolnienie miejsca przez usunięcie potencjalnie niepotrzebnych danych.
- Rozważ zmniejszenie parametru *Okres przechowywania danych* housekeeper przed uruchomieniem housekeepera.

Zmiana klucza głównego z przestojem

1. Usuń bieżący klucz główny tabeli `auditlog` i dodaj nowy klucz główny.

```
ALTER TABLE auditlog DROP PRIMARY KEY, ADD PRIMARY KEY (auditid, clock);
```

2. Przebuduj indeksy (opcjonalne, ale zdecydowanie zalecane, zobacz Ważne uwagi dotyczące przebudowy indeksów).

```
OPTIMIZE TABLE auditlog;
```

Zmiana klucza głównego bez przestoju

Ręczna metoda zmiany klucza głównego została opisana tutaj. Alternatywnie można użyć zestawu narzędzi pt-online-schema-change firmy Percona. Ten zestaw narzędzi automatycznie wykonuje następujące działania, jednocześnie minimalizując ilość miejsca używanego podczas modyfikacji tabeli `auditlog`.

1. Utwórz nową tabelę z nowym kluczem głównym i utwórz indeksy.

```
CREATE TABLE `auditlog_new` (
  `auditid`            varchar(25)                         NOT NULL,
  `userid`             bigint unsigned                     NULL,
  `username`           varchar(100)    DEFAULT ''          NOT NULL,
  `clock`              integer         DEFAULT '0'         NOT NULL,
```

```
  `ip`                varchar(39)     DEFAULT ''                NOT NULL,
  `action`            integer         DEFAULT '0'               NOT NULL,
  `resourcetype`      integer         DEFAULT '0'               NOT NULL,
  `resourceid`        bigint unsigned                           NULL,
  `resource_cuid`     varchar(25)                               NULL,
  `resourcename`      varchar(255)    DEFAULT ''                NOT NULL,
  `recordsetid`       varchar(25)                               NOT NULL,
  `details`           longtext                                  NOT NULL,
  PRIMARY KEY (auditid,clock)
) ENGINE=InnoDB;
CREATE INDEX `auditlog_1` ON `auditlog_new` (`userid`,`clock`);
CREATE INDEX `auditlog_2` ON `auditlog_new` (`clock`);
CREATE INDEX `auditlog_3` ON `auditlog_new` (`resourcetype`,`resourceid`);
```

2. Zamień tabele.

```
RENAME TABLE auditlog TO auditlog_old, auditlog_new TO auditlog;
```

3. Skopiuj dane ze starej tabeli do nowej tabeli.

```
INSERT INTO auditlog SELECT * FROM auditlog_old;
```

Można to zrobić partiami (wieloma instrukcjami `INSERT INTO` z klauzulami `WHERE clock`, zależnie od potrzeb), aby uniknąć nadmiernego zużycia zasobów.

4. Usuń starą tabelę.

```
DROP TABLE auditlog_old;
```

PostgreSQL

Ważne uwagi dotyczące przebudowy indeksów

PostgreSQL automatycznie przebudowuje indeksy dla klucza głównego podczas operacji `ALTER TABLE`. Zaleca się jednak również ręczne przebudowanie indeksów za pomocą instrukcji `REINDEX TABLE CONCURRENTLY`, aby zapewnić optymalną wydajność bazy danych.

Przebudowa indeksów może tymczasowo wymagać nawet trzykrotności przestrzeni dyskowej obecnie używanej przez indeksy. Aby uzyskać bieżący rozmiar indeksów, możesz wykonać następujące zapytanie:

```
SELECT pg_size_pretty(pg_indexes_size('auditlog'));
```

Jeśli dostępna przestrzeń dyskowa jest problemem, postępuj zgodnie z instrukcjami Zmiana klucza głównego bez przestoju. Dostępne są również inne opcje:

- Zwiększenie parametru PostgreSQL `maintenance_work_mem` może pomóc zmniejszyć użycie przestrzeni dyskowej podczas ręcznej przebudowy indeksów. Jednak modyfikacja tej zmiennej może wpłynąć na ogólne użycie pamięci przez bazę danych.
- Jeśli masz inny dysk lub tablespace z większą ilością dostępnego miejsca, możesz rozważyć zmianę lokalizacji pamięci tymczasowej dla przebudowy indeksów. Możesz ustawić parametr PostgreSQL `temp_tablespaces`, aby określić inny tablespace dla obiektów tymczasowych.
- Rozważ zwolnienie miejsca przez usunięcie potencjalnie niepotrzebnych danych.
- Rozważ zmniejszenie parametru *Okres przechowywania danych* housekeeper przed uruchomieniem housekeepera.

Zmiana klucza głównego z przestojem

1. Usuń bieżący klucz główny tabeli `auditlog` i dodaj nowy klucz główny.

```
ALTER TABLE auditlog DROP CONSTRAINT auditlog_pkey;
ALTER TABLE auditlog ADD PRIMARY KEY (auditid,clock);
```

2. Przebuduj indeksy (opcjonalne, ale zdecydowanie zalecane, zobacz Ważne uwagi dotyczące przebudowy indeksów).

```
REINDEX TABLE CONCURRENTLY auditlog;
```

Zmiana klucza głównego bez przestoju

Ręczna metoda zmiany klucza głównego jest opisana tutaj. Alternatywnie można rozważyć rozszerzenie `pg_repack` do utworzenia nowej tabeli, skopiowania danych i zamiany tabel.

1. Utwórz nową tabelę z nowym kluczem głównym i utwórz indeksy.

```
CREATE TABLE auditlog_new (
  auditid               varchar(25)                             NOT NULL,
  userid                bigint                                  NULL,
  username              varchar(100)    DEFAULT ''              NOT NULL,
  clock                 integer         DEFAULT '0'             NOT NULL,
  ip                    varchar(39)     DEFAULT ''              NOT NULL,
  action                integer         DEFAULT '0'             NOT NULL,
  resourcetype          integer         DEFAULT '0'             NOT NULL,
  resourceid            bigint                                  NULL,
  resource_cuid         varchar(25)                             NULL,
  resourcename          varchar(255)    DEFAULT ''              NOT NULL,
  recordsetid           varchar(25)                             NOT NULL,
  details               text            DEFAULT ''              NOT NULL,
  PRIMARY KEY (auditid,clock)
);
CREATE INDEX auditlog_new_1 ON auditlog_new (userid,clock);
CREATE INDEX auditlog_new_2 ON auditlog_new (clock);
CREATE INDEX auditlog_new_3 ON auditlog_new (resourcetype,resourceid);
```

2. Zamień tabele.

```
ALTER TABLE auditlog RENAME TO auditlog_old;
ALTER TABLE auditlog_new RENAME TO auditlog;
```

3. Skopiuj dane ze starej tabeli do nowej tabeli.

```
INSERT INTO auditlog SELECT * FROM auditlog_old;
```

Można to zrobić partiami (wieloma instrukcjami `INSERT INTO` z klauzulami `WHERE clock` według potrzeb), aby uniknąć nadmiernego zużycia zasobów.

4. Usuń starą tabelę.

```
DROP TABLE auditlog_old;
```

Zobacz także

- Aktualizacja bazy danych do kluczy głównych

5 Bezpieczne połączenie z bazą danych

Przegląd

Ta sekcja zawiera kroki konfiguracji Zabbix oraz przykłady konfiguracji dla bezpiecznych połączeń TLS pomiędzy:

Baza danych	Komponenty Zabbix
MySQL	Zabbix frontend, Zabbix serwer, Zabbix proxy
PostgreSQL	Zabbix frontend, Zabbix serwer, Zabbix proxy

Aby skonfigurować szyfrowanie połączeń w ramach systemu DBMS, szczegółowe informacje można znaleźć w oficjalnej dokumentacji producenta:

- MySQL: źródłowe i replikowane serwery baz danych.
- MySQL: serwery baz danych z replikacją grupową itp.
- PostgreSQL opcje szyfrowania.

Wszystkie przykłady opierają się na wydaniach GA MySQL CE (8.0) i PgSQL (13), dostępnych w oficjalnych repozytoriach dla CentOS 8.

Wymagania

Do skonfigurowania szyfrowania wymagane są następujące elementy:

- System operacyjny wspierany przez producenta, z OpenSSL >=1.1.X lub rozwiązaniem alternatywnym.

> **Note:**
> Zaleca się unikanie systemów operacyjnych, które osiągnęły status end-of-life, szczególnie w przypadku nowych instalacji

- Silnik bazy danych (RDBMS) zainstalowany i utrzymywany z oficjalnego repozytorium dostarczanego przez producenta. Systemy operacyjne są często dostarczane z nieaktualnymi wersjami oprogramowania bazodanowego, dla których obsługa szyfrowania nie jest zaimplementowana, na przykład systemy oparte na RHEL 7 oraz PostgreSQL 9.2, MariaDB 5.5 bez obsługi szyfrowania.

Terminologia

Ustawienie tej opcji wymusza użycie połączenia TLS z bazą danych przez serwer/proxy Zabbix oraz frontend do bazy danych:

- `required` — połącz przy użyciu TLS jako trybu transportu bez sprawdzania tożsamości
- `verify_ca` — połącz przy użyciu TLS i zweryfikuj certyfikat
- `verify_full` — połącz przy użyciu TLS, zweryfikuj certyfikat oraz sprawdź, czy tożsamość bazy danych (CN) określona przez DBHost jest zgodna z jej certyfikatem

Konfiguracja Zabbix

Frontend do bazy danych

Bezpieczne połączenie z bazą danych można skonfigurować podczas instalacji frontend:

- Zaznacz pole wyboru *Database TLS encryption* w kroku Configure DB connection, aby włączyć szyfrowanie transmisji.
- Zaznacz pole wyboru *Verify database certificate*, które pojawia się po zaznaczeniu pola *TLS encryption*, aby włączyć szyfrowanie z użyciem certyfikatów.

Note:
Dla MySQL pole wyboru *Database TLS encryption* jest wyłączone, jeśli *Database host* jest ustawiony na localhost, ponieważ połączenie korzystające z pliku socket (w systemach Unix) lub pamięci współdzielonej (w systemie Windows) nie może być szyfrowane.
Dla PostgreSQL pole wyboru *TLS encryption* jest wyłączone, jeśli wartość pola *Database host* zaczyna się od ukośnika lub pole jest puste.

Następujące parametry stają się dostępne w trybie szyfrowania TLS z użyciem certyfikatów (jeśli zaznaczone są oba pola wyboru):

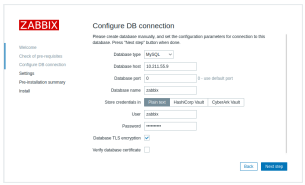
Parameter	Description
Database TLS CA file	Podaj pełną ścieżkę do prawidłowego pliku urzędu certyfikacji TLS (CA).
Database TLS key file	Podaj pełną ścieżkę do prawidłowego pliku klucza TLS.
Database TLS certificate file	Podaj pełną ścieżkę do prawidłowego pliku certyfikatu TLS.
Database host verification	Zaznacz to pole wyboru, aby włączyć weryfikację hosta. Wyłączone dla MYSQL, ponieważ biblioteka PHP MySQL nie pozwala pominąć kroku walidacji certyfikatu peera.
Database TLS cipher list	Podaj niestandardową listę prawidłowych szyfrów. Format listy szyfrów musi być zgodny ze standardem OpenSSL. Dostępne tylko dla MySQL.

Attention:
Parametry TLS muszą wskazywać prawidłowe pliki. Jeśli wskazują na nieistniejące lub nieprawidłowe pliki, spowoduje to błąd autoryzacji.
Jeśli pliki certyfikatów mają uprawnienia do zapisu, frontend generuje ostrzeżenie w raporcie System information, że „TLS certificate files must be read-only.” (wyświetlane tylko wtedy, gdy użytkownik PHP jest właścicielem certyfikatu).

Certyfikaty chronione hasłem nie są obsługiwane.

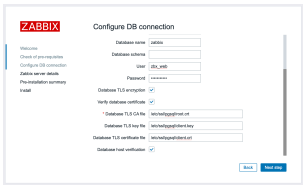
Przypadki użycia

Zabbix frontend używa interfejsu GUI do definiowania możliwych opcji: `required`, `verify_ca`, `verify_full`. Wymagane opcje należy określić w kroku kreatora instalacji *Configure DB connections*. Opcje te są mapowane do pliku konfiguracyjnego (zabbix.conf.php) w następujący sposób:

Ustawienia GUI	Plik konfiguracyjny	Opis	Wynik
	... // Used for TLS connection. $DB['ENCRYPTION'] = true; $DB['KEY_FILE'] = ''; $DB['CERT_FILE'] = ''; $DB['CA_FILE'] = ''; $DB['VERIFY_HOST'] = false; $DB['CIPHER_LIST'] = ''; ...	Zaznacz *Database TLS encryption* Pozostaw *Verify database certificate* niezaznaczone	Włącza tryb `required`.
	... $DB['ENCRYPTION'] = true; $DB['KEY_FILE'] = ''; $DB['CERT_FILE'] = ''; $DB['CA_FILE'] = '/etc/ssl/mysql/ca.pem'; $DB['VERIFY_HOST'] = false; $DB['CIPHER_LIST'] = ''; ...	1. Zaznacz *Database TLS encryption* i *Verify database certificate* 2. Podaj ścieżkę do *Database TLS CA file*	Włącza tryb `verify_ca`.

Ustawienia GUI	Plik konfiguracyjny	Opis	Wynik

	...
	// Used for TLS connection with strictly defined Cipher list.
	$DB['ENCRYPTION'] = true;
	$DB['KEY_FILE'] = '<key_file_path>';
	$DB['CERT_FILE'] = '<key_file_path>';
	$DB['CA_FILE'] = '<key_file_path>';
	$DB['VERIFY_HOST'] = true;
	$DB['CIPHER_LIST'] = '<cipher_list>';
	...
	
	Or:
	
	...
	// Used for TLS connection without Cipher list defined - selected by MySQL server
	$DB['ENCRYPTION'] = true;
	$DB['KEY_FILE'] = '<key_file_path>';
	$DB['CERT_FILE'] = '<key_file_path>';
	$DB['CA_FILE'] = '<key_file_path>';
	$DB['VERIFY_HOST'] = true;
	$DB['CIPHER_LIST'] = '';
	...
		1. Zaznacz *Database TLS encryption* i *Verify database certificate*
		2. Podaj ścieżkę do *Database TLS key file*
		3. Podaj ścieżkę do *Database TLS CA file*
		4. Podaj ścieżkę do *Database TLS certificate file*
		5. Podaj *Database TLS cipher list* (opcjonalnie)
			Włącza tryb `verify_full` dla MySQL.

	... $DB['ENCRYPTION'] = true; $DB['KEY_FILE'] = '<key_file_path>'; $DB['CERT_FILE'] = '<key_file_path>'; $DB['CA_FILE'] = '<key_file_path>'; $DB['VERIFY_HOST'] = true; $DB['CIPHER_LIST'] = ' '; ...	1. Zaznacz *Database TLS encryption* i *Verify database certificate* 2. Podaj ścieżkę do *Database TLS key file* 3. Podaj ścieżkę do *Database TLS CA file* 4. Podaj ścieżkę do *Database TLS certificate file* 5. Zaznacz *Database host verification*	Włącza tryb `verify_full` dla PostgreSQL.

Zobacz także: Przykłady konfiguracji szyfrowania dla MySQL, Przykłady konfiguracji szyfrowania dla PostgreSQL.

Konfiguracja serwera/proxy Zabbix

Bezpieczne połączenia z bazą danych można skonfigurować za pomocą odpowiednich parametrów w pliku konfiguracyjnym Zabbix serwer i/lub proxy.

Konfiguracja	Wynik
Brak	Połączenie z bazą danych bez szyfrowania.
1. Ustaw `DBTLSConnect=required`	Serwer/proxy nawiązują połączenie TLS z bazą danych. Nieszyfrowane połączenie nie jest dozwolone.
1. Ustaw `DBTLSConnect=verify_ca` 2. Ustaw `DBTLSCAFile` - określ plik urzędu certyfikacji TLS	Serwer/proxy nawiązują połączenie TLS z bazą danych po zweryfikowaniu certyfikatu bazy danych.
1. Ustaw `DBTLSConnect=verify_full` 2. Ustaw `DBTLSCAFile` - określ plik urzędu certyfikacji TLS	Serwer/proxy nawiązują połączenie TLS z bazą danych po zweryfikowaniu certyfikatu bazy danych oraz tożsamości hosta bazy danych.
1. Ustaw `DBTLSCAFile` - określ plik urzędu certyfikacji TLS 2. Ustaw `DBTLSCertFile` - określ plik certyfikatu klucza publicznego klienta 3. Ustaw `DBTLSKeyFile` - określ plik klucza prywatnego klienta	Serwer/proxy przedstawiają certyfikat klienta podczas łączenia z bazą danych.
1. Ustaw `DBTLSCipher` - lista szyfrów, które klient dopuszcza dla połączeń używających protokołów TLS do wersji TLS 1.2 włącznie lub `DBTLSCipher13` - lista szyfrów, które klient dopuszcza dla połączeń używających protokołu TLS 1.3	(MySQL) Połączenie TLS jest nawiązywane z użyciem szyfru z podanej listy. (PostgreSQL) Ustawienie tej opcji będzie traktowane jako błąd.

1 Konfiguracja szyfrowania MySQL

Przegląd

Ta sekcja zawiera kilka przykładów konfiguracji szyfrowania dla CentOS 8.2 i MySQL 8.4.0 i może służyć jako przewodnik szybkiego startu dotyczący szyfrowania połączenia z bazą danych.

Attention:
Jeśli host MySQL jest ustawiony na localhost, opcje szyfrowania nie będą dostępne. W takim przypadku połączenie między frontendem Zabbix a bazą danych używa pliku socket (w systemach Unix) lub pamięci współdzielonej (w systemie Windows) i nie może być szyfrowane.

Note:
Lista kombinacji szyfrowania nie ogranicza się do tych wymienionych na tej stronie. Dostępnych jest znacznie więcej kombinacji.

Wymagania wstępne

Zainstaluj bazę danych MySQL z oficjalnego repozytorium.

Szczegółowe informacje o korzystaniu z repozytorium MySQL znajdują się w dokumentacji MySQL.

Serwer MySQL jest gotowy do akceptowania bezpiecznych połączeń z użyciem certyfikatu z podpisem własnym.

Aby sprawdzić, którzy użytkownicy korzystają z szyfrowanego połączenia, uruchom następujące zapytanie (Performance Schema musi być włączone):

```
SELECT sbt.variable_value AS tls_version, t2.variable_value AS cipher, processlist_user AS user, processli
FROM performance_schema.status_by_thread  AS sbt
JOIN performance_schema.threads AS t ON t.thread_id = sbt.thread_id
JOIN performance_schema.status_by_thread AS t2 ON t2.thread_id = t.thread_id
WHERE sbt.variable_name = 'Ssl_version' and t2.variable_name = 'Ssl_cipher'
ORDER BY tls_version;
```

Szyfrowanie wyłącznie transportu

Konfiguracja MySQL

Nowoczesne wersje bazy danych są gotowe do użycia od razu po instalacji dla `required` trybu szyfrowania. Certyfikat po stronie serwera zostanie utworzony po wstępnej konfiguracji i uruchomieniu.

Utwórz użytkowników i role dla głównych komponentów:

```
mysql> CREATE USER
 'zbx_srv'@'%' IDENTIFIED WITH caching_sha2_password BY '<strong_password>',
 'zbx_web'@'%' IDENTIFIED WITH caching_sha2_password BY '<strong_password>'
 REQUIRE SSL
 PASSWORD HISTORY 5;

mysql> CREATE ROLE 'zbx_srv_role', 'zbx_web_role';

mysql> GRANT SELECT, UPDATE, DELETE, INSERT, CREATE, DROP, ALTER, INDEX, REFERENCES ON zabbix.* TO 'zbx_sr
mysql> GRANT SELECT, UPDATE, DELETE, INSERT ON zabbix.* TO 'zbx_web_role';

mysql> GRANT 'zbx_srv_role' TO 'zbx_srv'@'%';
mysql> GRANT 'zbx_web_role' TO 'zbx_web'@'%';

mysql> SET DEFAULT ROLE 'zbx_srv_role' TO 'zbx_srv'@'%';
mysql> SET DEFAULT ROLE 'zbx_web_role' TO 'zbx_web'@'%';
```

Należy pamiętać, że protokół X.509 nie jest używany do sprawdzania tożsamości, ale użytkownik jest skonfigurowany tak, aby używać wyłącznie połączeń szyfrowanych. Więcej informacji o konfigurowaniu użytkowników można znaleźć w dokumentacji MySQL.

Uruchom, aby sprawdzić połączenie (połączenie przez socket nie może być użyte do testowania bezpiecznych połączeń):

```
mysql -u zbx_srv -p -h 10.211.55.9 --ssl-mode=REQUIRED
```

Sprawdź bieżący stan i dostępne zestawy szyfrów:

```
mysql> status
--------------
mysql Ver 8.4.0 for Linux on x86_64 (MySQL Community Server - GPL)

Connection id: 62
Current database:
Current user: zbx_srv@bfdb.local
SSL: Cipher in use is TLS_AES_256_GCM_SHA384

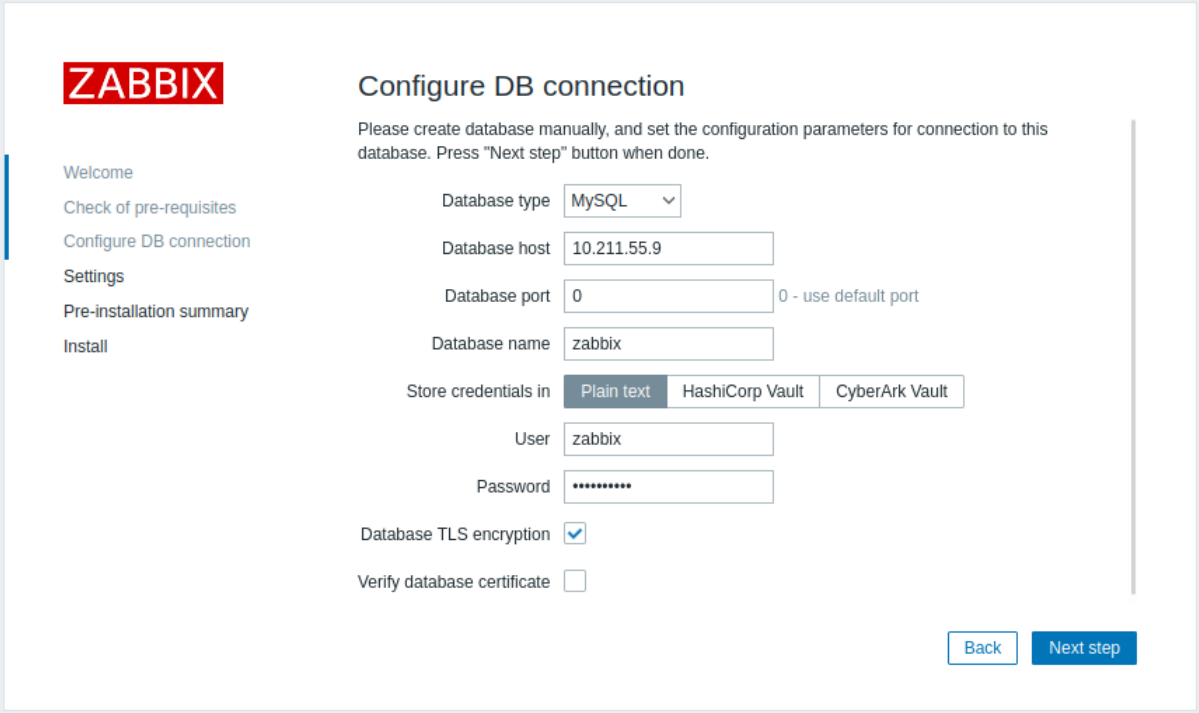

mysql> SHOW SESSION STATUS LIKE 'Ssl_cipher_list'\G;
*************************** 1. row ***************************
Variable_name: Ssl_cipher_list
Value: TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256:TLS_AES_128_CCM_SHA256:E
1 row in set (0.00 sec)

ERROR:
No query specified
```

Frontend

Aby włączyć szyfrowanie tylko transportu dla połączeń między frontend a bazą danych:

- Zaznacz *Database TLS encryption*
- Pozostaw *Verify database certificate* niezaznaczone



Serwer

Aby włączyć szyfrowanie wyłącznie transportu dla połączeń między serwerem a bazą danych, skonfiguruj */etc/zabbix/zabbix_server.conf*:

```
...
DBHost=10.211.55.9
DBName=zabbix
DBUser=zbx_srv
DBPassword=<strong_password>
DBTLSConnect=required
...
```

Szyfrowanie z weryfikacją urzędu certyfikacji

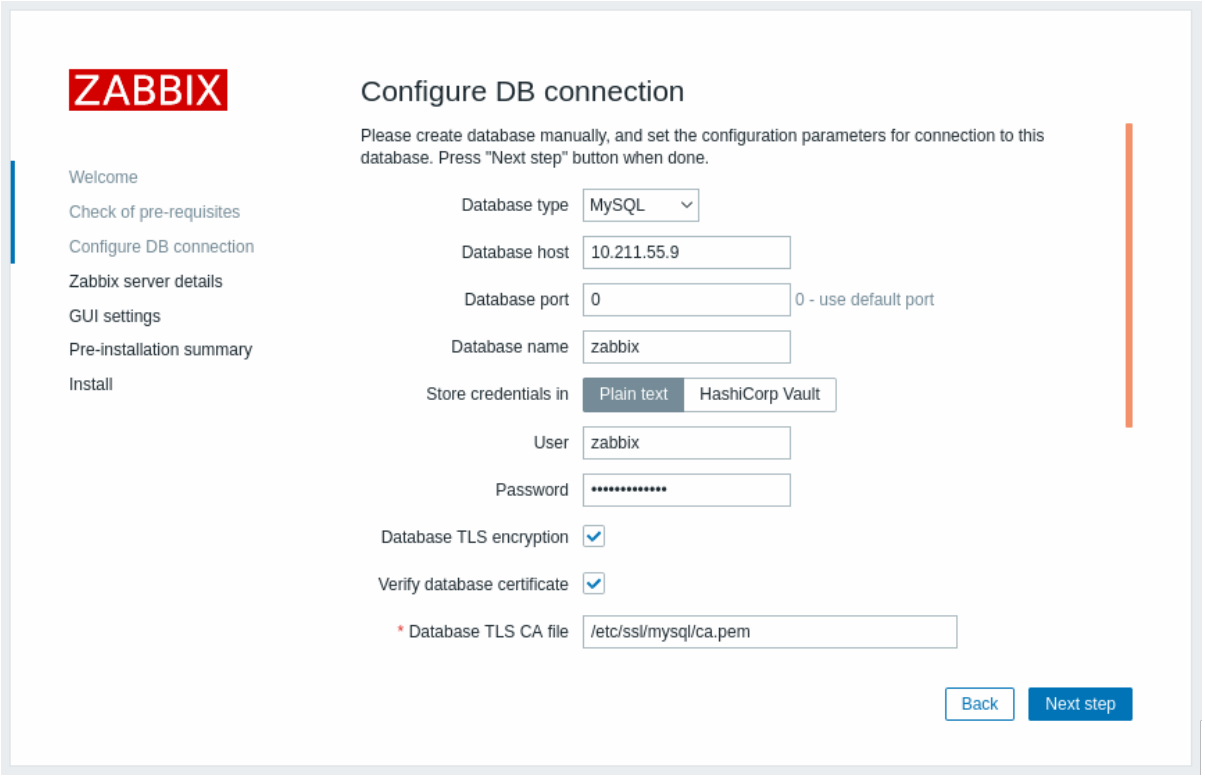
Skopiuj wymagany urząd certyfikacji MySQL na serwer frontend Zabbix i ustaw odpowiednie uprawnienia, aby serwer WWW mógł odczytać ten plik.

Note:
Ten tryb nie działa w RHEL 7 z powodu starszych bibliotek MySQL.

Frontend

Aby włączyć szyfrowanie z weryfikacją certyfikatu dla połączeń między frontend Zabbix a bazą danych:

- Zaznacz *Database TLS encryption* i *Verify database certificate*
- Określ ścieżkę do pliku Database TLS CA



Alternatywnie można to ustawić w pliku */etc/zabbix/web/zabbix.conf.php*:

```
...
$DB['ENCRYPTION'] = true;
$DB['KEY_FILE'] = '';
$DB['CERT_FILE'] = '';
$DB['CA_FILE'] = '/etc/ssl/mysql/ca.pem';
$DB['VERIFY_HOST'] = false;
$DB['CIPHER_LIST'] = '';
...
```

Aby rozwiązać problemy, użyj narzędzia wiersza poleceń, aby sprawdzić, czy połączenie jest możliwe dla wymaganego użytkownika:

```
    mysql -u zbx_web -p -h 10.211.55.9 --ssl-mode=REQUIRED --ssl-ca=/var/lib/mysql/ca.pem
```

Serwer

Aby włączyć szyfrowanie z weryfikacją certyfikatu dla połączeń między serwerem Zabbix a bazą danych, skonfiguruj */etc/zabbix/zabbix_server.c*

```
...
DBHost=10.211.55.9
DBName=zabbix
DBUser=zbx_srv
DBPassword=<strong_password>
DBTLSConnect=verify_ca
DBTLSCAFile=/etc/ssl/mysql/ca.pem
...
```

Szyfrowanie z pełną weryfikacją

Konfiguracja MySQL

Ustaw opcję konfiguracji serwera MySQL CE (*/etc/my.cnf.d/server-tls.cnf*) na:

```
[mysqld]
...
##### w tym przykładzie klucze znajdują się w katalogu datadir MySQL CE
ssl_ca=ca.pem
ssl_cert=server-cert.pem
ssl_key=server-key.pem

require_secure_transport=ON
tls_version=TLSv1.3
...
```

Klucze dla serwera i klienta MySQL CE (frontend Zabbix) należy utworzyć ręcznie zgodnie z dokumentacją MySQL CE: Creating SSL and RSA certificates and keys using MySQL lub Creating SSL certificates and keys using openssl

Attention:
Certyfikat serwera MySQL powinien zawierać pole Common Name ustawione na nazwę FQDN, ponieważ frontend Zabbix będzie używać nazwy DNS do komunikacji z bazą danych lub adresu IP hosta bazy danych.

Utwórz użytkownika MySQL:

```
mysql> CREATE USER
  'zbx_srv'@'%' IDENTIFIED WITH caching_sha2_password BY '<strong_password>',
  'zbx_web'@'%' IDENTIFIED WITH caching_sha2_password BY '<strong_password>'
  REQUIRE X509
  PASSWORD HISTORY 5;
```

Sprawdź, czy możliwe jest zalogowanie się przy użyciu tego użytkownika:

```
mysql -u zbx_web -p -h 10.211.55.9 --ssl-mode=VERIFY_IDENTITY --ssl-ca=/var/lib/mysql/ca.pem --ssl-cert=/v
```

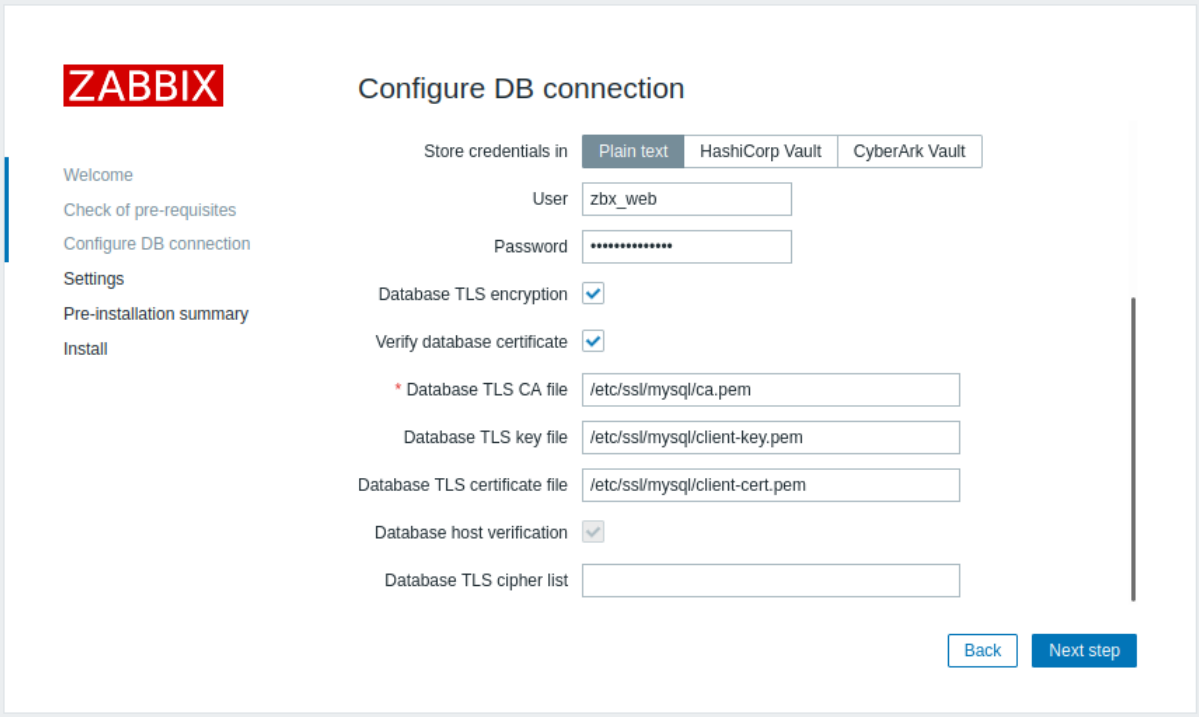
Frontend

Aby włączyć szyfrowanie z pełną weryfikacją dla połączeń między frontendem Zabbix a bazą danych:

- Zaznacz *Database TLS encryption* oraz *Verify database certificate*
- Określ ścieżkę do *Database TLS key file*
- Określ ścieżkę do *Database TLS CA file*
- Określ ścieżkę do *Database TLS certificate file*

Zwróć uwagę, że opcja *Database host verification* jest zaznaczona i wyszarzona — tego kroku nie można pominąć w przypadku MySQL.

Warning:
Jeśli pole *Database TLS cipher list* pozostanie puste, zostaną włączone wspólne szyfry dozwolone zarówno przez frontend (klienta), jak i serwer. Alternatywnie szyfry można ustawić jawnie, zgodnie z wymaganiami konfiguracji szyfrów.



Alternatywnie można to ustawić w pliku */etc/zabbix/web/zabbix.conf.php*:

```
...
// Used for TLS connection with strictly defined Cipher list.
$DB['ENCRYPTION'] = true;
$DB['KEY_FILE'] = '/etc/ssl/mysql/client-key.pem';
$DB['CERT_FILE'] = '/etc/ssl/mysql/client-cert.pem';
$DB['CA_FILE'] = '/etc/ssl/mysql/ca.pem';
```

```
$DB['VERIFY_HOST'] = true;
$DB['CIPHER_LIST'] = 'TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256:TLS_AES_1
...
// or
...
// Used for TLS connection without Cipher list defined - selected by MySQL server
$DB['ENCRYPTION'] = true;
$DB['KEY_FILE'] = '/etc/ssl/mysql/client-key.pem';
$DB['CERT_FILE'] = '/etc/ssl/mysql/client-cert.pem';
$DB['CA_FILE'] = '/etc/ssl/mysql/ca.pem';
$DB['VERIFY_HOST'] = true;
$DB['CIPHER_LIST'] = '';
...
```

Serwer

Aby włączyć szyfrowanie z pełną weryfikacją dla połączeń między serwerem Zabbix a bazą danych, skonfiguruj */etc/zabbix/zabbix_server.conf*:

```
...
DBHost=10.211.55.9
DBName=zabbix
DBUser=zbx_srv
DBPassword=<strong_password>
DBTLSConnect=verify_full
DBTLSCAFile=/etc/ssl/mysql/ca.pem
DBTLSCertFile=/etc/ssl/mysql/client-cert.pem
DBTLSKeyFile=/etc/ssl/mysql/client-key.pem
...
```

2 Konfiguracja szyfrowania PostgreSQL

Przegląd

Ta sekcja zawiera kilka przykładów konfiguracji szyfrowania dla CentOS 8.2 i PostgreSQL 13.

> **Note:**
> Połączenie między frontend Zabbix a PostgreSQL nie może być szyfrowane (parametry w GUI są wyłączone), jeśli wartość pola *Database host* zaczyna się od ukośnika lub pole jest puste.

Wymagania wstępne

Zainstaluj bazę danych PostgreSQL, korzystając z oficjalnego repozytorium.

PostgreSQL nie jest domyślnie skonfigurowany do akceptowania połączeń TLS. Postępuj zgodnie z instrukcjami w dokumentacji PostgreSQL dotyczącymi przygotowania certyfikatów z użyciem postgresql.conf, a także kontroli dostępu użytkowników za pośrednictwem ph_hba.conf.

Domyślnie gniazdo PostgreSQL jest powiązane z localhost; aby umożliwić zdalne połączenia sieciowe, należy włączyć nasłuchiwanie na rzeczywistym interfejsie sieciowym.

Ustawienia PostgreSQL dla wszystkich trybów mogą wyglądać następująco:

/var/lib/pgsql/13/data/postgresql.conf:

```
...
ssl = on
ssl_ca_file = 'root.crt'
ssl_cert_file = 'server.crt'
ssl_key_file = 'server.key'
ssl_ciphers = 'HIGH:MEDIUM:+3DES:!aNULL'
ssl_prefer_server_ciphers = on
ssl_min_protocol_version = 'TLSv1.3'
...
```

Aby skonfigurować kontrolę dostępu, dostosuj */var/lib/pgsql/13/data/pg_hba.conf*:

```
...
### require
```

```
hostssl all all 0.0.0.0/0 md5

### verify CA
hostssl all all 0.0.0.0/0 md5 clientcert=verify-ca

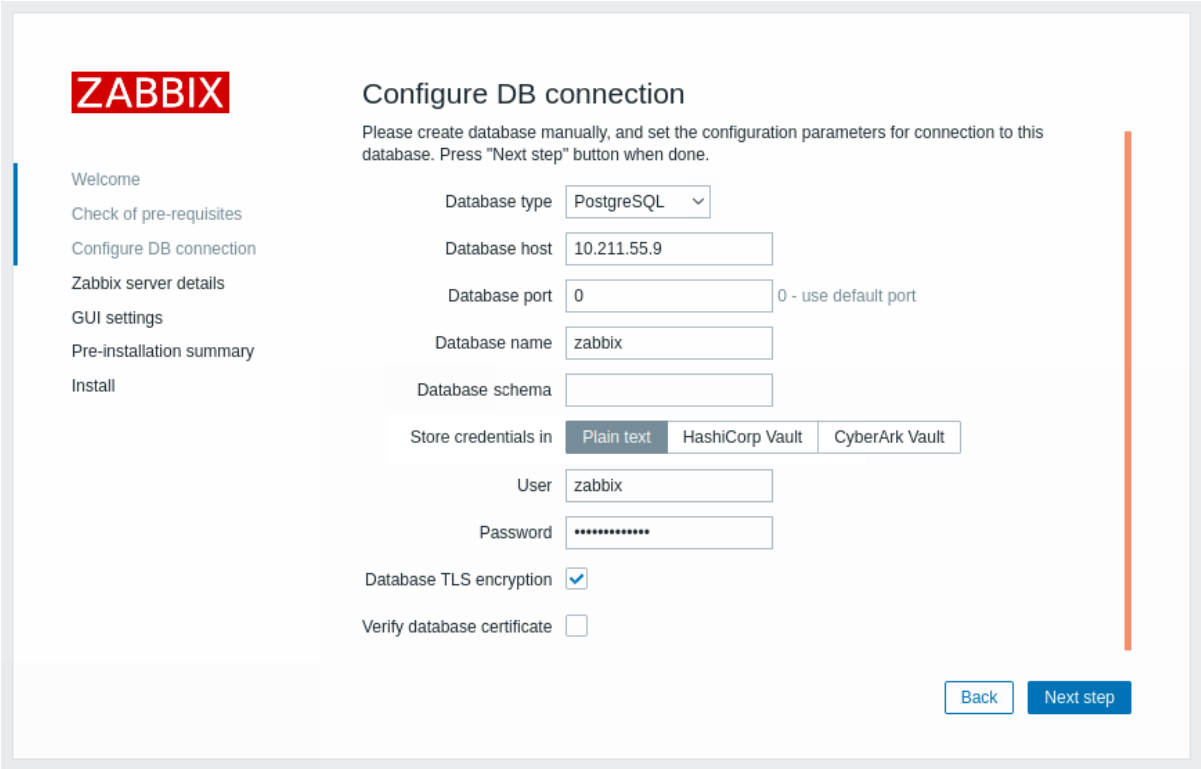
### verify full
hostssl all all 0.0.0.0/0 md5 clientcert=verify-full
...
```

Szyfrowanie wyłącznie transportu

Frontend

Aby włączyć szyfrowanie tylko transportu dla połączeń między frontend a bazą danych:

- Zaznacz *Database TLS encryption*
- Pozostaw *Verify database certificate* niezaznaczone



Serwer

Aby włączyć szyfrowanie wyłącznie transportu dla połączeń między serwerem a bazą danych, skonfiguruj plik */etc/zabbix/zabbix_server.conf*:

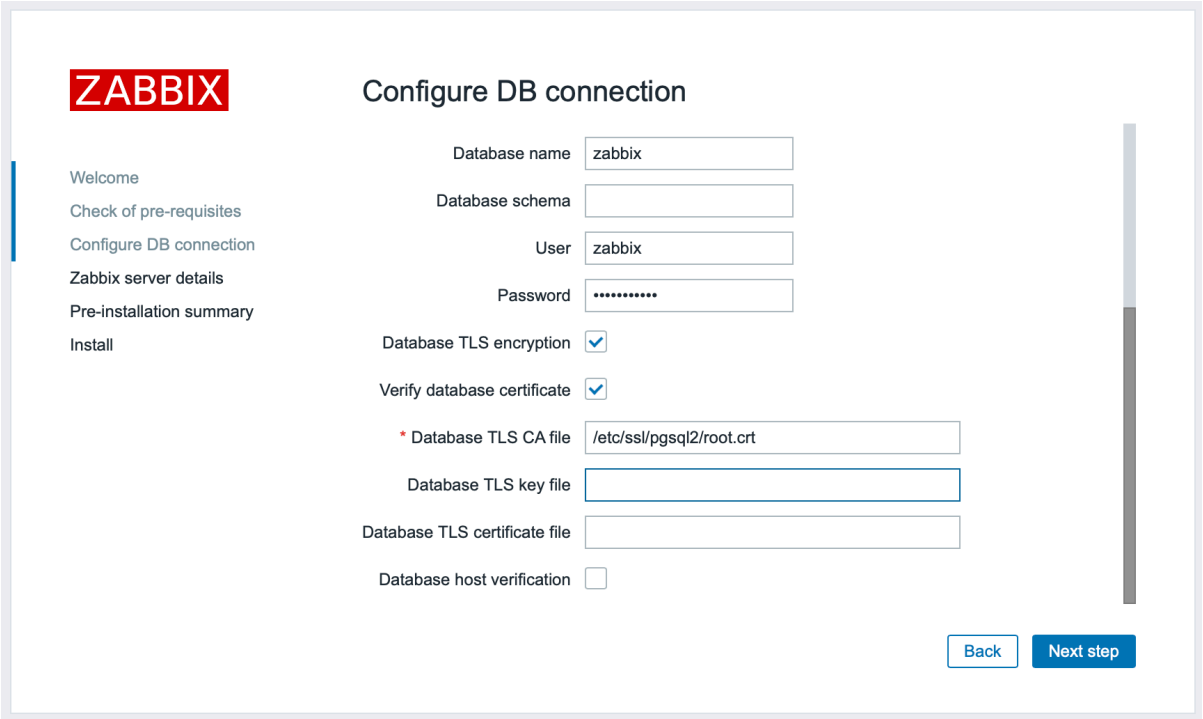
```
...
DBHost=10.211.55.9
DBName=zabbix
DBUser=zbx_srv
DBPassword=<strong_password>
DBTLSConnect=required
...
```

Szyfrowanie z weryfikacją urzędu certyfikacji

Frontend

Aby włączyć szyfrowanie z weryfikacją urzędu certyfikacji dla połączeń między frontendem Zabbix a bazą danych:

- Zaznacz *Database TLS encryption* i *Verify database certificate*
- Określ ścieżkę do *Database TLS CA file*



Alternatywnie można to ustawić w */etc/zabbix/web/zabbix.conf.php:*

```
...
$DB['ENCRYPTION'] = true;
$DB['KEY_FILE'] = '';
$DB['CERT_FILE'] = '';
$DB['CA_FILE'] = '/etc/ssl/pgsql/root.crt';
$DB['VERIFY_HOST'] = false;
$DB['CIPHER_LIST'] = '';
...
```

Serwer

Aby włączyć szyfrowanie z weryfikacją certyfikatu dla połączeń między serwer Zabbix a bazą danych, skonfiguruj */etc/zabbix/zabbix_server.con*

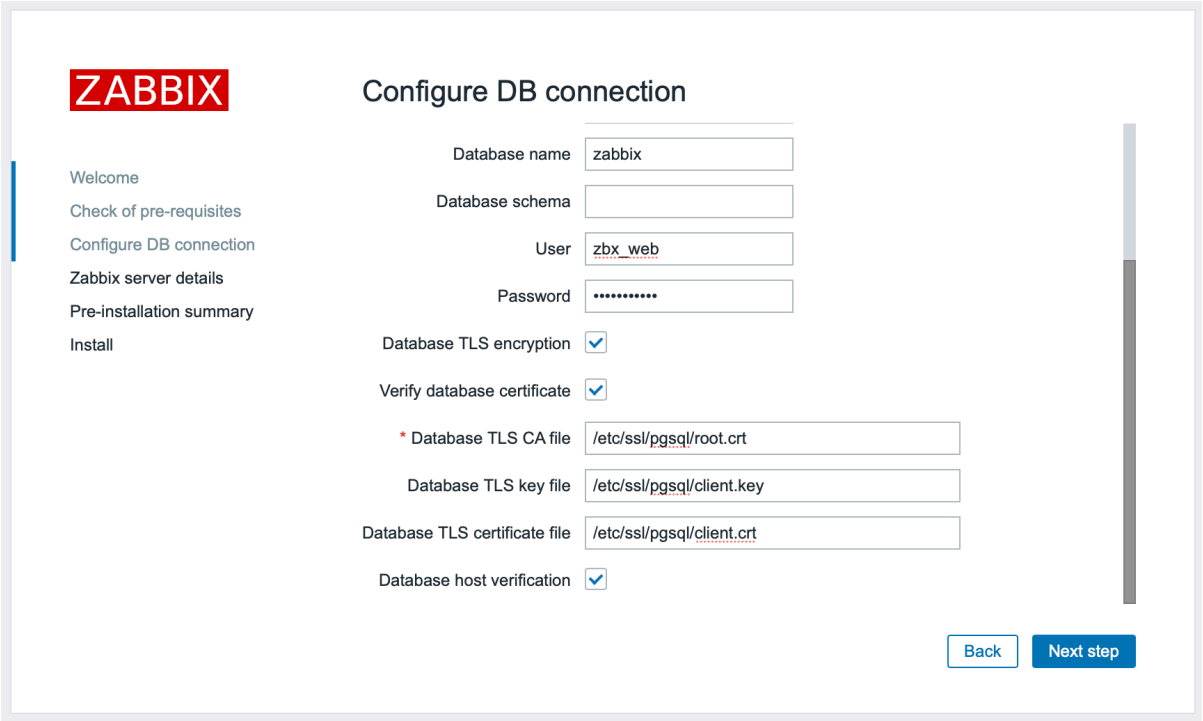
```
...
DBHost=10.211.55.9
DBName=zabbix
DBUser=zbx_srv
DBPassword=<strong_password>
DBTLSConnect=verify_ca
DBTLSCAFile=/etc/ssl/pgsql/root.crt
...
```

Szyfrowanie z pełną weryfikacją

Frontend

Aby włączyć szyfrowanie z użyciem certyfikatu oraz weryfikację tożsamości hosta bazy danych dla połączeń między frontend a bazą danych:

- Zaznacz *Database TLS encryption* i *Verify database certificate*
- Określ ścieżkę do *Database TLS key file*
- Określ ścieżkę do *Database TLS CA file*
- Określ ścieżkę do *Database TLS certificate file*
- Zaznacz *Database host verification*



Alternatywnie można to ustawić w */etc/zabbix/web/zabbix.conf.php:*

```
$DB['ENCRYPTION'] = true;
$DB['KEY_FILE'] = '';
$DB['CERT_FILE'] = '';
$DB['CA_FILE'] = '/etc/ssl/pgsql/root.crt';
$DB['VERIFY_HOST'] = true;
$DB['CIPHER_LIST'] = '';
...
```

Serwer

Aby włączyć szyfrowanie z użyciem certyfikatu oraz weryfikację tożsamości hosta bazy danych dla połączeń między serwerem Zabbix a bazą danych, skonfiguruj */etc/zabbix/zabbix_server.conf*:

```
...
DBHost=10.211.55.9
DBName=zabbix
DBUser=zbx_srv
DBPassword=<strong_password>
DBTLSConnect=verify_full
DBTLSCAFile=/etc/ssl/pgsql/root.crt
DBTLSCertFile=/etc/ssl/pgsql/client.crt
DBTLSKeyFile=/etc/ssl/pgsql/client.key
...
```

6 Bezpieczne połączenie z frontendem

Przegląd

Ta sekcja zawiera kroki konfiguracji Zabbix oraz przykłady konfiguracji dla bezpiecznych połączeń TLS między frontend Zabbix a serwer Zabbix.

Konfiguracja

Domyślnie komunikacja między frontendem Zabbix a serwerem Zabbix nie jest szyfrowana. Aby zwiększyć bezpieczeństwo, włącz TLS po obu stronach. Poniżej znajduje się przykład najprostszego sposobu, aby to zrobić.

1. Wygeneruj certyfikaty i klucze.

Utwórz katalog roboczy:

```
sudo mkdir -p /etc/zabbix/ssl && cd /etc/zabbix/ssl
```

Utwórz certyfikat CA (dostosuj wartość `MyZabbixCA`, aby odpowiadała rzeczywistej nazwie pospolitej):

```
sudo openssl genrsa -out ca.key 4096
sudo openssl req -new -x509 -days 3650 -key ca.key -out ca.crt -subj "/CN=MyZabbixCA/"
```

Wygeneruj klucz prywatny i certyfikat dla serwera Zabbix (dostosuj wartość `zabbix-server.example.com`, aby odpowiadała rzeczywistej nazwie pospolitej):

```
sudo openssl genrsa -out server.key 2048
sudo openssl req -new -key server.key -out server.csr -subj "/CN=zabbix-server.example.com/"
sudo openssl x509 -req -days 365 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -sha256 -out serv
```

Wygeneruj klucz prywatny i certyfikat dla frontendu Zabbix (dostosuj wartość `zabbix-frontend-node`, aby odpowiadała rzeczywistej nazwie pospolitej):

```
sudo openssl genrsa -out frontend.key 2048
sudo openssl req -new -key frontend.key -out frontend.csr -subj "/CN=zabbix-frontend-node/"
sudo openssl x509 -req -days 365 -in frontend.csr -CA ca.crt -CAkey ca.key -CAcreateserial -sha256 -out fr
```

2. Ustaw odpowiednie uprawnienia.

Dla serwera Zabbix (dostosuj właściciela/grupę zgodnie z użytkownikiem demona serwera Zabbix w swojej dystrybucji):

```
sudo chown root:zabbix /etc/zabbix/ssl/server.{crt,key} /etc/zabbix/ssl/ca.crt
sudo chmod 640 /etc/zabbix/ssl/server.key
sudo chmod 644 /etc/zabbix/ssl/server.crt /etc/zabbix/ssl/ca.crt
```

Dla frontendu (dostosuj właściciela/grupę zgodnie z użytkownikiem serwera WWW w swojej dystrybucji):

```
sudo chown root:www-data /etc/zabbix/ssl/frontend.{crt,key}
sudo chmod 640 /etc/zabbix/ssl/frontend.key
sudo chmod 644 /etc/zabbix/ssl/frontend.crt
```

3. Skonfiguruj serwer Zabbix.

W `zabbix_server.conf` dodaj:

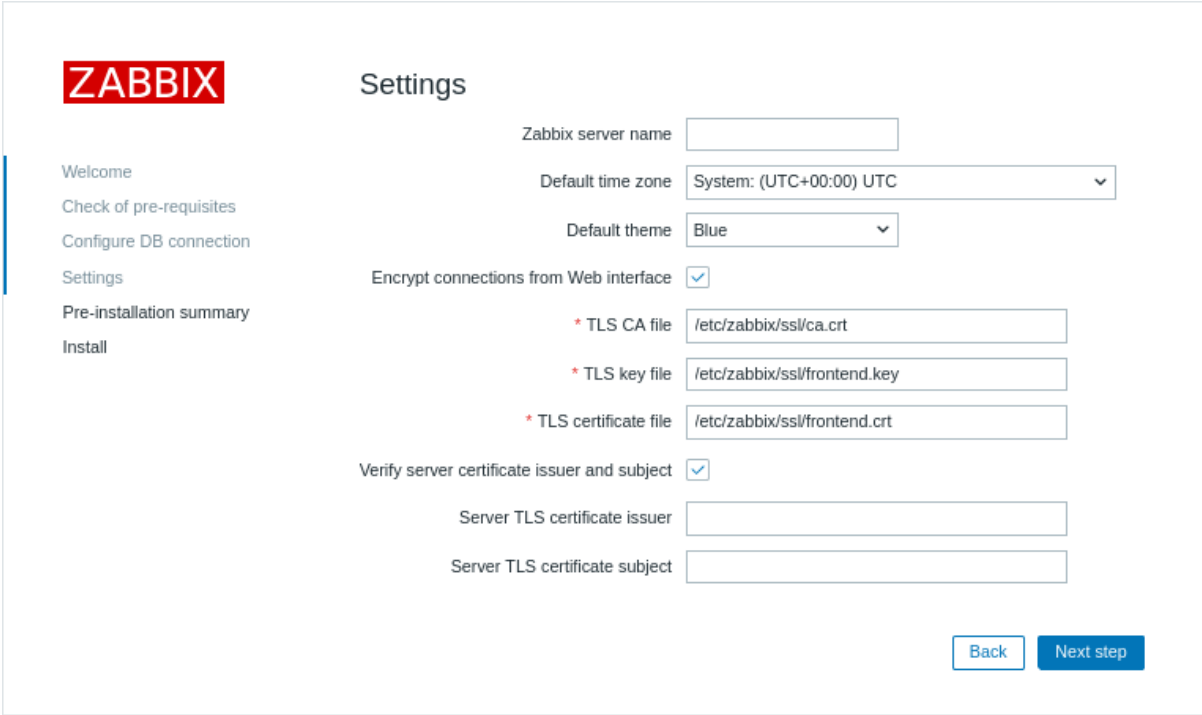
```
TLSFrontendAccept=cert
TLSCertFile=/etc/zabbix/ssl/server.crt
TLSKeyFile=/etc/zabbix/ssl/server.key
TLSCAFile=/etc/zabbix/ssl/ca.crt
#### Opcjonalnie:
#### TLSFrontendCertIssuer=/CN=MyZabbixCA/
#### TLSFrontendCertSubject=/CN=zabbix-frontend-node/
```

Następnie uruchom ponownie serwer:

```
sudo systemctl restart zabbix-server
```

4. Skonfiguruj frontend Zabbix.

Podczas instalacji interfejsu webowego włącz opcję *Encrypt connections from Web interface* (oraz opcję *Verify server certificate issuer and subject*, jeśli to konieczne) i wypełnij pola *TLS CA file*, *TLS key file*, *TLS certificate file* (oraz pola *Server TLS certificate issuer* i *Server TLS certificate subject*, jeśli to konieczne):



Parametr	Opis
TLS CA file	Podaj pełną ścieżkę do pliku certyfikatu urzędu certyfikacji (CA) używanego do weryfikacji certyfikatu serwera.
TLS key file	Podaj pełną ścieżkę do pliku klucza prywatnego klienta odpowiadającego certyfikatowi klienta.
TLS certificate file	Podaj pełną ścieżkę do pliku certyfikatu klienta, jeśli wymagana jest wzajemna autentykacja TLS.
Server TLS certificate issuer	Podaj nazwę wyróżniającą (DN) wystawcy, która ma zostać dopasowana do certyfikatu serwera.
Server TLS certificate subject	Podaj nazwę wyróżniającą (DN) podmiotu, która ma zostać dopasowana do certyfikatu serwera.

W istniejących instalacjach edytuj następujące pola w `zabbix.conf.php`:

```
$ZBX_SERVER_TLS['ACTIVE'] = '1';
$ZBX_SERVER_TLS['CA_FILE'] = '/etc/zabbix/ssl/ca.crt';
$ZBX_SERVER_TLS['KEY_FILE'] = '/etc/zabbix/ssl/frontend.key';
$ZBX_SERVER_TLS['CERT_FILE'] = '/etc/zabbix/ssl/frontend.crt';
// Opcjonalnie:
// $ZBX_SERVER_TLS['CERTIFICATE_ISSUER']  = '/CN=MyZabbixCA/';
// $ZBX_SERVER_TLS['CERTIFICATE_SUBJECT'] = '/CN=zabbix-server.example.com/';
```

5. Zweryfikuj szyfrowanie, potwierdzając, że we frontendzie Zabbix ani w pliku dziennika serwera Zabbix nie ma komunikatów o błędach:

```
tail -f /var/log/zabbix/zabbix_server.log
```

7 Konfiguracja TimescaleDB

Przegląd

Zabbix obsługuje TimescaleDB, rozwiązanie bazodanowe oparte na PostgreSQL, które automatycznie partycjonuje dane na fragmenty oparte na czasie, aby zapewnić wyższą wydajność przy dużej skali.

Warning:
Obecnie TimescaleDB nie jest obsługiwany przez Zabbix proxy.

Instrukcje na tej stronie można wykorzystać w następujących scenariuszach:

- Tworzenie bazy danych TimescaleDB lub migracja z istniejących tabel PostgreSQL do TimescaleDB (zobacz Konfiguracja).
- Aktualizacja schematu istniejącej bazy danych TimescaleDB podczas aktualizacji Zabbix (zobacz Aktualizacja schematu TimescaleDB).

Konfiguracja

Wymagania wstępne: rozszerzenie TimescaleDB w obsługiwanej wersji zainstalowane na serwerze bazy danych. Instrukcje instalacji znajdują się w dokumentacji TimescaleDB.

> **Warning:**
> Przed instalacją TimescaleDB zainstaluj obsługiwaną wersję PostgreSQL z oficjalnego repozytorium PostgreSQL.

Włącz rozszerzenie TimescaleDB dla określonej bazy danych, wykonując:

```
echo "CREATE EXTENSION IF NOT EXISTS timescaledb CASCADE;" | sudo -u postgres psql zabbix
```

Uruchomienie tego polecenia wymaga uprawnień administratora bazy danych.

> **Note:**
> Jeśli używasz schematu bazy danych innego niż 'public', musisz dodać klauzulę SCHEMA do powyższego polecenia. Np.: `echo "CREATE EXTENSION IF NOT EXISTS timescaledb SCHEMA yourschema CASCADE;" | sudo -u postgres psql zabbix`

Następnie uruchom skrypt `postgresql/timescaledb/schema.sql`. W przypadku nowych instalacji skrypt należy uruchomić po utworzeniu standardowej bazy danych PostgreSQL z początkowym schematem/danymi (zobacz tworzenie bazy danych).

```
cat /usr/share/zabbix/sql-scripts/postgresql/timescaledb/schema.sql | sudo -u zabbix psql zabbix
```

> **Attention:**
> Zignoruj komunikaty ostrzegawcze informujące o nieprzestrzeganiu najlepszych praktyk podczas uruchamiania skryptu `schema.sql` w TimescaleDB w wersji 2.9.0 i nowszej. Niezależnie od tego ostrzeżenia konfiguracja zostanie ukończona pomyślnie.

Migracja istniejących danych historii, trendów i dziennika audytu może zająć dużo czasu. Na czas migracji serwer Zabbix i frontend muszą być wyłączone.

Skrypt `schema.sql` ustawia następujące parametry housekeeping:

- Zastąp okres przechowywania historii pozycji
- Zastąp okres przechowywania trendów pozycji

Aby używać partycjonowanego housekeeping dla historii i trendów, obie te opcje muszą być włączone. Możliwe jest również włączenie zastępowania indywidualnie tylko dla historii albo tylko dla trendów.

Dla PostgreSQL i TimescaleDB skrypt `postgresql/timescaledb/schema.sql` ustawia dwa dodatkowe parametry:

- Włącz kompresję
- Kompresuj rekordy starsze niż 7 dni

Aby housekeeper mógł pomyślnie usuwać skompresowane dane, muszą być włączone obie opcje: *Override item history period* oraz *Override item trend period*. Jeśli nadpisywanie jest wyłączone, a tabele zawierają skompresowane fragmenty, housekeeper nie będzie usuwał danych z tych tabel, a ostrzeżenia o nieprawidłowej konfiguracji będą wyświetlane w sekcjach *Housekeeping* oraz *System information*.

Wszystkie te parametry można zmienić w *Administracja* > *Housekeeping* po instalacji.

> **Note:**
> Możesz uruchomić narzędzie timescaledb-tune dostarczane przez TimescaleDB, aby zoptymalizować parametry konfiguracji PostgreSQL w pliku `postgresql.conf`.

Aktualizacja schematu TimescaleDB

Podczas aktualizacji Zabbix do wersji zawierającej nowe hypertabele TimescaleDB, serwer Zabbix nie konfiguruje automatycznie tych hypertabel (na przykład podczas aktualizacji z Zabbix 6.4 do 8.0, ponieważ wersje 7.0.0 i 7.0.2 wprowadziły nowe hypertabele).

Aby skonfigurować nowe hypertabele TimescaleDB, wykonaj następujące kroki:

1. Uruchom serwer Zabbix; spowoduje to aktualizację istniejącej bazy danych.
2. Sprawdź w pliku dziennika serwera, czy aktualizacja bazy danych została zakończona; po jej zakończeniu zatrzymaj serwer Zabbix. Zwróć uwagę, że serwer zapisuje ostrzeżenie, jeśli próbuje włączyć kompresję dla tabeli, która nie jest hypertabelą.

3. Uruchom skrypt `postgresql/timescaledb/schema.sql`; spowoduje to skonfigurowanie nowych hypertabel TimescaleDB. Zwróć uwagę, że od Zabbix 7.0.0 lokalizacja i nazwa skryptu zostały zmienione z `postgresql/timescaledb.sql` na `postgresql/timescaledb/schema.sql`.

Attention:
Zignoruj komunikaty ostrzegawcze informujące o nieprzestrzeganiu najlepszych praktyk podczas uruchamiania skryptu `schema.sql` w TimescaleDB w wersji 2.9.0 i nowszej. Niezależnie od tego ostrzeżenia konfiguracja zostanie pomyślnie zakończona.

Kompresja TimescaleDB

Natywna kompresja TimescaleDB jest obsługiwana dla wszystkich tabel Zabbix, które są hypertabelami TimescaleDB. Podczas aktualizacji lub migracji do TimescaleDB początkowa kompresja dużych tabel może zająć dużo czasu.

Należy pamiętać, że kompresja jest obsługiwana w ramach licencji Timescale Community "timescale", natomiast nie jest obsługiwana w ramach licencji Apache 2.0 "apache". Jeśli Zabbix wykryje, że kompresja nie jest obsługiwana, do logu serwera Zabbix zostanie zapisany komunikat ostrzegawczy, a użytkownicy nie będą mogli włączyć kompresji we frontendzie.

Note:
Przed użyciem kompresji zaleca się użytkownikom zapoznanie się z mechanizmem kompresji w dokumentacji TimescaleDB.

Należy pamiętać, że istnieją pewne ograniczenia wynikające z kompresji, w szczególności:

- Modyfikacje skompresowanych chunków (wstawianie, usuwanie, aktualizacje) nie są dozwolone
- Zmiany schematu dla skompresowanych tabel nie są dozwolone

Ustawienia kompresji można zmienić w bloku *History, trends and audit log compression* w sekcji *Administration* > *Housekeeping* frontendu Zabbix.

Parametr	Domyślnie	Uwagi
Enable compression	Włączone	Zaznaczenie lub odznaczenie pola wyboru nie aktywuje/dezaktywuje kompresji natychmiast. Ponieważ kompresja jest obsługiwana przez Housekeeper, zmiany zaczną obowiązywać maksymalnie po 2 × `HousekeepingFrequency` godzinach (ustawianych w zabbix_server.conf) Po wyłączeniu kompresji nowe chunki, które mieszczą się w okresie kompresji, nie będą kompresowane. Jednak wszystkie wcześniej skompresowane dane pozostaną skompresowane. Aby zdekompresować wcześniej skompresowane chunki, postępuj zgodnie z instrukcjami w dokumentacji TimescaleDB.
Compress records older than	7d	W przypadku aktualizacji ze starszych wersji Zabbix z obsługą TimescaleDB kompresja nie będzie domyślnie włączona. Ten parametr nie może być mniejszy niż 7 dni. Ze względu na niezmienność skompresowanych chunków wszystkie opóźnione dane (np. dane opóźnione przez proxy), które są starsze niż ta wartość, zostaną odrzucone.

Aby uzyskać lepszą wydajność aktualizacji trendów, można obniżyć wartość "chunk_time_interval" dla tabel `trends` i `trends_uint` z 30 dni do 7 dni lub mniej, w zależności od tego, ile pozycji korzysta z trendów. Celem tego ustawienia jest stosowanie się do najlepszych praktyk TimescaleDB oraz zapewnienie, że rozmiar chunków pozostaje w granicach zasobów dostępnych w systemie.

8 Konfiguracja Elasticsearch

Zabbix może przechowywać dane historii w Elasticsearch jako alternatywę dla relacyjnej bazy danych.

Attention:
Obsługa Elasticsearch jest obecnie eksperymentalna.

Ten przewodnik opisuje konfigurację dla Elasticsearch 7.X. Jeśli używasz innej wersji, część funkcji może nie działać zgodnie z oczekiwaniami.

Konfiguracja obejmuje utworzenie lokalizacji przechowywania Elasticsearch dla każdego typu wartości, skonfigurowanie preprocessing (jeśli jest potrzebny) oraz połączenie Zabbix z instancją Elasticsearch.

Elasticsearch może przechowywać następujące typy wartości:

Typ wartości pozycji	Tabela bazy danych	Typ Elasticsearch
Numeryczny (unsigned)	history_uint	uint
Numeryczny (float)	history	dbl
Znakowy	history_str	str
Log	history_log	log
Tekst	history_text	text
Binarny	history_bin	nieobsługiwany przez Zabbix
JSON	history_json	json

Ważne uwagi

- Elasticsearch wymaga libcurl. Szczegóły znajdują się w wymaganiach.
- Housekeeper nie usuwa danych z Elasticsearch.
- Jeśli wszystkie dane historii są przechowywane w Elasticsearch, trendy **nie** są obliczane ani przechowywane w bazie danych. Rozważ wydłużenie okresu przechowywania historii.
- Gdy używany jest Elasticsearch, zapytania zakresowe pobierające wartości z bazy danych są ograniczone znacznikiem czasu okresu przechowywania danych.
- Elasticsearch nie jest obsługiwany przez Zabbix proxy; zamiast tego użyj SQLite.

Jeśli Elasticsearch nie jest jeszcze zainstalowany, przed kontynuowaniem zapoznaj się z oficjalnym przewodnikiem instalacji.

Konfigurowanie Elasticsearch

Aby przechowywać dane historii w Elasticsearch, należy:

- Utworzyć indeks dla każdego typu wartości, który chcesz przechowywać — to tutaj Elasticsearch zapisuje dane, podobnie jak tabela w relacyjnej bazie danych.
- Zdefiniować mapowanie dla każdego indeksu — określa ono strukturę danych, podobnie jak schemat tabeli.
- Skonfigurować pipeline przetwarzania, aby przetwarzać wartości przed zapisaniem (wymagane dla wartości JSON i indeksów opartych na dacie).

Elasticsearch może przechowywać dane w jednym indeksie dla każdego typu wartości lub w wielu indeksach opartych na dacie. Oba podejścia opisano poniżej.

Przechowywanie historii w pojedynczym indeksie

W tym podejściu wszystkie dane historii dla danego typu wartości są zapisywane w jednym indeksie (np. `uint` lub `text`).

Aby utworzyć indeks dla typu wartości *Numeric (unsigned)*, wyślij następujące żądanie (z `/uint` w adresie URL) do swojej instancji Elasticsearch:

```
curl -X PUT \
 http://localhost:9200/uint \
 -H 'content-type:application/json' \
 -d '{
     "settings": {
      "index": {
         "number_of_replicas": 1,
         "number_of_shards": 5
      }
   },
   "mappings": {
      "properties": {
         "itemid": { "type": "long" },
         "clock": { "format": "epoch_second", "type": "date" },
         "value": { "type": "long" }
      }
   }
}'
```

Elasticsearch odpowie potwierdzeniem, że indeks został utworzony:

```
{"acknowledged": true, "shards_acknowledged": true, "index": "uint"}
```

Podobne żądania należy wysłać dla każdego dodatkowego typu wartości, który chcesz przechowywać w Elasticsearch.

> **Note:**
> Mapowania dla wszystkich typów wartości są dostępne w repozytorium źródłowym Zabbix.

Na przykład, aby utworzyć indeks dla typu wartości *Text*:

```
curl -X PUT \
 http://localhost:9200/text \
 -H 'content-type:application/json' \
 -d '{
   "settings": {
      "index": {
         "number_of_replicas": 1,
         "number_of_shards": 5
      }
   },
   "mappings": {
      "properties": {
         "itemid": { "type": "long" },
         "clock": { "format": "epoch_second", "type": "date" },
         "value": {
            "fields": {
               "analyzed": { "index": true, "type": "text", "analyzer": "standard" }
            },
            "index": false,
            "type": "text"
         }
      }
   }
}'
```

Typ wartości JSON

W przeciwieństwie do innych typów wartości, wartości JSON wymagają dodatkowego przetwarzania przed zapisaniem.

Poniższy indeks używa oddzielnych pól dla sparsowanych i surowych wartości, dlatego do sparsowania każdej wartości jako JSON i zapisania jej w odpowiednim polu potrzebny jest ingest pipeline.

Aby utworzyć indeks dla typu wartości *JSON*, wyślij następujące żądanie (z `/json` w adresie URL) do swojej instancji Elasticsearch.

```
curl -X PUT \
 http://localhost:9200/json \
 -H 'content-type:application/json' \
 -d '{
   "settings": {
      "number_of_shards": 5,
      "number_of_replicas": 1
   },
   "mappings": {
      "dynamic": false,
      "properties": {
         "itemid": { "type": "long" },
         "clock": { "type": "date", "format": "epoch_second" },
         "ns": { "type": "long" },
         "value_parsed": { "type": "flattened" },
         "value_raw": { "type": "keyword", "ignore_above": 1000000 }
    }
  }
}'
```

Następnie utwórz ingest pipeline:

```
curl -X PUT \
 http://localhost:9200/_ingest/pipeline/json \
 -H 'content-type:application/json' \
 -d '{
   "processors": [
      {
         "json": {
            "field": "value",
            "target_field": "value_parsed",
            "ignore_failure": true
         }
      },
      {
         "set": {
            "if": "ctx.value_parsed == null",
            "field": "value_raw",
            "value": "{{{ value }}}"
         }
      }
   ],
   "on_failure": [
      {
         "set": {
            "field": "value_raw",
            "value": "{{{ value }}}"
         }
      }
   ]
}'
```

Elasticsearch odpowie potwierdzeniem, że ingest pipeline został utworzony:

```
{"acknowledged": true}
```

Przechowywanie historii w indeksach opartych na dacie

Zamiast zapisywać wszystkie dane historii w jednym indeksie (np. `uint`), Elasticsearch może rozdzielać te dane pomiędzy wiele indeksów opartych na dacie (np. `uint-2026-01-01`, `uint-2026-01-02`). Ułatwia to zarządzanie ilością danych i okresem ich przechowywania w czasie.

Aby to włączyć, należy:

- Utworzyć szablon indeksu dla każdego typu wartości, który ma być przechowywany — informuje to Elasticsearch, jakie mapowanie zastosować podczas automatycznego tworzenia nowego indeksu opartego na dacie.
- Utworzyć pipeline ingest dla każdego typu wartości — przetwarza on każdą przychodzącą wartość i kieruje ją do właściwego indeksu opartego na dacie.
- Skonfigurować parametr `HistoryStorageDateIndex` w pliku konfiguracyjnym serwera Zabbix — umożliwia to przechowywanie wartości w wielu indeksach opartych na dacie.

Szablony indeksów

Aby utworzyć szablon dla indeksu `text`, wyślij żądanie z następującymi szczegółami:

- Użyj `_template/text_template` w adresie URL swojej instancji Elasticsearch.
- Użyj `"text*"` w polu `"index_patterns"`, aby dopasować nazwę indeksu.
- Użyj mapowania dla typu wartości `text` (zobacz mapowania w repozytorium źródłowym Zabbix).

```
curl -X PUT \
 http://localhost:9200/_template/text_template \
 -H 'content-type:application/json' \
 -d '{
   "index_patterns": [ "text*" ],
   "settings": {
      "index": {
         "number_of_replicas": 1,
         "number_of_shards": 5
      }
```

```
   },
   "mappings": {
      "properties": {
         "itemid": { "type": "long" },
         "clock": { "format": "epoch_second", "type": "date" },
         "value": {
            "fields": {
               "analyzed": { "index": true, "type": "text", "analyzer": "standard" }
            },
            "index": false,
            "type": "text"
         }
      }
   }
}'
```

Szablon dla indeksu `json`:

```
curl -X PUT \
 http://localhost:9200/_template/json_template \
 -H 'content-type:application/json' \
 -d '{
   "index_patterns": [ "json*" ],
   "settings": {
      "number_of_shards": 5,
      "number_of_replicas": 1
   },
   "mappings": {
      "dynamic": false,
      "properties": {
         "itemid": { "type": "long" },
         "clock": { "type": "date", "format": "epoch_second" },
         "ns": { "type": "long" },
         "value_parsed": { "type": "flattened" },
         "value_raw": { "type": "keyword", "ignore_above": 1000000 }
      }
   }
}'
```

Potoki ingest

Aby utworzyć potok ingest dla indeksu `text`:

- Użyj `_ingest/pipeline/text-pipeline` w adresie URL swojej instancji Elasticsearch.
- Dołącz procesor `date_index_name`, aby kierować każdą wartość do właściwego indeksu opartego na dacie na podstawie jej znacznika czasu.

```
curl -X PUT \
 http://localhost:9200/_ingest/pipeline/text-pipeline \
 -H 'content-type:application/json' \
 -d '{
   "description": "daily text index naming",
   "processors": [
      {
         "date_index_name": {
            "field": "clock",
            "date_formats": ["UNIX"],
            "index_name_prefix": "text-",
            "date_rounding": "d"
         }
      }
   ]
}'
```

W przypadku indeksu `json` potok musi również przeanalizować wartość JSON przed skierowaniem jej do właściwego indeksu:

```
curl -X PUT \
 http://localhost:9200/_ingest/pipeline/json-pipeline \
 -H 'content-type:application/json' \
 -d '{
   "description": "daily json index naming"
   "processors": [
      {
         "json": {
            "field": "value",
            "target_field": "value_parsed",
            "ignore_failure": true
         }
      },
      {
         "script": {
            "source": "if (ctx.value_parsed == null || !(ctx.value_parsed instanceof Map)) { ctx.value_raw
         }
      },
      {
         "date_index_name": {
            "field": "clock",
            "date_formats": [ "UNIX" ],
            "index_name_prefix": "json-",
            "date_rounding": "d"
         }
      }
   ]
}'
```

Konfigurowanie serwera Zabbix

W pliku konfiguracyjnym serwera Zabbix (`zabbix_server.conf`) ustaw następujące parametry:

- `HistoryStorageURL` — adres URL instancji Elasticsearch.
- `HistoryStorageTypes` — rozdzielona przecinkami lista typów wartości do przechowywania w Elasticsearch.

Na przykład, aby przechowywać w Elasticsearch wartości typu *Character*, *Log*, *Text* i *JSON* (przy jednoczesnym pozostawieniu wartości *Numeric* w bazie danych):

```
HistoryStorageURL=http://localhost:9200
HistoryStorageTypes=str,log,text,json
```

Jeśli używasz indeksów opartych na dacie dla **wszystkich** wartości przechowywanych w Elasticsearch, ustaw również parametr `HistoryStorageDateIndex`:

```
HistoryStorageDateIndex=1
```

Po wprowadzeniu zmian uruchom ponownie serwer Zabbix:

```
systemctl restart zabbix-server
```

Konfigurowanie frontendu Zabbix

W pliku konfiguracyjnym frontendu Zabbix (`zabbix.conf.php`) zadeklaruj `$HISTORY` jako zmienną globalną i ustaw wartości `url` oraz `types` tak, aby odpowiadały konfiguracji serwera:

```
// Zabbix GUI configuration file.
global $DB, $HISTORY;

$HISTORY['url']   = 'http://localhost:9200';
$HISTORY['types'] = ['str', 'log', 'text', 'json'];
```

Rozwiązywanie problemów

Poniższe kroki mogą pomóc w rozwiązywaniu problemów z konfiguracją Elasticsearch:

1. Sprawdź, czy `auto_create_index` jest włączone:

```
curl -X GET \
 "http://localhost:9200/_cluster/settings?include_defaults=true&filter_path=**.auto_create_index"

#### {"defaults": {"action": {"auto_create_index": "false"} } }
```

Aby je włączyć, wyślij następujące żądanie:

```
curl -X PUT \
 http://localhost:9200/_cluster/settings \
 -H 'content-type:application/json' \
 -d '{
   "persistent": {
      "action.auto_create_index": "true"
   }
}'

#### {"acknowledged": true, "persistent": {"action": {"auto_create_index": "true"} }, "transient": {} }
```

2. Sprawdź, czy mapowania, szablony i potoki ingest są poprawne, wysyłając żądania GET do odpowiednich adresów URL:

```
curl -X GET http://localhost:9200/json
curl -X GET http://localhost:9200/_template/json*
curl -X GET http://localhost:9200/_ingest/pipeline/json*
```

Możesz porównać otrzymane odpowiedzi z oczekiwanymi odpowiedziami w dokumentacji API Elasticsearch.

3. Sprawdź, czy jakiekolwiek shardy są w stanie awarii; ponowne uruchomienie Elasticsearch może rozwiązać ten problem.
4. Sprawdź, czy konfiguracja Elasticsearch zezwala na dostęp z serwera Zabbix i frontendu Zabbix.
5. Użyj parametru konfiguracyjnego serwera Zabbix `LogSlowQueries`, aby zidentyfikować wolne zapytania.
6. Sprawdź logi Elasticsearch pod kątem błędów.
7. Jeśli musisz zresetować konfigurację Elasticsearch i zacząć od nowa, możesz usunąć wszystkie indeksy, szablony i potoki ingest:

```
curl -X DELETE "http://localhost:9200/_all"
curl -X DELETE "http://localhost:9200/_template/*"
curl -X DELETE "http://localhost:9200/_ingest/pipeline/*"
```

9 Uwagi dotyczące konfiguracji Nginx dla Zabbix w zależności od dystrybucji

RHEL

W systemach RHEL 8, 9 i 10 Nginx jest dostępny w AppStream — nie są potrzebne żadne dodatkowe repozytoria. Wystarczy włączyć i zainstalować go za pomocą:

```
dnf module list nginx
dnf -y install nginx
```

W systemie RHEL 7 Nginx można zainstalować z repozytorium CentOS 7 Extras (w przypadku korzystania z CentOS) za pomocą:

```
yum -y install nginx
```

Jeśli preferujesz najnowsze kompilacje z oficjalnego źródła, skonfiguruj oficjalne repozytorium NGINX w `/etc/yum.repos.d/nginx.repo`:

```
cat > /etc/yum.repos.d/nginx.repo << 'EOF'
[nginx-stable]
name=nginx stable repo
baseurl=https://nginx.org/packages/rhel/$releasever/$basearch/
gpgcheck=1
enabled=1
gpgkey=https://nginx.org/keys/nginx_signing.key
EOF
dnf -y install nginx
```

SLES 15

W SUSE Linux Enterprise Server 15 należy skonfigurować php-fpm (ścieżka do pliku konfiguracyjnego może się nieznacznie różnić w zależności od dodatku Service Pack):

```
cp /etc/php8/fpm/php-fpm.conf{.default,}
cp /etc/php8/fpm/php-fpm.d/www.conf{.default,}
sed -i 's/user = nobody/user = wwwrun/; s/group = nobody/group = www/' /etc/php8/fpm/php-fpm.d/www.conf
```

10 Uruchamianie agent jako root

Od wersji Zabbix **5.0.0** plik usługi systemd dla Zabbix agent w oficjalnych pakietach jawnie zawiera dyrektywy `User` i `Group`. Obie są ustawione na `zabbix`.

Nie ma już możliwości skonfigurowania, jako który użytkownik działa Zabbix agent, za pomocą pliku `zabbix_agentd.conf`, ponieważ agent pominie tę konfigurację i uruchomi się jako użytkownik określony w pliku usługi systemd. Aby uruchomić Zabbix agent jako root, należy wprowadzić modyfikacje opisane poniżej.

Zabbix agent

Aby zastąpić domyślnego użytkownika i grupę dla Zabbix agent, uruchom:

```
systemctl edit zabbix-agent
```

Następnie dodaj następującą zawartość:

```
[Service]
User=root
Group=root
```

Przeładuj daemony i uruchom ponownie usługę zabbix-agent:

```
systemctl daemon-reload
systemctl restart zabbix-agent
```

W przypadku **Zabbix agent** spowoduje to ponowne włączenie funkcji konfigurowania użytkownika w pliku `zabbix_agentd.conf`. Teraz należy ustawić parametry konfiguracyjne `User=root` i `AllowRoot=1` w pliku konfiguracyjnym agent.

Zabbix agent 2

Aby zastąpić domyślnego użytkownika i grupę dla Zabbix agent 2, uruchom:

```
systemctl edit zabbix-agent2
```

Następnie dodaj następującą zawartość:

```
[Service]
User=root
Group=root
```

Przeładuj demony i uruchom ponownie usługę zabbix-agent2:

```
systemctl daemon-reload
systemctl restart zabbix-agent2
```

W przypadku **Zabbix agent2** to całkowicie określa użytkownika, jako który jest uruchamiany. Nie są wymagane żadne dodatkowe modyfikacje.

11 Zabbix agent w systemie Microsoft Windows

Konfigurowanie agent

Obie generacje agentów Zabbix działają jako usługa systemu Windows. W przypadku Zabbix agent 2 w poniższych instrukcjach należy zastąpić *agentd* przez *agent2*.

Można uruchomić pojedynczą instancję agent Zabbix lub wiele instancji agent na hoście Microsoft Windows. Pojedyncza instancja może używać:

- domyślnego pliku konfiguracyjnego znajdującego się w tym samym katalogu co plik binarny agent;
- pliku konfiguracyjnego określonego w wierszu poleceń.

W przypadku wielu instancji każda instancja agent musi mieć własny plik konfiguracyjny (jedna z instancji może używać domyślnego pliku konfiguracyjnego).

Przykładowy plik konfiguracyjny jest dostępny w archiwum źródłowym Zabbix jako:

- `conf/zabbix_agentd.conf` dla Zabbix agent;
- `conf/zabbix_agent2.conf` dla Zabbix agent2.

Jeśli chcesz zainstalować Zabbix agent/agent 2 dla systemu Windows jako usługę z archiwum bez jawnego określania pliku konfiguracyjnego, to przed instalacją agent:

- `conf/zabbix_agentd.conf` należy ręcznie skopiować do katalogu, w którym zostanie zainstalowany plik zabbix_agentd.exe;
- `conf/zabbix_agent2.conf` oraz katalog `conf/zabbix_agent2.d` należy ręcznie skopiować do katalogu, w którym zostanie zainstalowany plik zabbix_agent2.exe.

Szczegółowe informacje na temat konfiguracji agenta Zabbix dla systemu Windows można znaleźć w opcjach pliku konfiguracyjnego.

Parametr Hostname

Aby wykonywać aktywne kontrole na hoście, agent Zabbix musi mieć zdefiniowaną nazwę hosta. Ponadto wartość nazwy hosta ustawiona po stronie agenta powinna dokładnie odpowiadać wartości „Host name" skonfigurowanej dla hosta we frontendzie.

Wartość nazwy hosta po stronie agenta można zdefiniować za pomocą parametru **Hostname** lub **HostnameItem** w pliku konfiguracyjnym agenta — albo zostaną użyte wartości domyślne, jeśli którykolwiek z tych parametrów nie zostanie określony.

Domyślną wartością parametru **HostnameItem** jest wartość zwracana przez klucz agenta „system.hostname". W systemie Windows zwraca on wynik funkcji gethostname(), która odpytuje dostawców przestrzeni nazw w celu określenia lokalnej nazwy hosta. Jeśli żaden dostawca przestrzeni nazw nie odpowie, zwracana jest nazwa NetBIOS.

Domyślną wartością parametru **Hostname** jest wartość zwracana przez parametr HostnameItem. W praktyce oznacza to, że jeśli oba te parametry nie są określone, rzeczywistą nazwą hosta będzie nazwa NetBIOS hosta; agent Zabbix użyje nazwy hosta NetBIOS do pobrania listy aktywnych kontroli z serwera Zabbix i wysłania do niego wyników.

Klucz „system.hostname" obsługuje dwa opcjonalne parametry — *type* i *transform*.

Type określa typ nazwy, którą pozycja ma zwracać:

- *netbios* (domyślnie) — zwraca nazwę hosta NetBIOS, która jest ograniczona do 15 znaków i zawiera wyłącznie WIELKIE LITERY;
- *host* — z uwzględnieniem wielkości liter, zwraca pełną, rzeczywistą nazwę hosta Windows (bez domeny);
- *shorthost* — zwraca część nazwy hosta przed pierwszą kropką. Zwróci pełny ciąg, jeśli nazwa nie zawiera kropki.
- *fqdn* — zwraca w pełni kwalifikowaną nazwę domenową (bez końcowej kropki).

Transform pozwala określić dodatkową regułę przekształcenia nazwy hosta:

- *none* (domyślnie) — użyj oryginalnej wielkości liter;
- *lower* — zamień tekst na małe litery.

Aby więc uprościć konfigurację pliku zabbix_agentd.conf i ją ujednolicić, można zastosować trzy różne podejścia:

1. Pozostawić parametry **Hostname** lub **HostnameItem** niezdefiniowane, a agent Zabbix użyje nazwy hosta NetBIOS jako nazwy hosta.
2. Pozostawić parametr **Hostname** niezdefiniowany i zdefiniować **HostnameItem** w następujący sposób:
   HostnameItem=system.hostname[host] — aby agent Zabbix używał pełnej, rzeczywistej (z uwzględnieniem wielkości liter) nazwy hosta Windows jako nazwy hosta
   HostnameItem=system.hostname[shorthost,lower] — aby agent Zabbix używał tylko części nazwy hosta przed pierwszą kropką, zamienionej na małe litery.
   HostnameItem=system.hostname[fqdn] — aby agent Zabbix używał w pełni kwalifikowanej nazwy domenowej jako nazwy hosta.

Nazwa hosta jest również używana jako część nazwy usługi Windows, która służy do instalowania, uruchamiania, zatrzymywania i odinstalowywania usługi Windows. Na przykład, jeśli plik konfiguracyjny agenta Zabbix zawiera `Hostname=Windows_db_server`, agent zostanie zainstalowany jako usługa Windows „`Zabbix Agent [Windows_db_server]`". Dlatego aby każda instancja agenta Zabbix miała inną nazwę usługi Windows, każda instancja musi używać innej nazwy hosta.

Instalacja agent jako usługi Windows

Przed zainstalowaniem agent skopiuj ręcznie plik `conf/zabbix_agentd.conf` do katalogu, w którym zostanie zainstalowany plik zabbix_agentd.exe.

Aby zainstalować pojedynczą instancję Zabbix agent z domyślnym plikiem konfiguracyjnym:

```
zabbix_agentd.exe --install
```

Attention:
W systemie 64-bitowym wymagana jest 64-bitowa wersja Zabbix agent, aby wszystkie kontrole związane z uruchomionymi procesami 64-bitowymi działały prawidłowo.

Jeśli chcesz użyć pliku konfiguracyjnego innego niż domyślny, powinieneś użyć następującego polecenia do instalacji usługi:

```
zabbix_agentd.exe --config <your_configuration_file> --install
```

Należy podać pełną ścieżkę do pliku konfiguracyjnego.

Wiele instancji Zabbix agent można zainstalować jako usługi w następujący sposób:

```
zabbix_agentd.exe --config <configuration_file_for_instance_1> --install --multiple-agents
zabbix_agentd.exe --config <configuration_file_for_instance_2> --install --multiple-agents
...
zabbix_agentd.exe --config <configuration_file_for_instance_N> --install --multiple-agents
```

Zainstalowana usługa powinna być teraz widoczna w Panelu sterowania.

Uruchamianie agent

Aby uruchomić usługę agent, możesz użyć Panelu sterowania lub zrobić to z wiersza poleceń.

Aby uruchomić pojedynczą instancję Zabbix agent z domyślnym plikiem konfiguracyjnym:

```
zabbix_agentd.exe --start
```

Aby uruchomić pojedynczą instancję Zabbix agent z innym plikiem konfiguracyjnym:

```
zabbix_agentd.exe --config <your_configuration_file> --start
```

Aby uruchomić jedną z wielu instancji Zabbix agent:

```
zabbix_agentd.exe --config <configuration_file_for_this_instance> --start --multiple-agents
```

Zatrzymywanie agent

Aby zatrzymać usługę agent, możesz użyć Panelu sterowania lub zrobić to z wiersza poleceń.

Aby zatrzymać pojedynczą instancję Zabbix agent uruchomioną z domyślnym plikiem konfiguracyjnym:

```
zabbix_agentd.exe --stop
```

Aby zatrzymać pojedynczą instancję Zabbix agent uruchomioną z innym plikiem konfiguracyjnym:

```
zabbix_agentd.exe --config <your_configuration_file> --stop
```

Aby zatrzymać jedną z wielu instancji Zabbix agent:

```
zabbix_agentd.exe --config <configuration_file_for_this_instance> --stop --multiple-agents
```

Odinstalowywanie usługi agenta Windows

Aby odinstalować pojedynczą instancję Zabbix agent przy użyciu domyślnego pliku konfiguracyjnego:

```
zabbix_agentd.exe --uninstall
```

Aby odinstalować pojedynczą instancję Zabbix agent przy użyciu niedomyślnego pliku konfiguracyjnego:

```
zabbix_agentd.exe --config <your_configuration_file> --uninstall
```

Aby odinstalować wiele instancji Zabbix agent z usług Windows:

```
zabbix_agentd.exe --config <configuration_file_for_instance_1> --uninstall --multiple-agents
zabbix_agentd.exe --config <configuration_file_for_instance_2> --uninstall --multiple-agents
...
zabbix_agentd.exe --config <configuration_file_for_instance_N> --uninstall --multiple-agents
```

Ograniczenia

Zabbix agent dla systemu Windows nie obsługuje niestandardowych konfiguracji systemu Windows, w których procesory CPU są rozmieszczone nierównomiernie pomiędzy węzłami NUMA. Jeśli logiczne procesory CPU są rozmieszczone nierównomiernie, metryki wydajności CPU mogą nie być dostępne dla niektórych procesorów CPU. Na przykład, jeśli istnieją 72 logiczne procesory CPU i 2 węzły NUMA, oba węzły muszą mieć po 36 procesorów CPU.

12 Konfiguracja SAML z Microsoft Entra ID

Przegląd

Ta sekcja zawiera wytyczne dotyczące konfigurowania logowania jednokrotnego i konfiguracja kont użytkowników w Zabbix z Microsoft Entra ID (dawniej Microsoft Azure Active Directory) przy użyciu uwierzytelniania SAML 2.0.

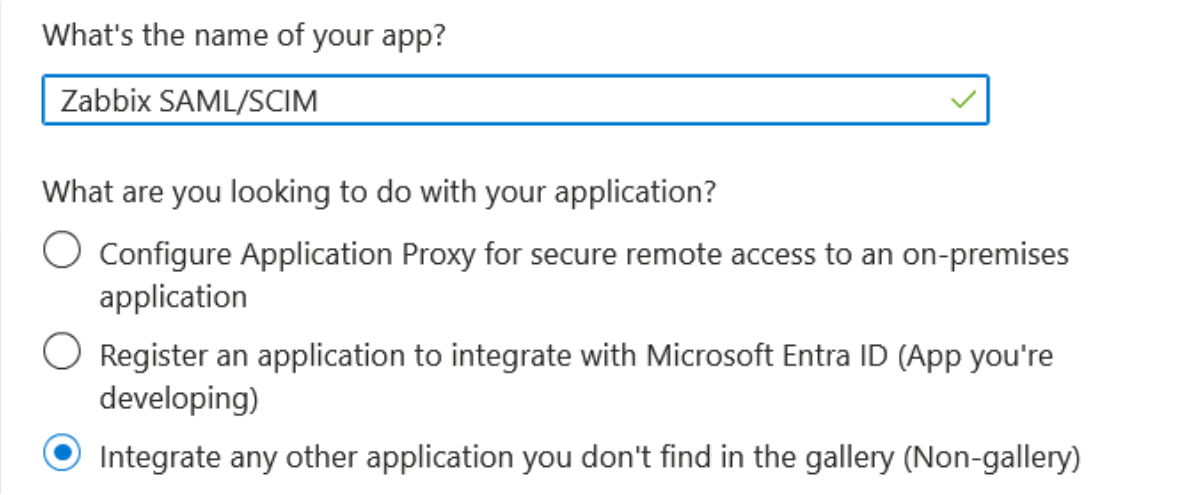
Konfiguracja ID Microsoft Entra

Tworzenie aplikacji

1. Zaloguj się do centrum administracyjnego Microsoft Entra pod adresem Microsoft Entra ID. Do celów testowych możesz utworzyć bezpłatne konto próbne w Microsoft Entra ID.

2. W centrum administracyjnym Microsoft Entra wybierz *Applications -> Enterprise applications -> New application -> Create your own application*.

3. Dodaj nazwę swojej aplikacji i wybierz opcję *Integrate any other application...*. Następnie kliknij *Create*.

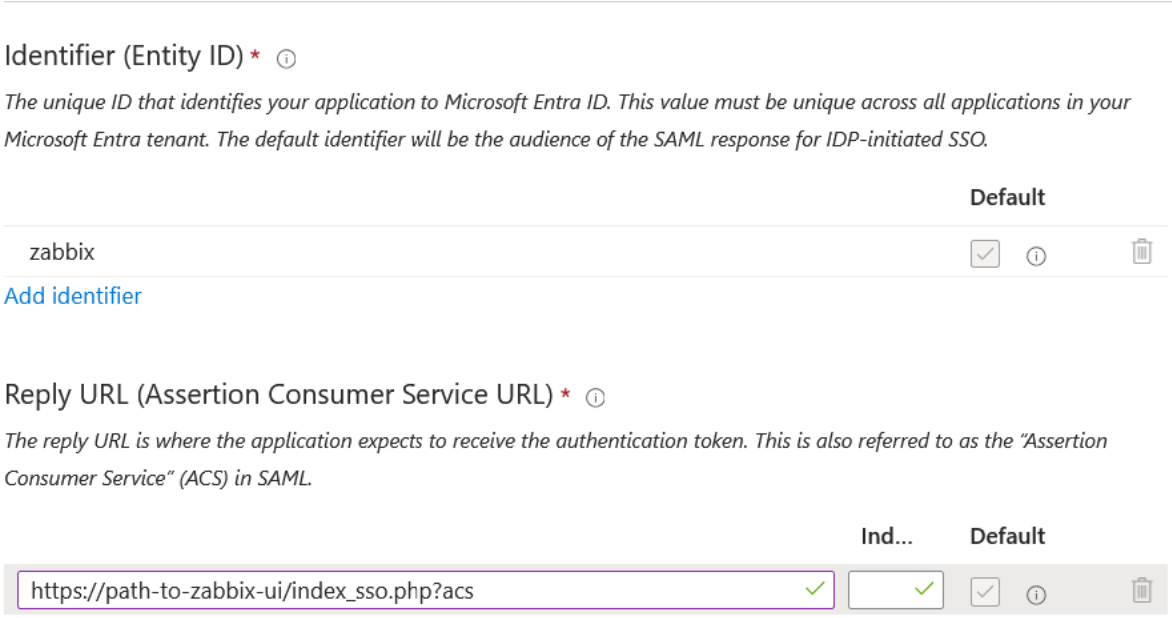


Konfigurowanie logowania jednokrotnego

1. Na stronie swojej aplikacji przejdź do *Set up single sign on* i kliknij *Get started*. Następnie wybierz *SAML*.

2. Edytuj *Basic SAML Configuration*:

- W polu *Identifier (Entity ID)* ustaw unikalną nazwę identyfikującą aplikację w Microsoft Entra ID, na przykład `zabbix`;
- W polu *Reply URL (Assertion Consumer Service URL)* ustaw punkt końcowy logowania jednokrotnego Zabbix: `https://<path-to-zabb`



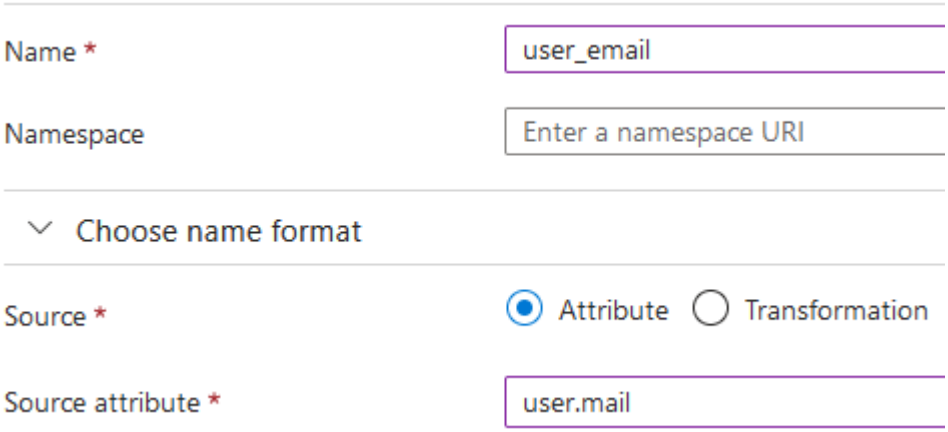
Zwróć uwagę, że wymagany jest protokół „https". Aby to działało z Zabbix, należy dodać do `conf/zabbix.conf.php` następujący wiersz:

```
$SSO['SETTINGS'] = ['use_proxy_headers' => true];
```

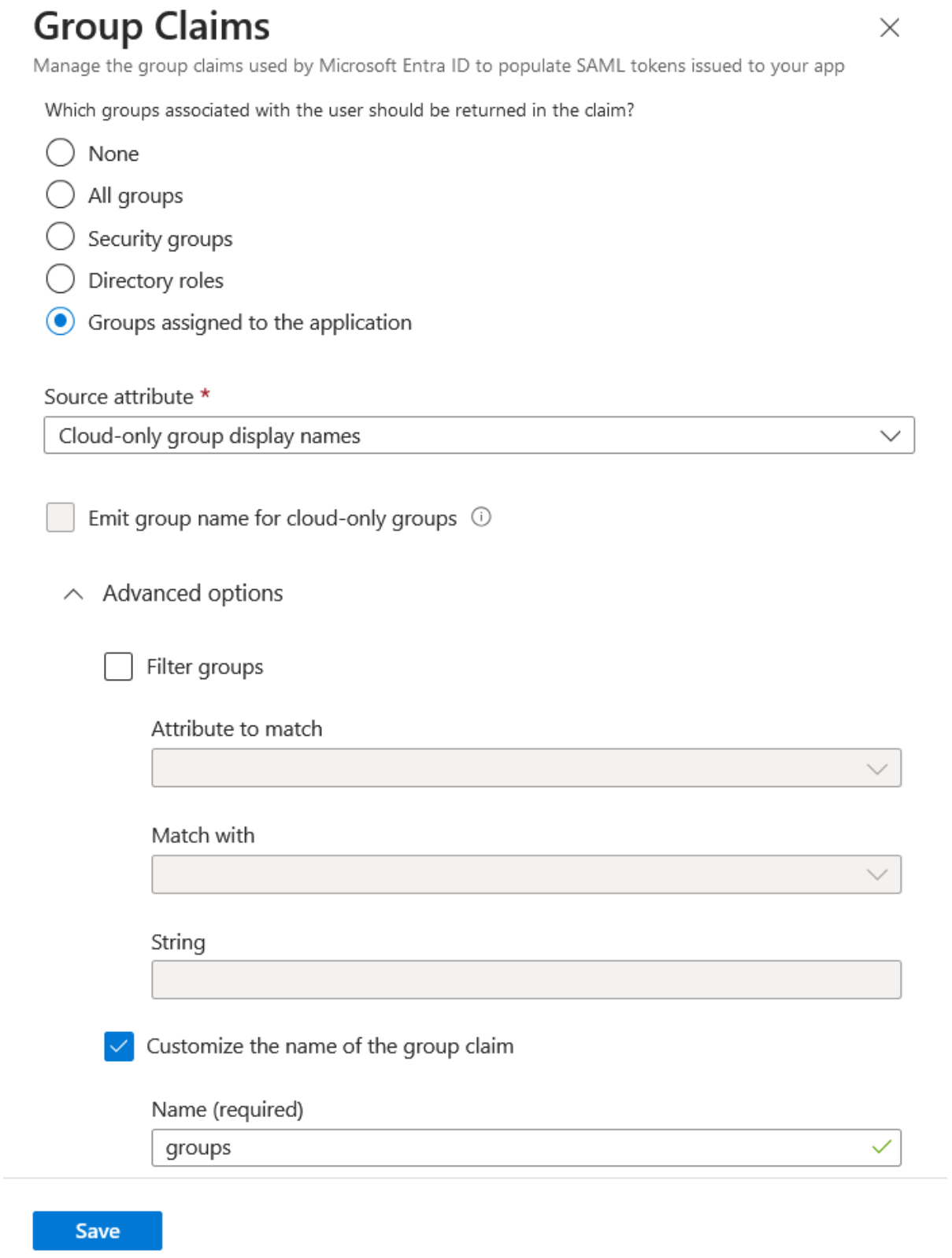
3. Edytuj *Attributes & Claims*. Musisz dodać wszystkie atrybuty, które chcesz przekazywać do Zabbix (user_name, user_lastname, user_email, user_mobile, groups).

Nazwy atrybutów są dowolne. Można używać różnych nazw atrybutów, jednak muszą one odpowiadać wartościom odpowiednich pól w ustawieniach Zabbix SAML.

- Kliknij *Add new claim*, aby dodać atrybut:



- Kliknij *Add a group claim*, aby dodać atrybut do przekazywania grup do Zabbix:



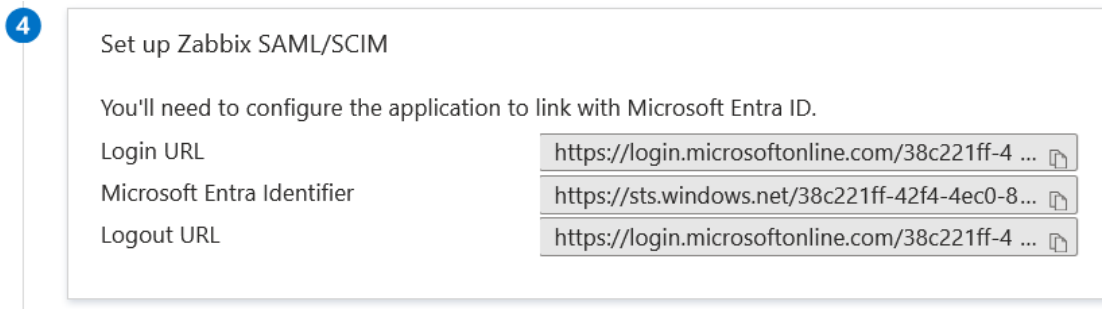
W tym claim ważne jest, aby do Zabbix były przekazywane nazwy grup (a nie identyfikatory grup) za pomocą wybranego *Source attribute*. W przeciwnym razie automatyczne provisionowanie użytkowników JIT nie będzie działać prawidłowo.

4. W sekcji *SAML Certificates* pobierz certyfikat Base64 udostępniony przez Entra ID i umieść go w `conf/certs` instalacji frontend Zabbix.

Ustaw dla niego uprawnienia 644, uruchamiając:

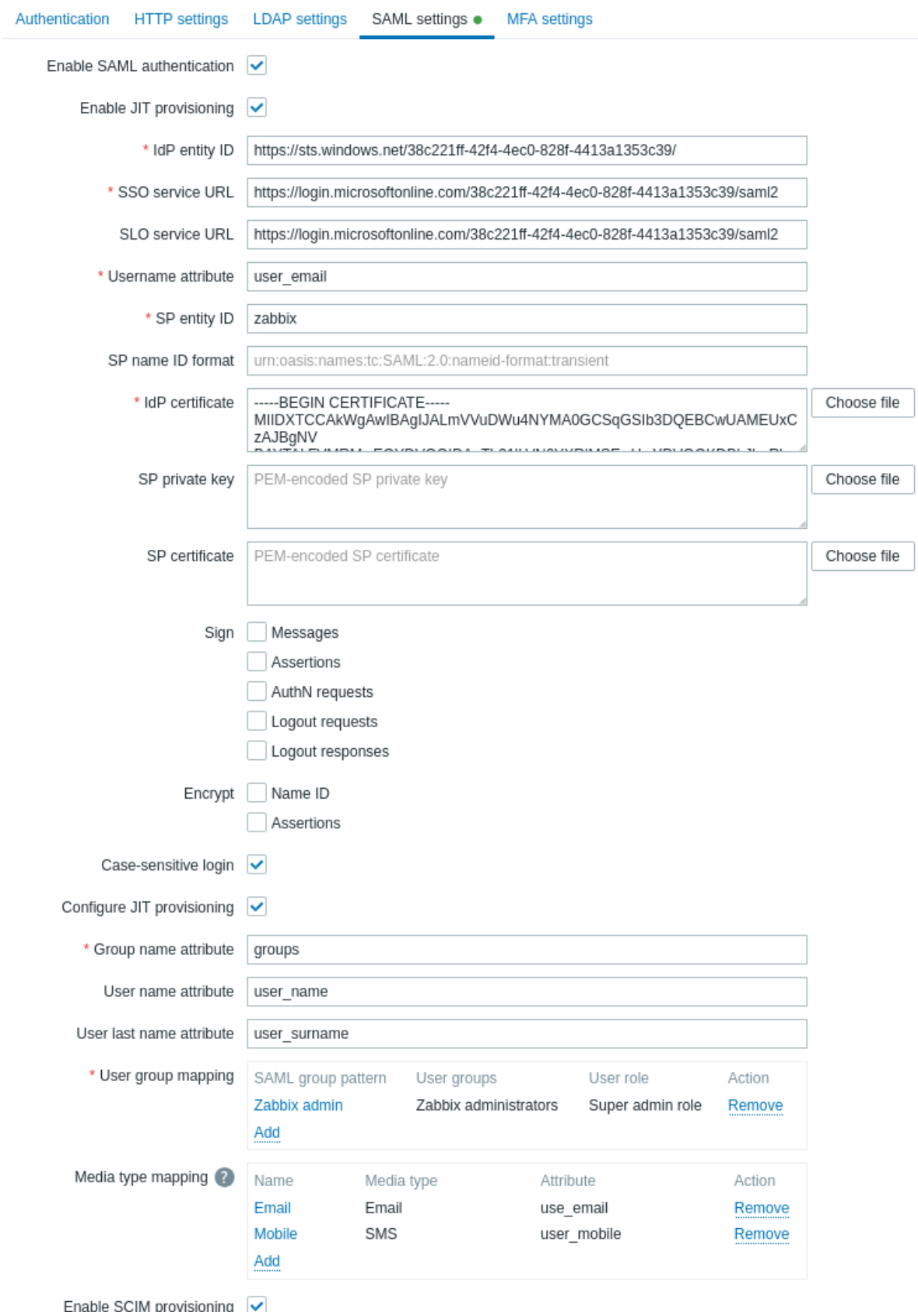
```
chmod 644 entra.cer
```

5. Użyj wartości z *Set up <your app name>* w Entra ID, aby skonfigurować uwierzytelnianie Zabbix SAML (zobacz następną sekcję):



Konfiguracja Zabbix

1. W Zabbix przejdź do ustawień SAML i wypełnij opcje konfiguracji na podstawie konfiguracji Entra ID:



Pole Zabbix	Pole konfiguracji w Entra ID	Przykładowa wartość
IdP entity ID	Identyfikator Microsoft Entra	
SSO service URL	Adres URL logowania	
SLO service URL	Adres URL wylogowania	
SP entity ID	Identyfikator (Entity ID)	
Username attribute	Atrybut niestandardowy (claim)	`user_email`
Group name attribute	Atrybut niestandardowy (claim)	`groups`
User name attribute	Atrybut niestandardowy (claim)	`user_name`

Pole Zabbix	Pole konfiguracji w Entra ID	Przykładowa wartość
User last name attribute	Atrybut niestandardowy (claim)	`user_lastname`

2. Dodaj certyfikat Base64 dostarczony przez Entra ID.

Jeśli w zabbix.conf.php ustawiono `$SSO['CERT_STORAGE'] = 'database'`, możesz wkleić treść certyfikatu lub przesłać plik certyfikatu we frontend podczas konfiguracji SAML — żadne pliki nie są wymagane w systemie plików.

Jeśli w zabbix.conf.php ustawiono `$SSO['CERT_STORAGE'] = 'file'`, certyfikat musi być dostępny w systemie plików (domyślnie w ui/conf/certs lub w ścieżce skonfigurowanej w zabbix.conf.php), a frontend nie będzie przechowywać certyfikatów w bazie danych. Pamiętaj, że jeśli `$SSO['CERT_STORAGE']` nie jest ustawione lub jest zakomentowane, zakładane jest przechowywanie w plikach, a certyfikaty są odczytywane z ui/conf/certs.

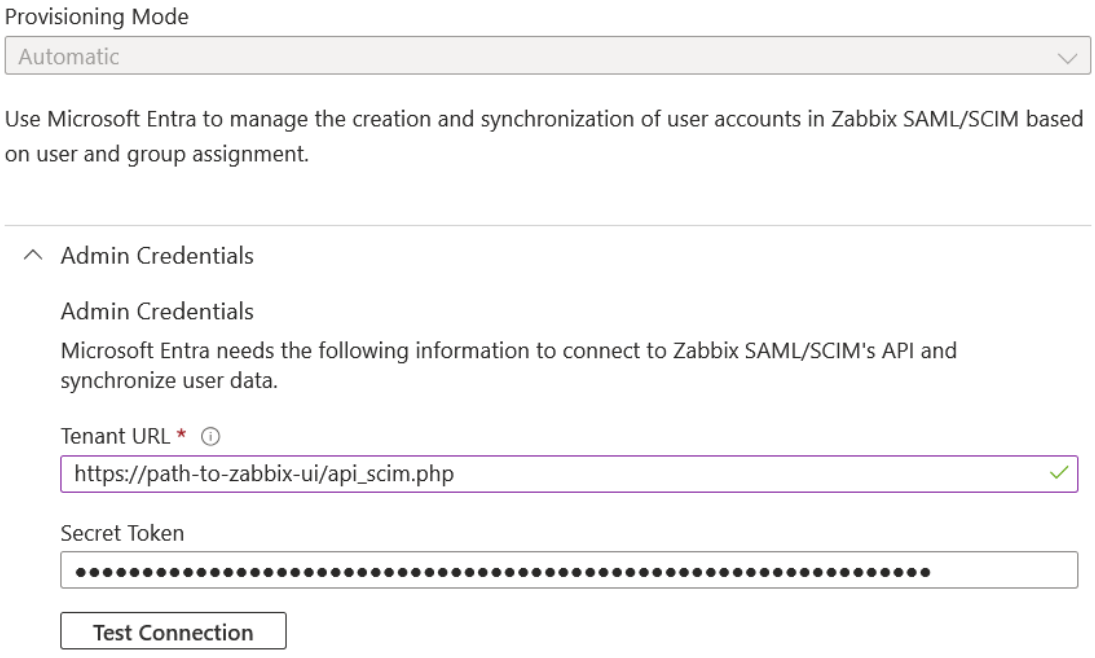
Wymagane jest również skonfigurowanie mapowania grup użytkowników. Mapowanie mediów jest opcjonalne.

3. Naciśnij przycisk *Update*, aby zapisać te ustawienia.

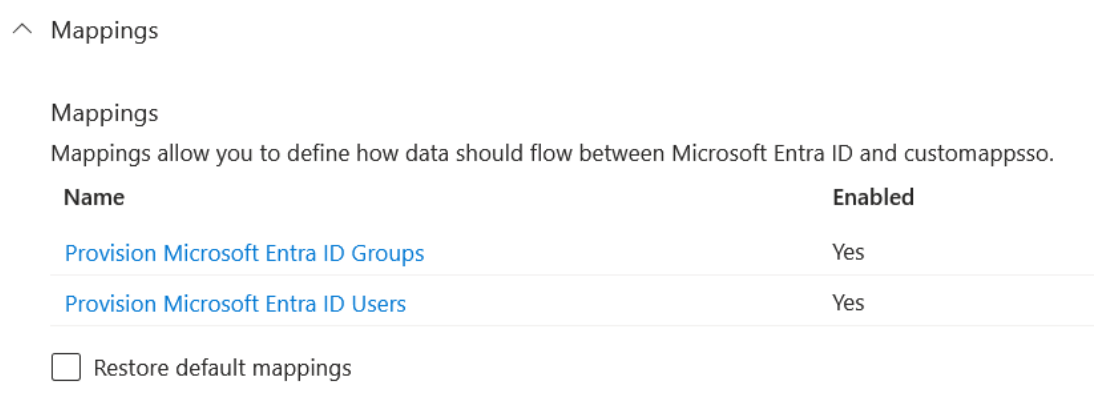
Provisioning użytkowników SCIM

1. Na stronie aplikacji Entra ID, z menu głównego otwórz stronę Provisioning. Kliknij *Get started*, a następnie wybierz tryb automatycznego provisioningu:

- W polu *Tenant URL* ustaw następującą wartość: `https://<path-to-zabbix-ui>/api_scim.php`
- W polu *Secret token* wprowadź token API Zabbix z uprawnieniami Super admin.
- Kliknij *Test connection*, aby sprawdzić, czy połączenie zostało nawiązane.

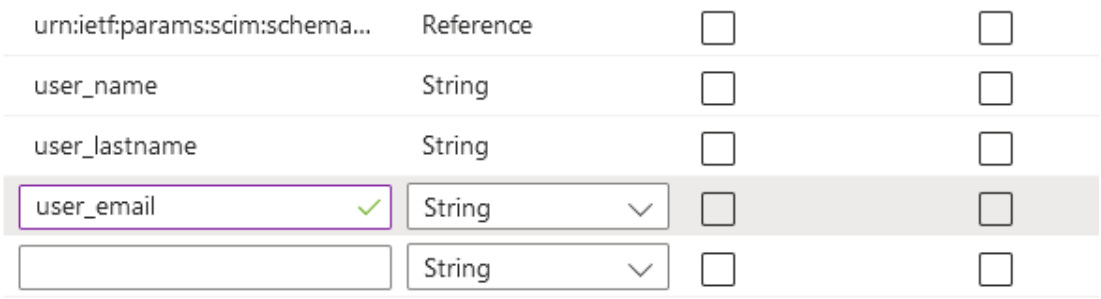


2. Teraz możesz dodać wszystkie atrybuty, które będą przekazywane do Zabbix za pomocą SCIM. Aby to zrobić, kliknij *Mappings*, a następnie *Provision Microsoft Entra ID Users*.



Na dole listy Attribute Mapping włącz opcję *Show advanced options*, a następnie kliknij *Edit attribute list for customappsso*.

Na dole listy atrybutów dodaj własne atrybuty typu ’String’:



Zapisz listę.

3. Teraz możesz dodać mapowania dla dodanych atrybutów. Na dole listy Attribute Mapping kliknij *Add New Mapping* i utwórz mapowania, jak pokazano poniżej:



Po dodaniu wszystkich mapowań zapisz listę mapowań.



4. Warunkiem wstępnym provisioningu użytkowników do Zabbix jest skonfigurowanie użytkowników i grup w Entra ID.

Aby to zrobić, przejdź do *Microsoft Entra admin center*, a następnie dodaj użytkowników/grupy na odpowiednich stronach Users i Groups.

5. Po utworzeniu użytkowników i grup w Entra ID możesz przejść do menu *Users and groups* swojej aplikacji i dodać je do aplikacji.

6. Przejdź do menu *Provisioning* swojej aplikacji i kliknij *Start provisioning*, aby użytkownicy zostali provisionowani do Zabbix.

Pamiętaj, że żądanie PATCH dla Users w Entra ID nie obsługuje zmian w mediach.

Podpisywanie żądań uwierzytelniania

Można skonfigurować Entra ID tak, aby weryfikował podpis podpisanych żądań uwierzytelniania.

Aby to działało, utwórz klucze publiczny/prywatny:

```
openssl req -x509 -newkey rsa:4096 -keyout /usr/share/zabbix/conf/certs/request-sign.key -out /usr/share/z
```

Przypisz uprawnienia:

```
chown apache /usr/share/zabbix/conf/certs/request-sign.key
chmod 400 /usr/share/zabbix/conf/certs/request-sign.key
```

Zaktualizuj konfigurację frontendu Zabbix, dodając:

```
$SSO['SP_KEY'] = 'conf/certs/request-sign.key';
$SSO['SP_CERT'] = 'conf/certs/request-sign.crt';
```

Rozwiązywanie problemów

Problemy z uwierzytelnianiem mogą wystąpić w przeglądarkach MicroSoft Edge, gdy użytkownik próbujący zalogować się do Zabbix przez SAML jest już zalogowany przy użyciu profilu MicroSoft Edge. Oznaką takiego problemu może być możliwość zalogowania się do Zabbix przy użyciu MicroSoft Edge w trybie prywatnym.

Aby uniknąć problemów z uwierzytelnianiem w takim przypadku, może być konieczne ustawienie parametru `requestedAuthnContext` na "false" w pliku konfiguracyjnym frontendu Zabbix (*zabbix.conf.php*).

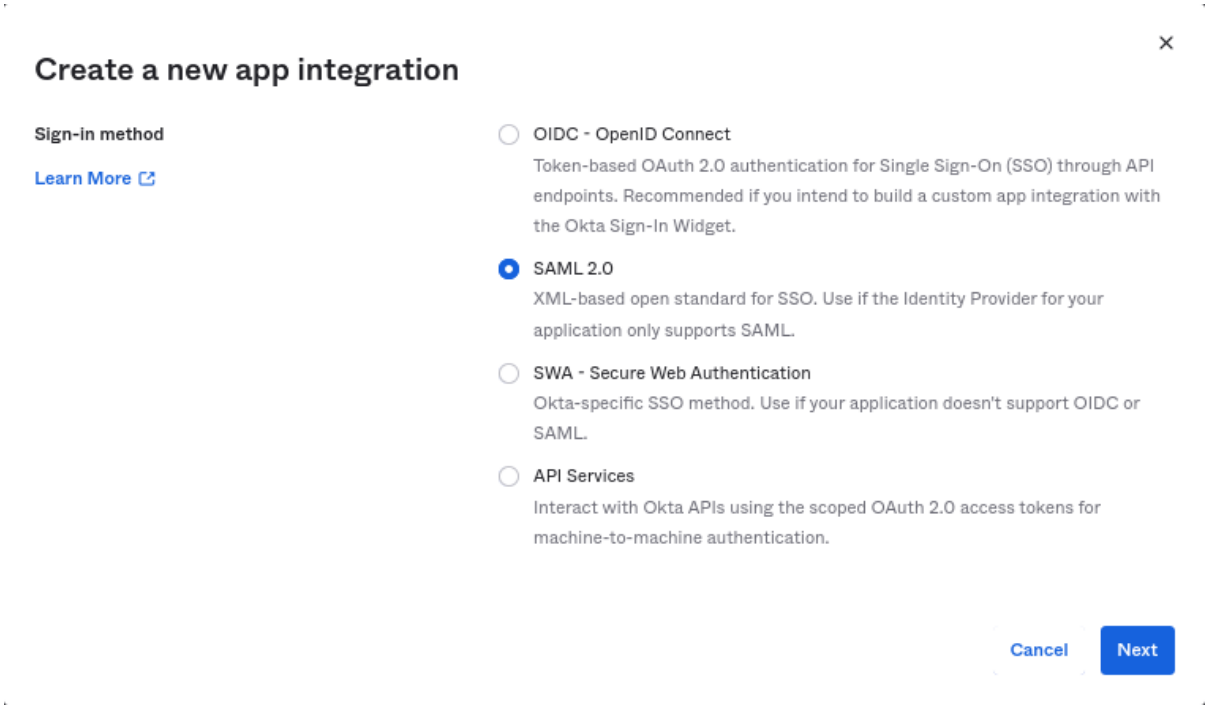
```
$SSO['SETTINGS'] = [
    'security' => [
        'requestedAuthnContext' => false
    ]
];
```

13 Konfiguracja SAML z Okta

Ta sekcja zawiera wskazówki dotyczące konfiguracji Okta w celu włączenia uwierzytelniania SAML 2.0 oraz provisioningu użytkowników dla Zabbix.

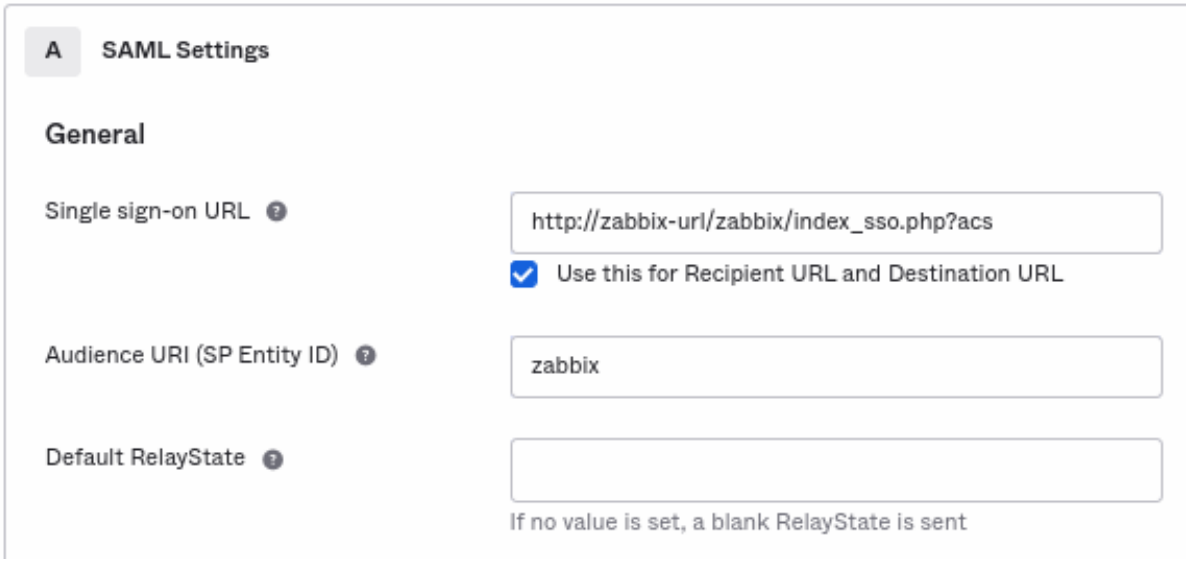
Konfiguracja Okta

1. Przejdź do https://developer.okta.com/signup/ i zarejestruj się/zaloguj na swoje konto.
2. W interfejsie webowym Okta przejdź do *Applications* → *Applications*.
3. Kliknij *Create App Integration*.

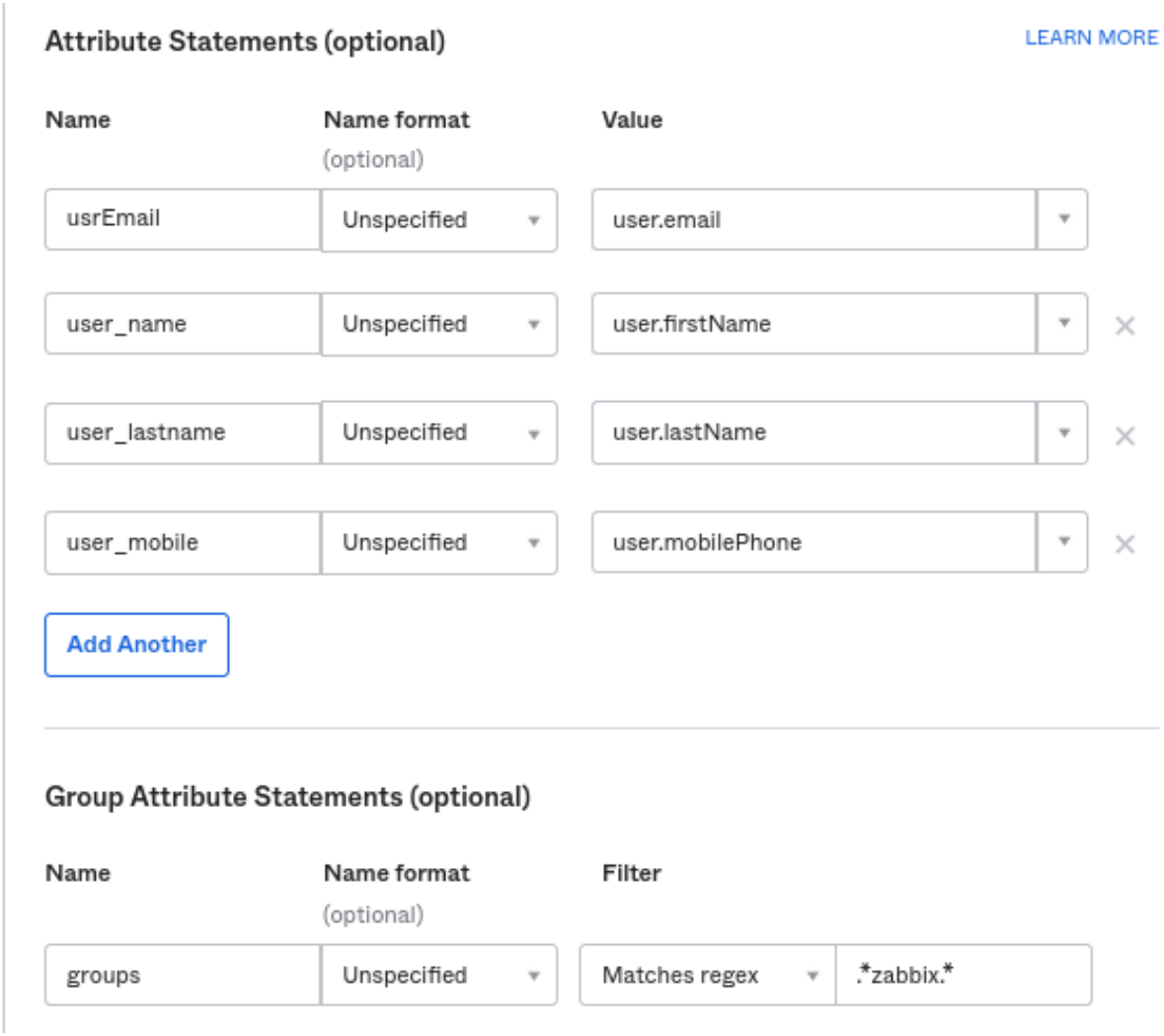


Wybierz „SAML 2.0" jako metodę logowania i kliknij *Next*.

4. W ustawieniach ogólnych wpisz nazwę aplikacji i kliknij *Next*.
5. W konfiguracji SAML wprowadź poniższe wartości, a następnie kliknij *Next*.



- W sekcji **General** dodaj:
  - *Single sign-on URL*: `http://<your-zabbix-url>/zabbix/index_sso.php?acs`
    Zwróć uwagę na użycie „http”, a nie „https”, aby parametr `acs` nie został obcięty w żądaniu. Pole wyboru *Use this for Recipient URL and Destination URL* również powinno być zaznaczone.
  - *Audience URI (SP Entity ID)*: `zabbix`
    Zwróć uwagę, że ta wartość będzie używana w asercji SAML jako unikalny identyfikator dostawcy usług (jeśli nie będzie zgodna, operacja zostanie odrzucona). W tym polu można podać adres URL lub dowolny ciąg danych.
  - *Default RelayState*:
    Pozostaw to pole puste; jeśli wymagane jest niestandardowe przekierowanie, można je dodać w Zabbix w ustawieniach *Users* > *Users*.
  - Pozostałe pola wypełnij zgodnie ze swoimi preferencjami.
- W sekcji **Attribute Statements/Group Attribute Statements** dodaj:



Te instrukcje atrybutów są wstawiane do asercji SAML udostępnianych Zabbix.

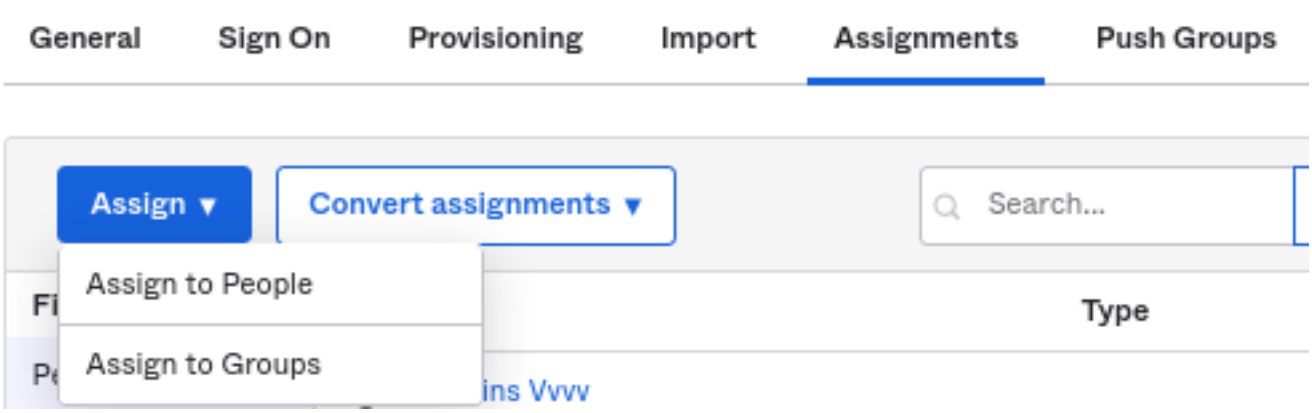
Nazwy atrybutów użyte tutaj są dowolnymi przykładami. Możesz użyć innych nazw atrybutów, jednak muszą one odpowiadać wartościom odpowiednich pól w ustawieniach SAML Zabbix.

Jeśli chcesz skonfigurować logowanie SAML do Zabbix *bez* provisioning użytkowników JIT, wymagany jest tylko atrybut adresu e-mail.

Note:
Jeśli planujesz używać połączenia szyfrowanego, wygeneruj prywatne i publiczne certyfikaty szyfrowania, a następnie prześlij certyfikat publiczny do Okta. Formularz przesyłania certyfikatu pojawi się, gdy parametr *Assertion Encryption* zostanie ustawiony na „Encrypted” (kliknij *Show Advanced Settings*, aby znaleźć ten parametr).

6. W następnej karcie wybierz „I’m a software vendor. I’d like to integrate my app with Okta” i kliknij *Finish*.

7. Przejdź do karty „Assignments” nowo utworzonej aplikacji i kliknij przycisk *Assign*, a następnie z listy rozwijanej wybierz „Assign to People”.



8. W wyświetlonym oknie przypisz aplikację osobom, które będą używać SAML 2.0 do uwierzytelniania w Zabbix, a następnie kliknij *Save and go back*.

9. Pobierz certyfikat IdP. Ustaw dla niego uprawnienia 644, uruchamiając:

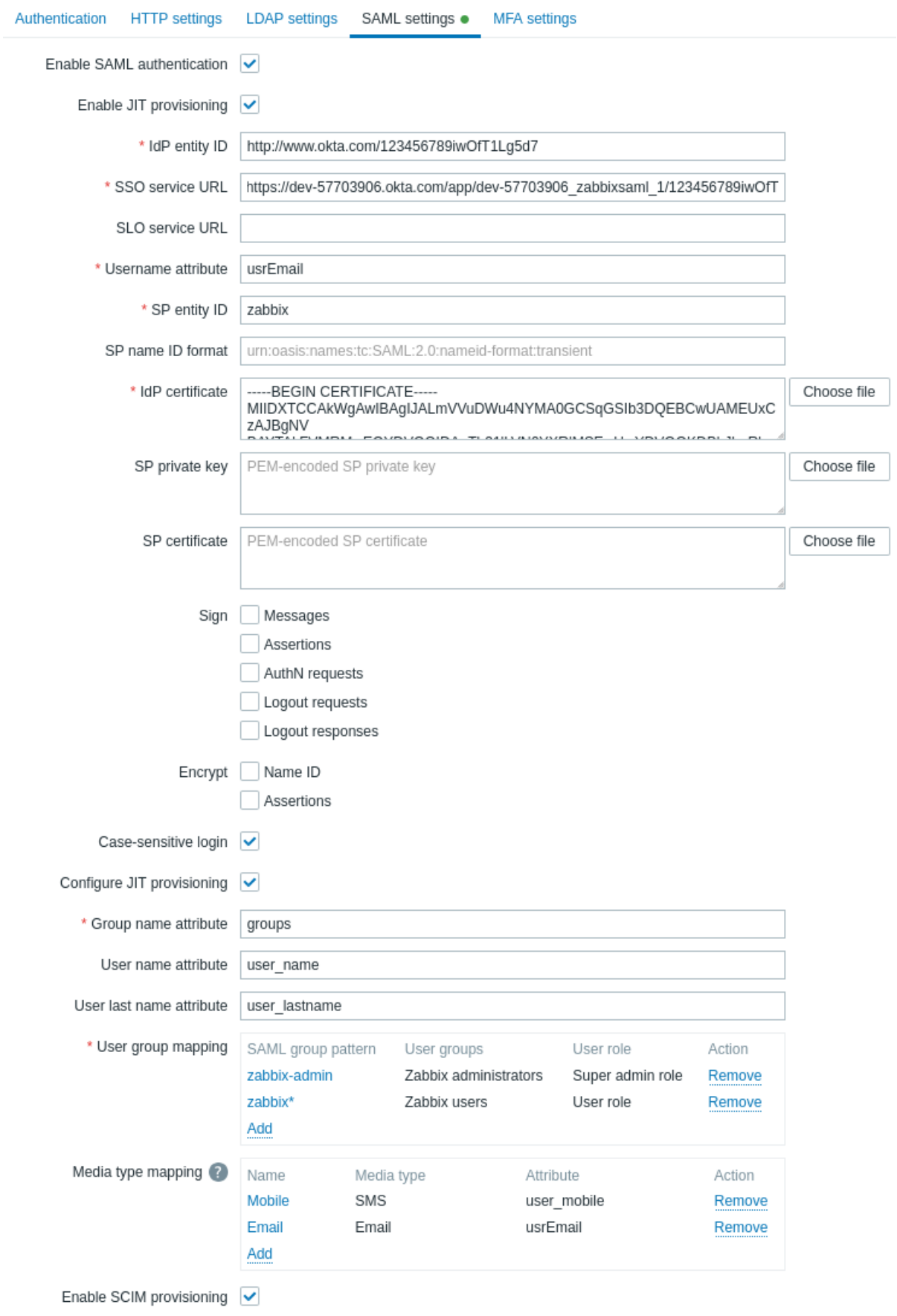
```
chmod 644 idp.crt
```

10. Przejdź do karty „Sign On” i kliknij przycisk *View Setup Instructions*.

Instructions konfiguracji zostaną otwarte w nowej karcie; pozostaw tę kartę otwartą podczas konfigurowania Zabbix.

Konfiguracja Zabbix

1. W Zabbix przejdź do ustawień SAML i wypełnij opcje konfiguracji na podstawie instrukcji konfiguracji z Okta:



Pole Zabbix	Pole konfiguracji w Okta	Przykładowa wartość
IdP entity ID	Identity Provider Issuer	
SSO service URL	Identity Provider Single Sign-On URL	
Username attribute	Attribute name	`usrEmail`
SP entity ID	Audience URI	`zabbix`
Group name attribute	Attribute name	`groups`

Pole Zabbix	Pole konfiguracji w Okta	Przykładowa wartość
User name attribute	Attribute name	`user_name`
User last name attribute	Attribute name	`user_lastname`

Należy również skonfigurować mapowanie grup użytkowników i mediów.

2. Dodaj certyfikat Base64 podany w instrukcjach konfiguracji Okta SAML.

Jeśli w zabbix.conf.php ustawiono `$SSO['CERT_STORAGE'] = 'database'`, możesz wkleić treść certyfikatu lub przesłać plik certyfikatu w frontendzie podczas konfiguracji SAML — żadne pliki w systemie plików nie są wymagane.

Jeśli w zabbix.conf.php ustawiono `$SSO['CERT_STORAGE'] = 'file'`, certyfikat musi być dostępny w systemie plików (domyślnie w ui/conf/certs lub w ścieżce skonfigurowanej w zabbix.conf.php), a frontend nie będzie przechowywać certyfikatów w bazie danych. Pamiętaj, że jeśli `$SSO['CERT_STORAGE']` nie jest ustawione lub jest zakomentowane, zakładane jest przechowywanie w plikach, a certyfikaty są odczytywane z ui/conf/certs.

3. Jeśli w Okta parametr *Assertion Encryption* został ustawiony na ”Encrypted”, w Zabbix również należy zaznaczyć pole wyboru ”Assertions” parametru *Encrypt*.

4. Naciśnij przycisk *Update*, aby zapisać te ustawienia.

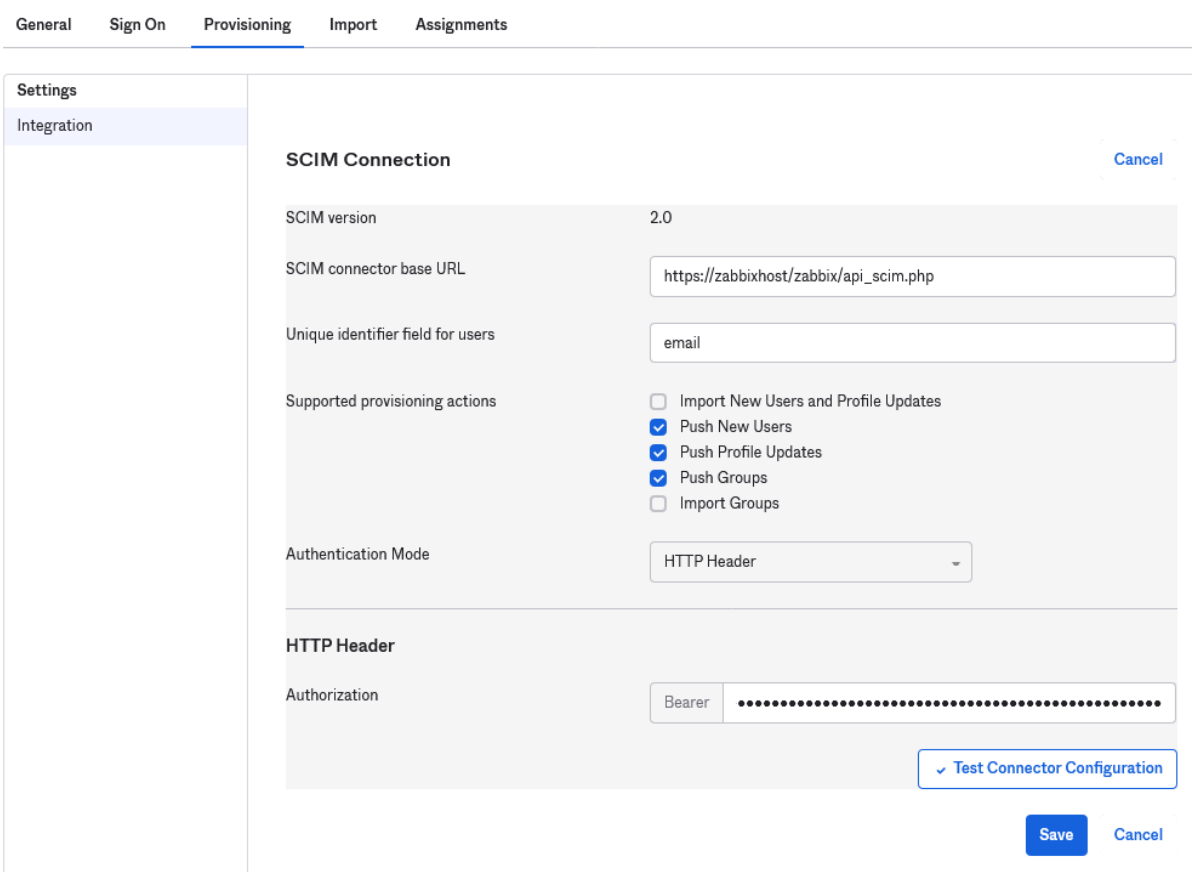
Provisioning SCIM

1. Aby włączyć provisioning SCIM, przejdź do ”General” -> ”App Settings” aplikacji w Okta.

Zaznacz pole wyboru *Enable SCIM provisioning*. W rezultacie pojawi się nowa karta *Provisioning*.

2. Przejdź do karty ”Provisioning”, aby skonfigurować połączenie SCIM:

- W polu *SCIM connector base URL* podaj ścieżkę do frontend Zabbix i dopisz do niej `api_scim.php`, tj.: `https://<your-zabbix-url>/zabbix/api_scim.php`
- *Unique identifier field for users*: `email`
- *Authentication mode*: `HTTP header`
- W polu *Authorization* wprowadź prawidłowy token API z uprawnieniami Super admin



Attention:
Jeśli występują problemy z uwierzytelnianiem, zobacz Przekazywanie nagłówka Authorization.

3. Kliknij *Test Connector Configuration*, aby przetestować połączenie. Jeśli wszystko jest poprawnie skonfigurowane, zostanie wyświetlony komunikat o powodzeniu.

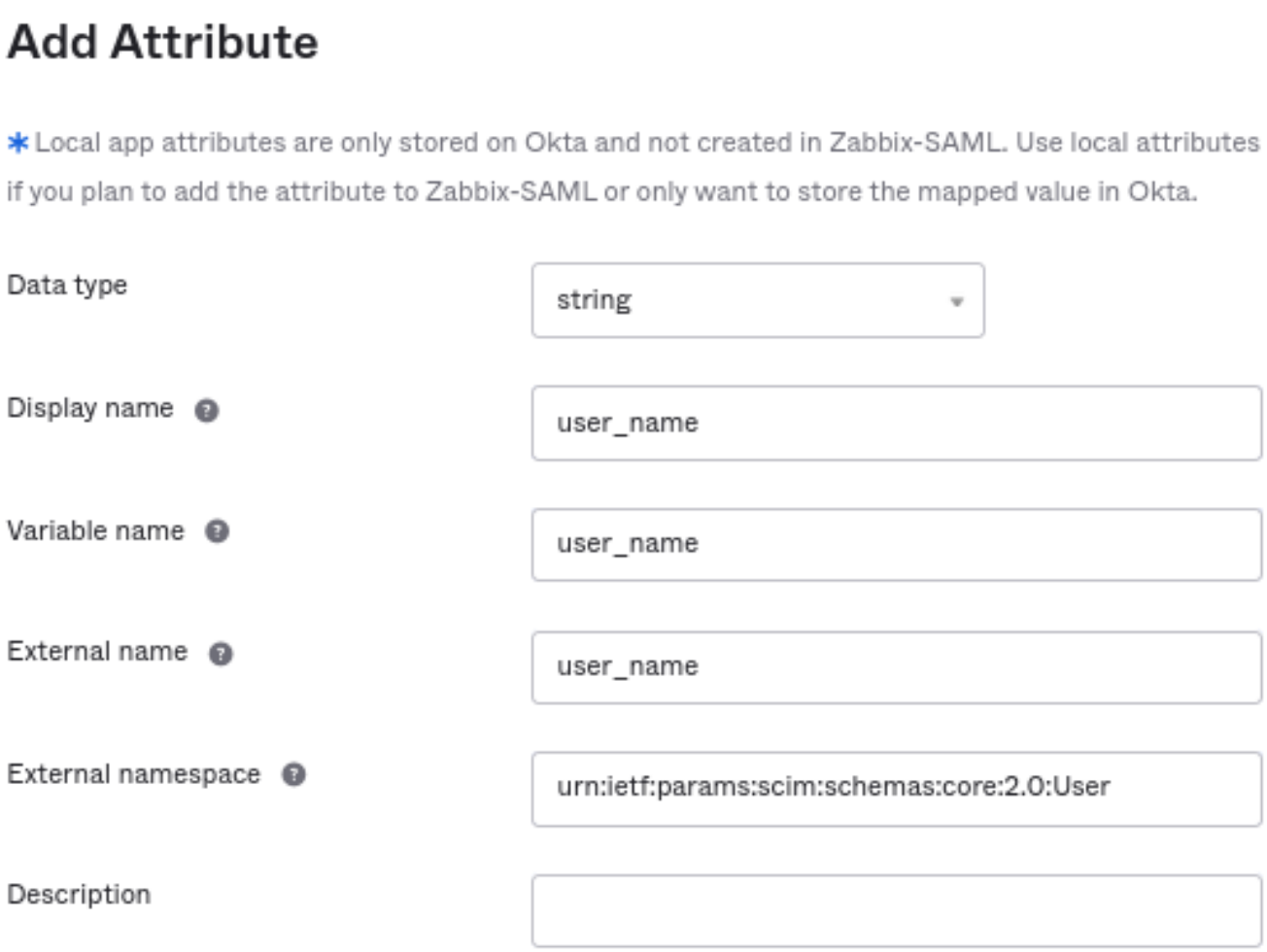
4. W ”Provisioning” -> ”To App” upewnij się, że zaznaczone są następujące pola wyboru:

- Create Users
- Update User Attributes
- Deactivate Users

Zapewni to wysyłanie tych typów żądań do Zabbix.

5. Upewnij się, że wszystkie atrybuty zdefiniowane w SAML są również zdefiniowane w SCIM. Możesz uzyskać dostęp do edytora profilu swojej aplikacji w ”Provisioning” -> ”To App”, klikając *Go to Profile Editor*.

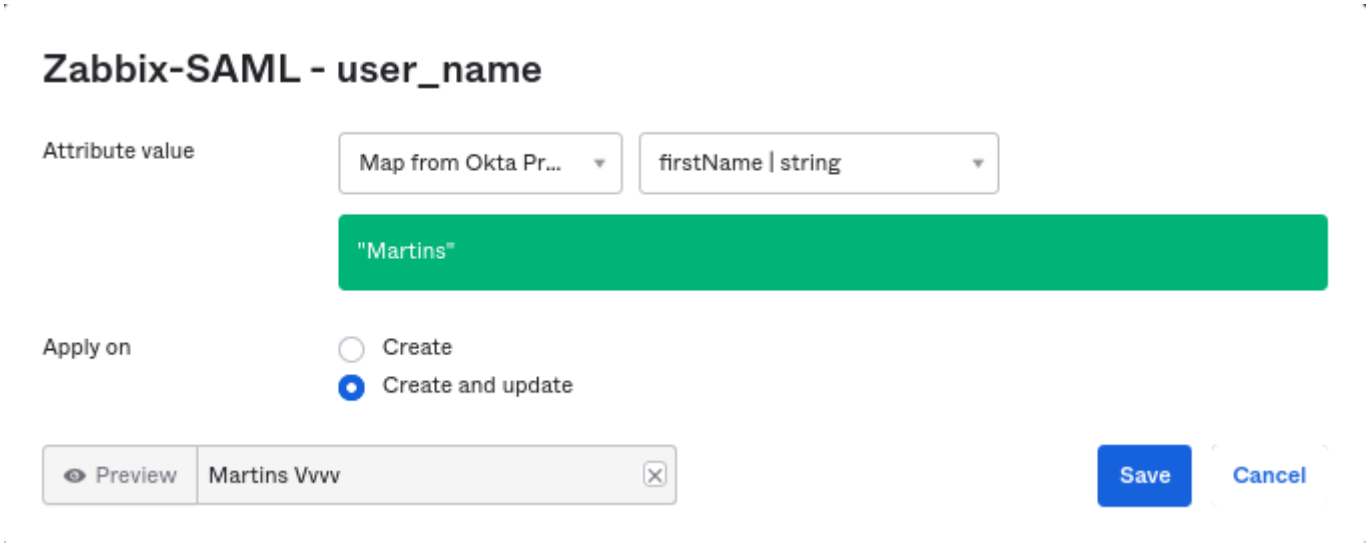
Kliknij *Add Attribute*. Wypełnij pola *Display name*, *Variable name*, *External name* nazwą atrybutu SAML, na przykład `user_name`.



Pole *External namespace* powinno być takie samo jak schemat użytkownika: `urn:ietf:params:scim:schemas:core:2.0:User`

6. Przejdź do ”Provisioning” -> ”To App” -> ”Attribute Mappings” swojej aplikacji. Kliknij *Show Unmapped Attributes* na dole. Pojawią się nowo dodane atrybuty.

7. Zmapuj każdy dodany atrybut.



8. Dodaj użytkowników na karcie ”Assignments”. Użytkownicy muszą wcześniej zostać dodani w *Directory -> People*. Wszystkie te przypisania zostaną wysłane jako żądania do Zabbix.

9. Dodaj grupy na karcie ”Push Groups”. Wzorzec mapowania grup użytkowników w ustawieniach Zabbix SAML musi odpowiadać grupie określonej tutaj. Jeśli nie ma zgodności, użytkownik nie może zostać utworzony w Zabbix.

Informacje o członkach grupy są wysyłane za każdym razem, gdy zostanie wprowadzona jakaś zmiana.

14 Konfiguracja SAML z OneLogin

Przegląd

Ta sekcja zawiera wytyczne dotyczące konfigurowania logowania jednokrotnego oraz aprowizacji użytkowników w Zabbix z OneLogin przy użyciu uwierzytelniania SAML 2.0.

Konfiguracja OneLogin

Tworzenie aplikacji

1. Zaloguj się na swoje konto w OneLogin. Do celów testowych możesz utworzyć bezpłatne konto deweloperskie w OneLogin.

2. W interfejsie web OneLogin przejdź do *Applications → Applications*.

3. Kliknij „Add App” i wyszukaj odpowiednią aplikację. Wytyczne na tej stronie opierają się na przykładzie aplikacji *SCIM Provisioner with SAML (SCIM v2 Enterprise, full SAML)*.

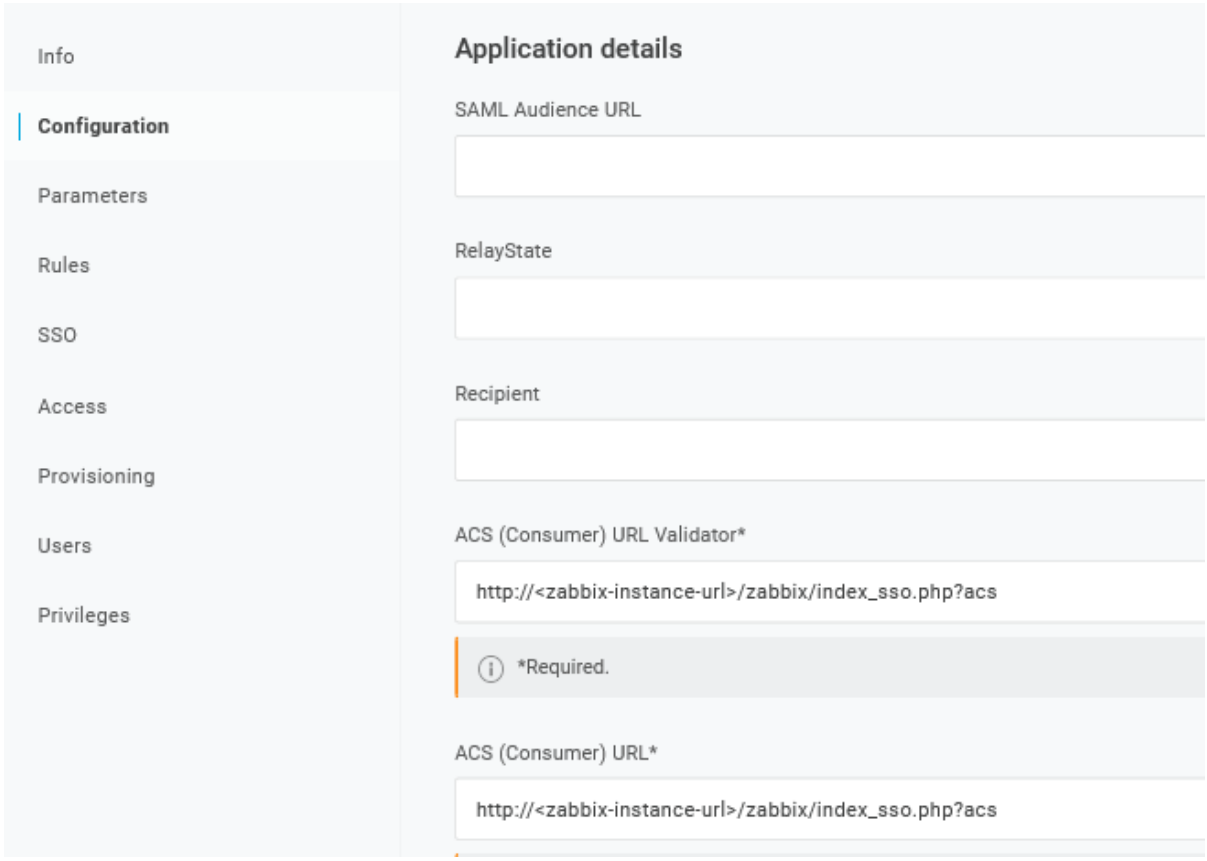
4. Na początek możesz dostosować wyświetlaną nazwę swojej aplikacji. Możesz również dodać ikonę i szczegóły aplikacji. Następnie kliknij *Save*.

Konfigurowanie provisioningu SSO/SCIM

1. W *Configuration -> Application details* ustaw endpoint logowania jednokrotnego Zabbix `http://<zabbix-instance-url>/zabbix/ind` jako wartość następujących pól:

- *ACS (Consumer) URL Validator*
- *ACS (Consumer) URL*

Zwróć uwagę na użycie „http”, a nie „https”, aby parametr `acs` nie został obcięty w żądaniu.



Możliwe jest również użycie „https". Aby to działało z Zabbix, należy dodać do `conf/zabbix.conf.php` następującą linię:

```
$SSO['SETTINGS'] = ['use_proxy_headers' => true];
```

Pozostaw pozostałe opcje z ich wartościami domyślnymi.

2. W *Configuration -> API connection* ustaw następujące wartości:

- *SCIM Base URL*: `https://<zabbix-instance-url>/zabbix/api_scim.php`
- *SCIM JSON Template*: powinien zawierać wszystkie atrybuty niestandardowe, które chcesz przekazać do Zabbix przez SCIM, takie jak `user_name`, `user_lastname`, `user_email` i `user_mobile`:

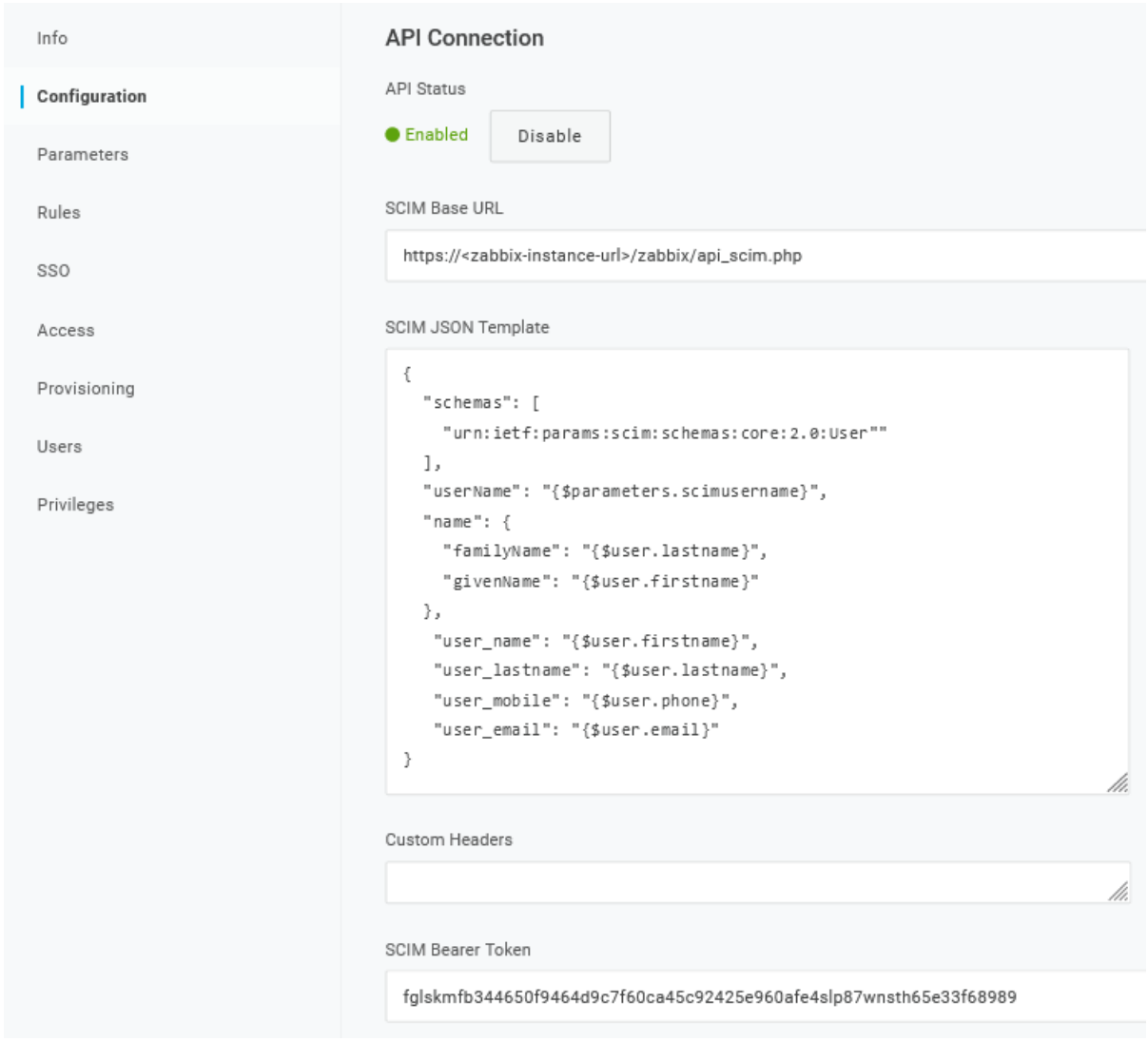
```
{
  "schemas": [
    "urn:ietf:params:scim:schemas:core:2.0:User"
  ],
  "userName": "{$parameters.scimusername}",
  "name": {
    "familyName": "{$user.lastname}",
    "givenName": "{$user.firstname}"
  },
   "user_name": "{$user.firstname}",
   "user_lastname": "{$user.lastname}",
   "user_mobile": "{$user.phone}",
   "user_email": "{$user.email}"
}
```

Nazwy atrybutów są dowolne. Można używać innych nazw atrybutów, jednak wymagane jest, aby odpowiadały one wartościom odpowiednich pól w ustawieniach Zabbix SAML.

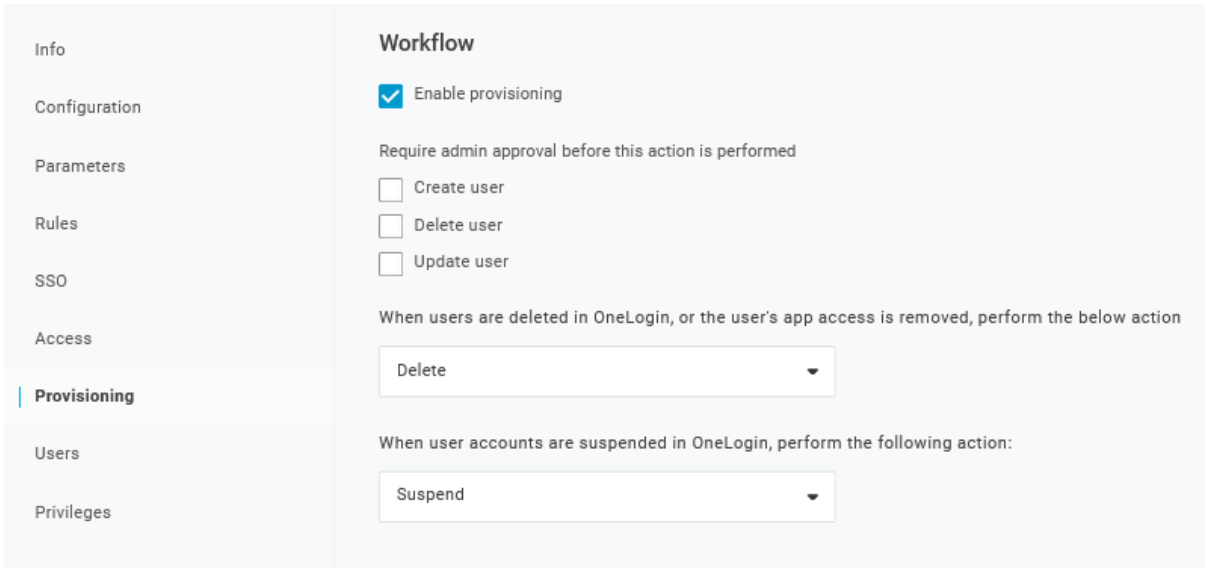
Pamiętaj, że aby provisioning użytkowników działał, OneLogin musi otrzymać w odpowiedzi atrybut „name" z wartościami „givenName" i „familyName", nawet jeśli nie było to wymagane przez dostawcę usługi. Dlatego konieczne jest określenie tego w schemacie w części konfiguracji aplikacji.

- *SCIM Bearer Token*: wprowadź token API Zabbix z uprawnieniami Super admin.

Kliknij *Enable*, aby aktywować połączenie.

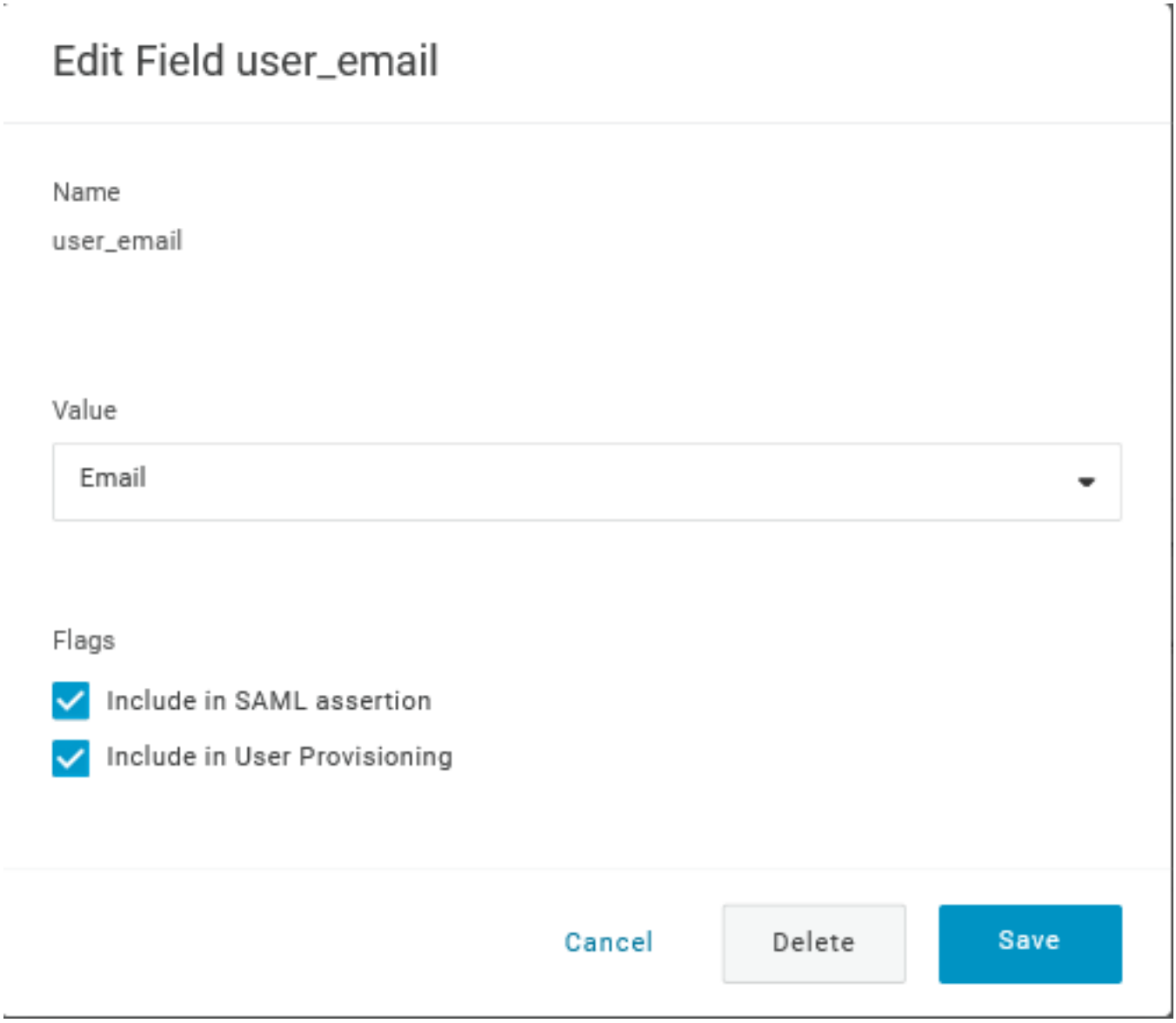


3. Na stronie *Provisioning* włącz opcję Provisioning:



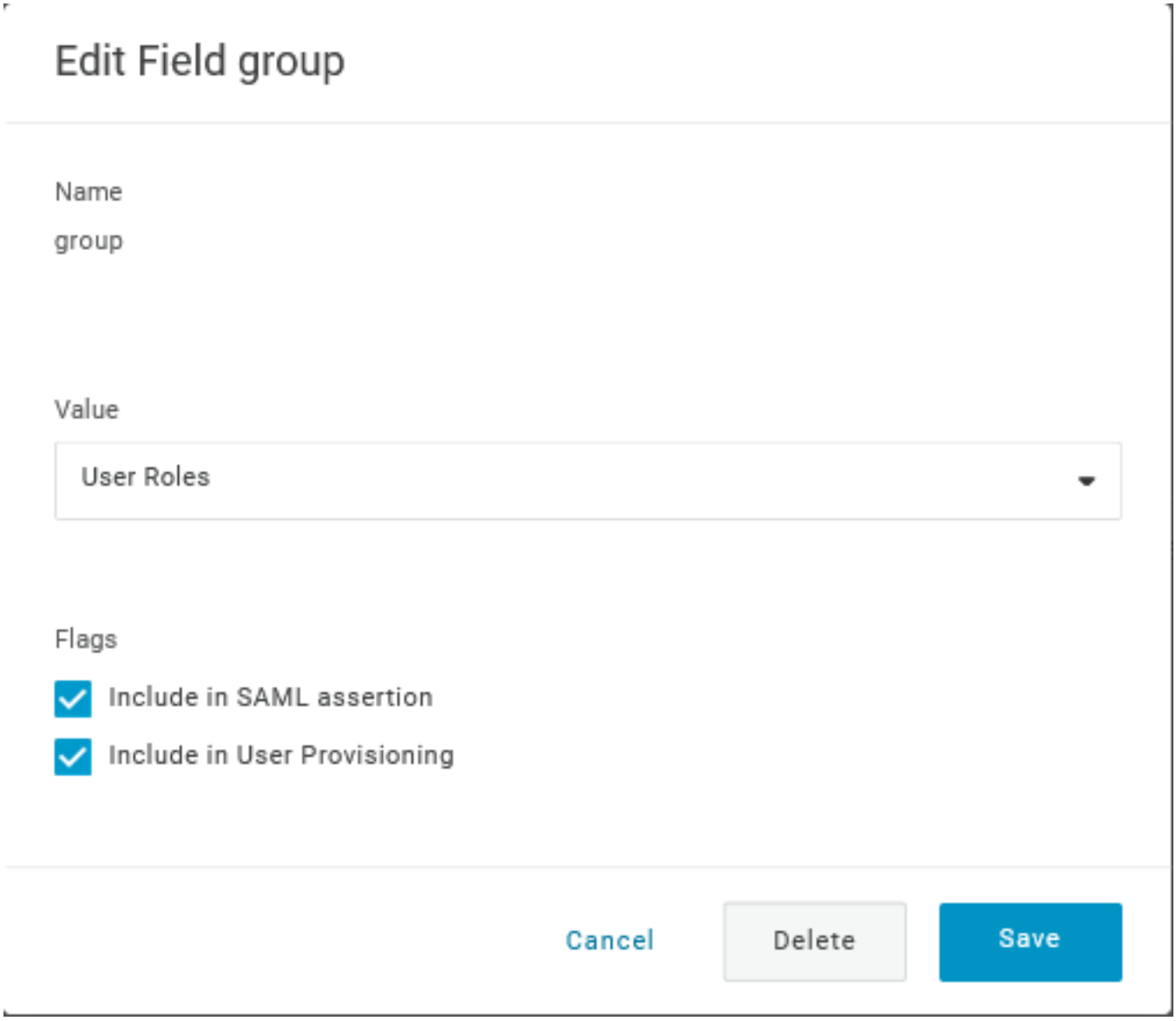
4. Strona *Parameters* zawiera listę parametrów domyślnych:

- Upewnij się, że „scimusername” odpowiada wartości loginu użytkownika w OneLogin (np. adresowi e-mail);
- Zaznacz opcję *Include in User Provisioning* dla parametru „Groups”;
- Kliknij „+”, aby utworzyć parametry niestandardowe wymagane do asercji SAML i provisioningu użytkowników, takie jak `user_name`, `user_lastname`, `user_email` i `user_mobile`:

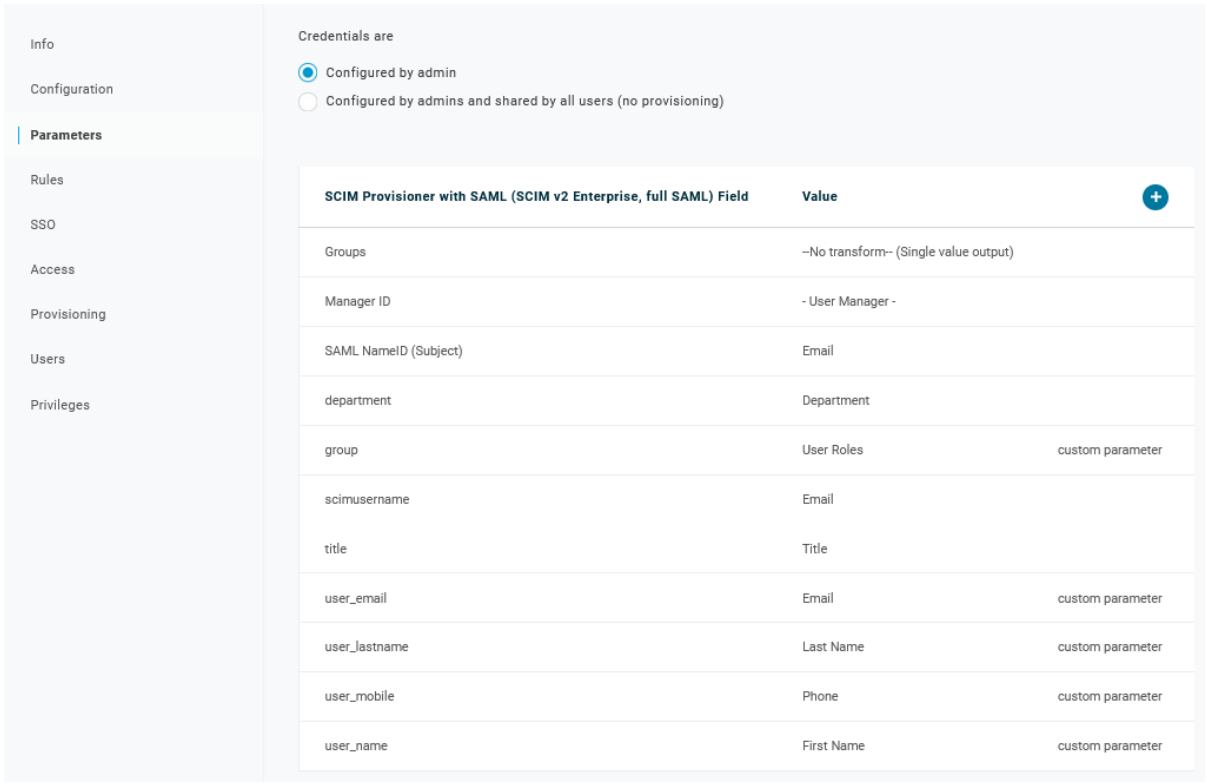


Podczas dodawania parametru pamiętaj, aby zaznaczyć zarówno opcję *Include in SAML assertion*, jak i *Include in User Provisioning*.

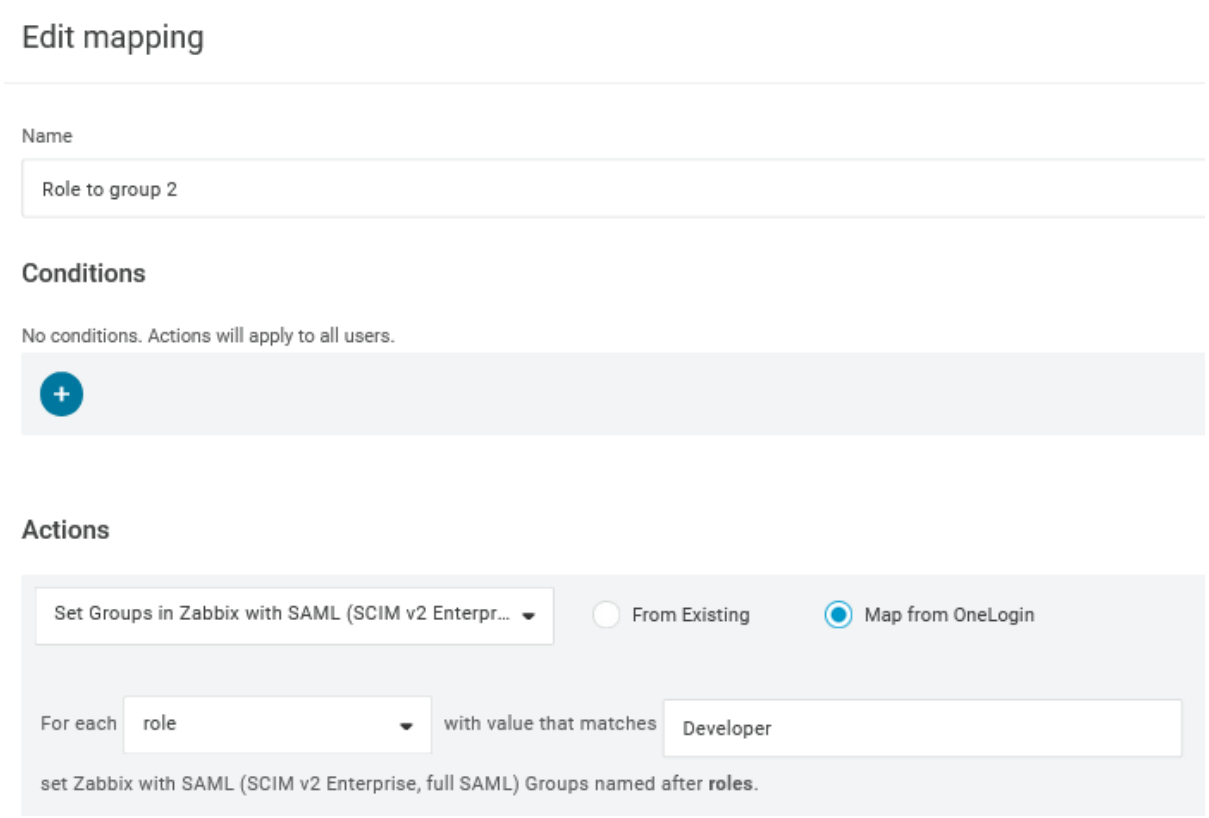
- Dodaj parametr „group”, który odpowiada rolom użytkowników w OneLogin. Role użytkowników będą przekazywane jako ciąg znaków rozdzielony średnikiem `;`. Role użytkowników OneLogin będą używane do tworzenia grup użytkowników w Zabbix:



Zweryfikuj listę parametrów:



5. Na stronie *Rules* utwórz mapowania ról użytkowników do domyślnego parametru Groups.



Możesz użyć wyrażenia regularnego, aby przekazywać określone role jako grupy. Nazwy ról nie powinny zawierać `;`, ponieważ OneLogin używa go jako separatora podczas wysyłania atrybutu z kilkoma rolami.

6. Pobierz certyfikat IdP. Ustaw dla niego uprawnienia 644, uruchamiając:

```
chmod 644 idp.crt
```

Konfiguracja Zabbix

1. W Zabbix przejdź do ustawień SAML i wypełnij opcje konfiguracji na podstawie konfiguracji OneLogin:



Pole Zabbix	Pole konfiguracji w OneLogin	Przykładowa wartość
IdP entity ID	Issuer URL (zobacz kartę SSO swojej aplikacji w OneLogin)	
SSO service URL	SAML 2.0 Endpoint (HTTP) (zobacz kartę SSO swojej aplikacji w OneLogin)	

Pole Zabbix	Pole konfiguracji w OneLogin	Przykładowa wartość
SLO service URL	SLO Endpoint (HTTP) (zobacz kartę SSO swojej aplikacji w OneLogin)	
Username attribute	Parametr niestandardowy	`user_email`
Group name attribute	Parametr niestandardowy	`group`
User name attribute	Parametr niestandardowy	`user_name`
User last name attribute	Parametr niestandardowy	`user_lastname`

Wymagane jest również skonfigurowanie mapowania grup użytkowników. Mapowanie mediów jest opcjonalne. Kliknij *Update*, aby zapisać te ustawienia.

2. Dodaj certyfikat Base64 dostarczony przez OneLogin.

Jeśli w zabbix.conf.php ustawiono `$SSO['CERT_STORAGE'] = 'database'`, możesz wkleić treść certyfikatu lub przesłać plik certyfikatu w frontend podczas konfiguracji SAML — żadne pliki w systemie plików nie są wymagane.

Jeśli w zabbix.conf.php ustawiono `$SSO['CERT_STORAGE'] = 'file'`, certyfikat musi być dostępny w systemie plików (domyślnie w ui/conf/certs lub w ścieżce skonfigurowanej w zabbix.conf.php), a frontend nie będzie przechowywać certyfikatów w bazie danych. Zwróć uwagę, że jeśli `$SSO['CERT_STORAGE']` nie jest ustawione lub jest zakomentowane, zakładane jest przechowywanie w plikach, a certyfikaty są odczytywane z ui/conf/certs.

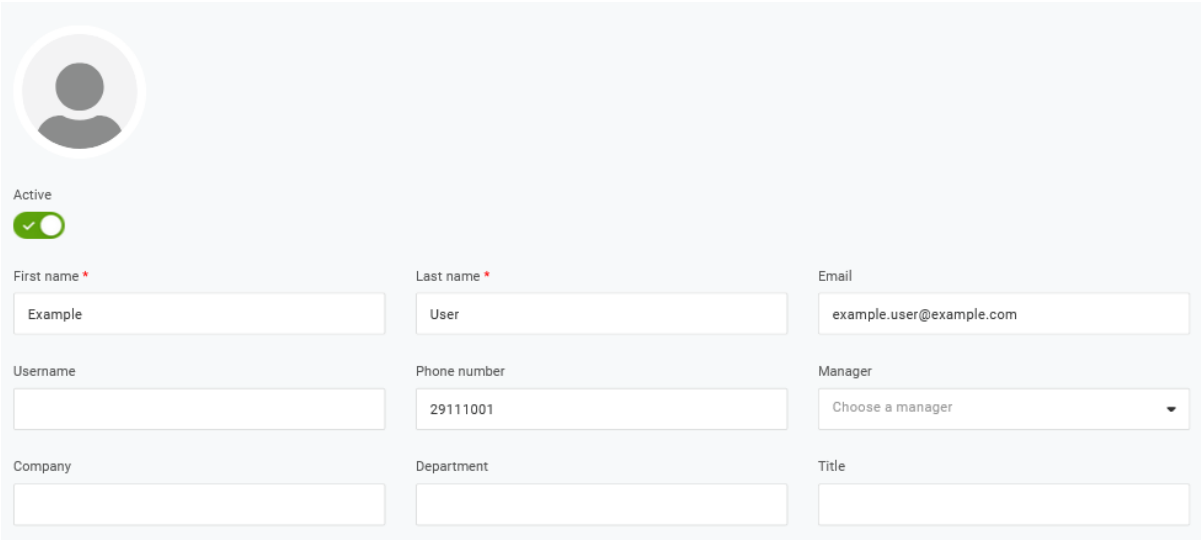
Dostęp do pobrania certyfikatu w OneLogin uzyskasz w *Applications* -> *SSO* -> kliknij *View details* pod bieżącym certyfikatem.

3. Naciśnij przycisk *Update*, aby zapisać te ustawienia.

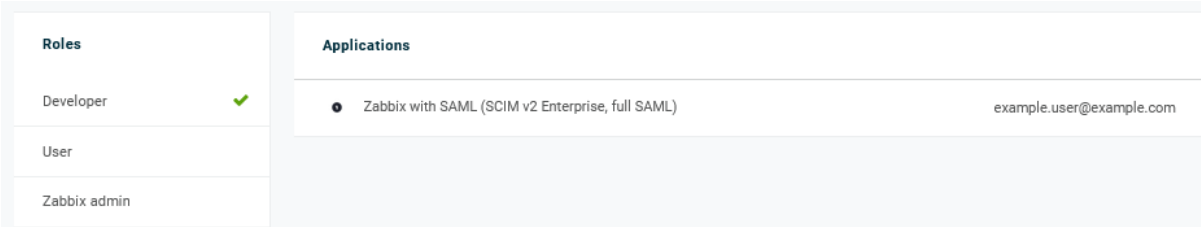
Provisioning użytkowników SCIM

Po włączeniu provisioningu użytkowników możliwe jest teraz dodawanie/aktualizowanie użytkowników i ich ról w OneLogin oraz ich natychmiastowe provisionowanie do Zabbix.

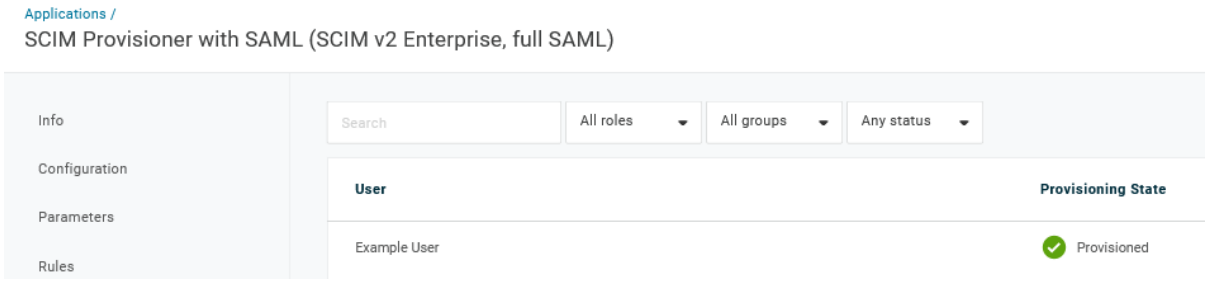
Na przykład możesz utworzyć nowego użytkownika:



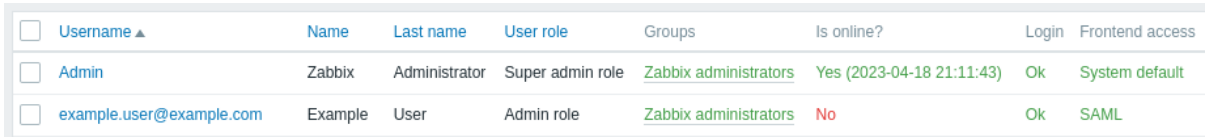
Dodać go do roli użytkownika oraz do aplikacji, która będzie provisionować użytkownika:



Po zapisaniu użytkownika zostanie on provisionowany do Zabbix. W sekcji Application -> Users możesz sprawdzić status provisioningu bieżących użytkowników aplikacji:



Jeśli provisioning zakończy się powodzeniem, użytkownik będzie widoczny na liście użytkowników Zabbix.



Username ▲	Name	Last name	User role	Groups	Is online?	Login	Frontend access
Admin	Zabbix	Administrator	Super admin role	Zabbix administrators	Yes (2023-04-18 21:11:43)	Ok	System default
example.user@example.com	Example	User	Admin role	Zabbix administrators	No	Ok	SAML

15 Konfigurowanie zaplanowanych raportów

Przegląd

Ta sekcja zawiera instrukcje dotyczące instalacji usługi internetowej Zabbix oraz konfiguracji Zabbix w celu umożliwienia generowania zaplanowanych raportów.

Instalacja

Nowy proces Zabbix web service oraz przeglądarka Google Chrome powinny zostać zainstalowane, aby umożliwić generowanie zaplanowanych raportów. Usługa web service może zostać zainstalowana na tej samej maszynie, na której zainstalowany jest serwer Zabbix, lub na innej maszynie. Przeglądarka Google Chrome powinna być zainstalowana na tej samej maszynie, na której zainstalowana jest usługa web service.

Oficjalny pakiet zabbix-web-service jest dostępny w repozytorium Zabbix. Przeglądarka Google Chrome nie jest dołączona do tych pakietów i musi zostać zainstalowana osobno.

Aby skompilować usługę internetową Zabbix ze źródeł, zobacz Installing Zabbix web service.

Po instalacji uruchom zabbix_web_service na maszynie, na której usługa internetowa jest zainstalowana:

```
zabbix_web_service
```

Konfiguracja

Aby zapewnić prawidłową komunikację między wszystkimi zaangażowanymi elementami, upewnij się, że plik konfiguracyjny serwera oraz parametry konfiguracyjne frontend są poprawnie skonfigurowane.

Serwer Zabbix

Należy zaktualizować następujące parametry w pliku konfiguracyjnym serwera Zabbix: *WebServiceURL* i *StartReportWriters*.

WebServiceURL

Ten parametr jest wymagany do włączenia komunikacji z usługą web service. Adres URL powinien mieć format `http[s]://host:port/repo`

- Domyślnie usługa web service nasłuchuje na porcie 10053. Inny port można określić w pliku konfiguracyjnym usługi web service.
- Podanie ścieżki `/report` jest obowiązkowe (ścieżka jest zakodowana na stałe i nie można jej zmienić).

Przykład:

```
WebServiceURL=http://localhost:10053/report
```

Attention:
Zdecydowanie zaleca się skonfigurowanie szyfrowania między serwerem Zabbix a usługą web service przy użyciu certyfikatów. Domyślnie dane przesyłane między serwerem Zabbix a usługą web service nie są szyfrowane, co może prowadzić do nieautoryzowanego dostępu.

StartReportWriters

Ten parametr określa, ile procesów zapisu raportów powinno zostać uruchomionych. Jeśli nie jest ustawiony lub ma wartość 0, generowanie raportów jest wyłączone. W zależności od wymaganej liczby i częstotliwości raportów można włączyć od 1 do 100 procesów zapisu raportów.

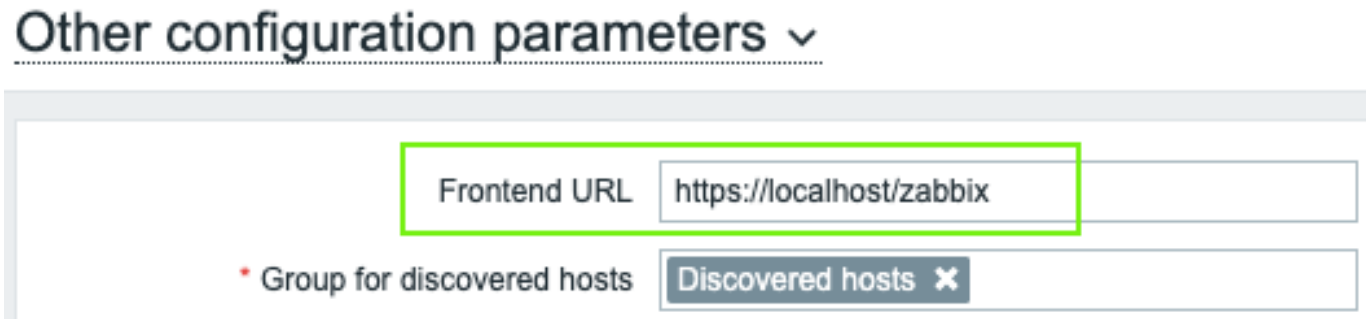
Przykład:

```
StartReportWriters=3
```

Zabbix frontend

Parametr *Frontend URL* powinien być ustawiony, aby umożliwić komunikację między Zabbix frontend a usługą internetową Zabbix:

- Przejdź do sekcji menu frontend *Administration* > *General* > *Other*
- Określ pełny adres URL interfejsu webowego Zabbix w parametrze *Frontend URL*



Note:
Po zakończeniu procedury konfiguracji możesz skonfigurować i wysłać raport testowy, aby upewnić się, że wszystko działa poprawnie.

16 Dodatkowe języki frontendu

Przegląd

Aby korzystać z języka innego niż angielski w interfejsie sieciowym Zabbix, jego ustawienia regionalne muszą być ustawione na serwerze WWW. Dodatkowo, wymagane jest rozszerzenie PHP gettext, aby tłumaczenia działały.

Installing locales

To list all installed languages, run:

```
locale -a
```

If some languages that are needed are not listed, open the */etc/locale.gen* file and uncomment the required locales. Since Zabbix uses UTF-8 encoding, you need to select locales with UTF-8 charset.

Now, run:

```
locale-gen
```

Restart the web server.

The locales should now be installed. It may be required to reload Zabbix frontend page in browser using Ctrl + F5 for new languages to appear.

Instalacja Zabbix

Jeśli instalujesz Zabbix bezpośrednio z repozytorium git Zabbix, pliki tłumaczeń należy wygenerować ręcznie. Aby wygenerować pliki tłumaczeń, uruchom:

```
make gettext
locale/make_mo.sh
```

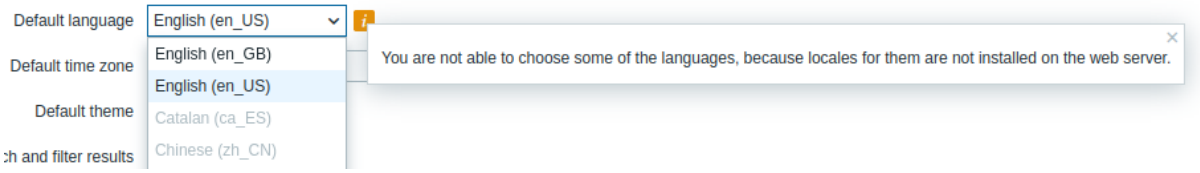
Ten krok nie jest wymagany podczas instalacji Zabbix z pakietów lub z plików źródłowych tar.gz.

Wybór języka

Istnieje kilka sposobów wyboru języka w interfejsie webowym Zabbix:

- Podczas instalacji interfejsu webowego - w kreatorze instalacji frontend. Wybrany język zostanie ustawiony jako domyślny dla systemu.
- Po instalacji domyślny język systemu można zmienić w sekcji menu *Administration→General→GUI*.
- Język dla konkretnego użytkownika można zmienić w profilu użytkownika.

Jeśli locale dla danego języka nie jest zainstalowane na komputerze, język ten będzie wyszarzony w selektorze języka Zabbix. Obok selektora języka wyświetlana jest pomarańczowa ikona, jeśli brakuje co najmniej jednego locale. Po kliknięciu tej ikony zostanie wyświetlony następujący komunikat: „Nie możesz wybrać niektórych języków, ponieważ locale dla nich nie są zainstalowane na serwerze webowym.”



2 Konfiguracja procesów

Użyj paska bocznego, aby uzyskać dostęp do treści w tej sekcji.

1 Serwer Zabbix

Przegląd

Parametry obsługiwane przez plik konfiguracyjny serwera Zabbix (zabbix_server.conf) są wymienione w tej sekcji.

Parametry są wymienione bez dodatkowych informacji. Kliknij parametr, aby zobaczyć pełne szczegóły.

Parameter	Description
AlertScriptsPath	Lokalizacja niestandardowych skryptów alertów.
AllowRoot	Zezwala serwerowi na działanie jako „root”.
AllowSoftwareUpdateCheck	Zezwala interfejsowi Zabbix na otrzymywanie informacji o aktualizacjach oprogramowania z zabbix.com.
AllowUnsupportedDBVersions	Zezwala serwerowi na pracę z nieobsługiwanymi wersjami bazy danych.
CacheSize	Rozmiar pamięci podręcznej konfiguracji.
CacheUpdateFrequency	Ten parametr określa, jak często Zabbix będzie aktualizował pamięć podręczną konfiguracji, w sekundach.
DBHost	Nazwa hosta bazy danych.
DBName	Nazwa bazy danych.
DBPassword	Hasło bazy danych.
DBPort	Port bazy danych, gdy nie jest używane lokalne gniazdo.
DBSchema	Nazwa schematu bazy danych. Używane dla PostgreSQL.
DBSocket	Ścieżka do pliku gniazda MySQL.
DBUser	Użytkownik bazy danych.
DBTLSConnect	Ustawienie tej opcji na określoną wartość wymusza użycie połączenia TLS z bazą danych.
DBTLSCAFile	Pełna ścieżka do pliku zawierającego certyfikaty głównych urzędów certyfikacji (CA) do weryfikacji certyfikatu bazy danych.
DBTLSCertFile	Pełna ścieżka do pliku zawierającego certyfikat serwera Zabbix do uwierzytelniania w bazie danych.
DBTLSKeyFile	Pełna ścieżka do pliku zawierającego klucz prywatny do uwierzytelniania w bazie danych.
DBTLSCipher	Lista szyfrów, które serwer Zabbix dopuszcza dla protokołów TLS do wersji TLS v1.2 włącznie. Obsługiwane tylko dla MySQL.
DBTLSCipher13	Lista pakietów szyfrów, które serwer Zabbix dopuszcza dla protokołu TLS v1.3. Obsługiwane tylko dla MySQL, począwszy od wersji 8.0.16.
DebugLevel	Określa poziom debugowania.
EnableGlobalScripts	Włącza skrypty globalne na serwerze Zabbix.
ExportDir	Katalog do eksportu zdarzeń, historii i trendów w czasie rzeczywistym w formacie JSON rozdzielanym znakami nowej linii. Jeśli ustawione, włącza eksport w czasie rzeczywistym.
ExportFileSize	Maksymalny rozmiar pojedynczego pliku eksportu w bajtach.
ExportType	Lista typów encji rozdzielonych przecinkami (events, history, trends) do eksportu w czasie rzeczywistym (domyślnie wszystkie typy).
ExternalScripts	Lokalizacja zewnętrznych skryptów.
Fping6Location	Lokalizacja fping6.
FpingLocation	Lokalizacja fping.
FrontendAllowedIP	Lista adresów IP lub zakresów CIDR rozdzielonych przecinkami, z których dozwolone jest łączenie z frontend.

Parameter	Description
HANodeName	Nazwa węzła klastra wysokiej dostępności.
HistoryCacheSize	Rozmiar pamięci podręcznej historii.
HistoryIndexCacheSize	Rozmiar pamięci podręcznej indeksu historii.
HistoryStorageDateIndex	Włącza przetwarzanie wstępne wartości historii w magazynie historii, aby przechowywać wartości w różnych indeksach na podstawie daty.
HistoryStorageURL	Adres URL HTTP[S] magazynu historii.
HistoryStorageTypes	Lista typów wartości rozdzielonych przecinkami, które mają być wysyłane do magazynu historii.
HousekeepingFrequency	Ten parametr określa, jak często Zabbix będzie wykonywał procedurę housekeeping, w godzinach.
Include	Możesz dołączyć pojedyncze pliki lub wszystkie pliki w katalogu do pliku konfiguracyjnego.
JavaGateway	Adres IP (lub nazwa hosta) Zabbix Java gateway.
JavaGatewayPort	Port, na którym nasłuchuje Zabbix Java gateway.
ListenBacklog	Maksymalna liczba oczekujących połączeń w kolejce TCP.
ListenIP	Lista adresów IP rozdzielonych przecinkami, na których trapper powinien nasłuchiwać.
ListenPort	Port nasłuchiwania dla trappera.
LoadModule	Moduł do załadowania podczas uruchamiania serwera.
LoadModulePath	Pełna ścieżka do lokalizacji modułów serwera.
LogFile	Nazwa pliku dziennika.
LogFileSize	Maksymalny rozmiar pliku dziennika.
LogSlowQueries	Określa, jak długo może trwać zapytanie do bazy danych, zanim zostanie zapisane w dzienniku, w milisekundach.
LogType	Typ wyjścia dziennika.
MaxConcurrentChecksPerPoller	Maksymalna liczba asynchronicznych kontroli, które mogą być wykonywane jednocześnie przez każdy poller HTTP agent, poller agent lub poller SNMP.
MaxHousekeeperDelete	W ramach jednego zadania w jednym cyklu housekeeping zostanie usuniętych nie więcej niż „MaxHousekeeperDelete” wierszy (odpowiadających [tablename], [field], [value]).
NodeAddress	Adres IP lub nazwa hosta z opcjonalnym portem do nadpisania sposobu, w jaki frontend powinien łączyć się z serwerem.
PidFile	Nazwa pliku PID.
ProblemHousekeepingFrequency	Określa, jak często Zabbix będzie usuwał problemy dla usuniętych wyzwalaczy.
ProxyConfigFrequency	Określa, jak często serwer Zabbix wysyła dane konfiguracyjne do proxy Zabbix.
ProxyDataFrequency	Określa, jak często serwer Zabbix żąda danych historii od proxy Zabbix.
ServiceManagerSyncFrequency	Określa, jak często Zabbix będzie synchronizował konfigurację menedżera usług.
SMSDevices	Lista plików modemów rozdzielonych przecinkami, których może używać serwer Zabbix.
SNMPTrapperFile	Plik tymczasowy używany do przekazywania danych z demona pułapek SNMP do serwera.
SocketDir	Katalog do przechowywania gniazd IPC używanych przez wewnętrzne usługi Zabbix.
SourceIP	Źródłowy adres IP.
SSHKeyLocation	Lokalizacja kluczy publicznych i prywatnych dla kontroli SSH i akcji.
SSLCertLocation	Lokalizacja plików certyfikatów klienta SSL do uwierzytelniania klienta.
SSLKeyLocation	Lokalizacja plików kluczy prywatnych SSL do uwierzytelniania klienta.
SSLCALocation	Nadpisuje lokalizację plików urzędu certyfikacji (CA) do weryfikacji certyfikatu serwera SSL.
StartAgentPollers	Liczba wstępnie rozwidlonych instancji asynchronicznych pollerów Zabbix agent.
StartAlerters	Liczba wstępnie rozwidlonych instancji alerterów.
StartBrowserPollers	Liczba wstępnie rozwidlonych instancji pollerów pozycji przeglądarkowych.
StartConnectors	Liczba wstępnie rozwidlonych instancji workerów konektorów.
StartDBSyncers	Liczba wstępnie rozwidlonych instancji synchronizatorów historii.
StartDiscoverers	Liczba wstępnie rozwidlonych instancji workerów wykrywania.
StartEscalators	Liczba wstępnie rozwidlonych instancji eskalatorów.
StartHistoryPollers	Liczba wstępnie rozwidlonych instancji pollerów historii.
StartHTTPAgentPollers	Liczba wstępnie rozwidlonych instancji asynchronicznych pollerów HTTP agent.
StartHTTPPollers	Liczba wstępnie rozwidlonych instancji pollerów HTTP.
StartIPMIPollers	Liczba wstępnie rozwidlonych instancji pollerów IPMI.
StartJavaPollers	Liczba wstępnie rozwidlonych instancji pollerów Java.
StartLLDProcessors	Liczba wstępnie rozwidlonych instancji workerów wykrywania niskiego poziomu (LLD).
StartODBCPollers	Liczba wstępnie rozwidlonych instancji pollerów ODBC.
StartPingers	Liczba wstępnie rozwidlonych instancji pingerów ICMP.
StartPollersUnreachable	Liczba wstępnie rozwidlonych instancji pollerów dla nieosiągalnych hostów (w tym IPMI i Java).
StartPollers	Liczba wstępnie rozwidlonych instancji pollerów.
StartPreprocessors	Liczba wstępnie uruchomionych instancji workerów przetwarzania wstępnego.
StartProxyPollers	Liczba wstępnie rozwidlonych instancji pollerów dla pasywnych proxy.
StartReportWriters	Liczba wstępnie rozwidlonych instancji modułów zapisujących raporty.

Parameter	Description
StartSNMPPollers	Liczba wstępnie rozwidlonych instancji asynchronicznych pollerów SNMP.
StartSNMPTrapper	Jeśli ustawione na 1, zostanie uruchomiony proces trappera SNMP.
StartTimers	Liczba wstępnie rozwidlonych instancji timerów.
StartTrappers	Liczba wstępnie rozwidlonych instancji trapperów.
StartVMwareCollectors	Liczba wstępnie rozwidlonych instancji kolektorów VMware.
StatsAllowedIP	Lista adresów IP rozdzielonych przecinkami, opcjonalnie w notacji CIDR, lub nazw DNS zewnętrznych instancji Zabbix. Żądanie statystyk będzie akceptowane tylko z adresów wymienionych tutaj.
Timeout	Określa, jak długo czekać (w sekundach) na ustanowienie połączenia i wymianę danych z proxy Zabbix, agent, usługą web oraz dla kontroli SNMP (z wyjątkiem pozycji SNMP `walk[OID]` i `get[OID]`).
TLSCAFile	Pełna ścieżka do pliku zawierającego certyfikaty głównych urzędów certyfikacji (CA) do weryfikacji certyfikatów peerów, używanego do szyfrowanej komunikacji między komponentami Zabbix.
TLSCertFile	Pełna ścieżka do pliku zawierającego certyfikat serwera lub łańcuch certyfikatów, używanego do szyfrowanej komunikacji między komponentami Zabbix.
TLSCipherAll	Ciąg priorytetów GnuTLS lub ciąg szyfrów OpenSSL (TLS 1.2). Nadpisuje domyślne kryteria wyboru pakietów szyfrów dla szyfrowania opartego na certyfikatach i PSK.
TLSCipherAll13	Ciąg szyfrów dla OpenSSL 1.1.1 lub nowszego w TLS 1.3. Nadpisuje domyślne kryteria wyboru pakietów szyfrów dla szyfrowania opartego na certyfikatach i PSK.
TLSCipherCert	Ciąg priorytetów GnuTLS lub ciąg szyfrów OpenSSL (TLS 1.2). Nadpisuje domyślne kryteria wyboru pakietów szyfrów dla szyfrowania opartego na certyfikatach.
TLSCipherCert13	Ciąg szyfrów dla OpenSSL 1.1.1 lub nowszego w TLS 1.3. Nadpisuje domyślne kryteria wyboru pakietów szyfrów dla szyfrowania opartego na certyfikatach.
TLSCipherPSK	Ciąg priorytetów GnuTLS lub ciąg szyfrów OpenSSL (TLS 1.2). Nadpisuje domyślne kryteria wyboru pakietów szyfrów dla szyfrowania opartego na PSK.
TLSCipherPSK13	Ciąg szyfrów dla OpenSSL 1.1.1 lub nowszego w TLS 1.3. Nadpisuje domyślne kryteria wyboru pakietów szyfrów dla szyfrowania opartego na PSK.
TLSCRLFile	Pełna ścieżka do pliku zawierającego unieważnione certyfikaty. Ten parametr jest używany do szyfrowanej komunikacji między komponentami Zabbix.
TLSFrontendAccept	Jakie połączenia przychodzące akceptować z frontend.
TLSFrontendCertIssuer	Dozwolony wystawca certyfikatu frontend.
TLSFrontendCertSubject	Dozwolony podmiot certyfikatu frontend.
TLSKeyFile	Pełna ścieżka do pliku zawierającego klucz prywatny serwera, używanego do szyfrowanej komunikacji między komponentami Zabbix.
TLSListen	Steruje TLS na gnieździe trappera.
TmpDir	Katalog tymczasowy.
TrapperTimeout	Określa limit czasu w sekundach dla: - pobierania danych historycznych z proxy Zabbix; - wysyłania danych konfiguracyjnych do proxy Zabbix; - wykonywania skryptów globalnych lub poleceń zdalnych na serwerze Zabbix.
TrendCacheSize	Rozmiar pamięci podręcznej trendów.
TrendFunctionCacheSize	Rozmiar pamięci podręcznej funkcji trendów.
UnavailableDelay	Określa, jak często sprawdzana jest dostępność hosta w okresie niedostępności.
UnreachableDelay	Określa, jak często sprawdzana jest dostępność hosta w okresie nieosiągalności.
UnreachablePeriod	Określa, po ilu sekundach nieosiągalności host jest traktowany jako niedostępny.
User	Porzuca uprawnienia na rzecz określonego, istniejącego użytkownika w systemie.
ValueCacheSize	Rozmiar pamięci podręcznej wartości historii.
Vault	Określa dostawcę vault.
VaultDBPath	Określa lokalizację, z której poświadczenia bazy danych powinny być pobierane za pomocą kluczy.
VaultPrefix	Niestandardowy prefiks dla ścieżki lub zapytania vault.
VaultTLSCertFile	Nazwa pliku certyfikatu SSL używanego do uwierzytelniania klienta.
VaultTLSKeyFile	Nazwa pliku klucza prywatnego SSL używanego do uwierzytelniania klienta.
VaultToken	Token uwierzytelniający HashiCorp vault.
VaultURL	Adres URL HTTP[S] serwera vault.
VMwareCacheSize	Rozmiar pamięci współdzielonej do przechowywania danych VMware.
VMwareFrequency	Opóźnienie w sekundach między pobieraniem danych z pojedynczej usługi VMware.
VMwarePerfFrequency	Opóźnienie w sekundach między pobieraniem statystyk liczników wydajności z pojedynczej usługi VMware.
VMwareTimeout	Maksymalna liczba sekund, przez którą kolektor vmware będzie czekał na odpowiedź z usługi VMware.

Parameter	Description
WebDriverURL	Adres URL HTTP[S] interfejsu WebDriver.
WebServiceURL	Adres URL HTTP[S] usługi web Zabbix w formacie <host:port>/report.

Wszystkie parametry są opcjonalne, chyba że wyraźnie zaznaczono, że dany parametr jest obowiązkowy.

Uwaga:

- Wartości domyślne odzwierciedlają wartości domyślne demona, a nie wartości w dostarczanych plikach konfiguracyjnych.
- Wartości obsługują zmienne środowiskowe.
- Zabbix obsługuje pliki konfiguracyjne tylko w kodowaniu UTF-8 bez BOM.
- Komentarze zaczynające się od „#” są obsługiwane tylko na początku linii.

Szczegóły parametrów

AlertScriptsPath

Lokalizacja niestandardowych skryptów alertów (zależy od zmiennej instalacyjnej *datadir* ustawianej podczas kompilacji).

Wartość domyślna: `/usr/local/share/zabbix/alertscripts`

AllowRoot

Zezwala serwerowi na działanie jako „root”. Jeśli opcja jest wyłączona, a serwer zostanie uruchomiony przez „root”, serwer spróbuje zamiast tego przełączyć się na użytkownika „zabbix”. Nie ma wpływu, jeśli został uruchomiony przez zwykłego użytkownika.

Domyślnie: 0
 Wartości: 0 - nie zezwalaj; 1 - zezwalaj

AllowSoftwareUpdateCheck

Zezwala interfejsowi użytkownika Zabbix na otrzymywanie informacji o aktualizacjach oprogramowania z zabbix.com.

Domyślnie: 1
 Wartości: 0 - nie zezwalaj; 1 - zezwalaj

AllowUnsupportedDBVersions

Zezwala serwerowi działać z nieobsługiwanymi wersjami bazy danych.

Domyślnie: 0
 Wartości: 0 - nie zezwalaj; 1 - zezwalaj

CacheSize

Rozmiar pamięci podręcznej konfiguracji, w bajtach. Rozmiar pamięci współdzielonej do przechowywania danych hostów, pozycji i wyzwalaczy.

Domyślnie: 32M
 Zakres: 128K-64G

CacheUpdateFrequency

Ten parametr określa, jak często Zabbix będzie aktualizował pamięć podręczną konfiguracji, w sekundach. Zobacz także opcje runtime control.

Wartość domyślna: 10
 Zakres: 1-3600

DBHost

Nazwa hosta bazy danych.
W przypadku MySQL `localhost` lub pusty ciąg znaków powoduje użycie gniazda. W przypadku PostgreSQL ustawienie pustego ciągu znaków powoduje użycie domyślnego gniazda domeny Unix; ustawienie ścieżki (np. /var/run/pgbouncer) powoduje użycie określonego gniazda domeny Unix.

Wartość domyślna: `localhost`

DBName

Nazwa bazy danych.

Wymagane: Tak

DBPassword

Hasło bazy danych. Zakomentuj ten wiersz, jeśli hasło nie jest używane.

DBPort

Port bazy danych, gdy nie jest używane domyślne gniazdo Unix-domain socket.[3]

Domyślnie dla MySQL: 3306

Domyślnie dla PostgreSQL: 5432

Zakres: 1024-65535

DBSchema

Nazwa schematu bazy danych. Używane dla PostgreSQL.

DBSocket

Ścieżka do pliku socket MySQL.[3]

DBUser

Użytkownik bazy danych.

DBTLSConnect

Ustawienie tej opcji na jedną z poniższych wartości wymusza użycie połączenia TLS z bazą danych:
required - połącz przy użyciu TLS
verify_ca - połącz przy użyciu TLS i zweryfikuj certyfikat
verify_full - połącz przy użyciu TLS, zweryfikuj certyfikat oraz sprawdź, czy tożsamość bazy danych określona przez DBHost odpowiada jej certyfikatowi

W przypadku MySQL, od wersji 5.7.11, oraz PostgreSQL obsługiwane są następujące wartości: `required`, `verify_ca`, `verify_full`.
W przypadku MariaDB, od wersji 10.2.6, obsługiwane są wartości `required` i `verify_full`.
Domyślnie opcja nie jest ustawiona, a zachowanie zależy od konfiguracji bazy danych.

DBTLSCAFile

Pełna ścieżka do pliku zawierającego certyfikaty nadrzędnego urzędu certyfikacji (CA) używane do weryfikacji certyfikatu bazy danych.

Obowiązkowe: nie (tak, jeśli DBTLSConnect ustawiono na *verify_ca* lub *verify_full*)

DBTLSCertFile

Pełna ścieżka do pliku zawierającego certyfikat serwer Zabbix używany do uwierzytelniania w bazie danych.

DBTLSKeyFile

Pełna ścieżka do pliku zawierającego klucz prywatny używany do uwierzytelniania w bazie danych.

DBTLSCipher

Lista szyfrów szyfrowania, które serwer Zabbix dopuszcza dla protokołów TLS do wersji TLS v1.2 włącznie. Obsługiwane tylko dla MySQL.

DBTLSCipher13

Lista szyfrów szyfrowania, na które serwer Zabbix zezwala dla protokołu TLS v1.3. Obsługiwane tylko dla MySQL, począwszy od wersji 8.0.16.

DebugLevel

Określ poziom debugowania:
0 - podstawowe informacje o uruchamianiu i zatrzymywaniu procesów Zabbix
1 - informacje krytyczne;
2 - informacje o błędach;
3 - ostrzeżenia;
4 - do debugowania (generuje dużo informacji);
5 - rozszerzone debugowanie (generuje jeszcze więcej informacji).
Zobacz także opcje kontroli w czasie działania.

Domyślnie: 3
 Zakres: 0-5

EnableGlobalScripts

Włącz skrypty globalne na serwerze Zabbix.
 Uwaga: wykonywanie skryptów globalnych jest domyślnie włączone. Jednak w przypadku nowych instalacji począwszy od Zabbix 7.0 parametr EnableGlobalScripts jest jawnie ustawiony na 0 (wyłączony).

Domyślnie: 1
 Wartości: 0 - wyłącz; 1 - włącz

ExportDir

Katalog do eksportu w czasie rzeczywistym zdarzeń, historii i trendów w formacie JSON rozdzielanym znakami nowej linii. Jeśli jest ustawiony, włącza eksport w czasie rzeczywistym.

ExportFileSize

Maksymalny rozmiar pojedynczego pliku eksportu w bajtach. Używane do rotacji, jeśli ustawiono `ExportDir`.

Wartość domyślna: 1G
 Zakres: 1M-1G

ExportType

Lista typów encji rozdzielonych przecinkami (zdarzenia, historia, trendy) dla eksportu w czasie rzeczywistym (domyślnie wszystkie typy). Prawidłowe tylko wtedy, gdy ustawiono ExportDir.
Uwaga: jeśli określono ExportType, ale nie określono ExportDir, jest to błąd konfiguracji i serwer nie uruchomi się.

Przykład eksportu historii i trendów:

```
ExportType=history,trends
```

Przykład tylko dla eksportu zdarzeń:

```
ExportType=events
```

ExternalScripts

Lokalizacja skryptów zewnętrznych (zależy od zmiennej instalacyjnej `datadir` ustawianej w czasie kompilacji).

Domyślnie: `/usr/local/share/zabbix/externalscripts`

Fping6Location

Lokalizacja fping6. Upewnij się, że plik binarny fping6 ma właściciela root oraz ustawioną flagę SUID. Pozostaw puste (”Fping6Location=”), jeśli narzędzie fping potrafi przetwarzać adresy IPv6.

Domyślnie: `/usr/sbin/fping6`

FpingLocation

Lokalizacja fping. Upewnij się, że plik binarny fping ma właściciela root oraz ustawioną flagę SUID.

Domyślnie: `/usr/sbin/fping`

FrontendAllowedIP

Lista adresów IP lub zakresów CIDR, z których dozwolone jest łączenie się z frontend. Jeśli ten parametr jest ustawiony, połączenie z frontend zostanie zaakceptowane tylko z adresów wymienionych tutaj. Domyślnie dla żądań frontend akceptowane są wszystkie połączenia. Jeśli obsługa IPv6 jest włączona, wtedy ’127.0.0.1’, ’::127.0.0.1’, ’::ffff:127.0.0.1’ są traktowane jednakowo, a ’::/0’ zezwoli na dowolny adres IPv4 lub IPv6. ’0.0.0.0/0’ może być użyte do zezwolenia na dowolny adres IPv4.

Przykład:

```
FrontendAllowedIP=127.0.0.1,192.168.1.0/24,::1,2001:db8::/32,zabbix.example.com
```

HANodeName

Nazwa węzła klastra wysokiej dostępności. Jeśli pole jest puste, serwer działa w trybie samodzielnym i tworzony jest węzeł z pustą nazwą.

HistoryCacheSize

Rozmiar pamięci podręcznej historii, w bajtach. Rozmiar pamięci współdzielonej do przechowywania danych historii.

Domyślnie: `16M`
 Zakres: 128K-16G

HistoryIndexCacheSize

Rozmiar pamięci podręcznej indeksu historii, w bajtach. Rozmiar pamięci współdzielonej do indeksowania danych historii przechowywanych w pamięci podręcznej historii. Rozmiar pamięci podręcznej indeksu wymaga około 100 bajtów do przechowywania w pamięci podręcznej jednej pozycji.

Domyślnie: `4M`
 Zakres: 128K-16G

HistoryStorageDateIndex

Włącz przetwarzanie wstępne wartości historii w magazynie historii, aby przechowywać wartości w różnych indeksach na podstawie daty.

Domyślnie: 0
 Wartości: 0 - wyłączone; 1 - włączone

HistoryStorageURL

Adres URL HTTP[S] magazynu historii. Ten parametr jest używany do konfiguracji Elasticsearch.

HistoryStorageTypes

Lista typów wartości oddzielonych przecinkami, które mają być wysyłane do magazynu historii. Ten parametr jest używany w konfiguracji Elasticsearch.

Domyślnie: `uint,dbl,str,log,text,json`

HousekeepingFrequency

Ten parametr określa, jak często Zabbix będzie wykonywać procedurę housekeeping, w godzinach. Housekeeping polega na usuwaniu nieaktualnych informacji z bazy danych.
Uwaga: Aby zapobiec przeciążeniu procesu housekeeper (na przykład gdy okresy historii i trendów zostaną znacznie skrócone), w jednym cyklu housekeeping usuwane są dla każdej pozycji nie więcej niż nieaktualne informacje z okresu równego 4-krotności wartości HousekeepingFrequency w godzinach. Tak więc, jeśli HousekeepingFrequency wynosi 1, w jednym cyklu zostaną usunięte nieaktualne informacje nie starsze niż 4 godziny (zaczynając od najstarszego wpisu).
Uwaga: Aby zmniejszyć obciążenie przy uruchamianiu serwera, housekeeping jest opóźniany o 30 minut po starcie serwera. Tak więc, jeśli HousekeepingFrequency wynosi 1, pierwsza procedura housekeeping po uruchomieniu serwera zostanie wykonana po 30 minutach, a następnie będzie powtarzana co godzinę.
Można wyłączyć automatyczny housekeeping, ustawiając HousekeepingFrequency na 0. W takim przypadku procedurę housekeeping można uruchomić tylko za pomocą opcji kontroli runtime *housekeeper_execute*, a okres nieaktualnych informacji usuwanych w jednym cyklu housekeeping wynosi 4-krotność okresu od ostatniego cyklu housekeeping, ale nie mniej niż 4 godziny i nie więcej niż 4 dni.
Zobacz także opcje runtime control oraz szczegóły dotyczące procedury housekeeping.

Domyślnie: 1
 Zakres: 0-24

Include

Możesz dołączyć pojedyncze pliki lub wszystkie pliki w katalogu w pliku konfiguracyjnym. Aby uwzględnić tylko odpowiednie pliki w określonym katalogu, obsługiwany jest znak wieloznaczny gwiazdki do dopasowywania wzorców. Zobacz uwagi specjalne dotyczące ograniczeń.

Przykład:

```
Include=/absolute/path/to/config/files/*.conf
```

JavaGateway

Adres IP (lub nazwa hosta) bramy Java gateway Zabbix. Wymagane tylko wtedy, gdy uruchomione są odpytywacze Java.

JavaGatewayPort

Port, na którym nasłuchuje Zabbix Java gateway.

Domyślnie: 10052
 Zakres: 1024-32767

ListenBacklog

Maksymalna liczba oczekujących połączeń w kolejce TCP.
Wartość domyślna jest stałą zakodowaną na stałe i zależy od systemu.
Maksymalna obsługiwana wartość również zależy od systemu; zbyt wysokie wartości mogą zostać po cichu obcięte do „maksimum określonego przez implementację”.

Domyślnie: SOMAXCONN
 Zakres: 0 - INT_MAX

ListenIP

Lista adresów IP rozdzielonych przecinkami, na których trapper powinien nasłuchiwać.
Jeśli ten parametr nie zostanie określony, trapper będzie nasłuchiwał na wszystkich interfejsach sieciowych.

Wartość domyślna: 0.0.0.0

ListenPort

Port nasłuchiwania dla trappera.

Domyślnie: 10051
 Zakres: 1024-32767

LoadModule

Moduł do załadowania podczas uruchamiania serwera. Moduły są używane do rozszerzania funkcjonalności serwera. Moduł musi znajdować się w katalogu określonym przez LoadModulePath lub ścieżka musi poprzedzać nazwę modułu. Jeśli poprzedzająca ścieżka jest bezwzględna (zaczyna się od ’/’), wtedy LoadModulePath jest ignorowane.
Formaty:
LoadModule=<module.so>
Loa
jest uwzględnienie wielu parametrów LoadModule.

LoadModulePath

Pełna ścieżka do lokalizacji modułów serwera. Wartość domyślna zależy od opcji kompilacji.

LogFile

Nazwa pliku dziennika.

Obowiązkowe: Tak, jeśli LogType jest ustawione na *file*; w przeciwnym razie nie

LogFileSize

Maksymalny rozmiar pliku dziennika w MB.
0 - wyłącza automatyczną rotację logów.
Uwaga: Jeśli zostanie osiągnięty limit rozmiaru pliku dziennika, a rotacja pliku nie powiedzie się z jakiegokolwiek powodu, istniejący plik dziennika zostanie obcięty i rozpocznie się jego zapis od nowa.

Wartość domyślna: 1
 Zakres: 0-1024
 Wymagane: Tak, jeśli LogType jest ustawiony na *file*; w przeciwnym razie nie

LogSlowQueries

Określa, jak długo może trwać zapytanie do bazy danych, zanim zostanie zapisane w logu, w milisekundach.
0 - nie zapisuj wolnych zapytań w logu.
Ta opcja jest włączana przy ustawieniu DebugLevel=3.

Domyślnie: 0
 Zakres: 0-3600000

LogType

Typ wyjścia logu:
file — zapisuje log do pliku określonego parametrem LogFile;
system — zapisuje log do syslog;
console — zapisuje log na standardowe wyjście.

Wartość domyślna: `file`

MaxConcurrentChecksPerPoller

Maksymalna liczba asynchronicznych kontroli, które mogą być wykonywane jednocześnie przez każdy proces odpytywania HTTP agent, agent lub SNMP. Zobacz StartHTTPAgentPollers, StartAgentPollers oraz StartSNMPPollers.

Wartość domyślna: 1000
 Zakres: 1-1000

MaxHousekeeperDelete

Tabela „housekeeper" zawiera „zadania" dla procedury housekeeping w formacie: `[housekeeperid]`, `[object]`, `[objectid]`.
 Nie więcej niż `MaxHousekeeperDelete` wierszy z tabel `history`, `history_str`, `history_log`, `history_uint`, `history_text`, `history_bin`, `history_json`, `trends`, `trends_uint` oraz `problem` zostanie usuniętych dla jednego zadania w jednym cyklu housekeeping.
 Jeśli ustawiono 0, wówczas nie jest używany żaden limit. W takim przypadku musisz wiedzieć, co robisz, aby nie przeciążyć bazy danych.[2]
Ten parametr ma zastosowanie wyłącznie do usuwania danych pozostawionych przez już usunięte pozycje.
 Zobacz także szczegóły dotyczące procedury housekeeping.

Wartość domyślna: 5000
 Zakres: 0-1000000

NodeAddress

Adres IP lub nazwa hosta z opcjonalnym portem, aby zastąpić sposób, w jaki frontend powinien łączyć się z serwerem.
Format: <adres>[:<port>]

Jeśli adres IP lub nazwa hosta nie są ustawione, zostanie użyta wartość ListenIP. Jeśli ListenIP nie jest ustawione, zostanie użyta wartość `localhost`.
Jeśli port nie jest ustawiony, zostanie użyta wartość ListenPort. Jeśli ListenPort nie jest ustawione, zostanie użyta wartość 10051.

Tę opcję można zastąpić adresem określonym w konfiguracji frontendu.

Zobacz także: parametr HANodeName; Włączanie wysokiej dostępności.

Wartość domyślna: `localhost:10051`

PidFile

Nazwa pliku PID.

Wartość domyślna: `/tmp/zabbix_server.pid`

ProblemHousekeepingFrequency

Określa, jak często Zabbix będzie usuwać problemy dla usuniętych wyzwalaczy, w sekundach.
 Zobacz także szczegóły dotyczące procedury housekeeping.

Wartość domyślna: 60
 Zakres: 1-3600

ProxyConfigFrequency

Określa, jak często serwer Zabbix wysyła dane konfiguracyjne do proxy Zabbix, w sekundach. Używane tylko dla proxy w trybie pasywnym.

Domyślnie: 10
 Zakres: 1-604800

ProxyDataFrequency

Określa, jak często serwer Zabbix żąda danych historii od proxy Zabbix, w sekundach. Używane tylko dla proxy w trybie pasywnym.

Domyślnie: 1
 Zakres: 1-3600

ServiceManagerSyncFrequency

Określa, jak często Zabbix będzie synchronizować konfigurację menedżera usług, w sekundach.

Domyślnie: 60
 Zakres: 1-3600

SMSDevices

Lista plików modemów oddzielonych przecinkami, które mogą być używane przez serwer Zabbix.
Wysyłanie wiadomości SMS nie jest możliwe, jeśli ten parametr nie jest ustawiony.

Przykład:

```
SMSDevices=/dev/ttyUSB0,/dev/ttyUSB1
```

SNMPTrapperFile

Plik tymczasowy używany do przekazywania danych z demona pułapek SNMP do serwera.
Musi być taki sam jak w pliku konfiguracyjnym zabbix_trap_receiver.pl lub SNMPTT.

Domyślnie: `/tmp/zabbix_traps.tmp`

SocketDir

Katalog do przechowywania gniazd IPC używanych przez wewnętrzne usługi Zabbix.

Wartość domyślna: `/tmp`

SourceIP

Źródłowy adres IP dla:

- połączeń wychodzących do Zabbix proxy i Zabbix agent
- połączeń bezagentowych (VMware, SSH, JMX, SNMP, Telnet i prostych testów)
- połączeń HTTP agent
- żądań HTTP JavaScript dla pozycji skryptowych
- żądań HTTP JavaScript dla preprocessing
- wysyłania e-maili z powiadomieniami (połączenia do serwera SMTP)
- powiadomień webhook (połączenia HTTP JavaScript)
- połączeń do Vault

SSHKeyLocation

Lokalizacja kluczy publicznych i prywatnych dla kontroli SSH oraz akcji.

SSLCertLocation

Lokalizacja plików certyfikatów klienta SSL do uwierzytelniania klienta.
Ten parametr jest używany tylko w monitorowaniu WWW.

SSLKeyLocation

Lokalizacja plików klucza prywatnego SSL do uwierzytelniania klienta.
Ten parametr jest używany tylko w monitorowaniu WWW.

SSLCALocation

Nadpisuje lokalizację plików urzędu certyfikacji (CA) używanych do weryfikacji certyfikatu SSL serwera. Jeśli nie jest ustawiony, użyty zostanie katalog systemowy.
Zwróć uwagę, że wartość tego parametru zostanie ustawiona jako opcja libcurl CURLOPT_CAPATH. W przypadku wersji libcurl wcześniejszych niż 7.42.0 ma to skutek tylko wtedy, gdy libcurl został skompilowany do użycia OpenSSL. Więcej informacji można znaleźć na stronie cURL.
Ten parametr jest używany w monitorowaniu WWW oraz przy uwierzytelnianiu SMTP.

StartAgentPollers

Liczba wstępnie rozwidlonych instancji pollerów Zabbix agent. Zobacz MaxConcurrentChecksPerPoller.

Domyślnie: 1
 Zakres: 0-1000

StartAlerters

Liczba wstępnie rozwidlonych instancji alerterów.

Domyślnie: 3
 Zakres: 1-100

StartBrowserPollers

Liczba wstępnie rozwidlonych instancji pollerów pozycji przeglądarkowych.

Domyślnie: 1
 Zakres: 0-1000

StartConnectors

Liczba wstępnie rozwidlonych instancji procesów roboczych connectora. Proces menedżera connectora jest uruchamiany automatycznie po uruchomieniu procesu roboczego connectora.

Domyślnie: 0
 Zakres: 0-1000

StartDBSyncers

Liczba wstępnie rozwidlonych instancji synchronizatorów historii.
Uwaga: Należy zachować ostrożność przy zmianie tej wartości, ponieważ jej zwiększenie może przynieść więcej szkody niż pożytku. Orientacyjnie, wartość domyślna powinna wystarczyć do obsługi do 4000 NVPS.

Domyślnie: 4
 Zakres: 1-100

StartDiscoverers

Liczba wstępnie rozwidlonych instancji workerów wykrywania[1].

Domyślnie: 5
 Zakres: 0-1000

StartEscalators

Liczba wstępnie rozwidlonych instancji eskalatorów.

Domyślnie: 1
 Zakres: 1-100

StartHistoryPollers

Liczba wstępnie utworzonych instancji history pollers.
Wymagane tylko dla kontroli obliczanych.

Domyślnie: 5
 Zakres: 0-1000

StartHTTPAgentPollers

Liczba wstępnie rozwidlonych instancji pollerów HTTP agent. Zobacz MaxConcurrentChecksPerPoller.

Domyślnie: 1
 Zakres: 0-1000

StartHTTPPollers

Liczba wstępnie rozwidlonych instancji HTTP pollers[1].

Domyślnie: 1
 Zakres: 0-1000

StartIPMIPollers

Liczba wstępnie rozwidlonych instancji modułów odpytujących IPMI.

Wartość domyślna: 0
 Zakres: 0-1000

StartJavaPollers

Liczba wstępnie rozwidlonych instancji Java pollers[1].

Domyślnie: 0
 Zakres: 0-1000

StartLLDProcessors

Liczba wstępnie rozwidlonych instancji workerów niskopoziomowego wykrywania (LLD)[1].
Proces menedżera LLD jest uruchamiany automatycznie po uruchomieniu workera LLD.

Domyślnie: 2
 Zakres: 1-100

StartODBCPollers

Liczba wstępnie rozwidlonych instancji ODBC pollers[1].

Domyślnie: 1
 Zakres: 0-1000

StartPingers

Liczba wstępnie rozwidlonych instancji ICMP pingers[1].

Domyślnie: 1
 Zakres: 0-1000

StartPollersUnreachable

Liczba wstępnie rozwidlonych instancji pollerów dla nieosiągalnych hostów (w tym IPMI i Java)[1].
Jeśli uruchomione są zwykłe pollery, pollery IPMI lub pollery Java, musi działać co najmniej jeden poller dla nieosiągalnych hostów.

Domyślnie: 1
 Zakres: 0-1000

StartPollers

Liczba wstępnie utworzonych instancji pollerów[1].

Domyślnie: 5
 Zakres: 0-1000

StartPreprocessors

Liczba wstępnie uruchomionych instancji wątków worker[1] przetwarzania wstępnego powinna być ustawiona na wartość nie mniejszą niż liczba dostępnych rdzeni CPU. Należy ustawić więcej workerów, jeśli przetwarzanie wstępne nie jest ograniczone przez CPU i obejmuje wiele żądań sieciowych.

Domyślnie: 16
 Zakres: 1-1000

StartProxyPollers

Liczba wstępnie utworzonych instancji pollerów dla pasywnych proxy[1].

Domyślnie: 1
 Zakres: 0-250

StartReportWriters

Liczba wstępnie rozwidlonych instancji modułów zapisujących raporty.
Jeśli ustawiono 0, generowanie raportów według harmonogramu jest wyłączone.
Proces menedżera raportów jest uruchamiany automatycznie po uruchomieniu modułu zapisującego raporty.

Wartość domyślna: 0
 Zakres: 0-100

StartSNMPPollers

Liczba wstępnie utworzonych instancji SNMP pollers. Zobacz MaxConcurrentChecksPerPoller.

Domyślnie: 1
 Zakres: 0-1000

StartSNMPTrapper

Jeśli ustawiono na 1, zostanie uruchomiony proces SNMP trapper.

Domyślnie: 0
 Zakres: 0-1

StartTimers

Liczba wstępnie rozwidlonych instancji timerów.
Timery przetwarzają okresy utrzymania.

Wartość domyślna: 1
 Zakres: 1-1000

StartTrappers

Liczba wstępnie rozwidlonych instancji trapperów[1].
Trappery akceptują połączenia przychodzące z Zabbix sender, aktywnych agentów i aktywnych proxy.

Domyślnie: 5
 Zakres: 0-1000

StartVMwareCollectors

Liczba wstępnie utworzonych instancji VMware collector.

Domyślnie: 0
 Zakres: 0-250

StatsAllowedIP

Lista adresów IP instancji zewnętrznych Zabbix, rozdzielonych przecinkami, opcjonalnie w notacji CIDR, lub nazw DNS. Żądanie statystyk będzie akceptowane tylko z adresów wymienionych tutaj. Jeśli ten parametr nie jest ustawiony, żadne żądania statystyk nie będą akceptowane.
Jeśli obsługa IPv6 jest włączona, wtedy '127.0.0.1', '::127.0.0.1', '::ffff:127.0.0.1' są traktowane jednakowo, a '::/0' zezwoli na dowolny adres IPv4 lub IPv6. '0.0.0.0/0' może być użyte do zezwolenia na dowolny adres IPv4.

Przykład:

```
StatsAllowedIP=127.0.0.1,192.168.1.0/24,::1,2001:db8::/32,zabbix.example.com
```

Timeout

Określa, jak długo czekać (w sekundach) na ustanowienie połączenia i wymianę danych z Zabbix proxy, agent, usługą web oraz starszymi kontrolami SNMP (pojedynczy numer OID lub ciąg znaków).

Ten parametr definiuje czas trwania różnych operacji komunikacyjnych:

- zdalne wykonywanie poleceń na Zabbix agent
- wykonywanie poleceń SSH/Telnet
- żądania do usługi web Zabbix
- limit czasu komunikacji dla żądania testowego typu nośnika oraz metody `history.push`

- ponowne planowanie pozycji, gdy interfejs IPMI staje się niedostępny
- wysyłanie odpowiedzi do Zabbix proxy w przypadku niepowodzenia wymiany danych z powodu problemów z uprawnieniami lub szyfrowaniem
- limit czasu dla asynchronicznych gniazd IPC oraz opcji kontroli w czasie działania
- połączenia JMX
- pobieranie statystyk ze zdalnego Zabbix proxy lub serwer
- wysyłanie odpowiedzi do Zabbix frontend
- asynchroniczne żądania DNS pollera
- odpowiedź dla heartbeat aktywnej kontroli
- pobieranie danych Zabbix agent (wartości) od aktywnych agentów
- pobieranie danych z Zabbix sender
- odpowiedź, gdy trapper nie może przetworzyć żądania
- wysyłanie listy aktywnych kontroli do Zabbix agent

Ten limit czasu **nie** będzie używany dla tych kontroli, które mają skonfigurowane ustawienia elastycznego limitu czasu we frontendzie (na poziomie globalnym, proxy lub pojedynczej pozycji).
Na przykład pozycje SNMP `walk[OID]` i `get[OID]` używają limitu czasu skonfigurowanego we frontendzie; starsze kontrole SNMP nadal używają wartości limitu czasu serwera.

Domyślnie: 3
 Zakres: 1-30

TLSCAFile

Pełna ścieżka do pliku zawierającego certyfikaty nadrzędnych urzędów certyfikacji (CA) do weryfikacji certyfikatu peera, używanego do szyfrowanej komunikacji między komponentami Zabbix.

TLSCertFile

Pełna ścieżka do pliku zawierającego certyfikat serwera lub łańcuch certyfikatów, używanego do szyfrowanej komunikacji między komponentami Zabbix.

TLSCipherAll

Ciąg priorytetów GnuTLS lub ciąg szyfrów OpenSSL (TLS 1.2). Zastępuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na certyfikatach i PSK.

Przykład:

```
TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256
```

TLSCipherAll13

Ciąg szyfrów dla OpenSSL 1.1.1 lub nowszego w TLS 1.3. Zastępuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na certyfikatach i PSK.

Przykład dla GnuTLS:

```
NONE:+VERS-TLS1.2:+ECDHE-RSA:+RSA:+ECDHE-PSK:+PSK:+AES-128-GCM:+AES-128-CBC:+AEAD:+SHA256:+SHA1:+CURVE-ALL
```

Przykład dla OpenSSL:

```
EECDH+aRSA+AES128:RSA+aRSA+AES128:kECDHEPSK+AES128:kPSK+AES128
```

TLSCipherCert

Ciąg priorytetów GnuTLS lub ciąg szyfrów OpenSSL (TLS 1.2). Nadpisuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na certyfikatach.

Przykład dla GnuTLS:

```
NONE:+VERS-TLS1.2:+ECDHE-RSA:+RSA:+AES-128-GCM:+AES-128-CBC:+AEAD:+SHA256:+SHA1:+CURVE-ALL:+COMP-NULL:+SIG
```

Przykład dla OpenSSL:

```
EECDH+aRSA+AES128:RSA+aRSA+AES128
```

TLSCipherCert13

Ciąg szyfrów dla OpenSSL 1.1.1 lub nowszego w TLS 1.3. Zastępuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na certyfikatach.

TLSCipherPSK

Ciąg priorytetów GnuTLS lub ciąg szyfrów OpenSSL (TLS 1.2). Nadpisuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na PSK.

Przykład dla GnuTLS:

```
NONE:+VERS-TLS1.2:+ECDHE-PSK:+PSK:+AES-128-GCM:+AES-128-CBC:+AEAD:+SHA256:+SHA1:+CURVE-ALL:+COMP-NULL:+SIG
```

Przykład dla OpenSSL:

```
kECDHEPSK+AES128:kPSK+AES128
```

TLSCipherPSK13

Ciąg szyfrów dla OpenSSL 1.1.1 lub nowszego w TLS 1.3. Nadpisuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na PSK.

Przykład:

```
TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256
```

TLSCRLFile

Pełna ścieżka do pliku zawierającego unieważnione certyfikaty. Ten parametr jest używany do szyfrowanej komunikacji między komponentami Zabbix.

TLSFrontendAccept

Jakie połączenia przychodzące akceptować z frontend.

Można określić wiele wartości, oddzielonych przecinkami:

- unencrypted - akceptuj połączenia bez szyfrowania.
- cert - akceptuj połączenia zabezpieczone TLS i certyfikatem.

Wartość domyślna: `unencrypted`

TLSFrontendCertIssuer

Dozwolony wystawca certyfikatu frontend.

TLSFrontendCertSubject

Dozwolony temat certyfikatu frontend.

TLSKeyFile

Pełna ścieżka do pliku zawierającego klucz prywatny serwera, używany do szyfrowanej komunikacji między komponentami Zabbix.

TLSListen

Steruje TLS na gnieździe trappera.

Obsługiwane wartości:

- required - akceptuj tylko połączenia TLS

TmpDir

Katalog tymczasowy.

Domyślnie: `/tmp`

TrapperTimeout

Określa limit czasu w sekundach dla:

- pobierania danych historycznych z proxy Zabbix
- wysyłania danych konfiguracyjnych do proxy Zabbix
- wykonywania skryptów globalnych lub poleceń zdalnych na serwerze Zabbix

Domyślnie: 300
 Zakres: 1-300

TrendCacheSize

Rozmiar pamięci podręcznej trendów, w bajtach.
Rozmiar pamięci współdzielonej do przechowywania danych trendów.

Domyślnie: `4M`
 Zakres: 128K-16G

TrendFunctionCacheSize

Rozmiar pamięci podręcznej funkcji trendu, w bajtach.
Rozmiar pamięci współdzielonej do buforowania obliczonych danych funkcji trendu.

Domyślnie: `4M`
 Zakres: 128K-2G

UnavailableDelay

Określa, jak często sprawdzana jest dostępność hosta w okresie niedostępności, w sekundach.

Domyślnie: 60
 Zakres: 1-3600

UnreachableDelay

Określa, jak często sprawdzana jest dostępność hosta w okresie nieosiągalności, w sekundach.

Domyślnie: 15
 Zakres: 1-3600

UnreachablePeriod

Określa, po ilu sekundach nieosiągalności host jest traktowany jako niedostępny.

Domyślnie: 45
 Zakres: 1-3600

Użytkownik

Obniż uprawnienia do określonego, istniejącego użytkownika w systemie.
Ma to skutek tylko w przypadku uruchomienia jako 'root' i przy wyłączonym AllowRoot.

Domyślnie: `zabbix`

ValueCacheSize

Rozmiar pamięci podręcznej wartości historii, w bajtach.
Rozmiar pamięci współdzielonej do buforowania żądań danych historii pozycji.
Ustawienie wartości 0 wyłącza pamięć podręczną wartości (niezalecane).
Gdy pamięć podręczna wartości wyczerpie pamięć współdzieloną, co 5 minut do dziennika serwera zapisywany jest komunikat ostrzegawczy.

Domyślnie: `8M`
 Zakres: 0,128K-64G

Vault

Określa dostawcę vault:
HashiCorp - HashiCorp KV Secrets Engine wersja 2
CyberArk - CyberArk Central Credential Provider
Musi odpowiadać dostawcy vault ustawionemu we frontend.

Wartość domyślna: `HashiCorp`

VaultDBPath

Ścieżka lub zapytanie Vault, zależnie od używanego Vault, skąd po kluczach zostaną pobrane poświadczenia do bazy danych.

Kluczami używanymi dla HashiCorp są 'password' i 'username'.

Przykładowa ścieżka z VaultPrefix=/v1/secret/data/zabbix/:

```
database
```

Przykładowa ścieżka bez VaultPrefix:

```
secret/zabbix/database
```

Kluczami używanymi dla CyberArk są 'Content' i 'UserName'.

Przykład:

```
AppID=zabbix_server&Query=Safe=passwordSafe;Object=zabbix_server_database
```

Ta opcja może być używana tylko wtedy, gdy DBUser i DBPassword nie są określone.

VaultPrefix

Niestandardowy prefiks dla ścieżki lub zapytania Vault, zależnie od Vault. Jeśli nie zostanie określony, zostaną użyte najbardziej odpowiednie wartości domyślne.
Należy pamiętać, że w przypadku HashiCorp po mountpoint automatycznie dodawane jest „data", jeśli VaultPrefix nie jest określony.

Przykładowy prefiks dla Hashicorp:

```
v1/secret/data/zabbix/
```

Przykładowy prefiks dla Cyberark:

```
/AIMWebService/api/Accounts?
```

VaultTLSCertFile

Nazwa pliku certyfikatu SSL używanego do uwierzytelniania klienta
 Plik certyfikatu musi być w formacie PEM1.
 Jeśli plik certyfikatu zawiera również klucz prywatny, pozostaw pole pliku klucza SSL puste.
 Katalog zawierający ten plik jest określony przez parametr konfiguracyjny SSLCertLocation.
Ta opcja może zostać pominięta, ale jest zalecana dla skarbca CyberArkCCP.

VaultTLSKeyFile

Nazwa pliku prywatnego klucza SSL używanego do uwierzytelniania klienta.
 Plik prywatnego klucza musi być w formacie PEM1.
 Katalog zawierający ten plik jest określony przez parametr konfiguracyjny SSLKeyLocation.
Ta opcja może zostać pominięta, ale jest zalecana dla skarbca CyberArkCCP.

VaultToken

Token uwierzytelniający HashiCorp Vault, który powinien zostać wygenerowany wyłącznie dla serwera Zabbix z uprawnieniami tylko do odczytu dla ścieżek określonych w makrach Vault oraz uprawnieniami tylko do odczytu dla ścieżki określonej w opcjonalnym parametrze konfiguracyjnym VaultDBPath.
Zdefiniowanie jednocześnie VaultToken i zmiennej środowiskowej VAULT_TOKEN jest błędem.

Obowiązkowe: Tak, jeśli Vault jest ustawiony na *HashiCorp*; w przeciwnym razie nie

VaultURL

Adres URL HTTP[S] serwera vault. Jeśli SSLCALocation nie jest określone, zostanie użyty katalog certyfikatów CA dla całego systemu.

Domyślnie: `https://127.0.0.1:8200`

VMwareCacheSize

Rozmiar pamięci współdzielonej do przechowywania danych VMware.
Do monitorowania użycia pamięci podręcznej VMware można użyć wewnętrznej kontroli VMware zabbix[vmware,buffer,...] (zobacz Kontrole wewnętrzne).
Należy pamiętać, że pamięć współdzielona nie jest przydzielana, jeśli nie skonfigurowano do uruchomienia żadnych instancji kolektora vmware.

Wartość domyślna: 8M
 Zakres: 256K-2G

VMwareFrequency

Opóźnienie w sekundach między pobieraniem danych z pojedynczej usługi VMware.
To opóźnienie powinno być ustawione na najmniejszy interwał aktualizacji dowolnej pozycji monitorowania VMware.

Domyślnie: 60
 Zakres: 10-86400

VMwarePerfFrequency

Opóźnienie w sekundach pomiędzy pobieraniem statystyk liczników wydajności z pojedynczej usługi VMware. To opóźnienie powinno być ustawione na najmniejszy interwał aktualizacji dowolnej monitorującej VMware pozycji, która używa liczników wydajności VMware.

Domyślnie: 60
 Zakres: 10-86400

VMwareTimeout

Maksymalna liczba sekund, przez którą kolektor vmware będzie oczekiwać na odpowiedź od usługi VMware (vCenter lub hipernadzorcy ESX).

Domyślnie: 10
 Zakres: 1-300

WebServiceURL

Adres URL HTTP[S] do usługi internetowej Zabbix w formacie `http[s]://host:port/report`.

Przykład:

```
WebServiceURL=http://localhost:10053/report
```

Uwaga: schemat (`http://`) można pominąć tylko w przypadku połączeń bez TLS (HTTP); jeśli skonfigurowano TLS, należy użyć `https://`.

WebDriverURL

Adres URL HTTP[S] interfejsu WebDriver.

Przykład (używany z samodzielnym serwerem Selenium WebDriver):

```
WebDriverURL=http://localhost:4444
```

Przypisy

[1] Należy pamiętać, że zbyt duża liczba procesów zbierania danych (pollerów, pollerów niedostępnych hostów, pollerów ODBC, pollerów HTTP, pollerów Java, pingerów, trapperów, proxypollerów) wraz z menedżerem IPMI, trapperem SNMP, workerami

przetwarzania wstępnego oraz workerami wykrywania może wyczerpać limit deskryptorów plików na proces dla menedżera przetwarzania wstępnego.

Warning:
Wyczerpanie limitu deskryptorów plików spowoduje zatrzymanie serwera Zabbix, zwykle krótko po uruchomieniu, choć czasami może to nastąpić później. Aby uniknąć takich problemów, przejrzyj plik konfiguracyjny serwera Zabbix, aby zoptymalizować liczbę równoległych kontroli i procesów. Dodatkowo, jeśli to konieczne, upewnij się, że limit deskryptorów plików jest ustawiony wystarczająco wysoko, sprawdzając i dostosowując limity systemowe.

[2] Gdy usuwanych jest wiele pozycji, zwiększa to obciążenie bazy danych, ponieważ housekeeper będzie musiał usunąć wszystkie dane historyczne, które te pozycje posiadały. Na przykład, jeśli trzeba usunąć tylko 1 prototyp pozycji z szablonu, ale ten szablon jest podłączony do 50 hostów, a dla każdego hosta prototyp jest rozwijany do 100 rzeczywistych pozycji, łącznie trzeba usunąć 5000 pozycji (1*50*100). Jeśli dla MaxHousekeeperDelete ustawiono 500 (MaxHousekeeperDelete=500), proces housekeeper będzie musiał usunąć do 2500000 wartości (5000*500) dla usuniętych pozycji z tabel historii i trendów w jednym cyklu.

[3] DBSocket i DBPort wzajemnie się wykluczają w konfiguracji serwera. Należy określić tylko jeden z nich albo pozostawić oba niezdefiniowane.

2 Zabbix proxy

Przegląd

Parametry obsługiwane przez plik konfiguracyjny Zabbix proxy (zabbix_proxy.conf) są wymienione w tej sekcji.

Parametry są wymienione bez dodatkowych informacji. Kliknij parametr, aby zobaczyć pełne szczegóły.

Parameter	Description
AllowRoot	Zezwala na uruchamianie proxy jako „root”.
AllowUnsupportedDBVersions	Zezwala proxy na pracę z nieobsługiwanymi wersjami bazy danych.
CacheSize	Rozmiar pamięci podręcznej konfiguracji.
ConfigFrequency	Ten parametr jest **przestarzały** (**deprecated**) (zamiast niego użyj ProxyConfigFrequency). Określa, jak często proxy pobiera dane konfiguracyjne z serwer Zabbix, w sekundach.
DataSenderFrequency	Proxy będzie wysyłać zebrane dane do serwer co N sekund.
DBHost	Nazwa hosta bazy danych.
DBName	Nazwa bazy danych lub ścieżka do pliku bazy danych dla SQLite3.
DBPassword	Hasło bazy danych.
DBPort	Port bazy danych, gdy nie jest używane lokalne gniazdo.
DBSchema	Nazwa schematu bazy danych. Używane dla PostgreSQL.
DBSocket	Ścieżka do pliku gniazda MySQL.
DBUser	Użytkownik bazy danych.
DBTLSConnect	Ustawienie tej opcji na określoną wartość wymusza użycie połączenia TLS z bazą danych.
DBTLSCAFile	Pełna ścieżka do pliku zawierającego certyfikaty głównych urzędów certyfikacji (CA) do weryfikacji certyfikatu bazy danych.
DBTLSCertFile	Pełna ścieżka do pliku zawierającego certyfikat Zabbix proxy do uwierzytelniania w bazie danych.
DBTLSKeyFile	Pełna ścieżka do pliku zawierającego klucz prywatny do uwierzytelniania w bazie danych.
DBTLSCipher	Lista szyfrów, które Zabbix proxy dopuszcza dla protokołów TLS do wersji TLS v1.2 włącznie. Obsługiwane tylko dla MySQL.
DBTLSCipher13	Lista pakietów szyfrów, które Zabbix proxy dopuszcza dla protokołu TLS v1.3. Obsługiwane tylko dla MySQL, począwszy od wersji 8.0.16.
DebugLevel	Poziom debugowania.
EnableRemoteCommands	Określa, czy zdalne polecenia z serwer Zabbix są dozwolone.
ExternalScripts	Lokalizacja zewnętrznych skryptów.
Fping6Location	Lokalizacja fping6.
FpingLocation	Lokalizacja fping.
HistoryCacheSize	Rozmiar pamięci podręcznej historii.
HistoryIndexCacheSize	Rozmiar pamięci podręcznej indeksu historii.
Hostname	Unikalna nazwa proxy z rozróżnianiem wielkości liter.
HostnameItem	Pozycja używana do ustawienia Hostname, jeśli nie jest zdefiniowane.
HousekeepingFrequency	Określa, jak często Zabbix będzie wykonywać procedurę housekeeping, w godzinach.
Include	Możesz dołączyć pojedyncze pliki lub wszystkie pliki z katalogu do pliku konfiguracyjnego.
JavaGateway	Adres IP (lub nazwa hosta) Zabbix Java gateway.
JavaGatewayPort	Port, na którym nasłuchuje Zabbix Java gateway.
ListenBacklog	Maksymalna liczba oczekujących połączeń w kolejce TCP.

Parameter	Description
ListenIP	Lista adresów IP oddzielonych przecinkami, na których trapper powinien nasłuchiwać.
ListenPort	Port nasłuchiwania dla trappera.
LoadModule	Moduł do załadowania przy uruchamianiu proxy.
LoadModulePath	Pełna ścieżka do lokalizacji modułów proxy.
LogFile	Nazwa pliku dziennika.
LogFileSize	Maksymalny rozmiar pliku dziennika.
LogRemoteCommands	Włącza rejestrowanie wykonywanych poleceń powłoki jako ostrzeżeń.
LogSlowQueries	Jak długo może trwać zapytanie do bazy danych, zanim zostanie zapisane w dzienniku.
LogType	Typ wyjścia dziennika.
MaxConcurrentChecksPerPoller	Maksymalna liczba asynchronicznych kontroli, które mogą być wykonywane jednocześnie przez każdy poller HTTP agent, poller agent lub poller SNMP.
PidFile	Nazwa pliku PID.
ProxyBufferMode	Określa mechanizm przechowywania danych historii, wykrywania i autorejestracji (dysk/pamięć/hybrydowy).
ProxyConfigFrequency	Określa, jak często proxy pobiera dane konfiguracyjne z serwer Zabbix, w sekundach.
ProxyLocalBuffer	Proxy będzie przechowywać dane lokalnie przez N godzin, nawet jeśli dane zostały już zsynchronizowane z serwer.
ProxyMemoryBufferAge	Maksymalny wiek danych w buforze pamięci proxy, w sekundach.
ProxyMemoryBufferSize	Rozmiar pamięci współdzielonej dla zebranych danych historii, wykrywania i autorejestracji.
ProxyMode	Tryb pracy proxy (active/passive).
ProxyOfflineBuffer	Proxy będzie przechowywać dane przez N godzin w przypadku braku łączności z serwer Zabbix.
Server	Jeśli ProxyMode jest ustawione na tryb active: adres IP lub nazwa DNS serwer Zabbix (address:port) albo klaster (address:port;address2:port), z którego pobierane są dane konfiguracyjne i do którego wysyłane są dane. Jeśli ProxyMode jest ustawione na tryb passive: lista adresów IP serwer Zabbix oddzielonych przecinkami, opcjonalnie w notacji CIDR, lub nazw DNS.
SNMPTrapperFile	Plik tymczasowy używany do przekazywania danych z demona pułapek SNMP do proxy.
SocketDir	Katalog do przechowywania gniazd IPC używanych przez wewnętrzne usługi Zabbix.
SourceIP	Źródłowy adres IP.
SSHKeyLocation	Lokalizacja kluczy publicznych i prywatnych dla kontroli SSH i akcji.
SSLCertLocation	Lokalizacja plików certyfikatów klienta SSL do uwierzytelniania klienta.
SSLKeyLocation	Lokalizacja plików kluczy prywatnych SSL do uwierzytelniania klienta.
SSLCALocation	Nadpisuje lokalizację plików urzędu certyfikacji (CA) do weryfikacji certyfikatu serwera SSL.
StartAgentPollers	Liczba wstępnie rozwidlonych instancji asynchronicznych pollerów Zabbix agent.
StartBrowserPollers	Liczba wstępnie rozwidlonych instancji pollerów pozycji przeglądarkowych.
StartDBSyncers	Liczba wstępnie rozwidlonych instancji synchronizatorów historii.
StartDiscoverers	Liczba wstępnie rozwidlonych instancji procesów wykrywania.
StartHTTPAgentPollers	Liczba wstępnie rozwidlonych instancji asynchronicznych pollerów HTTP agent.
StartHTTPPollers	Liczba wstępnie rozwidlonych instancji pollerów HTTP.
StartIPMIPollers	Liczba wstępnie rozwidlonych instancji pollerów IPMI.
StartJavaPollers	Liczba wstępnie rozwidlonych instancji pollerów Java.
StartODBCPollers	Liczba wstępnie rozwidlonych instancji pollerów ODBC.
StartPingers	Liczba wstępnie rozwidlonych instancji pingerów ICMP.
StartPollersUnreachable	Liczba wstępnie rozwidlonych instancji pollerów dla nieosiągalnych hostów (w tym IPMI i Java).
StartPollers	Liczba wstępnie rozwidlonych instancji pollerów.
StartPreprocessors	Liczba wstępnie uruchomionych instancji procesów wstępnego przetwarzania.
StartSNMPPollers	Liczba wstępnie rozwidlonych instancji asynchronicznych pollerów SNMP.
StartSNMPTrapper	Jeśli ustawione na 1, zostanie uruchomiony proces trappera SNMP.
StartTrappers	Liczba wstępnie rozwidlonych instancji trapperów.
StartVMwareCollectors	Liczba wstępnie rozwidlonych instancji kolektorów VMware.
StatsAllowedIP	Lista adresów IP oddzielonych przecinkami, opcjonalnie w notacji CIDR, lub nazw DNS zewnętrznych instancji Zabbix. Żądanie statystyk będzie akceptowane tylko z adresów wymienionych tutaj.
Timeout	Określa, jak długo czekać (w sekundach) na ustanowienie połączenia i wymianę danych z Zabbix proxy, agent, usługą webową oraz dla kontroli SNMP (z wyjątkiem pozycji SNMP `walk[OID]` i `get[OID]`).
TLSAccept	Jakie połączenia przychodzące od serwer Zabbix mają być akceptowane.
TLSCAFile	Pełna ścieżka do pliku zawierającego certyfikaty głównych urzędów certyfikacji (CA) do weryfikacji certyfikatu drugiej strony, używanego do szyfrowanej komunikacji między komponentami Zabbix.
TLSCertFile	Pełna ścieżka do pliku zawierającego certyfikat serwera lub łańcuch certyfikatów, używanego do szyfrowanej komunikacji między komponentami Zabbix.

Parameter	Description
TLSCipherAll	Ciąg priorytetów GnuTLS lub ciąg szyfrów OpenSSL (TLS 1.2). Nadpisuje domyślne kryteria wyboru pakietów szyfrów dla szyfrowania opartego na certyfikatach i PSK.
TLSCipherAll13	Ciąg szyfrów dla OpenSSL 1.1.1 lub nowszego w TLS 1.3. Nadpisuje domyślne kryteria wyboru pakietów szyfrów dla szyfrowania opartego na certyfikatach i PSK.
TLSCipherCert	Ciąg priorytetów GnuTLS lub ciąg szyfrów OpenSSL (TLS 1.2). Nadpisuje domyślne kryteria wyboru pakietów szyfrów dla szyfrowania opartego na certyfikatach.
TLSCipherCert13	Ciąg szyfrów dla OpenSSL 1.1.1 lub nowszego w TLS 1.3. Nadpisuje domyślne kryteria wyboru pakietów szyfrów dla szyfrowania opartego na certyfikatach.
TLSCipherPSK	Ciąg priorytetów GnuTLS lub ciąg szyfrów OpenSSL (TLS 1.2). Nadpisuje domyślne kryteria wyboru pakietów szyfrów dla szyfrowania opartego na PSK.
TLSCipherPSK13	Ciąg szyfrów dla OpenSSL 1.1.1 lub nowszego w TLS 1.3. Nadpisuje domyślne kryteria wyboru pakietów szyfrów dla szyfrowania opartego na PSK.
TLSConnect	Określa, w jaki sposób proxy powinno łączyć się z serwer Zabbix.
TLSCRLFile	Pełna ścieżka do pliku zawierającego unieważnione certyfikaty. Ten parametr jest używany do szyfrowanej komunikacji między komponentami Zabbix.
TLSKeyFile	Pełna ścieżka do pliku zawierającego klucz prywatny proxy, używanego do szyfrowanej komunikacji między komponentami Zabbix.
TLSListen	Steruje TLS na gnieździe trappera.
TLSPSKFile	Pełna ścieżka do pliku zawierającego klucz współdzielony proxy, używanego do szyfrowanej komunikacji z serwer Zabbix.
TLSPSKIdentity	Ciąg identyfikatora klucza współdzielonego, używany do szyfrowanej komunikacji z serwer Zabbix.
TLSServerCertIssuer	Dozwolony wystawca certyfikatu serwera.
TLSServerCertSubject	Dozwolony temat certyfikatu serwera.
TmpDir	Katalog tymczasowy.
TrapperTimeout	Określa limit czasu w sekundach dla: - pobierania danych konfiguracyjnych z serwer Zabbix; - wykonywania skryptu globalnego lub zdalnego polecenia.
UnavailableDelay	Jak często sprawdzana jest dostępność hosta w okresie niedostępności.
UnreachableDelay	Jak często sprawdzana jest dostępność hosta w okresie nieosiągalności.
UnreachablePeriod	Po ilu sekundach nieosiągalności host ma być traktowany jako niedostępny.
User	Obniża uprawnienia do określonego, istniejącego użytkownika w systemie.
Vault	Dostawca vault.
VaultDBPath	Lokalizacja, z której poświadczenia bazy danych powinny być pobierane za pomocą kluczy.
VaultPrefix	Niestandardowy prefiks dla ścieżki lub zapytania vault.
VaultTLSCertFile	Nazwa pliku certyfikatu SSL używanego do uwierzytelniania klienta.
VaultTLSKeyFile	Nazwa pliku klucza prywatnego SSL używanego do uwierzytelniania klienta.
VaultToken	Token uwierzytelniający HashiCorp vault.
VaultURL	Adres URL HTTP[S] serwera vault.
VMwareCacheSize	Rozmiar pamięci współdzielonej do przechowywania danych VMware.
VMwareFrequency	Opóźnienie w sekundach między pobieraniem danych z pojedynczej usługi VMware.
VMwarePerfFrequency	Opóźnienie w sekundach między pobieraniem statystyk liczników wydajności z pojedynczej usługi VMware.
VMwareTimeout	Maksymalna liczba sekund, przez którą kolektor vmware będzie czekać na odpowiedź od usługi VMware.
WebDriverURL	Adres URL HTTP[S] interfejsu WebDriver.

Wszystkie parametry są opcjonalne, chyba że wyraźnie zaznaczono, że parametr jest obowiązkowy.

Zwróć uwagę, że:

- Wartości domyślne odzwierciedlają wartości domyślne demona, a nie wartości w dostarczanych plikach konfiguracyjnych.
- Wartości obsługują zmienne środowiskowe.
- Zabbix obsługuje pliki konfiguracyjne tylko w kodowaniu UTF-8 bez BOM.
- Komentarze rozpoczynające się od „#” są obsługiwane tylko na początku linii.

Szczegóły parametrów

AllowRoot

Zezwala na uruchamianie proxy jako „root”. Jeśli wyłączone, a proxy zostanie uruchomiony przez „root”, proxy spróbuje zamiast tego przełączyć się na użytkownika „zabbix”. Nie ma wpływu, jeśli został uruchomiony przez zwykłego użytkownika.

Domyślnie: 0
 Wartości: 0 - nie zezwalaj; 1 - zezwalaj

AllowUnsupportedDBVersions

Zezwala proxy na pracę z nieobsługiwanymi wersjami bazy danych.

Domyślnie: 0
 Wartości: 0 - nie zezwalaj; 1 - zezwalaj

CacheSize

Rozmiar pamięci podręcznej konfiguracji, w bajtach. Rozmiar pamięci współdzielonej do przechowywania danych hostów i pozycji.

Domyślnie: 32M
 Zakres: 128K-64G

ConfigFrequency

Ten parametr jest **przestarzały** (zamiast niego użyj ProxyConfigFrequency).
Określa, jak często proxy pobiera dane konfiguracyjne z serwera Zabbix, w sekundach.
Parametr aktywnego proxy. Ignorowany dla pasywnych proxy (zobacz parametr ProxyMode).

Wartość domyślna: 3600
 Zakres: 1-604800

DataSenderFrequency

proxy będzie wysyłał zebrane dane do serwer co N sekund. Należy pamiętać, że aktywny proxy będzie nadal odpytywać serwer Zabbix co sekundę w celu sprawdzenia zadań zdalnych poleceń.
Parametr aktywnego proxy. Ignorowany dla pasywnych proxy (zobacz parametr ProxyMode).

Wartość domyślna: 1
 Zakres: 1-3600

DBHost

Nazwa hosta bazy danych.
W przypadku MySQL `localhost` lub pusty ciąg znaków powoduje użycie gniazda. W przypadku PostgreSQL tylko pusty ciąg znaków skutkuje próbą użycia gniazda.

Wartość domyślna: `localhost`

DBName

Nazwa bazy danych lub ścieżka do pliku bazy danych dla SQLite3 (architektura wieloprocesowa Zabbix nie pozwala na użycie bazy danych w pamięci, np. `:memory:`, `file::memory:?cache=shared` lub `file:memdb1?mode=memory&cache=shared`).
Ostrzeżenie: Nie próbuj używać tej samej bazy danych, której używa serwer Zabbix.

Wymagane: Tak

DBPassword

Hasło bazy danych. Zakomentuj tę linię, jeśli hasło nie jest używane. Ignorowane dla SQLite.

DBPort

Port bazy danych, gdy nie jest używane lokalne gniazdo.[1] Ignorowane dla SQLite.

Domyślnie dla MySQL: 3306

Domyślnie dla PostgreSQL: 5432

Zakres: 1024-65535

DBSchema

Nazwa schematu bazy danych. Używane dla PostgreSQL.

DBSocket

Ścieżka do pliku socket MySQL.[1]
Port bazy danych, gdy nie jest używany lokalny socket. Ignorowane dla SQLite.

Wartość domyślna: 3306

DBUser

Użytkownik bazy danych. Ignorowane dla SQLite.

DBTLSConnect

Ustawienie tej opcji wymusza użycie połączenia TLS z bazą danych:
required - połącz przy użyciu TLS
verify_ca - połącz przy użyciu TLS i zweryfikuj certyfikat
verify_full - połącz przy użyciu TLS, zweryfikuj certyfikat oraz sprawdź, czy tożsamość bazy danych określona przez DBHost odpowiada jej certyfikatowi
W MySQL od wersji 5.7.11 oraz w PostgreSQL obsługiwane są następujące wartości: ”required”, ”verify”, ”verify_full”.
W MariaDB od wersji 10.2.6 obsługiwane są wartości ”required” i ”verify_full”.
Domyślnie nie jest ustawiona żadna opcja, a zachowanie zależy od konfiguracji bazy danych.

DBTLSCAFile

Pełna ścieżka do pliku zawierającego certyfikaty nadrzędnego urzędu certyfikacji (CA) używane do weryfikacji certyfikatu bazy danych.

Obowiązkowe: nie (tak, jeśli DBTLSConnect ustawiono na *verify_ca* lub *verify_full*)

DBTLSCertFile

Pełna ścieżka do pliku zawierającego certyfikat proxy Zabbix używany do uwierzytelniania w bazie danych.

DBTLSKeyFile

Pełna ścieżka do pliku zawierającego klucz prywatny używany do uwierzytelniania w bazie danych.

DBTLSCipher

Lista szyfrów szyfrowania, na które proxy Zabbix zezwala dla protokołów TLS do wersji TLS v1.2 włącznie. Obsługiwane tylko dla MySQL.

DBTLSCipher13

Lista szyfrów pakietów szyfrujących, na które proxy Zabbix zezwala dla protokołu TLS v1.3. Obsługiwane tylko dla MySQL, począwszy od wersji 8.0.16.

DebugLevel

Określ poziom debugowania:
0 - podstawowe informacje o uruchamianiu i zatrzymywaniu procesów Zabbix
1 - informacje krytyczne;
2 - informacje o błędach;
3 - ostrzeżenia;
4 - do debugowania (generuje dużo informacji);
5 - rozszerzone debugowanie (generuje jeszcze więcej informacji).

Domyślnie: 3
 Zakres: 0-5

EnableRemoteCommands

Czy zdalne polecenia z serwer Zabbix są dozwolone.

Domyślnie: 0
 Wartości: 0 - niedozwolone; 1 - dozwolone

ExternalScripts

Lokalizacja skryptów zewnętrznych (zależy od zmiennej instalacyjnej `datadir` ustawianej podczas kompilacji).

Wartość domyślna: `/usr/local/share/zabbix/externalscripts`

Fping6Location

Lokalizacja fping6. Upewnij się, że plik binarny fping6 ma właściciela root oraz ustawioną flagę SUID. Pozostaw puste (`Fping6Location=`), jeśli narzędzie fping potrafi przetwarzać adresy IPv6.

Domyślnie: `/usr/sbin/fping6`

FpingLocation

Lokalizacja fping. Upewnij się, że plik binarny fping ma właściciela root oraz ustawioną flagę SUID.

Domyślnie: `/usr/sbin/fping`

HistoryCacheSize

Rozmiar pamięci podręcznej historii w bajtach. Rozmiar pamięci współdzielonej do przechowywania danych historii.

Domyślnie: `16M`
 Zakres: 128K-16G

HistoryIndexCacheSize

Rozmiar pamięci podręcznej indeksu historii, w bajtach. Rozmiar pamięci współdzielonej do indeksowania danych historii przechowywanych w pamięci podręcznej historii. Rozmiar pamięci podręcznej indeksu wymaga około 100 bajtów do buforowania jednej pozycji.

Domyślnie: `4M`
 Zakres: 128K-16G

Hostname

Unikalna nazwa proxy z rozróżnianiem wielkości liter. Upewnij się, że nazwa proxy jest znana serwerowi.
Dozwolone znaki: alfanumeryczne, '.', ' ', '_' i '-'. Maksymalna długość: 128

Wartość domyślna: ustawiana przez HostnameItem

HostnameItem

Pozycja używana do ustawienia Hostname, jeśli nie jest on zdefiniowany (zostanie uruchomiona na proxy podobnie jak na agencie). Ignorowane, jeśli Hostname jest ustawiony.
Nie obsługuje UserParameters, liczników wydajności ani aliasów, ale obsługuje system.run[].

Wartość domyślna: system.hostname

HousekeepingFrequency

Jak często Zabbix będzie wykonywać procedurę housekeeping (w godzinach). Housekeeping polega na usuwaniu nieaktualnych informacji z bazy danych.
Uwaga: Aby zmniejszyć obciążenie przy uruchamianiu proxy, housekeeping jest opóźniany o 30 minut po starcie proxy. Dlatego, jeśli HousekeepingFrequency wynosi 1, pierwsza procedura housekeeping po uruchomieniu proxy zostanie wykonana po 30 minutach, a następnie będzie powtarzana co godzinę.
Możliwe jest wyłączenie automatycznego housekeeping przez ustawienie HousekeepingFrequency na 0. W takim przypadku procedura housekeeping może zostać uruchomiona tylko za pomocą opcji kontroli wykonania *housekeeper_execute*.
Zobacz także opcje runtime control oraz szczegóły dotyczące procedury housekeeping.

Wartość domyślna: 1
 Zakres: 0-24

Include

Możesz dołączyć pojedyncze pliki lub wszystkie pliki w katalogu w pliku konfiguracyjnym.
Aby dołączać tylko odpowiednie pliki w określonym katalogu, obsługiwany jest znak wieloznaczny gwiazdki do dopasowywania wzorców.
Zobacz uwagi specjalne dotyczące ograniczeń.

Przykład:

```
Include=/absolute/path/to/config/files/*.conf
```

JavaGateway

Adres IP (lub nazwa hosta) bramy Java gateway Zabbix. Wymagane tylko wtedy, gdy uruchomione są odpytywacze Java.

JavaGatewayPort

Port, na którym nasłuchuje Zabbix Java gateway.

Domyślnie: 10052
 Zakres: 1024-32767

ListenBacklog

Maksymalna liczba oczekujących połączeń w kolejce TCP.
Wartość domyślna jest stałą zakodowaną na stałe i zależy od systemu.
Maksymalna obsługiwana wartość również zależy od systemu; zbyt wysokie wartości mogą zostać po cichu obcięte do „maksimum określonego przez implementację”.

Domyślnie: SOMAXCONN
 Zakres: 0 - INT_MAX

ListenIP

Lista adresów IP rozdzielonych przecinkami, na których trapper powinien nasłuchiwać.
Jeśli ten parametr nie zostanie określony, trapper będzie nasłuchiwał na wszystkich interfejsach sieciowych.

Wartość domyślna: 0.0.0.0

ListenPort

Port nasłuchiwania dla trappera.

Domyślnie: 10051
 Zakres: 1024-32767

LoadModule

Moduł do załadowania podczas uruchamiania proxy. Moduły są używane do rozszerzania funkcjonalności proxy. Moduł musi znajdować się w katalogu określonym przez LoadModulePath lub ścieżka musi poprzedzać nazwę modułu. Jeśli poprzedzająca ścieżka jest bezwzględna (zaczyna się od ’/’), wówczas LoadModulePath jest ignorowane.
Formaty:
LoadModule=<module.so>
LoadMod jest uwzględnienie wielu parametrów LoadModule.

LoadModulePath

Pełna ścieżka do lokalizacji modułów proxy. Wartość domyślna zależy od opcji kompilacji.

LogFile

Nazwa pliku dziennika.

Wymagane: Tak, jeśli parametr LogType jest ustawiony na *file*; w przeciwnym razie nie

LogFileSize

Maksymalny rozmiar pliku dziennika w MB.
0 - wyłącza automatyczną rotację plików dziennika.
Uwaga: Jeśli zostanie osiągnięty limit rozmiaru pliku dziennika, a rotacja pliku nie powiedzie się z jakiegokolwiek powodu, istniejący plik dziennika zostanie obcięty i rozpoczęty od nowa.

Wartość domyślna: 1
 Zakres: 0-1024

LogRemoteCommands

Włącz rejestrowanie wykonywanych poleceń powłoki jako ostrzeżeń.

Domyślnie: 0
 Wartości: 0 - wyłączone, 1 - włączone

LogType

Typ wyjścia logu:
file - zapisuj log do pliku określonego przez parametr LogFile;
system - zapisuj log do syslog;
console - zapisuj log na standardowe wyjście.

Wartość domyślna: `file`

LogSlowQueries

Jak długo zapytanie do bazy danych może trwać, zanim zostanie zapisane w logu (w milisekundach).
0 - nie zapisuj wolnych zapytań w logu.
Ta opcja jest włączana od DebugLevel=3.

Wartość domyślna: 0
 Zakres: 0-3600000

MaxConcurrentChecksPerPoller

Maksymalna liczba asynchronicznych kontroli, które mogą być wykonywane jednocześnie przez każdy moduł odpytywania HTTP agent, agent lub SNMP. Zobacz StartHTTPAgentPollers, StartAgentPollers oraz StartSNMPPollers.

Wartość domyślna: 1000
 Zakres: 1-1000

PidFile

Nazwa pliku PID.

Domyślnie: `/tmp/zabbix_proxy.pid`

ProxyBufferMode

Określa mechanizm przechowywania danych historii, wykrywania sieci i autorejestracji: *disk* — dane są przechowywane w bazie danych i wysyłane z bazy danych; *memory* — dane są przechowywane w pamięci i wysyłane z pamięci. Jeśli buforowi zabraknie pamięci, stare dane zostaną odrzucone. Przy zamykaniu bufor jest odrzucany. *hybrid* — bufor proxy zwykle działa jak w trybie pamięci, dopóki nie zabraknie mu pamięci lub najstarszy rekord nie przekroczy skonfigurowanego wieku. Jeśli tak się stanie, bufor jest opróżniany do bazy danych i działa jak w trybie dyskowym, dopóki wszystkie dane nie zostaną wysłane, po czym ponownie zaczyna działać w pamięci. Przy zamykaniu bufor pamięci jest opróżniany do bazy danych.

Zobacz także: Bufor pamięci proxy.

Wartość domyślna: `disk`
 Wartości: disk; memory; hybrid

ProxyConfigFrequency

Jak często proxy pobiera dane konfiguracyjne z serwera Zabbix, w sekundach.
Parametr aktywnego proxy. Ignorowany dla proxy pasywnych (zobacz parametr ProxyMode).

Domyślnie: 10
 Zakres: 1-604800

ProxyLocalBuffer

Proxy będzie przechowywać dane lokalnie przez N godzin, nawet jeśli dane zostały już zsynchronizowane z serwerem.
Tego parametru można użyć, jeśli lokalne dane będą wykorzystywane przez aplikacje innych firm.

Wartość domyślna: 0
 Zakres: 0-720

ProxyMemoryBufferAge

Maksymalny wiek danych w buforze pamięci proxy, w sekundach. Gdy jest włączony (wartość różna od zera) i rekordy w buforze pamięci proxy są starsze, wymusza to przełączenie bufora proxy w tryb bazy danych do momentu przesłania wszystkich rekordów do serwer. Ten parametr musi być mniejszy lub równy parametrowi ProxyOfflineBuffer.

Wartość domyślna: 0
 Zakres: 0;600-864000

ProxyMemoryBufferSize

Rozmiar pamięci współdzielonej cache dla zebranych danych historii, wykrywania i autorejestracji, w bajtach. Jeśli włączone (wartość różna od zera), proxy będzie przechowywać dane historii, wykrywania i autorejestracji w pamięci, chyba że cache będzie

pełny lub zapisane rekordy będą starsze niż zdefiniowany parametr ProxyMemoryBufferAge. Ten parametr nie może być używany razem z parametrem ProxyLocalBuffer.

Domyślnie: 0
 Zakres: 0;128K-2G

ProxyMode

Tryb pracy proxy.
0 - proxy w trybie aktywnym
1 - proxy w trybie pasywnym
Uwaga: poufne dane konfiguracyjne proxy mogą stać się dostępne dla stron mających dostęp do portu trappera serwera Zabbix podczas korzystania z aktywnego proxy. Jest to możliwe, ponieważ każdy może podszyć się pod aktywny proxy i zażądać danych konfiguracyjnych; uwierzytelnianie nie jest przeprowadzane.

Wartość domyślna: 0
 Zakres: 0-1

ProxyOfflineBuffer

Proxy będzie przechowywać dane przez N godzin w przypadku braku łączności z serwerem Zabbix.
Starsze dane zostaną utracone.

Wartość domyślna: 1
 Zakres: 1-720

Serwer

Jeśli ProxyMode jest ustawiony na *tryb aktywny*:
Adres IP lub nazwa DNS serwera Zabbix (adres:port) albo klaster (adres:port;adres2:port), z którego pobierane są dane konfiguracyjne i do którego wysyłane są dane.
Jeśli port nie jest określony, używany jest port domyślny.
Węzły klastra muszą być oddzielone średnikiem.

Jeśli ProxyMode jest ustawiony na *tryb pasywny*:
Lista adresów IP oddzielonych przecinkami, opcjonalnie w notacji CIDR, lub nazw DNS serwera Zabbix. Połączenia przychodzące będą akceptowane tylko z adresów wymienionych tutaj. Jeśli obsługa IPv6 jest włączona, wtedy '127.0.0.1', '::127.0.0.1', '::ffff:127.0.0.1' są traktowane jednakowo.
'::/0' zezwoli na dowolny adres IPv4 lub IPv6. '0.0.0.0/0' może być użyte do zezwolenia na dowolny adres IPv4.

Przykład:

```
Server=127.0.0.1,192.168.1.0/24,::1,2001:db8::/32,zabbix.example.com
```

Wymagane: tak

SNMPTrapperFile

Plik tymczasowy używany do przekazywania danych z demona pułapek SNMP do proxy.
Musi być taki sam jak w pliku konfiguracyjnym zabbix_trap_receiver.pl lub SNMPTT.

Wartość domyślna: `/tmp/zabbix_traps.tmp`

SocketDir

Katalog do przechowywania gniazd IPC używanych przez wewnętrzne usługi Zabbix.

Domyślnie: `/tmp`

SourceIP

Źródłowy adres IP dla:

- połączeń wychodzących do serwera Zabbix
- połączeń bez agenta (VMware, SSH, JMX, SNMP, Telnet oraz prostych kontroli)
- połączeń HTTP agent
- żądań HTTP JavaScript dla pozycji skryptowych
- żądań HTTP JavaScript dla preprocessingu
- połączeń z Vault

SSHKeyLocation

Lokalizacja kluczy publicznych i prywatnych dla kontroli SSH oraz akcji.

SSLCertLocation

Lokalizacja plików certyfikatów klienta SSL używanych do uwierzytelniania klienta.
Ten parametr jest używany tylko w monitorowaniu WWW.

SSLKeyLocation

Lokalizacja plików prywatnych kluczy SSL do uwierzytelniania klienta.
Ten parametr jest używany tylko w monitorowaniu WWW.

SSLCALocation

Lokalizacja plików urzędu certyfikacji (CA) do weryfikacji certyfikatu SSL serwera.
Należy pamiętać, że wartość tego parametru zostanie ustawiona jako opcja libcurl CURLOPT_CAPATH. W przypadku wersji libcurl wcześniejszych niż 7.42.0 ma to skutek tylko wtedy, gdy libcurl został skompilowany do użycia OpenSSL. Więcej informacji można znaleźć na stronie cURL.
Ten parametr jest używany w monitorowaniu WWW oraz w uwierzytelnianiu SMTP.

StartAgentPollers

Liczba wstępnie rozwidlonych instancji pollerów agenta Zabbix. Zobacz MaxConcurrentChecksPerPoller.

Domyślnie: 1
 Zakres: 0-1000

StartBrowserPollers

Liczba wstępnie utworzonych instancji pollerów pozycji przeglądarki.

Domyślnie: 1
 Zakres: 0-1000

StartDBSyncers

Liczba wstępnie rozwidlonych instancji synchronizatorów historii.
Uwaga: Zachowaj ostrożność podczas zmiany tej wartości — jej zwiększenie może przynieść więcej szkody niż pożytku.

Domyślnie: 4
 Zakres: 1-100

StartDiscoverers

Liczba wstępnie utworzonych instancji workerów wykrywania.

Domyślnie: 5
 Zakres: 0-1000

StartHTTPAgentPollers

Liczba wstępnie rozwidlonych instancji HTTP agent pollerów. Zobacz MaxConcurrentChecksPerPoller.

Domyślnie: 1
 Zakres: 0-1000

StartHTTPPollers

Liczba wstępnie rozwidlonych instancji HTTP pollers.

Domyślnie: 1
 Zakres: 0-1000

StartIPMIPollers

Liczba wstępnie rozwidlonych instancji modułów odpytujących IPMI.

Domyślnie: 0
 Zakres: 0-1000

StartJavaPollers

Liczba wstępnie rozwidlonych instancji sond Java.

Domyślnie: 0
 Zakres: 0-1000

StartODBCPollers

Liczba wstępnie utworzonych instancji ODBC pollers.

Domyślnie: 1
 Zakres: 0-1000

StartPingers

Liczba wstępnie utworzonych instancji pingers ICMP.

Domyślnie: 1
 Zakres: 0-1000

StartPollersUnreachable

Liczba wstępnie rozwidlonych instancji pollerów dla nieosiągalnych hostów (w tym IPMI i Java). Co najmniej jeden poller dla nieosiągalnych hostów musi być uruchomiony, jeśli uruchomione są zwykłe pollery, pollery IPMI lub pollery Java.

Domyślnie: 1
 Zakres: 0-1000

StartPollers

Liczba wstępnie rozwidlonych instancji pollerów.

Domyślnie: 5
 Zakres: 0-1000

StartPreprocessors

Liczba wstępnie uruchomionych instancji wątków worker przetwarzania wstępnego powinna być ustawiona na wartość nie mniejszą niż liczba dostępnych rdzeni CPU. Należy ustawić więcej workerów, jeśli przetwarzanie wstępne nie jest ograniczone wydajnością CPU i obejmuje wiele żądań sieciowych.

Domyślnie: 16
 Zakres: 1-1000

StartSNMPPollers

Liczba wstępnie utworzonych instancji SNMP pollerów. Zobacz MaxConcurrentChecksPerPoller.

Domyślnie: 1
 Zakres: 0-1000

StartSNMPTrapper

Jeśli ustawiono na 1, zostanie uruchomiony proces SNMP trapper.

Domyślnie: 0
 Zakres: 0-1

StartTrappers

Liczba wstępnie rozwidlonych instancji trapperów.
Trappery akceptują połączenia przychodzące od Zabbix sender oraz aktywnych agentów.

Domyślnie: 5
 Zakres: 0-1000

StartVMwareCollectors

Liczba wstępnie rozwidlonych instancji VMware collector.

Domyślnie: 0
 Zakres: 0-250

StatsAllowedIP

Lista adresów IP oddzielonych przecinkami, opcjonalnie w notacji CIDR, lub nazw DNS zewnętrznych instancji Zabbix. Żądanie statystyk będzie akceptowane wyłącznie z adresów wymienionych tutaj. Jeśli ten parametr nie jest ustawiony, żadne żądania statystyk nie będą akceptowane.
Jeśli obsługa IPv6 jest włączona, wtedy '127.0.0.1', '::127.0.0.1', '::ffff:127.0.0.1' są traktowane jednakowo, a '::/0' zezwoli na dowolny adres IPv4 lub IPv6. '0.0.0.0/0' może zostać użyte do zezwolenia na dowolny adres IPv4.

Przykład:

```
StatsAllowedIP=127.0.0.1,192.168.1.0/24,::1,2001:db8::/32,zabbix.example.com
```

Timeout

Określa, jak długo czekać (w sekundach) na ustanowienie połączenia i wymianę danych z serwerem Zabbix, agent, usługą web oraz starszymi kontrolami SNMP (pojedynczy numer OID lub ciąg znaków).

Ten parametr określa czas trwania różnych operacji komunikacyjnych:

- Zdalne wykonywanie poleceń na Zabbix agent
- Wykonywanie poleceń SSH / Telnet
- Ponowne planowanie pozycji, gdy interfejs IPMI staje się niedostępny
- Wysyłanie odpowiedzi do serwera Zabbix w przypadku niepowodzenia wymiany danych z powodu problemów z uprawnieniami lub szyfrowaniem
- Limit czasu dla asynchronicznych gniazd IPC i opcji kontroli w czasie działania
- Żądania DNS asynchronicznego pollera
- Odpowiedź dla heartbeat aktywnej kontroli
- Pobieranie danych Zabbix agent (wartości) od aktywnych agentów
- Pobieranie danych z Zabbix sender
- Wysyłanie listy aktywnych kontroli do Zabbix agent

Ten limit czasu **nie** będzie używany dla tych kontroli, które mają skonfigurowane ustawienia elastycznego limitu czasu we frontendzie (na poziomie globalnym, proxy lub pojedynczej pozycji).
Na przykład pozycje SNMP `walk[OID]` i `get[OID]` używają limitu czasu skonfigurowanego we frontendzie; starsze kontrole SNMP nadal używają wartości limitu czasu serwera.

Domyślnie: 3
 Zakres: 1-30

TLSAccept

Jakie połączenia przychodzące od serwera Zabbix mają być akceptowane. Używane dla proxy pasywnego, ignorowane dla proxy aktywnego. Można określić wiele wartości, oddzielonych przecinkami:
unencrypted — akceptuj połączenia bez szyfrowania (domyślnie)
psk — akceptuj połączenia z TLS i kluczem współdzielonym (PSK)
cert — akceptuj połączenia z TLS i certyfikatem

Wymagane: tak dla proxy pasywnego, jeśli zdefiniowano parametry certyfikatu TLS lub PSK (nawet dla połączenia *unencrypted*); w przeciwnym razie nie

TLSCAFile

Pełna ścieżka do pliku zawierającego certyfikaty nadrzędnych urzędów certyfikacji (CA) używane do weryfikacji certyfikatu peera, wykorzystywane w szyfrowanej komunikacji między komponentami Zabbix.

TLSCertFile

Pełna ścieżka do pliku zawierającego certyfikat proxy lub łańcuch certyfikatów, używanego do szyfrowanej komunikacji między komponentami Zabbix.

TLSCipherAll

Ciąg priorytetów GnuTLS lub ciąg szyfrów OpenSSL (TLS 1.2). Zastępuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na certyfikatach i PSK.

Przykład:

```
TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256
```

TLSCipherAll13

Ciąg szyfrów dla OpenSSL 1.1.1 lub nowszego w TLS 1.3. Zastępuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na certyfikatach i PSK.

Przykład dla GnuTLS:

```
NONE:+VERS-TLS1.2:+ECDHE-RSA:+RSA:+ECDHE-PSK:+PSK:+AES-128-GCM:+AES-128-CBC:+AEAD:+SHA256:+SHA1:+CURVE-ALL
```

Przykład dla OpenSSL:

```
EECDH+aRSA+AES128:RSA+aRSA+AES128:kECDHEPSK+AES128:kPSK+AES128
```

TLSCipherCert

Ciąg priorytetów GnuTLS lub ciąg szyfrów OpenSSL (TLS 1.2). Zastępuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na certyfikatach.

Przykład dla GnuTLS:

```
NONE:+VERS-TLS1.2:+ECDHE-RSA:+RSA:+AES-128-GCM:+AES-128-CBC:+AEAD:+SHA256:+SHA1:+CURVE-ALL:+COMP-NULL:+SIG
```

Przykład dla OpenSSL:

```
EECDH+aRSA+AES128:RSA+aRSA+AES128
```

TLSCipherCert13

Ciąg szyfrów dla OpenSSL 1.1.1 lub nowszego w TLS 1.3. Zastępuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na certyfikatach.

TLSCipherPSK

Ciąg priorytetów GnuTLS lub ciąg szyfrów OpenSSL (TLS 1.2). Nadpisuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na PSK.

Przykład dla GnuTLS:

```
NONE:+VERS-TLS1.2:+ECDHE-PSK:+PSK:+AES-128-GCM:+AES-128-CBC:+AEAD:+SHA256:+SHA1:+CURVE-ALL:+COMP-NULL:+SIG
```

Przykład dla OpenSSL:

```
kECDHEPSK+AES128:kPSK+AES128
```

TLSCipherPSK13

Ciąg szyfrów dla OpenSSL 1.1.1 lub nowszego w TLS 1.3. Zastępuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na PSK.

Przykład:

```
TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256
```

TLSConnect

Sposób, w jaki proxy powinien łączyć się z serwerem Zabbix. Używane dla aktywnego proxy, ignorowane dla pasywnego proxy. Można określić tylko jedną wartość:
unencrypted - połączenie bez szyfrowania (domyślnie)
psk - połączenie z użyciem TLS i klucza współdzielonego (PSK)
cert - połączenie z użyciem TLS i certyfikatu

Wymagane: tak dla aktywnego proxy, jeśli zdefiniowano parametry certyfikatu TLS lub PSK (nawet dla połączenia *unencrypted*); w przeciwnym razie nie

TLSCRLFile

Pełna ścieżka do pliku zawierającego unieważnione certyfikaty. Ten parametr jest używany do szyfrowanej komunikacji między komponentami Zabbix.

TLSKeyFile

Pełna ścieżka do pliku zawierającego klucz prywatny proxy, używanego do szyfrowanej komunikacji między komponentami Zabbix.

TLSListen

Steruje TLS na gnieździe trappera.

Obsługiwane wartości:

- required - akceptuj tylko połączenia TLS

TLSPSKFile

Pełna ścieżka do pliku zawierającego klucz współdzielony proxy, używany do szyfrowanej komunikacji z serwerem Zabbix.

TLSPSKIdentity

Ciąg tożsamości klucza współdzielonego, używany do szyfrowanej komunikacji z serwerem Zabbix.

TLSServerCertIssuer

Dozwolony wystawca certyfikatu serwera.

TLSServerCertSubject

Dozwolony temat certyfikatu serwera.

TmpDir

Katalog tymczasowy.

Domyślnie: `/tmp`

TrapperTimeout

Określa limit czasu w sekundach dla:
 - pobierania danych konfiguracyjnych z serwera Zabbix;
 - wykonywania skryptów globalnych lub poleceń zdalnych.

Wartość domyślna: 300
 Zakres: 1-300

UnavailableDelay

Jak często host jest sprawdzany pod kątem dostępności w okresie niedostępności, w sekundach.

Wartość domyślna: 60
 Zakres: 1-3600

UnreachableDelay

Jak często sprawdzana jest dostępność hosta w okresie niedostępności, w sekundach.

Domyślnie: 15
 Zakres: 1-3600

UnreachablePeriod

Po ilu sekundach nieosiągalności traktować host jako niedostępny.

Domyślnie: 45
 Zakres: 1-3600

Użytkownik

Obniża uprawnienia do określonego, istniejącego użytkownika w systemie.
Ma zastosowanie tylko w przypadku uruchomienia jako `root` i gdy opcja AllowRoot jest wyłączona.

Domyślnie: `zabbix`

Dostawca vault

Dostawca vault:
HashiCorp - HashiCorp KV Secrets Engine w wersji 2
CyberArk - CyberArk Central Credential Provider
Musi odpowiadać dostawcy vault ustawionemu we frontend.

Wartość domyślna: `HashiCorp`

VaultDBPath

Ścieżka lub zapytanie Vault, zależnie od używanego Vault, skąd będą pobierane poświadczenia do bazy danych za pomocą kluczy.

Klucze używane dla HashiCorp to 'password' i 'username'.

Przykładowa ścieżka z VaultPrefix=/v1/secret/data/zabbix/:

```
database
```

Przykładowa ścieżka bez VaultPrefix:

```
secret/zabbix/database
```

Klucze używane dla CyberArk to 'Content' i 'UserName'.

Przykład:

```
AppID=zabbix_server&Query=Safe=passwordSafe;Object=zabbix_proxy_database
```

Ta opcja może być używana tylko wtedy, gdy DBUser i DBPassword nie są określone.

VaultPrefix

Niestandardowy prefiks dla ścieżki lub zapytania Vault, w zależności od Vault. Jeśli nie zostanie określony, zostaną użyte najbardziej odpowiednie wartości domyślne.
Zwróć uwagę, że dla HashiCorp po mountpoint automatycznie dodawane jest `data`, jeśli VaultPrefix nie jest określony.
Zwróć uwagę, że dla HashiCorp po mountpoint automatycznie dodawane jest `data`, jeśli VaultPrefix nie jest określony.

Przykładowy prefiks dla Hashicorp:

```
v1/secret/data/zabbix/
```

Przykładowy prefiks dla Cyberark:

```
/AIMWebService/api/Accounts?
```

VaultTLSCertFile

Nazwa pliku certyfikatu SSL używanego do uwierzytelniania klienta. Plik certyfikatu musi być w formacie PEM1.
Jeśli plik certyfikatu zawiera również klucz prywatny, pozostaw pole pliku klucza SSL puste.
Katalog zawierający ten plik jest określany przez parametr konfiguracyjny SSLCertLocation.
Tę opcję można pominąć, ale jest zalecana dla skarbca CyberArkCCP.

VaultTLSKeyFile

Nazwa pliku prywatnego klucza SSL używanego do uwierzytelniania klienta. Plik prywatnego klucza musi być w formacie PEM1.
Katalog zawierający ten plik jest określany przez parametr konfiguracyjny SSLKeyLocation.
Tę opcję można pominąć, ale jest zalecana w przypadku sejfu CyberArkCCP vault.

VaultToken

Token uwierzytelniania HashiCorp vault, który powinien zostać wygenerowany wyłącznie dla proxy Zabbix z uprawnieniami tylko do odczytu dla ścieżki określonej w opcjonalnym parametrze konfiguracyjnym VaultDBPath.
Błędem jest jednoczesne zdefiniowanie VaultToken i zmiennej środowiskowej VAULT_TOKEN.

Obowiązkowe: Tak, jeśli Vault jest ustawiony na *HashiCorp*; w przeciwnym razie nie

VaultURL

Adres URL HTTP[S] serwera vault. Jeśli SSLCALocation nie jest określone, zostanie użyty katalog certyfikatów CA dla całego systemu.

Domyślnie: `https://127.0.0.1:8200`

VMwareCacheSize

Rozmiar pamięci współdzielonej do przechowywania danych VMware.
Wewnętrzna kontrola VMware `zabbix[vmware,buffer,...]` może być używana do monitorowania wykorzystania pamięci podręcznej VMware (zobacz Kontrole wewnętrzne).
Zwróć uwagę, że pamięć współdzielona nie jest przydzielana, jeśli nie skonfigurowano do uruchomienia żadnych instancji kolektora VMware.

Wartość domyślna: `8M`
 Zakres: 256K-2G

VMwareFrequency

Opóźnienie w sekundach między pobieraniem danych z pojedynczej usługi VMware.
To opóźnienie powinno być ustawione na najmniejszy interwał aktualizacji dowolnej pozycji monitorowania VMware.

Domyślnie: 60
 Zakres: 10-86400

VMwarePerfFrequency

Opóźnienie w sekundach między pobieraniem statystyk liczników wydajności z pojedynczej usługi VMware.
To opóźnienie powinno być ustawione na najmniejszy interwał aktualizacji dowolnej monitorującej VMware pozycji, która używa liczników wydajności VMware.

Domyślnie: 60
 Zakres: 10-86400

VMwareTimeout

Maksymalna liczba sekund, przez którą kolektor vmware będzie oczekiwał na odpowiedź od usługi VMware (vCenter lub hiperwizora ESX).

Domyślnie: 10
 Zakres: 1-300

WebDriverURL

Adres URL HTTP[S] interfejsu WebDriver.

Przykład (używany z samodzielnym serwerem Selenium WebDriver):

```
WebDriverURL=http://localhost:4444
```

Przypisy

[1] DBSocket i DBPort wzajemnie się wykluczają w konfiguracji proxy. Należy określić tylko jeden z nich lub pozostawić oba niezdefiniowane.

3 Zabbix agent (UNIX)

Przegląd

Parametry obsługiwane przez plik konfiguracyjny Zabbix agent (zabbix_agentd.conf) są wymienione w tej sekcji.

Parametry są podane bez dodatkowych informacji. Kliknij parametr, aby zobaczyć pełne szczegóły.

Parameter	Description
Alias	Ustawia alias dla klucza pozycji.
AllowKey	Zezwala na wykonywanie tych kluczy pozycji, które pasują do wzorca.
AllowRoot	Zezwala na uruchamianie agent jako 'root'.
BufferSend	Nie przechowuje danych w buforze dłużej niż N sekund.
BufferSize	Maksymalna liczba wartości w buforze pamięci.
DebugLevel	Poziom debugowania.
DenyKey	Zabrania wykonywania tych kluczy pozycji, które pasują do wzorca.
EnableRemoteCommands	Określa, czy zdalne polecenia z Zabbix serwer są dozwolone.
HeartbeatFrequency	Częstotliwość komunikatów heartbeat w sekundach.
HostInterface	Opcjonalny parametr definiujący interfejs hosta.
HostInterfaceItem	Opcjonalny parametr definiujący pozycję używaną do pobierania interfejsu hosta.
HostMetadata	Opcjonalny parametr definiujący metadane hosta.
HostMetadataItem	Opcjonalny parametr definiujący pozycję Zabbix agent używaną do pobierania metadanych hosta.
Hostname	Opcjonalny parametr definiujący nazwę hosta.
HostnameItem	Opcjonalny parametr definiujący pozycję Zabbix agent używaną do pobierania nazwy hosta.
Include	Możesz dołączyć pojedyncze pliki lub wszystkie pliki z katalogu do pliku konfiguracyjnego.
ListenBacklog	Maksymalna liczba oczekujących połączeń w kolejce TCP.
ListenIP	Lista adresów IP rozdzielonych przecinkami, na których agent powinien nasłuchiwać.
ListenPort	agent będzie nasłuchiwał na tym porcie połączeń od serwer.
LoadModule	Moduł do załadowania podczas uruchamiania agent.
LoadModulePath	Pełna ścieżka do lokalizacji modułów agent.
LogFile	Nazwa pliku dziennika.
LogFileSize	Maksymalny rozmiar pliku dziennika.
LogRemoteCommands	Włącza rejestrowanie wykonywanych poleceń powłoki jako ostrzeżeń.
LogType	Typ wyjścia dziennika.

Parameter	Description
MaxLinesPerSecond	Maksymalna liczba nowych wierszy, które agent wyśle na sekundę do Zabbix serwer lub proxy podczas przetwarzania aktywnych kontroli ’log’ i ’logrt’.
PidFile	Nazwa pliku PID.
RefreshActiveChecks	Jak często odświeżana jest lista aktywnych kontroli.
Server	Lista adresów IP rozdzielonych przecinkami, opcjonalnie w notacji CIDR, lub nazw DNS serwerów Zabbix i proxy Zabbix.
ServerActive	Adres Zabbix serwer/proxy lub konfiguracja klastra, z którego pobierane są aktywne kontrole.
SourceIP	Źródłowy adres IP.
StartAgents	Liczba wstępnie rozwidlonych instancji zabbix_agentd przetwarzających kontrole pasywne.
Timeout	Określa, jak długo czekać (w sekundach) na ustanowienie połączenia i wymianę danych z Zabbix proxy lub serwer.
TLSAccept	Jakie połączenia przychodzące akceptować.
TLSCAFile	Pełna ścieżka do pliku zawierającego certyfikaty nadrzędnych urzędów certyfikacji (CA) do weryfikacji certyfikatów partnera, używana do szyfrowanej komunikacji między komponentami Zabbix.
TLSCertFile	Pełna ścieżka do pliku zawierającego certyfikat agent lub łańcuch certyfikatów, używana do szyfrowanej komunikacji między komponentami Zabbix.
TLSCipherAll	Ciąg priorytetów GnuTLS lub ciąg szyfrów OpenSSL (TLS 1.2). Zastępuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na certyfikatach i PSK.
TLSCipherAll13	Ciąg szyfrów dla OpenSSL 1.1.1 lub nowszego w TLS 1.3. Zastępuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na certyfikatach i PSK.
TLSCipherCert	Ciąg priorytetów GnuTLS lub ciąg szyfrów OpenSSL (TLS 1.2). Zastępuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na certyfikatach.
TLSCipherCert13	Ciąg szyfrów dla OpenSSL 1.1.1 lub nowszego w TLS 1.3. Zastępuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na certyfikatach.
TLSCipherPSK	Ciąg priorytetów GnuTLS lub ciąg szyfrów OpenSSL (TLS 1.2). Zastępuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na PSK.
TLSCipherPSK13	Ciąg szyfrów dla OpenSSL 1.1.1 lub nowszego w TLS 1.3. Zastępuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na PSK.
TLSConnect	Określa, w jaki sposób agent powinien łączyć się z Zabbix serwer lub proxy.
TLSCRLFile	Pełna ścieżka do pliku zawierającego unieważnione certyfikaty. Ten parametr jest używany do szyfrowanej komunikacji między komponentami Zabbix.
TLSKeyFile	Pełna ścieżka do pliku zawierającego klucz prywatny agent, używana do szyfrowanej komunikacji między komponentami Zabbix.
TLSPSKFile	Pełna ścieżka do pliku zawierającego klucz współdzielony agent, używana do szyfrowanej komunikacji z Zabbix serwer.
TLSPSKIdentity	Ciąg tożsamości klucza współdzielonego, używany do szyfrowanej komunikacji z Zabbix serwer.
TLSServerCertIssuer	Dozwolony wystawca certyfikatu serwer (proxy).
TLSServerCertSubject	Dozwolony podmiot certyfikatu serwer (proxy).
UnsafeUserParameters	Zezwala na przekazywanie wszystkich znaków w argumentach do parametrów zdefiniowanych przez użytkownika.
User	Obniża uprawnienia do określonego, istniejącego użytkownika w systemie.
UserParameter	Parametr zdefiniowany przez użytkownika do monitorowania.
UserParameterDir	Domyślna ścieżka wyszukiwania dla poleceń UserParameter.

Wszystkie parametry są opcjonalne, chyba że wyraźnie stwierdzono, że dany parametr jest obowiązkowy.

Zwróć uwagę, że:

- Wartości domyślne odzwierciedlają wartości domyślne demona, a nie wartości w dostarczanych plikach konfiguracyjnych.
- Wartości obsługują zmienne środowiskowe.
- Zabbix obsługuje pliki konfiguracyjne tylko w kodowaniu UTF-8 bez BOM.
- Komentarze rozpoczynające się od ”#” są obsługiwane tylko na początku wiersza.

Szczegóły parametrów

Alias

Ustawia alias dla klucza pozycji. Może być używany do zastąpienia długiego i złożonego klucza pozycji krótszym i prostszym.
 Może występować wiele parametrów *Alias*. Wiele parametrów z tym samym kluczem *Alias* jest niedozwolonych.
 Różne klucze *Alias* mogą wskazywać ten sam klucz pozycji.
 Aliasy mogą być używane w parametrze *HostMetadataItem*, ale nie w parametrze *HostnameItem*.

Przykład 1: Pobieranie identyfikatora użytkownika „zabbix”.

```
Alias=zabbix.userid:vfs.file.regexp[/etc/passwd,"^zabbix:.:([0-9]+)",,,,\1]
```

Teraz skrócony klucz **zabbix.userid** może być używany do pobierania danych.

Przykład 2: Pobieranie wykorzystania CPU z parametrami domyślnymi i niestandardowymi.

```
Alias=cpu.util:system.cpu.util
Alias=cpu.util[*]:system.cpu.util[*]
```

Pozwala to używać klucza **cpu.util** do pobierania procentowego wykorzystania CPU z parametrami domyślnymi, a także **cpu.util[all, idle, avg15]** do pobierania szczegółowych danych o wykorzystaniu CPU.

Przykład 3: Uruchamianie wielu reguł odkrywania niskiego poziomu przetwarzających te same pozycje wykrywania.

```
Alias=vfs.fs.discovery[*]:vfs.fs.discovery
```

Teraz możliwe jest skonfigurowanie kilku reguł wykrywania używających **vfs.fs.discovery** z różnymi parametrami dla każdej reguły, np. **vfs.fs.discovery[foo]**, **vfs.fs.discovery[bar]** itd.

AllowKey

Zezwalaj na wykonywanie tych kluczy pozycji, które pasują do wzorca. Wzorzec klucza jest wyrażeniem wieloznacznym obsługującym znak "*", który dopasowuje dowolną liczbę dowolnych znaków.
Można zdefiniować wiele reguł dopasowywania kluczy w połączeniu z DenyKey. Parametry są przetwarzane jeden po drugim zgodnie z kolejnością ich występowania. Zobacz także: Ograniczanie kontroli agenta.

AllowRoot

Zezwala agentowi na działanie jako „root". Jeśli opcja jest wyłączona, a agent zostanie uruchomiony przez użytkownika „root", agent spróbuje zamiast tego przełączyć się na użytkownika „zabbix". Nie ma to wpływu, jeśli agent został uruchomiony przez zwykłego użytkownika.

Domyślnie: 0
 Wartości: 0 - nie zezwalaj; 1 - zezwalaj

BufferSend

Nie przechowuj danych w buforze dłużej niż N sekund.

Wartość domyślna: 5
 Zakres: 1-3600

BufferSize

Maksymalna liczba wartości w buforze pamięci. agent wyśle wszystkie zebrane dane do serwera Zabbix lub proxy, jeśli bufor będzie pełny.

Domyślnie: 100
 Zakres: 2-65535

DebugLevel

Określ poziom debugowania:
0 - podstawowe informacje o uruchamianiu i zatrzymywaniu procesów Zabbix
1 - informacje krytyczne;
2 - informacje o błędach;
3 - ostrzeżenia;
4 - do debugowania (generuje dużo informacji);
5 - rozszerzone debugowanie (generuje jeszcze więcej informacji).

Domyślnie: 3
 Zakres: 0-5

DenyKey

Zabrania wykonywania tych kluczy pozycji, które pasują do wzorca. Wzorzec klucza jest wyrażeniem wieloznacznym obsługującym znak "*", który dopasowuje dowolną liczbę dowolnych znaków.
Można zdefiniować wiele reguł dopasowania kluczy w połączeniu z AllowKey. Parametry są przetwarzane jeden po drugim zgodnie z kolejnością ich występowania. Zobacz także: Ograniczanie kontroli agenta.

EnableRemoteCommands

Czy zdalne polecenia z serwera Zabbix są dozwolone. Ten parametr jest **przestarzały**; zamiast niego użyj AllowKey=system.run[*] lub DenyKey=system.run[*].
Jest to wewnętrzny alias parametrów AllowKey/DenyKey zależnie od wartości:
0 - DenyKey=system.run[*]
1 - AllowKey=system.run[*]

Domyślnie: 0
 Wartości: 0 - nie zezwalaj, 1 - zezwalaj

HeartbeatFrequency

Częstotliwość komunikatów heartbeat w sekundach. Używana do monitorowania dostępności aktywnych kontroli.
0 - komunikaty heartbeat wyłączone.

Domyślnie: 60
 Zakres: 0-3600

HostInterface

Opcjonalny parametr określający interfejs hosta (adres IP lub nazwę DNS) używany podczas procesu autorejestracji. Ta wartość zostanie użyta do wypełnienia interfejsu w nowo utworzonym hoście i umożliwia jawną konfigurację adresu IP lub DNS. Więcej informacji można znaleźć w sekcji Using DNS as default interface.

Jeśli parametr nie jest zdefiniowany, wartość zostanie pobrana z HostInterfaceItem.

agent zgłosi błąd i nie uruchomi się, jeśli wartość przekroczy limit 255 znaków.

Zakres: 0-255 znaków

HostInterfaceItem

Opcjonalny parametr definiujący pozycję używaną do określenia interfejsu hosta (adresu IP lub nazwy DNS) podczas procesu autorejestracji. Ta wartość jest używana tylko wtedy, gdy HostInterface nie jest zdefiniowany. Więcej szczegółów można znaleźć w sekcji Używanie DNS jako domyślnego interfejsu.

Podczas żądania autorejestracji agent zapisze komunikat ostrzegawczy w logu, jeśli wartość zwrócona przez określoną pozycję przekracza limit 255 znaków.

Pozycja system.run[] jest obsługiwana niezależnie od ustawień AllowKey/DenyKey.

HostMetadata

Opcjonalny parametr definiujący metadane używane do identyfikacji lub rozróżniania hosta podczas procesu autorejestracji hosta (aktywny agent). HostMetadata umożliwia rozróżnianie hostów niezależnie od nazwy hosta.

Jeśli nie jest zdefiniowany, wartość zostanie pobrana z HostMetadataItem.

agent zgłosi błąd i nie uruchomi się, jeśli podana wartość przekracza limit 2034 bajtów lub jest ciągiem w formacie innym niż UTF-8. Gdy parametr oczekuje adresu IP lub nazwy DNS, wartości będące poprawnym UTF-8, ale niebędące poprawnymi adresami IP ani nazwami DNS, również zostaną odrzucone i zgłoszone jako nieprawidłowe.

Zakres: 0-2034 bajtów

HostMetadataItem

Opcjonalny parametr definiujący pozycję agenta Zabbix używaną do pobierania metadanych hosta. Ta opcja jest używana tylko wtedy, gdy parametr HostMetadata nie jest zdefiniowany.

Wartość HostMetadataItem jest pobierana przy każdej próbie autorejestracji i jest używana wyłącznie w procesie autorejestracji hosta (agent aktywny). HostMetadataItem umożliwia rozróżnianie hostów na podstawie czegoś więcej niż tylko nazwy hosta.

Parametry użytkownika i aliasy są obsługiwane. Pozycja system.run[] jest obsługiwana niezależnie od ustawień AllowKey/DenyKey.

Podczas żądania autorejestracji agent zapisze ostrzeżenie w logu, jeśli wartość zwrócona przez określoną pozycję przekroczy limit 65535 punktów kodowych UTF-8. Wartość zwrócona przez pozycję musi być ciągiem UTF-8, w przeciwnym razie zostanie zignorowana. Gdy parametr oczekuje adresu IP lub nazwy DNS, wartości będące poprawnym UTF-8, ale niebędące poprawnymi adresami IP ani nazwami DNS, również zostaną odrzucone i zgłoszone jako nieprawidłowe.

Hostname

Lista unikalnych nazw hostów rozdzielonych przecinkami, z rozróżnianiem wielkości liter. Wymagane dla aktywnych kontroli i musi odpowiadać nazwom hostów skonfigurowanym na serwerze. Wartość jest pobierana z HostnameItem, jeśli nie jest zdefiniowana.
Dozwolone znaki: alfanumeryczne, '.', ' ', '_' i '-'. Maksymalna długość: 128 znaków na nazwę hosta, 2048 znaków dla całego wiersza.

Domyślnie: Ustawiane przez HostnameItem

HostnameItem

Opcjonalny parametr definiujący pozycję agenta Zabbix używaną do pobierania nazwy hosta. Ta opcja jest używana tylko wtedy, gdy parametr Hostname nie jest zdefiniowany. Parametry użytkownika ani aliasy nie są obsługiwane, ale pozycja system.run[] jest obsługiwana niezależnie od wartości AllowKey/DenyKey.

Domyślnie: `system.hostname`

Include

Możesz dołączyć pojedyncze pliki lub wszystkie pliki w katalogu w pliku konfiguracyjnym. Aby uwzględnić tylko odpowiednie pliki w określonym katalogu, obsługiwany jest znak wieloznaczny gwiazdki do dopasowywania wzorców.
Zobacz uwagi specjalne dotyczące ograniczeń.

Przykład:

```
Include=/absolute/path/to/config/files/*.conf
```

ListenBacklog

Maksymalna liczba oczekujących połączeń w kolejce TCP.
Wartość domyślna jest stałą zakodowaną na sztywno i zależy od systemu.
Maksymalna obsługiwana wartość również zależy od systemu; zbyt wysokie wartości mogą zostać po cichu obcięte do „maksimum określonego przez implementację”.

Domyślnie: SOMAXCONN
 Zakres: 0 - INT_MAX

ListenIP

Lista adresów IP rozdzielonych przecinkami, na których agent powinien nasłuchiwać.

Wartość domyślna: 0.0.0.0

ListenPort

agent będzie nasłuchiwał na tym porcie połączeń z serwera.

Domyślnie: 10050
 Zakres: 1024-32767

LoadModule

Moduł do załadowania podczas uruchamiania agenta. Moduły są używane do rozszerzania funkcjonalności agenta. Moduł musi znajdować się w katalogu określonym przez LoadModulePath lub ścieżka musi poprzedzać nazwę modułu. Jeśli poprzedzająca ścieżka jest bezwzględna (zaczyna się od ’/’), wtedy LoadModulePath jest ignorowane.
Formaty:
LoadModule=<module.so>
LoadModule
jest uwzględnienie wielu parametrów LoadModule.

LoadModulePath

Pełna ścieżka do lokalizacji modułów agenta. Wartość domyślna zależy od opcji kompilacji.

LogFile

Nazwa pliku dziennika.

Wymagane: Tak, jeśli LogType jest ustawione na *file*; w przeciwnym razie nie

LogFileSize

Maksymalny rozmiar pliku dziennika w MB.
0 — wyłącza automatyczną rotację logów.
Uwaga: Jeśli zostanie osiągnięty limit rozmiaru pliku dziennika, a rotacja pliku nie powiedzie się z jakiegokolwiek powodu, istniejący plik dziennika zostanie obcięty i rozpoczęty od nowa.

Wartość domyślna: 1
 Zakres: 0-1024

LogRemoteCommands

Włącz rejestrowanie wykonywanych poleceń powłoki jako ostrzeżeń. Polecenia będą rejestrowane tylko wtedy, gdy są wykonywane zdalnie. Wpisy dziennika nie będą tworzone, jeśli system.run[] jest uruchamiane lokalnie przez parametry HostMetadataItem, HostInterfaceItem lub HostnameItem.

Domyślnie: 0
 Wartości: 0 - wyłączone, 1 - włączone

LogType

Typ wyjścia logu:
file - zapisuje log do pliku określonego parametrem LogFile;
system - zapisuje log do syslog;
console - zapisuje log na standardowe wyjście.

Wartość domyślna: file

MaxLinesPerSecond

Maksymalna liczba nowych linii, które agent wyśle na sekundę do serwera Zabbix lub proxy podczas przetwarzania aktywnych kontroli „log” i „logrt”. Podana wartość zostanie nadpisana przez parametr „maxlines” podany w kluczu pozycji „log” lub „logrt”.
Uwaga: Zabbix przetworzy 10 razy więcej nowych linii niż ustawiono w *MaxLinesPerSecond*, aby wyszukać wymagany ciąg znaków w pozycjach logów.

Wartość domyślna: 20
 Zakres: 1-1000

PidFile

Nazwa pliku PID.

Domyślnie: /tmp/zabbix_agentd.pid

RefreshActiveChecks

Jak często odświeżana jest lista aktywnych kontroli, w sekundach. Należy pamiętać, że po nieudanej próbie odświeżenia aktywnych kontroli kolejna próba odświeżenia zostanie podjęta za 60 sekund.

Domyślnie: 5
 Zakres: 1-86400

Serwer

Lista adresów IP oddzielonych przecinkami, opcjonalnie w notacji CIDR, lub nazw DNS serwerów Zabbix i proxy Zabbix. Połączenia przychodzące będą akceptowane tylko od hostów wymienionych tutaj. Jeśli obsługa IPv6 jest włączona, wtedy '127.0.0.1', '::127.0.0.1', '::ffff:127.0.0.1' są traktowane jednakowo, a '::/0' pozwoli na dowolny adres IPv4 lub IPv6. '0.0.0.0/0' może być użyte do zezwolenia na dowolny adres IPv4. Należy pamiętać, że „adresy IPv6 zgodne z IPv4" (prefiks 0000::/96) są obsługiwane, ale przestarzałe zgodnie z RFC4291. Spacje są dozwolone.

Przykład:

```
Server=127.0.0.1,192.168.1.0/24,::1,2001:db8::/32,zabbix.example.com
```

Wymagane: tak, jeśli StartAgents nie jest jawnie ustawione na 0

ServerActive

Adres serwera/proxy Zabbix lub konfiguracja klastra, z którego pobierane są aktywne kontrole. Adres serwera/proxy to adres IP lub nazwa DNS oraz opcjonalny port oddzielony dwukropkiem.
Konfiguracja klastra to jeden lub więcej adresów członków grupy serwera lub proxy oddzielonych średnikiem. Można określić wiele serwerów/klastrów Zabbix oraz proxy Zabbix, oddzielając je przecinkami. Jeśli nie są używane grupy proxy, nie należy określać więcej niż jednego proxy Zabbix z każdego serwera/klastra Zabbix. Jeśli określono proxy Zabbix, nie należy określać serwera/klastra Zabbix dla tego proxy.
Można podać wiele adresów oddzielonych przecinkami, aby równolegle używać kilku niezależnych serwerów Zabbix. Spacje są dozwolone.
Jeśli port nie został określony, używany jest port domyślny.
Adresy IPv6 muszą być ujęte w nawiasy kwadratowe, jeśli dla tego hosta określono port. Jeśli port nie został określony, nawiasy kwadratowe dla adresów IPv6 są opcjonalne.
Jeśli ten parametr nie zostanie określony, aktywne kontrole są wyłączone.

Przykład dla proxy Zabbix:

```
ServerActive=127.0.0.1:10051
```

Przykład dla grupy proxy Zabbix:

```
ServerActive=proxy1.example.com;proxy2.example.com;proxy3.example.com;proxy4.example.com;proxy5.example.co
```

Przykład dla wielu serwerów:

```
ServerActive=127.0.0.1:20051,zabbix.domain,[::1]:30051,::1,[12fc::1]
```

Przykład dla wysokiej dostępności:

```
ServerActive=zabbix.cluster.node1;zabbix.cluster.node2:20051;zabbix.cluster.node3
```

Przykład dla wysokiej dostępności z dwoma klastrami i jednym serwerem:

```
ServerActive=zabbix.cluster.node1;zabbix.cluster.node2:20051,zabbix.cluster2.node1;zabbix.cluster2.node2,z
```

SourceIP

Źródłowy adres IP dla:

- połączeń wychodzących do serwera Zabbix lub proxy Zabbix;
- nawiązywania połączeń podczas wykonywania niektórych pozycji (web.page.get, net.tcp.port itp.).

StartAgents

Liczba wstępnie utworzonych instancji zabbix_agentd, które przetwarzają kontrole pasywne. Jeśli ustawiono 0, kontrole pasywne są wyłączone, a agent nie będzie nasłuchiwał na żadnym porcie TCP.

Wartość domyślna: 10
 Zakres: 0-100

Timeout

Określa, jak długo czekać (w sekundach) na nawiązanie połączenia i wymianę danych z proxy lub serwerem Zabbix.

Ten parametr określa czas trwania różnych operacji komunikacyjnych, w tym:

- oczekiwania na odpowiedź od serwera Zabbix;
- wysyłania żądań do serwera Zabbix, w tym żądań konfiguracji pozycji oraz danych pozycji w aktywnych testach;
- pobierania danych logów przez logfile;
- wysyłania komunikatów heartbeat;
- maksymalnego czasu trwania testów `vfs.*`;

- użycia przez moduły agenta Zabbix;
- użycia jako wartości zapasowej w scenariuszach, gdy serwer lub proxy starszy niż wersja 7.0 wysyła testy bez limitów czasu.

Ten limit czasu **nie** będzie używany dla tych testów agenta, które mają konfigurowalne ustawienia limitu czasu we frontendzie (na poziomie globalnym, proxy lub pojedynczej pozycji).

Wartość domyślna: 3
 Zakres: 1-30

TLSAccept

Jakie połączenia przychodzące akceptować. Używane dla pasywnych kontroli. Można określić wiele wartości, oddzielonych przecinkami:
unencrypted - akceptuj połączenia bez szyfrowania (domyślnie)
psk - akceptuj połączenia z TLS i kluczem współdzielonym (PSK)
cert - akceptuj połączenia z TLS i certyfikatem

Wymagane: tak, jeśli zdefiniowano parametry certyfikatu TLS lub PSK (nawet dla połączenia *unencrypted*); w przeciwnym razie nie

TLSCAFile

Pełna ścieżka do pliku zawierającego certyfikaty nadrzędnych urzędów certyfikacji (CA) używane do weryfikacji certyfikatu peera, wykorzystywana do szyfrowanej komunikacji między komponentami Zabbix.

TLSCertFile

Pełna ścieżka do pliku zawierającego certyfikat agenta lub łańcuch certyfikatów, używanego do szyfrowanej komunikacji z komponentami Zabbix.

TLSCipherAll

Ciąg priorytetów GnuTLS lub ciąg szyfrów OpenSSL (TLS 1.2). Nadpisuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na certyfikatach i PSK.

Przykład:

```
TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256
```

TLSCipherAll13

Ciąg szyfrów dla OpenSSL 1.1.1 lub nowszego w TLS 1.3. Zastępuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na certyfikatach i PSK.

Przykład dla GnuTLS:

```
NONE:+VERS-TLS1.2:+ECDHE-RSA:+RSA:+ECDHE-PSK:+PSK:+AES-128-GCM:+AES-128-CBC:+AEAD:+SHA256:+SHA1:+CURVE-ALL
```

Przykład dla OpenSSL:

```
EECDH+aRSA+AES128:RSA+aRSA+AES128:kECDHEPSK+AES128:kPSK+AES128
```

TLSCipherCert

Ciąg priorytetów GnuTLS lub ciąg szyfrów OpenSSL (TLS 1.2). Nadpisuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na certyfikatach.

Przykład dla GnuTLS:

```
NONE:+VERS-TLS1.2:+ECDHE-RSA:+RSA:+AES-128-GCM:+AES-128-CBC:+AEAD:+SHA256:+SHA1:+CURVE-ALL:+COMP-NULL:+SIG
```

Przykład dla OpenSSL:

```
EECDH+aRSA+AES128:RSA+aRSA+AES128
```

TLSCipherCert13

Ciąg szyfrów dla OpenSSL 1.1.1 lub nowszego w TLS 1.3. Zastępuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na certyfikatach.

TLSCipherPSK

Ciąg priorytetów GnuTLS lub ciąg szyfrów OpenSSL (TLS 1.2). Nadpisuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na PSK.

Przykład dla GnuTLS:

```
NONE:+VERS-TLS1.2:+ECDHE-PSK:+PSK:+AES-128-GCM:+AES-128-CBC:+AEAD:+SHA256:+SHA1:+CURVE-ALL:+COMP-NULL:+SIG
```

Przykład dla OpenSSL:

```
kECDHEPSK+AES128:kPSK+AES128
```

TLSCipherPSK13

Ciąg szyfrów dla OpenSSL 1.1.1 lub nowszego w TLS 1.3. Zastępuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na PSK.

Przykład:

```
TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256
```

TLSConnect

Jak agent powinien łączyć się z serwerem lub proxy Zabbix. Używane dla aktywnych testów. Można określić tylko jedną wartość:
unencrypted - połączenie bez szyfrowania (domyślnie)
psk - połączenie z użyciem TLS i klucza współdzielonego (PSK)
cert - połączenie z użyciem TLS i certyfikatu

Wymagane: tak, jeśli zdefiniowano parametry certyfikatu TLS lub PSK (nawet dla połączenia *unencrypted*); w przeciwnym razie nie

TLSCRLFile

Pełna ścieżka do pliku zawierającego unieważnione certyfikaty. Ten parametr jest używany do szyfrowanej komunikacji między komponentami Zabbix.

TLSKeyFile

Pełna ścieżka do pliku zawierającego klucz prywatny agenta, używanego do szyfrowanej komunikacji między komponentami Zabbix.

TLSPSKFile

Pełna ścieżka do pliku zawierającego klucz współdzielony agenta, używany do szyfrowanej komunikacji z serwerem Zabbix.

TLSPSKIdentity

Ciąg tożsamości klucza współdzielonego, używany do szyfrowanej komunikacji z serwerem Zabbix.

TLSServerCertIssuer

Dozwolony wystawca certyfikatu serwera (proxy).

TLSServerCertSubject

Dozwolony temat certyfikatu serwera (proxy).

UnsafeUserParameters

Zezwala na przekazywanie wszystkich znaków w argumentach do parametrów zdefiniowanych przez użytkownika. Następujące znaki są niedozwolone: \ ' " ` * ? [ ] { } ~ $! & ; ( ) < > | # @ %
Dodatkowo znaki nowej linii są niedozwolone.

Wartość domyślna: 0
 Wartości: 0 - nie zezwalaj, 1 - zezwalaj

Użytkownik

Obniża uprawnienia do określonego, istniejącego użytkownika w systemie.
Ma zastosowanie tylko w przypadku uruchomienia jako `root`, gdy opcja AllowRoot jest wyłączona.

Wartość domyślna: `zabbix`

UserParameter

Parametr zdefiniowany przez użytkownika do monitorowania. Może istnieć kilka parametrów zdefiniowanych przez użytkownika.
Format: UserParameter=<key>,<shell command>
Należy pamiętać, że polecenie powłoki nie może zwracać pustego ciągu ani wyłącznie znaku końca linii. Polecenia powłoki mogą używać ścieżek względnych, jeśli określono parametr UserParameterDir.

Przykład:

```
UserParameter=system.test,who|wc -l
UserParameter=check_cpu,./custom_script.sh
```

UserParameterDir

Domyślna ścieżka wyszukiwania dla poleceń UserParameter. Jeśli jest używana, agent zmieni swój katalog roboczy na katalog określony tutaj przed wykonaniem polecenia. Dzięki temu polecenia UserParameter mogą mieć względny prefiks `./` zamiast pełnej ścieżki.
Dozwolony jest tylko jeden wpis.

Przykład:

```
UserParameterDir=/opt/myscripts
```

Zobacz także

1. Różnice w konfiguracji agenta Zabbix dla aktywnych i pasywnych kontroli począwszy od wersji 2.0.0

4 Zabbix agent 2 (UNIX)

Przegląd

Zabbix agent 2 to nowa generacja agenta Zabbix i może być używany zamiast agenta Zabbix.

Parametry obsługiwane przez plik konfiguracyjny Zabbix agent 2 (zabbix_agent2.conf) są wymienione w tej sekcji.

Parametry są wymienione bez dodatkowych informacji. Kliknij parametr, aby zobaczyć pełne szczegóły.

Parameter	Description
Alias	Ustawia alias dla klucza pozycji.
AllowKey	Zezwala na wykonywanie tych kluczy pozycji, które pasują do wzorca.
BufferSend	Nie przechowuje danych w buforze dłużej niż N sekund.
BufferSize	Maksymalna liczba wartości w buforze pamięci.
ControlSocket	Gniazdo sterujące używane do wysyłania poleceń w czasie działania za pomocą opcji '-R'.
DebugLevel	Poziom debugowania.
DenyKey	Zabrania wykonywania tych kluczy pozycji, które pasują do wzorca.
EnablePersistentBuffer	Włącza użycie lokalnej trwałej pamięci masowej dla aktywnych pozycji.
ForceActiveChecksOnStart	Wykonuje aktywne sprawdzenia natychmiast po restarcie dla pierwszej otrzymanej konfiguracji.
HeartbeatFrequency	Częstotliwość komunikatów heartbeat w sekundach.
HostInterface	Opcjonalny parametr definiujący interfejs hosta.
HostInterfaceItem	Opcjonalny parametr definiujący pozycję używaną do pobierania interfejsu hosta.
HostMetadata	Opcjonalny parametr definiujący metadane hosta.
HostMetadataItem	Opcjonalny parametr definiujący pozycję agenta Zabbix używaną do pobierania metadanych hosta.
Hostname	Opcjonalny parametr definiujący nazwę hosta.
HostnameItem	Opcjonalny parametr definiujący pozycję agenta Zabbix używaną do pobierania nazwy hosta.
Include	Możesz dołączyć pojedyncze pliki lub wszystkie pliki z katalogu do pliku konfiguracyjnego.
ListenIP	Lista adresów IP oddzielonych przecinkami, na których agent powinien nasłuchiwać.
ListenPort	Agent będzie nasłuchiwał na tym porcie połączeń z serwera.
LogFile	Nazwa pliku dziennika.
LogFileSize	Maksymalny rozmiar pliku dziennika.
LogType	Typ wyjścia dziennika.
PersistentBufferFile	Plik, w którym Zabbix agent 2 powinien przechowywać bazę danych SQLite.
PersistentBufferPeriod	Okres, przez który dane powinny być przechowywane, gdy nie ma połączenia z serwerem lub proxy.
PidFile	Nazwa pliku PID.
Plugins.<PluginName>.System.Capacity	Limit sprawdzeń na plugin, które mogą być wykonywane jednocześnie.
Plugins.Log.MaxLinesPerSecond	Maksymalna liczba nowych wierszy, które agent wyśle na sekundę do serwera Zabbix lub proxy podczas przetwarzania aktywnych sprawdzeń 'log' i 'logrt'.
Plugins.SystemRun.LogRemoteCommands	Włącza rejestrowanie wykonywanych poleceń powłoki jako ostrzeżeń.
PluginSocket	Ścieżka do gniazda UNIX dla komunikacji z ładowalnymi pluginami.
PluginTimeout	Limit czasu połączeń z ładowalnymi pluginami, w sekundach.
RefreshActiveChecks	Jak często odświeżana jest lista aktywnych sprawdzeń.
Server	Lista adresów IP oddzielonych przecinkami, opcjonalnie w notacji CIDR, lub nazw DNS serwerów Zabbix i proxy Zabbix.
ServerActive	Adres serwera/proxy Zabbix lub konfiguracja klastra, z którego pobierane są aktywne sprawdzenia.
SourceIP	Źródłowy adres IP.
StatusPort	Jeśli ustawiony, agent będzie nasłuchiwał na tym porcie żądań statusu HTTP (http://localhost:<port>/status).
Timeout	Określa, jak długo czekać (w sekundach) na ustanowienie połączenia i wymianę danych z proxy Zabbix lub serwerem.
TLSAccept	Jakie połączenia przychodzące akceptować.
TLSCAFile	Pełna ścieżka do pliku zawierającego certyfikaty nadrzędnych urzędów certyfikacji (CA) do weryfikacji certyfikatu peera, używana do szyfrowanej komunikacji między komponentami Zabbix.

Parameter	Description
TLSCertFile	Pełna ścieżka do pliku zawierającego certyfikat agenta lub łańcuch certyfikatów, używana do szyfrowanej komunikacji między komponentami Zabbix.
TLSCipherAll	Ciąg szyfrów OpenSSL (TLS 1.2). Zastępuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na certyfikatach i PSK.
TLSCipherAll13	Ciąg szyfrów OpenSSL (TLS 1.3) dla OpenSSL 1.1.1 lub nowszego. Zastępuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na certyfikatach i PSK.
TLSCipherCert	Ciąg szyfrów OpenSSL (TLS 1.2). Zastępuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na certyfikatach.
TLSCipherCert13	Ciąg szyfrów OpenSSL (TLS 1.3) dla OpenSSL 1.1.1 lub nowszego. Zastępuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na certyfikatach.
TLSCipherPSK	Ciąg szyfrów OpenSSL (TLS 1.2). Zastępuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na PSK.
TLSCipherPSK13	Ciąg szyfrów OpenSSL (TLS 1.3) dla OpenSSL 1.1.1 lub nowszego. Zastępuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na PSK.
TLSConnect	W jaki sposób agent powinien łączyć się z serwerem Zabbix lub proxy.
TLSCRLFile	Pełna ścieżka do pliku zawierającego unieważnione certyfikaty. Ten parametr jest używany do szyfrowanej komunikacji między komponentami Zabbix.
TLSKeyFile	Pełna ścieżka do pliku zawierającego klucz prywatny agenta, używana do szyfrowanej komunikacji między komponentami Zabbix.
TLSPSKFile	Pełna ścieżka do pliku zawierającego klucz współdzielony agenta, używana do szyfrowanej komunikacji z serwerem Zabbix.
TLSPSKIdentity	Ciąg identyfikatora klucza współdzielonego, używany do szyfrowanej komunikacji z serwerem Zabbix.
TLSServerCertIssuer	Dozwolony wystawca certyfikatu serwera (proxy).
TLSServerCertSubject	Dozwolony podmiot certyfikatu serwera (proxy).
UnsafeUserParameters	Zezwala na przekazywanie wszystkich znaków w argumentach do parametrów zdefiniowanych przez użytkownika.
UserParameter	Parametr zdefiniowany przez użytkownika do monitorowania.
UserParameterDir	Domyślna ścieżka wyszukiwania dla poleceń UserParameter.

Wszystkie parametry są opcjonalne, chyba że wyraźnie stwierdzono, że parametr jest obowiązkowy.

Uwaga:

- Wartości domyślne odzwierciedlają wartości domyślne procesu, a nie wartości w dostarczonych plikach konfiguracyjnych.
- Wartości obsługują zmienne środowiskowe.
- Zabbix obsługuje pliki konfiguracyjne tylko w kodowaniu UTF-8 bez BOM.
- Komentarze rozpoczynające się od "#" są obsługiwane tylko na początku wiersza.

Szczegóły parametrów

Alias

Ustawia alias dla klucza pozycji. Może być używany do zastąpienia długiego i złożonego klucza pozycji krótszym i prostszym.
 Może występować wiele parametrów *Alias*. Wiele parametrów z tym samym kluczem *Alias* jest niedozwolonych.
 Różne klucze *Alias* mogą wskazywać ten sam klucz pozycji.
 Aliasy mogą być używane w parametrze *HostMetadataItem*, ale nie w parametrze *HostnameItem*.

Przykład 1: Pobieranie identyfikatora użytkownika „zabbix".

```
Alias=zabbix.userid:vfs.file.regexp[/etc/passwd,"^zabbix:.:([0-9]+)",,,,\1]
```

Teraz skrócony klucz **zabbix.userid** może być używany do pobierania danych.

Przykład 2: Pobieranie wykorzystania CPU z parametrami domyślnymi i niestandardowymi.

```
Alias=cpu.util:system.cpu.util
Alias=cpu.util[*]:system.cpu.util[*]
```

Pozwala to używać klucza **cpu.util** do uzyskania procentowego wykorzystania CPU z parametrami domyślnymi, a także używać **cpu.util[all, idle, avg15]** do uzyskania szczegółowych danych o wykorzystaniu CPU.

Przykład 3: Uruchamianie wielu reguł odkrywania niskiego poziomu przetwarzających te same pozycje odkrywania.

```
Alias=vfs.fs.discovery[*]:vfs.fs.discovery
```

Teraz możliwe jest skonfigurowanie kilku reguł odkrywania używających **vfs.fs.discovery** z różnymi parametrami dla każdej reguły, np. **vfs.fs.discovery[foo]**, **vfs.fs.discovery[bar]** itd.

AllowKey

Zezwalaj na wykonywanie tych kluczy pozycji, które pasują do wzorca. Wzorzec klucza jest wyrażeniem wieloznacznym obsługującym znak "*", który dopasowuje dowolną liczbę dowolnych znaków.
Można zdefiniować wiele reguł dopasowania kluczy w połączeniu z DenyKey. Parametry są przetwarzane jeden po drugim zgodnie z kolejnością ich występowania. Zobacz także: Ograniczanie kontroli agenta.

BufferSend

Interwał czasu w sekundach określający, jak często wartości są wysyłane z bufora do serwera Zabbix. Należy pamiętać, że jeśli bufor jest pełny, dane zostaną wysłane wcześniej.

Domyślnie: 5
 Zakres: 1-3600

BufferSize

Maksymalna liczba wartości w buforze pamięci. agent wyśle wszystkie zebrane dane do serwera Zabbix lub proxy, jeśli bufor jest pełny. Ten parametr powinien być używany tylko wtedy, gdy trwały bufor jest wyłączony (*EnablePersistentBuffer=0*).

Domyślnie: 1000
 Zakres: 2-65535

ControlSocket

Gniazdo sterujące, używane do wysyłania poleceń w czasie działania za pomocą opcji '-R'.

Domyślnie: `/tmp/agent.sock`

DebugLevel

Określ poziom debugowania:
0 - podstawowe informacje o uruchamianiu i zatrzymywaniu procesów Zabbix
1 - informacje krytyczne;
2 - informacje o błędach;
3 - ostrzeżenia;
4 - do debugowania (generuje dużo informacji);
5 - rozszerzone debugowanie (generuje jeszcze więcej informacji).

Domyślnie: 3
 Zakres: 0-5

DenyKey

Zabrania wykonywania tych kluczy pozycji, które pasują do wzorca. Wzorzec klucza jest wyrażeniem wieloznacznym obsługującym znak "*", który dopasowuje dowolną liczbę dowolnych znaków.
Można zdefiniować wiele reguł dopasowania kluczy w połączeniu z AllowKey. Parametry są przetwarzane jeden po drugim zgodnie z kolejnością ich występowania. Zobacz także: Ograniczanie kontroli agenta.

EnablePersistentBuffer

Włącz użycie lokalnej trwałej pamięci masowej dla aktywnych pozycji. Jeśli trwała pamięć masowa jest wyłączona, użyty zostanie bufor pamięci.

Domyślnie: 0
 Wartości: 0 - wyłączone, 1 - włączone

ForceActiveChecksOnStart

Wykonuj aktywne sprawdzenia natychmiast po restarcie dla pierwszej otrzymanej konfiguracji. Dostępne również jako parametr konfiguracji dla każdej wtyczki, na przykład: `Plugins.Uptime.System.ForceActiveChecksOnStart=1`

Domyślnie: 0
 Wartości: 0 - wyłączone, 1 - włączone

HeartbeatFrequency

Częstotliwość komunikatów heartbeat w sekundach. Używana do monitorowania dostępności aktywnych testów.
0 - komunikaty heartbeat wyłączone.

Domyślnie: 60
 Zakres: 0-3600

HostInterface

Opcjonalny parametr definiujący interfejs hosta (adres IP lub nazwę DNS) używany podczas procesu autorejestracji hosta. Ta wartość zostanie użyta do wypełnienia interfejsu w nowo utworzonym hoście i umożliwia jawną konfigurację adresu IP lub DNS. Aby uzyskać więcej informacji, zobacz Używanie DNS jako domyślnego interfejsu.

Jeśli nie jest zdefiniowany, wartość zostanie pobrana z HostInterfaceItem.

agent zgłosi błąd i nie uruchomi się, jeśli wartość przekroczy limit 255 znaków.

Zakres: 0-255 znaków

HostInterfaceItem

Opcjonalny parametr definiujący pozycję używaną do określenia interfejsu hosta (adresu IP lub nazwy DNS) podczas procesu autoregistration hosta. Ta wartość jest używana tylko wtedy, gdy HostInterface nie jest zdefiniowany. Aby uzyskać więcej informacji, zobacz Using DNS as default interface.

Podczas żądania autorejestracji agent zapisze komunikat ostrzegawczy w logu, jeśli wartość zwrócona przez określoną pozycję przekracza limit 255 znaków.

Pozycja system.run[] jest obsługiwana niezależnie od ustawień AllowKey/DenyKey.

HostMetadata

Opcjonalny parametr określający metadane używane do identyfikacji lub rozróżniania hosta podczas procesu autorejestracji hosta. HostMetadata umożliwia rozróżnianie hostów niezależnie od nazwy hosta.

Jeśli nie jest zdefiniowany, wartość zostanie pobrana z HostMetadataItem.

agent zgłosi błąd i nie uruchomi się, jeśli podana wartość przekracza limit 2034 bajtów lub jest ciągiem znaków innym niż UTF-8. Gdy parametr oczekuje adresu IP lub nazwy DNS, wartości będące poprawnym UTF-8, ale niebędące prawidłowymi adresami IP ani nazwami DNS, również zostaną odrzucone i zgłoszone jako nieprawidłowe.

Zakres: 0-2034 bajtów

HostMetadataItem

Opcjonalny parametr definiujący pozycję agenta Zabbix używaną do pobierania metadanych hosta. Ta opcja jest używana tylko wtedy, gdy HostMetadata nie jest zdefiniowany.

Wartość HostMetadataItem jest pobierana przy każdej próbie autorejestracji i jest używana wyłącznie w procesie autorejestracji hosta. HostMetadataItem umożliwia rozróżnianie hostów na podstawie czegoś więcej niż tylko nazwy hosta.

Parametry użytkownika i aliasy są obsługiwane. Pozycja system.run[] jest obsługiwana niezależnie od ustawień AllowKey/DenyKey.

Podczas żądania autorejestracji agent zapisze komunikat ostrzegawczy w logu, jeśli wartość zwrócona przez określoną pozycję przekroczy limit 65535 punktów kodowych UTF-8. Wartość zwrócona przez pozycję musi być ciągiem UTF-8, w przeciwnym razie zostanie zignorowana. Gdy parametr oczekuje adresu IP lub nazwy DNS, wartości będące poprawnym UTF-8, ale niebędące prawidłowymi adresami IP ani nazwami DNS, również zostaną odrzucone i zgłoszone jako nieprawidłowe.

Hostname

Lista unikalnych nazw hostów rozdzielonych przecinkami, z rozróżnianiem wielkości liter. Wymagane dla aktywnych kontroli i musi odpowiadać nazwom hostów skonfigurowanym na serwerze. Wartość jest pobierana z HostnameItem, jeśli nie jest zdefiniowana.
Dozwolone znaki: alfanumeryczne, '.', ' ', '_' i '-'. Maksymalna długość: 128 znaków na nazwę hosta, 2048 znaków dla całego wiersza.

Domyślnie: Ustawiane przez HostnameItem

HostnameItem

Opcjonalny parametr definiujący pozycję używaną do pobierania nazwy hosta. Ta opcja jest używana tylko wtedy, gdy Hostname nie jest zdefiniowany. Parametry użytkownika ani aliasy nie są obsługiwane, ale pozycja system.run[] jest obsługiwana niezależnie od wartości AllowKey/DenyKey.

Wartość domyślna: `system.hostname`

Include

Możesz dołączyć pojedyncze pliki lub wszystkie pliki w katalogu w pliku konfiguracyjnym. Podczas instalacji Zabbix utworzy katalog include w /usr/local/etc, chyba że zostanie to zmienione podczas kompilacji. Ścieżka może być względna względem lokalizacji pliku *zabbix_agent2.conf*.
Aby dołączyć tylko odpowiednie pliki w określonym katalogu, obsługiwany jest znak wieloznaczny gwiazdki do dopasowywania wzorców.
Zobacz uwagi specjalne dotyczące ograniczeń.

Przykład:

```
Include=/absolute/path/to/config/files/*.conf
```

ListenIP

Lista adresów IP rozdzielonych przecinkami, na których agent powinien nasłuchiwać. Pierwszy adres IP jest wysyłany do serwera Zabbix, jeśli agent łączy się z nim, aby pobrać listę aktywnych kontroli.

Wartość domyślna: `0.0.0.0`

ListenPort

agent będzie nasłuchiwał na tym porcie połączeń z serwera.

Domyślnie: 10050
 Zakres: 1024-32767

LogFile

Nazwa pliku dziennika.

Domyślnie: `/tmp/zabbix_agent2.log`
 Wymagane: Tak, jeśli LogType jest ustawione na *file*; w przeciwnym razie nie

LogFileSize

Maksymalny rozmiar pliku dziennika w MB.
0 - wyłącza automatyczną rotację logów.
Uwaga: Jeśli zostanie osiągnięty limit rozmiaru pliku dziennika, a rotacja pliku nie powiedzie się z jakiegokolwiek powodu, istniejący plik dziennika zostanie obcięty i rozpoczęty od nowa.

Wartość domyślna: 1
 Zakres: 0-1024

LogType

Typ wyjścia logu:
file - zapisuj log do pliku określonego parametrem LogFile;
system - zapisuj log do syslog;
console - zapisuj log na standardowe wyjście

Domyślnie: `file`

PersistentBufferFile

Plik, w którym agent Zabbix 2 powinien przechowywać bazę danych SQLite. Musi to być pełna nazwa pliku. Ten parametr jest używany tylko wtedy, gdy trwały bufor jest włączony (*EnablePersistentBuffer=1*).

PersistentBufferPeriod

Okres, przez który dane powinny być przechowywane, gdy nie ma połączenia z serwerem lub proxy. Starsze dane zostaną utracone. Dane dziennika zostaną zachowane. Ten parametr jest używany tylko wtedy, gdy trwały bufor jest włączony (*EnablePersistentBuffer=1*).

Wartość domyślna: `1h`
 Zakres: 1m-365d

PidFile

Nazwa pliku PID.

Domyślnie: `/tmp/zabbix_agent2.pid`

Plugins.<PluginName>.System.Capacity

Limit kontroli na plugin `<PluginName>`, które mogą być wykonywane jednocześnie.

Domyślnie: 1000 Zakres: 1-1000

Plugins.Log.MaxLinesPerSecond

Maksymalna liczba nowych linii, które agent wyśle na sekundę do serwera Zabbix lub proxy podczas przetwarzania aktywnych kontroli 'log' i 'logrt'. Podana wartość zostanie nadpisana przez parametr 'maxlines' podany w kluczu pozycji 'log' i 'logrt'.
Uwaga: Zabbix przetworzy 10 razy więcej nowych linii niż ustawiono w *MaxLinesPerSecond*, aby wyszukać wymagany ciąg znaków w pozycjach logów.

Wartość domyślna: 20
 Zakres: 1-1000

Plugins.SystemRun.LogRemoteCommands

Włącz rejestrowanie wykonywanych poleceń powłoki jako ostrzeżeń. Polecenia będą rejestrowane tylko wtedy, gdy są wykonywane zdalnie. Wpisy dziennika nie będą tworzone, jeśli system.run[] jest uruchamiane lokalnie przez parametry HostMetadataItem, HostInterfaceItem lub HostnameItem.

Domyślnie: 0
 Wartości: 0 - wyłączone, 1 - włączone

PluginSocket

Ścieżka do gniazda UNIX używanego do komunikacji z ładowalnymi wtyczkami.

Domyślnie: `/tmp/agent.plugin.sock`

PluginTimeout

Limit czasu połączeń z ładowalnymi wtyczkami, w sekundach.

Wartość domyślna: `Timeout`
 Zakres: 1-30

RefreshActiveChecks

Jak często odświeżana jest lista aktywnych testów, w sekundach. Należy pamiętać, że po nieudanej próbie odświeżenia aktywnych testów kolejna próba odświeżenia zostanie podjęta za 60 sekund.

Wartość domyślna: 5
 Zakres: 1-86400

Serwer

Lista adresów IP oddzielonych przecinkami, opcjonalnie w notacji CIDR, lub nazw DNS serwerów Zabbix albo proxy Zabbix. Połączenia przychodzące będą akceptowane tylko od hostów wymienionych tutaj. Jeśli obsługa IPv6 jest włączona, wtedy '127.0.0.1', '::127.0.0.1', '::ffff:127.0.0.1' są traktowane jednakowo, a '::/0' zezwoli na dowolny adres IPv4 lub IPv6. Aby zezwolić na dowolny adres IPv4, można użyć '0.0.0.0/0'. Spacje są dozwolone. Jeśli ten parametr nie jest określony, wyłącza kontrole pasywne, a agent nie będzie nasłuchiwał na żadnym porcie TCP.

Przykład:

```
Server=127.0.0.1,192.168.1.0/24,::1,2001:db8::/32,zabbix.example.com
```

ServerActive

Adres serwera/proxy Zabbix lub konfiguracja klastra, z którego pobierane są aktywne kontrole. Adres serwera/proxy to adres IP lub nazwa DNS oraz opcjonalny port oddzielony dwukropkiem.
Konfiguracja klastra to jeden lub więcej adresów członków grupy serwera lub proxy, oddzielonych średnikiem. Można określić wiele serwerów/klastrów Zabbix oraz proxy Zabbix, oddzielając je przecinkami. Jeśli nie są używane grupy proxy, nie należy określać więcej niż jednego proxy Zabbix z każdego serwera/klastra Zabbix. Jeśli określono proxy Zabbix, nie należy określać serwera/klastra Zabbix dla tego proxy.
Można podać wiele adresów rozdzielonych przecinkami, aby równolegle używać kilku niezależnych serwerów Zabbix. Spacje są dozwolone.
Jeśli port nie został określony, używany jest port domyślny.
Adresy IPv6 muszą być ujęte w nawiasy kwadratowe, jeśli dla danego hosta określono port. Jeśli port nie został określony, nawiasy kwadratowe dla adresów IPv6 są opcjonalne.
Jeśli ten parametr nie zostanie określony, aktywne kontrole są wyłączone.

Przykład dla proxy Zabbix:

```
ServerActive=127.0.0.1:10051
```

Przykład dla grupy proxy Zabbix:

```
ServerActive=proxy1.example.com;proxy2.example.com;proxy3.example.com;proxy4.example.com;proxy5.example.co
```

Przykład dla wielu serwerów:

```
ServerActive=127.0.0.1:20051,zabbix.domain,[::1]:30051,::1,[12fc::1]
```

Przykład dla wysokiej dostępności:

```
ServerActive=zabbix.cluster.node1;zabbix.cluster.node2:20051;zabbix.cluster.node3
```

Przykład dla wysokiej dostępności z dwoma klastrami i jednym serwerem:

```
ServerActive=zabbix.cluster.node1;zabbix.cluster.node2:20051,zabbix.cluster2.node1;zabbix.cluster2.node2,z
```

SourceIP

Źródłowy adres IP dla:

- połączeń wychodzących do serwera Zabbix lub proxy Zabbix.
- nawiązywania połączeń podczas wykonywania niektórych pozycji (web.page.get, net.tcp.port itp.).

StatusPort

Jeśli ustawione, agent będzie nasłuchiwał na tym porcie żądań statusu HTTP (http://localhost:<port>/status).

Zakres: 1024-32767

Timeout

Określa, jak długo czekać (w sekundach) na ustanowienie połączenia i wymianę danych z proxy lub serwerem Zabbix.

Ten parametr definiuje czas trwania różnych operacji komunikacyjnych, w tym:

- oczekiwanie na odpowiedź od serwera Zabbix;
- wysyłanie żądań do serwera Zabbix, w tym żądań konfiguracji pozycji oraz danych pozycji w active checks;
- pobieranie danych logów przez logfile;
- wysyłanie komunikatów heartbeat;
- maksymalny czas trwania kontroli `vfs.*`;
- użycie jako wartości zapasowej w sytuacjach, gdy serwer lub proxy starszy niż wersja 7.0 wysyła kontrole bez limitów czasu.

Ten limit czasu **nie** będzie używany dla tych kontroli agenta, które mają konfigurowalne ustawienia limitu czasu w frontendzie (na poziomie globalnym, proxy lub pojedynczej pozycji).

Wartość domyślna: 3
 Zakres: 1-30

TLSAccept

Przychodzące połączenia do zaakceptowania. Używane dla pasywnych kontroli. Można określić wiele wartości, oddzielonych przecinkami:
unencrypted - akceptuj połączenia bez szyfrowania (domyślnie)
psk - akceptuj połączenia z TLS i kluczem współdzielonym (PSK)
cert - akceptuj połączenia z TLS i certyfikatem

Obowiązkowe: tak, jeśli zdefiniowano parametry certyfikatu TLS lub PSK (nawet dla połączenia *unencrypted*); w przeciwnym razie nie

TLSCAFile

Pełna ścieżka do pliku zawierającego certyfikaty głównego urzędu lub urzędów certyfikacji (CA) do weryfikacji certyfikatu peera, używana do szyfrowanej komunikacji między komponentami Zabbix.

TLSCertFile

Pełna ścieżka do pliku zawierającego certyfikat agenta lub łańcuch certyfikatów, używanego do szyfrowanej komunikacji z komponentami Zabbix.

TLSCipherAll

Ciąg szyfrów OpenSSL (TLS 1.2). Zastępuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na certyfikatach i PSK.

Przykład:

```
EECDH+aRSA+AES128:RSA+aRSA+AES128:kECDHEPSK+AES128:kPSK+AES128
```

TLSCipherAll13

Ciąg szyfrów OpenSSL (TLS 1.3) dla OpenSSL 1.1.1 lub nowszego. Zastępuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na certyfikatach i PSK.

Przykład:

```
TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256
```

TLSCipherCert

Ciąg szyfrów OpenSSL (TLS 1.2). Zastępuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na certyfikatach.

Przykład:

```
EECDH+aRSA+AES128:RSA+aRSA+AES128
```

Należy pamiętać, że ten parametr nie może być używany razem z `TLSAccept=cert,psk`; w przypadku połączenia certyfikatowego (`TLSConnect=cert`) należy zamiast tego użyć TLSCipherAll.

TLSCipherCert13

Ciąg szyfrów OpenSSL (TLS 1.3) dla OpenSSL 1.1.1 lub nowszego. Zastępuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na certyfikatach.

Należy pamiętać, że tego parametru nie można używać razem z `TLSAccept=cert,psk`; w przypadku połączenia certyfikatowego (`TLSConnect=cert`) należy zamiast tego użyć TLSCipherAll13.

TLSCipherPSK

Ciąg szyfrów OpenSSL (TLS 1.2). Zastępuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na PSK.

Przykład:

```
kECDHEPSK+AES128:kPSK+AES128
```

TLSCipherPSK13

Ciąg szyfrów OpenSSL (TLS 1.3) dla OpenSSL 1.1.1 lub nowszego. Zastępuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na PSK.

Przykład:

```
TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256
```

TLSConnect

Jak agent powinien łączyć się z serwerem Zabbix lub proxy. Używane dla aktywnych testów. Można określić tylko jedną wartość:
unencrypted - połącz bez szyfrowania (domyślnie)
psk - połącz przy użyciu TLS i klucza współdzielonego (PSK)
cert - połącz przy użyciu TLS i certyfikatu

Obowiązkowe: tak, jeśli zdefiniowano parametry certyfikatu TLS lub PSK (nawet dla połączenia *unencrypted*); w przeciwnym razie nie

TLSCRLFile

Pełna ścieżka do pliku zawierającego unieważnione certyfikaty. Ten parametr jest używany do szyfrowanej komunikacji między komponentami Zabbix.

TLSKeyFile

Pełna ścieżka do pliku zawierającego klucz prywatny agenta, używanego do szyfrowanej komunikacji między komponentami Zabbix.

TLSPSKFile

Pełna ścieżka do pliku zawierającego klucz współdzielony agent, używany do szyfrowanej komunikacji z serwer Zabbix.

TLSPSKIdentity

Ciąg tożsamości klucza współdzielonego, używany do szyfrowanej komunikacji z serwerem Zabbix.

TLSServerCertIssuer

Dozwolony wystawca certyfikatu serwera (proxy).

TLSServerCertSubject

Dozwolony temat certyfikatu serwera (proxy).

UnsafeUserParameters

Zezwala na przekazywanie wszystkich znaków w argumentach do parametrów zdefiniowanych przez użytkownika. Następujące znaki nie są dozwolone: \ ' " ` * ? [ ] { } ~ $! & ; ( ) < > | # @ %
Dodatkowo znaki nowej linii nie są dozwolone.

Wartość domyślna: 0
 Wartości: 0 - nie zezwalaj, 1 - zezwalaj

UserParameter

Parametr zdefiniowany przez użytkownika do monitorowania. Może istnieć kilka parametrów zdefiniowanych przez użytkownika.
Format: UserParameter=<key>,<polecenie powłoki>
Należy pamiętać, że polecenie powłoki nie może zwracać pustego ciągu ani wyłącznie znaku końca linii. Polecenia powłoki mogą używać ścieżek względnych, jeśli określono parametr UserParameterDir.

Przykład:

```
UserParameter=system.test,who|wc -l
UserParameter=check_cpu,./custom_script.sh
```

UserParameterDir

Domyślna ścieżka wyszukiwania dla poleceń UserParameter. Jeśli jest używana, agent zmieni swój katalog roboczy na określony tutaj przed wykonaniem polecenia. Dzięki temu polecenia UserParameter mogą mieć względny prefiks `./` zamiast pełnej ścieżki.
Dozwolony jest tylko jeden wpis.

Przykład:

```
UserParameterDir=/opt/myscripts
```

5 Zabbix agent (Windows)

Przegląd

Parametry obsługiwane przez plik konfiguracyjny agenta Zabbix dla systemu Windows (zabbix_agentd.conf) są wymienione w tej sekcji.

Parametry są wymienione bez dodatkowych informacji. Kliknij parametr, aby zobaczyć pełne szczegóły.

Parameter	Description
Alias	Ustawia alias dla klucza pozycji.
AllowKey	Zezwala na wykonywanie tych kluczy pozycji, które pasują do wzorca.

Parameter	Description
BufferSend	Nie przechowuje danych w buforze dłużej niż N sekund.
BufferSize	Maksymalna liczba wartości w buforze pamięci.
DebugLevel	Poziom debugowania.
DenyKey	Zabrania wykonywania tych kluczy pozycji, które pasują do wzorca.
EnableRemoteCommands	Określa, czy zdalne polecenia z serwera Zabbix są dozwolone.
HeartbeatFrequency	Częstotliwość komunikatów heartbeat w sekundach.
HostInterface	Opcjonalny parametr definiujący interfejs hosta.
HostInterfaceItem	Opcjonalny parametr definiujący pozycję używaną do pobierania interfejsu hosta.
HostMetadata	Opcjonalny parametr definiujący metadane hosta.
HostMetadataItem	Opcjonalny parametr definiujący pozycję agenta Zabbix używaną do pobierania metadanych hosta.
Hostname	Opcjonalny parametr definiujący nazwę hosta.
HostnameItem	Opcjonalny parametr definiujący pozycję agenta Zabbix używaną do pobierania nazwy hosta.
Include	Możesz dołączyć pojedyncze pliki lub wszystkie pliki z katalogu do pliku konfiguracyjnego.
ListenBacklog	Maksymalna liczba oczekujących połączeń w kolejce TCP.
ListenIP	Lista adresów IP rozdzielonych przecinkami, na których agent powinien nasłuchiwać.
ListenPort	Agent będzie nasłuchiwał na tym porcie połączeń z serwera.
LogFile	Nazwa pliku dziennika.
LogFileSize	Maksymalny rozmiar pliku dziennika.
LogRemoteCommands	Włącza rejestrowanie wykonywanych poleceń powłoki jako ostrzeżeń.
LogType	Typ danych wyjściowych dziennika.
MaxLinesPerSecond	Maksymalna liczba nowych wierszy, które agent wyśle na sekundę do serwera Zabbix lub proxy podczas przetwarzania aktywnych kontroli 'log' i 'logrt'.
PerfCounter	Definiuje nowy parametr <parameter_name>, który jest średnią wartością licznika wydajności systemu <perf_counter_path> dla określonego okresu <period> (w sekundach).
PerfCounterEn	Definiuje nowy parametr <parameter_name>, który jest średnią wartością licznika wydajności systemu <perf_counter_path> dla określonego okresu <period> (w sekundach). W porównaniu do PerfCounter ścieżki perfcounter muszą być w języku angielskim.
RefreshActiveChecks	Jak często odświeżana jest lista aktywnych kontroli.
Server	Lista adresów IP rozdzielonych przecinkami, opcjonalnie w notacji CIDR, lub nazw DNS serwerów Zabbix i proxy Zabbix.
ServerActive	Adres serwera/proxy Zabbix lub konfiguracja klastra, z którego pobierane są aktywne kontrole.
SourceIP	Źródłowy adres IP.
StartAgents	Liczba wstępnie utworzonych instancji zabbix_agentd przetwarzających kontrole pasywne.
Timeout	Określa, jak długo czekać (w sekundach) na ustanowienie połączenia i wymianę danych z proxy lub serwerem Zabbix.
TLSAccept	Jakie połączenia przychodzące akceptować.
TLSCAFile	Pełna ścieżka do pliku zawierającego certyfikaty głównych urzędów certyfikacji (CA) do weryfikacji certyfikatu peera, używana do szyfrowanej komunikacji między komponentami Zabbix.
TLSCertFile	Pełna ścieżka do pliku zawierającego certyfikat agenta lub łańcuch certyfikatów, używana do szyfrowanej komunikacji między komponentami Zabbix.
TLSConnect	Jak agent powinien łączyć się z serwerem Zabbix lub proxy.
TLSCRLFile	Pełna ścieżka do pliku zawierającego unieważnione certyfikaty. Ten parametr jest używany do szyfrowanej komunikacji między komponentami Zabbix.
TLSKeyFile	Pełna ścieżka do pliku zawierającego klucz prywatny agenta, używana do szyfrowanej komunikacji między komponentami Zabbix.
TLSPSKFile	Pełna ścieżka do pliku zawierającego klucz współdzielony agenta, używana do szyfrowanej komunikacji z serwerem Zabbix.
TLSPSKIdentity	Ciąg identyfikujący klucz współdzielony, używany do szyfrowanej komunikacji z serwerem Zabbix.
TLSServerCertIssuer	Dozwolony wystawca certyfikatu serwera (proxy).
TLSServerCertSubject	Dozwolony temat certyfikatu serwera (proxy).
UnsafeUserParameters	Zezwala na przekazywanie wszystkich znaków w argumentach do parametrów zdefiniowanych przez użytkownika.
UserParameter	Parametr zdefiniowany przez użytkownika do monitorowania.
UserParameterDir	Domyślna ścieżka wyszukiwania dla poleceń UserParameter.

Wszystkie parametry są opcjonalne, chyba że wyraźnie zaznaczono, że dany parametr jest obowiązkowy.

Uwaga:

- Wartości domyślne odzwierciedlają wartości domyślne demona, a nie wartości w dostarczonych plikach konfiguracyjnych.

- Wartości obsługują zmienne środowiskowe.
- Zabbix obsługuje pliki konfiguracyjne wyłącznie w kodowaniu UTF-8 bez BOM.
- Komentarze rozpoczynające się od "#" są obsługiwane tylko na początku wiersza.

Szczegóły parametrów

Alias

Ustawia alias dla klucza pozycji. Może być używany do zastąpienia długiego i złożonego klucza pozycji krótszym i prostszym.
 Może występować wiele parametrów *Alias*. Wiele parametrów z tym samym kluczem *Alias* jest niedozwolonych.
 Różne klucze *Alias* mogą wskazywać ten sam klucz pozycji.
 Aliasów można używać w *HostMetadataItem*, ale nie w parametrze *HostnameItem* ani *PerfCounter*.

Przykład 1: Pobieranie użycia pliku stronicowania w procentach z serwera.

```
Alias=pg_usage:perf_counter[\Paging File(_Total)\% Usage]
```

Teraz skrócony klucz **pg_usage** może być używany do pobierania danych.

Przykład 2: Pobieranie obciążenia CPU z parametrami domyślnymi i niestandardowymi.

```
Alias=cpu.load:system.cpu.load
Alias=cpu.load[*]:system.cpu.load[*]
```

Pozwala to używać klucza **cpu.load** do pobierania obciążenia CPU z parametrami domyślnymi, a także **cpu.load[percpu,avg15]** do pobierania szczegółowych danych o obciążeniu CPU.

Przykład 3: Uruchamianie wielu reguł odkrywania niskiego poziomu przetwarzających te same pozycje wykrywania.

```
Alias=vfs.fs.discovery[*]:vfs.fs.discovery
```

Teraz możliwe jest skonfigurowanie kilku reguł wykrywania używających **vfs.fs.discovery** z różnymi parametrami dla każdej reguły, np. **vfs.fs.discovery[foo]**, **vfs.fs.discovery[bar]** itd.

AllowKey

Zezwalaj na wykonywanie tych kluczy pozycji, które pasują do wzorca. Wzorzec klucza jest wyrażeniem wieloznacznym, które obsługuje znak "*" do dopasowania dowolnej liczby dowolnych znaków.
Można zdefiniować wiele reguł dopasowania kluczy w połączeniu z DenyKey. Parametry są przetwarzane jeden po drugim zgodnie z kolejnością ich występowania. Zobacz także: Ograniczanie kontroli agenta.

BufferSend

Nie przechowuj danych w buforze dłużej niż N sekund.

Domyślnie: 5
 Zakres: 1-3600

BufferSize

Maksymalna liczba wartości w buforze pamięci. agent wyśle wszystkie zebrane dane do serwera Zabbix lub proxy, jeśli bufor będzie pełny.

Domyślnie: 100
 Zakres: 2-65535

DebugLevel

Określ poziom debugowania:
0 - podstawowe informacje o uruchamianiu i zatrzymywaniu procesów Zabbix
1 - informacje krytyczne;
2 - informacje o błędach;
3 - ostrzeżenia;
4 - do debugowania (generuje dużo informacji);
5 - rozszerzone debugowanie (generuje jeszcze więcej informacji).

Domyślnie: 3
 Zakres: 0-5

DenyKey

Zabrania wykonywania tych kluczy pozycji, które pasują do wzorca. Wzorzec klucza jest wyrażeniem wieloznacznym obsługującym znak "*" do dopasowania dowolnej liczby dowolnych znaków.
Można zdefiniować wiele reguł dopasowania kluczy w połączeniu z AllowKey. Parametry są przetwarzane jeden po drugim zgodnie z kolejnością ich występowania. Zobacz także: Ograniczanie kontroli agenta.

EnableRemoteCommands

Czy zdalne polecenia z serwera Zabbix są dozwolone. Ten parametr jest **przestarzały**; zamiast niego użyj AllowKey=system.run[*] lub DenyKey=system.run[*].
Jest to wewnętrzny alias parametrów AllowKey/DenyKey, zależnie od wartości:
0 - DenyKey=system.run[*]
1 - AllowKey=system.run[*]

Domyślnie: 0
 Wartości: 0 - nie zezwalaj, 1 - zezwalaj

HeartbeatFrequency

Częstotliwość komunikatów heartbeat w sekundach. Używana do monitorowania dostępności aktywnych testów.
0 - komunikaty heartbeat wyłączone.

Domyślnie: 60
 Zakres: 0-3600

HostInterface

Opcjonalny parametr definiujący interfejs hosta (adres IP lub nazwę DNS) używany podczas procesu autorejestracji. Ta wartość zostanie użyta do wypełnienia interfejsu w nowo utworzonym hoście i umożliwia jawną konfigurację adresu IP lub DNS. Więcej informacji można znaleźć w sekcji Using DNS as default interface.

Jeśli parametr nie jest zdefiniowany, wartość zostanie pobrana z HostInterfaceItem.

agent zgłosi błąd i nie uruchomi się, jeśli wartość przekroczy limit 255 znaków.

Zakres: 0-255 znaków

HostInterfaceItem

Opcjonalny parametr definiujący pozycję używaną do określenia interfejsu hosta (adresu IP lub nazwy DNS) podczas procesu autoregistration. Ta wartość jest używana tylko wtedy, gdy HostInterface nie jest zdefiniowany. Więcej szczegółów można znaleźć w sekcji Using DNS as default interface.

Podczas żądania autorejestracji agent zapisze komunikat ostrzegawczy w logu, jeśli wartość zwrócona przez określoną pozycję przekroczy limit 255 znaków.

Pozycja system.run[] jest obsługiwana niezależnie od ustawień AllowKey/DenyKey.

HostMetadata

Opcjonalny parametr określający metadane używane do identyfikacji lub rozróżniania hosta podczas procesu autorejestracji hosta (aktywny agent). HostMetadata umożliwia rozróżnianie hostów niezależnie od nazwy hosta.

Jeśli nie jest zdefiniowany, wartość zostanie pobrana z HostMetadataItem.

agent zgłosi błąd i nie uruchomi się, jeśli podana wartość przekracza limit 2034 bajtów lub jest ciągiem w formacie innym niż UTF-8. Gdy parametr oczekuje adresu IP lub nazwy DNS, wartości będące poprawnym UTF-8, ale niebędące poprawnymi adresami IP ani nazwami DNS, również zostaną odrzucone i zgłoszone jako nieprawidłowe.

Metadane wielowierszowe nie są obsługiwane — dane wyjściowe zostaną obcięte przy pierwszym znaku końca linii.

Zakres: 0-2034 bajtów

HostMetadataItem

Opcjonalny parametr definiujący pozycję agenta Zabbix używaną do pobierania metadanych hosta. Ta opcja jest używana tylko wtedy, gdy HostMetadata nie jest zdefiniowany.

Wartość HostMetadataItem jest pobierana przy każdej próbie autorejestracji i jest używana wyłącznie w procesie autorejestracji hosta (agent aktywny). HostMetadataItem umożliwia rozróżnianie hostów na podstawie czegoś więcej niż tylko nazwy hosta.

Obsługiwane są parametry użytkownika, liczniki wydajności i aliasy. Pozycja system.run[] jest obsługiwana niezależnie od ustawień AllowKey/DenyKey.

Podczas żądania autorejestracji agent zapisze ostrzeżenie w logu, jeśli wartość zwrócona przez określoną pozycję przekroczy limit 65535 punktów kodowych UTF-8. Wartość zwrócona przez pozycję musi być ciągiem UTF-8, w przeciwnym razie zostanie zignorowana. Gdy parametr oczekuje adresu IP lub nazwy DNS, wartości będące poprawnym UTF-8, ale niebędące poprawnymi adresami IP ani nazwami DNS, również zostaną odrzucone i zgłoszone jako nieprawidłowe.

Metadane wielowierszowe nie są obsługiwane — dane wyjściowe zostaną obcięte przy pierwszym znaku końca linii.

Hostname

Lista unikalnych nazw hostów rozdzielonych przecinkami, z rozróżnianiem wielkości liter. Wymagane dla aktywnych kontroli i musi odpowiadać nazwom hostów skonfigurowanym na serwerze. Wartość jest pobierana z HostnameItem, jeśli nie jest zdefiniowana.
Dozwolone znaki: znaki alfanumeryczne, '.', ' ', '_' oraz '-'. Maksymalna długość: 128 znaków na nazwę hosta, 2048 znaków dla całego wiersza.

Domyślnie: Ustawiane przez HostnameItem

HostnameItem

Opcjonalny parametr, który definiuje pozycję agenta Zabbix używaną do pobierania nazwy hosta. Ta opcja jest używana tylko wtedy, gdy Hostname nie jest zdefiniowany. Parametry użytkownika, liczniki wydajności ani aliasy nie są obsługiwane, ale pozycja system.run[] jest obsługiwana niezależnie od wartości AllowKey/DenyKey.
Zobacz także bardziej szczegółowy opis.

Wartość domyślna: `system.hostname`

Include

Możesz dołączyć pojedyncze pliki lub wszystkie pliki w katalogu w pliku konfiguracyjnym (domyślnie znajdującym się w `C:\Program Files\Zabbix Agent`, jeśli Zabbix agent jest zainstalowany przy użyciu pakietów instalatora Windows MSI; znajdującym się w folderze określonym podczas instalacji, jeśli Zabbix agent jest zainstalowany jako archiwum zip). Wszystkie dołączone pliki muszą mieć poprawną składnię, w przeciwnym razie agent nie uruchomi się.
Aby uwzględnić tylko odpowiednie pliki w określonym katalogu, obsługiwany jest znak wieloznaczny gwiazdki do dopasowywania wzorców.
Zobacz uwagi specjalne dotyczące ograniczeń.

Przykład:

```
Include=C:\Program Files\Zabbix Agent\zabbix_agentd.d\*.conf
```

ListenBacklog

Maksymalna liczba oczekujących połączeń w kolejce TCP.
Wartość domyślna jest stałą zakodowaną na stałe, która zależy od systemu.
Maksymalna obsługiwana wartość również zależy od systemu; zbyt wysokie wartości mogą zostać po cichu obcięte do „maksimum określonego przez implementację”.

Domyślnie: `SOMAXCONN`
 Zakres: 0 - INT_MAX

ListenIP

Lista adresów IP rozdzielonych przecinkami, na których agent powinien nasłuchiwać.

Wartość domyślna: `0.0.0.0`

ListenPort

agent będzie nasłuchiwał na tym porcie połączeń z serwera.

Domyślnie: 10050
 Zakres: 1024-32767

LogFile

Nazwa pliku dziennika agenta.

Domyślnie: `c:\zabbix_agentd.log`
 Wymagane: Tak, jeśli LogType jest ustawione na *file*; w przeciwnym razie nie

LogFileSize

Maksymalny rozmiar pliku dziennika w MB.
0 - wyłącza automatyczną rotację logów.
Uwaga: Jeśli zostanie osiągnięty limit rozmiaru pliku dziennika, a rotacja pliku nie powiedzie się z jakiegokolwiek powodu, istniejący plik dziennika zostanie obcięty i rozpoczęty od nowa.

Domyślnie: 1
 Zakres: 0-1024

LogRemoteCommands

Włącz rejestrowanie wykonywanych poleceń powłoki jako ostrzeżeń. Polecenia będą rejestrowane tylko wtedy, gdy są wykonywane zdalnie. Wpisy dziennika nie będą tworzone, jeśli `system.run[]` jest uruchamiane lokalnie przez parametry HostMetadataItem, HostInterfaceItem lub HostnameItem.

Domyślnie: 0
 Wartości: 0 - wyłączone, 1 - włączone

LogType

Typ wyjścia logu:
file - zapisuj log do pliku określonego parametrem LogFile;
system - zapisuj log do dziennika zdarzeń systemu Windows;
console - zapisuj log na standardowe wyjście.

Domyślnie: `file`

MaxLinesPerSecond

Maksymalna liczba nowych linii, które agent wyśle na sekundę do serwera Zabbix lub proxy podczas przetwarzania aktywnych kontroli ’log’, ’logrt’ i ’eventlog’. Podana wartość zostanie nadpisana przez parametr ’maxlines’ podany w kluczu pozycji ’log’, ’logrt’ lub ’eventlog’.
Uwaga: Zabbix przetworzy 10 razy więcej nowych linii niż ustawiono w *MaxLinesPerSecond*, aby wyszukać wymagany ciąg znaków w pozycjach logów.

Domyślnie: 20
 Zakres: 1-1000

PerfCounter

Definiuje nowy parametr <parameter_name>, który jest średnią wartością licznika wydajności systemu <perf_counter_path> dla określonego okresu <period> (w sekundach).
Składnia: <parameter_name>,”<perf_counter_path>”,<period>

Na przykład, jeśli chcesz otrzymać średnią liczbę przerwań procesora na sekundę z ostatniej minuty, możesz zdefiniować nowy parametr ”interrupts” w następujący sposób:

```
PerfCounter = interrupts,"\Processor(0)\Interrupts/sec",60
```

Zwróć uwagę na podwójne cudzysłowy wokół ścieżki licznika wydajności. Nazwa parametru (interrupts) ma być używana jako klucz pozycji podczas tworzenia pozycji. Próbki do obliczania wartości średniej będą pobierane co sekundę.
Możesz uruchomić ”typeperf -qx”, aby uzyskać listę wszystkich liczników wydajności dostępnych w systemie Windows.

PerfCounterEn

Definiuje nowy parametr <parameter_name>, który jest średnią wartością licznika wydajności systemu <perf_counter_path> dla określonego okresu <period> (w sekundach). W porównaniu do PerfCounter ścieżki liczników wydajności muszą być w języku angielskim. Obsługiwane tylko w **Windows Server 2008/Vista** i nowszych.
Składnia: <parameter_name>,”<perf_counter_path>”,<period>

Na przykład, jeśli chcesz otrzymywać średnią liczbę przerwań procesora na sekundę z ostatniej minuty, możesz zdefiniować nowy parametr „interrupts” w następujący sposób:

```
PerfCounterEn = interrupts,"\Processor(0)\Interrupts/sec",60
```

Zwróć uwagę na podwójne cudzysłowy wokół ścieżki licznika wydajności. Nazwa parametru (interrupts) ma być używana jako klucz pozycji podczas tworzenia pozycji. Próbki do obliczania wartości średniej będą pobierane co sekundę.
Listę angielskich ciągów można znaleźć, przeglądając następujący klucz rejestru: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\009`.

RefreshActiveChecks

Jak często odświeżana jest lista aktywnych kontroli, w sekundach. Należy pamiętać, że po nieudanej próbie odświeżenia aktywnych kontroli kolejna próba zostanie podjęta za 60 sekund.

Domyślnie: 5
 Zakres: 1-86400

Serwer

Lista adresów IP oddzielonych przecinkami, opcjonalnie w notacji CIDR, lub nazw DNS serwerów Zabbix albo proxy Zabbix. Połączenia przychodzące będą akceptowane wyłącznie od hostów wymienionych tutaj. Jeśli obsługa IPv6 jest włączona, wtedy ’127.0.0.1’, ’::127.0.0.1’, ’::ffff:127.0.0.1’ są traktowane jednakowo, a ’::/0’ zezwoli na dowolny adres IPv4 lub IPv6. ’0.0.0.0/0’ może zostać użyte do zezwolenia na dowolny adres IPv4. Należy pamiętać, że „adresy IPv6 zgodne z IPv4” (prefiks 0000::/96) są obsługiwane, ale przestarzałe zgodnie z RFC4291. Spacje są dozwolone.

Przykład:

```
Server=127.0.0.1,192.168.1.0/24,::1,2001:db8::/32,zabbix.example.com
```

Wymagane: tak, jeśli StartAgents nie jest jawnie ustawione na 0

ServerActive

Adres serwera/proxy Zabbix lub konfiguracja klastra, z którego mają być pobierane aktywne testy. Adres serwera/proxy to adres IP lub nazwa DNS oraz opcjonalny port oddzielony dwukropkiem.
Konfiguracja klastra to jeden lub więcej adresów członków grupy serwera lub proxy, oddzielonych średnikiem. Można określić wiele serwerów/klastrów Zabbix oraz proxy Zabbix, oddzielając je przecinkami. Jeśli nie są używane grupy proxy, nie należy określać więcej niż jednego proxy Zabbix z każdego serwera/klastra Zabbix. Jeśli określono proxy Zabbix, to nie należy określać serwera/klastra Zabbix dla tego proxy.
Można podać wiele adresów rozdzielonych przecinkami, aby równolegle używać kilku niezależnych serwerów Zabbix. Spacje są dozwolone.
Jeśli port nie został określony, używany jest port domyślny.
Adresy IPv6 muszą być ujęte w nawiasy kwadratowe, jeśli dla danego hosta określono port. Jeśli port nie został określony, nawiasy kwadratowe dla adresów IPv6 są opcjonalne.
Jeśli ten parametr nie zostanie określony, aktywne testy są wyłączone.

Przykład dla proxy Zabbix:

```
ServerActive=127.0.0.1:10051
```

Przykład dla grupy proxy Zabbix:

```
ServerActive=proxy1.example.com;proxy2.example.com;proxy3.example.com;proxy4.example.com;proxy5.example.co
```

Przykład dla wielu serwerów:

```
ServerActive=127.0.0.1:20051,zabbix.domain,[::1]:30051,::1,[12fc::1]
```

Przykład dla wysokiej dostępności:

```
ServerActive=zabbix.cluster.node1;zabbix.cluster.node2:20051;zabbix.cluster.node3
```

Przykład dla wysokiej dostępności z dwoma klastrami i jednym serwerem:

```
ServerActive=zabbix.cluster.node1;zabbix.cluster.node2:20051,zabbix.cluster2.node1;zabbix.cluster2.node2,z
```

Zakres: (*)

SourceIP

Źródłowy adres IP dla:

- połączeń wychodzących do serwera Zabbix lub proxy Zabbix;
- nawiązywania połączeń podczas wykonywania niektórych pozycji (web.page.get, net.tcp.port itp.).

StartAgents

Liczba wstępnie utworzonych instancji zabbix_agentd, które przetwarzają pasywne testy. Jeśli ustawiono 0, pasywne testy są wyłączone, a agent nie będzie nasłuchiwał na żadnym porcie TCP.

Domyślnie: 10
 Zakres: 0-100 (*)

Timeout

Określa, jak długo czekać (w sekundach) na nawiązanie połączenia i wymianę danych z proxy lub serwerem Zabbix.

Ten parametr określa czas trwania różnych operacji komunikacyjnych, w tym:

- oczekiwanie na odpowiedź od serwera Zabbix;
- wysyłanie żądań do serwera Zabbix, w tym żądań konfiguracji pozycji oraz danych pozycji w active checks;
- pobieranie danych logów za pomocą monitorowania logfile lub dziennika zdarzeń Windows;
- wysyłanie komunikatów heartbeat;
- maksymalny czas trwania kontroli `vfs.*`;
- używany przez moduły agenta Zabbix;
- stosowany jako ustawienie zapasowe w sytuacjach, gdy serwer lub proxy starszy niż wersja 7.0 wysyła kontrole bez limitów czasu.

Ten limit czasu **nie** będzie używany dla tych kontroli agenta, które mają konfigurowalne ustawienia limitu czasu we frontendzie (na poziomie globalnym, proxy lub pojedynczej pozycji).

Domyślnie: 3
 Zakres: 1-30

TLSAccept

Przychodzące połączenia do akceptowania. Używane dla pasywnych testów. Można określić wiele wartości, oddzielonych przecinkami:
unencrypted - akceptuj połączenia bez szyfrowania (domyślnie)
psk - akceptuj połączenia z TLS i kluczem współdzielonym (PSK)
cert - akceptuj połączenia z TLS i certyfikatem

Wymagane: tak, jeśli zdefiniowano parametry certyfikatu TLS lub PSK (nawet dla połączenia *unencrypted*); w przeciwnym razie nie

TLSCAFile

Pełna ścieżka do pliku zawierającego certyfikaty nadrzędnych urzędów certyfikacji (CA) do weryfikacji certyfikatu peera, używana do szyfrowanej komunikacji między komponentami Zabbix.

TLSCertFile

Pełna ścieżka do pliku zawierającego certyfikat agenta lub łańcuch certyfikatów, używanego do szyfrowanej komunikacji z komponentami Zabbix.

TLSConnect

Jak agent powinien łączyć się z serwerem Zabbix lub proxy. Używane dla aktywnych testów. Można określić tylko jedną wartość:
unencrypted - połączenie bez szyfrowania (domyślnie)
psk - połączenie z użyciem TLS i klucza współdzielonego (PSK)
cert - połączenie z użyciem TLS i certyfikatu

Wymagane: tak, jeśli zdefiniowano parametry certyfikatu TLS lub PSK (nawet dla połączenia *unencrypted*); w przeciwnym razie nie

TLSCRLFile

Pełna ścieżka do pliku zawierającego unieważnione certyfikaty. Ten parametr jest używany do szyfrowanej komunikacji między komponentami Zabbix.

TLSKeyFile

Pełna ścieżka do pliku zawierającego klucz prywatny agenta, używanego do szyfrowanej komunikacji między komponentami Zabbix.

TLSPSKFile

Pełna ścieżka do pliku zawierającego klucz współdzielony agenta, używany do szyfrowanej komunikacji z serwerem Zabbix.

TLSPSKIdentity

Ciąg tożsamości klucza współdzielonego, używany do szyfrowanej komunikacji z serwerem Zabbix.

TLSServerCertIssuer

Dozwolony wystawca certyfikatu serwera (proxy).

TLSServerCertSubject

Dozwolony temat certyfikatu serwera (proxy).

UnsafeUserParameters

Zezwala na przekazywanie wszystkich znaków w argumentach do parametrów zdefiniowanych przez użytkownika. Następujące znaki są niedozwolone: \ ' " ` * ? [ ] { } ~ $! & ; ( ) < > | # @ %
Dodatkowo znaki nowej linii są niedozwolone.

Wartość domyślna: 0
 Wartości: 0 - nie zezwalaj, 1 - zezwalaj

UserParameter

Parametr zdefiniowany przez użytkownika do monitorowania. Może istnieć kilka parametrów zdefiniowanych przez użytkownika.
Format: UserParameter=<key>,<shell command>
Należy pamiętać, że polecenie powłoki nie może zwracać pustego ciągu ani wyłącznie znaku końca linii. Polecenia powłoki mogą mieć ścieżki względne, jeśli określono parametr UserParameterDir.

Przykład:

```
UserParameter=system.test,dir /b | find /c /v ""
UserParameter=check_cpu,.\custom\_script.bat
```

UserParameterDir

Domyślna ścieżka wyszukiwania dla poleceń UserParameter. Jeśli jest używana, agent zmieni swój katalog roboczy na określony tutaj przed wykonaniem polecenia. Dzięki temu polecenia UserParameter mogą mieć względny prefiks `./` zamiast pełnej ścieżki. Dozwolony jest tylko jeden wpis.

Przykład:

```
UserParameterDir=C:\opt\myscripts
```

Note:
(*) Liczba aktywnych serwerów wymienionych w ServerActive oraz liczba wstępnie utworzonych instancji dla pasywnych kontroli określona w StartAgents musi być mniejsza niż 64.

6 Zabbix agent 2 (Windows)

Przegląd

Zabbix agent 2 to nowa generacja agenta Zabbix i może być używany zamiast Zabbix agent.

Parametry obsługiwane przez plik konfiguracyjny Windows Zabbix agent 2 (zabbix_agent2.conf) są wymienione w tej sekcji.

Parametry są podane bez dodatkowych informacji. Kliknij parametr, aby zobaczyć pełne szczegóły.

Parameter	Description
Alias	Ustawia alias dla klucza pozycji.
AllowKey	Zezwala na wykonywanie tych kluczy pozycji, które pasują do wzorca.
BufferSend	Nie przechowuje danych w buforze dłużej niż N sekund.
BufferSize	Maksymalna liczba wartości w buforze pamięci.
ControlSocket	Gniazdo sterujące używane do wysyłania poleceń w czasie działania za pomocą opcji '-R'.
DebugLevel	Poziom debugowania.
DenyKey	Zabrania wykonywania tych kluczy pozycji, które pasują do wzorca.
EnablePersistentBuffer	Włącza użycie lokalnej trwałej pamięci masowej dla aktywnych pozycji.
ForceActiveChecksOnStart	Wykonuje aktywne testy natychmiast po restarcie dla pierwszej otrzymanej konfiguracji.
HeartbeatFrequency	Częstotliwość komunikatów heartbeat w sekundach.
HostInterface	Opcjonalny parametr definiujący interfejs hosta.
HostInterfaceItem	Opcjonalny parametr definiujący pozycję używaną do pobierania interfejsu hosta.
HostMetadata	Opcjonalny parametr definiujący metadane hosta.

Parameter	Description
HostMetadataItem	Opcjonalny parametr definiujący pozycję agenta Zabbix używaną do pobierania metadanych hosta.
Hostname	Opcjonalny parametr definiujący nazwę hosta.
HostnameItem	Opcjonalny parametr definiujący pozycję agenta Zabbix używaną do pobierania nazwy hosta.
Include	Możesz dołączyć pojedyncze pliki lub wszystkie pliki z katalogu do pliku konfiguracyjnego.
ListenIP	Lista adresów IP rozdzielonych przecinkami, na których agent powinien nasłuchiwać.
ListenPort	agent będzie nasłuchiwał na tym porcie połączeń z serwera.
LogFile	Nazwa pliku dziennika.
LogFileSize	Maksymalny rozmiar pliku dziennika.
LogType	Typ wyjścia dziennika.
PersistentBufferFile	Plik, w którym Zabbix agent 2 powinien przechowywać bazę danych SQLite.
PersistentBufferPeriod	Okres, przez który dane powinny być przechowywane, gdy nie ma połączenia z serwerem lub proxy.
Plugins.<PluginName>.System.Capacity	Limit testów na plugin, które mogą być wykonywane jednocześnie.
Plugins.Log.MaxLinesPerSecond	Maksymalna liczba nowych wierszy, które agent wyśle na sekundę do serwera Zabbix lub proxy podczas przetwarzania aktywnych testów 'log' i 'logrt'.
Plugins.SystemRun.LogRemoteCommands	Włącza rejestrowanie wykonywanych poleceń powłoki jako ostrzeżeń.
PluginSocket	Ścieżka do gniazda UNIX dla komunikacji z ładowalnymi pluginami.
PluginTimeout	Limit czasu połączeń z ładowalnymi pluginami, w sekundach.
PerfCounter	Definiuje nowy parametr <parameter_name>, który jest wartością średnią licznika wydajności systemu <perf_counter_path> dla określonego okresu <period> (w sekundach).
PerfCounterEn	Definiuje nowy parametr <parameter_name>, który jest wartością średnią licznika wydajności systemu <perf_counter_path> dla określonego okresu <period> (w sekundach). W porównaniu do PerfCounter ścieżki perfcounter muszą być w języku angielskim.
RefreshActiveChecks	Jak często odświeżana jest lista aktywnych testów.
Server	Lista adresów IP rozdzielonych przecinkami, opcjonalnie w notacji CIDR, lub nazw DNS serwerów Zabbix i proxy Zabbix.
ServerActive	Adres serwera/proxy Zabbix lub konfiguracja klastra, z którego pobierane są aktywne testy.
SourceIP	Źródłowy adres IP.
StatusPort	Jeśli ustawiony, agent będzie nasłuchiwał na tym porcie żądań statusu HTTP (http://localhost:<port>/status).
Timeout	Określa, jak długo czekać (w sekundach) na ustanowienie połączenia i wymianę danych z proxy lub serwerem Zabbix.
TLSAccept	Jakie połączenia przychodzące akceptować.
TLSCAFile	Pełna ścieżka do pliku zawierającego certyfikaty głównych urzędów certyfikacji (CA) do weryfikacji certyfikatu peera, używana do szyfrowanej komunikacji między komponentami Zabbix.
TLSCertFile	Pełna ścieżka do pliku zawierającego certyfikat agenta lub łańcuch certyfikatów, używana do szyfrowanej komunikacji między komponentami Zabbix.
TLSCipherAll13	Ciąg szyfrów OpenSSL (TLS 1.3). Zastępuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na certyfikatach i PSK.
TLSCipherCert13	Ciąg szyfrów OpenSSL (TLS 1.3). Zastępuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na certyfikatach.
TLSCipherPSK13	Ciąg szyfrów OpenSSL (TLS 1.3). Zastępuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na PSK.
TLSConnect	Jak agent powinien łączyć się z serwerem Zabbix lub proxy.
TLSCRLFile	Pełna ścieżka do pliku zawierającego unieważnione certyfikaty. Ten parametr jest używany do szyfrowanej komunikacji między komponentami Zabbix.
TLSKeyFile	Pełna ścieżka do pliku zawierającego klucz prywatny agenta, używana do szyfrowanej komunikacji między komponentami Zabbix.
TLSPSKFile	Pełna ścieżka do pliku zawierającego wstępnie współdzielony klucz agenta, używana do szyfrowanej komunikacji z serwerem Zabbix.
TLSPSKIdentity	Ciąg identyfikatora wstępnie współdzielonego klucza, używany do szyfrowanej komunikacji z serwerem Zabbix.
TLSServerCertIssuer	Dozwolony wystawca certyfikatu serwera (proxy).
TLSServerCertSubject	Dozwolony podmiot certyfikatu serwera (proxy).
UnsafeUserParameters	Zezwala na przekazywanie wszystkich znaków w argumentach do parametrów zdefiniowanych przez użytkownika.
UserParameter	Parametr zdefiniowany przez użytkownika do monitorowania.
UserParameterDir	Domyślna ścieżka wyszukiwania dla poleceń UserParameter.

Wszystkie parametry są opcjonalne, chyba że wyraźnie podano, że parametr jest obowiązkowy.

Należy pamiętać, że:

- Wartości domyślne odzwierciedlają wartości domyślne procesu, a nie wartości w dostarczonych plikach konfiguracyjnych;
- Wartości obsługują zmienne środowiskowe;
- Zabbix obsługuje pliki konfiguracyjne tylko w kodowaniu UTF-8 bez BOM;
- Komentarze rozpoczynające się od ”#” są obsługiwane tylko na początku wiersza.

Szczegóły parametrów

Alias

Ustawia alias dla klucza pozycji. Może być używany do zastąpienia długiego i złożonego klucza pozycji krótszym i prostszym.
 Może występować wiele parametrów *Alias*. Wiele parametrów z tym samym kluczem *Alias* jest niedozwolonych.
 Różne klucze *Alias* mogą wskazywać ten sam klucz pozycji.
 Aliasy mogą być używane w *HostMetadataItem*, ale nie w parametrze *HostnameItem*.

Przykład 1: Pobieranie użycia pliku stronicowania w procentach z serwera.

```
Alias=pg_usage:perf_counter[\Paging File(_Total)\% Usage]
```

Teraz skrócony klucz **pg_usage** może być używany do pobierania danych.

Przykład 2: Pobieranie obciążenia CPU z parametrami domyślnymi i niestandardowymi.

```
Alias=cpu.load:system.cpu.load
Alias=cpu.load[*]:system.cpu.load[*]
```

Pozwala to używać klucza **cpu.load** do pobierania obciążenia CPU z parametrami domyślnymi, a także klucza **cpu.load[percpu,avg15]** do pobierania szczegółowych danych o obciążeniu CPU.

Przykład 3: Uruchamianie wielu reguł low-level discovery przetwarzających te same pozycje wykrywania.

```
Alias=vfs.fs.discovery[*]:vfs.fs.discovery
```

Teraz możliwe jest skonfigurowanie kilku reguł wykrywania używających **vfs.fs.discovery** z różnymi parametrami dla każdej reguły, np. **vfs.fs.discovery[foo]**, **vfs.fs.discovery[bar]** itd.

AllowKey

Zezwalaj na wykonywanie tych kluczy pozycji, które pasują do wzorca. Wzorzec klucza jest wyrażeniem wieloznacznym obsługującym znak ”*” do dopasowania dowolnej liczby dowolnych znaków.
Można zdefiniować wiele reguł dopasowania kluczy w połączeniu z DenyKey. Parametry są przetwarzane jeden po drugim zgodnie z kolejnością ich występowania. Zobacz także: Ograniczanie kontroli agenta.

BufferSend

The time interval in seconds which determines how often values are sent from the buffer to Zabbix server.
Note, that if the buffer is full, the data will be sent sooner.

Default: 5
 Range: 1-3600

BufferSize

Maksymalna liczba wartości w buforze pamięci. agent wyśle wszystkie zebrane dane do serwera Zabbix lub proxy, jeśli bufor będzie pełny.
Tego parametru należy używać tylko wtedy, gdy trwały bufor jest wyłączony (*EnablePersistentBuffer=0*).

Domyślnie: 1000
 Zakres: 2-65535

ControlSocket

Gniazdo sterujące, używane do wysyłania poleceń w czasie działania za pomocą opcji ’-R’.

Domyślnie: `\\.\pipe\agent.sock`

DebugLevel

Określ poziom debugowania:
0 - podstawowe informacje o uruchamianiu i zatrzymywaniu procesów Zabbix
1 - informacje krytyczne;
2 - informacje o błędach;
3 - ostrzeżenia;
4 - do debugowania (generuje dużo informacji);
5 - rozszerzone debugowanie (generuje jeszcze więcej informacji).

Domyślnie: 3
 Zakres: 0-5

DenyKey

Zabrania wykonywania tych kluczy pozycji, które pasują do wzorca. Wzorzec klucza jest wyrażeniem wieloznacznym obsługującym znak "*", który dopasowuje dowolną liczbę dowolnych znaków.
Można zdefiniować wiele reguł dopasowania kluczy w połączeniu z AllowKey. Parametry są przetwarzane jeden po drugim zgodnie z kolejnością ich występowania. Zobacz także: Ograniczanie kontroli agenta.

EnablePersistentBuffer

Włącz użycie lokalnej trwałej pamięci masowej dla aktywnych pozycji. Jeśli trwała pamięć masowa jest wyłączona, użyty zostanie bufor pamięci.

Domyślnie: 0
 Wartości: 0 - wyłączone, 1 - włączone

ForceActiveChecksOnStart

Wykonuj aktywne kontrole natychmiast po restarcie dla pierwszej otrzymanej konfiguracji. Dostępne również jako parametr konfiguracji dla poszczególnych wtyczek, na przykład: `Plugins.Uptime.System.ForceActiveChecksOnStart=1`

Wartość domyślna: 0
 Wartości: 0 - wyłączone, 1 - włączone

HeartbeatFrequency

Częstotliwość komunikatów heartbeat w sekundach. Używana do monitorowania dostępności aktywnych testów.
0 - komunikaty heartbeat wyłączone.

Domyślnie: 60
 Zakres: 0-3600

HostInterface

Opcjonalny parametr definiujący interfejs hosta (adres IP lub nazwę DNS) używany podczas procesu autoregistration. Ta wartość zostanie użyta do wypełnienia interfejsu w nowo utworzonym hoście i umożliwia jawną konfigurację adresu IP lub DNS. Więcej informacji można znaleźć w sekcji Using DNS as default interface.

Jeśli nie jest zdefiniowany, wartość zostanie pobrana z HostInterfaceItem.

agent zgłosi błąd i nie uruchomi się, jeśli wartość przekroczy limit 255 znaków.

Zakres: 0-255 znaków

HostInterfaceItem

Opcjonalny parametr definiujący pozycję używaną do określenia interfejsu hosta (adresu IP lub nazwy DNS) podczas procesu autorejestracji. Ta wartość jest używana tylko wtedy, gdy HostInterface nie jest zdefiniowany. Więcej informacji można znaleźć w sekcji Używanie DNS jako domyślnego interfejsu.

Podczas żądania autorejestracji agent zapisze komunikat ostrzegawczy w logu, jeśli wartość zwrócona przez określoną pozycję przekroczy limit 255 znaków.

Pozycja system.run[] jest obsługiwana niezależnie od ustawień AllowKey/DenyKey.

HostMetadata

Opcjonalny parametr określający metadane używane do identyfikacji lub rozróżniania hosta podczas procesu autorejestracji hosta (aktywny agent). HostMetadata umożliwia rozróżnianie hostów nie tylko na podstawie nazwy hosta.

Jeśli nie jest zdefiniowany, wartość zostanie pobrana z HostMetadataItem.

agent zgłosi błąd i nie uruchomi się, jeśli podana wartość przekracza limit 2034 bajtów lub jest ciągiem znaków innym niż UTF-8. Gdy parametr oczekuje adresu IP lub nazwy DNS, wartości będące poprawnym UTF-8, ale niebędące poprawnymi adresami IP ani nazwami DNS, również zostaną odrzucone i zgłoszone jako nieprawidłowe.

Metadane wielowierszowe nie są obsługiwane — dane wyjściowe zostaną obcięte przy pierwszym znaku końca linii.

Zakres: 0-2034 bajtów

HostMetadataItem

Opcjonalny parametr definiujący pozycję agenta Zabbix używaną do pobierania metadanych hosta. Ta opcja jest używana tylko wtedy, gdy HostMetadata nie jest zdefiniowany.

Wartość HostMetadataItem jest pobierana przy każdej próbie autorejestracji i jest używana wyłącznie w procesie autorejestracji hosta (agent aktywny). HostMetadataItem umożliwia rozróżnianie hostów poza nazwą hosta.

Parametry użytkownika i aliasy są obsługiwane. Pozycja system.run[] jest obsługiwana niezależnie od ustawień AllowKey/DenyKey.

Podczas żądania autorejestracji agent zapisze komunikat ostrzegawczy w logu, jeśli wartość zwrócona przez określoną pozycję przekracza limit 65535 punktów kodowych UTF-8. Wartość zwrócona przez pozycję musi być ciągiem UTF-8, w przeciwnym razie zostanie zignorowana. Gdy parametr oczekuje adresu IP lub nazwy DNS, wartości będące poprawnym UTF-8, ale niebędące poprawnymi adresami IP ani nazwami DNS, również zostaną odrzucone i zgłoszone jako nieprawidłowe.

Metadane wielowierszowe nie są obsługiwane — dane wyjściowe zostaną obcięte przy pierwszym znaku końca wiersza.

Hostname

Lista unikalnych nazw hostów rozdzielonych przecinkami, z rozróżnianiem wielkości liter. Wymagane dla aktywnych kontroli i musi odpowiadać nazwom hostów skonfigurowanym na serwerze. Wartość jest pobierana z HostnameItem, jeśli nie jest zdefiniowana.
Dozwolone znaki: alfanumeryczne, '.', ' ', '_' i '-'. Maksymalna długość: 128 znaków na nazwę hosta, 2048 znaków dla całego wiersza.

Domyślnie: Ustawiane przez HostnameItem

HostnameItem

Opcjonalny parametr definiujący pozycję używaną do pobierania nazwy hosta. Ta opcja jest używana tylko wtedy, gdy parametr Hostname nie jest zdefiniowany. Parametry użytkownika ani aliasy nie są obsługiwane, ale pozycja system.run[] jest obsługiwana niezależnie od wartości AllowKey/DenyKey.

Wartość domyślna: `system.hostname`

Include

Możesz dołączyć pojedyncze pliki lub wszystkie pliki w katalogu w pliku konfiguracyjnym (domyślnie znajdującym się w `C:\Program Files\Zabbix Agent 2`, jeśli Zabbix agent jest zainstalowany przy użyciu pakietów instalatora Windows MSI; znajdującym się w folderze określonym podczas instalacji, jeśli Zabbix agent jest zainstalowany jako archiwum zip). Wszystkie dołączane pliki muszą mieć poprawną składnię, w przeciwnym razie agent nie uruchomi się. Ścieżka może być względna względem lokalizacji pliku *zabbix_agent2.conf* (np. `Include=.\zabbix_agent2.d\plugins.d\*.conf`).
Aby dołączyć tylko odpowiednie pliki w określonym katalogu, obsługiwany jest znak wieloznaczny gwiazdki do dopasowywania wzorców.
Zobacz uwagi specjalne dotyczące ograniczeń.

Przykład:

```
Include=C:\Program Files\Zabbix Agent2\zabbix_agent2.d\*.conf
```

ListenIP

Lista adresów IP rozdzielonych przecinkami, na których agent powinien nasłuchiwać. Pierwszy adres IP jest wysyłany do serwera Zabbix, jeśli nawiązuje z nim połączenie, w celu pobrania listy aktywnych kontroli.

Wartość domyślna: `0.0.0.0`

ListenPort

agent będzie nasłuchiwał na tym porcie połączeń z serwera.

Domyślnie: 10050
 Zakres: 1024-32767

LogFile

Nazwa pliku dziennika agenta.

Domyślnie: `c:\zabbix_agent2.log`
 Wymagane: Tak, jeśli LogType jest ustawione na *file*; w przeciwnym razie nie

LogFileSize

Maksymalny rozmiar pliku dziennika w MB.
0 - wyłącza automatyczną rotację logów.
Uwaga: Jeśli zostanie osiągnięty limit rozmiaru pliku dziennika, a rotacja pliku nie powiedzie się z jakiegokolwiek powodu, istniejący plik dziennika zostanie obcięty i rozpoczęty na nowo.

Wartość domyślna: 1
 Zakres: 0-1024

LogType

Typ wyjścia logu:
file - zapisuj log do pliku określonego parametrem LogFile;
console - zapisuj log na standardowe wyjście.

Wartość domyślna: `file`

PersistentBufferFile

Plik, w którym agent Zabbix 2 powinien przechowywać bazę danych SQLite. Musi to być pełna nazwa pliku. Ten parametr jest używany tylko wtedy, gdy trwały bufor jest włączony (*EnablePersistentBuffer=1*).

PersistentBufferPeriod

Okres, przez jaki dane powinny być przechowywane, gdy nie ma połączenia z serwerem lub proxy. Starsze dane zostaną utracone. Dane dziennika zostaną zachowane. Ten parametr jest używany tylko wtedy, gdy trwały bufor jest włączony (*EnablePersistentBuffer=1*).

Wartość domyślna: 1h
 Zakres: 1m-365d

Plugins.<PluginName>.System.Capacity

Limit sprawdzeń na plugin <PluginName>, które mogą być wykonywane jednocześnie.

Domyślnie: 1000 Zakres: 1-1000

Plugins.Log.MaxLinesPerSecond

Maksymalna liczba nowych wierszy na sekundę, które agent wyśle do serwera lub proxy Zabbix podczas przetwarzania aktywnych kontroli „log", „logrt" i „eventlog". Podana wartość zostanie nadpisana przez parametr „maxlines" podany w kluczu pozycji „log", „logrt" lub „eventlog".
Uwaga: Zabbix przetworzy 10 razy więcej nowych wierszy niż ustawiono w *MaxLinesPerSecond*, aby wyszukać wymagany ciąg znaków w pozycjach logów.

Domyślnie: 20
 Zakres: 1-1000

Plugins.SystemRun.LogRemoteCommands

Włącz rejestrowanie wykonywanych poleceń powłoki jako ostrzeżeń. Polecenia będą rejestrowane tylko wtedy, gdy są wykonywane zdalnie. Wpisy dziennika nie będą tworzone, jeśli system.run[] jest uruchamiane lokalnie przez parametry HostMetadataItem, HostInterfaceItem lub HostnameItem.

Domyślnie: 0
 Wartości: 0 - wyłączone, 1 - włączone

PluginSocket

Ścieżka do gniazda UNIX używanego do komunikacji z ładowalnymi wtyczkami.

Domyślnie: \\.\pipe\agent.plugin.sock

PluginTimeout

Limit czasu połączeń z ładowalnymi wtyczkami, w sekundach.

Wartość domyślna: Timeout
 Zakres: 1-30

PerfCounter

Definiuje nowy parametr <parameter_name>, który jest średnią wartością licznika wydajności systemu <perf_counter_path> dla określonego okresu <period> (w sekundach).
Składnia: <parameter_name>,"<perf_counter_path>",<period>

Na przykład, jeśli chcesz otrzymać średnią liczbę przerwań procesora na sekundę z ostatniej minuty, możesz zdefiniować nowy parametr "interrupts" w następujący sposób:

```
PerfCounter = interrupts,"\Processor(0)\Interrupts/sec",60
```

Zwróć uwagę na podwójne cudzysłowy wokół ścieżki licznika wydajności. Nazwa parametru (interrupts) ma być używana jako klucz pozycji podczas tworzenia pozycji. Próbki do obliczania wartości średniej będą pobierane co sekundę.
Możesz uruchomić "typeperf -qx", aby uzyskać listę wszystkich liczników wydajności dostępnych w systemie Windows.

PerfCounterEn

Definiuje nowy parametr <parameter_name>, który jest średnią wartością licznika wydajności systemu <perf_counter_path> dla określonego przedziału czasu <period> (w sekundach). W porównaniu z PerfCounter ścieżki perfcounter muszą być w języku angielskim. Obsługiwane tylko w systemach **Windows Server 2008/Vista** i nowszych.
Składnia: <parameter_name>,"<perf_counter_path>",<period>

Na przykład, jeśli chcesz otrzymywać średnią liczbę przerwań procesora na sekundę z ostatniej minuty, możesz zdefiniować nowy parametr „interrupts" w następujący sposób:

```
PerfCounterEn = interrupts,"\Processor(0)\Interrupts/sec",60
```

Zwróć uwagę na podwójne cudzysłowy wokół ścieżki licznika wydajności. Nazwa parametru (interrupts) ma być używana jako klucz pozycji podczas tworzenia pozycji. Próbki do obliczania wartości średniej będą pobierane co sekundę.
Listę angielskich ciągów można znaleźć, przeglądając następujący klucz rejestru: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\009.

RefreshActiveChecks

Jak często odświeżana jest lista aktywnych testów, w sekundach. Należy pamiętać, że po nieudanej próbie odświeżenia aktywnych testów kolejna próba odświeżenia zostanie podjęta za 60 sekund.

Domyślnie: 5
 Zakres: 1-86400

Serwer

Lista adresów IP oddzielonych przecinkami, opcjonalnie w notacji CIDR, lub nazw DNS serwerów Zabbix albo proxy Zabbix. Połączenia przychodzące będą akceptowane tylko od hostów wymienionych tutaj. Jeśli obsługa IPv6 jest włączona, wtedy '127.0.0.1', '::127.0.0.1', '::ffff:127.0.0.1' są traktowane jednakowo, a '::/0' zezwoli na dowolny adres IPv4 lub IPv6. '0.0.0.0/0' może zostać użyte do zezwolenia na dowolny adres IPv4. Spacje są dozwolone. Jeśli ten parametr nie jest określony, wyłącza sprawdzenia pasywne, a agent nie będzie nasłuchiwał na żadnym porcie TCP.

Przykład:

```
Server=127.0.0.1,192.168.1.0/24,::1,2001:db8::/32,zabbix.example.com
```

ServerActive

Adres serwera/proxy Zabbix lub konfiguracja klastra, z którego mają być pobierane aktywne testy. Adres serwera/proxy to adres IP lub nazwa DNS oraz opcjonalny port oddzielony dwukropkiem.
Konfiguracja klastra to jeden lub więcej adresów członków grupy serwera lub proxy oddzielonych średnikiem. Można podać wiele serwerów/klastrów Zabbix oraz proxy Zabbix, oddzielając je przecinkami. Jeśli nie są używane grupy proxy, nie należy podawać więcej niż jednego proxy Zabbix z każdego serwera/klastra Zabbix. Jeśli podano proxy Zabbix, nie należy podawać serwera/klastra Zabbix dla tego proxy.
Można podać wiele adresów rozdzielonych przecinkami, aby równolegle używać kilku niezależnych serwerów Zabbix. Spacje są dozwolone.
Jeśli port nie został określony, używany jest port domyślny.
Adresy IPv6 muszą być ujęte w nawiasy kwadratowe, jeśli dla tego hosta określono port. Jeśli port nie został określony, nawiasy kwadratowe dla adresów IPv6 są opcjonalne.
Jeśli ten parametr nie zostanie określony, aktywne testy są wyłączone.

Przykład dla proxy Zabbix:

```
ServerActive=127.0.0.1:10051
```

Przykład dla grupy proxy Zabbix:

```
ServerActive=proxy1.example.com;proxy2.example.com;proxy3.example.com;proxy4.example.com;proxy5.example.co
```

Przykład dla wielu serwerów:

```
ServerActive=127.0.0.1:20051,zabbix.domain,\[::1\]:30051,::1,\[12fc::1\]
```

Przykład dla wysokiej dostępności:

```
ServerActive=zabbix.cluster.node1;zabbix.cluster.node2:20051;zabbix.cluster.node3
```

Przykład wysokiej dostępności z dwoma klastrami i jednym serwerem:

```
ServerActive=zabbix.cluster.node1;zabbix.cluster.node2:20051,zabbix.cluster2.node1;zabbix.cluster2.node2,z
```

SourceIP

Źródłowy adres IP dla:

- połączeń wychodzących do serwera Zabbix lub proxy Zabbix;
- nawiązywania połączeń podczas wykonywania niektórych pozycji (web.page.get, net.tcp.port itp.).

StatusPort

Jeśli ustawione, agent będzie nasłuchiwał na tym porcie żądań statusu HTTP (http://localhost:<port>/status).

Zakres: 1024-32767

Timeout

Określa, jak długo czekać (w sekundach) na ustanowienie połączenia i wymianę danych z proxy lub serwerem Zabbix.

Ten parametr określa czas trwania różnych operacji komunikacyjnych, w tym:

- oczekiwania na odpowiedź od serwera Zabbix;
- wysyłania żądań do serwera Zabbix, w tym żądań konfiguracji pozycji oraz danych pozycji w active checks;
- pobierania danych logów za pomocą monitorowania logfile lub dziennika zdarzeń Windows;
- wysyłania komunikatów heartbeat;
- maksymalnego czasu trwania kontroli `vfs.*`;
- użycia jako wartości zapasowej w sytuacjach, gdy serwer lub proxy starszy niż wersja 7.0 wysyła kontrole bez limitów czasu.

Ten limit czasu **nie** będzie używany dla tych kontroli agenta, które mają konfigurowalne ustawienia limitu czasu we frontendzie (na poziomie globalnym, proxy lub pojedynczej pozycji).

Domyślnie: 3
 Zakres: 1-30

TLSAccept

Przychodzące połączenia do akceptowania. Używane dla pasywnych kontroli. Można określić wiele wartości, oddzielonych przecinkami:
unencrypted - akceptuj połączenia bez szyfrowania (domyślnie)
psk - akceptuj połączenia z TLS i kluczem współdzielonym (PSK)
cert - akceptuj połączenia z TLS i certyfikatem

Wymagane: tak, jeśli zdefiniowano parametry certyfikatu TLS lub PSK (nawet dla połączenia *unencrypted*); w przeciwnym razie nie

TLSCAFile

Pełna ścieżka do pliku zawierającego certyfikaty głównego urzędu lub urzędów certyfikacji (CA) do weryfikacji certyfikatu peera, używana do szyfrowanej komunikacji między komponentami Zabbix.

TLSCertFile

Pełna ścieżka do pliku zawierającego certyfikat agenta lub łańcuch certyfikatów, używanego do szyfrowanej komunikacji z komponentami Zabbix.

TLSCipherAll13

Ciąg szyfrów OpenSSL (TLS 1.3).
Zastępuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na certyfikatach i PSK.

Przykład:

```
TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256
```

TLSCipherCert13

Ciąg szyfrów OpenSSL (TLS 1.3). Zastępuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na certyfikatach.

Należy pamiętać, że tego parametru nie można używać razem z `TLSAccept=cert,psk`; w przypadku połączenia certyfikatowego (`TLSConnect=cert`) należy zamiast tego użyć TLSCipherAll13.

TLSCipherPSK13

Ciąg szyfrów OpenSSL (TLS 1.3). Zastępuje domyślne kryteria wyboru zestawu szyfrów dla szyfrowania opartego na PSK.

Przykład:

```
TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256
```

TLSConnect

Jak agent powinien łączyć się z serwerem lub proxy Zabbix. Używane dla aktywnych testów. Można określić tylko jedną wartość:
unencrypted - połączenie bez szyfrowania (domyślnie)
psk - połączenie z użyciem TLS i klucza współdzielonego (PSK)
cert - połączenie z użyciem TLS i certyfikatu

Wymagane: tak, jeśli zdefiniowano parametry certyfikatu TLS lub PSK (nawet dla połączenia *unencrypted*); w przeciwnym razie nie

TLSCRLFile

Pełna ścieżka do pliku zawierającego unieważnione certyfikaty. Ten parametr jest używany do szyfrowanej komunikacji między komponentami Zabbix.

TLSKeyFile

Pełna ścieżka do pliku zawierającego klucz prywatny agenta, używanego do szyfrowanej komunikacji między komponentami Zabbix.

TLSPSKFile

Pełna ścieżka do pliku zawierającego klucz współdzielony agenta, używany do szyfrowanej komunikacji z serwerem Zabbix.

TLSPSKIdentity

Ciąg tożsamości klucza współdzielonego, używany do szyfrowanej komunikacji z serwerem Zabbix.

TLSServerCertIssuer

Dozwolony wystawca certyfikatu serwera (proxy).

TLSServerCertSubject

Dozwolony temat certyfikatu serwera (proxy).

UnsafeUserParameters

Zezwala na przekazywanie wszystkich znaków w argumentach do parametrów zdefiniowanych przez użytkownika. Następujące znaki nie są dozwolone: \ ' " ` * ? [ ] { } ~ $! & ; ( ) < > | # @ %
Dodatkowo znaki nowej linii nie są dozwolone.

Wartość domyślna: 0
 Wartości: 0 - nie zezwalaj, 1 - zezwalaj

UserParameter

Parametr zdefiniowany przez użytkownika do monitorowania. Może istnieć kilka parametrów zdefiniowanych przez użytkownika.
Format: UserParameter=<key>,<shell command>
Należy pamiętać, że polecenie powłoki nie może zwracać pustego ciągu ani wyłącznie znaku końca linii. Polecenia powłoki mogą zawierać ścieżki względne, jeśli określono parametr UserParameterDir.

Przykład:

```
UserParameter=system.test,dir /b | find /c /v ""
UserParameter=check_cpu,.\custom\_script.bat
```

UserParameterDir

Domyślna ścieżka wyszukiwania dla poleceń UserParameter. Jeśli jest używana, agent zmieni swój katalog roboczy na określony tutaj przed wykonaniem polecenia. Dzięki temu polecenia UserParameter mogą mieć względny prefiks `.\` zamiast pełnej ścieżki.
Dozwolony jest tylko jeden wpis.

Przykład:

```
UserParameterDir=C:\opt\myscripts
```

7 Configuration parameters of plugins

See configuration parameters for Zabbix agent 2 plugins:

- Ceph plugin
- Docker plugin
- Ember+ plugin
- Memcached plugin
- Modbus plugin
- MongoDB plugin
- MQTT plugin
- MSSQL plugin
- MySQL plugin
- NVIDIA GPU plugin
- Oracle plugin
- PostgreSQL plugin
- Redis plugin
- S.M.A.R.T. plugin

Plugin configuration principles

This page describes plugin configuration principles and best practices.

All plugins are configured using *Plugins.** parameter, which can either be part of the Zabbix agent 2 configuration file or a plugin's own configuration file. If a plugin uses a separate configuration file, path to this file should be specified in the Include parameter of Zabbix agent 2 configuration file.

A typical plugin parameter has the following structure:

Plugins.<PluginName>.<Parameter>=<Value>

Additionally, there are two specific groups of parameters:

- *Plugins.<PluginName>.Default.<Parameter>=<Value>* used for defining default parameter values.
- *Plugins.<PluginName>.<SessionName>.<Parameter>=<Value>* used for defining separate sets of parameters for different monitoring targets via named sessions.

All parameter names should adhere to the following requirements:

- it is recommended to capitalize the names of your plugins
- the parameter should be capitalized
- special characters are not allowed
- nesting isn't limited by a maximum level
- the number of parameters is not limited

For example, to perform active checks that do not have *Scheduling* update interval immediately after the agent restart only for the Uptime plugin, set `Plugins.Uptime.System.ForceActiveChecksOnStart=1` in the configuration file. Similarly, to set custom limit for concurrent checks for the CPU plugin, set the `Plugins.CPU.System.Capacity=N` in the configuration file.

Default values

You can set default values for the connection-related parameters (URI, username, password, etc.) in the configuration file in the format:

```
Plugins.<PluginName>.Default.<Parameter>=<Value>
```

For example, `Plugins.Mysql.Default.Username=zabbix`, `Plugins.MongoDB.Default.Uri=tcp://127.0.0.1:27017`, etc.

If a value for such parameter is not provided in an item key or in the named session parameters, the plugin will use the default value. If a default parameter is also undefined, hardcoded defaults will be used.

Note:
If an item key does not have any parameters, Zabbix agent 2 will attempt to collect the metric using values defined in the default parameters section.

Named sessions

Named sessions represent an additional level of plugin parameters and can be used to specify separate sets of authentication parameters for each of the instances being monitored. Each named session parameter should have the following structure:

```
Plugins.<PluginName>.Sessions.<SessionName>.<Parameter>=<Value>
```

A session name can be used as a connString item key parameter instead of specifying a URI, username, and/or password separately.

In item keys, the first parameter can be either a connString or a URI. If the first key parameter doesn't match any session name, it will be treated as a URI. Note that passing embedded URI credentials in the item key is not supported, use named session parameters instead.

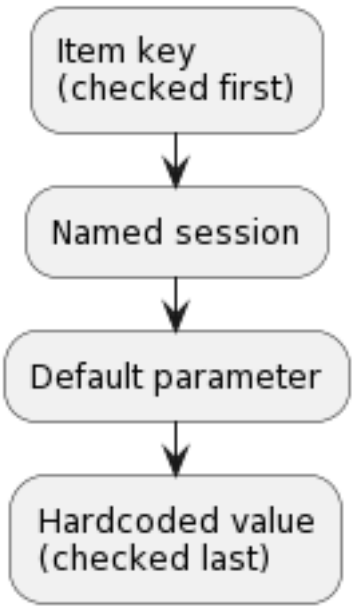
The list of available named session parameters depends on the plugin.

It is possible to override session parameters by specifying new values in the item key parameters (see example).

If a parameter is not defined for the named session, Zabbix agent 2 will use the value defined in the default plugin parameter.

Parameter priority

Zabbix agent 2 plugins search for connection-related parameter values in the following order:



1. The first item key parameter is compared to session names. If no match is found, it is treated as an actual value; in this case, step 3 will be skipped. If a match is found, the parameter value (usually, a URI) must be defined in the named session.
2. Other parameters will be taken from the item key if defined.
3. If an item key parameter (for example, password) is empty, plugin will look for the corresponding named session parameter.
4. If the session parameter is also not specified, the value defined in the corresponding default parameter will be used.

5. If all else fails, the plugin will use the hardcoded default value.

Example 1

Monitoring of two instances "MySQL1" and "MySQL2".

Configuration parameters:

```
Plugins.Mysql.Sessions.MySQL1.Uri=tcp://127.0.0.1:3306
Plugins.Mysql.Sessions.MySQL1.User=mysql1_user
Plugins.Mysql.Sessions.MySQL1.Password=unique_password
Plugins.Mysql.Sessions.MySQL2.Uri=tcp://192.0.2.0:3306
Plugins.Mysql.Sessions.MySQL2.User=mysql2_user
Plugins.Mysql.Sessions.MySQL2.Password=different_password
```

As a result of this configuration, each session name may be used as a connString in an item key, e.g., `mysql.ping[MySQL1]` or `mysql.ping[MySQL2]`.

Example 2

Providing some of the parameters in the item key.

Configuration parameters:

```
Plugins.PostgreSQL.Sessions.Session1.Uri=tcp://192.0.2.234:5432
Plugins.PostgreSQL.Sessions.Session1.User=old_username
Plugins.PostgreSQL.Sessions.Session1.Password=session_password
```

Item key: `pgsql.ping[session1,new_username,,postgres]`

As a result of this configuration, the agent will connect to PostgreSQL using the following parameters:

- URI from session parameter: `192.0.2.234:5432`
- Username from the item key: `new_username`
- Password from session parameter (since it is omitted in the item key): `session_password`
- Database name from the item key: `postgres`

Example 3

Collecting a metric using default configuration parameters.

Configuration parameters:

```
Plugins.PostgreSQL.Default.Uri=tcp://192.0.2.234:5432
Plugins.PostgreSQL.Default.User=zabbix
Plugins.PostgreSQL.Default.Password=password
```

Item key: `pgsql.ping[,,,postgres]`

As a result of this configuration, the agent will connect to PostgreSQL using the parameters:

- Default URI: `192.0.2.234:5432`
- Default username: `zabbix`
- Default password: `password`
- Database name from the item key: `postgres`

Connections

Some plugins support gathering metrics from multiple instances simultaneously. Both local and remote instances can be monitored. TCP and Unix-socket connections are supported.

It is recommended to configure plugins to keep connections to instances in an open state. The benefits are reduced network congestion, latency, and CPU and memory usage due to the lower number of connections. The client library takes care of this.

> **Note:**
> Time period for which unused connections should remain open can be determined by *Plugins.<PluginName>.KeepAlive* parameter. Example: *Plugins.Memcached.KeepAlive*

1 Ceph plugin

Overview

The configuration file of Zabbix agent 2 is used to configure plugins. These Zabbix agent 2 configuration parameters are supported for operating the Ceph plugin.

It is recommended to specify them in their own configuration file (e.g. `ceph.conf`) and then use the Include directive for adding this file to the Zabbix agent 2 configuration.

Note that:

- The default values reflect process defaults, not the values in the shipped configuration files;
- Values support environment variables;
- Zabbix supports configuration files only in UTF-8 encoding without BOM;
- Comments starting with "#" are only supported at the beginning of the line.

Parameters

Parameter	Mandatory	Range	Default	Description
Plugins.Ceph.Default.ApiKey				Default API key for connecting to Ceph; used if no value is specified in an item key or named session.
Plugins.Ceph.Default.Mode		native / restful	restful (deprecated)	Default mode for connecting to Ceph. The native mode is only supported on Linux and starting with Ceph 16. The restful mode will not work with Ceph version 20 or newer. Note that the user credential set differs for each mode and they are not compatible with each other.
Plugins.Ceph.Default.User				Default username for connecting to Ceph; used if no value is specified in an item key or named session.
Plugins.Ceph.Default.Uri			https://localhost:8003	Default URI for connecting to Ceph; used if no value is specified in an item key or named session. Should not include embedded credentials (they will be ignored). Must match the URI format. Only `https` scheme is supported; a scheme can be omitted. A port can be omitted (default=8003). Examples: `https://127.0.0.1:8003` `localhost`
Plugins.Ceph.InsecureSkipVerify		false / true	false	Determines whether an http client should verify the server's certificate chain and host name. If *true*, TLS accepts any certificate presented by the server and any host name in that certificate. In this mode, TLS is susceptible to man-in-the-middle attacks (should be used only for testing).
Plugins.Ceph.KeepAlive		60-900	300	The maximum time of waiting (in seconds) before unused plugin connections are closed.
Plugins.Ceph.Sessions.<SessionName>.ApiKey				Named session API key. **<SessionName>** - define name of a session for using in item keys.
Plugins.Ceph.Sessions.<SessionName>.Mode		native / restful	restful (deprecated)	Named session mode for connecting to Ceph. The native mode is only supported on Linux and starting with Ceph 16. The restful mode will not work with Ceph version 20 or newer. Note that the user credential set differs for each mode and they are not compatible with each other.
Plugins.Ceph.Sessions.<SessionName>.User				Named session username. **<SessionName>** - define name of a session for using in item keys.

Parameter	Mandatory	Range	Default	Description
Plugins.Ceph.Sessions.<SessionName>.Uri				Connection string of a named session. **<SessionName>** - define name of a session for using in item keys. Should not include embedded credentials (they will be ignored). Must match the URI format. Only `https` scheme is supported; a scheme can be omitted. A port can be omitted (default=8003). Examples: `https://127.0.0.1:8003` `localhost`
Plugins.Ceph.Timeout	no	1-30	global timeout	Request execution timeout (the duration, in seconds, to wait for a request to complete before shutting it down).

See also:

- Description of general Zabbix agent 2 configuration parameters: Zabbix agent 2 (UNIX) / Zabbix agent 2 (Windows)
- Instructions for configuring plugins

2 Docker plugin

Overview

The configuration file of Zabbix agent 2 is used to configure plugins. These Zabbix agent 2 configuration parameters are supported for operating the Docker plugin.

It is recommended to specify them in their own configuration file (e.g. `docker.conf`) and then use the Include directive for adding this file to the Zabbix agent 2 configuration.

Note that:

- The default values reflect process defaults, not the values in the shipped configuration files;
- Values support environment variables;
- Zabbix supports configuration files only in UTF-8 encoding without BOM;
- Comments starting with "#" are only supported at the beginning of the line.

Parameters

Parameter	Mandatory	Range	Default	Description
Plugins.Docker.Endpoint			unix:///var/run/docker.sock	Docker daemon unix-socket location. Must contain a scheme (only `unix://` is supported).
Plugins.Docker.Timeout	no	1-30	global timeout	Request execution timeout (the duration, in seconds, to wait for a request to complete before shutting it down).

See also:

- Description of general Zabbix agent 2 configuration parameters: Zabbix agent 2 (UNIX) / Zabbix agent 2 (Windows)
- Instructions for configuring plugins

3 Ember+ plugin

Overview

The configuration file of Zabbix agent 2 is used to configure plugins. These Zabbix agent 2 configuration parameters are supported for operating the Ember+ plugin.

It is recommended to specify them in their own configuration file (e.g. `emberplus.conf`) and then use the Include directive for adding this file to the Zabbix agent 2 configuration.

The Ember+ plugin is a loadable plugin and is available and fully described in the Ember+ plugin repository.

This plugin is currently only available to be built from the source (for both Unix and Windows).

Note that:

- The default values reflect process defaults, not the values in the shipped configuration files.
- Values support environment variables;
- Zabbix supports configuration files only in UTF-8 encoding without BOM.
- Comments starting with "#" are only supported at the beginning of the line.

Options

Parameter	Description
-V --version	Print the plugin version and license information.
-h --help	Print help information (shorthand).
-t, --test <item key>	Launch plugin for testing (plugin config ignored).

Parameters

Parameter	Mandatory	Range	Default	Description
Plugins.EmberPlus.Default.Uri			tcp://localhost:9998	The default URI to connect. The only supported schema is `tcp://`. A schema can be omitted. Embedded credentials will be ignored.
Plugins.EmberPlus.KeepAlive		60-900	300	The maximum time of waiting (in seconds) before unused plugin connections are closed.
Plugins.EmberPlus.Sessions.<SessionName>.Uri			tcp://localhost:9998	The URI to connect, for the named session. The only supported schema is `tcp://`. A schema can be omitted. Embedded credentials will be ignored. **<SessionName>** - define name of a session for using in item keys.
Plugins.EmberPlus.System.Path				Path to the Ember+ plugin executable. Example usage: `Plugins.EmberPlus.System.Path=/usr/libexec/zabbix/zabbix`
Plugins.EmberPlus.Timeout		1-30	global timeout	The duration, in seconds, to wait for a server to respond when first connecting and on follow-up operations in the session.

See also:

- Description of general Zabbix agent 2 configuration parameters: Zabbix agent 2 (UNIX) / Zabbix agent 2 (Windows)
- Instructions for configuring plugins

4 Memcached plugin

Overview

The configuration file of Zabbix agent 2 is used to configure plugins. These Zabbix agent 2 configuration parameters are supported for operating the Memcached plugin.

It is recommended to specify them in their own configuration file (e.g. `memcached.conf`) and then use the Include directive for adding this file to the Zabbix agent 2 configuration.

Note that:

- The default values reflect process defaults, not the values in the shipped configuration files;
- Values support environment variables;
- Zabbix supports configuration files only in UTF-8 encoding without BOM;
- Comments starting with "#" are only supported at the beginning of the line.

Parameters

Parameter	Mandatory	Range	Default	Description
Plugins.Memcached.Default.Password				Default password for connecting to Memcached; used if no value is specified in an item key or named session.

Parameter	Mandatory	Range	Default	Description

Plugins.Memcached.Default.Uri			tcp://localhost:11211	Default URI for connecting to Memcached; used if no value is specified in an item key or named session.
				
				Should not include embedded credentials (they will be ignored).
				Must match the URI format.
				Supported schemes: `tcp`, `unix`; a scheme can be omitted.
				A port can be omitted (default=11211).
				Examples: `tcp://localhost:11211`
				`localhost`
				`unix:/var/run/memcached.sock`

Plugins.Memcached.Default.User				Default username for connecting to Memcached; used if no value is specified in an item key or named session.
Plugins.Memcached.KeepAlive		60-900	300	The maximum time of waiting (in seconds) before unused plugin connections are closed.
Plugins.Memcached.Sessions.<SessionName>.Password				Named session password. **<SessionName>** - define name of a session for using in item keys.

Plugins.Memcached.Sessions.<SessionName>.Uri				Connection string of a named session.
				<SessionName> - define name of a session for using in item keys.
				
				Should not include embedded credentials (they will be ignored).
				Must match the URI format.
				Supported schemes: `tcp`, `unix`; a scheme can be omitted.
				A port can be omitted (default=11211).
				Examples: `tcp://localhost:11211`
				`localhost`
				`unix:/var/run/memcached.sock`

Plugins.Memcached.Sessions.<SessionName>.User				Named session username. **<SessionName>** - define name of a session for using in item keys.
Plugins.Memcached.Timeout		1-30	global timeout	Request execution timeout (the duration, in seconds, to wait for a request to complete before shutting it down).

See also:

- Description of general Zabbix agent 2 configuration parameters: Zabbix agent 2 (UNIX) / Zabbix agent 2 (Windows)
- Instructions for configuring plugins

5 Modbus plugin

Overview

The configuration file of Zabbix agent 2 is used to configure plugins. These Zabbix agent 2 configuration parameters are supported for operating the Modbus plugin.

It is recommended to specify them in their own configuration file (e.g. `modbus.conf`) and then use the Include directive for adding this file to the Zabbix agent 2 configuration.

Note that:

- The default values reflect process defaults, not the values in the shipped configuration files;
- Values support environment variables;
- Zabbix supports configuration files only in UTF-8 encoding without BOM;
- Comments starting with "#" are only supported at the beginning of the line.

Parameters

Parameter	Mandatory	Range	Default	Description
Plugins.Modbus.Sessions.<SessionName>.Endpoint				Endpoint is a connection string consisting of a protocol scheme, a host address and a port or serial port name and attributes. **<SessionName>** - define name of a session for using in item keys.
Plugins.Modbus.Sessions.<SessionName>.SlaveID				Slave ID of a named session. **<SessionName>** - define name of a session for using in item keys. Example: `Plugins.Modbus.Sessions.MB1.SlaveID=20` *Note* that this named session parameter is checked only if the value provided in the item key slave ID parameter is empty.
Plugins.Modbus.Sessions.<SessionName>.Timeout				Timeout of a named session in seconds. **<SessionName>** - define name of a session for using in item keys. Example: `Plugins.Modbus.Sessions.MB1.Timeout=2`

If you need to set the request execution timeout (how long to wait for a request to complete before shutting it down), use the item configuration form.

See also:

- Description of general Zabbix agent 2 configuration parameters: Zabbix agent 2 (UNIX) / Zabbix agent 2 (Windows)
- Instructions for configuring plugins

6 MongoDB plugin

Overview

The configuration file of Zabbix agent 2 is used to configure plugins. These Zabbix agent 2 configuration parameters are supported for operating the MongoDB plugin.

It is recommended to specify them in their own configuration file (e.g., `mongo.conf`) and then use the Include directive for adding this file to the Zabbix agent 2 configuration.

The MongoDB plugin is a loadable plugin and is available and fully described in the MongoDB plugin repository.

Note that:

- The default values reflect process defaults, not the values in the shipped configuration files.
- Values support environment variables.
- Zabbix supports configuration files only in UTF-8 encoding without BOM.
- Comments starting with "#" are only supported at the beginning of the line.

Options

Parameter	Description
-V --version	Print the plugin version and license information.
-h --help	Print help information (shorthand).
-t, --test <item key>	Launch plugin for testing (plugin config ignored).

Parameters

When connecting to MongoDB, the plugin checks its configuration in a specific order, which determines which value to use. The order, from highest to lowest priority, is as follows:

1. Parameters specified in the connection URI (e.g., query parameters defined after ? in `Plugins.MongoDB.Sessions.<session_name` have the highest priority).
2. Parameters in the Zabbix agent 2 item key (e.g., mongodb.collection.stats).
3. Parameters defined in a named session (e.g., `Plugins.MongoDB.Sessions.<SessionName>.User`, `Plugins.MongoDB.Sessions`
4. Default values (e.g., `Plugins.MongoDB.Default.User`, `Plugins.MongoDB.Default.Password`).

For example:

- If you specify the database for authenticating a connection to the MongoDB server in the `*.<SessionName>.Uri` parameter (e.g., `Plugins.MongoDB.Sessions.<session_name>.Uri=mongodb://user:password@127.0.0.1:27017/?authSource=a` then the plugin will consider the `*.<SessionName>.AuthSource` parameter to be set to `admin`, even if the `*.<SessionName>.AuthSource` parameter is set to a different value.
- If you specify the URI in the `*.<SessionName>.Uri` parameter (e.g., `Plugins.MongoDB.Sessions.<session_name>.Uri=mongo` but provide the username and the password in the Zabbix agent 2 item key, the plugin will use the username and password from the item key, even if `Plugins.MongoDB.Sessions.<SessionName>.User` and `Plugins.MongoDB.Sessions.<SessionNam` are configured.

Attention:
If the `mongodb+srv://` scheme is used, the URI may retrieve parameters from a DNS TXT record. Parameters obtained from this TXT record override all other configurations, including URI parameters, Zabbix Agent 2 item key parameters, and session parameters.
 Only one TXT record may exist for the hostname used in the connection string.

Parameter	Mandatory	Range	Default	Description
Plugins.MongoDB.System.Path	No			Path to the MongoDB plugin executable. Example usage: `Plugins.MongoDB.System.Path=/usr/libexec/zabbix/zabbix-ag`
Plugins.MongoDB.Timeout	No	1-30	global timeout	Request execution timeout (the duration, in seconds, to wait for a request to complete before shutting it down).
Plugins.MongoDB.KeepAlive	No	60-900	300	The maximum time of waiting (in seconds) before unused plugin connections are closed.
Plugins.MongoDB.Sessions.<SessionName>.Uri	No		`tcp://127.0.0.1:27017`	Connection string of a named session. **<SessionName>** - define name of a session for using in item keys. Must match the URI format. Supported schemes: `mongodb://` and `mongodb+srv://`; the `tcp://` scheme is deprecated and kept for backward compatibility with existing configurations. A port can be omitted (default=27017). Examples: `mongodb://127.0.0.1:27017`, `mongodb+srv://example.com`, `localhost`.
Plugins.MongoDB.Sessions.<SessionName>.User	No			Named session username. **<SessionName>** - define name of a session for using in item keys.
Plugins.MongoDB.Sessions.<SessionName>.Password	No			Named session password. **<SessionName>** - define name of a session for using in item keys.
Plugins.MongoDB.Sessions.<SessionName>.Direct	No		`false`	Connection method used to determine whether automatic discovery of MongoDB replica set nodes should be enabled or disabled. **<SessionName>** - define name of a session for using in item keys. Supported values: `true` - the plugin will connect only to the specified server, ignoring other members of the replica set; `false` - the plugin will automatically discover all nodes in the replica set. If the `tcp://` (deprecated) scheme is used, the parameter is set to `true` by default.
Plugins.MongoDB.Sessions.<SessionName>.AuthMechanism	No			Authentication mechanism for connecting to MongoDB server. **<SessionName>** - define name of a session for using in item keys. Supported values: `SCRAM-SHA-1`, `SCRAM-SHA-256`, and `MONGODB-X509`.

Parameter	Mandatory	Range	Default	Description
Plugins.MongoDB.Sessions.<SessionName>.AuthSource	No		admin	Database for authenticating connection to MongoDB server. **<SessionName>** - define name of a session for using in item keys. If the `MONGODB-X509` authentication mechanism is used, this parameter is automatically set to `$external`; modifying it to any other value will cause an error when launching.
Plugins.MongoDB.Sessions.<SessionName>.ReplicaSet	No			Replica set name, used for automatic discovery of MongoDB replica set nodes. **<SessionName>** - define name of a session for using in item keys. If this parameter is used with the `mongodb+srv://` scheme, it will behave as if multiple URLs have been provided; a DNS server may have a TXT record that can override this (or any other) parameter.
Plugins.MongoDB.Sessions.<SessionName>.ReadPreference	No			Order for connecting to MongoDB replica set nodes or fallback. **<SessionName>** - define name of a session for using in item keys. Supported values: `PrimaryMode`, `PrimaryPreferredMode`, `SecondaryMode`, `SecondaryPreferredMode`, and `NearestMode`. Unavailable if the `Plugins.MongoDB.Sessions.<SessionName>.Direct` parameter is set to `true`, the agent will fail to start.
Plugins.MongoDB.Sessions.<SessionName>.TLSConnect	No			Encryption type for communications between Zabbix agent 2 and monitored databases. **<SessionName>** - define name of a session for using in item keys. Supported values: `required` - require TLS connection; `verify\_ca` - verify certificates; `verify\_full` - verify certificates and IP address. Supported since plugin version 1.2.1.
Plugins.MongoDB.Sessions.<SessionName>.TLSCAFile	Yes, if Plugins.MongoDB.Sessions.<SessionName>.TLSConnect is set to one of: verify_ca, verify_full			Full pathname of a file containing the top-level CA(s) certificates for peer certificate verification, used for encrypted communications between Zabbix agent 2 and monitored databases. **<SessionName>** - define name of a session for using in item keys.
Plugins.MongoDB.Sessions.<SessionName>.TLSCertFile	Yes, if Plugins.MongoDB.Sessions.<SessionName>.TLSKeyFile is specified			Full pathname of a file containing the agent certificate or certificate chain, used for encrypted communications between Zabbix agent 2 and monitored databases. **<SessionName>** - define name of a session for using in item keys.
Plugins.MongoDB.Sessions.<SessionName>.TLSKeyFile	Yes, if Plugins.MongoDB.Sessions.<SessionName>.TLSCertFile is specified			Full pathname of a file containing the database private key used for encrypted communications between Zabbix agent 2 and monitored databases. **<SessionName>** - define name of a session for using in item keys.

Parameter	Mandatory	Range	Default	Description
Plugins.MongoDB.Default.Uri	No		tcp://127.0.0.1:27017	Default URI for connecting to MongoDB. Must match the URI format. Supported schemes: mongodb:// and mongodb+srv://. Deprecated scheme: tcp:// (used as the default for backward compatibility with existing configurations). A port can be omitted (default=27017). Examples: mongodb://127.0.0.1:27017, mongodb+srv://example.com, localhost.
Plugins.MongoDB.Default.User	No			Default username for connecting to MongoDB.
Plugins.MongoDB.Default.Password	No			Default password for connecting to MongoDB.
Plugins.MongoDB.Default.Direct	No		false	Default connection method used to determine whether automatic discovery of MongoDB replica set nodes should be enabled or disabled. Supported values: true - the plugin will connect only to the specified server, ignoring other members of the replica set; false - the plugin will automatically discover all nodes in the replica set. If the tcp:// (deprecated) scheme is used, the parameter is set to true by default.
Plugins.MongoDB.Default.AuthMechanism	No			Default authentication mechanism for connecting to MongoDB server. Supported values: SCRAM-SHA-1, SCRAM-SHA-256, and MONGODB-X509. If no value is specified either here, in an item key, in a named session, or in the URI, a SCRAM-based mechanism is used (if a username is provided; otherwise, no authentication will be used).
Plugins.MongoDB.Default.AuthSource	No		admin	Default database for authenticating connection to MongoDB server. If the MONGODB-X509 authentication mechanism is used, this parameter is automatically set to $external; modifying it to any other value will cause an error when launching.
Plugins.MongoDB.Default.ReplicaSet	No			Default replica set name; used for automatic discovery of MongoDB replica set nodes. If this parameter is used with the mongodb+srv:// scheme, it will behave as if multiple URLs have been provided; a DNS server may have a TXT record that can override this (or any other) parameter. Unavailable if the Plugins.MongoDB.Default.Direct parameter is set to true, the agent will fail to start.
Plugins.MongoDB.Default.ReadPreference	No			Default order for connecting to MongoDB replica set nodes or fallback. Supported values: PrimaryMode, PrimaryPreferredMode, SecondaryMode, SecondaryPreferredMode, and NearestMode. Unavailable if the Plugins.MongoDB.Default.Direct parameter is set to true, the agent will fail to start.

Parameter	Mandatory	Range	Default	Description
Plugins.MongoDB.Default.TLSConnect				Default encryption type for communications between Zabbix agent 2 and monitored databases. Supported values: `required` - requires TLS connection. `verify\_ca` - verifies certificates. `verify\_full` - verifies certificates and IP address. If no value is specified either here, in an item key, in a named session, or in the URI, a TLS connection will not be established.
Plugins.MongoDB.Default.TLSCAFile				Default pathname of a file containing the top-level CA(s) certificates for peer certificate verification. Used for encrypted communications between Zabbix agent 2 and monitored databases.
Plugins.MongoDB.Default.TLSCertFile				Default pathname of a file containing the MongoDB client certificate or certificate chain. Used for encrypted communications between Zabbix agent 2 and monitored databases.
Plugins.MongoDB.Default.TLSKeyFile				Default pathname of a file containing the MongoDB client private key used for encrypted communications between Zabbix agent 2 and monitored databases.

See also:

- Description of general Zabbix agent 2 configuration parameters: Zabbix agent 2 (UNIX) / Zabbix agent 2 (Windows)
- Instructions for configuring plugins

7 MQTT plugin

Overview

The configuration file of Zabbix agent 2 is used to configure plugins. These Zabbix agent 2 configuration parameters are supported for operating the MQTT plugin.

It is recommended to specify them in their own configuration file (e.g. `mqtt.conf`) and then use the Include directive for adding this file to the Zabbix agent 2 configuration.

Note that:

- The default values reflect process defaults, not the values in the shipped configuration files;
- Values support environment variables;
- Zabbix supports configuration files only in UTF-8 encoding without BOM;
- Comments starting with "#" are only supported at the beginning of the line.

Parameters

Parameter	Mandatory	Range	Default	Description
Plugins.MQTT.Default.Password				Default password for connecting to MQTT; used if no value is specified in an item key or named session.
Plugins.MQTT.Default.TLSCAFile				Full pathname of a file containing the top-level CA(s) certificates for peer certificate verification for encrypted communications between Zabbix agent 2 and MQTT broker; used if no value is specified in a named session.
Plugins.MQTT.Default.TLSCertFile				Full pathname of a file containing the agent certificate or certificate chain for encrypted communications between Zabbix agent 2 and MQTT broker; used if no value is specified in a named session.
Plugins.MQTT.Default.TLSKeyFile				Full pathname of a file containing the MQTT private key for encrypted communications between Zabbix agent 2 and MQTT broker; used if no value is specified in a named session.

Parameter	Mandatory	Range	Default	Description

Plugins.MQTT.Default.Topic				Default topic for MQTT subscription; used if no value is specified in an item key or named session.
				
				The topic may contain wildcards (”+”,”#”)
				Examples: `path/to/file`
				`path/to/#`
				`path/+/topic`

Plugins.MQTT.Default.Url			tcp://localhost:1883	Default MQTT broker connection string; used if no value is specified in an item key or named session.
				
				Should not include query parameters.
				Must match the URL format.
				Supported schemes: `tcp` (default), `ws`, `tls`; a scheme can be omitted.
				A port can be omitted (default=1883).
				Examples: `tcp://host:1883`
				`localhost`
				`ws://host:8080`

Plugins.MQTT.Default.User				Default username for connecting to MQTT; used if no value is specified in an item key or named session.
Plugins.MQTT.Sessions.<SessionName>.Password				Named session password. **<SessionName>** - define name of a session for using in item keys.
Plugins.MQTT.Sessions.<SessionName>.TLSCAFile				Full pathname of a file containing the top-level CA(s) certificates for peer certificate verification, used for encrypted communications between Zabbix agent 2 and MQTT broker. **<SessionName>** - define name of a session for using in item keys.
Plugins.MQTT.Sessions.<SessionName>.TLSCertFile				Full pathname of a file containing the agent certificate or certificate chain, used for encrypted communications between Zabbix agent 2 and MQTT broker. **<SessionName>** - define name of a session for using in item keys.
Plugins.MQTT.Sessions.<SessionName>.TLSKeyFile				Full pathname of a file containing the MQTT private key used for encrypted communications between Zabbix agent 2 and MQTT broker. **<SessionName>** - define name of a session for using in item keys.

Plugins.MQTT.Sessions.<SessionName>.Topic				Named session topic for MQTT subscription.
				<SessionName> - define name of a session for using in item keys.
				
				The topic may contain wildcards (”+”,”#”)
				Examples: `path/to/file`
				`path/to/#`
				`path/+/topic`

Plugins.MQTT.Sessions.<SessionName>.Url				Connection string of a named session.
				<SessionName> - define name of a session for using in item keys.
				
				Should not include query parameters.
				Must match the URL format.
				Supported schemes: `tcp` (default), `ws`, `tls`; a scheme can be omitted.
				A port can be omitted (default=1883).
				Examples: `tcp://host:1883`
				`localhost`
				`ws://host:8080`

Plugins.MQTT.Sessions.<SessionName>.User				Named session username. **<SessionName>** - define name of a session for using in item keys.

If you need to set the request execution timeout (how long to wait for a request to complete before shutting it down), use the item configuration form.

See also:

- Description of general Zabbix agent 2 configuration parameters: Zabbix agent 2 (UNIX) / Zabbix agent 2 (Windows)
- Instructions for configuring plugins

8 MSSQL plugin

Overview

The configuration file of Zabbix agent 2 is used to configure plugins. These Zabbix agent 2 configuration parameters are supported for operating the MSSQL plugin.

It is recommended to specify them in their own configuration file (e.g. `mssql.conf`) and then use the Include directive for adding this file to the Zabbix agent 2 configuration.

The MSSQL plugin is a loadable plugin and is available and fully described in the MSSQL plugin repository.

Note that:

- The default values reflect process defaults, not the values in the shipped configuration files.
- Values support environment variables;
- Zabbix supports configuration files only in UTF-8 encoding without BOM.
- Comments starting with "#" are only supported at the beginning of the line.

Options

Parameter	Description
-V --version	Print the plugin version and license information.
-h --help	Print help information (shorthand).
-t, --test <item key>	Launch plugin for testing (plugin config ignored).

Parameters

Parameter	Mandatory	Range	Default	Description
Plugins.MSSQL.CustomQueriesDir			`/usr/local/share/zabbix/custom-queries/mssql` for Unix systems `*:\Program Files\Zabbix Agent 2\Custom Queries\MSSQL` for Windows systems, where * is the drive name from the `ProgramFiles` environment variable	Specify the file path to a directory containing user-defined .sql files with custom queries that the plugin can execute. The plugin loads all available .sql files in the configured directory at startup. This means that any changes to the custom query files will not be reflected until the plugin is restarted. The plugin is started and stopped together with Zabbix agent 2.
Plugins.MSSQL.CustomQueriesEnabled			false	If set, enables the execution of the `mssql.custom.query` item key. If disabled, no queries will be loaded from the custom query directory path.
Plugins.MSSQL.Default.CACertPath				The default file path to the public key certificate of the certificate authority (CA) that issued the certificate of the MSSQL server. The certificate must be in PEM format.
Plugins.MSSQL.Default.Database				The default database name to connect to.

Parameter	Mandatory	Range	Default	Description
Plugins.MSSQL.Default.Encrypt				Specifies the default connection encryption type. Possible values are: *true* - data sending between plugin and server is encrypted; *false* - data sending between plugin and server is not encrypted beyond the login packet; *strict* - data sending between plugin and server is encrypted E2E using TDS8; *disable* - data sending between plugin and server is not encrypted.
Plugins.MSSQL.Default.HostNameInCertificate				The common name (CN) of the certificate of the MSSQL server by default.
Plugins.MSSQL.Default.Password				The password to be sent to a protected MSSQL server by default.
Plugins.MSSQL.Default.TLSMinVersion				The minimum TLS version to use by default. Possible values are: `1.0`, `1.1`, `1.2`, `1.3`.
Plugins.MSSQL.Default.TrustServerCertificate				Whether the plugin should trust the server certificate without validating it by default. Possible values: `true`, `false`.
Plugins.MSSQL.Default.Uri			sqlserver://localhost:1433	The default URI to connect. The only supported schema is `sqlserver://`. A schema can be omitted. Embedded credentials will be ignored.
Plugins.MSSQL.Default.User				The default username to be sent to a protected MSSQL server.
Plugins.MSSQL.KeepAlive		60-900	300	The maximum time of waiting (in seconds) before unused plugin connections are closed.
Plugins.MSSQL.Sessions.<SessionName>.CACertPath				The file path to the public key certificate of the certificate authority (CA) that issued the certificate of the MSSQL server for the named session. The certificate must be in PEM format. **<SessionName>** - define name of a session for using in item keys.
Plugins.MSSQL.Sessions.<SessionName>.Database				The database name to connect to for the named session. **<SessionName>** - define name of a session for using in item keys.
Plugins.MSSQL.Sessions.<SessionName>.Encrypt				Specifies the connection encryption type for the named session. Possible values are: *true* - data sending between plugin and server is encrypted; *false* - data sending between plugin and server is not encrypted beyond the login packet; *strict* - data sending between plugin and server is encrypted E2E using TDS8; *disable* - data sending between plugin and server is not encrypted. **<SessionName>** - define name of a session for using in item keys.
Plugins.MSSQL.Sessions.<SessionName>.HostNameInCertificate				The common name (CN) of the certificate of the MSSQL server for the named session. **<SessionName>** - define name of a session for using in item keys.
Plugins.MSSQL.Sessions.<SessionName>.Password				The password to be sent to a protected MSSQL server for the named session. **<SessionName>** - define name of a session for using in item keys.
Plugins.MSSQL.Sessions.<SessionName>.TLSMinVersion				The minimum TLS version to use for the named session. Possible values are: `1.0`, `1.1`, `1.2`, `1.3`. **<SessionName>** - define name of a session for using in item keys.
Plugins.MSSQL.Sessions.<SessionName>.TrustServerCertificate				Whether the plugin should trust the server certificate without validating it for the named session. Possible values: `true`, `false`. **<SessionName>** - define name of a session for using in item keys.

Parameter	Mandatory	Range	Default	Description
Plugins.MSSQL.Sessions.<SessionName>.Uri	no		sqlserver://localhost:1433	The URI to connect, for the named session. The only supported schema is `sqlserver://`. A schema can be omitted. Embedded credentials will be ignored. **<SessionName>** - define name of a session for using in item keys.
Plugins.MSSQL.Sessions.<SessionName>.User	no			The username to be sent to a protected MSSQL server for the named session. **<SessionName>** - define name of a session for using in item keys.
Plugins.MSSQL.System.Path	no			Path to the MSSQL plugin executable. Global setting for the MSSQL plugin. Applied to all connections. Example usage: `Plugins.MSSQL.System.Path=/usr/libexec/zabbix/zabbix-agen`
Plugins.MSSQL.Timeout	no	1-30	global timeout	The duration, in seconds, to wait for a server to respond when first connecting and on follow-up operations in the session.

See also:

- Description of general Zabbix agent 2 configuration parameters: Zabbix agent 2 (UNIX) / Zabbix agent 2 (Windows)
- Instructions for configuring plugins

9 MySQL plugin

Overview

The configuration file of Zabbix agent 2 is used to configure plugins. These Zabbix agent 2 configuration parameters are supported for operating the MySQL plugin.

It is recommended to specify them in their own configuration file (e.g. `mysql.conf`) and then use the Include directive for adding this file to the Zabbix agent 2 configuration.

Note that:

- The default values reflect process defaults, not the values in the shipped configuration files;
- Values support environment variables;
- Zabbix supports configuration files only in UTF-8 encoding without BOM;
- Comments starting with "#" are only supported at the beginning of the line.

Parameters

Parameter	Mandatory	Range	Default	Description
Plugins.Mysql.CallTimeout	no	1-30	global timeout	The maximum amount of time in seconds to wait for a request to be done.
Plugins.Mysql.CustomQueriesPath	no		`/usr/local/share/zabbix/custom-queries/mysql` for Unix systems `*:\Program Files\Zabbix Agent 2\Custom Queries\Mysql` for Windows systems, where * is the drive name from the `ProgramFiles` environment variable	Full path to a directory containing `*.sql` files with custom queries.

Parameter	Mandatory	Range	Default	Description
Plugins.Mysql.CustomQueriesEnabled			false	If set, enables the execution of the `mysql.custom.query` item key. If disabled, no queries will be loaded from the custom query directory path.
Plugins.Mysql.Default.Password				Default password for connecting to MySQL; used if no value is specified in an item key or named session.
Plugins.Mysql.Default.TLSCAFile	no (yes, if Plugins.Mysql.Default.TLSConnect is set to *verify_ca* or *verify_full*)			Full pathname of a file containing the top-level CA(s) certificates for peer certificate verification for encrypted communications between Zabbix agent 2 and monitored databases; used if no value is specified in a named session.
Plugins.Mysql.Default.TLSCertFile	no (yes, if Plugins.Mysql.Default.TLSConnect is set to *verify_ca* or *verify_full*)			Full pathname of a file containing the agent certificate or certificate chain for encrypted communications between Zabbix agent 2 and monitored databases; used if no value is specified in a named session.
Plugins.Mysql.Default.TLSConnect				Encryption type for communications between Zabbix agent 2 and monitored databases; used if no value is specified in a named session. Supported values: *required* - require TLS connection; *verify_ca* - verify certificates; *verify_full* - verify certificates and IP address.
Plugins.Mysql.Default.TLSKeyFile	no (yes, if Plugins.Mysql.Default.TLSConnect is set to *verify_ca* or *verify_full*)			Full pathname of a file containing the database private key for encrypted communications between Zabbix agent 2 and monitored databases; used if no value is specified in a named session.

Plugins.Mysql.Default.Uri			tcp://localhost:3306	Default URI for connecting to MySQL; used if no value is specified in an item key or named session.
				
				Should not include embedded credentials (they will be ignored).
				Must match the URI format.
				Supported schemes: `tcp`, `unix`; a scheme can be omitted.
				A port can be omitted (default=3306).
				Examples: `tcp://localhost:3306`
				`localhost`
				`unix:/var/run/mysql.sock`

Plugins.Mysql.Default.User				Default username for connecting to MySQL; used if no value is specified in an item key or named session.
Plugins.Mysql.KeepAlive		60-900	300	The maximum time of waiting (in seconds) before unused plugin connections are closed.
Plugins.Mysql.Sessions.<SessionName>.Password				Named session password. **<SessionName>** - define name of a session for using in item keys.
Plugins.Mysql.Sessions.<SessionName>.TLSCAFile	no (yes, if Plugins.Mysql.Sessions.<SessionName>.TLSConnect is set to *verify_ca* or *verify_full*)			Full pathname of a file containing the top-level CA(s) certificates for peer certificate verification, used for encrypted communications between Zabbix agent 2 and monitored databases. **<SessionName>** - define name of a session for using in item keys.
Plugins.Mysql.Sessions.<SessionName>.TLSCertFile	yes, if Plugins.Mysql.Sessions.<SessionName>.TLSKeyFile is specified			Full pathname of a file containing the agent certificate or certificate chain, used for encrypted communications between Zabbix agent 2 and monitored databases. **<SessionName>** - define name of a session for using in item keys.

Parameter	Mandatory	Range	Default	Description
Plugins.Mysql.Sessions.<SessionName>.TLSConnect				Encryption type for communications between Zabbix agent 2 and monitored databases. **<SessionName>** - define name of a session for using in item keys. Supported values: *required* - require TLS connection; *verify_ca* - verify certificates; *verify_full* - verify certificates and IP address.
Plugins.Mysql.Sessions.<SessionName>.TLSKeyFile	yes, if Plugins.Mysql.Sessions.<SessionName>.TLSCertFile is specified			Full pathname of a file containing the database private key used for encrypted communications between Zabbix agent 2 and monitored databases. **<SessionName>** - define name of a session for using in item keys.

Plugins.Mysql.Sessions.<SessionName>.Uri				Connection string of a named session.
				<SessionName> - define name of a session for using in item keys.
				
				Should not include embedded credentials (they will be ignored).
				Must match the URI format.
				Supported schemes: `tcp`, `unix`; a scheme can be omitted.
				A port can be omitted (default=3306).
				Examples: `tcp://localhost:3306`
				`localhost`
				`unix:/var/run/mysql.sock`

Plugins.Mysql.Sessions.<SessionName>.User				Named session username. **<SessionName>** - define name of a session for using in item keys.
Plugins.Mysql.Timeout		1-30	global timeout	The maximum time in seconds for waiting when a connection has to be established.

See also:

- Description of general Zabbix agent 2 configuration parameters: Zabbix agent 2 (UNIX) / Zabbix agent 2 (Windows)
- Instructions for configuring plugins

10 NVIDIA GPU plugin

Overview

The configuration file of Zabbix agent 2 is used to configure plugins. These Zabbix agent 2 configuration parameters are supported for operating the NVIDIA GPU plugin.

It is recommended to specify them in their own configuration file (e.g. `nvidiagpu.conf`) and then use the Include directive for adding this file to the Zabbix agent 2 configuration.

The NVIDIA GPU plugin is a loadable plugin and is available and fully described in the NVIDIA GPU plugin repository.

Note that:

- The default values reflect process defaults, not the values in the shipped configuration files;
- Values support environment variables;
- Zabbix supports configuration files only in UTF-8 encoding without BOM;
- Comments starting with ”#” are only supported at the beginning of the line.

Parameters

Parameter	Mandatory	Range	Default	Description
Plugins.NVIDIA.System.Path				Path to the NVIDIA GPU plugin executable. Example usage: `Plugins.NVIDIA.System.Path=/path/to/executable/nvidia`

Parameter	Mandatory	Range	Default	Description
Plugins.NVIDIA.Timeout		1-30	global timeout	Specifies the maximum time (in seconds) to wait for a server response during connection attempts and subsequent operations in the session. The global item-type timeout or individual item timeout will override this value if greater.

See also:

- Description of general Zabbix agent 2 configuration parameters: Zabbix agent 2 (UNIX) / Zabbix agent 2 (Windows)
- Instructions for configuring plugins

11 Oracle plugin

Overview

The configuration file of Zabbix agent 2 is used to configure plugins. These Zabbix agent 2 configuration parameters are supported for operating the Oracle plugin.

It is recommended to specify them in their own configuration file (e.g. `oracle.conf`) and then use the Include directive for adding this file to the Zabbix agent 2 configuration.

Note that:

- The default values reflect process defaults, not the values in the shipped configuration files.
- Values support environment variables.
- Zabbix supports configuration files only in UTF-8 encoding without BOM.
- Comments starting with "#" are only supported at the beginning of the line.

Parameters

Parameter	Mandatory	Range	Default	Description
Plugins.Oracle.CallTimeout		1-30	global timeout	The maximum wait time in seconds for a request to be completed.
Plugins.Oracle.ConnectTimeout		1-30	global timeout	The maximum wait time in seconds for a connection to be established.
Plugins.Oracle.CustomQueriesPath			`/usr/local/share/zabbix/oracle/custom.queries` for Unix systems `*:\Program Files\Zabbix Agent 2\Custom Queries\Oracle` for Windows systems, where `*` is the drive name from the `ProgramFiles` environment variable	Full path to a directory containing `*.sql` files with custom queries. Example: `/etc/zabbix/oracle/sql`
Plugins.Oracle.CustomQueriesEnabled			false	If set, enables the execution of the `oracle.custom.query` item key. If disabled, no queries will be loaded from the custom query directory path.
Plugins.Oracle.Default.Password				Default password for connecting to Oracle; used if no value is specified in an item key or named session.
Plugins.Oracle.Default.Service				Default service name for connecting to Oracle (SID is not supported); used if no value is specified in an item key or named session.

Parameter	Mandatory	Range	Default	Description
Plugins.Oracle.Default.Uri				Default URI for connecting to Oracle; used if no value is specified in an item key or named session. Should not include embedded credentials (they will be ignored). Must match the URI format. Only `tcp` and `tcps` schemes are supported; a scheme can be omitted. A port can be omitted (default=1521). It is also possible to specify the TNS key or TNS value as the connection string. The TNS value must be composed without whitespaces. Examples: `tcp://127.0.0.1:1521` `localhost` `zbx_tns_example` (TNS key) `(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=localhost)(POR` (TNS value)
Plugins.Oracle.Default.User				Default username for connecting to Oracle; used if no value is specified in an item key or named session.
Plugins.Oracle.KeepAlive		60-900	300	The maximum time of waiting (in seconds) before unused plugin connections are closed.
Plugins.Oracle.ResolveTNS		true / false	true	The option specifies how to interpret the connection string (ConnString) for connecting to the Oracle server. If it is set to false the default scheme and port will be added to ConnString (if absent). If the option is set to true, the default scheme and port will be omitted (unless explicitly specified in ConnString), and ConnString will be passed to the Oracle client as is. If the Oracle client finds ConnString in the tnsnames.ora file, the connection description found will be used to connect to the Oracle server.
Plugins.Oracle.Sessions.<SessionName>.Password				Named session password. **<SessionName>** - define name of a session for using in item keys.
Plugins.Oracle.Sessions.<SessionName>.Service				Named session service name to be used for connection (SID is not supported). **<SessionName>** - define name of a session for using in item keys.
Plugins.Oracle.Sessions.<SessionName>.Uri				Named session connection string for Oracle. **<SessionName>** - define name of a session for using in item keys. Should not include embedded credentials (they will be ignored). Must match the URI format. Only `tcp` and `tcps` schemes are supported; a scheme can be omitted. A port can be omitted (default=1521). It is also possible to specify the TNS key or TNS value as the connection string. The TNS value must be composed without whitespaces. Examples: `tcp://127.0.0.1:1521` `localhost` `zbx_tns_example` (TNS key) `(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=localhost)(POR` (TNS value)
Plugins.Oracle.Sessions.<SessionName>.User				Named session username. **<SessionName>** - define name of a session for using in item keys.

See also:

- Description of general Zabbix agent 2 configuration parameters: Zabbix agent 2 (UNIX) / Zabbix agent 2 (Windows)
- Instructions for configuring plugins

12 PostgreSQL plugin

Overview

The configuration file of Zabbix agent 2 is used to configure plugins. These Zabbix agent 2 configuration parameters are supported for operating the PostgreSQL plugin.

It is recommended to specify them in their own configuration file (e.g. `postgresql.conf`) and then use the Include directive for adding this file to the Zabbix agent 2 configuration.

The PostgreSQL plugin is a loadable plugin and is available and fully described in the PostgreSQL plugin repository.

Note that:

- The default values reflect process defaults, not the values in the shipped configuration files.
- Values support environment variables;
- Zabbix supports configuration files only in UTF-8 encoding without BOM.
- Comments starting with "#" are only supported at the beginning of the line.

Options

Parameter	Description
-V --version	Print the plugin version and license information.
-h --help	Print help information (shorthand).
-t, --test <item key>	Launch plugin for testing (plugin config ignored).

Parameters

Parameter	Mandatory	Range	Default	Description
Plugins.PostgreSQL.Default.CacheMode			prepare	Cache mode for the PostgreSQL connection. Supported values: *prepare* (default) - will create prepared statements on the PostgreSQL server; *describe* - will use the anonymous prepared statement to describe a statement without creating a statement on the server. Note that "describe" is primarily useful when the environment does not allow prepared statements such as when running a connection pooler like PgBouncer.
Plugins.PostgreSQL.CallTimeout		1-30	global timeout	Maximum wait time (in seconds) for a request to be completed.
Plugins.PostgreSQL.CustomQueriesPath			/usr/local/share/zabbix/custom-queries/postgresql for Unix systems *:\Program Files\Zabbix Agent 2\Custom Queries\PostgreSQL for Windows systems, where * is the drive name from the ProgramFiles environment variable	Full pathname of a directory containing files with custom queries.

Parameter	Mandatory	Range	Default	Description
Plugins.PostgreSQL.CustomQueriesEnabled			false	If set, enables the execution of the `postgresql.custom.query` item key. If disabled, no queries will be loaded from the custom query directory path.
Plugins.PostgreSQL.Default.Database				Default database for connecting to PostgreSQL; used if no value is specified in an item key or named session.
Plugins.PostgreSQL.Default.Password				Default password for connecting to PostgreSQL; used if no value is specified in an item key or named session.
Plugins.PostgreSQL.Default.TLSCAFile	(yes, if Plugins.PostgreSQL.Default.TLSConnect is set to *verify_ca* or *verify_full*)			Full pathname of a file containing the top-level CA(s) certificate for peer certificate verification for encrypted communications between Zabbix agent 2 and monitored databases; used if no value is specified in a named session.
Plugins.PostgreSQL.Default.TLSCertFile	(yes, if Plugins.PostgreSQL.Default.TLSConnect is set to *verify_ca* or *verify_full*)			Full pathname of a file containing the PostgreSQL certificate or certificate chain for encrypted communications between Zabbix agent 2 and monitored databases; used if no value is specified in a named session.
Plugins.PostgreSQL.Default.TLSConnect				Encryption type for communications between Zabbix agent 2 and monitored databases; used if no value is specified in a named session. Supported values: *required* - connect using TLS as transport mode without identity checks; *verify_ca* - connect using TLS and verify certificate; *verify_full* - connect using TLS, verify certificate and verify that database identity (CN) specified by DBHost matches its certificate. Undefined encryption type means unencrypted connection.
Plugins.PostgreSQL.Default.TLSKeyFile	(yes, if Plugins.PostgreSQL.Default.TLSConnect is set to *verify_ca* or *verify_full*)			Full pathname of a file containing the PostgreSQL private key for encrypted communications between Zabbix agent 2 and monitored databases; used if no value is specified in a named session.

Plugins.PostgreSQL.Default.Uri				Default URI for connecting to PostgreSQL; used if no value is specified in an item key or named session.
				
				Should not include embedded credentials (they will be ignored).
				Must match the URI format.
				Supported schemes: `tcp`, `unix`.
				Examples: `tcp://127.0.0.1:5432`
				`tcp://localhost`
				`unix:/var/run/postgresql/.s.PGSQL.5432`

Plugins.PostgreSQL.Default.User				Default username for connecting to PostgreSQL; used if no value is specified in an item key or named session.
Plugins.PostgreSQL.KeepAlive		60-900	300	Maximum time of waiting (in seconds) before unused plugin connections are closed.
Plugins.PostgreSQL.Sessions.<SessionName>.CachePreparedMode			prepare	Cache mode for the PostgreSQL connection. **<SessionName>** - define name of a session for using in item keys. Supported values: *prepare* (default) - will create prepared statements on the PostgreSQL server; *describe* - will use the anonymous prepared statement to describe a statement without creating a statement on the server. Note that "describe" is primarily useful when the environment does not allow prepared statements such as when running a connection pooler like PgBouncer.

Parameter	Mandatory	Range	Default	Description
Plugins.PostgreSQL.Sessions.<SessionName>.Database				Database for session connection. **<SessionName>** - define name of a session for using in item keys.
Plugins.PostgreSQL.Sessions.<SessionName>.Password		Must match the password format.		Password for session connection. **<SessionName>** - define name of a session for using in item keys.
Plugins.PostgreSQL.Sessions.<SessionName>.TLSCAFile	yes, if Plugins.PostgreSQL.Sessions.<SessionName>.TLSConnect is set to *verify_ca* or *verify_full*)			Full pathname of a file containing the top-level CA(s) certificate peer certificate verification. **<SessionName>** - define name of a session for using in item keys.
Plugins.PostgreSQL.Sessions.<SessionName>.TLSCertFile	yes, if Plugins.PostgreSQL.Sessions.<SessionName>.TLSKeyFile is specified			Full pathname of a file containing the PostgreSQL certificate or certificate chain. **<SessionName>** - define name of a session for using in item keys.
Plugins.PostgreSQL.Sessions.<SessionName>.TLSConnect				Encryption type for PostgreSQL connection. **<SessionName>** - define name of a session for using in item keys. Supported values: *required* - connect using TLS as transport mode without identity checks; *verify_ca* - connect using TLS and verify certificate; *verify_full* - connect using TLS, verify certificate and verify that database identity (CN) specified by DBHost matches its certificate. Undefined encryption type means unencrypted connection.
Plugins.PostgreSQL.Sessions.<SessionName>.TLSKeyFile	yes, if Plugins.PostgreSQL.Sessions.<SessionName>.TLSCertFile is specified			Full pathname of a file containing the PostgreSQL private key. **<SessionName>** - define name of a session for using in item keys.

Plugins.PostgreSQL.Sessions.<SessionName>.Uri				Connection string of a named session.
				<SessionName> - define name of a session for using in item keys.
				
				Should not include embedded credentials (they will be ignored).
				Must match the URI format.
				Supported schemes: `tcp`, `unix`.
				Examples: `tcp://127.0.0.1:5432`
				`tcp://localhost`
				`unix:/var/run/postgresql/.s.PGSQL.5432`

Plugins.PostgreSQL.Sessions.<SessionName>.User				Named session username. **<SessionName>** - define name of a session for using in item keys.
Plugins.PostgreSQL.System.Path	yes			Path to the PostgreSQL plugin executable. Example usage: `Plugins.PostgreSQL.System.Path=/usr/libexec/zabbix/zabbi`
Plugins.PostgreSQL.Timeout		1-30	global timeout	Request execution timeout (the duration, in seconds, to wait for a request to complete before shutting it down).

See also:

- Description of general Zabbix agent 2 configuration parameters: Zabbix agent 2 (UNIX) / Zabbix agent 2 (Windows)
- Instructions for configuring plugins

13 Redis plugin

Overview

The configuration file of Zabbix agent 2 is used to configure plugins. These Zabbix agent 2 configuration parameters are supported for operating the Redis plugin.

It is recommended to specify them in their own configuration file (e.g. `redis.conf`) and then use the Include directive for adding this file to the Zabbix agent 2 configuration.

Note that:

- The default values reflect process defaults, not the values in the shipped configuration files.
- Values support environment variables.
- Zabbix supports configuration files only in UTF-8 encoding without BOM.
- Comments starting with "#" are only supported at the beginning of the line.

Parameters

Parameter	Mandatory	Range	Default	Description
Plugins.Redis.Default.Password	no			Default password for connecting to Redis; used if no value is specified in an item key or named session.
Plugins.Redis.Default.TLSConnect	no			Client (Zabbix agent 2) TLS verification requirement. Supported values: `required` - encrypted, unverified (only for testing) `verify_ca` - encrypted, server certificate `verify_full` - encrypted, server certificate and server name verified with SAN An empty or unset value is treated as no tls.
Plugins.Redis.Default.TLSCAFile	no			Default full pathname of a file containing the top-level CA(s) certificates.
Plugins.Redis.Default.TLSCertFile	no			Default full pathname of a file containing the agent's certificate.
Plugins.Redis.Default.TLSKeyFile	no			Default full pathname of a file containing the agent's private key.

Plugins.Redis.Default.Uri	no		tcp://localhost:6379	Default URI for connecting to Redis; used if no value is specified in an item key or named session.
				
				Should not include embedded credentials (they will be ignored).
				Must match the URI format.
				Supported schemes: `tcp`, `unix`; a scheme can be omitted.
				A port can be omitted (default=6379).
				Examples: `tcp://localhost:6379`
				`localhost`
				`unix:/var/run/redis.sock`

Plugins.Redis.Default.User	no		default	Default user to send to the protected Redis server; used if no value is specified in an item key or named session.
Plugins.Redis.KeepAlive	no	60-900	300	The maximum time of waiting (in seconds) before unused plugin connections are closed.
Plugins.Redis.Sessions.<SessionName>.Password	no			Named session password. **<SessionName>** - define the session name to be used in item keys.
Plugins.Redis.Sessions.<SessionName>.TLSConnect	no			Client (Zabbix agent 2) TLS verification requirement. **<SessionName>** - define the session name to be used in item keys. Supported values: `required` - encrypted, unverified (only for testing) `verify_ca` - encrypted, server certificate `verify_full` - encrypted, server certificate and server name verified with SAN An empty or unset value is treated as no tls.

Parameter	Mandatory	Range	Default	Description
Plugins.Redis.Sessions.<SessionName>.TLSCAFile	no (yes, if TLSConnect is `verify_ca` or `verify_full`)			Full pathname of a file containing the top-level CA(s) certificates for Redis server certificate verification. **<SessionName>** - define the session name to be used in item keys.
Plugins.Redis.Sessions.<SessionName>.TLSCertFile	no			Full pathname of a file containing the agent's certificate for client authentication. **<SessionName>** - define the session name to be used in item keys.
Plugins.Redis.Sessions.<SessionName>.TLSKeyFile	no			Full pathname of a file containing the agent's private key for client authentication. **<SessionName>** - define the session name to be used in item keys.

Plugins.Redis.Sessions.<SessionName>.Uri	no		localhost:6379	Connection string of a named session.
				<SessionName> - define the session name to be used in item keys.
				
				Should not include embedded credentials (they will be ignored).
				Must match the URI format.
				Supported schemes: `tcp`, `unix`; a scheme can be omitted.
				A port can be omitted (default=6379).
				Examples: `tcp://localhost:6379`
				`localhost`
				`unix:/var/run/redis.sock`

Plugins.Redis.Sessions.<SessionName>.User	no		default	User to send to the protected Redis server. **<SessionName>** - define the session name to be used in item keys.
Plugins.Redis.Timeout	no	1-30	global timeout	Request execution timeout (the duration, in seconds, to wait for a request to complete before shutting it down).

See also:

- Description of general Zabbix agent 2 configuration parameters: Zabbix agent 2 (UNIX) / Zabbix agent 2 (Windows)
- Instructions for configuring plugins

14 SMART plugin

Overview

The configuration file of Zabbix agent 2 is used to configure plugins. These Zabbix agent 2 configuration parameters are supported for operating the SMART plugin.

It is recommended to specify them in their own configuration file (e.g. `smart.conf`) and then use the Include directive for adding this file to the Zabbix agent 2 configuration.

Note that:

- The default values reflect process defaults, not the values in the shipped configuration files;
- Values support environment variables;
- The path to the `smartctl` executable must be set either by adding its directory to the system's `PATH` environment variable or by configuring `Plugins.Smart.Path`; this applies to both Linux and Windows;
- Zabbix supports configuration files only in UTF-8 encoding without BOM;
- Comments starting with "#" are only supported at the beginning of the line.

Parameters

Parameter	Mandatory	Range	Default	Description
Plugins.Smart.Path	no		smartctl	Path to the smartctl executable.

Parameter	Mandatory	Range	Default	Description
Plugins.Smart.Timeout	no	1-30	global timeout	Request execution timeout (the duration, in seconds, to wait for a request to complete before shutting it down).

See also:

- Description of general Zabbix agent 2 configuration parameters: Zabbix agent 2 (UNIX) / Zabbix agent 2 (Windows)
- Instructions for configuring plugins

8 Zabbix Java gateway

Jeśli do uruchamiania Zabbix Java gateway używasz skryptów `startup.sh` i `shutdown.sh`, możesz określić wymagane parametry konfiguracji w pliku `settings.sh`. Skrypty uruchamiania i zatrzymywania wczytują plik ustawień i odpowiadają za konwersję zmiennych powłoki (wymienionych w pierwszej kolumnie) na właściwości Java (wymienione w drugiej kolumnie).

Jeśli uruchamiasz Zabbix Java gateway ręcznie, wykonując bezpośrednio polecenie `java`, wówczas odpowiednie właściwości Java określasz w wierszu poleceń.

Variable	Property	Mandatory	Range	Default	Description
LISTEN_IP	zabbix.listenIP	no		0.0.0.0	Adres IP, na którym nasłuchuje usługa.
LISTEN_PORT	zabbix.listenPort	no	1024-32767	10052	Port, na którym usługa nasłuchuje.
PID_FILE	zabbix.pidFile	no		/tmp/zabbix_java.pid	Nazwa pliku PID. Jeśli zostanie pominięty, Zabbix Java Gateway zostanie uruchomiony jako aplikacja konsolowa.
PROPERTIES_FILE	zabbix.propertiesFile	no			Nazwa pliku właściwości. Może być używany do ustawiania dodatkowych właściwości w formacie klucz-wartość, tak aby nie były widoczne w wierszu poleceń, lub do nadpisywania istniejących. Na przykład: ”javax.net.ssl.trustStorePassword=<p
START_POLLERS	zabbix.startPollers	no	1-1000	5	Liczba wątków roboczych do uruchomienia.
TIMEOUT	zabbix.timeout	no	1-30	3	Jak długo czekać na operacje sieciowe (w sekundach).

Warning:
Port 10052 nie jest zarejestrowany przez IANA registered.

9 Usługa internetowa Zabbix

Przegląd

Usługa internetowa Zabbix to proces używany do komunikacji z zewnętrznymi usługami internetowymi.

Parametry obsługiwane przez plik konfiguracyjny usługi internetowej Zabbix (zabbix_web_service.conf) są wymienione w tej sekcji.

Parametry są podane bez dodatkowych informacji. Kliknij parametr, aby zobaczyć pełne szczegóły.

Parameter	Description
AllowedIP	Lista adresów IP rozdzielonych przecinkami, opcjonalnie w notacji CIDR, lub nazw DNS serwerów Zabbix i proxy Zabbix.
DebugLevel	Poziom debugowania.
IgnoreURLCertErrors	Określa obsługę błędów walidacji certyfikatu TLS podczas uzyskiwania dostępu do adresu URL frontend.
Include	Możesz dołączyć pojedyncze pliki lub wszystkie pliki z katalogu do pliku konfiguracyjnego.
ListenPort	Usługa będzie nasłuchiwać na tym porcie połączeń z serwera.
LogFile	Nazwa pliku dziennika.
LogFileSize	Maksymalny rozmiar pliku dziennika.
LogType	Typ wyjścia dziennika.
Timeout	Maksymalny czas (w sekundach) poświęcony na formatowanie raportu PDF pulpitu.
TLSAccept	Jakie połączenia przychodzące mają być akceptowane.
TLSCAFile	Pełna ścieżka do pliku zawierającego certyfikaty nadrzędnych urzędów certyfikacji (CA) do weryfikacji certyfikatu peera, używana do szyfrowanej komunikacji między komponentami Zabbix.
TLSCertFile	Pełna ścieżka do pliku zawierającego certyfikat usługi lub łańcuch certyfikatów, używana do szyfrowanej komunikacji między komponentami Zabbix.
TLSKeyFile	Pełna ścieżka do pliku zawierającego klucz prywatny usługi, używana do szyfrowanej komunikacji między komponentami Zabbix.

Wszystkie parametry są opcjonalne, chyba że wyraźnie zaznaczono, że dany parametr jest obowiązkowy.

Zwróć uwagę, że:

- Wartości domyślne odzwierciedlają wartości domyślne procesu, a nie wartości w dostarczanych plikach konfiguracyjnych;
- Wartości obsługują zmienne środowiskowe;
- Zabbix obsługuje pliki konfiguracyjne tylko w kodowaniu UTF-8 bez BOM;
- Komentarze rozpoczynające się od ”#” są obsługiwane tylko na początku wiersza.

Szczegóły parametrów

AllowedIP

Lista adresów IP oddzielonych przecinkami, opcjonalnie w notacji CIDR, lub nazw DNS serwerów Zabbix i proxy Zabbix. Połączenia przychodzące będą akceptowane tylko od hostów wymienionych tutaj.
Jeśli obsługa IPv6 jest włączona, wtedy `127.0.0.1`, `::127.0.0.1`, `::ffff:127.0.0.1` są traktowane jednakowo, a `::/0` pozwoli na dowolny adres IPv4 lub IPv6. `0.0.0.0/0` może być użyte do zezwolenia na dowolny adres IPv4.

Przykład:

`127.0.0.1,192.168.1.0/24,::1,2001:db8::/32,zabbix.example.com`

Wymagane: tak

DebugLevel

Określ poziom debugowania:
0 - podstawowe informacje o uruchamianiu i zatrzymywaniu procesów Zabbix
1 - informacje krytyczne;
2 - informacje o błędach;
3 - ostrzeżenia;
4 - do debugowania (generuje dużo informacji);
5 - rozszerzone debugowanie (generuje jeszcze więcej informacji).

Domyślnie: 3
 Zakres: 0-5

IgnoreURLCertErrors

Określa obsługę błędów walidacji certyfikatu TLS podczas uzyskiwania dostępu do adresu URL frontendu:
0 - nie ignoruj błędów certyfikatu;
1 - ignoruj błędy certyfikatu.

Wartość domyślna: 0
 Zakres: 0-1

Include

Możesz dołączyć pojedyncze pliki lub wszystkie pliki w katalogu w pliku konfiguracyjnym. Podczas instalacji Zabbix utworzy katalog include w /usr/local/etc, chyba że zostanie to zmienione podczas kompilacji. Ścieżka może być względna względem lokalizacji pliku *zabbix_web_service.conf*.
Aby dołączyć tylko odpowiednie pliki w określonym katalogu, obsługiwany jest znak wieloznaczny gwiazdki do dopasowywania wzorców.
Zobacz uwagi specjalne dotyczące ograniczeń.

Przykład:

```
Include=/absolute/path/to/config/files/*.conf
```

ListenPort

Usługa będzie nasłuchiwać na tym porcie połączeń z serwera.

Domyślnie: 10053
 Zakres: 1024-32767

LogFile

Nazwa pliku dziennika.

Przykład:

`/tmp/zabbix_web_service.log`

Wymagane: Tak, jeśli LogType jest ustawione na *file*; w przeciwnym razie nie

LogFileSize

Maksymalny rozmiar pliku dziennika w MB.
0 - wyłącza automatyczną rotację logów.
Uwaga: Jeśli zostanie osiągnięty limit rozmiaru pliku dziennika, a rotacja pliku nie powiedzie się z jakiegokolwiek powodu, istniejący plik dziennika zostanie obcięty i rozpoczęty na nowo.

Wartość domyślna: 1
 Zakres: 0-1024

LogType

Typ wyjścia logu:
file - zapisuj log do pliku określonego przez parametr LogFile;
system - zapisuj log do syslog;
console - zapisuj log na standardowe wyjście.

Domyślnie: `file`

Timeout

Maksymalny czas (w sekundach) poświęcony na formatowanie raportu PDF pulpitu.

Domyślnie: 10
 Zakres: 1-30

TLSAccept

Jakie połączenia przychodzące akceptować:
unencrypted - akceptuj połączenia bez szyfrowania (domyślnie)
cert - akceptuj połączenia z TLS i certyfikatem

Wartość domyślna: `unencrypted`

TLSCAFile

Pełna ścieżka do pliku zawierającego certyfikaty nadrzędnych urzędów certyfikacji (CA) do weryfikacji certyfikatu strony komunikacji, używanego do szyfrowanej komunikacji między komponentami Zabbix.

TLSCertFile

Pełna ścieżka do pliku zawierającego certyfikat usługi lub łańcuch certyfikatów, używanego do szyfrowanej komunikacji z komponentami Zabbix.

TLSKeyFile

Pełna ścieżka do pliku zawierającego prywatny klucz usługi, używany do szyfrowanej komunikacji między komponentami Zabbix.

10 Zmienne środowiskowe

Przegląd

Zmienne środowiskowe umożliwiają konfigurowanie komponentów Zabbix bez wpisywania na stałe wartości w plikach konfiguracyjnych. Ułatwia to zarządzanie konfiguracją w dynamicznych środowiskach, takich jak Docker, gdzie zmienne mogą być przekazywane w czasie uruchamiania, aby dostosować ustawienia do różnych konfiguracji.

W najprostszym przypadku, ustawiając wartość parametru konfiguracyjnego DebugLevel serwera Zabbix na zmienną środowiskową, można następnie użyć jej do skonfigurowania serwera podczas uruchamiania:

```
#### Plik konfiguracyjny serwera Zabbix:
DebugLevel=${NEW_DEBUG_LEVEL}

#### Uruchamianie serwera Zabbix:
NEW_DEBUG_LEVEL=5 /usr/sbin/zabbix_server
```

Zmienne środowiskowe są obsługiwane przez następujące komponenty Zabbix:

- Serwer
- Proxy
- Agent (UNIX lub Windows)
- Agent 2 (UNIX lub Windows), w tym wtyczki
- Usługa web
- Zabbix sender (przy użyciu opcji -c, --config)

Ważne uwagi

- Gdy parametr konfiguracyjny jest ustawiony na zmienną środowiskową, która nie została określona podczas uruchamiania komponentu, użyta zostanie wartość domyślna parametru.
- W przypadku używania poleceń runtime (np. w celu zwiększenia poziomu logowania agent), należy określić wszystkie wcześniej używane zmienne środowiskowe. Wynika to z faktu, że komponenty Zabbix używają swojego pliku konfiguracyjnego do wykonywania poleceń runtime; jeśli zmienne środowiskowe zostaną pominięte, użyte zostaną domyślne wartości parametrów konfiguracyjnych. Zobacz Przykłady.
- Polecenie `userparameter_reload` runtime nie obsługuje ponownego wczytywania zmiennych środowiskowych. Podczas przeładowania zmienne są ignorowane i ponownie wczytywane są tylko parametry ze zwykłymi wartościami.
- Bieżące zmienne środowiskowe procesu, które były używane w plikach konfiguracyjnych, są czyszczone po uruchomieniu komponentu Zabbix. Zapewnia to, że procesy potomne (np. zdalne skrypty wykonywane przez Zabbix) nie mogą uzyskać dostępu do tych zmiennych. Należy jednak pamiętać, że początkowe zmienne procesu nadal mogą zostać odczytane (np. za pośrednictwem pliku `/proc/<PID>/environ`).

Składnia

Zmienne środowiskowe muszą używać następującej składni: `${alphanumerics/underscores}`.

Nazwa zmiennej może zawierać wyłącznie litery (a-z, A-Z), podkreślenia (_), oraz cyfry (0-9) i nie może zaczynać się od cyfry.

Zmienne, które nie są zgodne z wymaganą składnią lub są połączone ze zwykłą wartością, będą traktowane jako zwykłe wartości, co może powodować błędy.

Poprawna składnia zmiennych:

```
DebugLevel=${NEW_DEBUG_LEVEL}
Hostname=${ZBX_HOSTNAME}
LogFile=${LogFile_001}
```

Niepoprawna składnia zmiennych:

```
DebugLevel=${5_DebugLevel}
Hostname=${ZBX.HOSTNAME 1}
LogFile=/${HOME}/zabbix/zabbix_server.log
```

Note:
W systemie Windows nazwy zmiennych środowiskowych nie rozróżniają wielkości liter.

Przykłady

Poniższe przykłady pokazują, jak skonfigurować i używać zmiennych środowiskowych z komponentami Zabbix.

Przykład 1: Konfigurowanie i testowanie agenta Zabbix

1. Ustaw zmienne środowiskowe w pliku konfiguracyjnym agenta:

```
Hostname=${ZBX_HOSTNAME}
ServerActive=${ServerActive}
```

2. Przetestuj plik konfiguracyjny:

```
ZBX_HOSTNAME="New Zabbix agent" ServerActive=127.0.0.1 /usr/sbin/zabbix_agentd -c /etc/zabbix/zabbix_agent
```

3. Uruchom agenta ze zmiennymi środowiskowymi:

```
ZBX_HOSTNAME="New Zabbix agent" ServerActive=127.0.0.1 /usr/sbin/zabbix_agentd -c /etc/zabbix/zabbix_agent
```

Podczas używania poleceń runtime (na przykład w celu zwiększenia poziomu logowania agenta) należy podać wszystkie wcześniej użyte zmienne środowiskowe:

```
ZBX_HOSTNAME="New Zabbix agent" ServerActive=127.0.0.1 /usr/sbin/zabbix_agentd -c /etc/zabbix/zabbix_agent
```

Wynika to z tego, że agent używa swojego pliku konfiguracyjnego do wykonywania poleceń runtime; jeśli zmienne środowiskowe zostaną pominięte, zostaną użyte domyślne wartości parametrów konfiguracyjnych.

Alternatywnie, po ustawieniu zmiennych środowiskowych w pliku konfiguracyjnym agenta, możesz udostępnić je procesom (na przykład za pomocą polecenia `export`). Zmniejsza to ryzyko nieoczekiwanego zachowania spowodowanego brakiem zmiennych lub ich nieprawidłowym ustawieniem.

```
export ZBX_HOSTNAME="New Zabbix agent"
export ServerActive=127.0.0.1
/usr/sbin/zabbix_agentd -c /etc/zabbix/zabbix_agentd.conf --test-config
/usr/sbin/zabbix_agentd -c /etc/zabbix/zabbix_agentd.conf
/usr/sbin/zabbix_agentd -c /etc/zabbix/zabbix_agentd.conf -R log_level_increase
```

Przykład 2: Konfigurowanie agenta Zabbix dla kontenera

Jeśli tworzysz i konfigurujesz własny niestandardowy obraz dla komponentów Zabbix (np. agenta Zabbix), możesz zdefiniować parametry konfiguracyjne za pomocą zmiennych środowiskowych, a następnie uruchomić kontener z tymi zmiennymi.

1. Podczas przygotowywania obrazu ustaw zmienne środowiskowe w pliku konfiguracyjnym agenta:

```
Hostname=${ZBX_HOSTNAME}
BufferSize=${BUFSZ}
ListenPort=${LISTENPORT}
UserParameter=${_UsrPar01}
UserParameter=${_UsrPar02}
```

2. Po zbudowaniu obrazu kontenera uruchom kontener agenta (np. Docker) ze zmiennymi środowiskowymi:

```
docker run --name my-zabbix-agent -e ZBX_HOSTNAME="new-hostname" -e BUFSZ=1000 -e LISTENPORT=20050 -e _Usr
```

3. Podczas używania poleceń runtime (np. w celu zwiększenia poziomu logowania agenta) uzyskaj dostęp do powłoki kontenera i wykonaj polecenie runtime:

```
docker exec -it <containerid> sh
/usr/sbin/zabbix_agentd -R log_level_increase
```

> **Attention:**
> Polecenie runtime `userparameter_reload` nie obsługuje ponownego wczytywania zmiennych środowiskowych. Podczas ponownego wczytywania zmienne są ignorowane, a ponownie wczytywane są tylko parametry ze zwykłymi wartościami.

11 Dołączanie

Przegląd

Dodatkowe pliki lub katalogi mogą być dołączane do konfiguracji serwera, proxy, agenta i usługi web service przy użyciu parametru `Include`.

Uwagi dotyczące dołączania

Jeśli parametr `Include` jest używany do dołączania pliku, plik musi być dostępny do odczytu.

Jeśli parametr `Include` jest używany do dołączania katalogu:

- Wszystkie pliki w katalogu muszą być dostępne do odczytu.
- Nie należy zakładać żadnej konkretnej kolejności dołączania (np. pliki nie są dołączane w kolejności alfabetycznej). Dlatego nie należy definiować jednego parametru w kilku plikach "Include" (np. aby nadpisać ustawienie ogólne ustawieniem szczegółowym).
- Wszystkie pliki w katalogu są dołączane do konfiguracji.
- Należy uważać na kopie zapasowe plików tworzone automatycznie przez niektóre edytory tekstu. Na przykład, jeśli edycja pliku "include/my_specific.conf" powoduje utworzenie kopii zapasowej "include/my_specific_conf.BAK", wówczas oba pliki zostaną dołączone. Przenieś "include/my_specific.conf.BAK" poza katalog "Include". W systemie Linux zawartość katalogu "Include" można sprawdzić poleceniem "ls -al", aby wykryć zbędne pliki.

Jeśli parametr `Include` jest używany do dołączania plików przy użyciu wzorca:

- Wszystkie pliki pasujące do wzorca muszą być dostępne do odczytu.
- Nie należy zakładać żadnej konkretnej kolejności dołączania (np. pliki nie są dołączane w kolejności alfabetycznej). Dlatego nie należy definiować jednego parametru w kilku plikach "Include" (np. aby nadpisać ustawienie ogólne ustawieniem szczegółowym).

3 Protokoły

Użyj paska bocznego, aby uzyskać dostęp do treści w tej sekcji.

1 Protokół wymiany danych serwer-proxy

Przegląd

Wymiana danych serwer - proxy opiera się na formacie JSON.

Komunikaty żądania i odpowiedzi muszą zaczynać się od nagłówka i długości danych.

Pasywny proxy

Żądanie konfiguracji

Serwer najpierw wyśle puste żądanie `proxy config`. To żądanie jest wysyłane co `ProxyConfigFrequency` (parametr konfiguracji serwera) sekund.

Proxy odpowiada bieżącą wersją proxy, tokenem sesji i rewizją konfiguracji. Serwer odpowiada danymi konfiguracyjnymi, które wymagają aktualizacji.

name	value type	description
server→proxy:		
request	*string*	'proxy config'
proxy→server:		
version	*string*	Wersja proxy (<major>.<minor>.<build>).
session	*string*	Token sesji konfiguracji proxy.
config_revision	*number*	Rewizja konfiguracji proxy.
server→proxy:		
full_sync	*number*	1 - jeśli wysyłane są pełne dane konfiguracyjne; w przeciwnym razie brak (opcjonalne).
data	*array*	Obiekt danych tabeli. Brak, jeśli konfiguracja nie została zmieniona (opcjonalne).
<table>	*object*	Jeden lub więcej obiektów z danymi <table> (opcjonalne, zależnie od zmian).
fields	*array*	Tablica nazw pól.
-	*string*	Nazwa pola.
data	*array*	Tablica wierszy.
-	*array*	Tablica kolumn.
-	*string*,*number*	Wartość kolumny, której typ zależy od typu kolumny w schemacie bazy danych.
macro.secrets	*object*	Informacje o tajnych makrach; brak, jeśli nie ma zmian w makrach vault (opcjonalne).
config_revision	*number*	Rewizja pamięci podręcznej konfiguracji - wysyłana wraz z danymi konfiguracyjnymi (opcjonalne).
del_hostids	*array*	Tablica usuniętych hostid (opcjonalne).
-	*number*	Identyfikator hosta.
del_macro_hostids	*array*	Tablica hostid, dla których usunięto wszystkie makra (opcjonalne).
-	*number*	Identyfikator hosta.
proxy→server:		
response	*string*	Informacja o powodzeniu żądania ('success' lub 'failed').
version	*string*	Wersja proxy (<major>.<minor>.<build>).

Przykład:

server→proxy:

```
{
  "request":"proxy config"
}
```

proxy→server:

```
{
  "version": "8.0.0",
  "session": "0033124949800811e5686dbfd9bcea98",
  "config_revision": 0
}
```

server→proxy:

```
{
"full_sync": 1,
"data": {
"hosts": {
"fields": ["hostid", "host", "status", "ipmi_authtype", "ipmi_privilege", "ipmi_username", "ipmi_password"
"data": [
[10084, "Zabbix server", 0, -1, 2, "", "", "Zabbix server", 1, 1, "", "", "", ""]
]
},
"interface": {
"fields": ["interfaceid", "hostid", "main", "type", "useip", "ip", "dns", "port", "available"],
"data": [
[1, 10084, 1, 1, 1, "127.0.0.1", "", "10053", 1]
]
},
"interface_snmp": {
"fields": ["interfaceid", "version", "bulk", "community", "securityname", "securitylevel", "authpassphrase
"data": []
},
"host_inventory": {
"fields": ["hostid", "type", "type_full", "name", "alias", "os", "os_full", "os_short", "serialno_a", "ser
"data": [
[10084, "", "", "", "", "", "", "", "", "", "", "", "", "", "", "", "", "", "", "", "", "", "", "", "", "5
]
},
"items": {
"fields": ["itemid", "type", "snmp_oid", "hostid", "key_", "delay", "history", "status", "value_type", "tr
"data": [
[44161, 7, "", 10084, "agent.hostmetadata", "10s", "90d", 0, 1, "", "", "", "", 0, "", "", "", "", 0, null
[44162, 0, "", 10084, "agent.ping", "10s", "90d", 0, 3, "", "", "", "", 0, "", "", "", "", 0, 1, 0, "", nu
]
},
"item_rtdata": {
"fields": ["itemid", "lastlogsize", "mtime"],
"data": [
[44161, 0, 0],
[44162, 0, 0]
]
},
"item_preproc": {
"fields": ["item_preprocid", "itemid", "step", "type", "params", "error_handler", "error_handler_params"],
"data": []
},
"item_parameter": {
"fields": ["item_parameterid", "itemid", "name", "value"],
"data": []
},
"globalmacro": {
"fields": ["globalmacroid", "macro", "value", "type"],
"data": [
```

```
[2, "{$SNMP_COMMUNITY}", "public", 0]
]
},
"hosts_templates": {
"fields": ["hosttemplateid", "hostid", "templateid", "link_type"],
"data": []
},
"hostmacro": {
"fields": ["hostmacroid", "hostid", "macro", "value", "type", "automatic"],
"data": [
[5676, 10084, "{$M}", "AppID=zabbix_server&Query=Safe=passwordSafe;Object=zabbix:Content", 2, 0]
]
},
"drules": {
"fields": ["druleid", "name", "iprange", "delay"],
"data": [
[2, "Local network", "127.0.0.1", "10s"]
]
},
"dchecks": {
"fields": ["dcheckid", "druleid", "type", "key_", "snmp_community", "ports", "snmpv3_securityname", "snmpv
"data": [
[2, 2, 9, "system.uname", "", "10052", "", 0, "", "", 0, 0, 0, "", 1, 0]
]
},
"regexps": {
"fields": ["regexpid", "name"],
"data": [
[1, "File systems for discovery"],
[2, "Network interfaces for discovery"],
[3, "Storage devices for SNMP discovery"],
[4, "Windows service names for discovery"],
[5, "Windows service startup states for discovery"]
]
},
"expressions": {
"fields": ["expressionid", "regexpid", "expression", "expression_type", "exp_delimiter", "case_sensitive"]
"data": [
[1, 1, "^(btrfs|ext2|ext3|ext4|reiser|xfs|ffs|ufs|jfs|jfs2|vxfs|hfs|apfs|refs|ntfs|fat32|zfs)$", 3, ",", 0
[3, 3, "^(Physical memory|Virtual memory|Memory buffers|Cached memory|Swap space)$", 4, ",", 1],
[5, 4, "^(MMCSS|gupdate|SysmonLog|clr_optimization_v2.0.50727_32|clr_optimization_v4.0.30319_32)$", 4, ","
[6, 5, "^(automatic|automatic delayed)$", 3, ",", 1],
[7, 2, "^Software Loopback Interface", 4, ",", 1],
[8, 2, "^(In)?[Ll]oop[Bb]ack[0-9._]*$", 4, ",", 1],
[9, 2, "^NULL[0-9.]*$", 4, ",", 1],
[10, 2, "^[Ll]o[0-9.]*$", 4, ",", 1],
[11, 2, "^[Ss]ystem$", 4, ",", 1],
[12, 2, "^Nu[0-9.]*$", 4, ",", 1]
]
},
"settings": {
"fields": ["name", "type", "value_str", "value_int"],
"data": [
["autoreg_tls_accept", 2, "", 1],
["hk_history_global", 2, "", 0],
["snmptrap_logging", 2, "", 1],
["proxy_secrets_provider", 2, "", 0],
["hk_history", 1, "31d", 0],
["timeout_db_monitor", 1, "3s", 0],
["timeout_external_check", 1, "3s", 0],
["timeout_http_agent", 1, "3s", 0],
["timeout_simple_check", 1, "3s", 0],
```

```
["timeout_snmp_agent", 1, "3s", 0],
["timeout_ssh_agent", 1, "3s", 0],
["timeout_telnet_agent", 1, "3s", 0],
["timeout_zabbix_agent", 1, "3s", 0],
["timeout_browser", 1, "30s", 0]
]
},
"httptest": {
"fields": ["httptestid", "name", "delay", "agent", "authentication", "http_user", "http_password", "hostid
"data": []
},
"httptestitem": {
"fields": ["httptestitemid", "httptestid", "itemid", "type"],
"data": []
},
"httptest_field": {
"fields": ["httptest_fieldid", "httptestid", "type", "name", "value"],
"data": []
},
"httpstep": {
"fields": ["httpstepid", "httptestid", "name", "no", "url", "timeout", "posts", "required", "status_codes"
"data": []
},
"httpstepitem": {
"fields": ["httpstepitemid", "httpstepid", "itemid", "type"],
"data": []
},
"httpstep_field": {
"fields": ["httpstep_fieldid", "httpstepid", "type", "name", "value"],
"data": []
},
"config_autoreg_tls": {
"fields": ["autoreg_tlsid", "tls_psk_identity", "tls_psk"],
"data": [
[1, "", ""]
]
}
},
"macro.secrets": {
"AppID=zabbix_server&Query=Safe=passwordSafe;Object=zabbix": {
"Content": "738"
}
},
"config_revision": 2
}
```


proxy→server:


```
{
  "response": "success",
  "version": "8.0.0"
}
```


Żądanie danych

Żądanie `proxy data` służy do pobierania z proxy danych o dostępności interfejsów hosta, danych historycznych, danych wykrywania i danych autorejestracji. To żądanie jest wysyłane co `ProxyDataFrequency` (parametr konfiguracji serwera) sekund.

name	value type	description
server→proxy:		
request	*string*	'proxy data'
proxy→server:		
session	*string*	Token sesji danych.

name	value type	description
interface availability	*array*	*(opcjonalnie)* Tablica obiektów danych dostępności interfejsów.
interfaceid	*number*	Identyfikator interfejsu.
available	*number*	Dostępność interfejsu: **0**, *INTERFACE_AVAILABLE_UNKNOWN* - nieznana **1**, *INTERFACE_AVAILABLE_TRUE* - dostępny **2**, *INTERFACE_AVAILABLE_FALSE* - niedostępny
error	*string*	Komunikat błędu interfejsu lub pusty ciąg.
history data	*array*	*(opcjonalnie)* Tablica obiektów danych historycznych.
itemid	*number*	Identyfikator pozycji.
clock	*number*	Znacznik czasu wartości pozycji (sekundy).
ns	*number*	Znacznik czasu wartości pozycji (nanosekundy).
value	*string*	*(opcjonalnie)* Wartość pozycji.
id	*number*	Identyfikator wartości (licznik rosnący, unikalny w obrębie jednej sesji danych).
timestamp	*number*	*(opcjonalnie)* Znacznik czasu pozycji typu log.
source	*string*	*(opcjonalnie)* Wartość źródła pozycji eventlog.
severity	*number*	*(opcjonalnie)* Wartość ważności pozycji eventlog.
eventid	*number*	*(opcjonalnie)* Wartość eventid pozycji eventlog.
state	*string*	*(opcjonalnie)* Stan pozycji: **0**, *ITEM_STATE_NORMAL* **1**, *ITEM_STATE_NOTSUPPORTED*
lastlogsize	*number*	*(opcjonalnie)* Ostatni rozmiar logu dla pozycji typu log.
mtime	*number*	*(opcjonalnie)* Czas modyfikacji dla pozycji typu log.
discovery data	*array*	*(opcjonalnie)* Tablica obiektów danych wykrywania.
clock	*number*	Znacznik czasu danych wykrywania.
druleid	*number*	Identyfikator reguły wykrywania.
dcheckid	*number*	Identyfikator kontroli wykrywania lub null dla danych reguły wykrywania.
type	*number*	Typ kontroli wykrywania: **-1** dane reguły wykrywania **0**, *SVC_SSH* - kontrola usługi SSH **1**, *SVC_LDAP* - kontrola usługi LDAP **2**, *SVC_SMTP* - kontrola usługi SMTP **3**, *SVC_FTP* - kontrola usługi FTP **4**, *SVC_HTTP* - kontrola usługi HTTP **5**, *SVC_POP* - kontrola usługi POP **6**, *SVC_NNTP* - kontrola usługi NNTP **7**, *SVC_IMAP* - kontrola usługi IMAP **8**, *SVC_TCP* - kontrola dostępności portu TCP **9**, *SVC_AGENT* - agent Zabbix **10**, *SVC_SNMPv1* - agent SNMPv1 **11**, *SVC_SNMPv2* - agent SNMPv2 **12**, *SVC_ICMPPING* - ping ICMP **13**, *SVC_SNMPv3* - agent SNMPv3 **14**, *SVC_HTTPS* - kontrola usługi HTTPS **15**, *SVC_TELNET* - kontrola dostępności Telnet
ip	*string*	Adres IP hosta.
dns	*string*	Nazwa DNS hosta.
port	*number*	*(opcjonalnie)* Numer portu usługi.
key_	*string*	*(opcjonalnie)* Klucz pozycji dla kontroli wykrywania typu **9** *SVC_AGENT*
value	*string*	*(opcjonalnie)* Wartość odebrana z usługi; dla większości usług może być pusta.
status	*number*	*(opcjonalnie)* Stan usługi: **0**, *DOBJECT_STATUS_UP* - usługa działa **1**, *DOBJECT_STATUS_DOWN* - usługa nie działa

name	value type	description
auto reg- is- tra- tion	*array*	*(opcjonalnie)* Tablica obiektów danych autorejestracji.
clock	*number*	Znacznik czasu danych autorejestracji.
host	*string*	Nazwa hosta.
ip	*string*	*(opcjonalnie)* Adres IP hosta.
dns	*string*	*(opcjonalnie)* Rozwiązana nazwa DNS z adresu IP.
port	*string*	*(opcjonalnie)* Port hosta.
host_metadata	*string*	*(opcjonalnie)* Metadane hosta wysłane przez agent na podstawie parametru konfiguracji agent HostMetadata lub HostMetadataItem.
tasks	*array*	*(opcjonalnie)* Tablica zadań.
type	*number*	Typ zadania: **0**, *ZBX_TM_TASK_PROCESS_REMOTE_COMMAND_RESULT* - wynik zdalnego polecenia
status	*number*	Stan wykonania zdalnego polecenia: **0**, *ZBX_TM_REMOTE_COMMAND_COMPLETED* - zdalne polecenie zakończone pomyślnie **1**, *ZBX_TM_REMOTE_COMMAND_FAILED* - wykonanie zdalnego polecenia nie powiodło się
error	*string*	*(opcjonalnie)* Komunikat błędu.
parent_taskid	*number*	ID zadania nadrzędnego.
more	*number*	*(opcjonalnie)* 1 - jest więcej danych historycznych do wysłania.
clock	*number*	*(opcjonalnie)* Znacznik czasu transferu danych (sekundy).
ns	*number*	*(opcjonalnie)* Znacznik czasu transferu danych (nanosekundy).
version	*string*	Wersja proxy (<major>.<minor>.<build>).
server→proxy:		
response	*string*	Informacja o powodzeniu żądania (’success’ lub ’failed’).
tasks	*array*	*(opcjonalnie)* Tablica zadań.
type	*number*	Typ zadania: **1**, *ZBX_TM_TASK_PROCESS_REMOTE_COMMAND* - zdalne polecenie
clock	*number*	Czas utworzenia zadania.
ttl	*number*	Czas w sekundach, po którym zadanie wygasa.
commandtype	*number*	Typ zdalnego polecenia: **0**, *ZBX_SCRIPT_TYPE_CUSTOM_SCRIPT* - użyj niestandardowego skryptu **1**, *ZBX_SCRIPT_TYPE_IPMI* - użyj IPMI **2**, *ZBX_SCRIPT_TYPE_SSH* - użyj SSH **3**, *ZBX_SCRIPT_TYPE_TELNET* - użyj Telnet **4**, *ZBX_SCRIPT_TYPE_GLOBAL_SCRIPT* - użyj skryptu globalnego (obecnie funkcjonalnie równoważnego skryptowi niestandardowemu)
command	*string*	Zdalne polecenie do wykonania.
execute_on	*number*	Cel wykonania dla skryptów niestandardowych: **0**, *ZBX_SCRIPT_EXECUTE_ON_AGENT* - wykonaj skrypt na agent **1**, *ZBX_SCRIPT_EXECUTE_ON_SERVER* - wykonaj skrypt na serwerze **2**, *ZBX_SCRIPT_EXECUTE_ON_PROXY* - wykonaj skrypt na proxy
port	*number*	*(opcjonalnie)* Port dla poleceń Telnet i SSH.
authtype	*number*	*(opcjonalnie)* Typ uwierzytelniania dla poleceń SSH.
username	*string*	*(opcjonalnie)* Nazwa użytkownika dla poleceń Telnet i SSH.
password	*string*	*(opcjonalnie)* Hasło dla poleceń Telnet i SSH.
publickey	*string*	*(opcjonalnie)* Klucz publiczny dla poleceń SSH.
privatekey	*string*	*(opcjonalnie)* Klucz prywatny dla poleceń SSH.
parent_taskid	*number*	ID zadania nadrzędnego.
hostid	*number*	ID docelowego hosta.

Przykład:

server→proxy:

```
{
  "request": "proxy data"
}
```

proxy→server:

```
{
    "session": "12345678901234567890123456789012"
    "interface availability": [
        {
            "interfaceid": 1,
            "available": 1,
            "error": ""
    },
        {
            "interfaceid": 2,
            "available": 2,
            "error": "Get value from agent failed: cannot connect to [[127.0.0.1]:10049]: [111] Connection
    },
        {
            "interfaceid": 3,
            "available": 1,
            "error": ""
    },
        {
            "interfaceid": 4,
            "available": 1,
            "error": ""
    }
    ],
    "history data":[
        {
            "itemid":"12345",
            "clock":1478609647,
            "ns":332510044,
            "value":"52956612",
            "id": 1
        },
        {
            "itemid":"12346",
            "clock":1478609647,
            "ns":330690279,
            "state":1,
            "value":"Cannot find information for this network interface in /proc/net/dev.",
            "id": 2
        }
    ],
    "discovery data":[
        {
            "clock":1478608764,
            "drule":2,
            "dcheck":3,
            "type":12,
            "ip":"10.3.0.10",
            "dns":"vdebian",
            "status":1
        },
        {
            "clock":1478608764,
            "drule":2,
            "dcheck":null,
            "type":-1,
```

```
            "ip":"10.3.0.10",
            "dns":"vdebian",
            "status":1
        }
    ],
    "auto registration":[
        {
            "clock":1478608371,
            "host":"Logger1",
            "ip":"10.3.0.1",
            "dns":"localhost",
            "port":"10050"
        },
        {
            "clock":1478608381,
            "host":"Logger2",
            "ip":"10.3.0.2",
            "dns":"localhost",
            "port":"10050"
        }
    ],
    "tasks":[
        {
            "type": 0,
            "status": 0,
            "parent_taskid": 10
        },
        {
            "type": 0,
            "status": 1,
            "error": "No permissions to execute task.",
            "parent_taskid": 20
        }
    ],
    "version":"8.0.0"
}
```


server→proxy:


```
{
  "response": "success",
  "tasks":[
      {
         "type": 1,
         "clock": 1478608371,
         "ttl": 600,
         "commandtype": 2,
         "command": "restart_service1.sh",
         "execute_on": 2,
         "port": 80,
         "authtype": 0,
         "username": "userA",
         "password": "password1",
         "publickey": "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCqGKukO1De7zhZj6+H0qtjTkVxwTCpvKe",
         "privatekey": "lsuusFncCzWBQ7RKNUSesmQRMSGkVb1/3j+skZ6UtW+5u09lHNsj6tQ5QCqGKukO1De7zhd",
         "parent_taskid": 10,
         "hostid": 10070
      },
      {
         "type": 1,
         "clock": 1478608381,
         "ttl": 600,
         "commandtype": 1,
```

```
        "command": "restart_service2.sh",
        "execute_on": 0,
        "authtype": 0,
        "username": "",
        "password": "",
        "publickey": "",
        "privatekey": "",
        "parent_taskid": 20,
        "hostid": 10084
      }
  ]
}
```

Żądanie zadań

Wymiana `proxy tasks` obsługuje dostarczanie i potwierdzanie zadań zdalnych poleceń między serwerem a pasywnym proxy. Gdy serwer odpytuje proxy o wyniki zadań, wysyła puste żądanie `proxy tasks` w interwale zdefiniowanym przez `ProxyDataFrequency`. Proxy odpowiada swoją bieżącą wersją oraz wszystkimi oczekującymi wynikami zadań (w tym znacznikami czasu). Następnie serwer potwierdza odbiór, zwracając `response`, i może dołączyć nowe zadania do wykonania przez proxy.

name	value type	description
serwer→proxy:		
request	*string*	'proxy tasks'
proxy→serwer:		
version	*string*	Wersja proxy (<major>.<minor>.<build>).
clock	*number*	*(opcjonalnie)* Znacznik czasu transferu danych (sekundy).
ns	*number*	*(opcjonalnie)* Znacznik czasu transferu danych (nanosekundy).
serwer→proxy:		
response	*string*	Informacja o powodzeniu żądania ('success' lub 'failed').

Przykład:

serwer→proxy:

```
{
  "request":"proxy tasks"
}
```

proxy→serwer:

```
{
  "version":"7.0.0",
  "clock":1721059872,
  "ns":848141522
}
```

serwer→proxy:

```
{
  "response":"success"
}
```

Aktywny proxy

Żądanie konfiguracji

Żądanie `proxy config` jest wysyłane przez aktywny proxy w celu pobrania danych konfiguracyjnych proxy. To żądanie jest wysyłane co `ProxyConfigFrequency` (parametr konfiguracyjny proxy) sekund.

name	value type	description
proxy→server:		
request	*string*	'proxy config'
host	*string *	Nazwa proxy.
version	*string*	Wersja proxy (<major>.<minor>.<build>).
session	*string*	Token sesji konfiguracji proxy.

name	value type	description
config_revision	*number*	Wersja konfiguracji proxy.
hostmap_revision	*number*	Bieżąca wersja mapowania host-proxy.
server→proxy:		
full_sync	*number*	1 - jeśli wysyłane są pełne dane konfiguracyjne, w przeciwnym razie pole nie występuje (opcjonalne).
data	*array*	Obiekt danych tabeli. Nie występuje, jeśli konfiguracja nie została zmieniona (opcjonalne).
<table>	*object*	Jeden lub więcej obiektów z danymi <table> (opcjonalne, zależnie od zmian).
fields	*array*	Tablica nazw pól.
-	*string*	Nazwa pola.
data	*array*	Tablica wierszy.
-	*array*	Tablica kolumn.
-	*string*,*number*	Wartość kolumny z typem zależnym od typu kolumny w schemacie bazy danych.
macro.secrets	*object*	Informacje o tajnych makrach; pole nie występuje, jeśli nie ma zmian w makrach vault (opcjonalne).
proxy_group	*string*	Nazwa grupy proxy, do której należy proxy.
config_revision	*number*	Wersja pamięci podręcznej konfiguracji - wysyłana wraz z danymi konfiguracyjnymi (opcjonalne).
del_hostids	*array*	Tablica usuniętych hostid (opcjonalne).
-	*number*	Identyfikator hosta.
del_macro_hostids	*array*	Tablica hostid, dla których usunięto wszystkie makra (opcjonalne).
-	*number*	Identyfikator hosta.

Przykład:

proxy→server:

```
{
  "request": "proxy config",
  "host": "Zabbix proxy",
  "version":"8.0.0",
  "session": "fd59a09ff4e9d1fb447de1f04599bcf6",
  "config_revision": 0
}
```

server→proxy:

```
{
"full_sync": 1,
"data": {
"hosts": {
"fields": ["hostid", "host", "status", "ipmi_authtype", "ipmi_privilege", "ipmi_username", "ipmi_password"
"data": [
[10084, "Zabbix server", 0, -1, 2, "", "", "Zabbix server", 1, 1, "", "", "", ""]
]
},
"interface": {
"fields": ["interfaceid", "hostid", "main", "type", "useip", "ip", "dns", "port", "available"],
"data": [
[1, 10084, 1, 1, 1, "127.0.0.1", "", "10053", 1]
]
},
"interface_snmp": {
"fields": ["interfaceid", "version", "bulk", "community", "securityname", "securitylevel", "authpassphrase
"data": []
},
"host_inventory": {
```

```
"fields": ["hostid", "type", "type_full", "name", "alias", "os", "os_full", "os_short", "serialno_a", "ser
"data": [
[10084, "", "", "",
```

```
[5, "Windows service startup states for discovery"]
]
},
"expressions": {
"fields": ["expressionid", "regexpid", "expression", "expression_type", "exp_delimiter", "case_sensitive"]
"data": [
[1, 1, "^(btrfs|ext2|ext3|ext4|reiser|xfs|ffs|ufs|jfs|jfs2|vxfs|hfs|apfs|refs|ntfs|fat32|zfs)$", 3, ",", 0
[3, 3, "^(Physical memory|Virtual memory|Memory buffers|Cached memory|Swap space)$", 4, ",", 1],
[5, 4, "^(MMCSS|gupdate|SysmonLog|clr_optimization_v2.0.50727_32|clr_optimization_v4.0.30319_32)$", 4, ","
[6, 5, "^(automatic|automatic delayed)$", 3, ",", 1],
[7, 2, "^Software Loopback Interface", 4, ",", 1],
[8, 2, "^(In)?[Ll]oop[Bb]ack[0-9._]*$", 4, ",", 1],
[9, 2, "^NULL[0-9.]*$", 4, ",", 1],
[10, 2, "^[Ll]o[0-9.]*$", 4, ",", 1],
[11, 2, "^[Ss]ystem$", 4, ",", 1],
[12, 2, "^Nu[0-9.]*$", 4, ",", 1]
]
},
"settings": {
"fields": ["name", "type", "value_str", "value_int"],
"data": [
["autoreg_tls_accept", 2, "", 1],
["hk_history_global", 2, "", 0],
["snmptrap_logging", 2, "", 1],
["proxy_secrets_provider", 2, "", 0],
["hk_history", 1, "31d", 0],
["timeout_db_monitor", 1, "3s", 0],
["timeout_external_check", 1, "3s", 0],
["timeout_http_agent", 1, "3s", 0],
["timeout_simple_check", 1, "3s", 0],
["timeout_snmp_agent", 1, "3s", 0],
["timeout_ssh_agent", 1, "3s", 0],
["timeout_telnet_agent", 1, "3s", 0],
["timeout_zabbix_agent", 1, "3s", 0],
["timeout_browser", 1, "30s", 0]
]
},
"httptest": {
"fields": ["httptestid", "name", "delay", "agent", "authentication", "http_user", "http_password", "hostid
"data": []
},
"httptestitem": {
"fields": ["httptestitemid", "httptestid", "itemid", "type"],
"data": []
},
"httptest_field": {
"fields": ["httptest_fieldid", "httptestid", "type", "name", "value"],
"data": []
},
"httpstep": {
"fields": ["httpstepid", "httptestid", "name", "no", "url", "timeout", "posts", "required", "status_codes"
"data": []
},
"httpstepitem": {
"fields": ["httpstepitemid", "httpstepid", "itemid", "type"],
"data": []
},
"httpstep_field": {
"fields": ["httpstep_fieldid", "httpstepid", "type", "name", "value"],
"data": []
},
"config_autoreg_tls": {
```

```
"fields": ["autoreg_tlsid", "tls_psk_identity", "tls_psk"],
"data": [
[1, "", ""]
]
}
},
"macro.secrets": {
"AppID=zabbix_server&Query=Safe=passwordSafe;Object=zabbix": {
"Content": "738"
}
},
"config_revision": 2
}
```

Żądanie danych

Żądanie `proxy data` jest wysyłane przez proxy w celu przekazania danych o dostępności interfejsów hosta, historii, wykrywaniu i autorejestracji. To żądanie jest wysyłane co `DataSenderFrequency` sekund (parametr konfiguracji proxy). Należy pamiętać, że aktywny proxy nadal będzie odpytywać serwer Zabbix co sekundę w celu pobrania zadań zdalnych poleceń (z pustym żądaniem `proxy data`).

name	value type	description
proxy→server:		
request	*string*	'proxy data'
host	*string*	Nazwa proxy.
session	*string*	Token sesji danych.
interface availability	*array*	*(optional)* Tablica obiektów danych dostępności interfejsu.
interfaceid	*number*	Identyfikator interfejsu.
available	*number*	Dostępność interfejsu: **0**, *INTERFACE_AVAILABLE_UNKNOWN* - nieznana **1**, *INTERFACE_AVAILABLE_TRUE* - dostępny **2**, *INTERFACE_AVAILABLE_FALSE* - niedostępny
error	*string*	Komunikat błędu interfejsu lub pusty ciąg.
history data	*array*	*(optional)* Tablica obiektów danych historycznych.
itemid	*number*	Identyfikator pozycji.
clock	*number*	Znacznik czasu wartości pozycji (sekundy).
ns	*number*	Znacznik czasu wartości pozycji (nanosekundy).
value	*string*	*(optional)* Wartość pozycji.
id	*number*	Identyfikator wartości (licznik rosnący, unikalny w obrębie jednej sesji danych).
timestamp	*number*	*(optional)* Znacznik czasu pozycji typu log.
source	*string*	*(optional)* Wartość source pozycji eventlog.
severity	*number*	*(optional)* Wartość severity pozycji eventlog.
eventid	*number*	*(optional)* Wartość eventid pozycji eventlog.
state	*string*	*(optional)* Stan pozycji: **0**, *ITEM_STATE_NORMAL* **1**, *ITEM_STATE_NOTSUPPORTED*
lastlogsize	*number*	*(optional)* Ostatni rozmiar logu dla pozycji typu log.
mtime	*number*	*(optional)* Czas modyfikacji dla pozycji typu log.
discovery data	*array*	*(optional)* Tablica obiektów danych wykrywania.
clock	*number*	Znacznik czasu danych wykrywania.
druleid	*number*	Identyfikator reguły wykrywania.
dcheckid	*number*	Identyfikator kontroli wykrywania lub null dla danych reguły wykrywania.

name	value type	description
type	*number*	Typ kontroli wykrywania: **-1** dane reguły wykrywania **0**, *SVC_SSH* - kontrola usługi SSH **1**, *SVC_LDAP* - kontrola usługi LDAP **2**, *SVC_SMTP* - kontrola usługi SMTP **3**, *SVC_FTP* - kontrola usługi FTP **4**, *SVC_HTTP* - kontrola usługi HTTP **5**, *SVC_POP* - kontrola usługi POP **6**, *SVC_NNTP* - kontrola usługi NNTP **7**, *SVC_IMAP* - kontrola usługi IMAP **8**, *SVC_TCP* - kontrola dostępności portu TCP **9**, *SVC_AGENT* - agent Zabbix **10**, *SVC_SNMPv1* - agent SNMPv1 **11**, *SVC_SNMPv2* - agent SNMPv2 **12**, *SVC_ICMPPING* - ping ICMP **13**, *SVC_SNMPv3* - agent SNMPv3 **14**, *SVC_HTTPS* - kontrola usługi HTTPS **15**, *SVC_TELNET* - kontrola dostępności Telnet
ip	*string*	Adres IP hosta.
dns	*string*	Nazwa DNS hosta.
port	*number*	*(optional)* Numer portu usługi.
key_	*string*	*(optional)* Klucz pozycji dla kontroli wykrywania typu **9** *SVC_AGENT*
value	*string*	*(optional)* Wartość odebrana z usługi; dla większości usług może być pusta.
status	*number*	*(optional)* Stan usługi: **0**, *DOBJECT_STATUS_UP* - usługa działa **1**, *DOBJECT_STATUS_DOWN* - usługa nie działa
autoregistration	*array*	*(optional)* Tablica obiektów danych autorejestracji.
clock	*number*	Znacznik czasu danych autorejestracji.
host	*string*	Nazwa hosta.
ip	*string*	*(optional)* Adres IP hosta.
dns	*string*	*(optional)* Rozwiązana nazwa DNS z adresu IP.
port	*string*	*(optional)* Port hosta.
host_metadata	*string*	*(optional)* Metadane hosta wysłane przez agent (na podstawie parametru konfiguracji agenta HostMetadata lub HostMetadataItem).
tasks	*array*	*(optional)* Tablica zadań.
type	*number*	Typ zadania: **0**, *ZBX_TM_TASK_PROCESS_REMOTE_COMMAND_RESULT* - wynik zdalnego polecenia
status	*number*	Stan wykonania zdalnego polecenia: **0**, *ZBX_TM_REMOTE_COMMAND_COMPLETED* - zdalne polecenie zakończone pomyślnie **1**, *ZBX_TM_REMOTE_COMMAND_FAILED* - zdalne polecenie nie powiodło się
error	*string*	*(optional)* Komunikat błędu.
parent_taskid	*number*	ID zadania nadrzędnego.
more	*number*	*(optional)* 1 - jest więcej danych historycznych do wysłania
clock	*number*	*(optional)* Znacznik czasu przesyłania danych (sekundy).
ns	*number*	*(optional)* Znacznik czasu przesyłania danych (nanosekundy).
version	*string*	Wersja proxy (<major>.<minor>.<build>).
server→proxy:		
response	*string*	Informacja o powodzeniu żądania (’success’ lub ’failed’).
upload	*string*	Kontrola wysyłania danych historycznych (historia, autorejestracja, dostępność hosta, wykrywanie sieci). Możliwe wartości: **enabled** - normalne działanie **disabled** - serwer nie przyjmuje danych (prawdopodobnie z powodu przekroczenia limitu pamięci podręcznej wewnętrznej)

name	value type	description
tasks	*array*	*(optional)* Tablica zadań.
type	*number*	Typ zadania: **1**, *ZBX_TM_TASK_PROCESS_REMOTE_COMMAND* - zdalne polecenie
clock	*number*	Czas utworzenia zadania.
ttl	*number*	Czas w sekundach, po którym zadanie wygasa.
commandtype	*number*	Typ zdalnego polecenia: **0**, *ZBX_SCRIPT_TYPE_CUSTOM_SCRIPT* - użyj skryptu niestandardowego **1**, *ZBX_SCRIPT_TYPE_IPMI* - użyj IPMI **2**, *ZBX_SCRIPT_TYPE_SSH* - użyj SSH **3**, *ZBX_SCRIPT_TYPE_TELNET* - użyj Telnet **4**, *ZBX_SCRIPT_TYPE_GLOBAL_SCRIPT* - użyj skryptu globalnego (obecnie funkcjonalnie równoważnego skryptowi niestandardowemu)
command	*string*	Zdalne polecenie do wykonania.
execute_on	*number*	Cel wykonania dla skryptów niestandardowych: **0**, *ZBX_SCRIPT_EXECUTE_ON_AGENT* - wykonaj skrypt na agent **1**, *ZBX_SCRIPT_EXECUTE_ON_SERVER* - wykonaj skrypt na serwerze **2**, *ZBX_SCRIPT_EXECUTE_ON_PROXY* - wykonaj skrypt na proxy
port	*number*	*(optional)* Port dla poleceń Telnet i SSH.
authtype	*number*	*(optional)* Typ uwierzytelniania dla poleceń SSH.
username	*string*	*(optional)* Nazwa użytkownika dla poleceń Telnet i SSH.
password	*string*	*(optional)* Hasło dla poleceń Telnet i SSH.
publickey	*string*	*(optional)* Klucz publiczny dla poleceń SSH.
privatekey	*string*	*(optional)* Klucz prywatny dla poleceń SSH.
parent_taskid	*number*	ID zadania nadrzędnego.
hostid	*number*	ID docelowego hosta.

Przykład:

proxy→server:


```
{
"request": "proxy data",
"host": "Zabbix proxy",
"session": "818cdd1b537bdc5e50c09ed4969235b6",
"interface availability": [{
"interfaceid": 1,
"available": 1,
"error": ""
}],
"history data": [{
"id": 1114,
"itemid": 44162,
"clock": 1665730632,
"ns": 798953105,
"value": "1"
}, {
"id": 1115,
"itemid": 44161,
"clock": 1665730633,
"ns": 811684663,
"value": "58"
}],
"auto registration": [{
"clock": 1665730633,
"host": "Zabbix server",
"ip": "127.0.0.1",
"dns": "localhost",
"port": "10053",
"host_metadata": "58",
```

```
"tls_accepted": 1
}],
"discovery data": [{
"clock": 1665732232,
"drule": 2,
"dcheck": 2,
"ip": "127.0.0.1",
"dns": "localhost",
"port": 10052,
"status": 1
}, {
"clock": 1665732232,
"drule": 2,
"dcheck": null,
"ip": "127.0.0.1",
"dns": "localhost",
"status": 1
}],
"host data": [{
"hostid": 10084,
"active_status": 1
}],
"tasks": [{
"type": 3,
"clock": 1665730985,
"ttl": 0,
"status": -1,
"info": "Remote commands are not enabled",
"parent_taskid": 3
}],
"version": "8.0.0",
"clock": 1665730643,
"ns": 65389964
}
```


server→proxy:


```
{
"upload": "enabled",
"response": "success",
"tasks": [{
"type": 2,
"clock": 1665730986,
"ttl": 600,
"commandtype": 0,
"command": "ping -c 3 127.0.0.1; case $? in [01]) true;; *) false;; esac",
"execute_on": 2,
"port": 0,
"authtype": 0,
"username": "",
"password": "",
"publickey": "",
"privatekey": "",
"alertid": 0,
"parent_taskid": 4,
"hostid": 10084
}]
}
```


2 Protokół Zabbix agent/agent2

Więcej informacji o protokołach Zabbix agent i Zabbix agent 2 można znaleźć na stronie Passive and active agent checks.

4 Protokół pluginów Zabbix agent 2

Protokół Zabbix agent 2 opiera się na modelu kodu, rozmiaru i danych.

Kod

Typ	Rozmiar	Komentarze
Bajt	4	Typ ładunku, obecnie obsługiwany jest tylko JSON.

Rozmiar

Type	Size	Comments
Bajt	4	Rozmiar bieżącego ładunku w bajtach.

Dane ładunku

Typ	Rozmiar	Komentarze
Byte	Zdefiniowany przez pole *Rozmiar*	Dane w formacie JSON.

Definicja danych payloadu

Wspólne dane

Te parametry są obecne we wszystkich żądaniach/odpowiedziach:

Nazwa	Typ	Komentarze
id	uint32	Dla żądań — inkrementowany identyfikator używany do powiązania żądań z odpowiedziami. Unikalny w obrębie kierunku żądania (tj. od agent do wtyczki lub od wtyczki do agent). Dla odpowiedzi — ID odpowiadającego żądania.
type	uint32	Typ żądania.

Żądanie logowania

Żądanie wysyłane przez wtyczkę w celu zapisania komunikatu dziennika w pliku dziennika agenta.

direction	plugin → agent
response	no

Parametry specyficzne dla żądań logowania:

Name	Type	Comments
severity	uint32	Poziom ważności komunikatu (poziom logowania).
message	string	Komunikat do zapisania w dzienniku.

Przykład:

```
{"id":0,"type":1,"severity":3,"message":"message"}
```

Żądanie rejestracji

Żądanie wysyłane przez agent podczas fazy uruchamiania agent w celu uzyskania udostępnianych metryk do zarejestrowania wtyczki.

direction	agent → plugin
response	yes

Parametry specyficzne dla żądań rejestracji:

Name	Type	Comments
version	string	Wersja protokołu <major>.<minor>

Przykład:

```
{"id":1,"type":2,"version":"1.0"}
```

Odpowiedź rejestracji

Odpowiedź pluginu na żądanie rejestracji.

kierunek	plugin → agent
odpowiedź	n/d

Parametry specyficzne dla odpowiedzi rejestracji:

Nazwa	Typ	Uwagi
name	string	Nazwa pluginu.
metrics	array of strings (optional)	Metryki wraz z opisami używanymi w pluginie. Zwraca RegisterMetrics(). Nieobecne, jeśli zwracany jest błąd.
interfaces	uint32 (optional)	Maska bitowa interfejsów obsługiwanych przez plugin. Nieobecne, jeśli zwracany jest błąd.
error	string (optional)	Komunikat błędu zwracany, jeśli plugin nie może zostać uruchomiony. Nieobecne, jeśli zwracane są metryki.

Przykłady:

```
{"id":2,"type":3,"metrics":["external.test", "External exporter Test."], "interfaces": 4}
```

lub

```
{"id":2,"type":3,"error":"error message"}
```

Żądanie Start

Żądanie wykonania funkcji Start interfejsu Runner.

direction	agent → plugin
response	nie

Żądanie nie ma specyficznych parametrów, zawiera tylko parametry wspólnych danych.

Przykład:

```
{"id":3,"type":4}
```

Żądanie zakończenia

Żądanie wysyłane przez agent w celu zamknięcia wtyczki.

direction	agent → plugin
response	no

Żądanie nie ma specyficznych parametrów, zawiera jedynie parametry wspólnych danych.

Przykład:

```
{"id":3,"type":5}
```

Żądanie eksportu

Żądanie wykonania funkcji Export interfejsu Exporter.

direction	agent → plugin
response	nie

Parametry specyficzne dla żądań eksportu:

Name	Type	Comments
key	string	Klucz pluginu.
parameters	array of strings (optional)	Parametry funkcji Export.

Przykład:

```
{"id":4,"type":6,"key":"test.key","parameters":["foo","bar"]}
```

Odpowiedź eksportu

Odpowiedź z funkcji Export interfejsu Exporter.

kierunek	plugin → agent
odpowiedź	n/d

Parametry specyficzne dla odpowiedzi eksportu:

Nazwa	Typ	Komentarze
value	string (optional)	Wartość odpowiedzi z funkcji Export. Nieobecne, jeśli zwracany jest błąd.
error	string (optional)	Komunikat błędu, jeśli funkcja Export nie została wykonana pomyślnie. Nieobecne, jeśli zwracana jest wartość.

Przykłady:

```
{"id":5,"type":7,"value":"response"}
```

lub

```
{"id":5,"type":7,"error":"error message"}
```

Konfiguracja żądania

Żądanie wykonania funkcji *Configure* interfejsu *Configurator*.

direction	agent → plugin
response	n/a

Parametry specyficzne dla żądań *Configure*:

Name	Type	Comments
global_options	JSON object	Obiekt JSON zawierający globalne opcje konfiguracji agenta.
private_options	JSON object (optional)	Obiekt JSON zawierający prywatne opcje konfiguracji pluginu, jeśli zostały podane.

Przykład:

```
{"id":6,"type":8,"global_options":{...},"private_options":{...}}
```

Walidacja żądania

Żądanie wykonania funkcji *Validate* interfejsu *Configurator*.

direction	agent → plugin
response	yes

Parametry specyficzne dla żądań *Validate*:

Name	Type	Comments
private_options	JSON object (optional)	Obiekt JSON zawierający prywatne opcje konfiguracji pluginu, jeśli zostały podane.

Przykład:

```
{"id":7,"type":9,"private_options":{...}}
```

Walidacja odpowiedzi

Odpowiedź z funkcji *Validate* interfejsu *Configurator*.

direction	plugin → agent
response	n/a

Parametry specyficzne dla odpowiedzi *Validate*:

Name	Type	Comments
error	string (optional)	Komunikat o błędzie zwracany, jeśli funkcja Validate nie zostanie wykonana pomyślnie. Nieobecny, jeśli wykonanie zakończy się powodzeniem.

Przykład:

```
{"id":8,"type":10}
```

lub

```
{"id":8,"type":10,"error":"error message"}
```

5 Protokół Zabbix sender

Przegląd

serwer Zabbix i proxy Zabbix używają protokołu komunikacyjnego opartego na JSON do odbierania danych z Zabbix sender. Dane mogą być odbierane za pomocą pozycji trapper lub pozycji HTTP agent z włączonym przechwytywaniem.

Komunikaty żądania i odpowiedzi muszą zaczynać się od nagłówka i długości danych.

Żądanie Zabbix sender

```
{
    "request": "sender data",
    "data": [
        {
            "host": "<hostname>",
            "key": "trap",
            "value": "test value"
        }
    ]
}
```

Odpowiedź serwera Zabbix

```
{
    "response": "success",
    "info": "processed: 1; failed: 0; total: 1; seconds spent: 0.060753"
}
```

Żądanie Zabbix sender ze znacznikiem czasu

Alternatywnie Zabbix sender może wysłać żądanie ze znacznikiem czasu i nanosekundami.

```
{
    "request": "sender data",
    "data": [
        {
            "host": "<hostname>",
            "key": "trap",
            "value": "test value",
            "clock": 1516710794,
            "ns": 592397170
        },
        {
            "host": "<hostname>",
            "key": "trap",
            "value": "test value",
            "clock": 1516710795,
            "ns": 192399456
        }
    ],
    "clock": 1516712029,
    "ns": 873386094
}
```

Odpowiedź serwera Zabbix

```
{
    "response": "success",
    "info": "processed: 2; failed: 0; total: 2; seconds spent: 0.060904"
}
```

6 Nagłówek

Przegląd

Nagłówek jest obecny we wszystkich komunikatach żądania i odpowiedzi między komponentami Zabbix. Jest wymagany do określenia długości komunikatu, tego, czy jest on skompresowany, czy nie, oraz tego, czy jest to duży pakiet, czy nie.

Protokół komunikacyjny Zabbix ma limit rozmiaru pakietu wynoszący 1 GB na połączenie. Limit 1 GB ma zastosowanie zarówno do długości odebranych danych pakietu, jak i do długości danych po dekompresji.

Podczas wysyłania konfiguracji do Zabbix proxy limit rozmiaru pakietu jest zwiększany do 4 GB, aby umożliwić synchronizację dużych konfiguracji. Gdy długość danych przed kompresją przekracza 4 GB, Zabbix server automatycznie zaczyna używać formatu dużych pakietów (flaga 0x04), co zwiększa limit rozmiaru pakietu do 16 GB.

Należy pamiętać, że chociaż format dużych pakietów może być używany do wysyłania dowolnych danych, obecnie tylko synchronizator konfiguracji Zabbix proxy może obsługiwać pakiety większe niż 1 GB.

Structure

The header consists of four fields. All numbers in the header are formatted as little-endian.

Field	Size	Size (large packet)	Description
<PROTOCOL>	4	4	"ZBXD" or 5A 42 58 44
<FLAGS>	1	1	Protocol flags: 0x01 - Zabbix communications protocol 0x02 - compression 0x04 - large packet

Field	Size	Size (large packet)	Description
<DATALEN>	4	8	Data length.
<RESERVED>	4	8	When compression is used (0x02 flag) - the length of uncompressed data When compression is not used - 00 00 00 00

Przykłady

Poniżej znajdują się fragmenty kodu pokazujące, jak dodać nagłówek protokołu Zabbix do danych, które chcesz wysłać, aby uzyskać pakiet, który należy wysłać do Zabbix, tak aby został poprawnie zinterpretowany. Te fragmenty kodu zakładają, że dane nie są większe niż 1 GB, dlatego format dużych pakietów nie jest używany.

Python

```
packet = b"ZBXD\1" + struct.pack("<II", len(data), 0) + data
```

lub

```
def zbx_create_header(plain_data_size, compressed_data_size=None):
    protocol = b"ZBXD"
    flags = 0x01
    if compressed_data_size is None:
        datalen = plain_data_size
        reserved = 0
    else:
        flags |= 0x02
        datalen = compressed_data_size
        reserved = plain_data_size
    return protocol + struct.pack("<BII", flags, datalen, reserved)

packet = zbx_create_header(len(data)) + data
```

Perl

```
my $packet = "ZBXD\1" . pack("(II)<", length($data), 0) . $data;
```

lub

```
sub zbx_create_header($;$)
{
    my $plain_data_size = shift;
    my $compressed_data_size = shift;

    my $protocol = "ZBXD";
    my $flags = 0x01;
    my $datalen;
    my $reserved;

    if (!defined($compressed_data_size))
    {
        $datalen = $plain_data_size;
        $reserved = 0;
    }
    else
    {
        $flags |= 0x02;
        $datalen = $compressed_data_size;
        $reserved = $plain_data_size;
    }

    return $protocol . chr($flags) . pack("(II)<", $datalen, $reserved);
}

my $packet = zbx_create_header(length($data)) . $data;
```

PHP

```
$packet = "ZBXD\1" . pack("VV", strlen($data), 0) . $data;
```

lub

```
function zbx_create_header($plain_data_size, $compressed_data_size = null)
{
    $protocol = "ZBXD";
    $flags = 0x01;
    if (is_null($compressed_data_size))
    {
        $datalen = $plain_data_size;
        $reserved = 0;
    }
    else
    {
        $flags |= 0x02;
        $datalen = $compressed_data_size;
        $reserved = $plain_data_size;
    }
    return $protocol . chr($flags) . pack("VV", $datalen, $reserved);
}

$packet = zbx_create_header(strlen($data)) . $data;
```

Bash

```
datalen=$(printf "%08x" ${#data})
datalen="\\x${datalen:6:2}\\x${datalen:4:2}\\x${datalen:2:2}\\x${datalen:0:2}"
printf "ZBXD\1${datalen}\0\0\0\0%s" "$data"
```

7 Protokół eksportu JSON rozdzielanego znakami nowej linii

Ta sekcja przedstawia szczegóły protokołu eksportu w formacie JSON rozdzielanym znakami nowej linii, używanego w:

- eksporcie danych do plików
- przesyłaniu strumieniowym do systemów zewnętrznych

Można eksportować następujące dane:

- zdarzenia wyzwalaczy
- wartości pozycji
- trendy (tylko eksport do plików)

Wszystkie pliki mają rozszerzenie .ndjson. Każdy wiersz pliku eksportu jest obiektem JSON.

Zdarzenia wyzwalaczy

Następujące informacje są eksportowane dla zdarzenia problemu:

Field	Type	Description
clock	number	Liczba sekund od Epoch do momentu wykrycia problemu (część całkowita).
ns	number	Liczba nanosekund, które należy dodać do `clock`, aby uzyskać dokładny czas wykrycia problemu.
value	number	1 (zawsze).
eventid	number	ID zdarzenia problemu.
name	string	Nazwa zdarzenia problemu.
severity	number	Poziom ważności zdarzenia problemu (0 - Niesklasyfikowane, 1 - Informacja, 2 - Ostrzeżenie, 3 - Średni, 4 - Wysoki, 5 - Katastrofa).
hosts	array	Lista hostów uwzględnionych w wyrażeniu wyzwalacza; w tablicy powinien znajdować się co najmniej jeden element.
-	object	
host	string	Nazwa hosta.

Field		Type	Description
	name	string	Widoczna nazwa hosta.
groups		array	Lista grup hostów wszystkich hostów uwzględnionych w wyrażeniu wyzwalacza; w tablicy powinien znajdować się co najmniej jeden element.
-		string	Nazwa grupy hostów.
tags		array	Lista tagów problemu (może być pusta).
-		object	
	tag	string	Nazwa tagu.
	value	string	Wartość tagu (może być pusta).

Następujące informacje są eksportowane dla zdarzenia odzyskania:

Field	Type	Description
clock	number	Liczba sekund od Epoch do momentu rozwiązania problemu (część całkowita).
ns	number	Liczba nanosekund, które należy dodać do `clock`, aby uzyskać dokładny czas rozwiązania problemu.
value	number	0 (zawsze).
eventid	number	ID zdarzenia odzyskania.
p_eventid	number	ID zdarzenia problemu.

Przykłady

Problem:

```
{"clock":1519304285,"ns":123456789,"value":1,"name":"Agent Zabbix jest niedostępny na hoście Host B lub po
```

Odzyskanie:

```
{"clock":1519304345,"ns":987654321,"value":0,"eventid":43,"p_eventid":42}
```

Problem (generowanie wielu zdarzeń problemów):

```
{"clock":1519304286,"ns":123456789,"value":1,"eventid":43,"name":"Agent Zabbix jest niedostępny na hoście
```

```
{"clock":1519304286,"ns":123456789,"value":1,"eventid":43,"name":"Agent Zabbix jest niedostępny na hoście
```

Odzyskanie:

```
{"clock":1519304346,"ns":987654321,"value":0,"eventid":44,"p_eventid":43}
```

```
{"clock":1519304346,"ns":987654321,"value":0,"eventid":44,"p_eventid":42}
```

Wartości pozycji

Dla zebranej wartości pozycji eksportowane są następujące informacje:

Pole	Typ	Opis
host	object	Nazwa hosta pozycji.
host	string	Nazwa hosta.
name	string	Widoczna nazwa hosta.
groups	array	Lista grup hostów hosta pozycji; w tablicy powinien znajdować się co najmniej jeden element.
-	string	Nazwa grupy hostów.
item_tags	array	Lista tagów pozycji (może być pusta).
-	object	
tag	string	Nazwa tagu.
value	string	Wartość tagu (może być pusta).
itemid	number	ID pozycji.
name	string	Widoczna nazwa pozycji.
clock	number	Liczba sekund od Epoch do momentu zebrania wartości (część całkowita).

Pole	Typ	Opis
ns	number	Liczba nanosekund, które należy dodać do `clock`, aby uzyskać dokładny czas zebrania wartości.
timestamp (*Log* only)	number	0, jeśli niedostępne.
source (*Log* only)	string	Pusty ciąg, jeśli niedostępne.
severity (*Log* only)	number	0, jeśli niedostępne.
eventid (*Log* only)	number	0, jeśli niedostępne.
value	number (for numeric items) or string (for text items)	Zebrana wartość pozycji.
type	number	Typ zebranej wartości: 0 - liczba zmiennoprzecinkowa, 1 - znak, 2 - log, 3 - liczba całkowita bez znaku, 4 - tekst, 5 - binarny, 6 - JSON

Przykłady

Wartość numeryczna (unsigned):

```
{"host":{"host":"Host B","name":"Host B visible"},"groups":["Group X","Group Y","Group Z"],"item_tags":[{"
```

Wartość numeryczna (float):

```
{"host":{"host":"Host B","name":"Host B visible"},"groups":["Group X","Group Y","Group Z"],"item_tags":[{"
```

Wartość znakowa, tekstowa:

```
{"host":{"host":"Host B","name":"Host B visible"},"groups":["Group X","Group Y","Group Z"],"item_tags":[{"
```

Wartość logu:

```
{"host":{"host":"Host A","name":"Host A visible"},"groups":["Group X","Group Y","Group Z"],"item_tags":[{"
```

Trendy

Następujące informacje są eksportowane dla obliczonej wartości trendu:

Pole	Typ	Opis
host	object	Nazwa hosta hosta pozycji.
host	string	Nazwa hosta.
name	string	Widoczna nazwa hosta.
groups	array	Lista grup hostów hosta pozycji; w tablicy powinien znajdować się co najmniej jeden element.
-	string	Nazwa grupy hostów.
item_tags	array	Lista tagów pozycji (może być pusta).
-	object	
tag	string	Nazwa tagu.
value	string	Wartość tagu (może być pusta).
itemid	number	ID pozycji.
name	string	Widoczna nazwa pozycji.
clock	number	Liczba sekund od Epoki do momentu zebrania wartości (część całkowita).
count	number	Liczba wartości zebranych dla danej godziny.
min	number	Minimalna wartość pozycji dla danej godziny.
avg	number	Średnia wartość pozycji dla danej godziny.
max	number	Maksymalna wartość pozycji dla danej godziny.

Pole	Typ	Opis
type	number	Typ wartości: 0 - liczba zmiennoprzecinkowa, 3 - liczba całkowita bez znaku

Przykłady

Wartość numeryczna (unsigned):

```
{"host":{"host":"Host B","name":"Host B visible"},"groups":["Group X","Group Y","Group Z"],"item_tags":[{"
```

Wartość numeryczna (float):

```
{"host":{"host":"Host B","name":"Host B visible"},"groups":["Group X","Group Y","Group Z"],"item_tags":[{"
```

4 Pozycje

Aby uzyskać dostęp do treści w tej sekcji, skorzystaj z paska bocznego.

1 parametry vm.memory.size

Przegląd

Ta sekcja zawiera szczegółowe informacje o niektórych parametrach pozycji agent vm.memory.size[<mode>].

Parametry

Dla tej pozycji dostępne są następujące parametry:

- **active** - pamięć aktualnie używana lub używana jeszcze bardzo niedawno, a więc znajdująca się w RAM
- **anon** - pamięć niezwiązana z plikiem (nie można jej z niego ponownie odczytać)
- **available** - dostępna pamięć, obliczana różnie w zależności od platformy (zobacz tabelę poniżej)
- **buffers** - pamięć podręczna dla takich elementów jak metadane systemu plików
- **cached** - pamięć podręczna dla różnych danych
- **exec** - kod wykonywalny, zwykle pochodzący z pliku (programu)
- **file** - pamięć podręczna zawartości ostatnio używanych plików
- **free** - pamięć, która jest natychmiast dostępna dla każdego podmiotu żądającego pamięci
- **inactive** - pamięć oznaczona jako nieużywana
- **pavailable** - pamięć „available” jako procent wartości „total” (obliczana jako `available/total*100`)
- **pinned** - to samo co „wired”
- **pused** - pamięć „used” jako procent wartości „total” (obliczana jako `used/total*100`)
- **shared** - pamięć, do której jednocześnie może uzyskiwać dostęp wiele procesów
- **slab** - całkowita ilość pamięci używanej przez jądro do buforowania struktur danych na własne potrzeby
- **total** - całkowita dostępna pamięć fizyczna
- **used** - używana pamięć, obliczana różnie w zależności od platformy (zobacz tabelę poniżej)
- **wired** - pamięć oznaczona jako mająca zawsze pozostawać w RAM. Nigdy nie jest przenoszona na dysk.

Warning:
Niektóre z tych parametrów są specyficzne dla platformy i mogą nie być dostępne na Twojej platformie. Szczegóły znajdują się w pozycjach agenta Zabbix.

Obliczanie wartości **available** i **used** zależnie od platformy:

Platforma	**”available”**	**”used”**
AIX	free + cached	rzeczywiście używana pamięć
FreeBSD	inactive + cached + free	active + wired + cached
HP UX	free	total - free
Linux<3.14	free + buffers + cached	total - free

Platforma	**”available”**	**”used”**
Linux 3.14+ (również backportowane do 3.10 w RHEL 7)	/proc/meminfo, szczegóły można znaleźć w sekcji „MemAvailable” dokumentacji jądra Linux documentation. Zwróć uwagę, że free + buffers + cached nie jest już równe „available”, ponieważ nie cała pamięć podręczna stron może zostać zwolniona, a w obliczeniach używany jest niski próg znaku wodnego.	total - free
NetBSD	inactive + execpages + file + free	total - free
OpenBSD	inactive + free + cached	active + wired
OSX	inactive + free	active + wired
Solaris	free	total - free
Win32	free	total - free

Attention:
Suma *vm.memory.size[used]* i *vm.memory.size[available]* nie musi być równa wartości total. Na przykład w FreeBSD:
* Pamięci active, inactive, wired i cached są uznawane za używane, ponieważ przechowują użyteczne informacje.
* Jednocześnie pamięci inactive, cached i free są uznawane za dostępne, ponieważ te rodzaje pamięci mogą zostać natychmiast przydzielone procesom żądającym większej ilości pamięci.

Tak więc pamięć inactive jest jednocześnie używana i dostępna. Z tego powodu pozycja *vm.memory.size[used]* jest przeznaczona wyłącznie do celów informacyjnych, natomiast *vm.memory.size[available]* jest przeznaczona do użycia w wyzwalaczach.

Zobacz także

1. Dodatkowe szczegóły dotyczące obliczania pamięci w różnych Systemach Operacyjnych

2 Pasywne i aktywne kontrole agenta

Przegląd

Ta sekcja zawiera szczegółowe informacje o kontrolach pasywnych i aktywnych wykonywanych przez Zabbix agent i Zabbix agent 2.

Zabbix używa protokołu komunikacyjnego opartego na JSON do komunikacji z agentami.

Protokoły Zabbix agent i Zabbix agent 2 zostały ujednolicone od wersji Zabbix 7.0. Różnica między żądaniami/odpowiedziami Zabbix agent i Zabbix agent 2 jest wyrażona przez wartość znacznika „variant”.

Pasywne sprawdzenia

Pasywne sprawdzenie to proste żądanie danych. Serwer Zabbix lub proxy pyta o pewne dane (na przykład obciążenie CPU), a agent Zabbix odsyła wynik do serwera.

Pasywne sprawdzenia są wykonywane asynchronicznie — nie jest wymagane odebranie odpowiedzi na jedno żądanie przed rozpoczęciem innych sprawdzeń. Rozwiązywanie DNS również odbywa się asynchronicznie.

Agent poller będzie próbował połączyć się ze wszystkimi adresami zwróconymi przez wyszukiwanie DNS. Zapewnia to, że jeśli jeden adres IP jest nieosiągalny, poller spróbuje użyć kolejnego dostępnego adresu, zwiększając prawdopodobieństwo pomyślnego połączenia. To ulepszenie dotyczy zarówno serwera Zabbix, jak i proxy.

Maksymalna współbieżność asynchronicznych sprawdzeń wynosi 1000 (zdefiniowana przez MaxConcurrentChecksPerPoller).

Liczba asynchronicznych agent pollerów jest określana przez parametr StartAgentPollers.

Żądanie serwera

Definicję nagłówka i długości danych można znaleźć w szczegółach protokołu.

```
{
  "request": "passive checks",
  "data": [
    {
      "key": "agent.version",
      "timeout": 3
    }
```

```
  ]
}
```

Pole		Typ	Wymagane	Wartość
request		*string*	tak	`"passive checks"`
data		*array of object*	tak	Pasywna pozycja sprawdzenia.
	key	*string*	tak	Klucz pozycji z rozwiniętymi makrami.
	timeout	*number*	tak	Limit czasu komunikacji.

Odpowiedź agenta

```
{
  "version": "8.0.0",
  "variant": 2,
  "data": [
    {
      "value": "8.0.0"
    }
  ]
}
```

Pole		Typ	Wymagane	Wartość
version		*string*	tak	Numer wersji agenta.
variant		*number*	tak	Wariant agenta (*1* - agent Zabbix, *2* - agent Zabbix 2).
data		*array of object*	tak	Zawiera wynik sprawdzenia.
	value	*string*	nie	Wartość pozycji, jeśli sprawdzenie zakończyło się powodzeniem.
	error	*string*	nie	Komunikat błędu, jeśli sprawdzenie nie zakończyło się powodzeniem.

Na przykład dla obsługiwanych pozycji:

1. Serwer otwiera połączenie TCP
2. Serwer wysyła **<HEADER><DATALEN>{”request”:”passive checks”,”data”:[{”key”:”agent.ping”,”timeout”:3}]}**
3. Agent odczytuje żądanie i odpowiada **<HEADER><DATALEN>{”version”:”8.0.0”,”variant”:2,”data”:[{”value”:1}]}**
4. Serwer przetwarza dane, aby uzyskać wartość, w naszym przypadku „1”
5. Połączenie TCP zostaje zamknięte

Na przykład dla nieobsługiwanych pozycji:

1. Serwer otwiera połączenie TCP
2. Serwer wysyła **<HEADER><DATALEN>{”request”:”passive checks”,”data”:[{”key”:”vfs.fs.size[/nono]”,”timeout”:3}]}**
3. Agent odczytuje żądanie i odpowiada **<HEADER><DATALEN>{”version”:”8.0.0”,”variant”:2,”data”:[{”error”:”Unsupported item key.”}]}**
4. Serwer przetwarza dane, zmienia stan pozycji na nieobsługiwaną z określonym komunikatem błędu
5. Połączenie TCP zostaje zamknięte

Przełączenie awaryjne na stary protokół

Aby upewnić się, że serwer lub proxy Zabbix mogą współpracować z agentami z wersji wcześniejszych niż 7.2, które używają protokołu tekstowego, zaimplementowano przełączenie awaryjne na stary protokół.

Pasywne kontrole są wykonywane z użyciem protokołu JSON (7.0 i nowsze) po restarcie lub po zmianie konfiguracji interfejsu. Jeśli w odpowiedzi nie zostanie odebrany prawidłowy JSON (agent wysłał „ZBX_NOTSUPPORTED”), Zabbix zapisze interfejs w pamięci podręcznej jako używający starego protokołu i **ponowi** kontrolę, wysyłając tylko klucz pozycji.

Należy pamiętać, że co godzinę serwer/proxy Zabbix ponownie spróbuje pracować z nowym protokołem na wszystkich interfejsach, w razie potrzeby przełączając się z powrotem na stary protokół.

Kontrole aktywne

Kontrole aktywne wymagają bardziej złożonego przetwarzania. agent musi najpierw pobrać z serwera/proxy listę pozycji i/lub zdalnych poleceń do niezależnego przetwarzania.

Serwery/proxy, z których mają być pobierane kontrole aktywne, są wymienione w parametrze ’ServerActive’ w pliku konfiguracyjnym agenta. Częstotliwość odpytywania o te kontrole jest ustawiana przez parametr ’RefreshActiveChecks’ w tym samym pliku

konfiguracyjnym. Jeśli jednak odświeżenie kontroli aktywnych się nie powiedzie, ponowna próba nastąpi po zakodowanych na stałe 60 sekundach.

Note:
Od wersji Zabbix 6.4 agent (w trybie aktywnym) nie otrzymuje już od serwera/proxy pełnej kopii konfiguracji co dwie minuty (domyślnie). Zamiast tego, aby zmniejszyć ruch sieciowy i zużycie zasobów, co 5 sekund (domyślnie) wykonywana jest przyrostowa synchronizacja konfiguracji, podczas której serwer/proxy dostarcza pełną kopię konfiguracji **tylko** wtedy, gdy agent jeszcze jej nie otrzymał lub gdy coś zmieniło się w konfiguracji hosta, makrach globalnych albo globalnych wyrażeniach regularnych.

Agent następnie okresowo wysyła nowe wartości do serwera(ów). Jeśli agent otrzymał jakiekolwiek zdalne polecenia do wykonania, wynik ich wykonania również zostanie wysłany. Należy pamiętać, że wykonywanie zdalnych poleceń na aktywnym agencie jest obsługiwane od Zabbix agent 7.0.

Note:
Jeśli agent znajduje się za zaporą sieciową, warto rozważyć używanie wyłącznie aktywnych kontroli, ponieważ w takim przypadku nie trzeba modyfikować zapory, aby zezwolić na początkowe połączenia przychodzące.

Pobieranie listy pozycji

Żądanie agent

Żądanie active checks służy do pobrania aktywnych kontroli, które mają być przetwarzane przez agent. To żądanie jest wysyłane przez agent przy uruchomieniu, a następnie w odstępach określonych przez RefreshActiveChecks.

```
{
  "request": "active checks",
  "host": "Zabbix server",
  "host_metadata": "mysql,nginx",
  "interface": "zabbix.server.lan",
  "ip": "159.168.1.1",
  "port": 12050,
  "version": "8.0.0",
  "variant": 2,
  "config_revision": 1,
  "session": "e3dcbd9ace2c9694e1d7bbd030eeef6e"
}
```

Field	Type	Mandatory	Value
request	*string*	yes	`active checks`
host	*string*	yes	Nazwa hosta.
host_metadata	*string*	no	Parametr konfiguracyjny HostMetadata lub wartość metryki HostMetadataItem.
interface	*string*	no	Parametr konfiguracyjny HostInterface lub wartość metryki HostInterfaceItem.
ip	*string*	no	Pierwszy adres IP z parametru konfiguracyjnego ListenIP, jeśli jest ustawiony.
port	*number*	no	Wartość parametru konfiguracyjnego ListenPort, jeśli jest ustawiona i nie jest domyślnym portem nasłuchiwania agent.
version	*string*	yes	Numer wersji agent.
variant	*number*	yes	Wariant agent (*1* - Zabbix agent, *2* - Zabbix agent 2).
config_revision	*number*	no	Identyfikator konfiguracji dla przyrostowej synchronizacji konfiguracji.
session	*string*	no	Identyfikator sesji dla przyrostowej synchronizacji konfiguracji.

Odpowiedź serwera

Odpowiedź active checks jest wysyłana przez serwer z powrotem do agent po przetworzeniu żądania active checks.

```
{
  "response": "success",
  "config_revision": 2,
  "data": [
    {
      "key": "system.uptime",
      "itemid": 1234,
      "delay": "10s",
      "lastlogsize": 0,
```

```
      "mtime": 0
    },
    {
      "key": "agent.version",
      "itemid": 5678,
      "delay": "10m",
      "lastlogsize": 0,
      "mtime": 0,
      "timeout": "30s"
    }
  ],
  "commands": [
    {
      "command": "df -h --output=source,size / | awk 'NR>1 {print $2}'",
      "id": 1324,
      "wait": 1
    }
  ]
}
```

Field	Type	Mandatory	Value
response	*string*	yes	`success` | `failed`
info	*string*	no	Informacje o błędzie w przypadku niepowodzenia.
data	*array of objects*	no	Pozycje aktywnych kontroli. Pomijane, jeśli konfiguracja hosta nie uległa zmianie.
key	*string*	no	Klucz pozycji z rozwiniętymi makrami.
itemid	*number*	no	Identyfikator pozycji.
delay	*string*	no	Interwał aktualizacji pozycji. Elastyczne interwały/interwały harmonogramu są obsługiwane zarówno przez Zabbix agent, jak i Zabbix agent 2 od wersji Zabbix 7.0.
lastlogsize	*number*	no	Wartość lastlogsize pozycji.
mtime	*number*	no	Wartość mtime pozycji.
timeout	*string*	no	Timeout pozycji.
refresh_unsupported	*number*	no	Interwał odświeżania nieobsługiwanych pozycji.
regexp	*array of objects*	no	Globalne wyrażenia regularne.
name	*string*	no	Nazwa globalnego wyrażenia regularnego.
expression	*string*	no	Globalne wyrażenie regularne.
expression_type	*number*	no	Typ globalnego wyrażenia regularnego.
exp_delimiter	*string*	no	Separator globalnego wyrażenia regularnego.
case_sensitive	*number*	no	Ustawienie rozróżniania wielkości liter dla globalnego wyrażenia regularnego.
commands	*array of objects*	no	Zdalne polecenia do wykonania. Dołączane, jeśli wykonanie zdalnego polecenia zostało wyzwolone przez operację akcji lub ręczne wykonanie skryptu. Należy pamiętać, że wykonywanie zdalnych poleceń na aktywnym agent jest obsługiwane od Zabbix agent 7.0. Starsze aktywne agenty zignorują wszelkie zdalne polecenia dołączone do odpowiedzi serwera active checks.
command	*string*	no	Zdalne polecenie.
id	*number*	no	Identyfikator zdalnego polecenia.
wait	*number*	no	Tryb wykonania zdalnego polecenia (”0” (nowait) dla poleceń z operacji akcji; ”1” (wait) dla poleceń z ręcznego wykonania skryptu).
config_revision	*number*	no	Identyfikator konfiguracji dla przyrostowej synchronizacji konfiguracji. Pomijany, jeśli konfiguracja hosta nie uległa zmianie. Zwiększany, jeśli konfiguracja hosta uległa zmianie.

Serwer musi odpowiedzieć sukcesem.

Na przykład:

1. Agent otwiera połączenie TCP

2. Agent żąda listy kontroli
3. Serwer odpowiada listą pozycji i zdalnych poleceń do wykonania
4. Agent analizuje odpowiedź
5. Połączenie TCP zostaje zamknięte
6. Agent rozpoczyna okresowe zbieranie danych i wykonuje zdalne polecenia (obsługiwane od Zabbix agent 7.0)

Attention:
Należy pamiętać, że (wrażliwe) dane konfiguracyjne mogą stać się dostępne dla stron mających dostęp do portu trappera serwera Zabbix podczas korzystania z aktywnej kontroli. Jest to możliwe, ponieważ każdy może udawać aktywnego agenta i żądać danych konfiguracyjnych pozycji; uwierzytelnianie nie odbywa się, chyba że używane są opcje szyfrowania.

Wysyłanie zebranych danych

Wysyłanie przez agent

Żądanie danych agenta zawiera zebrane wartości pozycji oraz wartości dla wykonanych zdalnych poleceń (jeśli występują).

```
{
  "request": "agent data",
  "data": [
    {
      "id": 1,
      "itemid": 5678,
      "value": "7.0.0",
      "clock": 1712830783,
      "ns": 76808644
    },
    {
      "id": 2,
      "itemid": 1234,
      "value": "69672",
      "clock": 1712830783,
      "ns": 77053975
    }
  ],
  "commands": [
    {
      "id": 1324,
      "value": "16G"
    }
  ],
  "session": "8495cd52070e6ca52b371f29c8574165",
  "host": "Zabbix server",
  "version": "8.0.0",
  "variant": 2
}
```

Pole	Typ	Wymagane	Wartość
request	*string*	tak	`agent data`
data	*array of objects*	tak	Wartości pozycji.
id	*number*	tak	Identyfikator wartości (inkrementowany licznik używany do sprawdzania zduplikowanych wartości w przypadku problemów z siecią).
itemid	*number*	tak	Identyfikator pozycji.
value	*string*	nie	Wartość pozycji.
lastlogsize	*number*	nie	lastlogsize pozycji.
mtime	*number*	nie	mtime pozycji.
state	*number*	nie	Stan pozycji.
source	*string*	nie	Źródło dziennika zdarzeń wartości.
eventid	*number*	nie	eventid dziennika zdarzeń wartości.
severity	*number*	nie	Poziom ważności dziennika zdarzeń wartości.
timestamp	*number*	nie	Znacznik czasu dziennika zdarzeń wartości.
clock	*number*	tak	Znacznik czasu wartości (sekundy od Epoch).

Pole	Typ	Wymagane	Wartość
ns	*number*	tak	Nanosekundy znacznika czasu wartości.
commands	*array of objects*	nie	Wynik wykonania zdalnych poleceń. Należy pamiętać, że wykonywanie zdalnych poleceń na aktywnym agencie jest obsługiwane od Zabbix agent 7.0. Starsze aktywne agenty zignorują wszelkie zdalne polecenia zawarte w odpowiedzi serwera aktywnych testów.
id	*number*	nie	Identyfikator zdalnego polecenia.
value	*string*	nie	Wynik wykonania zdalnego polecenia, jeśli wykonanie zakończyło się powodzeniem.
error	*string*	nie	Komunikat błędu wykonania zdalnego polecenia, jeśli wykonanie się nie powiodło.
session	*string*	tak	Unikalny identyfikator sesji generowany przy każdym uruchomieniu agent.
host	*string*	tak	Nazwa hosta.
version	*string*	tak	Numer wersji agent.
variant	*number*	tak	Wariant agent (*1* - Zabbix agent, *2* - Zabbix agent 2).

Wirtualny identyfikator jest przypisywany do każdej wartości. Identyfikator wartości to prosty rosnący licznik, unikalny w obrębie jednej sesji danych (identyfikowanej przez token sesji). Ten identyfikator służy do odrzucania zduplikowanych wartości, które mogą zostać wysłane w środowiskach o słabej łączności.

Odpowiedź serwera

Odpowiedź na dane agenta jest wysyłana przez serwer z powrotem do agent po przetworzeniu żądania danych agenta.

```
{
  "response": "success",
  "info": "processed: 2; failed: 0; total: 2; seconds spent: 0.003534"
}
```

Pole	Typ	Wymagane	Wartość
response	*string*	tak	`success` | `failed`
info	*string*	tak	Wyniki przetwarzania pozycji.

Attention:
Jeśli wysyłanie niektórych wartości nie powiedzie się po stronie serwera (na przykład dlatego, że host lub pozycja zostały wyłączone albo usunięte), agent nie podejmie ponownej próby wysłania tych wartości.

Na przykład:

1. Agent otwiera połączenie TCP
2. Agent wysyła listę wartości
3. Serwer przetwarza dane i odsyła status
4. Połączenie TCP zostaje zamknięte

Attention:
Komunikat błędu zostanie przycięty do 2048 znaków po stronie serwera.

Wiadomość heartbeat

Agent wysyła

Wiadomość heartbeat jest wysyłana przez aktywnego agenta do serwera/proxy Zabbix co HeartbeatFrequency sekund (skonfigurowane w pliku konfiguracyjnym Zabbix agent/ agent 2).

Jest używana do monitorowania dostępności aktywnych kontroli.

```
{
  "request": "active check heartbeat",
  "host": "Zabbix server",
  "heartbeat_freq": 60,
  "version": "8.0.0",
  "variant": 2
}
```

Pole	Typ	Obowiązkowe	Wartość
request	*string*	tak	`active check heartbeat`
host	*string*	tak	Nazwa hosta.
heartbeat_freq	*number*	tak	Częstotliwość heartbeat agenta (parametr konfiguracyjny HeartbeatFrequency).
version	*string*	tak	Numer wersji agenta.
variant	*number*	tak	Wariant agenta (*1* - Zabbix agent, *2* - Zabbix agent 2).

Odpowiedź przekierowująca

Gdy host został ponownie przypisany, serwer może polecić agentowi przekierowanie heartbeat (oraz kolejnych aktywnych kontroli) do innej instancji proxy lub serwera.

```
{
  "response": "failed",
  "redirect": {
    "revision": 2,
    "address": "192.0.2.0:10055"
  }
}
```

Pole		Typ	Obowiązkowe	Wartość
response		*string*	tak	`success` | `failed`
redirect		*object*	tak	Instrukcje przekierowania.
	revision	*number*	tak	Identyfikator rewizji konfiguracji.
	address	*string*	tak	Adres docelowego serwera/proxy.

Starszy protokół XML

Note:
Zabbix przyjmie do 16 MB danych XML zakodowanych w Base64, ale pojedyncza zdekodowana wartość nie powinna być dłuższa niż 64 KB, w przeciwnym razie zostanie obcięta do 64 KB podczas dekodowania.

3 Minimalny poziom uprawnień dla pozycji agenta Windows

Przegląd

Podczas monitorowania systemów przy użyciu agent, dobrą praktyką jest pozyskiwanie metryk z host, na którym agent jest zainstalowany. Aby stosować zasadę najmniejszych uprawnień, konieczne jest określenie, jakie metryki są pozyskiwane przez agent.

Tabela w tym dokumencie umożliwia wybór minimalnych uprawnień gwarantujących poprawne działanie Zabbix agent.

Jeśli do działania agent wybrano innego użytkownika niż „LocalSystem", to aby agent działał jako usługa systemu Windows, nowy użytkownik musi mieć uprawnienie „Log on as a service" w „Local Policy→User Rights Assignment" oraz prawo do tworzenia, zapisywania i usuwania pliku dziennika Zabbix agent. Użytkownik Active Directory musi zostać dodany do grupy *Performance Monitor Users*.

Note:
W przypadku pracy z uprawnieniami agent opartymi na grupie „minimalnie technicznie akceptowalnej" wymagane jest wcześniejsze nadanie uprawnień do obiektów przeznaczonych do monitorowania.

Typowe pozycje agenta obsługiwane w systemie Windows

Klucz pozycji	Grupa użytkowników	
	Zalecane	Minimalne technicznie akceptowalne (funkcjonalność jest ograniczona)
agent.hostname	Goście	Goście
agent.ping	Goście	Goście
agent.variant	Goście	Goście
agent.version	Goście	Goście
log	Administratorzy	Goście
log.count	Administratorzy	Goście
logrt	Administratorzy	Goście
logrt.count	Administratorzy	Goście
net.dns	Goście	Goście
net.dns.perf	Goście	Goście
net.dns.record	Goście	Goście
net.if.discovery	Goście	Goście
net.if.in	Goście	Goście
net.if.out	Goście	Goście
net.if.total	Goście	Goście
net.tcp.listen	Goście	Goście
net.tcp.port	Goście	Goście
net.tcp.service	Goście	Goście
net.tcp.service.perf	Goście	Goście
net.udp.service	Goście	Goście
net.udp.service.perf	Goście	Goście
proc.num	Administratorzy	Goście
system.cpu.discovery	Użytkownicy monitora wydajności	Użytkownicy monitora wydajności
system.cpu.load	Użytkownicy monitora wydajności	Użytkownicy monitora wydajności
system.cpu.num	Goście	Goście
system.cpu.util	Użytkownicy monitora wydajności	Użytkownicy monitora wydajności
system.hostname	Goście	Goście
system.localtime	Goście	Goście
system.run	Administratorzy	Goście
system.sw.arch	Goście	Goście
system.swap.size	Goście	Goście
system.uname	Goście	Goście
system.uptime	Użytkownicy monitora wydajności	Użytkownicy monitora wydajności
vfs.dir.count	Administratorzy	Goście
vfs.dir.get	Administratorzy	Goście

Klucz pozycji	Grupa użytkowników	
vfs.dir.size	Administratorzy	Goście
vfs.file.cksum	Administratorzy	Goście
vfs.file.contents	Administratorzy	Goście
vfs.file.exists	Administratorzy	Goście
vfs.file.md5sum	Administratorzy	Goście
vfs.file.regexp	Administratorzy	Goście
vfs.file.regmatch	Administratorzy	Goście
vfs.file.size	Administratorzy	Goście
vfs.file.time	Administratorzy	Goście
vfs.fs.discovery	Administratorzy	Goście
vfs.fs.size	Administratorzy	Goście
vfs.fs.get	Administratorzy	Goście
vm.memory.size	Goście	Goście
web.page.get	Goście	Goście
web.page.perf	Goście	Goście
web.page.regexp	Goście	Goście
zabbix.stats	Goście	Goście

Klucze pozycji specyficzne dla systemu Windows

Klucz pozycji	Grupa użytkowników	
	Zalecane	Minimalne technicznie akceptowalne (funkcjonalność jest ograniczona)
eventlog	Czytelnicy dziennika zdarzeń	Goście
net.if.list	Goście	Goście
perf_counter	Użytkownicy monitora wydajności	Użytkownicy monitora wydajności
proc_info	Administratorzy	Goście
service.discovery	Goście	Goście
service.info	Goście	Goście
services	Goście	Goście
wmi.get	Administratorzy	Goście
vm.vmemory.size	Goście	Goście

4 Kodowanie zwracanych wartości

Serwer Zabbix oczekuje, że każda zwracana wartość tekstowa będzie w kodowaniu UTF8. Dotyczy to wszystkich typów kontroli: Zabbix agent, SSH, Telnet itd.

Różne monitorowane systemy/urządzenia i kontrole mogą zwracać w wartości znaki spoza ASCII. W takich przypadkach prawie wszystkie możliwe klucze **zabbix** zawierają dodatkowy parametr klucza pozycji - **<encoding>**. Ten parametr klucza jest opcjonalny, ale należy go określić, jeśli zwracana wartość nie jest w kodowaniu UTF8 i zawiera znaki spoza ASCII. W przeciwnym razie wynik może być nieoczekiwany i nieprzewidywalny.

Poniżej znajduje się opis zachowania w takich przypadkach dla różnych backendów baz danych.

MySQL

Jeśli wartość zawiera znak spoza ASCII w kodowaniu innym niż UTF8, ten znak oraz kolejne zostaną odrzucone podczas zapisywania tej wartości w bazie danych. Żadne komunikaty ostrzegawcze nie zostaną zapisane w pliku *zabbix_server.log*.

Dotyczy co najmniej wersji MySQL 5.1.61

PostgreSQL

Jeśli wartość zawiera znak spoza ASCII w kodowaniu innym niż UTF8, doprowadzi to do nieudanego zapytania SQL (PGRES_FATAL_ERROR:ERROR invalid byte sequence for encoding), a dane nie zostaną zapisane. Odpowiedni komunikat ostrzegawczy zostanie zapisany w pliku *zabbix_server.log*.
Dotyczy co najmniej PostgreSQL w wersji 9.1.3

5 Obsługa dużych plików

Obsługa dużych plików, często skracana do LFS, to termin odnoszący się do możliwości pracy z plikami większymi niż 2 GB w 32-bitowych systemach operacyjnych. Obsługa dużych plików wpływa co najmniej na monitorowanie plików dziennika oraz wszystkie pozycje vfs.file.*. Obsługa dużych plików zależy od możliwości systemu w czasie kompilacji Zabbix, ale jest całkowicie wyłączona w 32-bitowym Solarisie ze względu na niezgodność z procfs i swapctl.

6 Czujnik

Przegląd

Każdy układ czujnika ma własny katalog w drzewie sysfs `/sys/devices`. Aby znaleźć wszystkie układy czujników, łatwiej jest śledzić dowiązania symboliczne urządzeń z `/sys/class/hwmon/hwmon*`, gdzie `*` jest liczbą rzeczywistą (0,1,2,...).

Odczyty czujników znajdują się albo w katalogu `/sys/class/hwmon/hwmon*/` dla urządzeń wirtualnych, albo w katalogu `/sys/class/hwmon/hwmon*/device` dla urządzeń niewirtualnych. Plik o nazwie `name`, znajdujący się w katalogach `hwmon*` lub `hwmon*/device`, zawiera nazwę układu, która odpowiada nazwie sterownika jądra używanego przez układ czujnika.

W każdym pliku znajduje się tylko jedna wartość odczytu czujnika. Wspólny schemat nazewnictwa plików zawierających odczyty czujników wewnątrz dowolnego z wyżej wymienionych katalogów to: `<type><number>_<item>`, gdzie

- **type** - dla układów czujników jest to ”in” (napięcie), ”temp” (temperatura), ”fan” (wentylator) itd.
- **item** - ”input” (wartość zmierzona), ”max” (górny próg), ”min” (dolny próg) itd.
- **number** - zawsze używany dla elementów, które mogą występować więcej niż raz (zwykle zaczyna się od 1, z wyjątkiem napięć, które zaczynają się od 0). Jeśli pliki nie odnoszą się do konkretnego elementu, mają prostą nazwę bez numeru.

Informacje dotyczące czujników dostępnych na hoście można uzyskać za pomocą narzędzi **sensors-detect** i **sensors** (pakiet lm-sensors). **Sensors-detect** pomaga określić, które moduły są wymagane dla dostępnych czujników. Po załadowaniu modułów program **sensors** może zostać użyty do wyświetlenia odczytów wszystkich układów czujników. Etykiety odczytów czujników używane przez ten program mogą różnić się od wspólnego schematu nazewnictwa (`<type><number>_<item>`):

- jeśli istnieje plik o nazwie `<type><number>_label`, wtedy etykieta z tego pliku zostanie użyta zamiast nazwy `<type><number><item>`;
- jeśli nie ma pliku `<type><number>_label`, program przeszukuje `/etc/sensors.conf` (może to być także `/etc/sensors3.conf` lub inny plik) pod kątem podstawienia nazwy.

To etykietowanie pozwala użytkownikowi określić, jaki rodzaj sprzętu jest używany. Jeśli nie ma ani pliku `<type><number>_label`, ani etykiety w pliku konfiguracyjnym, typ sprzętu można określić na podstawie atrybutu name (`hwmon*/device/name`). Rzeczywiste nazwy czujników akceptowane przez `zabbix_agent` można uzyskać, uruchamiając program **sensors** z parametrem `-u` (`sensors -u`).

W programie **sensors** dostępne czujniki są rozdzielone według typu magistrali (adapter ISA, adapter PCI, adapter SPI, urządzenie wirtualne, interfejs ACPI, adapter HID).

Uzyskiwanie identyfikatorów sensorów

Etykiety sensorów, wyświetlane przez polecenie `sensors`, nie zawsze mogą być używane bezpośrednio, ponieważ sposób etykietowania różni się w zależności od producenta układu. Na przykład dane wyjściowe `sensors` mogą zawierać następujące wiersze:

```
sensors
in0:         +2.24 V  (min =  +0.00 V, max =  +3.32 V)
Vcore:       +1.15 V  (min =  +0.00 V, max =  +2.99 V)
+3.3V:       +3.30 V  (min =  +2.97 V, max =  +3.63 V)
+12V:       +13.00 V  (min =  +0.00 V, max = +15.94 V)
M/B Temp:    +30.0°C  (low  = -127.0°C, high = +127.0°C)
```

Spośród nich tylko jedna nazwa wyświetlana odpowiada bezpośrednio identyfikatorowi wewnętrznemu:

```
zabbix_get -s 127.0.0.1 -k sensor[lm85-i2c-0-2e,in0]
2.240000
```

Próba użycia innych etykiet wyświetlanych (takich jak Vcore lub +12V) nie zadziała:

```
zabbix_get -s 127.0.0.1 -k sensor[lm85-i2c-0-2e,Vcore]
ZBX_NOTSUPPORTED
```

Aby znaleźć wewnętrzny identyfikator sensora akceptowany przez Zabbix, uruchom `sensors -u`. W danych wyjściowych można zaobserwować następujące elementy:

```
sensors -u
...
Vcore:
  in1_input: 1.15
  in1_min: 0.00
  in1_max: 2.99
  in1_alarm: 0.00
...
+12V:
  in4_input: 13.00
  in4_min: 0.00
  in4_max: 15.94
  in4_alarm: 0.00
...
```

Zatem etykieta Vcore odpowiada identyfikatorowi in1, a +12V odpowiada in4. Zgodnie ze specyfikacją kernel hwmon sysfs są to napięcia na pinach układu i ogólnie rzecz biorąc mogą wymagać skalowania.

```
zabbix_get -s 127.0.0.1 -k sensor[lm85-i2c-0-2e,in1]
1.301000
```

Zabbix może pobierać nie tylko odczyty napięcia (in), ale także natężenia prądu (curr), temperatury (temp) i prędkości wentylatora (fan).

Zgodność

Starsze dystrybucje

Odczyty czujników są pobierane z katalogu /proc/sys/dev/sensors:

- **device** - nazwa urządzenia (jeśli użyto <mode>, jest to wyrażenie regularne)
- **sensor** - nazwa czujnika (jeśli użyto <mode>, jest to wyrażenie regularne)
- **mode** - możliwe wartości: avg, max, min (jeśli ten parametr zostanie pominięty, device i sensor są traktowane dosłownie)

Przykładowy klucz: sensor[w83781d-i2c-0-2d,temp1].

Bieżące dystrybucje

Odczyty sensorów są pobierane z katalogu /sys/class/hwmon:

- **device** - nazwa urządzenia (bez wyrażeń regularnych). Nazwa urządzenia może być rzeczywistą nazwą urządzenia (np. 0000:00:18.3) lub nazwą uzyskaną za pomocą programu sensors (np. k8temp-pci-00c3). Wybór, której nazwy użyć, należy do użytkownika.
- **sensor** - nazwa sensora (bez wyrażeń regularnych).
- **mode** - możliwe wartości: avg, max, min (jeśli ten parametr zostanie pominięty, device i sensor są traktowane dosłownie).

Przykładowe klucze:

sensor[k8temp-pci-00c3,temp,max] lub sensor[0000:00:18.3,temp1].

sensor[smsc47b397-isa-0880,in,avg] lub sensor[smsc47b397.2176,in1].

7 Uwagi dotyczące parametru memtype w pozycjach proc.mem

Przegląd

Parametr **memtype** jest obsługiwany na platformach Linux, AIX, FreeBSD i Solaris.

Trzy typowe wartości parametru „memtype" są obsługiwane na wszystkich tych platformach: pmem, rss i vsize. Dodatkowo na niektórych platformach obsługiwane są specyficzne dla platformy wartości parametru „memtype".

AIX

Zobacz wartości obsługiwane dla parametru „memtype" w systemie AIX w tabeli.

Obsługiwana wartość	Opis	Źródło w strukturze procentry64	Próbuje zachować zgodność z
vsize [1]	Rozmiar pamięci wirtualnej	pi_size	
pmem	Procent pamięci rzeczywistej	pi_prm	ps -o pmem
rss	Rozmiar rezydentnego zestawu pamięci	pi_trss + pi_drss	ps -o rssize
size	Rozmiar procesu (kod + dane)	pi_dvm	”ps gvw” kolumna SIZE
dsize	Rozmiar danych	pi_dsize	
tsize	Rozmiar tekstu (kodu)	pi_tsize	”ps gvw” kolumna TSIZ
sdsize	Rozmiar danych z biblioteki współdzielonej	pi_sdsize	
drss	Rozmiar rezydentnego zestawu danych	pi_drss	
trss	Rozmiar rezydentnego zestawu tekstu	pi_trss	

Uwagi dotyczące AIX:

1. Wybierając parametry dla klucza pozycji proc.mem[] w AIX, postaraj się określić wąskie kryteria wyboru procesów. W przeciwnym razie istnieje ryzyko, że do wyniku proc.mem[] zostaną wliczone niepożądane procesy.

Przykład:

```
$ zabbix_agentd -t proc.mem[,,,NonExistingProcess,rss]
proc.mem[,,,NonExistingProcess,rss]           [u|2879488]
```

Ten przykład pokazuje, że podanie tylko parametru wiersza poleceń (wyrażenia regularnego do dopasowania) powoduje samouzględnianie przez Zabbix agent — prawdopodobnie nie jest to oczekiwane zachowanie.

2. Nie używaj `ps -ef` do przeglądania procesów — pokazuje ono tylko procesy niejądrowe. Użyj `ps -Af`, aby zobaczyć wszystkie procesy, które będą widoczne dla Zabbix agent.
3. Przejdźmy przez przykład `topasrec`, aby zobaczyć, jak Zabbix agent `proc.mem[]` wybiera procesy.

```
$ ps -Af | grep topasrec
root 10747984        1   0   Mar 16      -  0:00 /usr/bin/topasrec  -L -s 300 -R 1 -r 6 -o /var/perf daily
```

`proc.mem[]` ma argumenty:

```
proc.mem[<name>,<user>,<mode>,<cmdline>,<memtype>]
```

Pierwszym kryterium jest nazwa procesu (argument <name>). W naszym przykładzie agent Zabbix zobaczy ją jako ’topasrec’. Aby dopasowanie zadziałało, należy albo podać ’topasrec’, albo pozostawić to pole puste. Drugim kryterium jest nazwa użytkownika (argument <user>). Aby dopasowanie zadziałało, należy albo podać ’root’, albo pozostawić to pole puste. Trzecim kryterium używanym przy wyborze procesu jest argument <cmdline>. agent Zabbix zobaczy jego wartość jako ’/usr/bin/topasrec -L -s 300 -R 1 -r 6 -o /var/perf/daily/ -ypersistent=1 -O type=bin -ystart_time=04:08:54,Mar16,2023’. Aby dopasowanie zadziałało, należy albo podać wyrażenie regularne pasujące do tego ciągu, albo pozostawić to pole puste.

Argumenty <mode> i <memtype> są stosowane po użyciu trzech kryteriów wymienionych powyżej.

FreeBSD

Zobacz wartości obsługiwane dla parametru ’memtype’ w systemie FreeBSD w tabeli.

Obsługiwana wartość	Opis	Źródło w strukturze kinfo_proc	Próbuje zachować zgodność z
vsize	Rozmiar pamięci wirtualnej	kp_eproc.e_vm.vm_map.size lub ki_size	ps -o vsz
pmem	Procent pamięci rzeczywistej	obliczany na podstawie rss	ps -o pmem
rss	Rozmiar zestawu rezydentnego	kp_eproc.e_vm.vm_rssize lub ki_rssize	ps -o rss
size [1]	Rozmiar procesu (kod + dane + stos)	tsize + dsize + ssize	
tsize	Rozmiar tekstu (kodu)	kp_eproc.e_vm.vm_tsize lub ki_tsize	ps -o tsiz
dsize	Rozmiar danych	kp_eproc.e_vm.vm_dsize lub ki_dsize	ps -o dsiz

Obsługiwana wartość	Opis	Źródło w strukturze kinfo_proc	Próbuje zachować zgodność z
ssize	Rozmiar stosu	kp_eproc.e_vm.vm_ssize lub ki_ssize	ps -o ssiz

Linux

Obsługiwane wartości parametru „memtype” w systemie Linux przedstawiono w tabeli.

Obsługiwana wartość	Opis	Źródło w pliku /proc/<pid>/status
vsize [1]	Rozmiar pamięci wirtualnej	VmSize
pmem	Procent pamięci rzeczywistej	(VmRSS/total_memory) * 100
rss	Rozmiar zestawu rezydentnego	VmRSS
data	Rozmiar segmentu danych	VmData
exe	Rozmiar segmentu kodu	VmExe
hwm	Szczytowy rozmiar zestawu rezydentnego	VmHWM
lck	Rozmiar zablokowanej pamięci	VmLck
lib	Rozmiar bibliotek współdzielonych	VmLib
peak	Szczytowy rozmiar pamięci wirtualnej	VmPeak
pin	Rozmiar przypiętych stron	VmPin
pte	Rozmiar wpisów tablic stron	VmPTE
size	Rozmiar segmentów kodu + danych + stosu procesu	VmExe + VmData + VmStk
stk	Rozmiar segmentu stosu	VmStk
swap	Rozmiar używanej przestrzeni wymiany	VmSwap

Uwagi dotyczące systemu Linux:

1. Nie wszystkie wartości „memtype” są obsługiwane przez starsze jądra Linux. Na przykład jądra Linux 2.4 nie obsługują wartości `hwm`, `pin`, `peak`, `pte` i `swap`.
2. Zauważyliśmy, że samomonitorowanie procesu aktywnego sprawdzania agenta Zabbix za pomocą `proc.mem[...,...,...,...,dat` pokazuje wartość o 4 kB większą niż raportowana przez wiersz `VmData` w pliku /proc/<pid>/status agenta. W momencie samopomiaru segment danych agenta zwiększa się o 4 kB, a następnie wraca do poprzedniego rozmiaru.

Solaris

Zobacz wartości obsługiwane dla parametru „memtype” w systemie Solaris w tabeli.

Obsługiwana wartość	Opis	Źródło w strukturze psinfo	Próbuje zachować zgodność z
vsize [1]	Rozmiar obrazu procesu	pr_size	ps -o vsz
pmem	Procent pamięci rzeczywistej	pr_pctmem	ps -o pmem
rss	Rozmiar rezydentnego zestawu stron Może być zaniżony — zobacz opis rss w „man ps”.	pr_rssize	ps -o rss

Przypisy

1 Wartość domyślna.

8 Uwagi dotyczące wybierania procesów w pozycjach proc.mem i proc.num

Procesy modyfikujące swoją linię poleceń

Niektóre programy wykorzystują modyfikowanie swojej linii poleceń jako metodę wyświetlania bieżącej aktywności. Użytkownik może zobaczyć tę aktywność, uruchamiając polecenia `ps` i `top`. Przykładami takich programów są *PostgreSQL*, *Sendmail*, *Zabbix*.

Zobaczmy przykład z Linuksa. Załóżmy, że chcemy monitorować liczbę procesów Zabbix agent.

Polecenie `ps` pokazuje interesujące nas procesy jako

```
$ ps -fu zabbix
UID        PID  PPID  C STIME TTY          TIME CMD
...
zabbix    6318     1  0 12:01 ?        00:00:00 sbin/zabbix_agentd -c /home/zabbix/zabbix_agentd.conf
zabbix    6319  6318  0 12:01 ?        00:00:01 sbin/zabbix_agentd: collector [idle 1 sec]
zabbix    6320  6318  0 12:01 ?        00:00:00 sbin/zabbix_agentd: listener #1 [waiting for connection]
zabbix    6321  6318  0 12:01 ?        00:00:00 sbin/zabbix_agentd: listener #2 [waiting for connection]
zabbix    6322  6318  0 12:01 ?        00:00:00 sbin/zabbix_agentd: listener #3 [waiting for connection]
zabbix    6323  6318  0 12:01 ?        00:00:00 sbin/zabbix_agentd: active checks #1 [idle 1 sec]
...
```

Wybieranie procesów według nazwy i użytkownika działa:

```
$ zabbix_get -s localhost -k 'proc.num[zabbix_agentd,zabbix]'
6
```

Teraz zmieńmy nazwę pliku wykonywalnego zabbix_agentd na zabbix_agentd_30 i uruchommy go ponownie.

ps pokazuje teraz

```
$ ps -fu zabbix
UID        PID  PPID  C STIME TTY          TIME CMD
...
zabbix    6715     1  0 12:53 ?        00:00:00 sbin/zabbix_agentd_30 -c /home/zabbix/zabbix_agentd.conf
zabbix    6716  6715  0 12:53 ?        00:00:00 sbin/zabbix_agentd_30: collector [idle 1 sec]
zabbix    6717  6715  0 12:53 ?        00:00:00 sbin/zabbix_agentd_30: listener #1 [waiting for connection
zabbix    6718  6715  0 12:53 ?        00:00:00 sbin/zabbix_agentd_30: listener #2 [waiting for connection
zabbix    6719  6715  0 12:53 ?        00:00:00 sbin/zabbix_agentd_30: listener #3 [waiting for connection
zabbix    6720  6715  0 12:53 ?        00:00:00 sbin/zabbix_agentd_30: active checks #1 [idle 1 sec]
...
```

Teraz wybieranie procesów według nazwy i użytkownika daje niepoprawny wynik:

```
$ zabbix_get -s localhost -k 'proc.num[zabbix_agentd_30,zabbix]'
1
```

Dlaczego zwykła zmiana nazwy pliku wykonywalnego na dłuższą prowadzi do tak odmiennego wyniku?

Zabbix agent zaczyna od sprawdzenia nazwy procesu. Otwierany jest plik /proc/<pid>/status i sprawdzany jest wiersz Name. W naszym przypadku wiersze Name są następujące:

```
$ grep Name /proc/{6715,6716,6717,6718,6719,6720}/status
/proc/6715/status:Name:   zabbix_agentd_3
/proc/6716/status:Name:   zabbix_agentd_3
/proc/6717/status:Name:   zabbix_agentd_3
/proc/6718/status:Name:   zabbix_agentd_3
/proc/6719/status:Name:   zabbix_agentd_3
/proc/6720/status:Name:   zabbix_agentd_3
```

Nazwa procesu w pliku status jest obcinana do 15 znaków.

Podobny wynik można zobaczyć przy użyciu polecenia ps:

```
$ ps -u zabbix
  PID TTY          TIME CMD
...
 6715 ?        00:00:00 zabbix_agentd_3
 6716 ?        00:00:01 zabbix_agentd_3
 6717 ?        00:00:00 zabbix_agentd_3
 6718 ?        00:00:00 zabbix_agentd_3
 6719 ?        00:00:00 zabbix_agentd_3
 6720 ?        00:00:00 zabbix_agentd_3
 ...
```

Oczywiście nie jest to równe wartości parametru name proc.num[], czyli zabbix_agentd_30. Po nieudanej próbie dopasowania nazwy procesu z pliku status Zabbix agent przechodzi do pliku /proc/<pid>/cmdline.

To, jak agent widzi plik „cmdline”, można zilustrować, uruchamiając polecenie

```
$ for i in 6715 6716 6717 6718 6719 6720; do cat /proc/$i/cmdline | awk '{gsub(/\x0/,"<NUL>"); print};'; d
sbin/zabbix_agentd_30<NUL>-c<NUL>/home/zabbix/zabbix_agentd.conf<NUL>
```

```
sbin/zabbix_agentd_30: collector [idle 1 sec]<NUL><NUL><NUL><NUL><NUL><NUL><NUL><NUL><NUL><NUL><NUL><NUL><
sbin/zabbix_agentd_30: listener #1 [waiting for connection]<NUL><NUL><NUL><NUL><NUL><NUL><NUL><NUL><NUL><N
sbin/zabbix_agentd_30: listener #2 [waiting for connection]<NUL><NUL><NUL><NUL><NUL><NUL><NUL><NUL><NUL><N
sbin/zabbix_agentd_30: listener #3 [waiting for connection]<NUL><NUL><NUL><NUL><NUL><NUL><NUL><NUL><NUL><N
sbin/zabbix_agentd_30: active checks #1 [idle 1 sec]<NUL><NUL><NUL><NUL><NUL><NUL><NUL><NUL><NUL><NUL><NUL
```

Pliki `/proc/<pid>/cmdline` w naszym przypadku zawierają niewidoczne, niedrukowalne bajty null, używane do kończenia łańcuchów w języku *C*. W tym przykładzie bajty null są pokazane jako „<NUL>”.

Zabbix agent sprawdza „cmdline” dla procesu głównego i pobiera `zabbix_agentd_30`, co odpowiada wartości naszego parametru `name` `zabbix_agentd_30`. Dlatego proces główny jest zliczany przez pozycja `proc.num[zabbix_agentd_30,zabbix]`.

Podczas sprawdzania kolejnego procesu agent pobiera `zabbix_agentd_30: collector [idle 1 sec]` z pliku `cmdline` i nie spełnia to warunku naszego parametru `name` `zabbix_agentd_30`. Zatem zliczany jest tylko proces główny, który nie modyfikuje swojej linii poleceń. Pozostałe procesy agent modyfikują swoją linię poleceń i są ignorowane.

Ten przykład pokazuje, że parametr `name` nie może być używany w `proc.mem[]` i `proc.num[]` do wybierania procesów w takim przypadku.

Note:
Dla pozycja `proc.get[]`, gdy Zabbix agent sprawdza „cmdline” pod kątem nazwy procesu, użyje tylko tej części nazwy, która zaczyna się od ostatniego ukośnika i kończy na pierwszej spacji lub dwukropku. Nazwa procesu pobrana z pliku cmdline zostanie użyta tylko wtedy, gdy jej początek całkowicie odpowiada skróconej nazwie procesu w pliku `status`. Algorytm jest taki sam zarówno dla nazwy procesu w filtrze, jak i w wyjściu JSON.

Użycie parametru `cmdline` z odpowiednim wyrażeniem regularnym daje poprawny wynik:

```
$ zabbix_get -s localhost -k 'proc.num[,zabbix,,zabbix_agentd_30[ :]]'
6
```

Zachowaj ostrożność podczas używania pozycji `proc.get[]`, `proc.mem[]` i `proc.num[]` do monitorowania programów, które modyfikują swoje linie poleceń.

Przed wstawieniem parametrów `name` i `cmdline` do pozycji `proc.get[]`, `proc.mem[]` i `proc.num[]` możesz chcieć przetestować te parametry przy użyciu pozycji `proc.num[]` i polecenia `ps`.

Wątki jądra Linux

W pozycjach `proc.get[]`, `proc.mem[]` i `proc.num[]` nie można wybierać wątków za pomocą parametru `cmdline`

Jako przykład weźmy jeden z wątków jądra:

```
$ ps -ef| grep kthreadd
root         2     0  0 09:33 ?        00:00:00 [kthreadd]
```

Można go wybrać za pomocą parametru `name` procesu:

```
$ zabbix_get -s localhost -k 'proc.num[kthreadd,root]'
1
```

Jednak wybieranie według parametru `cmdline` procesu nie działa:

```
$ zabbix_get -s localhost -k 'proc.num[,root,,kthreadd]'
0
```

Powodem jest to, że agent Zabbix pobiera wyrażenie regularne określone w parametrze `cmdline` i stosuje je do zawartości pliku procesu `/proc/<pid>/cmdline`. W przypadku wątków jądra ich pliki `/proc/<pid>/cmdline` są puste. Dlatego parametr `cmdline` nigdy nie pasuje.

Zliczanie wątków w pozycjach `proc.mem[]` i `proc.num[]`

Wątki jądra Linux są zliczane przez pozycję `proc.num[]`, ale nie raportują pamięci w pozycji `proc.mem[]`. Na przykład:

```
$ ps -ef | grep kthreadd
root         2     0  0 09:51 ?        00:00:00 [kthreadd]

$ zabbix_get -s localhost -k 'proc.num[kthreadd]'
1

$ zabbix_get -s localhost -k 'proc.mem[kthreadd]'
ZBX_NOTSUPPORTED: Cannot get amount of "VmSize" memory.
```

Ale co się stanie, jeśli istnieje proces użytkownika o tej samej nazwie co wątek jądra? Wtedy może to wyglądać tak:

```
$ ps -ef | grep kthreadd
root         2     0  0 09:51 ?        00:00:00 [kthreadd]
zabbix    9611  6133  0 17:58 pts/1    00:00:00 ./kthreadd

$ zabbix_get -s localhost -k 'proc.num[kthreadd]'
2

$ zabbix_get -s localhost -k 'proc.mem[kthreadd]'
4157440
```

`proc.num[]` zliczył zarówno wątek jądra, jak i proces użytkownika. `proc.mem[]` raportuje pamięć tylko dla procesu użytkownika i traktuje pamięć wątku jądra tak, jakby wynosiła 0. Różni się to od przypadku powyżej, gdy zgłaszane było ZBX_NOTSUPPORTED.

Zachowaj ostrożność podczas używania pozycji `proc.mem[]` i `proc.num[]`, jeśli nazwa programu przypadkowo odpowiada nazwie jednego z wątków.

Przed wstawieniem parametrów do pozycji `proc.mem[]` i `proc.num[]` warto przetestować parametry za pomocą pozycji `proc.num[]` oraz polecenia `ps`.

9 Szczegóły implementacji kontroli net.tcp.service i net.udp.service

Implementacja kontroli net.tcp.service i net.udp.service została szczegółowo opisana na tej stronie dla różnych usług określonych w parametrze service.

Parametry pozycji net.tcp.service

ftp

Tworzy połączenie TCP i oczekuje, że pierwsze 4 znaki odpowiedzi będą równe ”220 ”, a następnie wysyła ”QUIT\r\n”. Jeśli nie określono portu, używany jest domyślny port 21.

http

Tworzy połączenie TCP bez oczekiwania i wysyłania czegokolwiek. Jeśli nie określono portu, używany jest domyślny port 80.

https

Używa biblioteki libcurl (i działa wyłącznie z nią), nie weryfikuje autentyczności certyfikatu, nie weryfikuje nazwy hosta w certyfikacie SSL, pobiera jedynie nagłówek odpowiedzi (żądanie HEAD). Jeśli nie określono portu, używany jest domyślny port 443.

imap

Tworzy połączenie TCP i oczekuje, że pierwsze 4 znaki odpowiedzi będą równe ”* OK”, a następnie wysyła ”a1 LOGOUT\r\n”. Jeśli nie określono portu, używany jest domyślny port 143.

ldap

Otwiera połączenie z serwerem LDAP i wykonuje operację wyszukiwania LDAP z filtrem ustawionym na (objectClass=*). Oczekuje pomyślnego pobrania pierwszego atrybutu pierwszego wpisu. Jeśli nie określono portu, używany jest domyślny port 389.

nntp

Tworzy połączenie TCP i oczekuje, że pierwsze 3 znaki odpowiedzi będą równe ”200” lub ”201”, a następnie wysyła ”QUIT\r\n”. Jeśli nie określono portu, używany jest domyślny port 119.

pop

Tworzy połączenie TCP i oczekuje, że pierwsze 3 znaki odpowiedzi będą równe ”+OK”, a następnie wysyła ”QUIT\r\n”. Jeśli nie określono portu, używany jest domyślny port 110.

smtp

Tworzy połączenie TCP i oczekuje, że pierwsze 3 znaki odpowiedzi będą równe ”220”, po których następuje spacja, znak końca linii lub myślnik. Linie zawierające myślnik należą do odpowiedzi wielowierszowej i odpowiedź będzie odczytywana ponownie aż do otrzymania linii bez myślnika. Następnie wysyła ”QUIT\r\n”. Jeśli nie określono portu, używany jest domyślny port 25.

ssh

Tworzy połączenie TCP. Jeśli połączenie zostało ustanowione, obie strony wymieniają ciąg identyfikacyjny (SSH-major.minor-XXXX), gdzie major i minor to wersje protokołu, a XXXX to ciąg znaków. Zabbix sprawdza, czy znaleziono ciąg zgodny ze specyfikacją, a następnie odsyła ciąg ”SSH-major.minor-zabbix_agent\r\n” lub ”0\n” w przypadku niezgodności. Jeśli nie określono portu, używany jest domyślny port 22.

tcp

Tworzy połączenie TCP bez oczekiwania i wysyłania czegokolwiek. W przeciwieństwie do innych kontroli wymaga określenia parametru portu.

telnet

Tworzy połączenie TCP i oczekuje monitu logowania (':' na końcu). Jeśli nie określono portu, używany jest domyślny port 23.

Parametry pozycji net.udp.service

ntp

Wysyła pakiet SNTP przez UDP i sprawdza poprawność odpowiedzi zgodnie z RFC 4330, sekcja 5. Jeśli nie określono portu, używany jest domyślny port 123.

10 parametrów proc.get

Przegląd

Pozycja **proc.get**[<name>,<user>,<cmdline>,<mode>] jest obsługiwana w systemach Linux, Windows, FreeBSD, OpenBSD i NetBSD.

Lista parametrów procesu zwracanych przez pozycję różni się w zależności od systemu operacyjnego i wartości argumentu „mode".

Linux

Następujące parametry procesu są zwracane w systemie Linux dla każdego trybu:

mode=process	mode=thread	mode=summary
pid: PID	pid: PID	name: nazwa procesu
ppid: PID procesu nadrzędnego	ppid: PID procesu nadrzędnego	processes: liczba procesów
name: nazwa procesu	name: nazwa procesu	vsize: rozmiar pamięci wirtualnej
cmdline: polecenie z argumentami	user: użytkownik (rzeczywisty), z uprawnieniami którego działa proces	pmem: procent pamięci rzeczywistej
user: użytkownik (rzeczywisty), z uprawnieniami którego działa proces	group: grupa (rzeczywista), z uprawnieniami której działa proces	rss: rozmiar rezydentnego zestawu pamięci
group: grupa (rzeczywista), z uprawnieniami której działa proces	uid: identyfikator użytkownika	data: rozmiar segmentu danych
uid: identyfikator użytkownika	gid: identyfikator grupy, z uprawnieniami której działa proces	exe: rozmiar segmentu kodu
gid: identyfikator grupy, z uprawnieniami której działa proces	tid: identyfikator wątku	lib: rozmiar bibliotek współdzielonych
vsize: rozmiar pamięci wirtualnej	tname: nazwa wątku	lck: rozmiar zablokowanej pamięci
pmem: procent pamięci rzeczywistej	cputime_user: całkowity czas CPU spędzony w trybie użytkownika (wartość wyrażona w taktach zegara — podziel przez `getconf CLK_TCK` lub `sysconf(_SC_CLK_TCK)`, aby uzyskać sekundy)	pin: rozmiar przypiętych stron
rss: rozmiar rezydentnego zestawu pamięci	cputime_system: całkowity czas CPU spędzony w trybie systemowym (wartość wyrażona w taktach zegara — podziel przez `getconf CLK_TCK` lub `sysconf(_SC_CLK_TCK)`, aby uzyskać sekundy)	pte: rozmiar wpisów tablicy stron
data: rozmiar segmentu danych	state: stan wątku	size: rozmiar segmentów kodu + danych + stosu procesu
exe: rozmiar segmentu kodu	ctx_switches: liczba przełączeń kontekstu	stk: rozmiar segmentu stosu
hwm: szczytowy rozmiar rezydentnego zestawu pamięci	page_faults: liczba błędów stron	swap: rozmiar używanej przestrzeni wymiany
lck: rozmiar zablokowanej pamięci		cputime_user: całkowity czas CPU spędzony w trybie użytkownika (wartość wyrażona w taktach zegara — podziel przez `getconf CLK_TCK` lub `sysconf(_SC_CLK_TCK)`, aby uzyskać sekundy)

mode=process	mode=thread	mode=summary
lib: rozmiar bibliotek współdzielonych		cputime_system: całkowity czas CPU spędzony w trybie systemowym (wartość wyrażona w taktach zegara — podziel przez `getconf CLK_TCK` lub `sysconf(_SC_CLK_TCK)`, aby uzyskać sekundy)
peak: szczytowy rozmiar pamięci wirtualnej		ctx_switches: liczba przełączeń kontekstu
pin: rozmiar przypiętych stron		threads: liczba wątków
pte: rozmiar wpisów tablicy stron		page_faults: liczba błędów stron
size: rozmiar segmentów kodu + danych + stosu procesu		pss: pamięć o proporcjonalnym rozmiarze zestawu
stk: rozmiar segmentu stosu		
swap: rozmiar używanej przestrzeni wymiany		
cputime_user: całkowity czas CPU spędzony w trybie użytkownika (wartość wyrażona w taktach zegara — podziel przez `getconf CLK_TCK` lub `sysconf(_SC_CLK_TCK)`, aby uzyskać sekundy)		
cputime_system: całkowity czas CPU spędzony w trybie systemowym (wartość wyrażona w taktach zegara — podziel przez `getconf CLK_TCK` lub `sysconf(_SC_CLK_TCK)`, aby uzyskać sekundy)		
state: stan procesu (pobierany bezpośrednio z procfs, forma długa)		
ctx_switches: liczba przełączeń kontekstu		
threads: liczba wątków		
page_faults: liczba błędów stron		
pss: pamięć o proporcjonalnym rozmiarze zestawu		

Systemy operacyjne oparte na BSD

Następujące parametry procesu są zwracane w systemach FreeBSD, OpenBSD i NetBSD dla każdego trybu:

mode=process	mode=thread	mode=summary
pid: PID	pid: PID	name: nazwa procesu
ppid: PID procesu nadrzędnego	ppid: PID procesu nadrzędnego	processes: liczba procesów
jid: ID jaila (tylko FreeBSD)	jid: ID jaila (tylko FreeBSD)	vsize: rozmiar pamięci wirtualnej
jname: nazwa jaila (tylko FreeBSD)	jname: nazwa jaila (tylko FreeBSD)	pmem: procent pamięci rzeczywistej (tylko FreeBSD)
name: nazwa procesu	name: nazwa procesu	rss: rozmiar rezydentnego zestawu pamięci
cmdline: polecenie z argumentami	user: użytkownik (rzeczywisty), z którego uprawnieniami działa proces	size: rozmiar procesu (kod + dane + stos)
user: użytkownik (rzeczywisty), z którego uprawnieniami działa proces	group: grupa (rzeczywista), z której uprawnieniami działa proces	tsize: rozmiar tekstu (kodu)
group: grupa (rzeczywista), z której uprawnieniami działa proces	uid: ID użytkownika	dsize: rozmiar danych
uid: ID użytkownika	gid: ID grupy, z której uprawnieniami działa proces	ssize: rozmiar stosu
gid: ID grupy, z której uprawnieniami działa proces	tid: ID wątku	cputime_user: całkowity czas CPU spędzony w trybie użytkownika (podawany w sekundach)

mode=process	mode=thread	mode=summary
vsize: rozmiar pamięci wirtualnej	tname: nazwa wątku	cputime_system: całkowity czas CPU spędzony w trybie systemowym (podawany w sekundach)
pmem: procent pamięci rzeczywistej (tylko FreeBSD)	cputime_user: całkowity czas CPU spędzony w trybie użytkownika (podawany w sekundach)	ctx_switches: liczba przełączeń kontekstu
rss: rozmiar rezydentnego zestawu pamięci	cputime_system: całkowity czas CPU spędzony w trybie systemowym (podawany w sekundach)	threads: liczba wątków (nieobsługiwane w NetBSD)
size: rozmiar procesu (kod + dane + stos)	state: stan wątku	stk: rozmiar segmentu stosu
tsize: rozmiar tekstu (kodu)	ctx_switches: liczba przełączeń kontekstu	page_faults: liczba błędów strony
dsize: rozmiar danych	io_read_op: liczba operacji wejścia wymaganych przez system	fds: liczba deskryptorów plików (tylko OpenBSD)
ssize: rozmiar stosu	io_write_op: liczba operacji wyjścia wymaganych przez system	swap: rozmiar używanej przestrzeni wymiany
cputime_user: całkowity czas CPU spędzony w trybie użytkownika (podawany w sekundach)		io_read_op: liczba operacji wejścia wymaganych przez system
cputime_system: całkowity czas CPU spędzony w trybie systemowym (podawany w sekundach)		io_write_op: liczba operacji wyjścia wymaganych przez system
state: stan procesu (uśpienie dyskowe/działający/uśpiony/zatrzymanie śledzenia/zombie/inny)		
ctx_switches: liczba przełączeń kontekstu		
threads: liczba wątków (nieobsługiwane w NetBSD)		
page_faults: liczba błędów strony		
fds: liczba deskryptorów plików (tylko OpenBSD)		
swap: rozmiar używanej przestrzeni wymiany		
io_read_op: liczba operacji wejścia wymaganych przez system		
io_write_op: liczba operacji wyjścia wymaganych przez system		

Windows

Następujące parametry procesu są zwracane w systemie Windows dla każdego trybu:

mode=process	mode=thread	mode=summary
pid: PID	pid: PID	name: nazwa procesu
ppid: PID procesu nadrzędnego	ppid: PID procesu nadrzędnego	processes: liczba procesów
name: nazwa procesu	name: nazwa procesu	vmsize: rozmiar pamięci wirtualnej
user: użytkownik, z uprawnieniami którego działa proces	user: użytkownik, z uprawnieniami którego działa proces	wkset: rozmiar zestawu roboczego procesu
sid: SID użytkownika	sid: SID użytkownika	cputime_user: całkowity czas CPU spędzony w trybie użytkownika (raportowany w milisekundach)
vmsize: rozmiar pamięci wirtualnej	tid: ID wątku	cputime_system: całkowity czas CPU spędzony w trybie systemowym (raportowany w milisekundach)
wkset: rozmiar zestawu roboczego procesu		threads: liczba wątków

mode=process	mode=thread	mode=summary
cputime_user: całkowity czas CPU spędzony w trybie użytkownika (raportowany w milisekundach)		page_faults: liczba błędów strony
cputime_system: całkowity czas CPU spędzony w trybie systemowym (raportowany w milisekundach)		handles: liczba uchwytów
threads: liczba wątków		io_read_b: odczytane bajty IO
page_faults: liczba błędów strony		io_write_b: zapisane bajty IO
handles: liczba uchwytów		io_read_op: operacje odczytu IO
io_read_b: odczytane bajty IO		io_write_op: operacje zapisu IO
io_write_b: zapisane bajty IO		io_other_b: bajty IO przesłane w operacjach innych niż odczyt i zapis
io_read_op: operacje odczytu IO		io_other_op: operacje IO inne niż odczyt i zapis
io_write_op: operacje zapisu IO		
io_other_b: bajty IO przesłane w operacjach innych niż odczyt i zapis		
io_other_op: operacje IO inne niż odczyt i zapis		

11 Ustawienia nieosiągalnego/niedostępnego interfejsu hosta

Przegląd

Kilka parametrów konfiguracji określa, jak serwer Zabbix powinien się zachować, gdy sprawdzenie przez agent (Zabbix, SNMP, IPMI, JMX) zakończy się niepowodzeniem, a interfejs hosta stanie się nieosiągalny.

Nieosiągalny interfejs

Interfejs hosta jest traktowany jako nieosiągalny po nieudanym sprawdzeniu (błąd sieciowy, przekroczenie limitu czasu) przez agenty Zabbix, SNMP, IPMI lub JMX. Od wersji Zabbix 6.2.0 aktywne sprawdzenia agenta Zabbix również wpływają na dostępność interfejsu. Gdy aktywne sprawdzenia stają się niedostępne, mają wpływ na ogólny status dostępności interfejsu agenta.

Od momentu, gdy interfejs staje się nieosiągalny, **UnreachableDelay** określa, jak często jest on sprawdzany ponownie przy użyciu jednej z pozycji (w tym reguł LLD).
Te ponowne sprawdzenia są wykonywane przez unreachable pollers (lub IPMI pollers w przypadku sprawdzeń IPMI).
Domyślnie odstęp między kolejnymi sprawdzeniami osiągalności wynosi 15 sekund.

> **Attention:**
> Sprawdzenia wykonywane przez asynchroniczne pollery nie są przenoszone do unreachable pollers.

W logu serwera Zabbix nieosiągalność jest wskazywana przez komunikaty takie jak:

```
Zabbix agent item "system.cpu.load[percpu,avg1]" on host "New host" failed: first network error, wait for
Zabbix agent item "system.cpu.load[percpu,avg15]" on host "New host" failed: another network error, wait f
```

Komunikaty logu określają dokładną pozycję, która zakończyła się niepowodzeniem, oraz jej typ (agent Zabbix).

> **Note:**
> Parametr *Timeout* również wpływa na to, jak wcześnie interfejs jest sprawdzany ponownie w czasie nieosiągalności. Jeśli Timeout jest ustawiony na 20 sekund, a UnreachableDelay na 30 sekund, następne sprawdzenie nastąpi po 50 sekundach od pierwszej próby.

Parametr **UnreachablePeriod** określa całkowity czas trwania okresu nieosiągalności.
Domyślnie wartość UnreachablePeriod wynosi 45 sekund.
Ta wartość powinna być kilkukrotnie większa niż UnreachableDelay, aby zapewnić wielokrotne ponowne sprawdzenie interfejsu przed oznaczeniem go jako niedostępnego.

Wewnętrzna pozycja zabbix[host,active_agent,available] umożliwia monitorowanie dostępności aktywnych sprawdzeń w scenariuszach nieosiągalności.

Przełączanie interfejsu z powrotem na dostępny

Po zakończeniu okresu niedostępności interfejs jest ponownie odpytywany, ze zmniejszonym priorytetem dla pozycji, która spowodowała przejście interfejsu w stan niedostępności. Jeśli niedostępny interfejs pojawi się ponownie, monitorowanie automatycznie wraca do normy:

```
wznowienie kontroli Zabbix agent na hoście "New host": połączenie przywrócone
```

Note:
Gdy interfejs staje się dostępny, host nie odpytuje natychmiast wszystkich swoich pozycji z dwóch powodów:
- Mogłoby to przeciążyć host.
- Czas przywrócenia interfejsu nie zawsze pokrywa się z planowanym czasem harmonogramu odpytywania pozycji.

Dlatego po przywróceniu dostępności interfejsu pozycje nie są odpytywane natychmiast, lecz są przeplanowywane na następną rundę odpytywania.

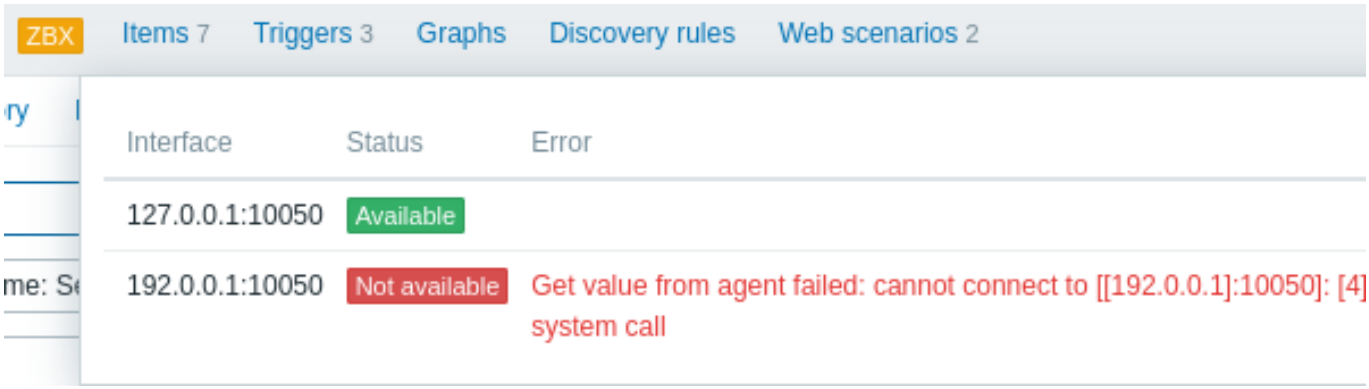
Niedostępny interfejs

Po zakończeniu okresu UnreachablePeriod, jeśli interfejs nie pojawi się ponownie, jest on traktowany jako niedostępny.

W logu serwera jest to sygnalizowane komunikatami takimi jak:

```
temporarily disabling Zabbix agent checks on host "New host": interface unavailable
```

a we frontend ikona dostępności hosta zmienia kolor z zielonego/szarego na żółty/czerwony (szczegóły niedostępnego interfejsu można zobaczyć w dymku podpowiedzi, który jest wyświetlany po najechaniu kursorem na ikonę dostępności hosta):



Parametr **UnavailableDelay** określa, jak często interfejs jest sprawdzany w czasie jego niedostępności.

Domyślnie jest to 60 sekund (więc w tym przypadku „temporarily disabling" z komunikatu logu powyżej będzie oznaczać wyłączenie sprawdzania na jedną minutę).

Gdy połączenie z interfejsem zostanie przywrócone, monitorowanie również automatycznie wraca do normy:

```
enabling Zabbix agent checks on host "New host": interface became available
```

12 Zdalne monitorowanie statystyk Zabbix

Przegląd

Możliwe jest udostępnienie zdalnie niektórych wewnętrznych metryk serwera i proxy Zabbix innej instancji Zabbix lub narzędziu zewnętrznemu. Może to być przydatne, aby osoby zapewniające wsparcie/dostawcy usług mogli zdalnie monitorować serwery/proxy Zabbix swoich klientów lub w organizacjach, w których Zabbix nie jest głównym narzędziem monitorującym, aby wewnętrzne metryki Zabbix mogły być monitorowane przez system zewnętrzny w ramach nadrzędnej konfiguracji monitoringu.

Wewnętrzne statystyki Zabbix są udostępniane dla konfigurowalnego zestawu adresów wymienionych w nowym parametrze 'StatsAllowedIP' server/proxy. Żądania będą akceptowane wyłącznie z tych adresów.

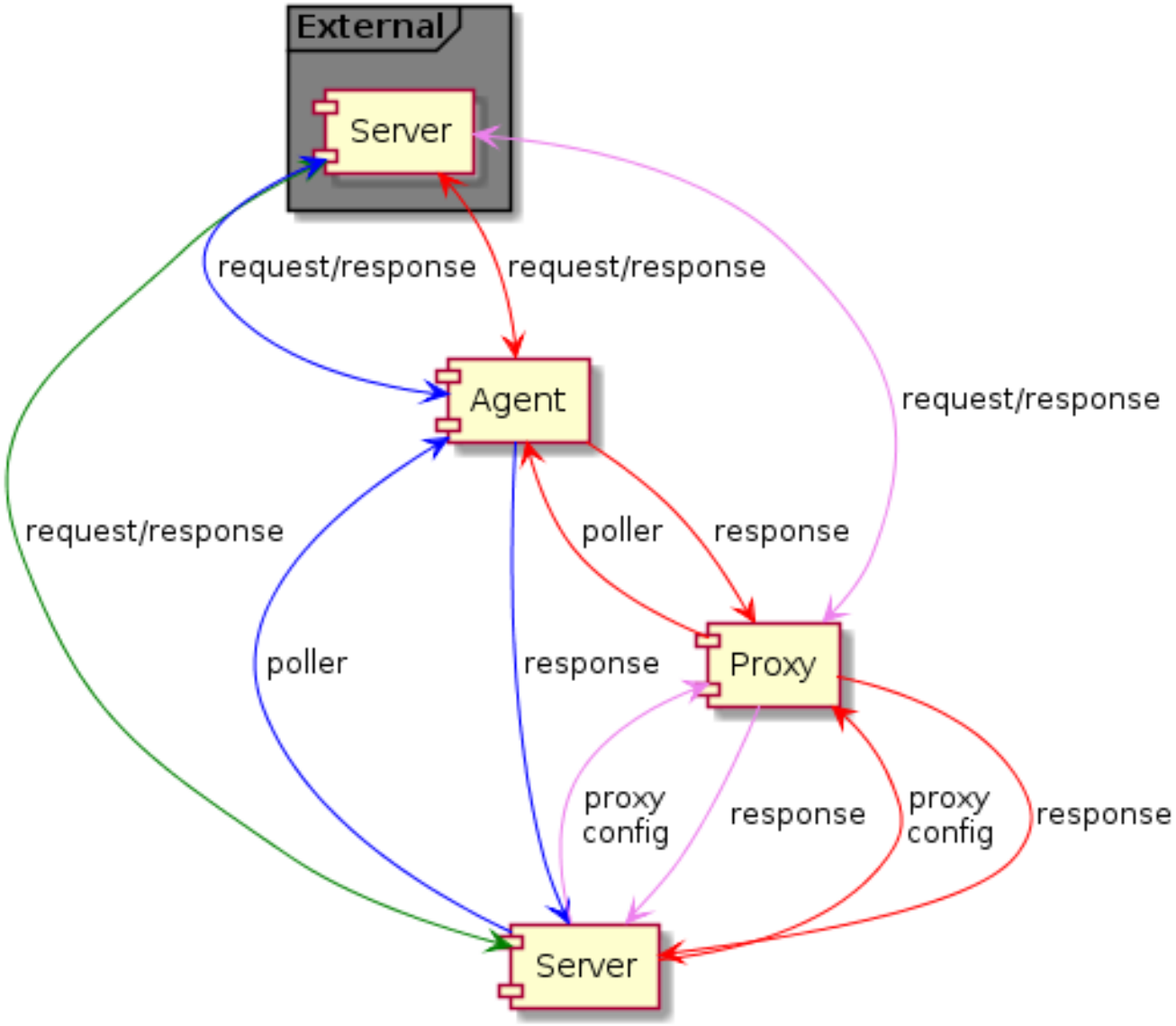
Pozycje

Aby skonfigurować odpytywanie wewnętrznych statystyk na innej instancji Zabbix, można użyć dwóch pozycji:

- wewnętrzna pozycja `zabbix[stats,<ip>,<port>]` — do bezpośrednich zdalnych zapytań do serwera/proxy Zabbix. `<ip>` i `<port>` są używane do identyfikacji instancji docelowej.
- pozycja agenta `zabbix.stats[<ip>,<port>]` — do zdalnych zapytań do serwera/proxy Zabbix opartych na agencie. `<ip>` i `<port>` są używane do identyfikacji instancji docelowej.

Zobacz także: Pozycje wewnętrzne, Pozycje agenta Zabbix

Poniższy diagram ilustruje użycie jednej z tych pozycji w zależności od kontekstu.



- — Serwer → zewnętrzna instancja Zabbix (`zabbix[stats,<ip>,<port>]`)
- — Serwer → proxy → zewnętrzna instancja Zabbix (`zabbix[stats,<ip>,<port>]`)
- — Serwer → agent → zewnętrzna instancja Zabbix (`zabbix.stats[<ip>,<port>]`)
- — Serwer → proxy → agent → zewnętrzna instancja Zabbix (`zabbix.stats[<ip>,<port>]`)

Aby upewnić się, że instancja docelowa zezwala na odpytywanie jej przez instancję zewnętrzną, podaj adres instancji zewnętrznej w parametrze `StatsAllowedIP` na instancji docelowej.

Udostępniane metryki

Pozycje statystyk zbierają statystyki zbiorczo i zwracają JSON, który stanowi podstawę dla pozycji zależnych do pobierania z niego danych. Następujące metryki wewnętrzne są zwracane przez dowolną z tych dwóch pozycji:

- `zabbix[boottime]`
- `zabbix[hosts]`
- `zabbix[items]`
- `zabbix[items_unsupported]`
- `zabbix[preprocessing]` (tylko serwer)
- `zabbix[preprocessing_queue]` (tylko serwer)
- `zabbix[process,<type>,<mode>,<state>]` (tylko statystyki oparte na typie procesu)
- `zabbix[rcache,<cache>,<mode>]`
- `zabbix[requiredperformance]`
- `zabbix[triggers]` (tylko serwer)
- `zabbix[uptime]`
- `zabbix[vcache,buffer,<mode>]` (tylko serwer)

- zabbix[vcache,cache,<parameter>]
- zabbix[version]
- zabbix[vmware,buffer,<mode>]
- zabbix[wcache,<cache>,<mode>] (typ pamięci podręcznej „trends” tylko dla serwera)

Szablony

Szablony są dostępne do zdalnego monitorowania wewnętrznych metryk serwera Zabbix lub proxy z zewnętrznej instancji:

- Stan zdalnego serwera Zabbix
- Stan zdalnego proxy Zabbix

Należy pamiętać, że aby użyć szablonu do zdalnego monitorowania wielu zewnętrznych instancji, wymagany jest oddzielny host dla monitorowania każdej zewnętrznej instancji.

Proces trapper

Odbieranie żądań metryk wewnętrznych z zewnętrznej instancji Zabbix jest obsługiwane przez proces trapper, który weryfikuje żądanie, zbiera metryki, tworzy bufor danych JSON i odsyła przygotowany JSON z powrotem, na przykład z serwera:

```
{
  "response": "success",
  "data": {
    "boottime": N,
    "uptime": N,
    "hosts": N,
    "items": N,
    "items_unsupported": N,
    "preprocessing": {
        "queued": {
          "count": N,
          "size": N
        },
        "direct": {
          "count": N,
          "size": N
        },
        "queue": N
    },
    "preprocessing_queue": N,
    "process": {
      "alert manager": {
        "busy": {
          "avg": N,
          "max": N,
          "min": N
        },
        "idle": {
          "avg": N,
          "max": N,
          "min": N
        },
        "count": N
      },
...
    },
    "queue": N,
    "rcache": {
      "total": N,
      "free": N,
      "pfree": N,
      "used": N,
      "pused": N
    },
    "requiredperformance": N,
    "triggers": N,
```

```
    "uptime": N,
    "vcache": {
      "buffer": {
        "total": N,
        "free": N,
        "pfree": N,
        "used": N,
        "pused": N
      },
      "cache": {
        "requests": N,
        "hits": N,
        "misses": N,
        "mode": N
      }
    },
    "vmware": {
      "total": N,
      "free": N,
      "pfree": N,
      "used": N,
      "pused": N
    },
    "version": "N",
    "wcache": {
      "values": {
        "all": N,
        "float": N,
        "uint": N,
        "str": N,
        "log": N,
        "text": N,
        "not supported": N
      },
      "history": {
        "pfree": N,
        "free": N,
        "total": N,
        "used": N,
        "pused": N
      },
      "index": {
        "pfree": N,
        "free": N,
        "total": N,
        "used": N,
        "pused": N
      },
      "trend": {
        "pfree": N,
        "free": N,
        "total": N,
        "used": N,
        "pused": N
      }
    }
  }
}
```

Wewnętrzne pozycje kolejki

Istnieją także dwie dodatkowe pozycje, które umożliwiają zdalne odpytywanie statystyk wewnętrznej kolejki w innej instancji Zabbix:

- wewnętrzna pozycja `zabbix[stats,<ip>,<port>,queue,<from>,<to>]` — do bezpośrednich zapytań o wewnętrzną kolejkę do zdalnego serwera/proxy Zabbix
- pozycja agenta `zabbix.stats[<ip>,<port>,queue,<from>,<to>]` — do opartych na agencie zapytań o wewnętrzną kolejkę do zdalnego serwera/proxy Zabbix

Zobacz także: Wewnętrzne pozycje, Pozycje agenta Zabbix

13 Konfigurowanie Kerberos z Zabbix

Przegląd

Uwierzytelnianie Kerberos może być używane w monitorowaniu WWW oraz w pozycjach HTTP w Zabbix.

Ta strona opisuje przykład konfiguracji Kerberos dla serwera Zabbix, aby wykonywać monitorowanie WWW `www.example.com` z użyciem principal Kerberos dla procesu Zabbix w Debian/Ubuntu.

Konfiguracja

1. Zainstaluj KDC i narzędzia klienckie:

```
sudo apt update
sudo apt install krb5-kdc krb5-admin-server krb5-user
```

Podczas konfiguracji pakietów odpowiedz na wyświetlane pytania, np.:

```
Default Kerberos version 5 realm: EXAMPLE.COM
Kerberos servers for your realm: localhost (lub twój FQDN)
Administrative server for your Kerberos realm: localhost (lub twój FQDN)
```

2. Przypisz przyjazną nazwę hosta (opcjonalnie, do testów lokalnych).

Edytuj /etc/hosts i dodaj wpis dla swojego DC oraz serwera WWW, jeśli nie masz DNS:

```
sudo vi /etc/hosts
```

Przykładowy wiersz, który możesz dodać:

```
192.168.1.100  dc01.example.com dc01
```

3. Skonfiguruj klienta Kerberos i realm KDC:

```
sudo vi /etc/krb5.conf
```

Przykładowe ustawienia:

```
[libdefaults]
    default_realm = EXAMPLE.COM
    dns_lookup_realm = false
    dns_lookup_kdc = false
    rdns = false
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true

[realms]
    EXAMPLE.COM = {
        kdc = dc01.example.com
        admin_server = dc01.example.com
    }

[domain_realm]
    .example.com = EXAMPLE.COM
    example.com = EXAMPLE.COM
```

Jeśli planujesz używać `.localdomain` lub innych niepublicznych nazw, dodaj jawne mapowania domena→realm, aby mapowanie nazwa hosta→realm działało poprawnie.
Niezgodności w tym miejscu powodują błędy `Server not found in Kerberos database`.

4. Zainicjalizuj bazę danych Kerberos (jednorazowo, na hoście KDC).
Po wyświetleniu monitu ustaw bezpieczne hasło główne:

```
sudo krb5_newrealm
```

5. Utwórz principal `HTTP/host.fqdn@REALM`, używając dokładnej nazwy hosta, z której będą korzystać klienci; preferowane są małe litery (np. `HTTP/web.example.com@EXAMPLE.COM`).
Niezgodność wielkości liter/nazwy powoduje `Server not found in Kerberos database`.

```
sudo kadmin.local
```

Wewnątrz `kadmin.local`:

```
addprinc kerb-admin@EXAMPLE.COM     # principal administracyjny
addprinc -randkey HTTP/dc01.example.com@EXAMPLE.COM
ktadd -k /etc/apache2/http.keytab HTTP/dc01.example.com@EXAMPLE.COM
quit
```

Przenieś keytab na host WWW (lub pozostaw lokalnie, jeśli to ta sama maszyna) i ustaw uprawnienia umożliwiające użycie przez Apache:

```
chown www-data:www-data /etc/apache2/http.keytab
chmod 600 /etc/apache2/http.keytab
#### weryfikacja
sudo -u www-data -k /etc/apache2/http.keytab
```

6. Zainstaluj i włącz moduł Apache GSSAPI:

```
sudo apt install libapache2-mod-auth-gssapi
sudo a2enmod auth_gssapi
sudo a2enmod headers
sudo systemctl restart apache2
```

> **Attention:**
> Nie wszystkie wersje mod_auth_gssapi obsługują każdą dyrektywę `Gssapi*`.
> Jeśli Apache kończy działanie z błędem `Invalid command 'GssapiCredStore'`, usuń nieobsługiwaną dyrektywę lub zaktualizuj moduł.

7. Skonfiguruj VirtualHost (dostosuj `DocumentRoot` / ścieżkę do interfejsu Zabbix):

```
sudo vi /etc/apache2/sites-available/zabbix.conf
```

Wewnątrz `zabbix.conf`:

```
<VirtualHost *:80>
    ServerName dc01.example.com
    DocumentRoot /usr/share/zabbix/ui
    <Directory /usr/share/zabbix/ui>
        Options FollowSymLinks
        AllowOverride None
        Require all granted
        AuthType GSSAPI
        AuthName "Kerberos Login"
        GssapiCredStore keytab:/etc/apache2/http.keytab
        GssapiLocalName On
        Require valid-user
    </Directory>
    RequestHeader set X-Remote-User %{REMOTE_USER}s env=REMOTE_USER
    RequestHeader unset Authorization
</VirtualHost>
```

Uruchom ponownie Apache:

```
sudo systemctl restart apache2
```

8. Włącz/uruchom usługi KDC i zweryfikuj porty nasłuchujące (host KDC):

```
sudo systemctl enable --now krb5-kdc krb5-admin-server
ss -tnlp | grep :80    # lub: sudo netstat -tnlp | grep :80
```

9. Uzyskaj TGT do testów (uruchom jako użytkownik, który będzie używać ticketu).

Na liście ticketów powinien być widoczny krbtgt/EXAMPLE.COM@EXAMPLE.COM.
Uruchom kinit jako ten sam użytkownik systemu operacyjnego, który potrzebuje ticketu (np. zabbix dla testów WWW lub www-data/Apache dla interaktywnych testów SSO w przeglądarce).
Tickety wydane innemu użytkownikowi systemu operacyjnego nie będą widoczne, chyba że zostaną odpowiednio dostosowane KRB5CCNAME i uprawnienia.

```
kinit kerb-admin@EXAMPLE.COM
klist
```

10. Przetestuj wymianę SPNEGO za pomocą curl (z klienta z prawidłowym TGT).
200 OK (lub przekierowanie do aplikacji) oznacza, że SPNEGO zadziałało poprawnie:

```
curl -v --negotiate -u : http://dc01.example.com/
```

11. Opcjonalnie, jeśli interfejs Zabbix ma akceptować logowanie uwierzytelniane przez HTTP, włącz HTTP auth w frontendzie Zabbix (ui/conf/zabbix.conf.php):

```
$ALLOW_HTTP_AUTH = true;
```

W interfejsie WWW przejdź do *Users* > *Authentication* i otwórz kartę *HTTP settings*.
Zaznacz pole wyboru *Enable HTTP authentication* i kliknij *Ok* w wyskakującym oknie.
Wybierz „HTTP login form" z listy rozwijanej *Default login form*.
Zdecyduj, czy *Case-sensitive login* odpowiada polityce twojego katalogu.
Kliknij przycisk *Update*, aby zakończyć.

12. Konfiguracja przeglądarki (jako przykład użyto Firefox): ustaw network.negotiate-auth.trusted-uris na host(y) wykonujące Negotiate (dc01.example.com), aby przeglądarka automatycznie wysyłała tokeny Kerberos.

W about:config:

```
network.negotiate-auth.trusted-uris = dc01.example.com
```

Po wejściu na http://dc01.example.com powinieneś zostać od razu zalogowany do Zabbix bez formularza.

13. Utrzymuj klucze/tickety aktualne.
Domyślny czas życia ticketu Kerberos wynosi około 10 godzin.
Dodaj cron/systemd timer, aby uniknąć wygaśnięcia:

```
####dla usługi WWW
kinit -kt /etc/apache2/http.keytab HTTP/dc01.example.com@EXAMPLE.COM
####dla użytkownika monitorowania
kinit -kt /var/lib/zabbix/kerb.keytab kerb-admin@EXAMPLE.COM
```

14. Kontrole porządkowe:

- klist -k /etc/apache2/http.keytab — sprawdź, czy principal usługi jest obecny w keytab.
- sudo tail -f /var/log/apache2/error.log — obserwuj błędy GSSAPI (gss_acquire_cred[_from]() failed to get server creds oznacza problem z keytab/uprawnieniami lub brak principal).
- Zwracanie 401/403 przez curl --negotiate często oznacza nieprawidłowy principal, brak ticketu, niedopasowanie nagłówka hosta lub problem z uprawnieniami systemu plików; sprawdź logi i mapowania domen w /etc/krb5.conf.

Uwagi dotyczące bezpieczeństwa i uprawnień do plików

Pliki keytab muszą być dostępne do odczytu wyłącznie dla konta, które ich potrzebuje. Przykładowe uprawnienia: 0400 z właścicielem zabbix:zabbix dla pliku keytab użytkownika zabbix lub 0440 i root:www-data dla pliku keytab Apache.

Unikaj przechowywania na hoście długotrwałych haseł w postaci zwykłego tekstu. Tam, gdzie to możliwe, używaj plików keytab lub principali maszyn przyłączonych do domeny.

Podczas uruchamiania testów lub skryptów, które ustawiają KRB5CCNAME lub kopiują pliki keytab, po zakończeniu operacji dokładnie sprawdź właściciela i uprawnienia — odrzucanie poświadczeń przez serwer WWW często wynika z problemu z uprawnieniami do plików.

14 parametry modbus.get

Przegląd

Poniższa tabela przedstawia szczegóły parametrów pozycji modbus.get.

Parametry

Parameter	Opis	Defaults	Example
endpoint	Protokół i adres endpointu, zdefiniowane jako `protocol://connection_string` Możliwe wartości protokołu: *rtu*, *ascii* (tylko Agent 2), *tcp* Format connection string: dla *tcp* - `address:port` dla linii szeregowej: *rtu*, *ascii* - `port_name:speed:params` gdzie 'speed' - 1200, 9600 itd. 'params' - bity danych (5,6,7 lub 8), parzystość (n,e lub o dla brak/parzysta/nieparzysta), bity stopu (1 lub 2)	protocol: brak protokół *rtu/ascii*: port_name: brak speed: 115200 params: 8n1 protokół *tcp*: address: brak port: 502	tcp://192.168.6.1:511 tcp://192.168.6.2 tcp://[::1]:511 tcp://::1 tcp://localhost:511 tcp://localhost rtu://COM1:9600:8n ascii://COM2:1200:7o2 rtu://ttyS0:9600 ascii://ttyS1
slave id	Adres Modbus urządzenia, do którego jest przeznaczony (1 do 247), zobacz MODBUS Messaging Implementation Guide (strona 23) urządzenie tcp (nie GW) zignoruje to pole	serial: 1 tcp: 255 (0xFF)	2
function	Puste lub wartość obsługiwanej funkcji: 1 - Odczyt cewki, 2 - Odczyt wejścia dyskretnego, 3 - Odczyt rejestrów przechowujących, 4 - Odczyt rejestrów wejściowych	puste	3
address	Adres pierwszego rejestru, cewki lub wejścia. Jeśli 'function' jest puste, wtedy 'address' powinien należeć do zakresu dla: Cewka - 00001 - 09999 Wejście dyskretne - 10001 - 19999 Rejestr wejściowy - 30001 - 39999 Rejestr przechowujący - 40001 - 49999 Jeśli 'function' nie jest puste, pole 'address' będzie miało zakres od 0 do 65535 i zostanie użyte bez modyfikacji (PDU)	pusta function: 00001 niepusta function: 0	9999
count	Liczba sekwencyjnych wartości 'type', które zostaną odczytane z urządzenia, gdzie: dla cewki lub wejścia dyskretnego 'type' = 1 bit dla pozostałych przypadków: (count*sizeof(type))/2 = rzeczywista liczba rejestrów do odczytu Jeśli 'offset' nie jest równe 0, wartość ta zostanie dodana do 'rzeczywistej liczby' Dopuszczalny zakres dla 'rzeczywistej liczby' to 1:65535	1	2

Parameter	Opis	Defaults	Example
type	Typ danych: dla Read Coil i Read Discrete Input - *bit* dla Read Holding Registers i Read Input Registers: *int8* - 8bit *uint8* - 8bit (bez znaku) *int16* - 16bit *uint16* - 16bit (bez znaku) *int32* - 32bit *uint32* - 32bit (bez znaku) *float* - 32bit *uint64* - 64bit (bez znaku) *double* - 64bit	bit uint16	uint64
endianness	Typ kolejności bajtów: *be* - Big Endian *le* - Little Endian *mbe* - Mid-Big Endian *mle* - Mid-Little Endian Ograniczenia: dla 1 bitu - be dla 8 bitów - be,le dla 16 bitów - be,le	be	le
offset	Liczba rejestrów, począwszy od 'address', których wynik zostanie odrzucony. Rozmiar każdego rejestru to 16bit (potrzebne do obsługi urządzeń, które nie obsługują losowego dostępu do odczytu).	0	4

15 Tworzenie niestandardowych nazw liczników wydajności dla VMware

Przegląd

Ścieżka licznika wydajności VMware ma format `group/counter[rollup]`, gdzie:

- `group` — grupa licznika wydajności, na przykład *cpu*
- `counter` — nazwa licznika wydajności, na przykład *usagemhz*
- `rollup` — typ agregacji licznika wydajności, na przykład *average*

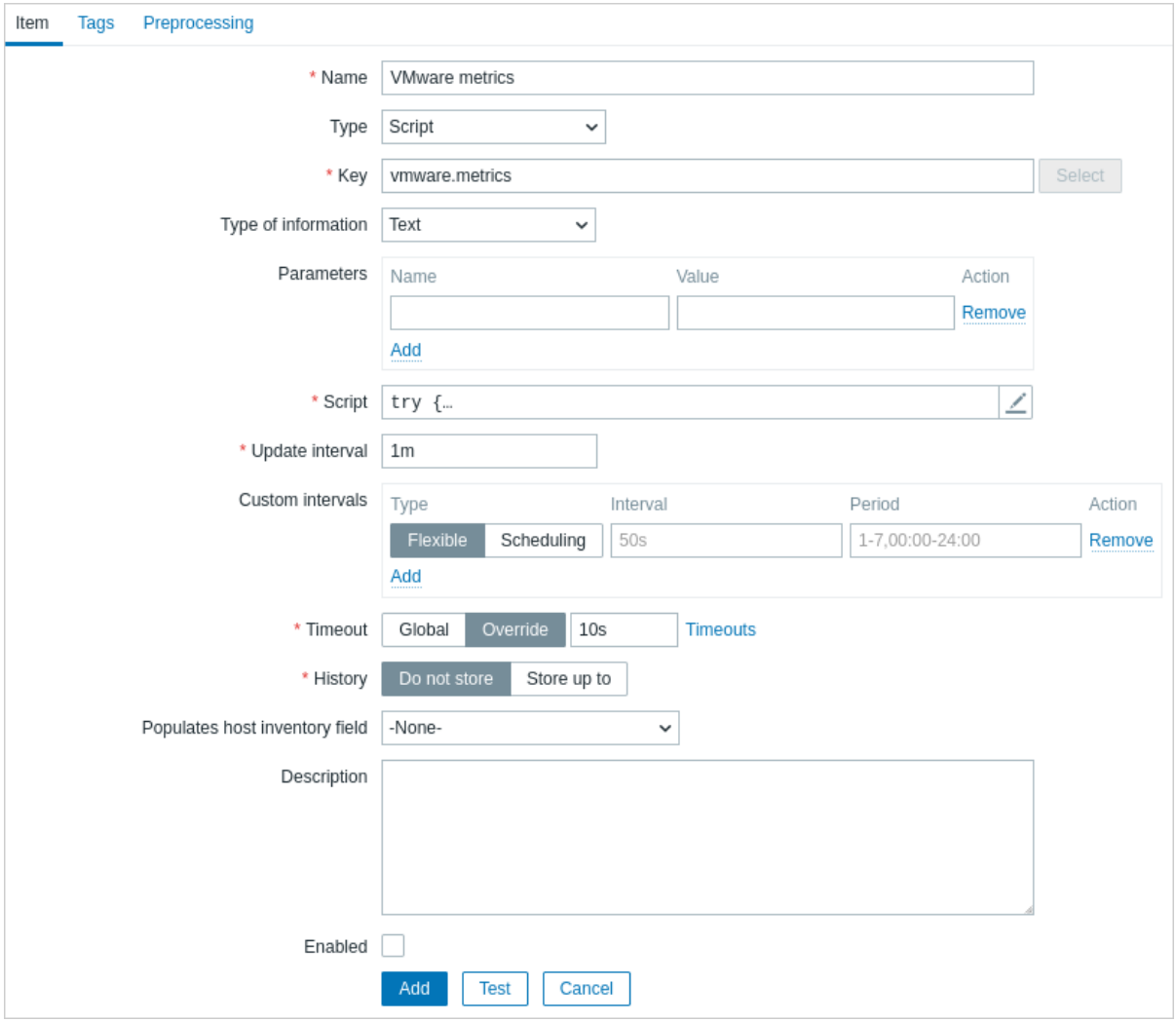
Tak więc powyższy przykład da następującą ścieżkę licznika: `cpu/usagemhz[average]`

Opisy grup liczników wydajności, nazwy liczników oraz typy agregacji można znaleźć w dokumentacji VMware.

Możliwe jest uzyskanie nazw wewnętrznych oraz tworzenie niestandardowych nazw liczników wydajności przy użyciu pozycji skryptowej w Zabbix.

Konfiguracja

1. Utwórz wyłączoną pozycję Script na głównym hoście VMware (tam, gdzie znajduje się pozycja **eventlog[]**) z następującymi parametrami:



- *Nazwa*: Metryki VMware
- *Typ*: Script
- *Klucz*: vmware.metrics
- *Typ informacji*: Tekst
- *Skrypt*: skopiuj i wklej skrypt podany poniżej
- *Limit czasu*: 10
- *Historia*: Nie przechowuj
- *Włączone*: niezaznaczone

Skrypt

```
try {
    Zabbix.log(4, 'vmware metrics script');

    var result, resp,
    req = new HttpRequest();
    req.addHeader('Content-Type: application/xml');
    req.addHeader('SOAPAction: "urn:vim25/6.0"');

    login = '<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:urn="urn:vi
    <soapenv:Header/>\
    <soapenv:Body>\
        <urn:Login>\
            <urn:_this type="SessionManager">SessionManager</urn:_this>\
            <urn:userName>{$VMWARE.USERNAME}</urn:userName>\
            <urn:password>{$VMWARE.PASSWORD}</urn:password>\
        </urn:Login>\
    </soapenv:Body>\
</soapenv:Envelope>'
    resp = req.post("{$VMWARE.URL}", login);
    if (req.getStatus() != 200) {
```

```
        throw 'Response code: '+req.getStatus();
    }

    query = '<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:urn="urn:vi
<soapenv:Header/>\
    <soapenv:Body>\
        <urn:RetrieveProperties>\
            <urn:_this type="PropertyCollector">propertyCollector</urn:_this>\
            <urn:specSet>\
                <urn:propSet>\
                   <urn:type>PerformanceManager</urn:type>\
                   <urn:pathSet>perfCounter</urn:pathSet>\
                </urn:propSet>\
                <urn:objectSet>\
                   <urn:obj type="PerformanceManager">PerfMgr</urn:obj>\
                </urn:objectSet>\
            </urn:specSet>\
        </urn:RetrieveProperties>\
    </soapenv:Body>\
</soapenv:Envelope>'
    resp = req.post("{$VMWARE.URL}", query);
    if (req.getStatus() != 200) {
        throw 'Response code: '+req.getStatus();
    }
    Zabbix.log(4, 'vmware metrics=' + resp);
    result = resp;

    logout = '<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:urn="urn:v
    <soapenv:Header/>\
    <soapenv:Body>\
        <urn:Logout>\
            <urn:_this type="SessionManager">SessionManager</urn:_this>\
        </urn:Logout>\
    </soapenv:Body>\
</soapenv:Envelope>'

    resp = req.post("{$VMWARE.URL}",logout);
    if (req.getStatus() != 200) {
        throw 'Response code: '+req.getStatus();
    }

} catch (error) {
    Zabbix.log(4, 'vmware call failed : '+error);
    result = {};
}

return result;
```

Po skonfigurowaniu pozycji naciśnij przycisk *Test*, a następnie *Get value*.



Skopiuj otrzymany XML do dowolnego formatera XML i znajdź żądaną metrykę.

Przykład XML dla jednej metryki:

```
<PerfCounterInfo xsi:type="PerfCounterInfo">
    <key>6</key>
```

```
    <nameInfo>
        <label>Usage in MHz</label>
        <summary>CPU usage in megahertz during the interval</summary>
        <key>usagemhz</key>
    </nameInfo>
    <groupInfo>
        <label>CPU</label>
        <summary>CPU</summary>
        <key>cpu</key>
    </groupInfo>
    <unitInfo>
        <label>MHz</label>
        <summary>Megahertz</summary>
        <key>megaHertz</key>
    </unitInfo>
    <rollupType>average</rollupType>
    <statsType>rate</statsType>
    <level>1</level>
    <perDeviceLevel>3</perDeviceLevel>
</PerfCounterInfo>
```

Użyj XPath, aby wyodrębnić ścieżkę licznika z otrzymanego XML. Dla powyższego przykładu XPath będzie następujący:

pole	xPath	wartość
group	//groupInfo[../key=6]/key	cpu
counter	//nameInfo[../key=6]/key	usagemhz
rollup	//rollupType[../key=6]	average

Wynikowa ścieżka licznika wydajności w tym przypadku to: `cpu/usagemhz[average]`

16 Wartości zwracane dla system.sw.packages.get

Przegląd

Ta sekcja zawiera szczegółowe informacje o wartościach zwracanych dla pozycji agenta Zabbix `system.sw.packages.get`.

Szczegóły

Dane wyjściowe tej pozycji są tablicą obiektów, z których każdy zawiera następujące klucze:

- **name** - nazwa pakietu
- **manager** - menedżer pakietów, który zgłosił te dane (`rpm`, `dpkg`, `pacman`, `pkgtool` lub `portage`)
- **version** - wersja pakietu
- **size** - rozmiar nieskompresowanego pakietu w bajtach (jeśli niedostępny, ustawione na 0)
- **arch** - architektura pakietu
- **buildtime** - obiekt z 2 wpisami:
  - **timestamp** - znacznik czasu UNIX określający moment zbudowania pakietu (jeśli niedostępny, ustawione na 0)
  - **value** - czytelna dla człowieka data i godzina zbudowania pakietu (jeśli niedostępne, ustawione na pusty ciąg)
- **installtime** - obiekt z 2 wpisami:
  - **timestamp** - znacznik czasu UNIX określający moment zainstalowania pakietu (jeśli niedostępny, ustawione na 0)
  - **value** - czytelna dla człowieka data i godzina zainstalowania pakietu (jeśli niedostępne, ustawione na pusty ciąg)

Przykład:

```
[
    {
        "name": "util-linux-core",
        "manager": "rpm",
        "version": "2.37.4-3.el9",
        "size": 1296335,
        "arch": "x86_64",
        "buildtime": {
            "timestamp" : 1653552239,
            "value" : "Sep 20 01:39:40 2021 UTC"
```

```
        },
        "installtime": {
            "timestamp" : 1660780885,
            "value" : "Aug 18 00:01:25 2022 UTC"
        }
    },
    {
        "name": "xfonts-base",
        "manager": "dpkg",
        "version": "1:1.0.5",
        "size": 7337984,
        "arch": "all",
        "buildtime": {
            "timestamp": 0,
            "value": ""
        },
        "installtime": {
            "timestamp": 0,
            "value": ""
        }
    }
]
```

17 Wartości zwracane dla net.dns.get

Przegląd

Ta sekcja zawiera szczegółowe informacje o wartościach zwracanych dla pozycji Zabbix agent 2 `net.dns.get`.

Szczegóły

Dane wyjściowe tej pozycji są obiektem zawierającym informacje o rekordzie DNS na podstawie parametrów podanych w kluczu pozycji.

Na przykład pozycja `net.dns.get[,example.com]` może zwrócić następujący JSON dla zapytania odrzuconego:

```
{
    "flags": [
        "RA"
    ],
    "query_time": "0.019030",
    "question_section": [
        {
            "qclass": "IN",
            "qname": "example.com.",
            "qtype": "SOA"
        }
    ],
    "response_code": "REFUSED",
    "zbx_error_code": 0
}
```

Po podaniu adresu IP serwera DNS pozycja `net.dns.get[192.0.2.0,example.com]` może zwrócić następujący JSON:

```
{
    "answer_section": [
        {
            "class": "IN",
            "name": "example.com.",
            "rdata": {
                "expire": 1209600,
                "mbox": "noc.dns.example.org.",
                "minttl": 3600,
                "ns": "ns.example.org.",
                "refresh": 7200,
```

```
                "retry": 3600,
                "serial": 2022091378
            },
            "rdlength": 44,
            "ttl": 1205,
            "type": "SOA"
        }
    ],
    "flags": [
        "RA"
    ],
    "query_time": "0.029556",
    "question_section": [
        {
            "qclass": "IN",
            "qname": "example.com.",
            "qtype": "SOA"
        }
    ],
    "response_code": "NOERROR",
    "zbx_error_code": 0
}
```


Jeśli wystąpi problem z połączeniem, pozycja `net.dns.get[192.0.2.0,example.com]` może zwrócić błąd:


```
{
    "zbx_error_code": -1,
    "zbx_error_msg": "Communication error: read udp 192.0.2.0:12345->192.0.2.0:53: i/o timeout"
}
```


Możliwe są następujące typy kodów błędów:

Scenariusz	"zbx_error_code"	"zbx_error_msg"
Brak błędów, odpowiedź DNS została odebrana i przeanalizowana.	0	
DNS jest niedostępny.	-1	"Communication error"
Podczas parsowania JSON wystąpił błąd	-2	"Received unexpected response"

Przy użyciu dodatkowych parametrów pozycja `net.dns.get[192.0.2.0,example.com,ANY,5,5,tcp,"cdflag,rdflag,dnssec,nsi` może zwrócić następujący JSON:


```
{
    "additional_section": [
        {
            "extended_rcode": 32768,
            "name": ".",
            "rdata": {
                "options": [
                {
                    "code": 0,
                    "nsid": "67 70 64 6e 73 2d 6c 70 70"
                }
                ]
        },
            "rdlength": 13,
            "type": "OPT",
            "udp_payload": 512
        }
    ],
    "answer_section": [
        {
            "class": "IN",
            "name": "example.com.",
            "rdata": {
```

```
                "a": "192.0.2.0"
            },
            "rdlength": 4,
            "ttl": 19308,
            "type": "A"
        },
        {
            "class": "IN",
            "name": "example.com.",
            "rdata": {
                "algorithm": 13,
                "expiration": 1704715951,
                "inception": 1702910624,
                "key_tag": 21021,
                "labels": 2,
                "orig_ttl": 86400,
                "signature": "HVBOBcJJQy0S08J3f8kviPj8UkEUj7wmyiMyQqPSWgQIY9SCEJ5plq6KuxJmtAek1txZWXDo+6tp
                "signer_name": "example.com.",
                "type_covered": "A"
            },
            "rdlength": 95,
            "ttl": 19308,
            "type": "RRSIG"
        }
    ],
    "flags": [
        "RD",
        "RA",
        "AD",
        "CD"
    ],
    "query_time": "0.058221",
    "question_section": [
        {
            "qclass": "IN",
            "qname": "example.com.",
            "qtype": "ANY"
        }
    ],
    "response_code": "NOERROR",
    "zbx_error_code": 0
}
```


Zobacz także

Aby uzyskać więcej informacji o rekordach DNS, zobacz:

- Domain Names - Implementation and Specification
- Domain Name System (DNS) Parameters

18 Uwagi dotyczące pozycji system.cpu.util w systemie Windows

system.cpu.util pozycja dostarcza procent wykorzystania CPU.

Gdy w Zabbix agent dla Windows uruchamiany jest proces collectora, inicjalizowany jest bufor dla N pozycji dla N procesorów logicznych (wątków). Wartości są okresowo aktualizowane w buforze przy użyciu liczników wydajności Windows. Wartości te są zwracane, gdy żądane jest `system.cpu.util[n]`, gdzie 0 <= n < N.

Jeszcze jedna pozycja w buforze jest używana dla `system.cpu.util[total]`.

Zabbix automatycznie wybiera różne liczniki wydajności, aby obsługiwać zarówno systemy NUMA, jak i starsze wersje Windows bez obsługi grup procesorów.

Jeśli liczba procesorów logicznych (wątków) jest mniejsza lub równa 64, a liczba grup procesorów jest równa 1, wtedy:

```
N to liczba procesorów logicznych (wątków).

\Processor(_Total)\% Processor Time
\Processor(0)\% Processor Time
\Processor(1)\% Processor Time
\Processor(2)\% Processor Time
...
\Processor(N-1)\% Processor Time
```

W przeciwnym razie:

```
G to liczba grup procesorów, a N to liczba procesorów logicznych (wątków) w grupie.

\Processor Information(_Total)\% Processor Time
\Processor Information(0,0)\% Processor Time
\Processor Information(0,1)\% Processor Time
\Processor Information(0,2)\% Processor Time
...
\Processor Information(0,N-1)\% Processor Time
...
\Processor Information(G-1,0)\% Processor Time
\Processor Information(G-1,1)\% Processor Time
\Processor Information(G-1,2)\% Processor Time
...
\Processor Information(G-1,N-1)\% Processor Time
```

19 Obsługa dużych wartości JSON

Aby zapewnić niezawodną obsługę dużych wartości dla typu danych JSON data type (1MiB lub więcej), przejrzyj i w razie potrzeby zastosuj następujące zmiany konfiguracyjne:

1. Jeśli używasz MySQL lub MariaDB, zwiększ maksymalny dozwolony rozmiar pakietu w `/etc/mysql/my.cnf` (w niektórych systemach wartość domyślna może wynosić 1MB):

```
[mysqld]
max_allowed_packet=128M

[mysqldump]
max_allowed_packet=1G
```

2. W razie potrzeby dostosuj dodatkowe server system variables oraz InnoDB system variables w MySQL/MariaDB. Na przykład:

```
innodb_io_capacity=1900
connect_timeout=600
wait_timeout=57600
interactive_timeout=57600
net_read_timeout=7200
net_write_timeout=7200
net-buffer-length=32704
```

3. Zwiększ `HistoryCacheSize` do 2G w pliku konfiguracyjnym serwera Zabbix.

4. Jeśli używasz Zabbix proxy, zwiększ `HistoryCacheSize` do 2G oraz `ProxyMemoryBufferSize` do 2G w pliku konfiguracyjnym proxy.

5. Jeśli używasz Zabbix agent, zwiększ limity czasu komunikacji między serwerem/proxy Zabbix a agentem (np. limity czasu pozycji lub wartość parametru `Timeout` w plikach konfiguracyjnych Zabbix server/proxy i agent). W przeciwnym razie komunikaty między nimi mogą nie zostać ukończone i mogą pojawić się błędy, takie jak *"message length does not match expected length"*. Przejrzyj również inne limity czasu, jeśli to konieczne, takie jak limit czasu script timeout lub limit czasu item test.

5 Obsługiwane funkcje

Zobacz Wyrażenie wyzwalacza.

6 Makra

Możliwe jest użycie gotowych obsługiwanych makr oraz makr użytkownika obsługiwanych w zależności od lokalizacji.

1 Makra obsługiwane przez lokalizację

Przegląd

Tabela makr obsługiwanych w danej lokalizacji zawiera informacje referencyjne o wszystkich makrach (wbudowanych, wyrażeń oraz definiowanych przez użytkownika), które są obsługiwane w określonej lokalizacji.

Jeśli obsługiwane są wszystkie makra z powiązanej grupy, podawana jest tylko nazwa grupy. Kliknij nazwę każdego makra lub nazwę grupy, aby zobaczyć pełne szczegóły dotyczące makr.

Lista szczegółów makr zawiera szczegółowy wykaz wszystkich makr **wbudowanych**, pogrupowanych według obszaru zastosowania. Należy pamiętać, że aby dostosować wartości makr (na przykład skrócić je lub wyodrębnić określone podciągi), można użyć funkcji makr.

Makra obsługiwane według lokalizacji

Lokalizacja	Obsługiwane makra	Komentarze
Akcja		
Warunek okresu czasu, Domyślny czas trwania kroku operacji, Czas trwania kroku	Makra definiowane przez użytkownika (tylko globalne)	Pojedyncze makro musi wypełniać całe pole; wiele makr/mieszanie z tekstem nie jest obsługiwane
Powiadomienia i polecenia		
Oparte na wyzwalaczach	Makra akcji Makra daty/czasu {ESC.HISTORY} Makra zdarzenia, makra zdarzenia przyczyny/objawu Makra aktualizacji zdarzenia: {EVENT.UPDATE.HISTORY}, {EVENT.UPDATE.STATUS} Makro wyrażenia: {?EXPRESSION} {FUNCTION.VALUE} Makra hosta: {HOST.CONN}, {HOST.DESCRIPTION}, {HOST.DNS}, {HOST.HOST}, {HOST.ID}, {HOST.IP}, {HOST.NAME}, {HOST.PORT} Makra hosta docelowego (tylko polecenia) Makra inwentarza hosta Makra pozycji (z wyjątkiem {ITEM.STATE}, {ITEM.STATE.ERROR}) Makra proxy Makra wyzwalacza: {TRIGGER.DESCRIPTION}, {TRIGGER.EVENTS.*}, {TRIGGER.EXPRESSION}, {TRIGGER.EXPRESSION.EXPLAIN}, {TRIGGER.EXPRESSION.RECOVERY}, {TRIGGER.ID}, {TRIGGER.HOSTGROUP.NAME}, {TRIGGER.NAME}, {TRIGGER.NAME.ORIG}, {TRIGGER.NSEVERITY}, {TRIGGER.SEVERITY}, {TRIGGER.STATUS}, {TRIGGER.TEMPLATE.NAME}, {TRIGGER.URL}, {TRIGGER.URL.NAME}, {TRIGGER.VALUE} Makra definiowane przez użytkownika	Zobacz także: Używanie makr w wiadomościach

Lokalizacja	Obsługiwane makra	Komentarze
Aktualizacja problemu	Makra akcji Makra daty/czasu {ESC.HISTORY} Makra zdarzenia, makra zdarzenia przyczyny/objawu, makra zdarzenia odzyskania Makra aktualizacji zdarzenia: wszystkie (z wyjątkiem {EVENT.UPDATE.NSEVERITY}, {EVENT.UPDATE.SEVERITY}) Makro wyrażenia: {?EXPRESSION} Makra funkcji Makra hosta: {HOST.CONN}, {HOST.DESCRIPTION}, {HOST.DNS}, {HOST.HOST}, {HOST.ID}, {HOST.IP}, {HOST.NAME}, {HOST.PORT} Makra hosta docelowego (tylko polecenia) Makra inwentarza hosta Makra pozycji (z wyjątkiem {ITEM.STATE}, {ITEM.STATE.ERROR}) Makra proxy Makra wyzwalacza: {TRIGGER.DESCRIPTION}, {TRIGGER.EVENTS.*}, {TRIGGER.EXPRESSION}, {TRIGGER.EXPRESSION.EXPLAIN}, {TRIGGER.EXPRESSION.RECOVERY}, {TRIGGER.ID}, {TRIGGER.HOSTGROUP.NAME}, {TRIGGER.NAME}, {TRIGGER.NAME.ORIG}, {TRIGGER.NSEVERITY}, {TRIGGER.SEVERITY}, {TRIGGER.STATUS}, {TRIGGER.TEMPLATE.NAME}, {TRIGGER.URL}, {TRIGGER.URL.NAME}, {TRIGGER.VALUE} {USER.FULLNAME} Makra definiowane przez użytkownika	
Odzyskanie problemu	Makra zdarzenia odzyskania {FUNCTION.RECOVERY.VALUE} {TRIGGER.EXPRESSION.RECOVERY.EXPLAIN}	
Wykrywanie	Makra akcji Makra daty/czasu Makra wykrywania Makra zdarzenia: {EVENT.AGE}, {EVENT.DATE}, {EVENT.ID}, {EVENT.OBJECT}, {EVENT.SOURCE}, {EVENT.TIME}, {EVENT.TIMESTAMP} Makra hosta docelowego (tylko polecenia) Makra proxy	
Autorejestracja	Makra akcji Makra daty/czasu Makra zdarzenia: {EVENT.AGE}, {EVENT.DATE}, {EVENT.ID}, {EVENT.OBJECT}, {EVENT.SOURCE}, {EVENT.TIME}, {EVENT.TIMESTAMP} Makra hosta: {HOST.HOST}, {HOST.IP}, {HOST.PORT}, {HOST.METADATA} Makra hosta docelowego (tylko polecenia) Makra proxy	
Oparte na usługach	Makra akcji Makra daty/czasu {ESC.HISTORY} Makra zdarzenia: wszystkie z wyjątkiem {EVENT.ACK.STATUS}, {EVENT.OPDATA} Makra usługi Makra definiowane przez użytkownika	
Odzyskanie usługi	Makra zdarzenia (z wyjątkiem {EVENT.ACK.STATUS}, {EVENT.OPDATA}), makra zdarzenia odzyskania	

Lokalizacja	Obsługiwane makra	Komentarze
Aktualizacja usługi	Makra akcji Makra daty/czasu {ESC.HISTORY} Makra zdarzenia (z wyjątkiem {EVENT.ACK.STATUS}, {EVENT.OPDATA}) Makra aktualizacji zdarzenia: {EVENT.UPDATE.DATE}, {EVENT.UPDATE.NSEVERITY}, {EVENT.UPDATE.SEVERITY}, {EVENT.UPDATE.STATUS}, {EVENT.UPDATE.TIME}, {EVENT.UPDATE.TIMESTAMP} Makra usługi Makra definiowane przez użytkownika	
Powiadomienia wewnętrzne	Makra akcji Makra daty/czasu {ESC.HISTORY} Makra zdarzenia (z wyjątkiem {EVENT.NSEVERITY}, {EVENT.SEVERITY}), makra zdarzenia odzyskania Makra hosta: {HOST.CONN}, {HOST.DESCRIPTION}, {HOST.DNS}, {HOST.HOST}, {HOST.IP}, {HOST.NAME}, {HOST.PORT} Makra inwentarza hosta Makra pozycji: {ITEM.DESCRIPTION}, {ITEM.DESCRIPTION.ORIG}, {ITEM.ID}, {ITEM.KEY}, {ITEM.KEY.ORIG}, {ITEM.NAME}, {ITEM.NAME.ORIG}, {ITEM.VALUETYPE} Makra proxy	
Oparte na pozycjach	Makra pozycji: {ITEM.STATE}, {ITEM.STATE.ERROR}	
Oparte na regułach LLD	Makra powiadomienia low-level discovery	
Oparte na wyzwalaczach	Makra wyzwalacza: {TRIGGER.DESCRIPTION}, {TRIGGER.EXPRESSION}, {TRIGGER.EXPRESSION.RECOVERY}, {TRIGGER.HOSTGROUP.NAME}, {TRIGGER.ID}, {TRIGGER.NAME}, {TRIGGER.NAME.ORIG}, {TRIGGER.NSEVERITY}, {TRIGGER.SEVERITY}, {TRIGGER.STATE}, {TRIGGER.STATE.ERROR}, {TRIGGER.TEMPLATE.NAME}, {TRIGGER.URL}, {TRIGGER.URL.NAME} Makra definiowane przez użytkownika	
Parametry skryptu alertu	Makra alertu Makra definiowane przez użytkownika (tylko globalne)	
Connector		
Pole URL, Username, Password, Bearer token, HTTP proxy, SSL certificate, SSL key file, SSL key password	Makra definiowane przez użytkownika (tylko globalne)	
Pole Timeout	Makra definiowane przez użytkownika (tylko globalne)	Pojedyncze makro musi wypełniać całe pole; wiele makr/mieszanie z tekstem nie jest obsługiwane.

Lokalizacja	Obsługiwane makra	Komentarze
Nazwa wykresu	Makro wyrażenia: {?EXPRESSION}	W tym makrze w tej lokalizacji obsługiwana jest tylko pojedyncza funkcja **avg**, **last**, **max**, **min** z sekundami jako parametrem (mogą być używane sufiksy czasu). Makro {HOST.HOST<1-9>} może być użyte jako host wewnątrz makra (zobacz także makra indeksowane). Przykład użycia: {?avg(/{HOST.HOST}/item.key,1h)} Nieobsługiwane użycie: {?last(/host/item1)/last(/host/item2)} {?last(/host/item1)*10} {?count(/host/item1,5m)}
Host, prototyp hosta		
Interfejs IP/DNS	Makra hosta: {HOST.CONN}, {HOST.DNS}, {HOST.HOST}, {HOST.IP}, {HOST.NAME} Makra definiowane przez użytkownika [1]	[1] W przypadku adresu IP pojedyncze makro musi wypełniać całe pole; wiele makr/mieszanie z tekstem nie jest obsługiwane
Port interfejsu	Makra definiowane przez użytkownika	Pojedyncze makro musi wypełniać całe pole; wiele makr/mieszanie z tekstem nie jest obsługiwane
SNMP community *SNMPv3 Context name, Security name, Authentication passphrase, Privacy passphrase* *IPMI username, password*	Makra definiowane przez użytkownika	
Pozycja, prototyp pozycji, reguła LLD		
Nazwa	Makra definiowane przez użytkownika	Nieobsługiwane w nazwach reguł LLD.
Opis	Makra definiowane przez użytkownika	

Lokalizacja	Obsługiwane makra	Komentarze
	Parametry klucza	Makra hosta: {HOST.CONN}, {HOST.DNS}, {HOST.HOST}, {HOST.IP}, {HOST.NAME}, {HOST.PORT} Makra definiowane przez użytkownika	Obsługiwane makra {HOST.*} zostaną rozwinięte do interfejsu wybranego dla pozycji. Gdy są używane w pozycjach bez interfejsów, zostaną rozwinięte odpowiednio do interfejsu Zabbix agent, SNMP, JMX lub IPMI hosta w tej kolejności priorytetu albo do wartości 'UNKNOWN', jeśli host nie ma żadnego interfejsu.
	Pola Update interval, Custom intervals, Timeout (dostępne dla obsługiwanych typów pozycji), Store up to (dla historii/trendów)	Makra definiowane przez użytkownika	Pojedyncze makro musi wypełniać całe pole; wiele makr/mieszanie z tekstem nie jest obsługiwane.
	Pola Delete lost resources, Disable lost resources	Makra definiowane przez użytkownika	Te pola są obsługiwane tylko dla reguł LLD. Pojedyncze makro musi wypełniać całe pole; wiele makr/mieszanie z tekstem nie jest obsługiwane.
	Parametry kroku przetwarzania wstępnego (w tym skrypty niestandardowe), *parametry niestandardowej obsługi błędów* (*Set value to* i *Set error to*)	Makra definiowane przez użytkownika	
	Wyrażenia regularne filtra	Makra hosta: {HOST.CONN}, {HOST.DNS}, {HOST.HOST}, {HOST.IP}, {HOST.NAME}, {HOST.PORT} Makra definiowane przez użytkownika	Te pola są obsługiwane tylko dla reguł LLD.
	Wyrażenia regularne filtra nadpisania	Makra definiowane przez użytkownika	Te pola są obsługiwane tylko dla reguł LLD.
	Operacje nadpisania: *Update interval*, *History storage period*, *Trend storage period* (dla prototypów pozycji)	Makra definiowane przez użytkownika	Te pola są obsługiwane tylko dla reguł LLD. Pojedyncze makro musi wypełniać całe pole; wiele makr/mieszanie z tekstem nie jest obsługiwane.
Typy pozycji			

Lokalizacja	Obsługiwane makra	Komentarze
Browser pozycja *nazwy i wartości parametrów*	Makra hosta: {HOST.CONN}, {HOST.DNS}, {HOST.HOST}, {HOST.IP}, {HOST.NAME}, {HOST.PORT} Makra inwentarza hosta Makra pozycji: {ITEM.ID}, {ITEM.KEY}, {ITEM.KEY.ORIG} Makra definiowane przez użytkownika	
Script pozycja *nazwy i wartości parametrów*		
Formuła pozycji **Calculated/aggregate** (*stałe wyrażenia*, *parametry funkcji*, *parametry klucza pozycji*, (tylko aggregate item) *warunki filtra* (nazwa grupy hostów i nazwa tagu))	Makra definiowane przez użytkownika	
Database monitor pozycja *pola Username, Password, SQL query*	Makra definiowane przez użytkownika	
HTTP agent pozycja *pola URL, Query fields, Request body, Headers (names and values), SSL certificate file, SSL key file*	Makra hosta: {HOST.CONN}, {HOST.DNS}, {HOST.HOST}, {HOST.IP}, {HOST.NAME}, {HOST.PORT} Makra pozycji: {ITEM.ID}, {ITEM.KEY}, {ITEM.KEY.ORIG} Makra definiowane przez użytkownika	Adresy URL zawierające tajne makro nie będą działać, ponieważ makro w nich zostanie rozwinięte jako ”******”
HTTP agent pozycja *pole HTTP Proxy*	Makra pozycji: {ITEM.ID}, {ITEM.KEY}, {ITEM.KEY.ORIG} Makra definiowane przez użytkownika	
HTTP agent pozycja *pola Required status codes, HTTP authentication username/password, SSL key password*	Makra definiowane przez użytkownika	
HTTP agent pozycja *pole Allowed hosts*	Makra hosta: {HOST.CONN}, {HOST.DNS}, {HOST.HOST}, {HOST.IP}, {HOST.NAME}, {HOST.PORT} Makra definiowane przez użytkownika	
JMX agent pozycja *pole Endpoint*	Makra hosta: {HOST.CONN}, {HOST.DNS}, {HOST.HOST}, {HOST.IP}, {HOST.PORT} Makra definiowane przez użytkownika	
Trapper pozycja *pole Allowed hosts*		
SNMP agent pozycja *pole SNMP OID*	Makra definiowane przez użytkownika	
SSH and Telnet pozycja *skrypt*	Makra hosta: {HOST.CONN}, {HOST.DNS}, {HOST.HOST}, {HOST.IP}, {HOST.NAME}, {HOST.PORT} Makra definiowane przez użytkownika	
SSH agent pozycja *pola Username, Public key file, Private key file, Password*	Makra definiowane przez użytkownika	
Telnet agent pozycja *pola Username, Password*	Makra definiowane przez użytkownika	
Mapa		

Lokalizacja	Obsługiwane makra	Komentarze
URL, nazwa URL	Makra hosta: {HOST.CONN}, {HOST.DESCRIPTION}, {HOST.DNS}, {HOST.HOST}, {HOST.ID}, {HOST.IP}, {HOST.NAME}, {HOST.PORT} {HOSTGROUP.ID} Makra inwentarza hosta Makra mapy {TRIGGER.ID}	
Etykieta elementu	Makro wyrażenia: {?EXPRESSION} [1] Makra hosta: {HOST.CONN}, {HOST.DESCRIPTION}, {HOST.DNS}, {HOST.HOST}, {HOST.ID}, {HOST.IP}, {HOST.NAME}, {HOST.PORT} {HOSTGROUP.ID} Makra inwentarza hosta Makra mapy Makra wyzwalacza: {TRIGGER.EVENTS.*}, {TRIGGER.ID}, {TRIGGER.PROBLEM.EVENTS.*}, {TRIGGERS.ACK}, {TRIGGERS.PROBLEM.ACK}, {TRIGGERS.PROBLEM.UNACK}, {TRIGGERS.UNACK}	[1] W tym makrze w tej lokalizacji obsługiwana jest tylko pojedyncza funkcja **avg**, **last**, **max**, **min** z sekundami jako parametrem (mogą być używane sufiksy czasu). Makro {HOST.HOST<1-9>} może być użyte jako host wewnątrz makra. Przykład użycia: {?avg(/{HOST.HOST}/item.key,1h)} Nieobsługiwane użycie: {?last(/host/item1)/last(/host/item2)} {?last(/host/item1)*10} {?count(/host/item1,5m)}
Etykieta łącza	Makro wyrażenia: {?EXPRESSION} [1]	
Etykieta kształtu *Pole tekstowe w kształtach mapy*	Makro wyrażenia: {?EXPRESSION} [1] {MAP.NAME}	
Wykrywanie sieci		
Pole Update interval	Makra definiowane przez użytkownika (tylko globalne)	Pojedyncze makro musi wypełniać całe pole; wiele makr/mieszanie z tekstem nie jest obsługiwane.
Pola SNMP community, SNMP OID *Pola SNMPv3 Context name, Security name, Authentication passphrase, Privacy passphrase*	Makra definiowane przez użytkownika (tylko globalne)	
Proxy		
Address for active agents > *Port* (jeśli proxy należy do grupy) Dla trybu passive proxy: pola interfejsu *Address* i *Port* *Timeouts for item types* w trybie nadpisania	Makra definiowane przez użytkownika (tylko globalne)	Pojedyncze makro musi wypełniać całe pole; wiele makr/mieszanie z tekstem nie jest obsługiwane.
Grupa proxy		

Lokalizacja	Obsługiwane makra	Komentarze
Pola Failover period, Minimum number of proxies	Makra definiowane przez użytkownika (tylko globalne)	Pojedyncze makro musi wypełniać całe pole; wiele makr/mieszanie z tekstem nie jest obsługiwane.
Skrypty		
Polecenia, tekst potwierdzenia (Typ: script, ręczna **akcja hosta**)	Makra hosta: {HOST.CONN}, {HOST.DNS}, {HOST.HOST}, {HOST.ID} [1], {HOST.IP}, {HOST.NAME}, {HOST.PORT} Makra inwentarza hosta [2] {MANUALINPUT} Makra nazwy użytkownika Makra definiowane przez użytkownika	[1] Tylko tekst potwierdzenia [2] Obsługiwane dla Zabbix server i Zabbix proxy
Polecenia (Typ: script, ręczna **akcja zdarzenia**)	Makra daty/czasu Makra zdarzenia, makra zdarzenia przyczyny/objawu, makra zdarzenia odzyskania (jeśli odzyskanie nastąpiło) Makra aktualizacji zdarzenia: {EVENT.UPDATE.HISTORY}, {EVENT.UPDATE.STATUS} {FUNCTION.VALUE} Makra hosta: {HOST.CONN}, {HOST.DESCRIPTION}, {HOST.DNS}, {HOST.HOST}, {HOST.ID}, {HOST.IP}, {HOST.NAME}, {HOST.PORT} Makra inwentarza hosta Makra pozycji (z wyjątkiem {ITEM.STATE}, {ITEM.STATE.ERROR}) {MANUALINPUT} Makra proxy Makra wyzwalacza: {TRIGGER.DESCRIPTION}, {TRIGGER.EVENTS.*}, {TRIGGER.EXPRESSION}, {TRIGGER.EXPRESSION.EXPLAIN}, {TRIGGER.EXPRESSION.RECOVERY}, {TRIGGER.EXPRESSION.RECOVERY.EXPLAIN}, {TRIGGER.HOSTGROUP.NAME}, {TRIGGER.ID}, {TRIGGER.NAME}, {TRIGGER.NAME.ORIG}, {TRIGGER.NSEVERITY}, {TRIGGER.SEVERITY}, {TRIGGER.STATUS}, {TRIGGER.TEMPLATE.NAME}, {TRIGGER.URL}, {TRIGGER.URL.NAME}, {TRIGGER.VALUE} Makra nazwy użytkownika Makra definiowane przez użytkownika	
Tekst potwierdzenia (Typ: script, ręczna **akcja zdarzenia**)	Makra zdarzenia: {EVENT.ID}, {EVENT.NAME}, {EVENT.NSEVERITY}, {EVENT.SEVERITY}, {EVENT.STATUS}, {EVENT.VALUE} Makra hosta: {HOST.CONN}, {HOST.DNS}, {HOST.HOST}, {HOST.ID}, {HOST.IP}, {HOST.NAME}, {HOST.PORT} Makra inwentarza hosta {MANUALINPUT} Makra nazwy użytkownika Makra definiowane przez użytkownika	
URL, tekst potwierdzenia (Typ: URL, ręczna **akcja hosta/zdarzenia**)		
Nazwa i wartość tagu	Makra hosta: {HOST.CONN}, {HOST.DNS}, {HOST.HOST}, {HOST.ID}, {HOST.IP}, {HOST.NAME}, {HOST.PORT} Makra inwentarza hosta Makra pozycji: {ITEM.LASTVALUE*}, {ITEM.LOG.*}, {ITEM.VALUE*} Makra wyzwalacza: {TRIGGER.ID} (tylko wartość tagu wyzwalacza) Makra definiowane przez użytkownika	Makra nazwy i wartości tagu są rozwijane tylko podczas procesu generowania zdarzenia.

Lokalizacja	Obsługiwane makra	Komentarze
Wyzwalacz		
Nazwa	Makra hosta: {HOST.CONN}, {HOST.DNS}, {HOST.HOST}, {HOST.IP}, {HOST.NAME}, {HOST.PORT} Makra pozycji: {ITEM.LASTVALUE*}, {ITEM.LOG.*}, {ITEM.VALUE*} Makra/referencje pozycyjne: $1 . . . $9 Makra definiowane przez użytkownika	
Nazwa zdarzenia	Makra daty/czasu: {TIME}, {TIMESTAMP} Makro wyrażenia: {?EXPRESSION} Makra funkcji Makra hosta: {HOST.CONN}, {HOST.DNS}, {HOST.HOST}, {HOST.IP}, {HOST.NAME}, {HOST.PORT} Makra pozycji: {ITEM.LASTVALUE*}, {ITEM.LOG.*}, {ITEM.VALUE*} Makra wyzwalacza: {TRIGGER.EXPRESSION.EXPLAIN}	
Dane operacyjne	Makra hosta: {HOST.CONN}, {HOST.DNS}, {HOST.HOST}, {HOST.IP}, {HOST.NAME}, {HOST.PORT} Makra pozycji: {ITEM.LASTVALUE*}, {ITEM.LOG.*}, {ITEM.VALUE*} Makra definiowane przez użytkownika	
Wyrażenie	{TRIGGER.VALUE} Makra definiowane przez użytkownika [1]	[1] Tylko w stałych i parametrach funkcji; tajne makra nie są obsługiwane
Pola Tag for matching, Menu entry name, Menu entry URL	Makra definiowane przez użytkownika	Adresy URL zawierające tajne makro nie będą działać, ponieważ makro w nich zostanie rozwinięte jako ”******”.
Opis	Makra hosta: {HOST.CONN}, {HOST.DNS}, {HOST.HOST}, {HOST.IP}, {HOST.NAME}, {HOST.PORT} Makra pozycji: {ITEM.LASTVALUE*}, {ITEM.LOG.*}, {ITEM.VALUE*} Makra definiowane przez użytkownika	
URL	{EVENT.ID} Makra hosta: {HOST.CONN}, {HOST.DNS}, {HOST.HOST}, {HOST.ID}, {HOST.IP}, {HOST.NAME}, {HOST.PORT} Makra pozycji: {ITEM.LASTVALUE*}, {ITEM.LOG.*}, {ITEM.VALUE*} {TRIGGER.ID}	
Polecenia parametrów użytkownika	Makra/referencje pozycyjne: $1 . . . $9	
Scenariusz web		
Pola Name, Agent, HTTP proxy	Makra definiowane przez użytkownika	
Pole Update interval	Makra definiowane przez użytkownika	Pojedyncze makro musi wypełniać całe pole; wiele makr/mieszanie z tekstem nie jest obsługiwane.
Pola Variables, Headers, SSL certificate, SSL key file	Makra hosta: {HOST.CONN}, {HOST.DNS}, {HOST.HOST}, {HOST.IP}, {HOST.NAME}, {HOST.PORT} Makra definiowane przez użytkownika	
Pola User, Password, SSL key password	Makra definiowane przez użytkownika	

Lokalizacja	Obsługiwane makra	Komentarze
Krok scenariusza web *pola Name, Variables (tylko wartości)*	Makra definiowane przez użytkownika	
Krok scenariusza web *pola Timeout, Required status codes*	Makra definiowane przez użytkownika	Pojedyncze makro musi wypełniać całe pole; wiele makr/mieszanie z tekstem nie jest obsługiwane.
Krok scenariusza web *pola URL, Headers (names and values), Required string*	Makra hosta: {HOST.CONN}, {HOST.DNS}, {HOST.HOST}, {HOST.IP}, {HOST.NAME}, {HOST.PORT} Makra definiowane przez użytkownika	
Krok scenariusza web *pole Post*	Makra hosta: {HOST.CONN}, {HOST.DNS}, {HOST.HOST}, {HOST.IP}, {HOST.NAME}, {HOST.PORT}	
Typ nośnika web-hook		
Wartości parametrów	Makra alertu Wszystkie makra obsługiwane w powiadomieniach o problemach opartych na wyzwalaczach (zobacz wyżej)	Pojedyncze makro musi wypełniać całe pole; wiele makr/mieszanie z tekstem nie jest obsługiwane.
Skrypt JavaScript, nazwa parametru skryptu *JavaScript*	Makra definiowane przez użytkownika (tylko globalne)	
Menu entry name, Menu entry URL	{EVENT.TAGS.<tag name>}	
Widżety		
Gauge widżet *pole Description*	Makra hosta: {HOST.CONN}, {HOST.DESCRIPTION}, {HOST.DNS}, {HOST.HOST}, {HOST.ID}, {HOST.IP}, {HOST.NAME}, {HOST.PORT} Makra inwentarza hosta Makra pozycji (z wyjątkiem {ITEM.STATE.ERROR}) Makra definiowane przez użytkownika (tylko globalne)	
Honeycomb widżet *pole Primary/secondary label*		
Item value widżet *pole Description*		
Top hosts widżet *kolumna Text data*	Makra hosta: {HOST.CONN}, {HOST.DESCRIPTION}, {HOST.DNS}, {HOST.HOST}, {HOST.ID}, {HOST.IP}, {HOST.NAME}, {HOST.PORT} Makra inwentarza hosta Makra definiowane przez użytkownika (tylko globalne)	
URL (Dynamic) widżet *pole URL*	Makra hosta: {HOST.CONN}, {HOST.DNS}, {HOST.HOST}, {HOST.ID}, {HOST.IP}, {HOST.NAME}, {HOST.PORT} Makra definiowane przez użytkownika macros	
Inne lokalizacje		
Pole Working time	Makra definiowane przez użytkownika (tylko globalne)	Pojedyncze makro musi wypełniać całe pole; wiele makr/mieszanie z tekstem nie jest obsługiwane.

Lokalizacja	Obsługiwane makra	Komentarze
Pole Timeouts for item types (ustawienie globalne)		
Nośnik użytkownika *pole When active*	Makra definiowane przez użytkownika (tylko globalne)	
Typ nośnika Email *pola Username, Password*	Makra definiowane przez użytkownika (tylko globalne)	Zalecane są tajne makra.
Raporty zaplanowane *pola Subject, Message*	Makra daty/czasu: {TIME}, {TIMESTAMP}	

Szczegóły makr

Ta lista zawiera szczegóły dotyczące każdego wbudowanego makra, pogrupowane według obszaru zastosowania:

- Makra akcji
- Makra alertów
- Makra daty/czasu
- Makra wykrywania
- Makra zdarzeń
  - Makra aktualizacji zdarzeń
  - Makra zdarzeń przyczyny/objawu
  - Makra zdarzeń odzyskiwania
- Makra eskalacji
- Makra funkcji
- Makra hosta
  - Makra hosta docelowego
- Makra grup hostów
- Makra inwentarza hosta
- Makra pozycji
- Makra powiadomień wykrywania niskiego poziomu
- Makra map
- Makra proxy
- Makra skryptów
- Makra usług
- Makra wyzwalaczy
- Makra nazw użytkowników

Makra akcji

{ACTION.ID}

Numeryczny identyfikator ID wyzwolonej akcji.

{ACTION.NAME}

Nazwa uruchomionej akcji.

Makra alertów

{ALERT.MESSAGE}

Wartość *Domyślna wiadomość* z konfiguracji akcji.

{ALERT.SENDTO}

Wartość *Send to* z konfiguracji mediów użytkownika.

{ALERT.SUBJECT}

Wartość *Default subject* z konfiguracji akcji.

Makra daty i czasu

{DATE}

Bieżąca data w formacie `yyyy.mm.dd`.

{TIME}

Bieżący czas w formacie `hh:mm:ss`.

{TIMESTAMP}

Bieżący czas w formacie znacznika czasu UNIX.

Makra wykrywania

{DISCOVERY.DEVICE.IPADDRESS}

Adres IP wykrytego urządzenia.
 Dostępne zawsze, nie zależy od dodania hosta.

{DISCOVERY.DEVICE.DNS}

Nazwa DNS wykrytego urządzenia.
 Zawsze dostępna, nie zależy od dodania hosta.

{DISCOVERY.DEVICE.STATUS}

Status wykrytego urządzenia (UP/DOWN).

{DISCOVERY.DEVICE.UPTIME}

Czas od ostatniej zmiany statusu wykrywania dla określonego urządzenia.
 Na przykład: 1h 29m 01s.
 Dla urządzeń ze statusem DOWN jest to okres ich niedostępności.

{DISCOVERY.RULE.NAME}

Nazwa reguły wykrywania, która wykryła obecność lub brak urządzenia/usługi.

{DISCOVERY.SERVICE.NAME}

Nazwa wykrytej usługi.
 Na przykład: HTTP.

{DISCOVERY.SERVICE.PORT}

Port wykrytej usługi.
 Na przykład: 80.

{DISCOVERY.SERVICE.STATUS}

Status wykrytej usługi (UP/DOWN).

{DISCOVERY.SERVICE.UPTIME}

Czas, jaki upłynął od ostatniej zmiany statusu wykrywania dla określonej usługi.
 Na przykład: 1h 29m 01s.
 Dla usług ze statusem DOWN jest to okres ich niedostępności.

Makra eskalacji

{ESC.HISTORY}

Dziennik wcześniej wysłanych powiadomień, ich krok eskalacji i status (*wysłane*, *w trakcie* lub *nieudane*).

Makra zdarzeń

{EVENT.ACK.STATUS}

Status potwierdzenia zdarzenia (Tak/Nie).

{EVENT.AGE}

Wiek zdarzenia, które wyzwoliło akcję, z dokładnością do jednej sekundy.
 Przydatne w eskalowanych wiadomościach. Na przykład: 9m 13s.

{EVENT.DATE}

Data zdarzenia, które wyzwoliło akcję, w formacie `rrrr.mm.dd`.
 Na przykład: 2025.04.14.

{EVENT.DURATION}

Czas trwania zdarzenia (różnica czasu między zdarzeniami problemu i odzyskania), z dokładnością do jednej sekundy.
 Przydatne w wiadomościach odzyskiwania problemu.

{EVENT.ID}

Numeryczny identyfikator zdarzenia, które wywołało akcję.

{EVENT.NAME}

Nazwa zdarzenia, które wyzwoliło akcję.

{EVENT.NSEVERITY}

Wartość liczbowa ważności zdarzenia.
 Możliwe wartości: *0* - Niesklasyfikowane, *1* - Informacja, *2* - Ostrzeżenie, *3* - Średni, *4* - Wysoki, *5* - Katastrofa.

{EVENT.OBJECT}

Wartość liczbowa obiektu zdarzenia.
 Możliwe wartości: *0* - Wyzwalacz, *1* - Wykryty host, *2* - Wykryta usługa, *3* - Autorejestracja, *4* - Pozycja, *5* - Reguła wykrywania niskiego poziomu.

{EVENT.OPDATA}

Dane operacyjne bazowego wyzwalacza problemu.

{EVENT.SEVERITY}

Nazwa ważności zdarzenia.

{EVENT.SOURCE}

Wartość liczbowa źródła zdarzenia.
 Możliwe wartości: *0* - Wyzwalacz, *1* - Wykrywanie, *2* - Autorejestracja, *3* - Wewnętrzne, *4* - Usługa.

{EVENT.STATUS}

Słowna wartość zdarzenia, które wyzwoliło akcję.

{EVENT.TAGS}

Lista tagów zdarzenia oddzielonych przecinkami.
Rozwijane do pustego ciągu znaków, jeśli nie istnieją żadne tagi.

{EVENT.TAGSJSON}

Tablica JSON zawierająca obiekty tagów zdarzenia.
Rozwijana do pustej tablicy, jeśli nie istnieją żadne tagi.

{EVENT.TAGS.<tag name>}

Wartość tagu zdarzenia, do której odwołuje się nazwa tagu.
 Nazwa tagu zawierająca znaki niealfanumeryczne (w tym nieangielskie wielobajtowe znaki UTF) musi być ujęta w podwójny cudzysłów. Cudzysłowy i ukośniki odwrotne wewnątrz nazwy tagu ujętej w cudzysłów muszą być poprzedzone znakiem ucieczki, czyli ukośnikiem odwrotnym.

{EVENT.TIME}

Czas zdarzenia, które wyzwoliło akcję, w formacie `hh:mm:ss`.
 Na przykład: 12:57:53.

{EVENT.TIMESTAMP}

Znacznik czasu UNIX zdarzenia, które wyzwoliło akcję.

{EVENT.VALUE}

Wartość liczbowa zdarzenia, które wyzwoliło akcję.
 Możliwe wartości: *1* - problem, *0* - odzyskiwanie.

Makra zdarzeń przyczyny/objawu

{EVENT.CAUSE.ACK.STATUS}

Status potwierdzenia zdarzenia przyczyny (Tak/Nie).
 Używane w kontekście zdarzenia symptomu.

{EVENT.CAUSE.AGE}

Wiek zdarzenia będącego przyczyną, z dokładnością do jednej sekundy.
 Przydatne w eskalowanych wiadomościach.
 Używane w kontekście zdarzenia objawowego.

{EVENT.CAUSE.DATE}

Data zdarzenia będącego przyczyną w formacie `rrrr.mm.dd`.
 Używane w kontekście zdarzenia objawu.

{EVENT.CAUSE.DURATION}

Czas trwania zdarzenia przyczyny (różnica czasu między zdarzeniami problemu i odzyskania), z dokładnością do jednej sekundy.
 Przydatne w wiadomościach odzyskiwania problemu.
 Używane w kontekście zdarzenia symptomu.

{EVENT.CAUSE.ID}

Numeryczny identyfikator zdarzenia będącego przyczyną.
 Używany w kontekście zdarzenia objawowego.

{EVENT.CAUSE.NAME}

Nazwa zdarzenia przyczyny.
 Używane w kontekście zdarzenia objawu.

{EVENT.CAUSE.NSEVERITY}

Wartość liczbowa ważności zdarzenia będącego przyczyną.
 Możliwe wartości: *0* - Niesklasyfikowane, *1* - Informacja, *2* - Ostrzeżenie, *3* - Średnie, *4* - Wysokie, *5* - Katastrofa.
 Używane w kontekście zdarzenia objawowego.

{EVENT.CAUSE.OBJECT}

Wartość liczbowa obiektu zdarzenia będącego przyczyną.
 Możliwe wartości: *0* - Wyzwalacz, *1* - Wykryty host, *2* - Wykryta usługa, *3* - Autorejestracja, *4* - Pozycja, *5* - Reguła wykrywania niskiego poziomu.
 Używane w kontekście zdarzenia będącego symptomem.

{EVENT.CAUSE.OPDATA}

Dane operacyjne bazowego wyzwalacza problemu.
 Używane w kontekście zdarzenia symptomu.

{EVENT.CAUSE.SEVERITY}

Nazwa poziomu ważności zdarzenia będącego przyczyną.
 Możliwe wartości: *Niesklasyfikowane*, *Informacja*, *Ostrzeżenie*, *Średni*, *Wysoki*, *Katastrofa*.
 Używane w kontekście zdarzenia będącego symptomem.

{EVENT.CAUSE.SOURCE}

Wartość liczbowa źródła zdarzenia przyczyny.
 Możliwe wartości: *0* - Wyzwalacz, *1* - Odkrywanie, *2* - Autorejestracja, *3* - Wewnętrzne.
 Używane w kontekście zdarzenia objawu.

{EVENT.CAUSE.STATUS}

Słowna wartość zdarzenia będącego przyczyną.
 Używana w kontekście zdarzenia objawowego.

{EVENT.CAUSE.TAGS}

Lista tagów zdarzenia przyczyny, rozdzielonych przecinkami.
Rozwijane do pustego ciągu znaków, jeśli tagi nie istnieją.
 Używane w kontekście zdarzenia objawu.

{EVENT.CAUSE.TAGSJSON}

Tablica JSON zawierająca obiekty tagów zdarzenia będącego przyczyną.
Rozwijana do pustej tablicy, jeśli nie istnieją żadne tagi.
 Używana w kontekście zdarzenia objawowego.

{EVENT.CAUSE.TAGS.<tag name>}

Wartość tagu zdarzenia-przyczyny, do której odwołuje się nazwa tagu.
 Nazwa tagu zawierająca znaki niealfanumeryczne (w tym nieangielskie wielobajtowe znaki UTF) musi być ujęta w podwójny cudzysłów. Cudzysłowy i ukośniki odwrotne wewnątrz nazwy tagu ujętej w cudzysłów muszą być poprzedzone ukośnikiem odwrotnym.
 Używane w kontekście zdarzenia objawu.

{EVENT.CAUSE.TIME}

Czas zdarzenia będącego przyczyną w formacie `hh:mm:ss`.
 Używane w kontekście zdarzenia objawowego.

{EVENT.CAUSE.TIMESTAMP}

Znacznik czasu UNIX zdarzenia będącego przyczyną.
 Używany w kontekście zdarzenia objawowego.

{EVENT.CAUSE.UPDATE.HISTORY}

Dziennik aktualizacji problemu będącego przyczyną (potwierdzenia itp.).
 Używane w kontekście zdarzenia objawu.

{EVENT.CAUSE.VALUE}

Wartość liczbowa zdarzenia będącego przyczyną.
 Możliwe wartości: *1* - Problem, *0* - Odzyskiwanie.
 Używane w kontekście zdarzenia objawowego.

{EVENT.SYMPTOMS}

Lista zdarzeń symptomów. Zawiera następujące szczegóły: nazwę hosta, nazwę zdarzenia, ważność, wiek, tagi usługi i wartości.
 To makro jest używane w kontekście zdarzenia przyczyny i zwraca informacje o zdarzeniach symptomów.

Makra zdarzenia odzyskania

{EVENT.RECOVERY.DATE}

Data zdarzenia odzyskania w formacie `yyyy.mm.dd`.

{EVENT.RECOVERY.ID}

Numeryczny identyfikator zdarzenia odzyskania.

{EVENT.RECOVERY.NAME}

Nazwa zdarzenia odzyskiwania.

{EVENT.RECOVERY.STATUS}

Słowna wartość zdarzenia odzyskiwania.

{EVENT.RECOVERY.TAGS}

Lista tagów zdarzenia odzyskania, rozdzielona przecinkami. Rozwijana do pustego ciągu znaków, jeśli nie istnieją żadne tagi.

{EVENT.RECOVERY.TAGSJSON}

Tablica JSON zawierająca obiekty tagów zdarzenia odzyskiwania. Rozwijana do pustej tablicy, jeśli nie istnieją żadne tagi.

{EVENT.RECOVERY.TIME}

Czas zdarzenia odzyskania w formacie `hh:mm:ss`.

{EVENT.RECOVERY.TIMESTAMP}

Znacznik czasu UNIX zdarzenia odzyskania.

{EVENT.RECOVERY.VALUE}

Wartość liczbowa zdarzenia odzyskiwania.

Makra aktualizacji zdarzenia

{EVENT.UPDATE.ACTION}

Czytelna dla człowieka nazwa działania(ń) wykonanych podczas aktualizacji problemu.
 Przyjmuje następujące wartości: *acknowledged*, *unacknowledged*, *commented*, *changed severity from (original severity) to (updated severity)* oraz *closed* (w zależności od tego, ile działań zostanie wykonanych w ramach jednej aktualizacji).

{EVENT.UPDATE.ACTIONJSON}

Tablica JSON zawierająca szczegóły działania(ń) wykonanych podczas aktualizacji problemu.
 Możliwe wartości właściwości JSON:
- true (dla właściwości `acknowledge`, `unacknowledge`, `close`, `unsuppress`, `cause` i `symptom`);
- <ciąg znaków wiadomości> (dla właściwości `message`);
- znacznik czasu (dla właściwości `suppress_until` i `timestamp`) lub 0 (dla właściwości `suppress_until`, jeśli wyciszenie jest bezterminowe);
- 0, 1, 2, 3, 4, 5 (dla właściwości ważności `old` i `new`).

Na przykład: `{"acknowledge":true,"message":"Monthly maintenance.","severity":{"old":2,"new":1},"suppress_unti`

{EVENT.UPDATE.DATE}

Data aktualizacji zdarzenia (potwierdzenia itp.) w formacie `rrrr.mm.dd`.

{EVENT.UPDATE.HISTORY}

Dziennik aktualizacji problemu (potwierdzeń itd.).

{EVENT.UPDATE.MESSAGE}

Wiadomość aktualizacji problemu.

{EVENT.UPDATE.NSEVERITY}

Wartość liczbowa nowego poziomu ważności zdarzenia ustawionego podczas operacji aktualizacji problemu.

{EVENT.UPDATE.SEVERITY}

Nazwa nowego poziomu ważności zdarzenia ustawionego podczas operacji aktualizacji problemu.

{EVENT.UPDATE.STATUS}

Wartość numeryczna statusu aktualizacji problemu.
 Możliwe wartości: *0* - webhook został wywołany z powodu zdarzenia problemu/odzyskania, *1* - operacja aktualizacji.

{EVENT.UPDATE.TIME}

Czas aktualizacji zdarzenia (potwierdzenia itp.) w formacie `hh:mm:ss`.

{EVENT.UPDATE.TIMESTAMP}

Znacznik czasu UNIX aktualizacji zdarzenia update (potwierdzenia itp.).

Makra funkcji

{FUNCTION.VALUE}

Wartość N-tej funkcji opartej na pozycji w wyrażeniu wyzwalacza w momencie wystąpienia zdarzenia.
 Zliczane są tylko funkcje z `/host/key` jako pierwszym parametrem.

 To makro może być używane z indeksem numerycznym, np. {FUNCTION.VALUE<1-9>}, aby wskazać pierwszą, drugą, trzecią itd. funkcję w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{FUNCTION.RECOVERY.VALUE}

Wartość N-tej funkcji opartej na pozycji w wyrażeniu odzyskiwania w momencie wystąpienia zdarzenia.*
 Liczone są tylko funkcje z `/host/key` jako pierwszym parametrem.

 To makro może być używane z indeksem numerycznym, np. {FUNCTION.RECOVERY.VALUE<1-9>}, aby wskazać pierwszą, drugą, trzecią itd. funkcję w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

Makra hosta

{HOST.CONN}

Adres IP lub nazwa DNS hosta, w zależności od ustawień hosta.
 W skryptach globalnych, polach IP/DNS interfejsu oraz scenariuszach web makro zostanie rozwinięte do głównego interfejsu agent. Jeśli interfejs agent nie jest zdefiniowany, zostanie użyty główny interfejs SNMP. Jeśli interfejs SNMP również nie jest zdefiniowany, zostanie użyty główny interfejs JMX. Jeśli interfejs JMX także nie jest zdefiniowany, zostanie użyty główny interfejs IPMI. Jeśli host nie ma żadnego interfejsu, makro zostanie rozwinięte do 'UNKNOWN'.

 To makro może być używane z indeksem numerycznym jako {HOST.CONN<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{HOST.DESCRIPTION}

Opis hosta.

 To makro może być używane z indeksem numerycznym jako {HOST.DESCRIPTION<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{HOST.DNS}

Nazwa DNS hosta.
 W skryptach globalnych, polach IP/DNS interfejsu oraz scenariuszach web makro zostanie rozwinięte do głównego interfejsu agent. Jeśli interfejs agent nie jest zdefiniowany, zostanie użyty główny interfejs SNMP. Jeśli interfejs SNMP również nie jest zdefiniowany, zostanie użyty główny interfejs JMX. Jeśli interfejs JMX także nie jest zdefiniowany, zostanie użyty główny interfejs IPMI. Jeśli host nie ma żadnego interfejsu, makro zostanie rozwinięte do 'UNKNOWN'.

 To makro może być używane z indeksem numerycznym jako {HOST.DNS<1-9>}, aby wskazywać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{HOST.HOST}

Techniczna nazwa hosta.
 Funkcje makr nie są obsługiwane dla tego makra, jeśli jest ono używane jako symbol zastępczy w pierwszym parametrze funkcji historii, na przykład `last(/{HOST.HOST}/{ITEM.KEY})`.

 To makro może być używane z indeksem numerycznym jako {HOST.HOST<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{HOST.ID}

ID hosta.

 Ten makro może być używane z indeksem numerycznym jako {HOST.ID<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{HOST.IP}

Adres IP hosta.
 W skryptach globalnych, polach IP/DNS interfejsu oraz scenariuszach WWW makro zostanie rozwinięte do głównego interfejsu agent. Jeśli interfejs agent nie jest zdefiniowany, zostanie użyty główny interfejs SNMP. Jeśli interfejs SNMP również nie jest zdefiniowany, zostanie użyty główny interfejs JMX. Jeśli interfejs JMX także nie jest zdefiniowany, zostanie użyty główny interfejs IPMI. Jeśli host nie ma żadnego interfejsu, makro zostanie rozwinięte do wartości 'UNKNOWN'.

 To makro może być używane z indeksem numerycznym jako {HOST.IP<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{HOST.METADATA}

Metadane hosta.

 Używane tylko do aktywnej autorejestracji agenta.

{HOST.NAME}

Widoczna nazwa hosta.

 To makro może być używane z indeksem numerycznym jako {HOST.NAME<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{HOST.PORT}

Port hosta (agent).
 W skryptach globalnych, polach IP/DNS interfejsu oraz scenariuszach WWW makro zostanie rozwinięte do głównego interfejsu agent. Jeśli interfejs agent nie jest zdefiniowany, zostanie użyty główny interfejs SNMP. Jeśli interfejs SNMP również nie jest zdefiniowany, zostanie użyty główny interfejs JMX. Jeśli interfejs JMX także nie jest zdefiniowany, zostanie użyty główny interfejs IPMI. Jeśli host nie ma żadnego interfejsu, makro zostanie rozwinięte do 'UNKNOWN'.

 To makro może być używane z indeksem numerycznym jako {HOST.PORT<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

Makra hosta docelowego

{HOST.TARGET.CONN}

Adres IP lub nazwa DNS hosta docelowego.

{HOST.TARGET.DNS}

Nazwa DNS docelowego hosta.

{HOST.TARGET.HOST}

Techniczna nazwa docelowego hosta.

{HOST.TARGET.IP}

Adres IP docelowego hosta.

{HOST.TARGET.NAME}

Widoczna nazwa docelowego hosta.

Makra grup hostów

{HOSTGROUP.ID}

ID grupy hostów.

Makra inwentarza hosta

{INVENTORY.ALIAS}

Pole *Alias* w inwentarzu hosta.

 Ten makro może być używane z indeksem numerycznym, np. {INVENTORY.ALIAS<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.ASSET.TAG}

Pole *Asset tag* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.ASSET.TAG<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.CHASSIS}

Pole *Chassis* w inwentarzu hosta.

 Ten makro może być używane z indeksem numerycznym, np. {INVENTORY.CHASSIS<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.CONTACT}

Pole *Kontakt* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.CONTACT<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.CONTRACT.NUMBER}

Pole *Numer umowy* w inwentarzu hosta.

 Ta makroinstrukcja może być używana z indeksem numerycznym, np. {INVENTORY.CONTRACT.NUMBER<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makroinstrukcje indeksowane.

{INVENTORY.DEPLOYMENT.STATUS}

Pole *Status wdrożenia* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.DEPLOYMENT.STATUS<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.HARDWARE}

Pole *Sprzęt* w inwentarzu hosta.

 Ten makro może być używane z indeksem numerycznym, np. {INVENTORY.HARDWARE<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.HARDWARE.FULL}

Pole *Sprzęt (pełne szczegóły)* w inwentarzu hosta.

 Ten makro może być używane z indeksem numerycznym, np. {INVENTORY.HARDWARE.FULL<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.HOST.NETMASK}

Pole *Maska podsieci hosta* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.HOST.NETMASK<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.HOST.NETWORKS}

Pole *Sieci hosta* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.HOST.NETWORKS<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.HOST.ROUTER}

Pole *Host router* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.HOST.ROUTER<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.HW.ARCH}

Pole *Architektura sprzętowa* w inwentarzu hosta.

 Ten makro może być używane z indeksem numerycznym, np. {INVENTORY.HW.ARCH<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.HW.DATE.DECOMM}

Pole *Data wycofania sprzętu z eksploatacji* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.HW.DATE.DECOMM<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.HW.DATE.EXPIRY}

Pole *Data wygaśnięcia konserwacji sprzętu* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.HW.DATE.EXPIRY<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.HW.DATE.INSTALL}

Pole *Data instalacji sprzętu* w inwentarzu hosta.

 Ten makro może być używane z indeksem numerycznym, np. {INVENTORY.HW.DATE.INSTALL<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.HW.DATE.PURCHASE}

Pole *Data zakupu sprzętu* w inwentarzu hosta.

 Ten makro może być używane z indeksem numerycznym, np. {INVENTORY.HW.DATE.PURCHASE<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.INSTALLER.NAME}

Pole *Nazwa instalatora* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.INSTALLER.NAME<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.LOCATION}

Pole *Lokalizacja* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.LOCATION<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.LOCATION.LAT}

Pole *Szerokość geograficzna lokalizacji* w inwentarzu hosta.

 Ta makroinstrukcja może być używana z indeksem numerycznym, np. {INVENTORY.LOCATION.LAT<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makroinstrukcje indeksowane.

{INVENTORY.LOCATION.LON}

Pole *Długość geograficzna lokalizacji* w inwentarzu hosta.

 Ten makro może być używane z indeksem numerycznym, np. {INVENTORY.LOCATION.LON<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.MACADDRESS.A}

Pole *MAC address A* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.MACADDRESS.A<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.MACADDRESS.B}

Pole *MAC address B* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.MACADDRESS.B<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.MODEL}

Pole *Model* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.MODEL<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.NAME}

Pole *Nazwa* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.NAME<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.NOTES}

Pole *Notatki* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.NOTES<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.OOB.IP}

Pole *adresu IP OOB* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.OOB.IP<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.OOB.NETMASK}

Pole *maski podsieci OOB* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.OOB.NETMASK<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.OOB.ROUTER}

Pole *routera OOB* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.OOB.ROUTER<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.OS}

Pole *OS* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.OS<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.OS.FULL}

Pole *OS (Full details)* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.OS.FULL<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.OS.SHORT}

Pole *OS (Short)* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.OS.SHORT<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.POC.PRIMARY.CELL}

Pole *Primary POC cell* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.POC.PRIMARY.CELL<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.POC.PRIMARY.EMAIL}

Pole *E-mail głównego punktu kontaktowego* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.POC.PRIMARY.EMAIL<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.POC.PRIMARY.NAME}

Pole *Nazwa głównego punktu kontaktowego* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.POC.PRIMARY.NAME<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.POC.PRIMARY.NOTES}

Pole *Uwagi głównego punktu kontaktowego* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.POC.PRIMARY.NOTES<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.POC.PRIMARY.PHONE.A}

Pole *Primary POC phone A* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.POC.PRIMARY.PHONE.A<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.POC.PRIMARY.PHONE.B}

Pole *Primary POC phone B* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.POC.PRIMARY.PHONE.B<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.POC.PRIMARY.SCREEN}

Pole *Nazwa ekranu głównego punktu kontaktowego* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.POC.PRIMARY.SCREEN<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.POC.SECONDARY.CELL}

Pole *Secondary POC cell* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.POC.SECONDARY.CELL<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.POC.SECONDARY.EMAIL}

Pole *E-mail dodatkowego punktu kontaktowego (POC)* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.POC.SECONDARY.EMAIL<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.POC.SECONDARY.NAME}

Pole *Nazwa dodatkowego punktu kontaktowego (POC)* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.POC.SECONDARY.NAME<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.POC.SECONDARY.NOTES}

Pole *Uwagi dodatkowego punktu kontaktowego* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.POC.SECONDARY.NOTES<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.POC.SECONDARY.PHONE.A}

Pole *Secondary POC phone A* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.POC.SECONDARY.PHONE.A<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.POC.SECONDARY.PHONE.B}

Pole *Secondary POC phone B* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.POC.SECONDARY.PHONE.B<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.POC.SECONDARY.SCREEN}

Pole *Nazwa ekranu dodatkowego POC* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.POC.SECONDARY.SCREEN<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.SERIALNO.A}

Pole *Numer seryjny A* w inwentarzu hosta.

 Ten makro może być używane z indeksem numerycznym, np. {INVENTORY.SERIALNO.A<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.SERIALNO.B}

Pole *Numer seryjny B* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.SERIALNO.B<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.SITE.ADDRESS.A}

Pole *Adres lokalizacji A* w inwentarzu hosta.

 Ten makro może być używane z indeksem numerycznym, np. {INVENTORY.SITE.ADDRESS.A<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.SITE.ADDRESS.B}

Pole *Adres lokalizacji B* w inwentarzu hosta.

 Ten makro może być używane z indeksem numerycznym, np. {INVENTORY.SITE.ADDRESS.B<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.SITE.ADDRESS.C}

Pole *Adres lokalizacji C* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.SITE.ADDRESS.C<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.SITE.CITY}

Pole *Miasto lokalizacji* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.SITE.CITY<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.SITE.COUNTRY}

Pole *Kraj lokalizacji* w inwentarzu hosta.

 Ta makroinstrukcja może być używana z indeksem numerycznym, np. {INVENTORY.SITE.COUNTRY<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makroinstrukcje indeksowane.

{INVENTORY.SITE.NOTES}

Pole *Uwagi dotyczące lokalizacji* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.SITE.NOTES<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.SITE.RACK}

Pole *Lokalizacja szafy w lokalizacji* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.SITE.RACK<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.SITE.STATE}

Pole *Województwo/stan* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.SITE.STATE<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.SITE.ZIP}

Pole *Kod pocztowy lokalizacji* w inwentarzu hosta.

 Ta makroinstrukcja może być używana z indeksem numerycznym, np. {INVENTORY.SITE.ZIP<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makroinstrukcje indeksowane.

{INVENTORY.SOFTWARE}

Pole *Oprogramowanie* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.SOFTWARE<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.SOFTWARE.APP.A}

Pole *Aplikacja A* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.SOFTWARE.APP.A<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.SOFTWARE.APP.B}

Pole *Aplikacja B* oprogramowania w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.SOFTWARE.APP.B<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.SOFTWARE.APP.C}

Pole *Aplikacja C* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.SOFTWARE.APP.C<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.SOFTWARE.APP.D}

Pole *Aplikacja D* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.SOFTWARE.APP.D<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.SOFTWARE.APP.E}

Pole *Aplikacja oprogramowania E* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.SOFTWARE.APP.E<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.SOFTWARE.FULL}

Pole *Oprogramowanie (pełne szczegóły)* w inwentarzu hosta.

 Ta makroinstrukcja może być używana z indeksem numerycznym, np. {INVENTORY.SOFTWARE.FULL<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makroinstrukcje indeksowane.

{INVENTORY.TAG}

Pole *Tag* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.TAG<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.TYPE}

Pole *Typ* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.TYPE<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.TYPE.FULL}

Pole *Typ (pełne szczegóły)* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.TYPE.FULL<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.URL.A}

Pole *URL A* w inwentarzu hosta.

 Ta makroinstrukcja może być używana z indeksem numerycznym, np. {INVENTORY.URL.A<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makroinstrukcje indeksowane.

{INVENTORY.URL.B}

Pole *URL B* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.URL.B<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.URL.C}

Pole *URL C* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.URL.C<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{INVENTORY.VENDOR}

Pole *Vendor* w inwentarzu hosta.

 To makro może być używane z indeksem numerycznym, np. {INVENTORY.VENDOR<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

Makra pozycji

{ITEM.DESCRIPTION}

Opis N-tej pozycji w wyrażeniu wyzwalacza, która spowodowała powiadomienie.

 To makro może być używane z indeksem numerycznym jako {ITEM.DESCRIPTION<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{ITEM.DESCRIPTION.ORIG}

Oryginalny opis (z nierozwiniętymi makrami) N-tej pozycji w wyrażeniu wyzwalacza, która spowodowała powiadomienie.

 To makro może być używane z indeksem numerycznym jako {ITEM.DESCRIPTION.ORIG<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{ITEM.ID}

Numeryczny identyfikator N-tej pozycji w wyrażeniu wyzwalacza, która spowodowała powiadomienie.

 To makro może być używane z indeksem numerycznym jako {ITEM.ID<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{ITEM.KEY}

Klucz N-tej pozycji w wyrażeniu wyzwalacza, która spowodowała powiadomienie.
 Funkcje makr nie są obsługiwane dla tego makra, jeśli jest ono używane jako symbol zastępczy w pierwszym parametrze funkcji historii, na przykład `last(/{HOST.HOST}/{ITEM.KEY}`
To makro może być używane z indeksem numerycznym jako {ITEM.KEY<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{ITEM.KEY.ORIG}

Oryginalny klucz (z nierozwiniętymi makrami) N-tej pozycji w wyrażeniu wyzwalacza, która spowodowała powiadomienie.

 To makro może być używane z indeksem numerycznym jako {ITEM.KEY.ORIG<1-9>}, aby wskazać pierwszy, drugi, trzeci itd. host w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{ITEM.LASTVALUE}

Najnowsza wartość N-tej pozycji w wyrażeniu wyzwalacza, która spowodowała powiadomienie.
 W frontendzie zostanie rozwinięta do *UNKNOWN*, jeśli najnowsza wartość historii została zebrana dawniej niż wynosi czas *Max history display period* (ustawiany w sekcji menu Administration → General).
 W przypadku użycia w nazwie problemu makro nie zostanie rozwinięte do najnowszej wartości pozycji podczas przeglądania zdarzeń problemów; zamiast tego zachowa wartość pozycji z momentu wystąpienia problemu.
W przypadku użycia w powiadomieniach, w niektórych sytuacjach makro może nie zostać rozwinięte do najnowszej wartości pozycji w momencie wyzwolenia wyzwalacza. Na przykład, jeśli pozycja szybko otrzyma dwie wartości, „A” i „B”, a wyzwalacz uruchomi się dla „A”, powiadomienia mogą pokazywać „B” jako najnowszą wartość z powodu niewielkiego opóźnienia przetwarzania — najnowsza wartość pozycji zmieniła się między momentem wyzwolenia wyzwalacza a utworzeniem powiadomienia. Aby tego uniknąć, można użyć makra {ITEM.VALUE}, które rozwija się do wartości z momentu wyzwolenia wyzwalacza, zapewniając użycie poprawnej wartości w powiadomieniu.
 Jest aliasem dla `last(/{HOST.HOST}/{ITEM.KEY})`.
 Rozwinięta wartość dla pozycji tekstowych/logów jest obcinana do 20 znaków przez frontend w następujących miejscach:
- Dane operacyjne;
- Opis wyzwalacza;
- URL-e wyzwalacza;
- Etykiety URL-i wyzwalacza;
- Opis widżetu wartości pozycji.
Aby uzyskać pełną wartość, można użyć funkcji makr, ponieważ żadne wartości nie są obcinane przez serwer. Na przykład: `{{ITEM.LASTVALUE}.regsub("(.*)", \1)}`.

 To makro może być używane z indeksem numerycznym, np. {ITEM.LASTVALUE<1-9>}, aby wskazać pierwszą, drugą, trzecią itd. pozycję w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{ITEM.LASTVALUE.AGE}

Czas, jaki upłynął między pobraniem ostatniej wartości pozycji a obliczeniem makra.
 Wyświetlany w formacie czytelnym dla użytkownika (np. 1m 45s).

 To makro może być używane z indeksem numerycznym, np. {ITEM.LASTVALUE.AGE<1-9>}, aby wskazać pierwszą, drugą, trzecią itd. pozycję w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{ITEM.LASTVALUE.DATE}

Data, kiedy została zebrana najnowsza wartość pozycji.
 Wyświetlana w formacie `YYYYMMDD`.
 Strefa czasowa serwera jest używana w nazwach wyzwalaczy (na liście Monitoring -> Problems), nazwach zdarzeń oraz nazwach i wartościach tagów. We wszystkich pozostałych przypadkach używana jest strefa czasowa użytkownika.

 To makro może być używane z indeksem numerycznym, np. {ITEM.LASTVALUE.DATE<1-9>}, aby wskazać pierwszą, drugą, trzecią itd. pozycję w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{ITEM.LASTVALUE.TIME}

Czas, kiedy została zebrana najnowsza wartość pozycji.
 Wyświetlany w formacie `HHMMSS`.
 Strefa czasowa serwera jest używana w nazwach wyzwalaczy (na liście Monitoring -> Problems), nazwach zdarzeń oraz nazwach i wartościach tagów. We wszystkich pozostałych przypadkach używana jest strefa czasowa użytkownika.

 To makro może być używane z indeksem numerycznym, np. {ITEM.LASTVALUE.TIME<1-9>}, aby wskazać pierwszą, drugą, trzecią itd. pozycję w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{ITEM.LASTVALUE.TIMESTAMP}

Znacznik czasu UNIX określający moment pobrania najnowszej wartości pozycji.

 To makro może być używane z indeksem numerycznym, np. {ITEM.LASTVALUE.TIMESTAMP<1-9>}, aby wskazać pierwszą, drugą, trzecią itd. pozycję w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{ITEM.LOG.AGE}

Wiek zdarzenia logu.
Z dokładnością do jednej sekundy.

 To makro może być używane z indeksem numerycznym, np. {ITEM.LOG.AGE<1-9>}, aby wskazać pierwszą, drugą, trzecią itd. pozycję w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{ITEM.LOG.DATE}

Data, kiedy wpis dziennika został zapisany do logu.

 To makro może być używane z indeksem numerycznym, np. {ITEM.LOG.DATE<1-9>}, aby wskazać pierwszą, drugą, trzecią itd. pozycję w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{ITEM.LOG.EVENTID}

ID zdarzenia w dzienniku zdarzeń.
 Tylko do monitorowania dziennika zdarzeń Windows.

 To makro może być używane z indeksem numerycznym, np. {ITEM.LOG.EVENTID<1-9>}, aby wskazać pierwszą, drugą, trzecią itd. pozycję w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{ITEM.LOG.NSEVERITY}

Numeryczny poziom ważności zdarzenia w dzienniku zdarzeń.
 Tylko do monitorowania dziennika zdarzeń Windows.

 To makro może być używane z indeksem numerycznym, np. {ITEM.LOG.NSEVERITY<1-9>}, aby wskazać pierwszą, drugą, trzecią itd. pozycję w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{ITEM.LOG.SEVERITY}

Słowny poziom ważności zdarzenia w dzienniku zdarzeń.
 Tylko do monitorowania dziennika zdarzeń Windows.

 To makro może być używane z indeksem numerycznym, np. {ITEM.LOG.SEVERITY<1-9>}, aby wskazać pierwszą, drugą, trzecią itd. pozycję w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{ITEM.LOG.SOURCE}

Źródło zdarzenia w dzienniku zdarzeń.
 Tylko do monitorowania dziennika zdarzeń systemu Windows.

 Ten makro może być używany z indeksem numerycznym, np. {ITEM.LOG.SOURCE<1-9>}, aby wskazać pierwszą, drugą, trzecią itd. pozycję w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{ITEM.LOG.TIME}

Czas, kiedy wpis dziennika został zapisany do dziennika.

 To makro może być używane z indeksem numerycznym, np. {ITEM.LOG.TIME<1-9>}, aby wskazać pierwszą, drugą, trzecią itd. pozycję w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{ITEM.LOG.TIMESTAMP}

Znacznik czasu UNIX określający moment zapisania wpisu dziennika w logu.

 To makro może być używane z indeksem numerycznym, np. {ITEM.LOG.TIMESTAMP<1-9>}, aby wskazać pierwszą, drugą, trzecią itd. pozycję w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{ITEM.NAME}

Nazwa pozycji ze wszystkimi makrami rozwiniętymi.

 To makro może być używane z indeksem numerycznym, np. {ITEM.NAME<1-9>}, aby wskazać pierwszą, drugą, trzecią itd. pozycję w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{ITEM.NAME.ORIG}

Oryginalna nazwa (z nierozwiniętymi makrami) pozycji.

 To makro może być używane z indeksem numerycznym, np. {ITEM.NAME.ORIG<1-9>}, aby wskazać pierwszą, drugą, trzecią itd. pozycję w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{ITEM.STATE}

Najnowszy stan N-tej pozycji w wyrażeniu wyzwalacza, która spowodowała powiadomienie.
 Możliwe wartości: *Not supported*, *Normal*.

 To makro może być używane z indeksem numerycznym, np. {ITEM.STATE<1-9>}, aby wskazać pierwszą, drugą, trzecią itd. pozycję w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{ITEM.STATE.ERROR}

Komunikat błędu zawierający szczegóły, dlaczego pozycja stała się nieobsługiwana.
 Jeśli pozycja przejdzie w stan nieobsługiwany, a następnie natychmiast ponownie stanie się obsługiwana, pole błędu może być puste.

{ITEM.VALUE}

Rozwijane do jednej z następujących wartości:

- Historyczna (z momentu wystąpienia zdarzenia) wartość N-tej pozycji w wyrażeniu wyzwalacza, jeśli jest używane w kontekście zmiany stanu wyzwalacza, na przykład podczas wyświetlania zdarzeń lub wysyłania powiadomień;
- Najnowsza wartość N-tej pozycji w wyrażeniu wyzwalacza, jeśli jest używane poza kontekstem zmiany stanu wyzwalacza, na przykład podczas wyświetlania listy wyzwalaczy w wyskakującym oknie wyboru. W takim przypadku działa tak samo jak {ITEM.LASTVALUE}.

W pierwszym przypadku zostanie rozwinięte do *UNKNOWN*, jeśli wartość historyczna została już usunięta lub nigdy nie była przechowywana.
W drugim przypadku, i tylko we frontendzie, zostanie rozwinięte do *UNKNOWN*, jeśli najnowsza wartość historyczna została zebrana dawniej niż *Max history display period* (ustawiane w sekcji menu Administration→General).
Rozwinięta wartość dla pozycji tekstowych/log jest obcinana przez frontend do 20 znaków w następujących miejscach:
- Dane operacyjne;
- Opis wyzwalacza;
- URL-e wyzwalacza;
- Etykiety URL-i wyzwalacza;
- Opis widżetu wartości pozycji.
Aby rozwinąć do pełnej wartości, można użyć funkcji makr, ponieważ żadne wartości nie są obcinane przez serwer. Na przykład: `{{ITEM.VALUE}.regsub("(.*)", \1)}`.

Tego makra można używać z indeksem numerycznym, np. {ITEM.VALUE<1-9>}, aby wskazać pierwszą, drugą, trzecią itd. pozycję w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{ITEM.VALUE.AGE}

Czas, jaki upłynął między zebraniem wartości pozycji a obliczeniem makra.
 Wyświetlany w formacie czytelnym dla człowieka (np. 1m 45s).

 To makro może być używane z indeksem numerycznym, np. {ITEM.VALUE.AGE<1-9>}, aby wskazać pierwszą, drugą, trzecią itd. pozycję w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{ITEM.VALUE.DATE}

Data, kiedy wartość pozycji została zebrana.
 Wyświetlana w formacie `YYYYMMDD`.
 Strefa czasowa serwera jest używana w nazwach wyzwalaczy (na liście Monitoring -> Problems), nazwach zdarzeń oraz nazwach i wartościach tagów. We wszystkich pozostałych przypadkach używana jest strefa czasowa użytkownika.

 To makro może być używane z indeksem numerycznym, np. {ITEM.VALUE.DATE<1-9>}, aby wskazać pierwszą, drugą, trzecią itd. pozycję w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{ITEM.VALUE.TIME}

Czas, kiedy wartość pozycji została zebrana.
 Wyświetlany w formacie `HHMMSS`.
 Strefa czasowa serwera jest używana w nazwach wyzwalaczy (na liście Monitoring -> Problems), nazwach zdarzeń oraz nazwach i wartościach tagów. We wszystkich pozostałych przypadkach używana jest strefa czasowa użytkownika.

 To makro może być używane z indeksem numerycznym, np. {ITEM.VALUE.TIME<1-9>}, aby wskazać pierwszą, drugą, trzecią itd. pozycję w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{ITEM.VALUE.TIMESTAMP}

Znacznik czasu UNIX określający moment zebrania wartości pozycji.

 To makro może być używane z indeksem numerycznym, np. {ITEM.VALUE.TIMESTAMP<1-9>}, aby wskazać pierwszą, drugą, trzecią itd. pozycję w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{ITEM.VALUETYPE}

Typ wartości N-tej pozycji w wyrażeniu wyzwalacza, która spowodowała powiadomienie.
 Możliwe wartości: *0* - Liczba zmiennoprzecinkowa, *1* - Znak, *2* - Log, *3* - Liczba całkowita bez znaku, *4* - Tekst.

 To makro może być używane z indeksem numerycznym, np. {ITEM.VALUETYPE<1-9>}, aby wskazać pierwszą, drugą, trzecią itd. pozycję w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

Makra powiadomień wykrywania niskiego poziomu

{LLDRULE.DESCRIPTION}

Opis reguły wykrywania niskiego poziomu, która spowodowała powiadomienie.

{LLDRULE.DESCRIPTION.ORIG}

Oryginalny opis (z nierozwiniętymi makrami) reguły wykrywania niskiego poziomu, która spowodowała powiadomienie.

{LLDRULE.ID}

Numeryczny identyfikator reguły wykrywania niskiego poziomu, która spowodowała powiadomienie.

{LLDRULE.KEY}

Klucz reguły wykrywania niskiego poziomu, która spowodowała powiadomienie.

{LLDRULE.KEY.ORIG}

Oryginalny klucz (z nierozwiniętymi makrami) reguły wykrywania niskiego poziomu, która spowodowała powiadomienie.

{LLDRULE.NAME}

Nazwa reguły wykrywania niskiego poziomu, która spowodowała powiadomienie.

{LLDRULE.NAME.ORIG}

Oryginalna nazwa (z nierozwiniętymi makrami) reguły wykrywania niskiego poziomu, która spowodowała powiadomienie.

{LLDRULE.STATE}

Najnowszy stan reguły wykrywania niskiego poziomu.
 Możliwe wartości: *Nieobsługiwane*, *Normalny*.

 To makro może być używane z indeksem numerycznym, np. {LLDRULE.STATE<1-9>}, aby wskazać pierwszą, drugą, trzecią itd. pozycję w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{LLDRULE.STATE.ERROR}

Komunikat błędu zawierający szczegóły, dlaczego reguła wykrywania niskiego poziomu stała się nieobsługiwana.
 Jeśli reguła wykrywania niskiego poziomu przejdzie w stan nieobsługiwany, a następnie natychmiast ponownie stanie się obsługiwana, pole błędu może być puste.

Makra mapy

{MAP.ID}

ID mapy sieciowej.

{MAP.NAME}

Nazwa mapy sieciowej.

Makra proxy

{PROXY.DESCRIPTION}

Opis proxy.
 Rozwijane jako jedno z poniższych:

- Proxy N-tej pozycji w wyrażeniu wyzwalacza (w powiadomieniach opartych na wyzwalaczach). Można tutaj używać makr indeksowanych;
- Proxy, które wykonało wykrywanie (w powiadomieniach o wykrywaniu). Użyj tutaj {PROXY.DESCRIPTION}, bez indeksowania;
- Proxy, do którego zarejestrował się aktywny agent (w powiadomieniach o autorejestracji). Użyj tutaj {PROXY.DESCRIPTION}, bez indeksowania.

To makro może być używane z indeksem numerycznym, np. {PROXY.DESCRIPTION<1-9>}, aby wskazać pierwszą, drugą, trzecią itd. pozycję w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

{PROXY.NAME}

Nazwa proxy.
 Rozwiązuje się do jednej z następujących wartości:

- Proxy N-tej pozycji w wyrażeniu wyzwalacza (w powiadomieniach opartych na wyzwalaczach). Można tutaj używać makr indeksowanych;
- Proxy, który wykonał wykrywanie (w powiadomieniach o wykrywaniu). Użyj tutaj {PROXY.NAME}, bez indeksowania;
- Proxy, do którego zarejestrował się aktywny agent (w powiadomieniach o autorejestracji). Użyj tutaj {PROXY.NAME}, bez indeksowania.

To makro może być używane z indeksem numerycznym, np. {PROXY.NAME<1-9>}, aby wskazać pierwszą, drugą, trzecią itd. pozycję w wyrażeniu wyzwalacza. Zobacz makra indeksowane.

Makra skryptu

{MANUALINPUT}

Wartość ręcznego wejścia określona przez użytkownika w czasie wykonywania skryptu.

Makra usługi

{SERVICE.DESCRIPTION}

Opis usługi z rozwiązanymi makrami.

{SERVICE.ID}

Numeryczny identyfikator usługi, która wywołała akcję.

{SERVICE.NAME}

Nazwa usługi z rozwiniętymi makrami.

{SERVICE.ROOTCAUSE}

Lista zdarzeń problemowych wyzwalaczy, które spowodowały awarię usługi, posortowana według ważności i nazwy hosta.
 Zawiera następujące szczegóły: nazwa hosta, nazwa zdarzenia, ważność, wiek, tagi usługi i wartości.

{SERVICE.TAGS}

Lista tagów zdarzenia usługi rozdzielonych przecinkami.
 Tagi zdarzenia usługi można zdefiniować w sekcji tagów konfiguracji usługi. Rozwijane do pustego ciągu znaków, jeśli nie istnieją żadne tagi.

{SERVICE.TAGSJSON}

Tablica JSON zawierająca obiekty tagów zdarzenia usługi.
 Tagi zdarzenia usługi można zdefiniować w sekcji tagów konfiguracji usługi. Rozwijane do pustej tablicy, jeśli nie istnieją żadne tagi.

{SERVICE.TAGS.<tag name>}

Wartość tagu zdarzenia usługi wskazana przez nazwę tagu.
 Tagi zdarzeń usługi można zdefiniować w sekcji tagów konfiguracji usługi.
 Nazwa tagu zawierająca znaki niealfanumeryczne (w tym nieangielskie wielobajtowe znaki UTF) musi być ujęta w podwójny cudzysłów. Cudzysłowy i ukośniki odwrotne wewnątrz nazwy tagu ujętej w cudzysłów muszą być poprzedzone ukośnikiem odwrotnym.

Makra wyzwalaczy

{TRIGGER.DESCRIPTION}

Opis wyzwalacza.
 Wszystkie makra obsługiwane w opisie wyzwalacza zostaną rozwinięte, jeśli `{TRIGGER.DESCRIPTION}` zostanie użyte w tekście powiadomienia.

{TRIGGER.EVENTS.ACK}

Liczba potwierdzonych zdarzeń dla elementu mapy na mapach lub dla wyzwalacza, który wygenerował bieżące zdarzenie w powiadomieniach.

{TRIGGER.EVENTS.PROBLEM.ACK}

Liczba potwierdzonych zdarzeń problemów dla wszystkich wyzwalaczy, niezależnie od ich stanu.

{TRIGGER.EVENTS.PROBLEM.UNACK}

Liczba niepotwierdzonych zdarzeń problemowych dla wszystkich wyzwalaczy, niezależnie od ich stanu.

{TRIGGER.EVENTS.UNACK}

Liczba niepotwierdzonych zdarzeń dla elementu mapy na mapach lub dla wyzwalacza, który wygenerował bieżące zdarzenie w powiadomieniach.

{TRIGGER.EXPRESSION}

Wyrażenie wyzwalacza.

{TRIGGER.EXPRESSION.EXPLAIN}

Częściowo obliczone wyrażenie wyzwalacza.
 Funkcje oparte na pozycjach są obliczane i zastępowane wynikami w momencie generowania zdarzenia, natomiast wszystkie pozostałe funkcje są wyświetlane w postaci zapisanej w wyrażeniu. Może być używane do debugowania wyrażeń wyzwalaczy.

{TRIGGER.EXPRESSION.RECOVERY}

Wyrażenie odzyskiwania wyzwalacza, jeśli *OK event generation* w konfiguracji wyzwalacza jest ustawione na „Recovery expression”; w przeciwnym razie zwracany jest pusty ciąg.

{TRIGGER.EXPRESSION.RECOVERY.EXPLAIN}

Częściowo obliczone wyrażenie odzyskiwania wyzwalacza.
 Funkcje oparte na pozycjach są obliczane i zastępowane wynikami w momencie generowania zdarzenia, natomiast wszystkie pozostałe funkcje są wyświetlane w postaci zapisanej w wyrażeniu. Może być używane do debugowania wyrażeń odzyskiwania wyzwalacza.

{TRIGGER.HOSTGROUP.NAME}

Posortowana (według zapytania SQL) lista grup hostów, rozdzielonych przecinkiem i spacją, w których zdefiniowany jest wyzwalacz.

{TRIGGER.ID}

Numeryczny identyfikator wyzwalacza, który uruchomił tę akcję.

{TRIGGER.NAME}

Nazwa wyzwalacza z rozwiniętymi makrami.
 Zwróć uwagę, że `{EVENT.NAME}` może być używane w akcjach do wyświetlania nazwy wywołanego zdarzenia/problemu z rozwiniętymi makrami.

{TRIGGER.NAME.ORIG}

Oryginalna nazwa wyzwalacza (z nierozwiniętymi makrami).

{TRIGGER.NSEVERITY}

Numeryczny poziom ważności wyzwalacza.
 Możliwe wartości: *0* - Niesklasyfikowany, *1* - Informacja, *2* - Ostrzeżenie, *3* - Średni, *4* - Wysoki, *5* - Katastrofa.

{TRIGGER.PROBLEM.EVENTS.PROBLEM.ACK}

Liczba potwierdzonych zdarzeń problemów dla wyzwalaczy w stanie problemu.

{TRIGGER.PROBLEM.EVENTS.PROBLEM.UNACK}

Liczba niepotwierdzonych zdarzeń problemów dla wyzwalaczy w stanie problemu.

{TRIGGER.SEVERITY}

Nazwa ważności wyzwalacza.
 Może być zdefiniowana w *Administration > General > Trigger displaying options*.

{TRIGGER.STATE}

Najnowszy stan wyrażenia wyzwalacza.
 Możliwe wartości: *Nieznany*, *Normalny*.

{TRIGGER.STATE.ERROR}

Komunikat błędu zawierający szczegóły, dlaczego wyzwalacz stał się nieobsługiwany.
 Jeśli wyzwalacz przejdzie w stan nieobsługiwany, a następnie natychmiast ponownie stanie się obsługiwany, pole błędu może być puste.

{TRIGGER.STATUS}

Wartość wyzwalacza w momencie wykonania kroku operacji.
 Możliwe wartości: *Problem*, *OK*.

{TRIGGER.TEMPLATE.NAME}

Posortowana (według zapytania SQL) lista szablonów, oddzielona przecinkami i spacjami, w których zdefiniowano wyzwalacz, lub *UNKNOWN*, jeśli wyzwalacz jest zdefiniowany w hoście.

{TRIGGER.URL}

URL wyzwalacza.

{TRIGGER.URL.NAME}

Etykieta dla URL wyzwalacza.

{TRIGGER.VALUE}

Bieżąca numeryczna wartość wyzwalacza.
 Możliwe wartości: *0* - wyzwalacz jest w stanie OK, *1* - wyzwalacz jest w stanie Problem.

{TRIGGERS.ACK}

Liczba potwierdzonych wyzwalaczy dla elementu mapy, bez uwzględniania stanu wyzwalacza.
 Wyzwalacz jest uznawany za potwierdzony, jeśli wszystkie jego zdarzenia problemowe są potwierdzone.

{TRIGGERS.PROBLEM.ACK}

Liczba potwierdzonych wyzwalaczy problemów dla elementu mapy.
 Wyzwalacz jest uznawany za potwierdzony, jeśli wszystkie jego zdarzenia problemowe są potwierdzone.

{TRIGGERS.PROBLEM.UNACK}

Liczba niepotwierdzonych wyzwalaczy problemów dla elementu mapy.
 Wyzwalacz jest uznawany za niepotwierdzony, jeśli co najmniej jedno z jego zdarzeń problemu nie zostało potwierdzone.

{TRIGGERS.UNACK}

Liczba niepotwierdzonych wyzwalaczy dla elementu mapy, niezależnie od stanu wyzwalacza.
 Wyzwalacz jest uznawany za niepotwierdzony, jeśli co najmniej jedno z jego zdarzeń problemowych nie zostało potwierdzone.

Makra nazwy użytkownika

{USER.FULLNAME}

Imię, nazwisko i nazwa użytkownika użytkownika, który dodał potwierdzenie zdarzenia lub uruchomił skrypt.

{USER.NAME}

Nazwa użytkownika, który uruchomił skrypt.

{USER.SURNAME}

Nazwisko użytkownika, który uruchomił skrypt.

{USER.USERNAME}

Nazwa użytkownika, który uruchomił skrypt.

Makra indeksowane

Składnia makr indeksowanych **{MACRO<1-9>}** może odwoływać się wyłącznie do N-tej pozycji, funkcji lub hosta w polu *Expression* wyzwalacza:

- **{HOST.IP1}, {HOST.IP2}, {HOST.IP3}** są rozwijane do adresów IP pierwszego, drugiego i trzeciego hosta w wyrażeniu wyzwalacza (jeśli występują).
- **{ITEM.VALUE1}, {ITEM.VALUE2}, {ITEM.VALUE3}** są rozwijane do wartości pierwszej, drugiej i trzeciej pozycji w wyrażeniu wyzwalacza w momencie zdarzenia (jeśli występują).
- **{FUNCTION.VALUE1}, {FUNCTION.VALUE2}, {FUNCTION.VALUE3}** są rozwijane do wartości pierwszej, drugiej i trzeciej funkcji opartych na pozycjach w momencie zdarzenia (jeśli występują).

W kontekście wyzwalaczy makra indeksowane zawsze odnoszą się do pola *Expression* w konfiguracji wyzwalacza, a nie do pola *Recovery expression*. Na przykład w zdarzeniu odzyskania **{ITEM.VALUE2}** zostanie rozwinięte do wartości drugiej pozycji z wyrażenia problemu w momencie odzyskania.

Makro **{HOST.HOST<1-9>}** jest również obsługiwane w makrze wyrażenia `{?func(/host/key,param)}` w **nazwach wykresów**. Na przykład `{?func(/{HOST.HOST2}/key,param)}` w nazwie wykresu zostanie rozwinięte do hosta drugiej pozycji na wykresie.

Warning:
Makra indeksowane nie będą rozwijane w żadnym innym kontekście poza przypadkami wymienionymi tutaj. W innych kontekstach używaj makr bez indeksu (**{HOST.HOST}, {HOST.IP}** itd.).

2 Makra użytkownika obsługiwane według lokalizacji

Przegląd

Ta sekcja zawiera listę miejsc, w których obsługiwane są makra definiowane przez użytkownika.

Note:
Dla *Akcji*, *Odkrywania sieci*, *Proxy* oraz wszystkich lokalizacji wymienionych w sekcji *Inne lokalizacje* na tej stronie obsługiwane są tylko makra użytkownika na poziomie globalnym. W wymienionych lokalizacjach makra na poziomie hosta i na poziomie szablonu nie będą rozwijane.

Note:
Aby dostosować wartości makr (na przykład skrócić je lub wyodrębnić określone podciągi), można użyć funkcji makr.

Akcje

W akcjach makra użytkownika mogą być używane w następujących polach:

Lokalizacja		Wiele makr/mieszanie z tekstem[1]
Powiadomienia i polecenia oparte na wyzwalaczach		tak
Wewnętrzne powiadomienia oparte na wyzwalaczach		tak
Powiadomienia o aktualizacji problemu		tak
Powiadomienia i polecenia oparte na usługach		tak
Powiadomienia o aktualizacji usługi		tak
Warunek okresu czasu		nie
Operacje		
	Domyślny czas trwania kroku operacji	nie
	Czas trwania kroku	nie

Hosty/prototypy hostów

W konfiguracji hosta i prototypu hosta makra użytkownika mogą być używane w następujących polach:

Lokalizacja		Wiele makr/mieszanie z tekstem[1]
IP/DNS interfejsu		tylko DNS
Port interfejsu		nie
SNMP v1, v2		
	Społeczność SNMP	tak
SNMP v3		
	Nazwa kontekstu	tak
	Nazwa bezpieczeństwa	tak
	Hasło uwierzytelniania	tak
	Hasło prywatności	tak
IPMI		
	Nazwa użytkownika	tak
	Hasło	tak
Tagi[2]		
	Nazwy tagów	tak
	Wartości tagów	tak

Pozycje / prototypy pozycji

W konfiguracji pozycji lub prototypu pozycji makra użytkownika mogą być używane w następujących polach:

Lokalizacja	Wiele makr/mieszanie z tekstem[1]
Nazwa pozycji	tak
Parametry klucza pozycji	tak
Interwał aktualizacji	nie
Niestandardowe interwały	nie

Lokalizacja	Wiele makr/mieszanie z tekstem[1]
Limit czasu (dostępny dla obsługiwanych typów pozycji)	nie
Przechowuj do (dla historii i trendów)	nie
Opis	tak
Pozycja obliczana/agregująca	
Formuła (stałe wyrażenia i parametry funkcji; parametry klucza pozycji; (*tylko pozycja agregująca*) warunki filtra (nazwa grupy hostów i nazwa tagu))	tak
Monitor bazy danych	
Nazwa użytkownika	tak
Hasło	tak
Zapytanie SQL	tak
HTTP agent	
URL[3]	tak
Pola zapytania	tak
Treść żądania	tak
Nagłówki (nazwy i wartości)	tak
Wymagane kody statusu	tak
HTTP proxy	tak
Nazwa użytkownika do uwierzytelniania HTTP	tak
Hasło do uwierzytelniania HTTP	tak
Plik certyfikatu SSL	tak
Plik klucza SSL	tak
Hasło klucza SSL	tak
Dozwolone hosty	tak
JMX agent	
Punkt końcowy JMX	tak
Pozycja skryptowa	
Nazwy i wartości parametrów	tak
Pozycja przeglądarki	
Nazwy i wartości parametrów	tak
SNMP agent	
OID SNMP	tak
SSH agent	
Nazwa użytkownika	tak
Plik klucza publicznego	tak
Plik klucza prywatnego	tak

Lokalizacja	Wiele makr/mieszanie z tekstem[1]
Hasło	tak
Skrypt	tak
TELNET agent	
Nazwa użytkownika	tak
Hasło	tak
Skrypt	tak
Zabbix trapper	
Dozwolone hosty	tak
Tagi[2]	
Nazwy tagów	tak
Wartości tagów	tak
Kroki przetwarzania wstępnego	
Parametry (w tym niestandardowe skrypty)	tak
Parametry niestandardowej obsługi błędów (pola *Ustaw wartość na* i *Ustaw błąd na*)	tak

Odkrywanie niskiego poziomu

W regule odkrywania niskiego poziomu makra użytkownika mogą być używane w następujących polach:

Lokalizacja		Wiele makr/
Parametry klucza		tak
Interwał aktualizacji		nie
Niestandardowy interwał		nie
Limit czasu (dostępny dla obsługiwanych typów pozycji)		nie
Usuń utracone zasoby		nie
Wyłącz utracone zasoby		nie
Opis		tak
SNMP agent		
	OID SNMP	tak
SSH agent		
	Nazwa użytkownika	tak
	Plik klucza publicznego	tak
	Plik klucza prywatnego	tak
	Hasło	tak
	Skrypt	tak
TELNET agent		
	Nazwa użytkownika	tak
	Hasło	tak
	Skrypt	tak
Zabbix trapper		
	Dozwolone hosty	tak
Monitor bazy danych		
	Nazwa użytkownika	tak
	Hasło	tak
	Zapytanie SQL	tak
JMX agent		
	Punkt końcowy JMX	tak
HTTP agent		
	URL[3]	tak
	Pola zapytania	tak
	Treść żądania	tak
	Nagłówki (nazwy i wartości)	tak
	Wymagane kody statusu	tak

Lokalizacja		Wiele makr/
	Nazwa użytkownika do uwierzytelniania HTTP	tak
	Hasło do uwierzytelniania HTTP	tak
Filtry		
	Wyrażenie regularne	tak
Nadpisania		
	Filtry: wyrażenie regularne	tak
	Operacje: interwał aktualizacji (dla prototypów pozycji)	nie
	Operacje: okres przechowywania historii (dla prototypów pozycji)	nie
	Operacje: okres przechowywania trendów (dla prototypów pozycji)	nie

Odkrywanie sieci

W regule odkrywania sieci makra użytkownika mogą być używane w następujących polach:

Lokalizacja		Wiele makr/mieszanie z tekstem[1]
Interwał aktualizacji		nie
SNMP v1, v2		
	Społeczność SNMP	tak
	OID SNMP	tak
SNMP v3		
	Nazwa kontekstu	tak
	Nazwa bezpieczeństwa	tak
	Hasło uwierzytelniania	tak
	Hasło prywatności	tak
	OID SNMP	tak

Proxy

W konfiguracji proxy makra użytkownika mogą być używane w następujących polach:

Lokalizacja	Wiele makr/mieszanie z tekstem[1]
Adres dla aktywnych agentów > *Port* (jeśli proxy należy do grupy)	nie
Adres interfejsu i port (dla pasywnego proxy)	nie
Timeouty dla typów pozycji	nie

Grupy proxy

W konfiguracji grupy proxy makra użytkownika mogą być używane w następujących polach:

Lokalizacja	Wiele makr/mieszanie z tekstem[1]
Okres przełączenia awaryjnego	nie
Minimalna liczba proxy	nie

Szablony

W konfiguracji szablonu makra użytkownika mogą być używane w następujących polach:

Lokalizacja		Wiele makr/mieszanie z tekstem[1]
Tagi[2]		
	Nazwy tagów	tak
	Wartości tagów	tak

Wyzwalacze

W konfiguracji wyzwalacza makra użytkownika mogą być używane w następujących polach:

Lokalizacja	Wiele makr/mieszanie z tekstem[1]
Nazwa	tak
Dane operacyjne	tak
Wyrażenie (tylko w stałych i parametrach funkcji; tajne makra nie są obsługiwane)	tak
Tag do dopasowania	tak
Nazwa wpisu menu	tak
URL wpisu menu[3]	tak
Opis	tak
Tagi[2]	
Nazwy tagów	tak
Wartości tagów	tak

Scenariusz web

W konfiguracji scenariusza web makra użytkownika mogą być używane w następujących polach:

Lokalizacja		Wiele makr/mieszanie z tekstem[1]
Nazwa		tak
Interwał aktualizacji		nie
Agent		tak
HTTP proxy		tak
Zmienne (tylko wartości)		tak
Nagłówki (nazwy i wartości)		tak
Kroki		
	Nazwa	tak
	URL[3]	tak
	Zmienne (tylko wartości)	tak
	Nagłówki (nazwy i wartości)	tak
	Limit czasu	nie
	Wymagany ciąg znaków	tak
	Wymagane kody statusu	nie
Uwierzytelnianie		
	Użytkownik	tak
	Hasło	tak
	Certyfikat SSL	tak

Lokalizacja		Wiele makr/mieszanie z tekstem[1]
Tagi[2]	Plik klucza SSL	tak
	Hasło klucza SSL	tak
	Nazwy tagów	tak
	Wartości tagów	tak

Inne lokalizacje

Oprócz lokalizacji wymienionych tutaj makra użytkownika mogą być używane w następujących polach:

Lokalizacja	Wiele makr/mieszanie z tekstem[1]
Skrypty globalne (URL, skrypt, SSH, Telnet, IPMI), w tym tekst potwierdzenia	tak
Webhooki	
Skrypt JavaScript	nie
Nazwa parametru skryptu JavaScript	nie
Wartość parametru skryptu JavaScript	tak
Pulpity	
Kolumna typu danych *Tekst* w widżecie pulpitu *Top hosts*	tak
Parametr *Opis* w widżetach pulpitu *Wartość pozycji* i *Wskaźnik*	tak
Parametr *Tekst* etykiety głównej/pomocniczej w widżecie pulpitu *Honeycomb*	tak
Parametr *URL*[3] w widżecie pulpitu *URL*	tak
Użytkownicy → *Użytkownicy* → *Media*	
Gdy aktywne	tak
Administracja → *Ogólne* → *GUI*	
Czas pracy	nie
Administracja → *Ogólne* → *Limity czasu*	
Limity czasu dla typów pozycji	nie

Lokalizacja	Wiele makr/mieszanie z tekstem[1]
Administracja → *Ogólne* → *Konek-tory*	
URL	tak
Nazwa użytkownika	tak
Hasło	tak
Token Bearer	tak
Limit czasu	nie
HTTP proxy	tak
Plik certyfikatu SSL	tak
Plik klucza SSL	tak
Hasło klucza SSL	tak
Alerty → *Typy mediów* → *Sz-ablony wiado-mości*	
Temat	tak
Wiadomość	tak
Alerty → *Typy mediów* → *Skrypt*	
Parametry skryptu	tak
Alerty → *Typy mediów* → *Typ mediów*	
Pola *Nazwa użytkownika* i *Hasło* dla typu mediów *Email* (gdy *Uwierzytelnianie* jest ustawione na „Nazwa użytkownika i hasło”; zalecane są tajne makra)	tak

Aby zobaczyć pełną listę wszystkich makr obsługiwanych w Zabbix, zobacz obsługiwane makra.

Przypisy

[1] Jeśli wiele makr w polu lub makra zmieszane z tekstem nie są obsługiwane w danej lokalizacji, pojedyncze makro musi wypełniać całe pole.

[2] Makra używane w nazwach i wartościach tagów są rozwijane tylko podczas procesu generowania zdarzenia.

[3] Adresy URL zawierające tajne makro nie będą działać, ponieważ makro w nich zostanie rozwinięte jako ”******”.

7 Symbole jednostek

Przegląd

Praca z dużymi wartościami, takimi jak 86400, 104857600 lub 1000000, może być trudna i prowadzić do błędów. Aby uprościć konfigurację i poprawić czytelność, Zabbix obsługuje symbole jednostek (sufiksy), które działają jako mnożniki wartości.

Wyrażenia wyzwalaczy bez sufiksów:

```
last(/host/system.uptime)<86400
avg(/host/system.cpu.load,600s)<10
last(/host/vm.memory.size[available])<20971520
```

Wyrażenia wyzwalaczy z sufiksami:

```
last(/host/system.uptime)<1d
avg(/host/system.cpu.load,10m)<10
last(/host/vm.memory.size[available])<20M
```

Sufiksy mogą również uprościć konfigurację innych obiektów, takich jak pozycje, widgety itp., a także pomóc w wyświetlaniu wartości pozycji w formacie czytelnym dla człowieka.

Note:
Aby sprawdzić, czy pole konfiguracji danego obiektu obsługuje sufiksy, zawsze należy zajrzeć na odpowiednią stronę dotyczącą konfigurowanego obiektu.

Przyrostki czasu

Frontend Zabbix obsługuje następujące przyrostki czasu w konfiguracji encji:

- **s** - sekundy *(po użyciu działa tak samo jak wartość surowa)*
- **m** - minuty
- **h** - godziny
- **d** - dni
- **w** - tygodnie
- **M** - miesiące *(funkcje trendów tylko)*
- **y** - lata *(funkcje trendów tylko)*

Przyrostki czasu są obsługiwane tylko z liczbami całkowitymi. Na przykład 1h jest obsługiwane, ale 1,5h lub 1.5h nie jest obsługiwane; zamiast tego użyj 90m.

Przyrostki rozmiaru pamięci

Zabbix obsługuje następujące przyrostki rozmiaru pamięci:

- **K** - kilobajty
- **M** - megabajty
- **G** - gigabajty
- **T** - terabajty

Przyrostki wartości pozycji

Przyrostki mogą być również używane do wyświetlania numerycznych wartości pozycji w formacie czytelnym dla człowieka.

Aby to włączyć, użyj jednego z następujących przyrostków w polu *Units* podczas konfigurowania pozycji:

- **B** - bajty
- **Bps** - bajty na sekundę
- **s** - sekundy, wyświetlane z użyciem maksymalnie trzech największych niezerowych jednostek czasu
- **uptime** - czas działania w formacie hh:mm:ss lub N dni, hh:mm:ss
- **unixtime** - znacznik czasu Unix, formatowany jako yyyy.mm.dd hh:mm:ss

Obowiązują następujące dodatkowe zasady dotyczące interpretacji i wyświetlania tych przyrostków:

- Dla B i Bps Zabbix używa przelicznika o podstawie 2 (1K = 1024B), zgodnie ze standardem JEDEC.
- Dla innych jednostek (takich jak Hz, W itp.) Zabbix używa przelicznika o podstawie 10 (1K = 1000).
- Dla s (sekund):
  - Format obejmuje yyy mmm ddd hhh mmm sss ms; wyświetlane są tylko maksymalnie trzy największe niezerowe jednostki czasu (np. 1M 10d 4h).
  - Jeśli jednostka ma wartość zero i znajduje się pomiędzy dwiema niezerowymi jednostkami, jest pomijana (np. 10d 56m zamiast 10d 0h 56m).

Gdy używane jest pole *Units*, do wartości pozycji automatycznie stosowane są następujące przyrostki mnożnika:

- **K**, **M**, **G**, **T** - kilo, mega, giga, tera
- **P**, **E**, **Z**, **Y** - peta, eksa, zetta, jota *(są stosowane tylko we frontendzie)*

Aby zapobiec konwersji jednostek, użyj prefiksu ! (np. !B lub !s).

Poniższe przykłady pokazują, jak odebrane wartości pozycji są konwertowane na podstawie określonych jednostek:

```
1 B → 1 B
1024 B → 1 KB
1536 B → 1.5 KB
881764 B → 881.76 KB
881764 !B → 881764 B

0.0000155 s → 0.016ms
3470400 s → 1M 10d 4h
2606400 s → 1M 4h
2592000 s → 1M
2592001 s → 1M
2592001 !s → 2592001 s

17764 uptime → 04:56:04
86400 uptime → 1 day, 00:00:00
881764 uptime → 10 days, 04:56:04
32417764 uptime → 375 days, 04:56:04
32417764 !uptime → 32417764 uptime

881764 unixtime → 1970-01-11 04:56:04 AM

17764 Hz → 17.76 KHz
86400 Hz → 86.4 KHz
881764 Hz → 881.76 KHz
32417764 Hz → 32.42 MHz

0 ! → 0
0 !! → 0 !
```

Note:
Przed Zabbix 4.0 istniała zakodowana na stałe lista wykluczonych jednostek, obejmująca `ms`, `rpm`, `RPM`, `%`. Ta lista została wycofana, dlatego poprawnym sposobem zapobiegania konwersji takich jednostek jest użycie `!ms`, `!rpm`, `!RPM`, `!%`.

8 Składnia okresu czasu

Przegląd

Aby ustawić przedział czasu, należy użyć następującego formatu:

`d-d,hh:mm-hh:mm`

gdzie symbole oznaczają:

Symbol	Opis
d	Dzień tygodnia: 1 - poniedziałek, 2 - wtorek, ... , 7 - niedziela
hh	Godziny: 00-24
mm	Minuty: 00-59

Możesz określić więcej niż jeden przedział czasu, używając separatora średnika (;):

`d-d,hh:mm-hh:mm;d-d,hh:mm-hh:mm...`

Pozostawienie przedziału czasu pustego jest równoznaczne z 1-7,00:00-24:00, co jest wartością domyślną.

Attention:
Górna granica przedziału czasu nie jest uwzględniana. Dlatego jeśli określisz 09:00-18:00, ostatnią sekundą uwzględnioną w tym przedziale czasu jest 17:59:59.

Przykłady

Godziny pracy. Od poniedziałku do piątku od 9:00 do 18:00:

```
1-5,09:00-18:00
```

Godziny pracy plus weekend. Od poniedziałku do piątku od 9:00 do 18:00 oraz w sobotę i niedzielę od 10:00 do 16:00:

```
1-5,09:00-18:00;6-7,10:00-16:00
```

9 Wykonywanie poleceń

Zabbix używa wspólnej funkcjonalności dla kontroli zewnętrznych, parametrów użytkownika, pozycji system.run, niestandardowych skryptów alertów, zdalnych poleceń i globalnych skryptów.

Kroki wykonywania

> **Note:**
> Domyślnie wszystkie skrypty w Zabbix są wykonywane przy użyciu powłoki *sh* i nie ma możliwości zmiany domyślnej powłoki. Aby użyć innej powłoki, można zastosować obejście: utworzyć plik skryptu i wywołać ten skrypt podczas wykonywania polecenia.

Polecenie/skrypt jest wykonywane w podobny sposób zarówno na platformach Unix, jak i Windows:

1. Zabbix (proces nadrzędny) tworzy potok do komunikacji
2. Zabbix ustawia potok jako wyjście dla tworzonego procesu potomnego
3. Zabbix tworzy proces potomny (uruchamia polecenie/skrypt)
4. Dla procesu potomnego tworzona jest nowa grupa procesów (w Unix) lub zadanie (w Windows)
5. Zabbix odczytuje z potoku do momentu wystąpienia limitu czasu lub gdy nikt nie zapisuje do drugiego końca (WSZYSTKIE uchwyty/deskriptory plików zostały zamknięte). Należy pamiętać, że proces potomny może utworzyć więcej procesów i zakończyć działanie, zanim one zakończą działanie lub zamkną uchwyt/deskrpytor pliku.
6. Jeśli limit czasu nie został osiągnięty, Zabbix czeka, aż początkowy proces potomny zakończy działanie lub wystąpi limit czasu
7. Jeśli początkowy proces potomny zakończył działanie i limit czasu nie został osiągnięty, Zabbix sprawdza kod wyjścia początkowego procesu potomnego i porównuje go z 0 (wartość różna od zera jest uznawana za błąd wykonania, tylko dla niestandardowych skryptów alertów, zdalnych poleceń i skryptów użytkownika wykonywanych na serwer i proxy Zabbix)
8. Na tym etapie zakłada się, że wszystko zostało wykonane i całe drzewo procesów (tj. grupa procesów lub zadanie) jest kończone

> **Attention:**
> Zabbix zakłada, że polecenie/skrypt zakończyło przetwarzanie, gdy początkowy proces potomny zakończył działanie ORAZ żaden inny proces nie utrzymuje już otwartego uchwytu wyjściowego/deskriptora pliku. Gdy przetwarzanie zostanie zakończone, WSZYSTKIE utworzone procesy są kończone.

Wszystkie podwójne cudzysłowy i ukośniki odwrotne w poleceniu są poprzedzane ukośnikami odwrotnymi, a polecenie jest ujmowane w podwójne cudzysłowy.

Sprawdzanie kodu wyjścia

Kody wyjścia są sprawdzane przy następujących warunkach:

- Tylko dla niestandardowych skryptów alertów, zdalnych poleceń i skryptów użytkownika wykonywanych na serwer Zabbix i proxy Zabbix.
- Każdy kod wyjścia różny od 0 jest uznawany za błąd wykonania.
- Zawartość standardowego strumienia błędów i standardowego wyjścia dla nieudanych wykonań jest zbierana i dostępna we frontendzie (gdzie wynik wykonania jest wyświetlany).
- Dodatkowy wpis w logu może zostać utworzony dla zdalnych poleceń wykonywanych na Zabbix agent/proxy po włączeniu parametru LogRemoteCommands w agent/proxy.

Możliwe komunikaty we frontendzie i wpisy w logu dla nieudanych poleceń/skryptów:

- Zawartość standardowego strumienia błędów i standardowego wyjścia dla nieudanych wykonań (jeśli występuje).
- "Proces zakończył działanie z kodem: N." (dla pustego wyjścia i kodu wyjścia różnego od 0).
- "Proces został zakończony sygnałem: N." (dla procesu zakończonego sygnałem, tylko w systemie Linux).
- "Proces został nieoczekiwanie zakończony." (dla procesu zakończonego z nieznanych przyczyn).

Zobacz także

- Kontrole zewnętrzne
- Parametry użytkownika
- pozycje system.run
- Niestandardowe skrypty alertów
- Zdalne polecenia
- Skrypty globalne

10 Zgodność wersji

Obsługiwane agenty

Aby zachować zgodność z Zabbix 8.0, agent Zabbix nie może być starszy niż wersja 1.4 i nie może być nowszy niż 8.0.

Może być konieczne sprawdzenie konfiguracji starszych agentów, ponieważ niektóre parametry uległy zmianie, na przykład parametry związane z logowaniem dla wersji wcześniejszych niż 3.0.

Aby w pełni wykorzystać najnowsze funkcje, metryki, lepszą wydajność oraz zmniejszone zużycie pamięci, używaj najnowszego obsługiwanego agenta.

Uwagi dotyczące Windows XP

- W 32-bitowym systemie Windows XP nie używaj agentów Zabbix nowszych niż 6.0.x;
- W systemach Windows XP/Server 2003 nie używaj szablonów agentów nowszych niż Zabbix 4.0.x. Nowsze szablony używają angielskich liczników wydajności, które są obsługiwane dopiero od Windows Vista/Server 2008.

Obsługiwane agenty 2

Starsze agenty Zabbix 2 od wersji 4.4 wzwyż są kompatybilne z Zabbix 8.0; Zabbix agent 2 nie może być nowszy niż 8.0.

Należy pamiętać, że podczas używania Zabbix agent 2 w wersjach 4.4 i 5.0 domyślnie stosowany jest interwał 10 minut do odświeżania nieobsługiwanych pozycji.

Aby w pełni wykorzystać najnowszą funkcjonalność, metryki, lepszą wydajność oraz zmniejszone zużycie pamięci, używaj najnowszego obsługiwanego agenta 2.

Obsługiwane proxy Zabbix

Aby zapewnić pełną zgodność z Zabbix 8.0, proxy muszą mieć tę samą główną wersję co serwer. Tylko proxy Zabbix 8.0.x są w pełni zgodne z serwerem Zabbix 8.0.x.

Nieaktualne proxy są częściowo obsługiwane: nadal mogą zbierać dane i wykonywać skrypty, ale nie mogą otrzymywać aktualizacji konfiguracji, takich jak nowe pozycje.

W odniesieniu do serwera Zabbix, proxy mogą być:

- *Aktualne* (proxy i serwer mają tę samą główną wersję);
- *Nieaktualne* (wersja proxy jest starsza niż wersja serwera, ale jest częściowo obsługiwana);
- *Nieobsługiwane* (wersja proxy jest starsza niż wersja poprzedniego wydania LTS serwera *lub* wersja proxy jest nowsza niż główna wersja serwera).

Przykłady:

Wersja serwera	Wersja proxy *aktualna*	Wersja proxy *nieaktualna*	Wersja proxy *nieobsługiwana*
6.4	6.4	6.0, 6.2	Starsza niż 6.0; nowsza niż 6.4
7.0	7.0	6.0, 6.2, 6.4	Starsza niż 6.0; nowsza niż 7.0
7.2	7.2	7.0	Starsza niż 7.0; nowsza niż 7.2
7.4	7.4	7.0	Starsza niż 7.0; nowsza niż 7.4
8.0	8.0	7.0, 7.2, 7.4	Starsza niż 7.0; nowsza niż 8.0

Funkcjonalność obsługiwana przez proxy:

Wersja proxy	Aktualizacja danych	Aktualizacja konfiguracji	Zadania
Bieżąca	Tak	Tak	Tak

Wersja proxy	Aktualizacja danych	Aktualizacja konfiguracji	Zadania
Nieaktualna	Tak	Nie	Polecenia zdalne (np. skrypty powłoki); Natychmiastowe sprawdzenia wartości pozycji (tj. *Wykonaj teraz*); Uwaga: testy przetwarzania wstępnego z rzeczywistą wartością nie są obsługiwane.
Nieobsługiwana	Nie	Nie	Nie

Ostrzeżenia dotyczące używania niekompatybilnych wersji demonów Zabbix są zapisywane w logu.

Obsługiwane pliki XML

Pliki XML nie starsze niż w wersji 1.8 są obsługiwane do importu w Zabbix 8.0.

Attention:
W formacie eksportu XML zależności wyzwalaczy są przechowywane wyłącznie według nazwy. Jeśli istnieje kilka wyzwalaczy o tej samej nazwie (na przykład o różnych poziomach ważności i wyrażeniach), pomiędzy którymi zdefiniowano zależność, ich import nie jest możliwy. Takie zależności należy ręcznie usunąć z pliku XML i dodać ponownie po imporcie.

12 Biblioteka dynamiczna Zabbix sender dla systemu Windows

Przegląd

W środowisku Windows aplikacje mogą wysyłać dane do serwera/proxy Zabbix przy użyciu biblioteki dynamicznej Zabbix sender (zabbix_sender.dll), zamiast uruchamiać proces zewnętrzny (zabbix_sender.exe).

Do kompilowania aplikacji użytkownika z użyciem zabbix_sender.dll wymagane są pliki zabbix_sender.h i zabbix_sender.lib.

Jak ją uzyskać

Istnieją dwa sposoby uzyskania pliku zabbix_sender.dll.

1. Pobierz pliki zabbix_sender.h, zabbix_sender.lib i zabbix_sender.dll jako archiwum ZIP.

Podczas wybierania opcji pobierania upewnij się, że w polu *Encryption* wybrano „No encryption", a w polu *Packaging* — „Archive". Następnie pobierz Zabbix agent (nie Zabbix agent 2).

Pliki zabbix_sender.h, zabbix_sender.lib i zabbix_sender.dll będą znajdować się w pobranym archiwum ZIP w katalogu `bin\dev`. Rozpakuj pliki w wybranej lokalizacji.

2. Zbuduj zabbix_sender.dll ze źródeł (zobacz instrukcje).

Biblioteka dynamiczna wraz z plikami deweloperskimi będzie znajdować się w katalogu `bin\winXX\dev`. Aby z niej korzystać, dołącz plik nagłówkowy zabbix_sender.h i linkuj z biblioteką zabbix_sender.lib.

Zobacz także

- przykład prostego narzędzia Zabbix sender zaimplementowanego przy użyciu biblioteki dynamicznej Zabbix sender, ilustrujący sposób użycia biblioteki;
- plik zabbix_sender.h zawierający funkcje interfejsu biblioteki dynamicznej Zabbix sender. Plik ten zawiera dokumentację wyjaśniającą przeznaczenie każdej funkcji interfejsu, jej argumenty oraz wartość zwracaną.

13 Aktualizacja monitorowania usług

Overview In Zabbix 6.0, service monitoring functionality has been reworked significantly (see What's new in Zabbix 6.0.0 for the list of changes).

This page describes how services and SLAs defined in earlier Zabbix versions are changed during an upgrade to Zabbix 6.0 or newer.

Usługi W starszych wersjach Zabbix usługi miały dwa typy zależności: miękkie i twarde. Po aktualizacji wszystkie zależności staną się równorzędne.

Jeśli usługa „Usługa podrzędna" była wcześniej powiązana z „Usługa nadrzędna 1" za pomocą zależności twardej, a dodatkowo z „Usługa nadrzędna 2" za pomocą zależności miękkiej, po aktualizacji „Usługa podrzędna" będzie miała dwie usługi nadrzędne: „Usługa nadrzędna 1" i „Usługa nadrzędna 2".

Mapowanie problemów na usługi oparte na wyzwalaczach zostało zastąpione mapowaniem opartym na tagach. W Zabbix 6.0 i nowszych formularz konfiguracji usługi ma nowy parametr *Tagi problemów*, który umożliwia określenie jednej lub wielu par nazwy i wartości tagu do dopasowywania problemów. Wyzwalacze, które zostały powiązane z usługą, otrzymają nowy tag `ServiceLink : <trigger ID>:<trigger name>` (wartość tagu zostanie obcięta do 32 znaków). Powiązane usługi otrzymają tag problemu `ServiceLink` o tej samej wartości.

Zasady obliczania statusu

„Status calculation algorithm" zostanie zaktualizowany zgodnie z następującymi zasadami:

- Nie obliczaj → Ustaw status na OK
- Problem, jeśli co najmniej jedno dziecko ma problem → Najbardziej krytyczny spośród usług podrzędnych
- Problem, jeśli wszystkie dzieci mają problemy → Najbardziej krytyczny, jeśli wszystkie usługi podrzędne mają problemy

SLA Wcześniej cele SLA musiały być definiowane osobno dla każdej usługi. Od wersji Zabbix 6.0 SLA stało się odrębną encją, która zawiera informacje o harmonogramie usługi, oczekiwanym celu poziomu usługi (SLO) oraz okresach przestoju wyłączonych z obliczeń. Po skonfigurowaniu SLA można przypisać do wielu usług za pomocą tagów usługi.

Podczas aktualizacji:

- Identyczne SLA zdefiniowane dla każdej usługi zostaną zgrupowane i dla każdej grupy zostanie utworzone jedno SLA.
- Każda usługa, której to dotyczy, otrzyma specjalny tag `SLA:<ID>`, a ten sam tag zostanie określony w parametrze *Service tags* odpowiedniego SLA.
- Czas utworzenia usługi, nowa metryka w raportach SLA, zostanie ustawiony na 01/01/2000 00:00 dla istniejących usług.

14 Inne problemy

Logowanie i systemd

Zalecamy utworzenie użytkownika *zabbix* jako użytkownika systemowego, to znaczy bez możliwości logowania. Niektórzy użytkownicy ignorują to zalecenie i używają tego samego konta do logowania (np. przez SSH) na host uruchamiający Zabbix. Może to spowodować awarię demona Zabbix przy wylogowaniu. W takim przypadku w logu serwera Zabbix pojawi się coś podobnego do poniższego:

```
zabbix_server [27730]: [file:'selfmon.c',line:375] lock failed: [22] Invalid argument
zabbix_server [27716]: [file:'dbconfig.c',line:5266] lock failed: [22] Invalid argument
zabbix_server [27706]: [file:'log.c',line:238] lock failed: [22] Invalid argument
```

a w logu agenta Zabbix:

```
zabbix_agentd [27796]: [file:'log.c',line:238] lock failed: [22] Invalid argument
```

Dzieje się tak z powodu domyślnego ustawienia systemd `RemoveIPC=yes` skonfigurowanego w `/etc/systemd/logind.conf`. Po wylogowaniu z systemu semafory utworzone wcześniej przez Zabbix są usuwane, co powoduje awarię.

Cytat z dokumentacji systemd:

```
RemoveIPC=

Określa, czy obiekty IPC System V i POSIX należące do użytkownika mają być usuwane, gdy
użytkownik całkowicie się wyloguje. Przyjmuje argument logiczny. Jeśli jest włączone,
użytkownik nie może korzystać z zasobów IPC po zakończeniu ostatniej sesji użytkownika.
Obejmuje to semafory System V, pamięć współdzieloną i kolejki komunikatów,
a także pamięć współdzieloną POSIX i kolejki komunikatów. Należy pamiętać, że obiekty IPC
użytkownika root i innych użytkowników systemowych są wyłączone spod działania tego ustawienia.
Wartość domyślna to "yes".
```

Istnieją 2 rozwiązania tego problemu:

1. (zalecane) Przestań używać konta *zabbix* do czegokolwiek innego niż procesy Zabbix; utwórz dedykowane konto do innych zastosowań.

2. (niezalecane) Ustaw `RemoveIPC=no` w `/etc/systemd/logind.conf` i uruchom ponownie system. Pamiętaj, że `RemoveIPC` jest parametrem obejmującym cały system, więc jego zmiana wpłynie na cały system.

Używanie frontend Zabbix za proxy

Jeśli frontend Zabbix działa za serwerem proxy, ścieżka cookie w pliku konfiguracyjnym proxy musi zostać przepisana tak, aby odpowiadała ścieżce reverse proxy. Zobacz przykłady poniżej. Jeśli ścieżka cookie nie zostanie przepisana, użytkownicy mogą napotkać problemy z autoryzacją podczas próby logowania do frontend Zabbix.

Przykładowa konfiguracja dla nginx

```
# ..
location / {
# ..
proxy_cookie_path /zabbix /;
proxy_pass http://192.168.0.94/zabbix/;
# ..
```

Przykładowa konfiguracja dla Apache

```
# ..
ProxyPass "/" http://host/zabbix/
ProxyPassReverse "/" http://host/zabbix/
ProxyPassReverseCookiePath /zabbix /
ProxyPassReverseCookieDomain host zabbix.example.com
# ..
```

16 Przykłady znaków ucieczki

Przegląd

Ta strona zawiera przykłady poprawnego stosowania znaków ucieczki podczas używania wyrażeń regularnych w różnych kontekstach.

> **Note:**
> Podczas korzystania z konstruktora wyrażeń wyzwalacza poprawne znaki ucieczki w wyrażeniach regularnych są dodawane automatycznie.

Przykłady

Makro użytkownika z kontekstem

Wyrażenie regularne: `\.+\"[a-z]+<br>` Makro użytkownika z kontekstem: `{$MACRO:regex:"\.+\\"[a-z]+"}`

Uwaga:

- ukośniki odwrotne nie są poprzedzane znakiem ucieczki;
- cudzysłowy są poprzedzane znakiem ucieczki.

Funkcja makra wewnątrz parametru klucza pozycji

Wyrażenie regularne: `.+:(\d+)$<br>` Klucz pozycji: `net.tcp.service[tcp,,"{{$ENDPOINT}.regsub(\".+:(\d+)$\",\1)}"]`

Uwaga:

- wyrażenie regularne wewnątrz funkcji makra `regsub` jest ujęte w podwójny cudzysłów (ponieważ zawiera zamykający nawias);
- cudzysłowy wokół wyrażenia regularnego są poprzedzane znakiem ucieczki (ponieważ cały trzeci parametr pozycji jest ujęty w podwójny cudzysłów);
- trzeci parametr klucza pozycji jest ujęty w podwójny cudzysłów, ponieważ zawiera przecinek.

Funkcja makra LLD

Wyrażenie regularne: `\.+\"([a-z]+)<br>` Makro LLD: `{{#MACRO}.iregsub("\.+\\"([a-z]+)", \1)}`

Uwaga:

- ukośniki odwrotne nie są poprzedzane znakiem ucieczki;
- cudzysłowy są poprzedzane znakiem ucieczki.

Funkcja makra LLD wewnątrz kontekstu makra użytkownika

Wyrażenie regularne: `\.+\"([a-z]+)<br>` Makro LLD: `{{#MACRO}.iregsub("\.+\\"([a-z]+)", \1)}<br>` Makro użytkownika z kontekstem: `{$MACRO:"{{#MACRO}.iregsub(\"\.+\\\"[a-z]+\", \1)}"}`

Uwaga:

- sposób poprzedzania znakiem ucieczki ukośników odwrotnych dla LLD nie zmienia się;
- przy wstawianiu makra LLD do kontekstu makra użytkownika należy umieścić je w ciągu znaków:

1. wokół wyrażenia makra dodawane są cudzysłowy;
2. cudzysłowy są poprzedzane znakiem ucieczki; łącznie wprowadzane są 3 nowe ukośniki odwrotne.

Parametr tekstowy funkcji (dowolnej)

Jako przykład użyto `concat`.

Zawartość ciągu: `\.+\"[a-z]+<br>` Wyrażenie: `concat("abc", "\\.\\\"[a-z]+")`

Uwaga:

- parametry tekstowe wymagają poprzedzania znakiem ucieczki zarówno ukośników odwrotnych, jak i cudzysłowów.

Funkcja makra LLD wewnątrz parametru tekstowego funkcji

Wyrażenie regularne: `\.+\"([a-z]+)<br>` Makro LLD: `{{#MACRO}.iregsub("\.+\\"([a-z]+)", \1)}<br>` Wyrażenie: `concat("abc, "{{#MACRO}.iregsub(\"\\.+\\\\\"([a-z]+)\", \\1)}")`

Uwaga:

- parametry tekstowe wymagają poprzedzania znakiem ucieczki zarówno ukośników odwrotnych, jak i cudzysłowów;
- dodawana jest kolejna warstwa poprzedzania znakiem ucieczki, ponieważ makro zostanie rozwiązane dopiero po usunięciu cudzysłowów z ciągu;

Makro użytkownika z kontekstem wewnątrz parametru tekstowego funkcji

Wyrażenie regularne: `\.+\"[a-z]+<br>` Makro użytkownika z kontekstem: `{$MACRO:regex:"\.+\\"[a-z]+"}<br>` Wyrażenie: `concat("abc, "{$MACRO:regex:\"\\.+\\\\\"[a-z]+\"}")`

Uwaga:

- podobnie jak w poprzednim przykładzie potrzebna jest dodatkowa warstwa poprzedzania znakiem ucieczki;
- ukośniki odwrotne i cudzysłowy są poprzedzane znakiem ucieczki tylko dla najwyższego poziomu poprzedzania znakiem ucieczki (ponieważ jest to parametr tekstowy).

Funkcja makra LLD wewnątrz kontekstu makra użytkownika wewnątrz funkcji

Wyrażenie regularne: `\.+\"([a-z])+<br>` Makro LLD: `{{#MACRO}.iregsub("\.+\\"([a-z]+)", \1)}<br>` Makro użytkownika z kontekstem: `{$MACRO:"{{#MACRO}.iregsub(\"\.+\\\"([a-z]+)\", \1)}"}<br>` Wyrażenie: `concat("abc, "{$MACRO:\"{{#MACRO}.iregsub(\\\"\.+\\\\\\\"([a-z]+)\\\", \\1)}\"}")`

Zwróć uwagę na trzy warstwy poprzedzania znakiem ucieczki:

1. Dla funkcji makra LLD, bez poprzedzania znakiem ucieczki ukośników odwrotnych;
2. Dla makra użytkownika z kontekstem, bez poprzedzania znakiem ucieczki ukośników odwrotnych;
3. Dla parametru tekstowego funkcji, z poprzedzaniem znakiem ucieczki ukośników odwrotnych.

Makro użytkownika z kontekstem bezpośrednio wewnątrz ciągu

Wyrażenie regularne: `\.+\"[a-z]+<br>` Makro użytkownika z kontekstem: `{$MACRO:regex:"\.+\\"[a-z]+"}<br>` Wewnątrz ciągu w pewnym wyrażeniu, na przykład: `func(arg1, arg2, arg3)="{$MACRO:regex:\"\\.+\\\\\"[a-z]+\"}"`

Uwaga:

- ciągi również wymagają poprzedzania znakiem ucieczki ukośników odwrotnych;
- ciągi również wymagają poprzedzania znakiem ucieczki cudzysłowów;
- ponownie jest to przypadek z 2 poziomami poprzedzania znakiem ucieczki:

1. Poprzedzanie znakiem ucieczki dla kontekstu makra użytkownika bez poprzedzania znakiem ucieczki ukośników odwrotnych;
2. Poprzedzanie znakiem ucieczki wynikające z tego, że jest to ciąg, z poprzedzaniem znakiem ucieczki ukośników odwrotnych.

21 Przewodniki szybkiego odniesienia

Przegląd

Ta sekcja dokumentacji zawiera szybkie instrukcje dotyczące konfiguracji Zabbix dla niektórych często wymaganych celów monitorowania.

Została zaprojektowana z myślą o nowych użytkownikach Zabbix i może służyć jako przewodnik po innych sekcjach dokumentacji, które zawierają informacje niezbędne do realizacji zadania.

Dostępne są następujące krótkie przewodniki:

- Monitorowanie systemu Linux za pomocą agent Zabbix
- Monitorowanie systemu Windows za pomocą agent Zabbix
- Monitorowanie Apache przez HTTP
- Monitorowanie MySQL za pomocą agent Zabbix 2
- Monitorowanie VMware za pomocą Zabbix
- Monitorowanie ruchu sieciowego za pomocą Zabbix
- Monitorowanie ruchu sieciowego za pomocą Zabbix z użyciem sprawdzeń aktywnych
- Monitorowanie witryn internetowych za pomocą pozycji przeglądarki
- Monitorowanie certyfikatów witryn internetowych za pomocą agent Zabbix 2 (pasywne)
- Monitorowanie przełącznika sieciowego lub routera za pomocą Zabbix
- Monitorowanie dziennika zdarzeń systemu Windows z użyciem sprawdzeń aktywnych

1. Monitor Linux with Zabbix agent

Wprowadzenie Ta strona przeprowadzi Cię przez kroki wymagane do rozpoczęcia podstawowego monitorowania maszyn z systemem Linux za pomocą Zabbix.
Kroki opisane w tym samouczku można zastosować do dowolnego systemu operacyjnego opartego na Linuksie.

Dla kogo jest ten przewodnik

Ten przewodnik jest przeznaczony dla nowych użytkowników Zabbix i zawiera minimalny zestaw kroków wymaganych do włączenia podstawowego monitorowania Twojej maszyny z systemem Linux. Jeśli szukasz opcji zaawansowanego dostosowywania lub potrzebujesz bardziej zaawansowanej konfiguracji, zobacz sekcję Konfiguracja w podręczniku Zabbix.

Wymagania wstępne

Przed przystąpieniem do tego przewodnika należy pobrać i zainstalować serwer Zabbix oraz frontend Zabbix zgodnie z instrukcjami dla używanego systemu operacyjnego.

Instalacja Zabbix agent Zabbix agent to proces odpowiedzialny za zbieranie danych.

Sprawdź wersję swojego serwera Zabbix:

```
zabbix_server -V
```

Zainstaluj Zabbix agent w tej samej wersji (zalecane) na maszynie z systemem Linux, którą chcesz monitorować. W zależności od potrzeb monitorowania może to być ta sama maszyna, na której zainstalowany jest serwer Zabbix, lub zupełnie inna maszyna.

Wybierz najbardziej odpowiednią metodę instalacji:

- Uruchom jako kontener Docker — zobacz listę dostępnych obrazów w repozytorium Docker Zabbix.
- Zainstaluj z pakietów Zabbix (dostępne dla Alma Linux, CentOS, Debian, Oracle Linux, Raspberry Pi OS, RHEL, Rocky Linux, SUSE Linux Enterprise Server, Ubuntu).
- Skompiluj ze źródeł.

Skonfiguruj Zabbix do monitorowania Zabbix agent może zbierać metryki w trybie aktywnym lub pasywnym (jednocześnie).

> **Note:**
> Sprawdzenie pasywne to proste żądanie danych. Zabbix serwer lub proxy prosi o określone dane (na przykład obciążenie CPU), a Zabbix agent odsyła wynik do serwera. Sprawdzenia aktywne wymagają bardziej złożonego przetwarzania. Agent musi najpierw pobrać z serwera(ów) listę pozycji do niezależnego przetwarzania, a następnie zbiorczo odesłać dane. Więcej informacji znajduje się w Pasywne i aktywne sprawdzenia agenta.

Szablony monitorowania dostarczane przez Zabbix zwykle oferują dwie alternatywy — szablon dla Zabbix agent oraz szablon dla Zabbix agent (active). W pierwszym przypadku agent będzie zbierać metryki w trybie pasywnym. Takie szablony zapewniają identyczne wyniki monitorowania, ale z użyciem różnych protokołów komunikacyjnych.

Dalsza konfiguracja Zabbix zależy od tego, czy wybierzesz szablon dla aktywnych czy pasywnych sprawdzeń Zabbix agent.

Kontrole pasywne Zabbix agent

1. Otwórz plik konfiguracyjny agenta na maszynie, na której agent jest zainstalowany.

```
sudo vi /etc/zabbix/zabbix_agentd.conf
```

2. Dodaj adres IP lub nazwę DNS (oraz opcjonalny port) swojego serwera Zabbix do parametru server. Na przykład:

```
Server=192.0.2.0:10051
```

Zabbix agent będzie używać tego adresu do akceptowania połączeń przychodzących wyłącznie od określonych serwerów Zabbix lub proxy w celu pobierania danych.

3. Uruchom ponownie Zabbix agent.

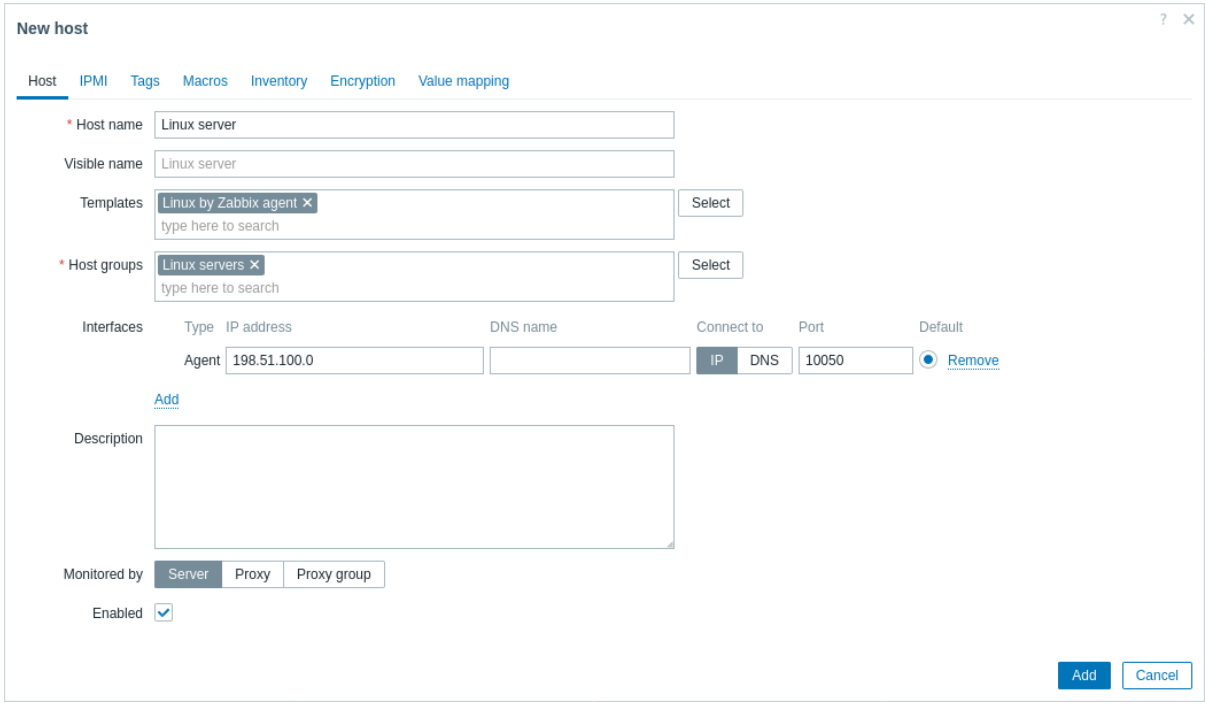
```
systemctl restart zabbix-agent
```

Zabbix frontend

1. Zaloguj się do Zabbix frontend.

2. Utwórz host w interfejsie webowym Zabbix.

- W polu *Host name* wprowadź nazwę hosta (np. „Linux server”).
- W polu *Templates* wpisz lub wybierz szablon „Linux by Zabbix agent”, który zostanie podłączony do hosta.
- W polu *Host groups* wpisz lub wybierz grupę hostów (np. „Linux servers”).
- W parametrze *Interfaces* dodaj interfejs *Agent* i określ adres IP lub nazwę DNS maszyny z systemem Linux, na której zainstalowano agent.



3. Kliknij *Add*, aby dodać hosta. Ten host będzie reprezentować monitorowaną maszynę z systemem Linux.

Kontrole aktywne Zabbix agent

1. Otwórz plik konfiguracyjny agent na maszynie, na której agent jest zainstalowany.

```
sudo vi /etc/zabbix/zabbix_agentd.conf
```

2. Dodaj adres IP lub nazwę DNS (oraz opcjonalny port) swojego serwera Zabbix do parametru ServerActive. Na przykład:

```
ServerActive=192.0.2.0:10051
```

Zabbix agent użyje tego adresu do połączenia z portem trapper serwera Zabbix (domyślnie: 10051) i zażądania danych konfiguracyjnych dla aktywnych kontroli.

3. Zdefiniuj parametr Hostname, który musi odpowiadać nazwie hosta zdefiniowanej w frontend Zabbix. W naszym przykładzie jest to:

```
Hostname=Linux server
```

Wartość Hostname musi się zgadzać, ponieważ w przypadku aktywnych kontroli Zabbix agent używa jej do pobrania prawidłowej konfiguracji hosta z serwera. Dokładniej mówiąc, agent inicjuje połączenie z serwerem i identyfikuje się za pomocą wartości Hostname. Następnie serwer dostarcza konfigurację monitorowania dla tego hosta. Jeśli te wartości będą się różnić, agent nie otrzyma odpowiedniej konfiguracji, co spowoduje brak metryk lub problemy z monitorowaniem.

4. Uruchom ponownie Zabbix agent.

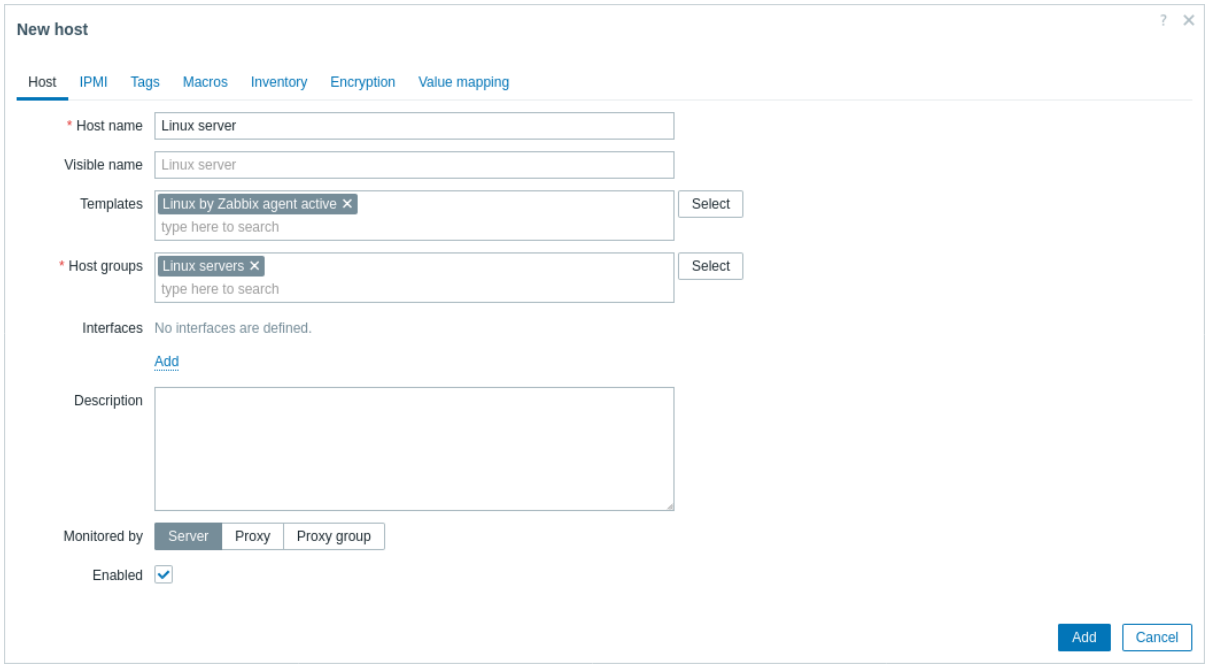
```
systemctl restart zabbix-agent
```

Zabbix frontend

1. Zaloguj się do Zabbix frontend.

2. Utwórz hosta w interfejsie webowym Zabbix.

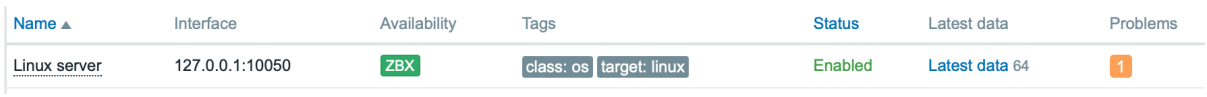
- W polu *Host name* wprowadź nazwę hosta (np. „Linux server”), która odpowiada wartości parametru *Hostname* zdefiniowanej wcześniej w pliku konfiguracyjnym agenta.
- W polu *Templates* wpisz lub wybierz szablon „Linux by Zabbix agent active”, który zostanie podłączony do hosta.
- W polu *Host groups* wpisz lub wybierz grupę hostów (np. „Linux servers”).
- Pozostaw *Interfaces* niezdefiniowane; interfejs nie jest wymagany dla aktywnych testów, ponieważ agent inicjuje połączenie z serwerem, zamiast nasłuchiwać połączenia z serwera.



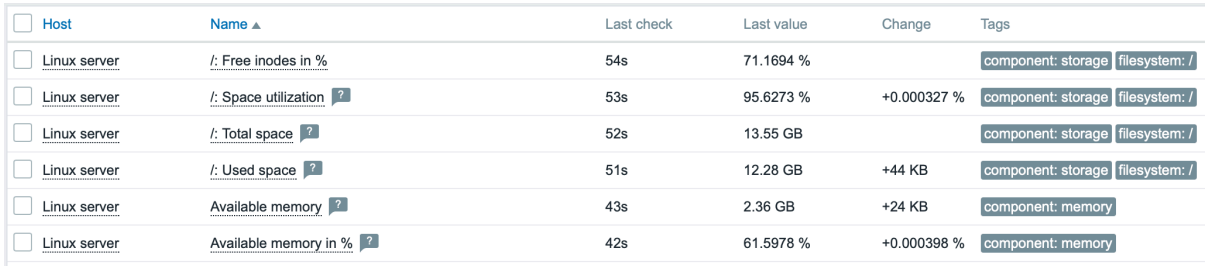
3. Kliknij *Add*, aby dodać hosta. Ten host będzie reprezentować monitorowaną maszynę z systemem Linux.

Wyświetlanie zebranych metryk Gratulacje! Na tym etapie Zabbix już monitoruje Twoją maszynę z systemem Linux.

Aby wyświetlić zebrane metryki, otwórz sekcję menu *Monitoring->Hosts* menu section i kliknij *Latest data* obok hosta.

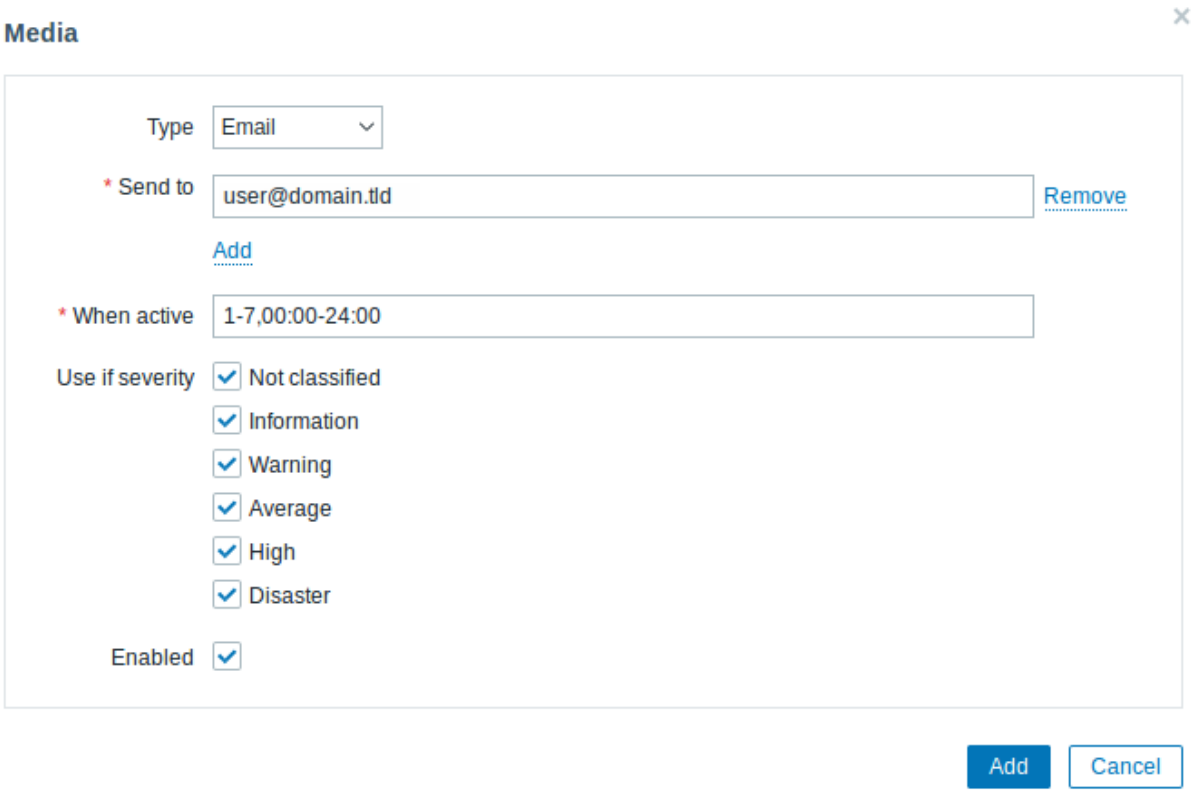


Ta czynność otworzy listę wszystkich najnowszych metryk zebranych z hosta serwera Linux.



Konfiguracja alertów o problemach Zabbix może powiadamiać o problemach z infrastrukturą na wiele sposobów. Ten przewodnik zawiera kroki konfiguracji wysyłania alertów e-mail.

1. Przejdź do *Ustawienia użytkownika -> Profil*, przełącz się na kartę *Media* i dodaj swój adres e-mail.



2. Postępuj zgodnie z przewodnikiem Otrzymywanie powiadomień o problemach.

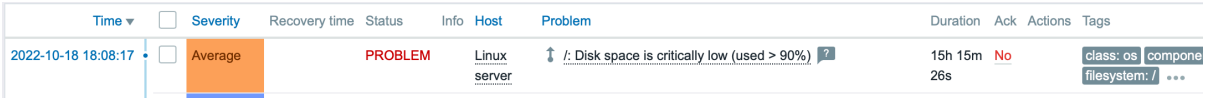
Następnym razem, gdy Zabbix wykryje problem, powinieneś otrzymać alert e-mail.

Przetestuj swoją konfigurację W systemie Linux możesz zasymulować wysokie obciążenie CPU i w rezultacie otrzymać alert o problemie, uruchamiając:

```
cat /dev/urandom | md5sum
```

Może być konieczne uruchomienie kilku procesów md5sum, aby obciążenie CPU przekroczyło próg.

Gdy Zabbix wykryje problem, pojawi się on w sekcji Monitoring->Problems.



Jeśli alerty są skonfigurowane, otrzymasz również powiadomienie o problemie.

Zobacz także:

- Tworzenie pozycji - jak rozpocząć monitorowanie dodatkowych metryk (monitorowanie niestandardowe bez szablonów).
- Pozycje Zabbix agent, Pozycje Zabbix agent dla Windows - pełna lista metryk, które można monitorować przy użyciu Zabbix agent w systemie Windows.
- Eskalacje problemów - jak tworzyć wieloetapowe scenariusze alertów (np. najpierw wysłać wiadomość do administratora systemu, a następnie, jeśli problem nie zostanie rozwiązany w ciągu 45 minut, wysłać wiadomość do kierownika centrum danych).
- Instalacja z pakietów - jak instalować komponenty Zabbix przy użyciu oficjalnych pakietów RPM i DEB dla różnych dystrybucji Linuksa, zapewniając dostęp do najnowszych funkcji i poprawek błędów.

2 Monitorowanie systemu Windows za pomocą agent Zabbix

Wprowadzenie Ta strona przeprowadzi Cię przez kroki wymagane do rozpoczęcia podstawowego monitorowania maszyn z systemem Windows za pomocą Zabbix.

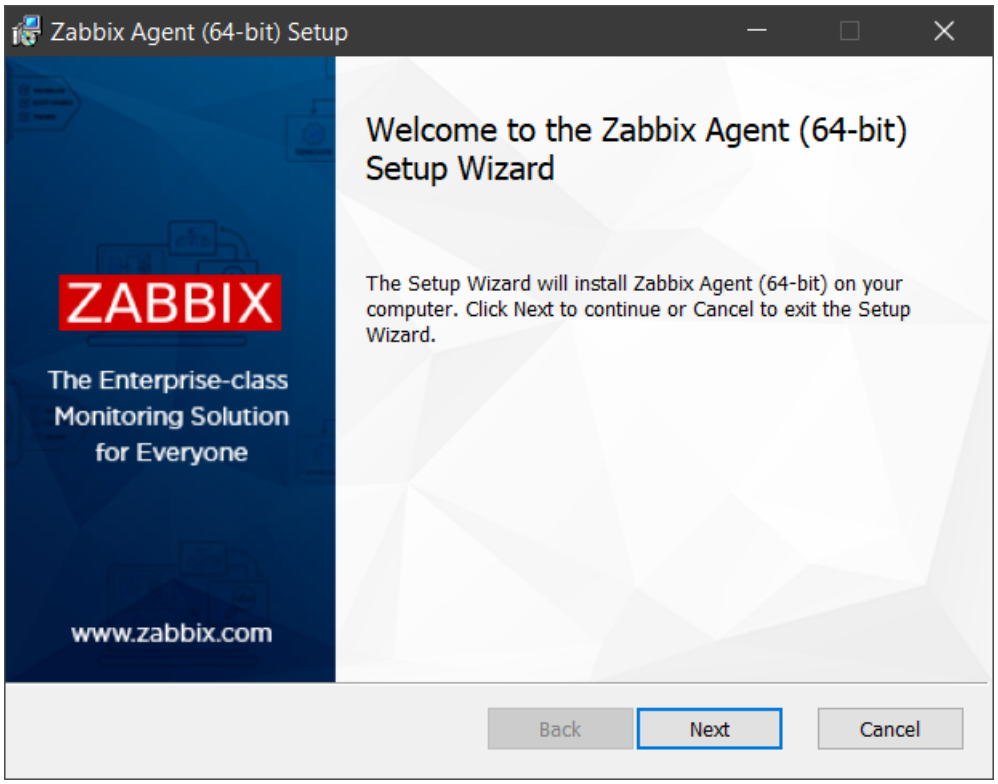
Dla kogo jest ten przewodnik

Ten przewodnik jest przeznaczony dla nowych użytkowników Zabbix i zawiera minimalny zestaw kroków wymaganych do włączenia podstawowego monitorowania maszyny z systemem Windows. Jeśli szukasz opcji zaawansowanego dostosowania lub potrzebujesz bardziej zaawansowanej konfiguracji, zobacz sekcję Configuration w podręczniku Zabbix.

Wymagania wstępne

Przed kontynuowaniem tego przewodnika instalacji musisz pobrać i zainstalować serwer Zabbix oraz frontend Zabbix zgodnie z instrukcjami dla swojego systemu operacyjnego.

Instalacja agenta Zabbix Agent Zabbix to proces odpowiedzialny za zbieranie danych. Należy go zainstalować na komputerze z systemem Windows, który ma być monitorowany. Postępuj zgodnie z instrukcjami instalacji agenta Zabbix dla systemu Windows.



Konfiguracja Zabbix do monitorowania Zabbix agent może zbierać metryki w trybie aktywnym lub pasywnym (jednocześnie).

Note:
Sprawdzenie pasywne jest prostym żądaniem danych. Serwer Zabbix lub proxy prosi o określone dane (na przykład obciążenie CPU), a Zabbix agent odsyła wynik do serwera. Sprawdzenia aktywne wymagają bardziej złożonego przetwarzania. Agent musi najpierw pobrać z serwera(ów) listę pozycji do niezależnego przetwarzania, a następnie zbiorczo odesłać dane. Więcej informacji można znaleźć w Pasywne i aktywne sprawdzenia agenta.

Szablony monitorowania dostarczane przez Zabbix zwykle oferują dwie alternatywy — szablon dla Zabbix agent oraz szablon dla Zabbix agent (active). W pierwszym przypadku agent będzie zbierać metryki w trybie pasywnym. Takie szablony zapewniają identyczne wyniki monitorowania, ale z użyciem różnych protokołów komunikacyjnych.

Dalsza konfiguracja Zabbix zależy od tego, czy wybierzesz szablon dla aktywnych czy pasywnych sprawdzeń Zabbix agent.

Pasywne kontrole Zabbix frontend

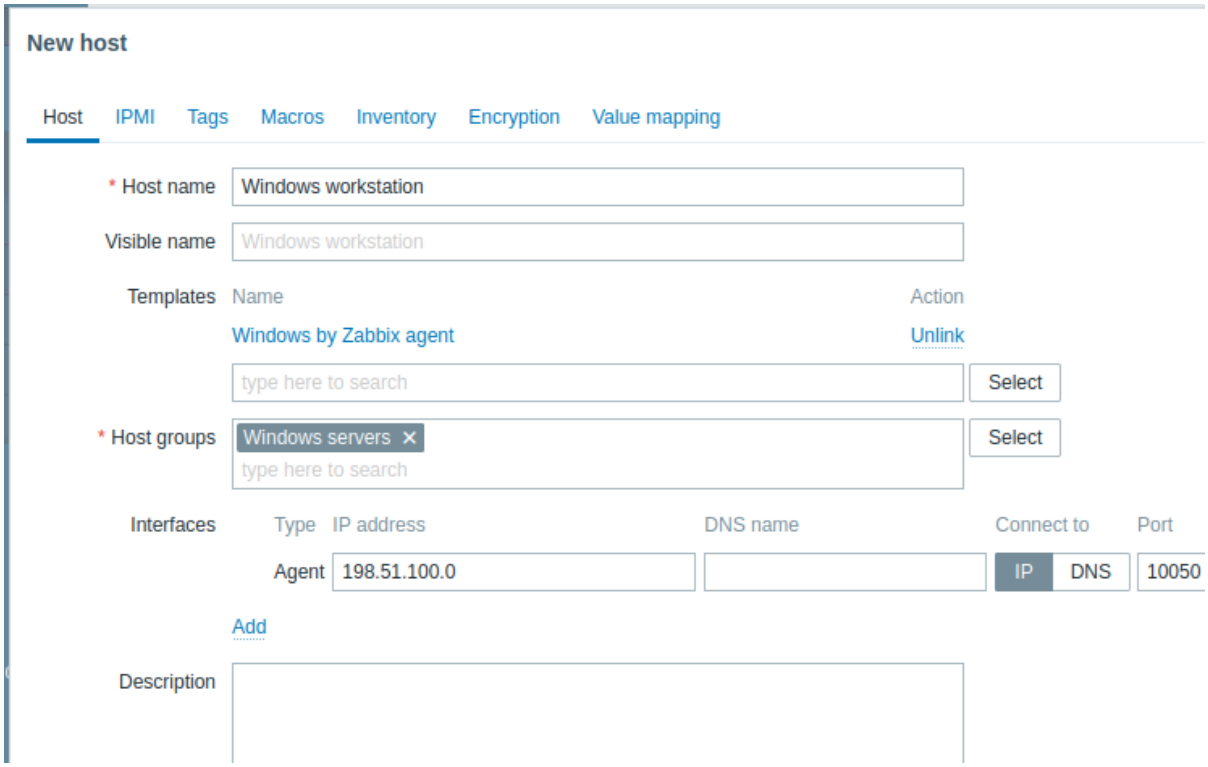
1. Zaloguj się do Zabbix frontend.

2. Utwórz hosta w interfejsie webowym Zabbix.

Ten host będzie reprezentował Twoją maszynę z systemem Windows.

3. W parametrze *Interfaces* dodaj interfejs *Agent* i określ adres IP lub nazwę DNS maszyny z systemem Windows, na której zainstalowano agent.

4. W parametrze *Templates* wpisz lub wybierz *Windows by Zabbix agent*.



Zabbix agent

W przypadku sprawdzeń pasywnych agent Zabbix musi znać adres IP lub nazwę DNS serwera Zabbix. Jeśli podczas instalacji agent podałeś poprawne informacje, plik konfiguracyjny jest już zaktualizowany. W przeciwnym razie musisz określić je ręcznie. Przejdź do folderu `C:\Program files\Zabbix Agent`, otwórz plik *zabbix_agentd.conf* i dodaj IP/DNS swojego serwera Zabbix do parametru *Server*.

Przykład:

```
Server=192.0.2.22
```

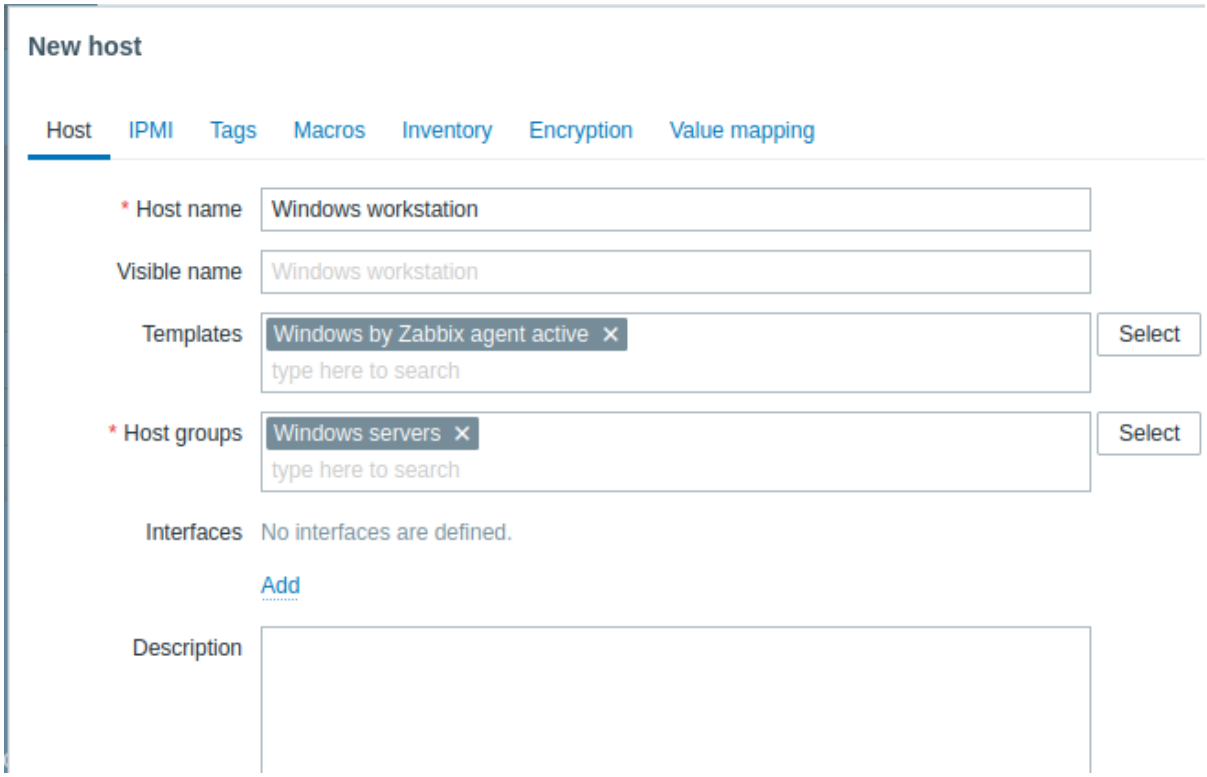
Aktywne kontrole Frontend Zabbix

1. Zaloguj się do frontend Zabbix.

2. Utwórz host w interfejsie webowym Zabbix.

Ten host będzie reprezentował Twój komputer z systemem Windows.

3. W parametrze *Templates* wpisz lub wybierz *Windows by Zabbix agent active*.



Zabbix agent

W folderze `C:\Program files\Zabbix Agent` otwórz plik *zabbix_agentd.conf* i dodaj:

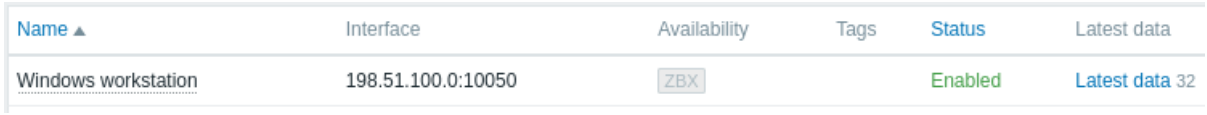
- Nazwę hosta utworzonego w interfejsie webowym Zabbix do parametru *Hostname*.
- Adres IP lub nazwę DNS maszyny serwera Zabbix do parametru *ServerActive* (może być już wstępnie uzupełniony, jeśli został podany podczas konfiguracji Zabbix agent).

Przykład:

```
ServerActive= 192.0.2.22
Hostname=Windows workstation
```

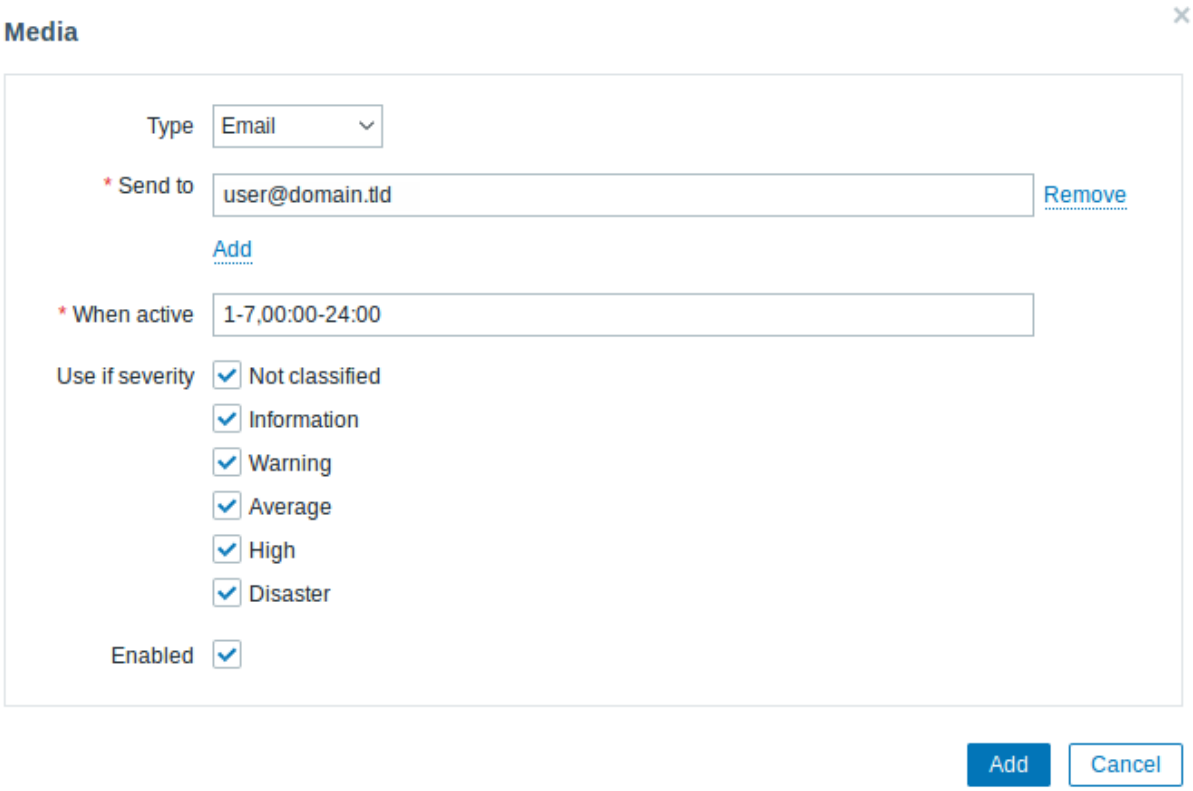
Wyświetlanie zebranych metryk Gratulacje! Na tym etapie Zabbix już monitoruje Twoją maszynę z systemem Windows.

Aby wyświetlić zebrane metryki, otwórz sekcję menu *Monitoring->Hosts* menu section i kliknij *Latest data* obok hosta.



Konfiguracja alertów o problemach Zabbix może powiadamiać o problemach z infrastrukturą na wiele sposobów. Ten przewodnik zawiera kroki konfiguracji wysyłania alertów e-mail.

1. Przejdź do *Ustawienia użytkownika -> Profil*, przełącz się na kartę *Media* i dodaj swój adres e-mail.



2. Postępuj zgodnie z przewodnikiem Otrzymywanie powiadomień o problemach.

Następnym razem, gdy Zabbix wykryje problem, powinieneś otrzymać alert e-mail.

Note:
W systemie Windows możesz użyć narzędzia CpuStres, aby zasymulować wysokie obciążenie CPU i w rezultacie otrzymać alert o problemie.

Zobacz także:

- Tworzenie pozycji — jak rozpocząć monitorowanie dodatkowych metryk (monitoring niestandardowy bez szablonów).
- Pozycje agenta Zabbix, Pozycje agenta Zabbix dla Windows — pełna lista metryk, które można monitorować za pomocą agenta Zabbix w systemie Windows.
- Eskalacje problemów — jak tworzyć wieloetapowe scenariusze alertów (np. najpierw wysłać wiadomość do administratora systemu, a następnie, jeśli problem nie zostanie rozwiązany w ciągu 45 minut, wysłać wiadomość do kierownika centrum danych).

3. Monitor Apache via HTTP

Wprowadzenie Ta strona pokazuje szybki i prosty sposób na rozpoczęcie monitorowania serwera WWW Apache bez instalowania żadnego dodatkowego oprogramowania.

Dla kogo jest ten przewodnik

Ten przewodnik jest przeznaczony dla nowych użytkowników Zabbix i zawiera minimalny zestaw kroków wymaganych do włączenia podstawowego monitorowania instalacji Apache. Jeśli szukasz opcji zaawansowanego dostosowania lub potrzebujesz bardziej zaawansowanej konfiguracji, zobacz sekcję Configuration podręcznika Zabbix.

Wymagania wstępne

Przed przystąpieniem do korzystania z tego przewodnika instalacji należy pobrać i zainstalować serwer Zabbix oraz frontend Zabbix zgodnie z instrukcjami dla używanego systemu operacyjnego.

Przygotowanie Apache 1. Sprawdź, której wersji Apache używasz:

W systemie opartym na RHEL uruchom:

```
httpd -v
```

W Debianie/Ubuntu uruchom:

```
apache2 -v
```

2. Upewnij się, że moduł Status jest włączony w Twojej instancji Apache.

W systemie opartym na RHEL uruchom:

```
httpd -M | grep status
status_module (shared)
```

W Debianie/Ubuntu uruchom:

```
apache2ctl -M | grep status
status_module (shared)
```

Jeśli nie widzisz status_module na liście, włącz moduł, uruchamiając:

W systemie opartym na RHEL uruchom:

```
LoadModule status_module /usr/lib/apache2/modules/mod_status.so
```

W Debianie/Ubuntu uruchom:

```
sudo /usr/sbin/a2enmod status
```

3. Edytuj plik konfiguracyjny Apache, aby zezwolić na dostęp do raportów statusu z adresu IP serwera Zabbix.

W systemie opartym na RHEL: `/etc/httpd/conf.modules.d/status.conf`:

```
sudo vi /etc/httpd/conf.modules.d/status.conf
```

W Debianie/Ubuntu: `/etc/apache2/mods-enabled/status.conf`:

```
sudo vi /etc/apache2/mods-enabled/status.conf
```

Dodaj następujące linie do pliku (**zastąp 198.51.100.255** adresem IP swojego serwera Zabbix):

- Dla Apache 2.2:
  <Location /server-status> SetHandler server-status

  Order Deny,Allow Deny from all Allow from 198.51.100.255 </Location>
- Dla Apache 2.4:
  <Location ”/server-status”> SetHandler server-status Require ip 198.51.100.255 </Location>

4. Uruchom ponownie Apache

W systemie opartym na RHEL uruchom:

```
sudo systemctl restart httpd
```

W Debianie/Ubuntu uruchom:

```
sudo systemctl restart apache2
```

5. Aby sprawdzić, czy wszystko jest skonfigurowane poprawnie, uruchom (**zastąp 198.51.100.255** adresem IP swojego serwera Zabbix):

```
curl 198.51.100.255/server-status
```

Odpowiedź powinna zawierać statystyki serwera WWW Apache.

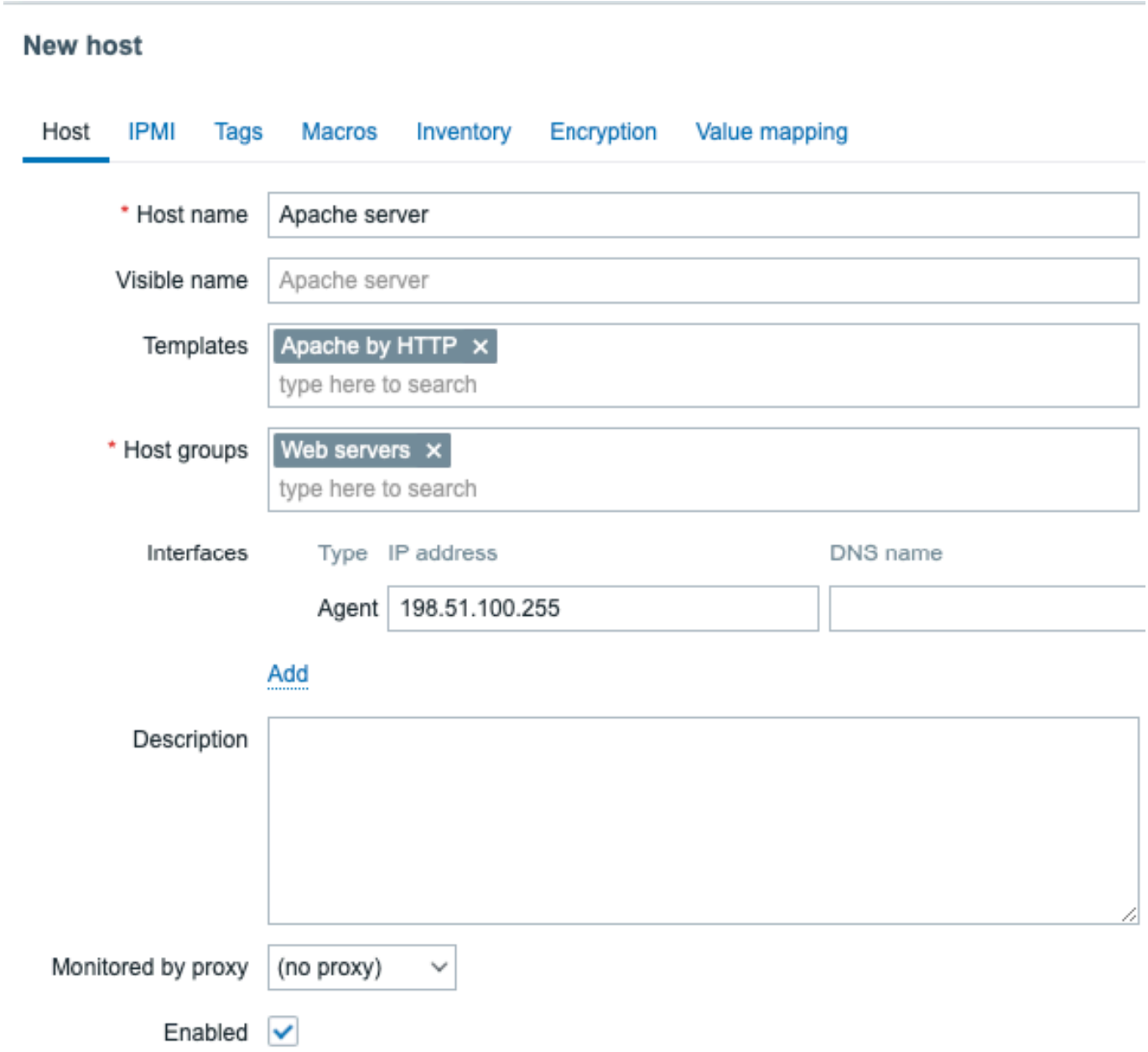
Skonfiguruj Zabbix do monitorowania 1. Zaloguj się do frontend Zabbix.

2. Utwórz hosta w interfejsie webowym Zabbix.

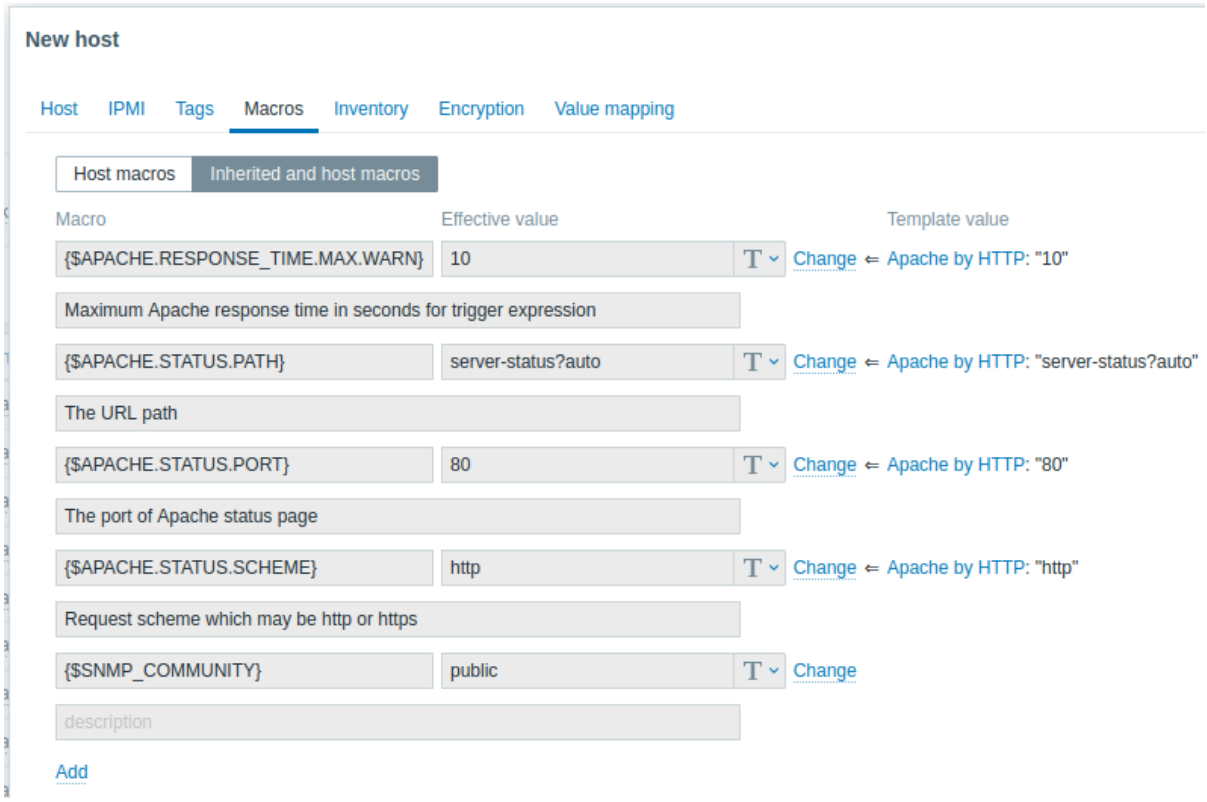
Ten host będzie reprezentował Twój serwer Apache.

3. W parametrze *Interfaces* dodaj interfejs *Agent* i podaj adres IP swojej instancji Apache. **Nie musisz instalować Zabbix agent na tej maszynie**, interfejs będzie używany wyłącznie do rozwiązywania makra {HOST.CONN}. To makro jest używane w pozycjach szablonu do lokalizowania instancji Apache.

4. W parametrze *Templates* wpisz lub wybierz *Apache by HTTP*.



5. Przejdź do zakładki **Macros** i wybierz tryb *Inherited and host macros*. Sprawdź, czy wartości makr {$APACHE.STATUS.PORT} i {$APACHE.STATUS.SCHEME} odpowiadają ustawieniom Twojej instalacji. Domyślnie port to 80, a schemat to http. Zmień wartości makr, jeśli używasz innego portu i/lub schematu.



Wyświetlanie zebranych metryk Gratulacje! Na tym etapie Zabbix monitoruje już Twój serwer WWW Apache.

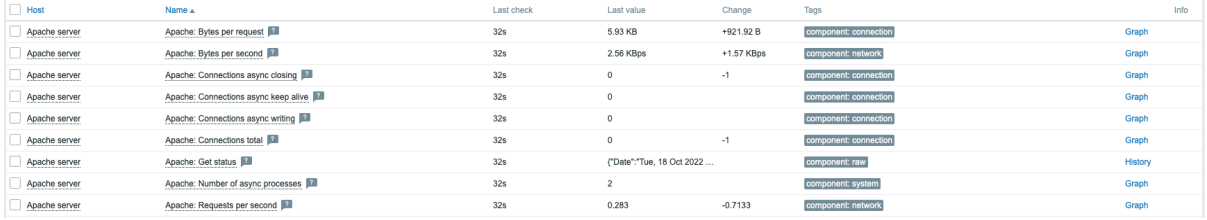
Aby wyświetlić zebrane metryki, otwórz sekcję menu *Monitoring->Hosts* menu section i kliknij *Dashboards* obok hosta.



Ta czynność przeniesie Cię do pulpitu hosta z najważniejszymi metrykami zebranymi ze strony Apache /server-status.

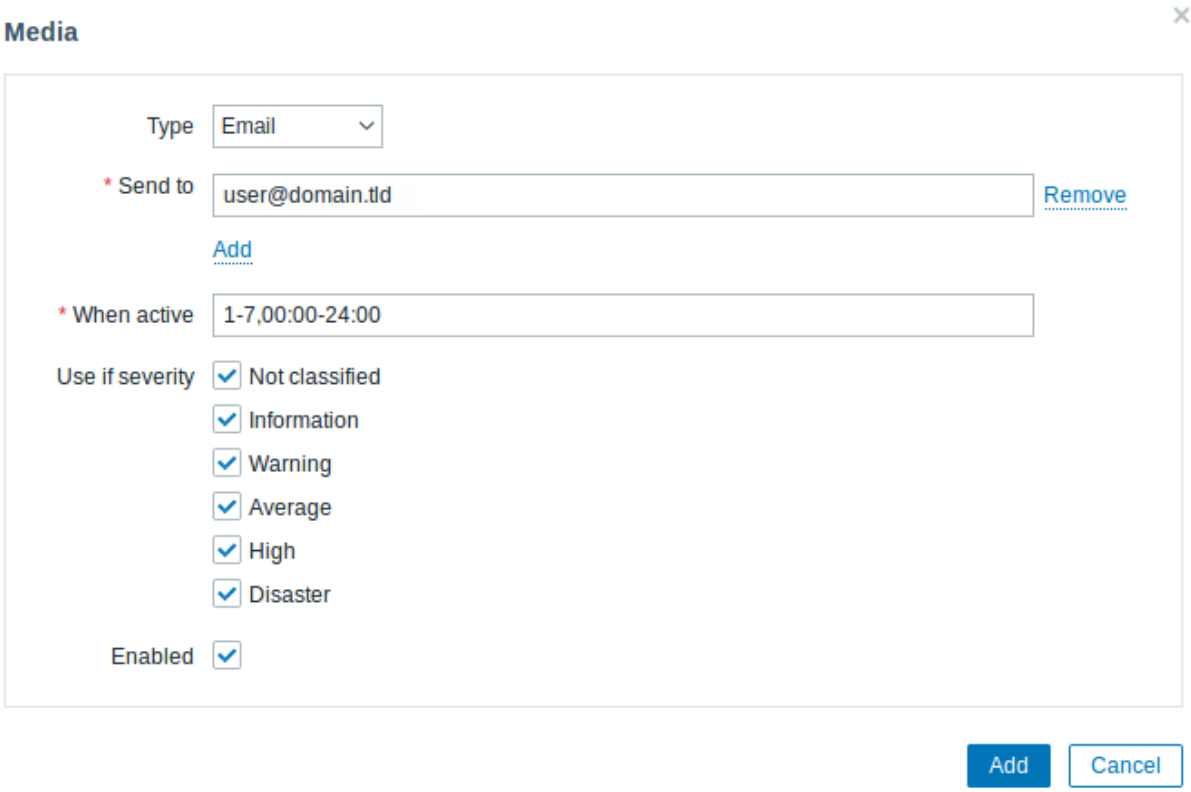


Alternatywnie, w sekcji *Monitoring->Hosts* możesz kliknąć *Latest data*, aby wyświetlić wszystkie ostatnio zebrane metryki na liście.



Konfiguracja alertów o problemach Zabbix może powiadamiać o problemach z infrastrukturą na wiele sposobów. Ten przewodnik zawiera kroki konfiguracji wysyłania alertów e-mail.

1. Przejdź do *Ustawienia użytkownika -> Profil*, przełącz się na kartę *Media* i dodaj swój adres e-mail.

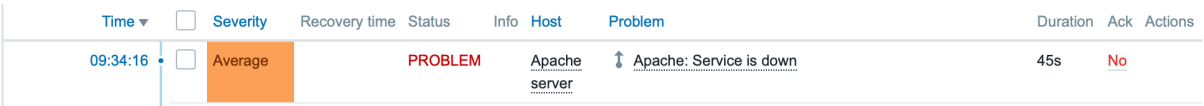


2. Postępuj zgodnie z przewodnikiem Otrzymywanie powiadomień o problemach.

Następnym razem, gdy Zabbix wykryje problem, powinieneś otrzymać alert e-mail.

Przetestuj swoją konfigurację Aby zasymulować rzeczywisty problem i otrzymać testowy alert o problemie:

1. Otwórz konfigurację hosta *Apache server* w Zabbix.
2. Przejdź do zakładki Makra i wybierz *Inherited and host macros*.
3. Naciśnij *Change* obok makra {$APACHE.STATUS.PORT} i ustaw inny port.
4. Naciśnij Update, aby zapisać konfigurację hosta.
5. Za kilka minut Zabbix wykryje problem *Apache service is down*, ponieważ nie będzie już mógł połączyć się z instancją. Pojawi się on w sekcji Monitoring->Problems.



Jeśli alerty są skonfigurowane, otrzymasz również powiadomienie o problemie.

6. Zmień wartość makra z powrotem, aby rozwiązać problem i kontynuować monitorowanie Apache.

Zobacz także:

- Wzmacnianie zabezpieczeń serwera WWW - zalecane ustawienia zwiększające bezpieczeństwo serwera WWW.
- Tworzenie pozycji - jak rozpocząć monitorowanie dodatkowych metryk.
- Pozycje HTTP - jak monitorować niestandardowe metryki przy użyciu HTTP agent.
- Eskalacje problemów - jak tworzyć wieloetapowe scenariusze alertów (np. najpierw wysłać wiadomość do administratora systemu, a następnie, jeśli problem nie zostanie rozwiązany w ciągu 45 minut, wysłać wiadomość do kierownika centrum danych).

4. Monitor MySQL with Zabbix agent 2

Wprowadzenie

Ta strona przeprowadzi Cię przez kroki wymagane do rozpoczęcia podstawowego monitorowania serwera MySQL.

Aby monitorować serwer MySQL, dostępnych jest kilka podejść: Zabbix agent, Zabbix agent 2 lub standard Open Database Connectivity (ODBC). Głównym celem tego przewodnika jest monitorowanie serwera MySQL za pomocą Zabbix agent 2, co jest podejściem **zalecanym** ze względu na jego bezproblemową konfigurację w różnych środowiskach. Jednak ta strona zawiera również instrukcje dotyczące innych podejść, więc możesz wybrać to, które najlepiej odpowiada Twoim wymaganiom.

Dla kogo jest ten przewodnik

Ten przewodnik jest przeznaczony dla nowych użytkowników Zabbix i zawiera minimalny zestaw kroków wymaganych do włączenia podstawowego monitorowania serwera MySQL. Jeśli szukasz opcji zaawansowanego dostosowywania lub potrzebujesz bardziej zaawansowanej konfiguracji, zobacz sekcję Konfiguracja w podręczniku Zabbix.

Wymagania wstępne

Przed przystąpieniem do tego przewodnika należy pobrać i zainstalować serwer Zabbix, frontend Zabbix oraz agent Zabbix 2 zgodnie z instrukcjami dla używanego systemu operacyjnego.

W zależności od środowiska niektóre kroki opisane w tym przewodniku mogą się nieznacznie różnić. Ten przewodnik opiera się na środowisku działającym pod kontrolą Ubuntu.

Utwórz użytkownika MySQL

Aby monitorować serwer MySQL, Zabbix wymaga dostępu do niego oraz do jego procesów. Twoja instalacja MySQL ma już użytkownika z wymaganym poziomem dostępu (użytkownika „zabbix", który został utworzony podczas instalacji Zabbix), jednak ten użytkownik ma więcej uprawnień, niż jest to konieczne do prostego monitorowania (uprawnienia do DROP baz danych, DELETE wpisów z tabel itp.). Dlatego należy utworzyć użytkownika MySQL przeznaczonego *wyłącznie* do monitorowania serwera MySQL.

1. Połącz się z klientem MySQL, utwórz użytkownika „zbx_monitor" (zastąp <*password*> dla użytkownika „zbx_monitor" wybranym przez siebie hasłem) i przyznaj użytkownikowi niezbędne uprawnienia za pomocą GRANT:

```
mysql -u root -p
# Enter password:

mysql> CREATE USER 'zbx_monitor'@'%' IDENTIFIED BY '<password>';
mysql> GRANT REPLICATION CLIENT,PROCESS,SHOW DATABASES,SHOW VIEW ON *.* TO 'zbx_monitor'@'%';
mysql> quit;
```

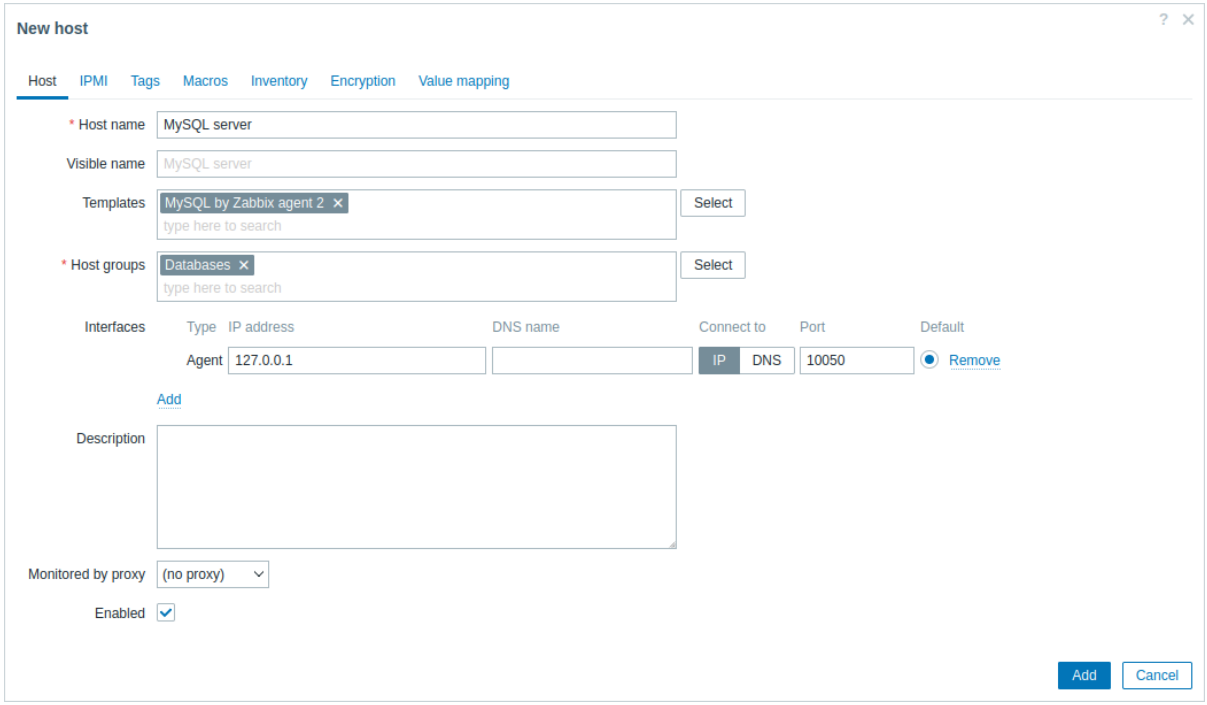
Po utworzeniu użytkownika możesz przejść do następnego kroku.

Skonfiguruj frontend Zabbix

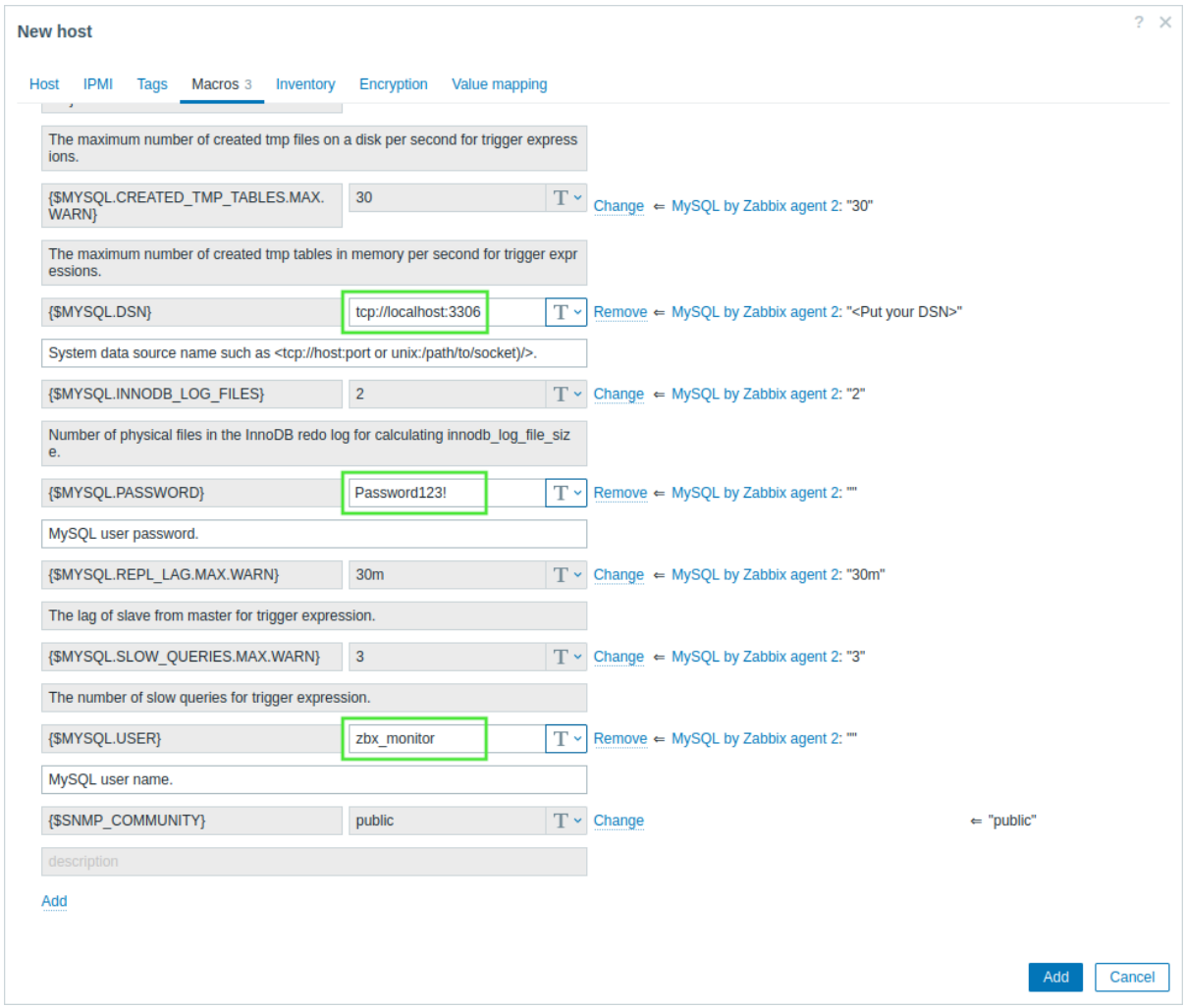
1. Zaloguj się do frontend Zabbix.

2. Utwórz hosta w interfejsie webowym Zabbix:

- W polu *Host name* wprowadź nazwę hosta (np. „MySQL server").
- W polu *Templates* wpisz lub wybierz szablon „MySQL by Zabbix agent 2", który zostanie podłączony do hosta.
- W polu *Host groups* wpisz lub wybierz grupę hostów (np. „Databases").
- W polu *Interfaces* dodaj interfejs typu „Agent" i podaj adres IP swojego serwera MySQL. W tym przewodniku użyto adresu „127.0.0.1" (localhost) do monitorowania serwera MySQL zainstalowanego na tej samej maszynie co serwer Zabbix i Zabbix agent 2.



- Na karcie *Macros* przełącz się na *Inherited and host macros*, odszukaj następujące makra i kliknij *Change* obok wartości makra, aby je zaktualizować:
  - {$MYSQL.DSN} - ustaw źródło danych serwera MySQL (connection string of a named session z pliku konfiguracyjnego wtyczki MySQL dla Zabbix agent 2). W tym przewodniku użyto domyślnego źródła danych „tcp://localhost:3306" do monitorowania serwera MySQL zainstalowanego na tej samej maszynie co serwer Zabbix i Zabbix agent 2.
  - {$MYSQL.PASSWORD} - ustaw hasło wcześniej utworzonego użytkownika MySQL „zbx_monitor".
  - {$MYSQL.USER} - ustaw nazwę wcześniej utworzonego użytkownika MySQL „zbx_monitor".

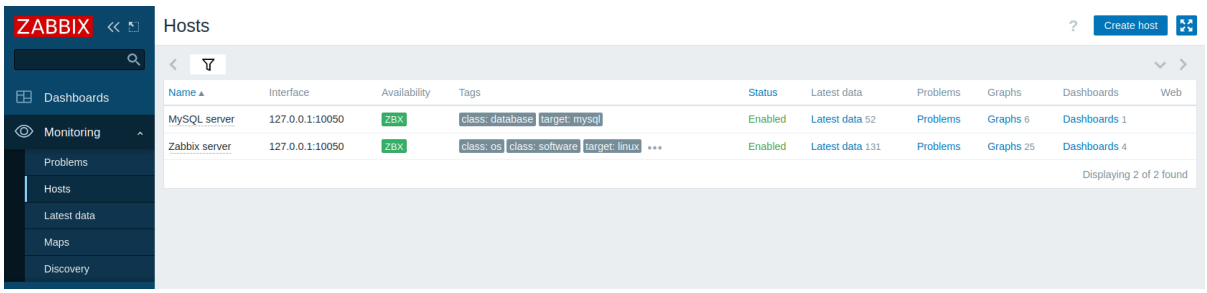


3. Kliknij *Add*, aby dodać hosta. Ten host będzie reprezentował Twój serwer MySQL.

Wyświetlanie zebranych metryk

Gratulacje! Na tym etapie Zabbix monitoruje już Twój serwer MySQL.

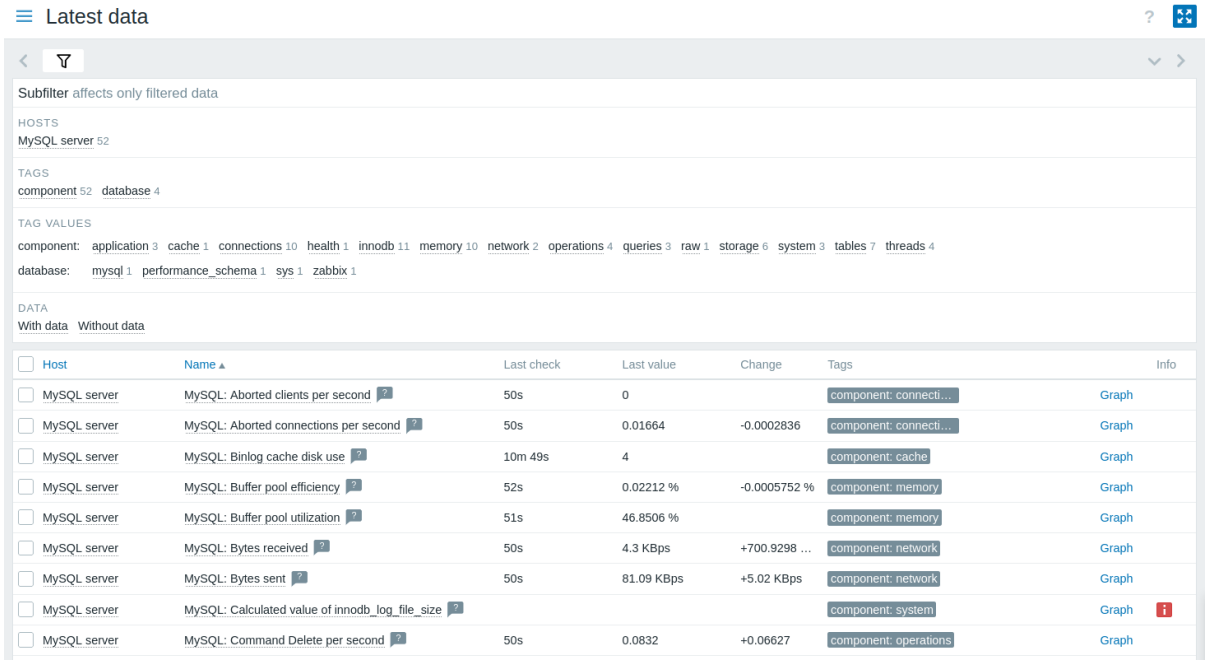
Aby wyświetlić zebrane metryki, przejdź do sekcji menu *Monitoring → Hosts* i kliknij *Dashboards* obok hosta.



Ta czynność przeniesie Cię do pulpitu hosta (skonfigurowanego na poziomie szablonu) z najważniejszymi metrykami zebranymi z serwera MySQL.



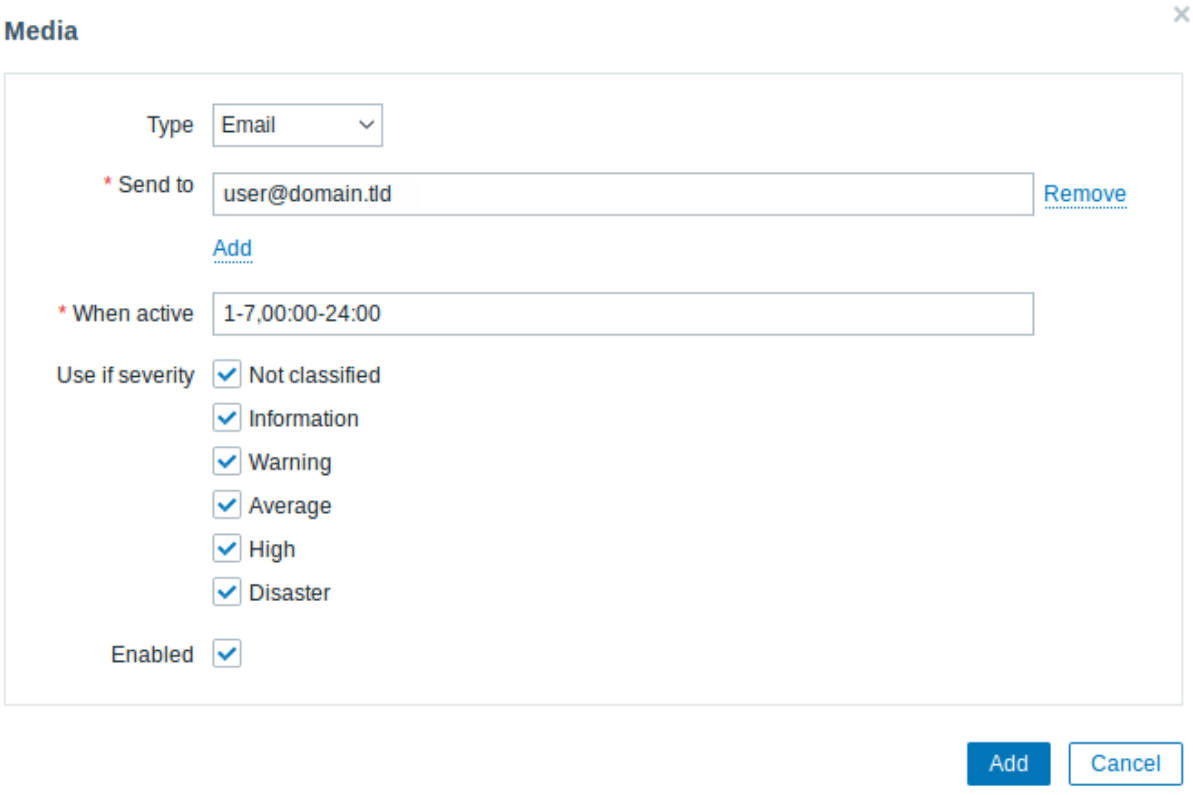
Alternatywnie, w sekcji menu *Monitoring → Hosts* możesz kliknąć *Latest data*, aby wyświetlić wszystkie najnowsze zebrane metryki w formie listy. Zwróć uwagę, że pozycja *MySQL: Calculated value of innodb_log_file_size* zgodnie z oczekiwaniami nie będzie miała danych, ponieważ wartość zostanie obliczona na podstawie danych z ostatniej godziny.



Skonfiguruj alerty o problemach

Zabbix może powiadamiać Cię o problemach z infrastrukturą na wiele sposobów. Ten przewodnik przedstawia podstawowe kroki konfiguracji wysyłania alertów e-mail.

1. Przejdź do *Ustawienia użytkownika → Profil*, przejdź do zakładki *Media* i dodaj swój adres e-mail.



2. Postępuj zgodnie z przewodnikiem Otrzymywanie powiadomienia o problemie.

Następnym razem, gdy Zabbix wykryje problem, powinieneś otrzymać alert e-mail.

Przetestuj swoją konfigurację

Aby przetestować swoją konfigurację, możemy zasymulować rzeczywisty problem, aktualizując konfigurację hosta w Zabbix frontend.

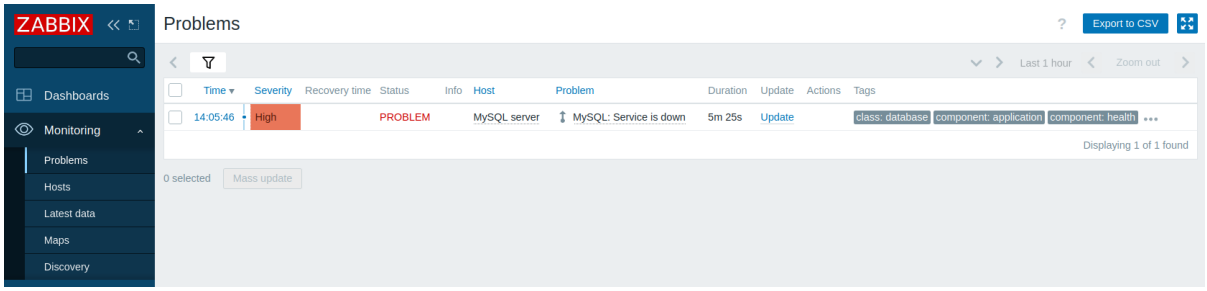
1. Otwórz konfigurację swojego hosta serwera MySQL w Zabbix.

2. Przejdź do zakładki *Macros* i wybierz *Inherited and host macros*.

3. Kliknij *Change* obok, na przykład, wcześniej skonfigurowanej wartości makra {$MYSQL.USER} i ustaw inną nazwę użytkownika MySQL.

4. Kliknij *Update*, aby zaktualizować konfigurację hosta.

5. Za kilka chwil Zabbix wykryje problem „MySQL: Service is down", ponieważ nie będzie mógł połączyć się z serwerem MySQL. Problem pojawi się w *Monitoring → Problems*.



Jeśli alerty są skonfigurowane, otrzymasz również powiadomienie o problemie.

6. Zmień wartość makra z powrotem na poprzednią, aby rozwiązać problem i kontynuować monitorowanie serwera MySQL.

Inne podejścia do monitorowania MySQL

Zamiast monitorować serwer MySQL za pomocą Zabbix agent 2, można również użyć Zabbix agent lub standardu Open Database Connectivity (ODBC). Chociaż zalecane jest używanie Zabbix agent 2, mogą istnieć środowiska, które nie obsługują Zabbix agent 2 lub wymagają niestandardowego podejścia.

Kluczowa różnica między Zabbix agent a ODBC polega na metodzie zbierania danych — Zabbix agent jest instalowany bezpośrednio na serwerze MySQL i zbiera dane przy użyciu wbudowanej funkcjonalności, natomiast ODBC opiera się na sterowniku ODBC, aby nawiązać połączenie z serwerem MySQL i pobierać dane za pomocą zapytań SQL.

Chociaż wiele kroków konfiguracji jest podobnych do monitorowania serwera MySQL za pomocą Zabbix agent 2, istnieją pewne istotne różnice — należy skonfigurować Zabbix agent lub ODBC, aby możliwe było monitorowanie serwera MySQL. Poniższe instrukcje przeprowadzą Cię przez te **różnice**.

Monitorowanie MySQL za pomocą agent Zabbix

Aby monitorować serwer MySQL za pomocą agent Zabbix, należy pobrać i zainstalować serwer Zabbix, frontend Zabbix oraz agent Zabbix zgodnie z instrukcjami dla używanego systemu operacyjnego.

Po pomyślnym zainstalowaniu wymaganych komponentów Zabbix należy utworzyć użytkownika MySQL zgodnie z opisem w sekcji *Tworzenie użytkownika MySQL*.

Po utworzeniu użytkownika MySQL należy skonfigurować agent Zabbix tak, aby mógł nawiązać połączenie z serwerem MySQL i go monitorować. Obejmuje to skonfigurowanie wielu parametrów użytkownika do wykonywania niestandardowych kontroli agent, a także dostarczenie agent Zabbix niezbędnych poświadczeń do łączenia się z serwerem MySQL jako wcześniej utworzony użytkownik „zbx_monitor".

Skonfiguruj agent Zabbix

1. Przejdź do katalogu dodatkowych konfiguracji agenta Zabbix.

```
cd /usr/local/etc/zabbix/zabbix_agentd.d
```

> **Attention:**
> Katalog dodatkowych konfiguracji agenta Zabbix powinien znajdować się w tym samym katalogu co plik konfiguracji agenta Zabbix (*zabbix_agentd.conf*). W zależności od systemu operacyjnego i instalacji Zabbix ten katalog może znajdować się w innej lokalizacji niż podano w tym przewodniku. Domyślne lokalizacje można sprawdzić w parametrze `Include` w pliku konfiguracji agenta Zabbix.

Zamiast definiować wszystkie niezbędne parametry użytkownika do monitorowania serwera MySQL w pliku konfiguracji agenta Zabbix, parametry te zostaną zdefiniowane w osobnym pliku w katalogu dodatkowych konfiguracji.

2. Utwórz plik *template_db_mysql.conf* w katalogu dodatkowych konfiguracji agenta Zabbix.

```
vi template_db_mysql.conf
```

3. Skopiuj zawartość pliku *template_db_mysql.conf* (znajdującego się w repozytorium Zabbix) do utworzonego pliku *template_db_mysql.conf* i zapisz zmiany.

4. Uruchom ponownie agent Zabbix, aby zaktualizować jego konfigurację.

```
systemctl restart zabbix-agent
```

Po skonfigurowaniu parametrów użytkownika agenta Zabbix możesz przejść do konfiguracji poświadczeń, które umożliwią agentowi Zabbix dostęp do serwera MySQL.

5. Przejdź do katalogu domowego agenta Zabbix (jeśli nie istnieje w systemie, należy go utworzyć; domyślnie: */var/lib/zabbix*).

```
cd /var/lib/zabbix
```

6. Utwórz plik *.my.cnf* w katalogu domowym agenta Zabbix.

```
vi .my.cnf
```

7. Skopiuj poniższą zawartość do pliku *.my.cnf* (zastąp *<password>* hasłem użytkownika „zbx_monitor”).

```
[client]
user='zbx_monitor'
password='<password>'
```

Skonfiguruj frontend Zabbix i przetestuj swoją konfigurację

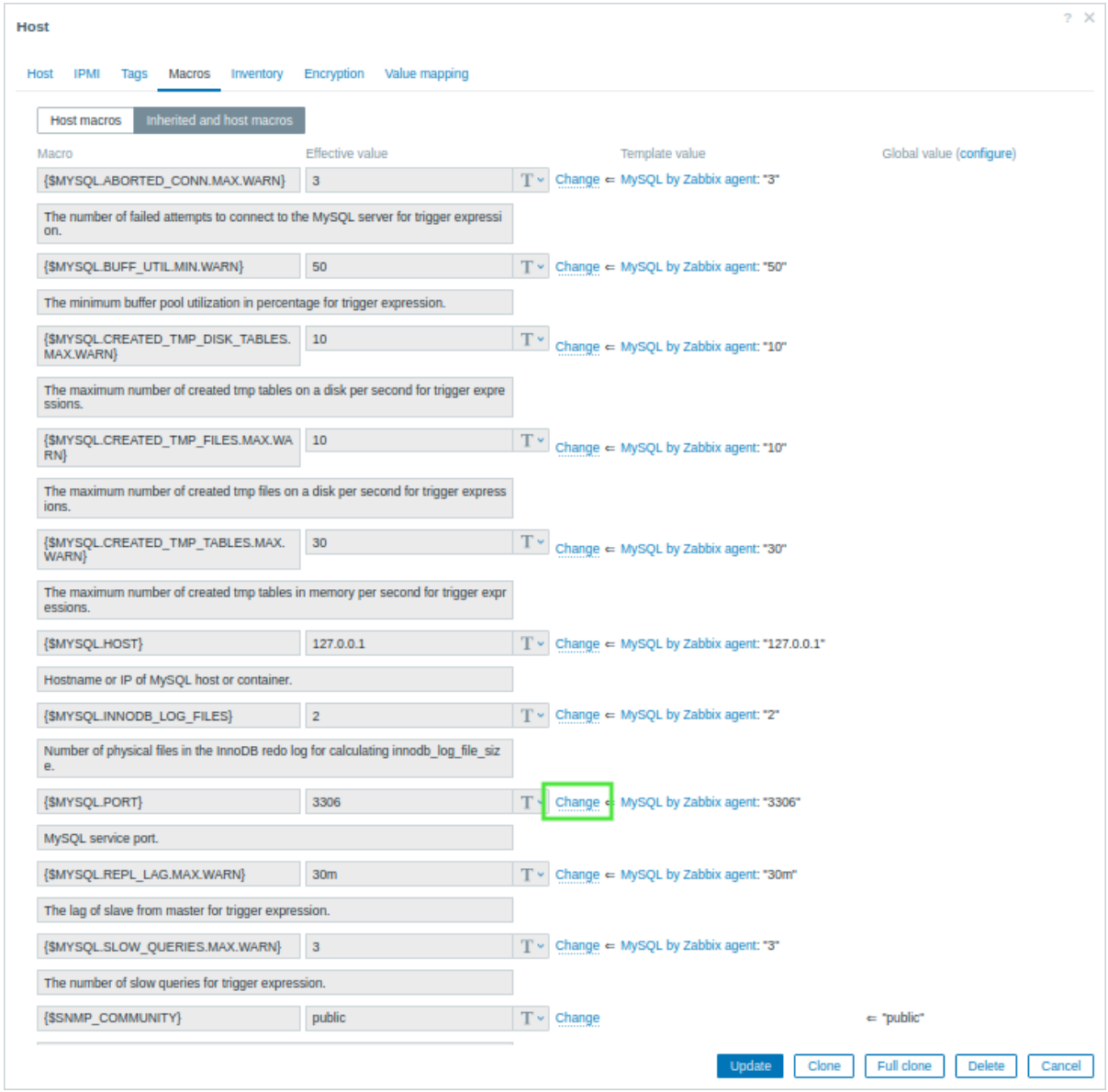
Aby skonfigurować frontend Zabbix, postępuj zgodnie z instrukcjami w sekcji *Skonfiguruj frontend Zabbix*, wprowadzając następujące zmiany:

- W polu *Templates* wpisz lub wybierz szablon „MySQL by Zabbix agent”, który zostanie podlinkowany do hosta.
- Konfiguracja *Macros* nie jest wymagana.

Po skonfigurowaniu frontendu Zabbix możesz wyświetlić zebrane metryki i skonfigurować alerty problemów.

Aby przetestować swoją konfigurację, postępuj zgodnie z instrukcjami w sekcji *Przetestuj swoją konfigurację*, wprowadzając następujące zmiany:

- W sekcji *Inherited and host macros* konfiguracji hosta serwera MySQL kliknij *Change* obok wartości makra {$MYSQL.PORT} i ustaw inny port (np. „6033”).



Monitorowanie MySQL za pomocą ODBC

Aby monitorować serwer MySQL za pomocą ODBC, należy pobrać i zainstalować serwer Zabbix oraz frontend Zabbix.

Po pomyślnym zainstalowaniu wymaganych komponentów Zabbix należy utworzyć użytkownika MySQL zgodnie z opisem w sekcji *Tworzenie użytkownika MySQL*.

Po utworzeniu użytkownika MySQL należy skonfigurować ODBC. Obejmuje to instalację jednej z najczęściej używanych implementacji API ODBC typu open source — unixODBC — oraz sterownika unixODBC, a także edycję pliku konfiguracyjnego sterownika ODBC.

Konfiguracja ODBC

1. Zainstaluj unixODBC. Zalecanym sposobem instalacji unixODBC jest użycie domyślnych repozytoriów pakietów systemu operacyjnego Linux.

```
apt install unixodbc
```

2. Zainstaluj sterownik bazy danych MariaDB unixODBC. Mimo że używasz bazy danych MySQL, sterownik MariaDB unixODBC jest używany ze względu na kwestie kompatybilności.

```
apt install odbc-mariadb
```

3. Sprawdź lokalizację plików konfiguracyjnych ODBC *odbcinst.ini* i *odbc.ini*.

```
odbcinst -j
```

Wynik wykonania tego polecenia powinien być podobny do poniższego.

```
unixODBC 2.3.9
DRIVERS............: /etc/odbcinst.ini
```

```
SYSTEM DATA SOURCES: /etc/odbc.ini
FILE DATA SOURCES..: /etc/ODBCDataSources
...
```

4. Aby skonfigurować sterownik ODBC do monitorowania bazy danych MySQL, potrzebujesz nazwy sterownika, która znajduje się w pliku *odbcinst.ini*. W poniższym przykładzie pliku *odbcinst.ini* nazwa sterownika to "MariaDB Unicode".

```
[MariaDB Unicode]
Driver=libmaodbc.so
Description=MariaDB Connector/ODBC(Unicode)
Threading=0
UsageCount=1
```

5. Skopiuj poniższą zawartość do pliku *odbc.ini* (zastąp <*password*> hasłem użytkownika "zbx_monitor"). Ten przewodnik używa adresu "127.0.0.1" (localhost) jako adresu serwera MySQL do monitorowania serwera MySQL zainstalowanego na tej samej maszynie co sterownik ODBC. Zwróć uwagę na nazwę źródła danych (DSN) "test", która będzie wymagana podczas konfiguracji frontend Zabbix.

```
[test]
Driver=MariaDB Unicode
Server=127.0.0.1
User=zbx_monitor
Password=<password>
Port=3306
Database=zabbix
```

Skonfiguruj frontend Zabbix i przetestuj swoją konfigurację

Aby skonfigurować frontend Zabbix, postępuj zgodnie z instrukcjami w sekcji *Skonfiguruj frontend Zabbix*, wprowadzając następujące zmiany:

- W polu *Templates* wpisz lub wybierz szablon „MySQL by ODBC", który zostanie podłączony do hosta.
- Konfigurowanie *Interfaces* nie jest wymagane.
- Wartość makra {$MYSQL.DSN} w sekcji *Inherited and host macros* konfiguracji hosta serwera MySQL powinna być ustawiona na nazwę DSN z pliku *odbc.ini*.

Po skonfigurowaniu frontend Zabbix możesz wyświetlić zebrane metryki, skonfigurować alerty problemów oraz przetestować swoją konfigurację.

Zobacz także

- Tworzenie pozycji — jak rozpocząć monitorowanie dodatkowych metryk.
- Eskalacje problemów — jak tworzyć wieloetapowe scenariusze alertów (np. najpierw wysłać wiadomość do administratora systemu, a następnie, jeśli problem nie zostanie rozwiązany w ciągu 45 minut, wysłać wiadomość do kierownika centrum danych).
- Monitorowanie ODBC — jak skonfigurować ODBC w innych dystrybucjach Linuksa oraz jak rozpocząć monitorowanie dodatkowych metryk związanych z bazą danych za pomocą ODBC.
- Szablon *MySQL by Zabbix agent* — dodatkowe informacje o szablonie *MySQL by Zabbix agent*.
- Szablon *MySQL by Zabbix agent 2* — dodatkowe informacje o szablonie *MySQL by Zabbix agent 2*.
- Szablon *MySQL by ODBC* — dodatkowe informacje o szablonie *MySQL by ODBC*.

5 Monitoruj VMware za pomocą Zabbix

Wprowadzenie

Ta strona przeprowadzi Cię przez kroki wymagane by rozpocząć podstawowe monitorowanie VMware.

Dla kogo jest ten przewodnik

Ten przewodnik jest przeznaczony dla nowych użytkowników Zabbix i zawiera minimalny zestaw kroków wymaganych do włączenia podstawowego monitorowania VMware. Jeśli szukasz opcji zaawansowanego dostosowania lub potrzebujesz bardziej zaawansowanej konfiguracji, zobacz sekcję Monitorowanie maszyn wirtualnych lub sekcję Konfiguracja w podręczniku Zabbix.

Wymagania wstępne

Przed kontynuowaniem tego przewodnika należy pobrać i zainstalować serwer Zabbix oraz frontend Zabbix zgodnie z instrukcjami dla używanego systemu operacyjnego.

W zależności od środowiska niektóre kroki w tym przewodniku mogą się nieznacznie różnić. Ten przewodnik opiera się na środowisku działającym pod kontrolą Ubuntu.

Zakłada się, że VMware jest już skonfigurowane. Ten przewodnik nie obejmuje konfiguracji VMware.

Konfiguracja serwera Zabbix

Aby monitorować VMware, należy włączyć procesy Zabbix *vmware collector*. Więcej informacji o sposobie działania monitorowania VMware można znaleźć w sekcji Monitorowanie maszyn wirtualnych.

1. Otwórz plik konfiguracyjny serwera Zabbix.

```
vi /etc/zabbix/zabbix_server.conf
```

2. Odszukaj parametr `StartVMwareCollectors` w pliku konfiguracyjnym serwera Zabbix i ustaw go na 2 lub więcej (wartość domyślna to 0).

```
##### Option: StartVMwareCollectors
###       Number of pre-forked vmware collector instances.
###
### Mandatory: no
### Range: 0-250
### Default:
### StartVMwareCollectors=0

StartVMwareCollectors=2
```

3. Uruchom ponownie serwer Zabbix.

```
systemctl restart zabbix-server
```

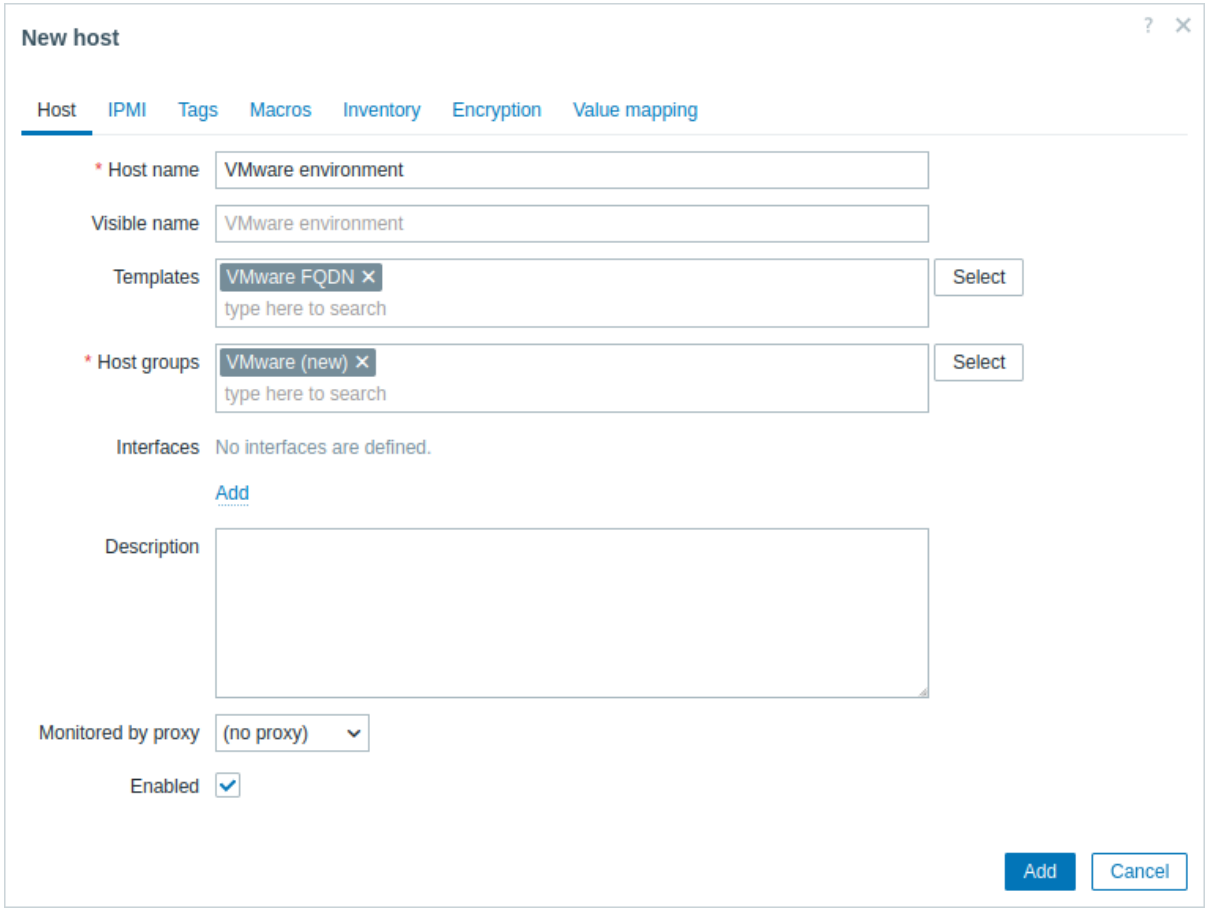
Po uruchomieniu procesów *vmware collector* przejdź do następnego kroku.

Konfiguracja frontendu Zabbix

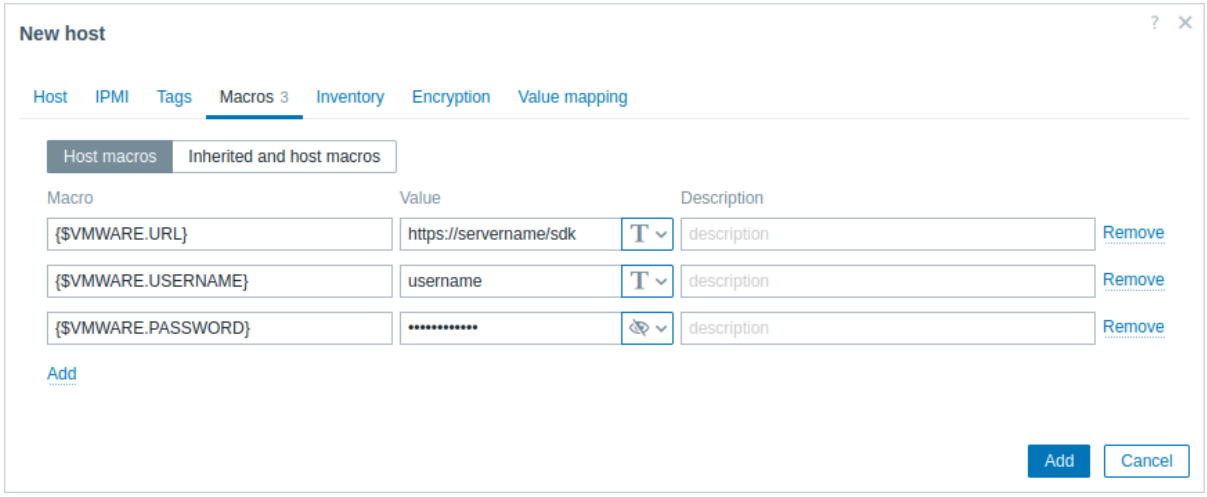
1. Zaloguj się do frontendu Zabbix.

2. Utwórz host w interfejsie webowym Zabbix:

- W polu *Host name* wprowadź nazwę hosta (na przykład „VMware environment”).
- W polu *Templates* wpisz lub wybierz szablon „VMware FQDN” (lub „VMware”). Więcej informacji o tych szablonach znajdziesz w sekcji Monitorowanie maszyn wirtualnych.
- W polu *Host groups* wpisz lub wybierz grupę hostów (na przykład nową grupę hostów „VMware”).



- Na karcie *Macros* ustaw następujące makra hosta:
  - {$VMWARE.URL} — URL SDK usługi VMware (vCenter lub hiperwizora ESXi) (https://servername/sdk)
  - {$VMWARE.USERNAME} — nazwa użytkownika usługi VMware
  - {$VMWARE.PASSWORD} — hasło użytkownika {$VMWARE.USERNAME} usługi VMware



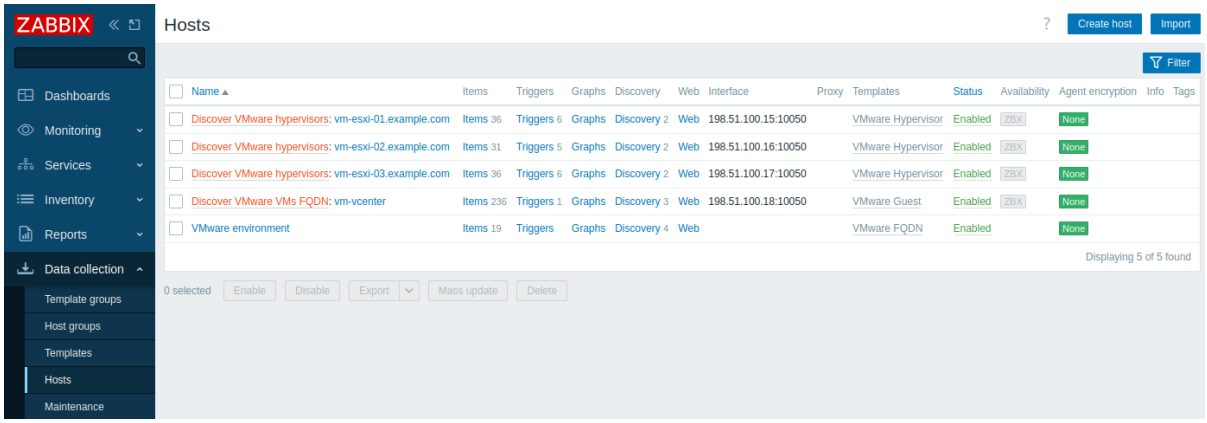
3. Kliknij przycisk *Add*, aby utworzyć host. Ten host będzie reprezentował Twoje środowisko VMware.

Wyświetlanie zebranych metryk

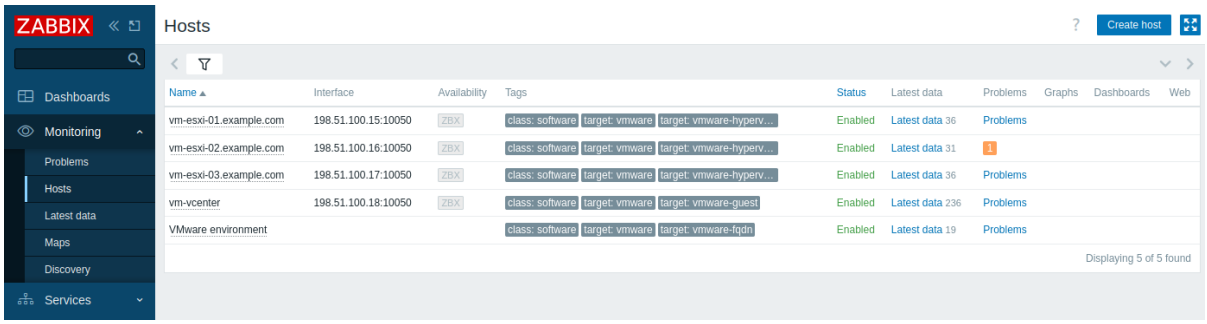
Gratulacje! Na tym etapie Zabbix już monitoruje Twoje środowisko VMware.

W zależności od konfiguracji środowiska VMware, Zabbix może wykryć, a następnie utworzyć hosty dla wykrytych encji. Pamiętaj, że wykrywanie i tworzenie hostów może również zostać wykonane ręcznie, jeśli to konieczne.

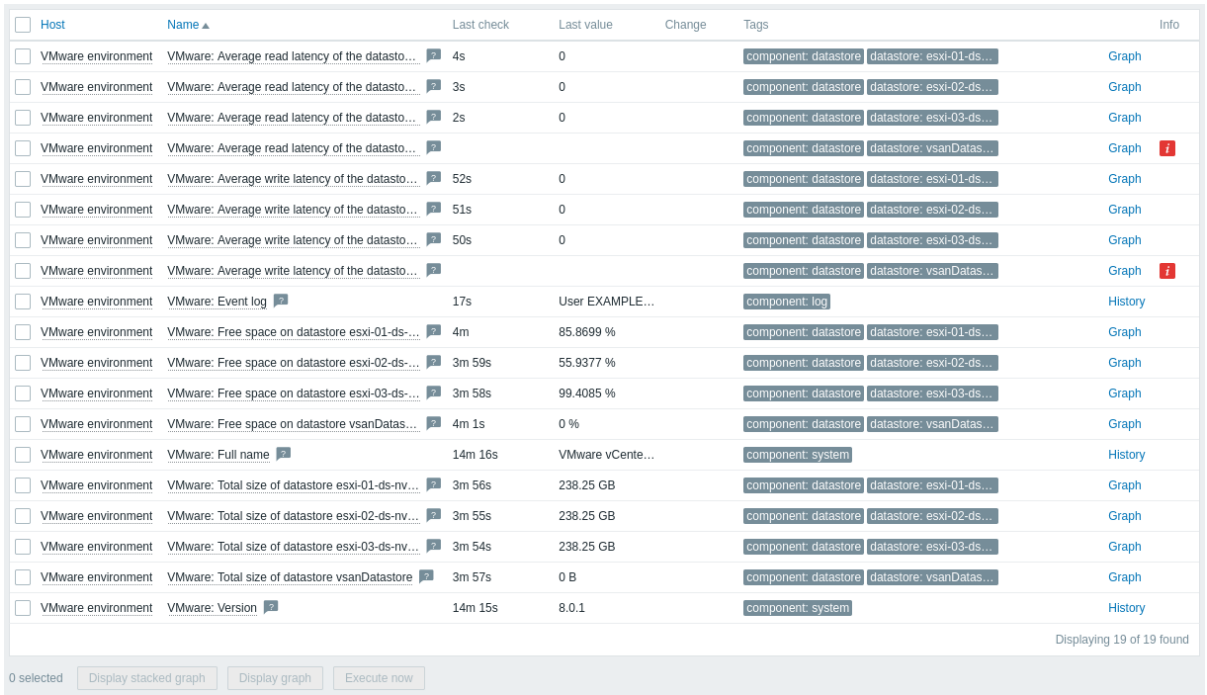
Aby wyświetlić utworzone hosty, przejdź do sekcji menu *Data collection → Hosts*.



Aby wyświetlić zebrane metryki, przejdź do sekcji menu *Monitoring → Hosts* i kliknij *Latest data* obok utworzonego hosta „VMware environment" lub jednego z hostów utworzonych dla wykrytych encji.



Ta czynność otworzy listę wszystkich najnowszych metryk zebranych z wybranego hosta.

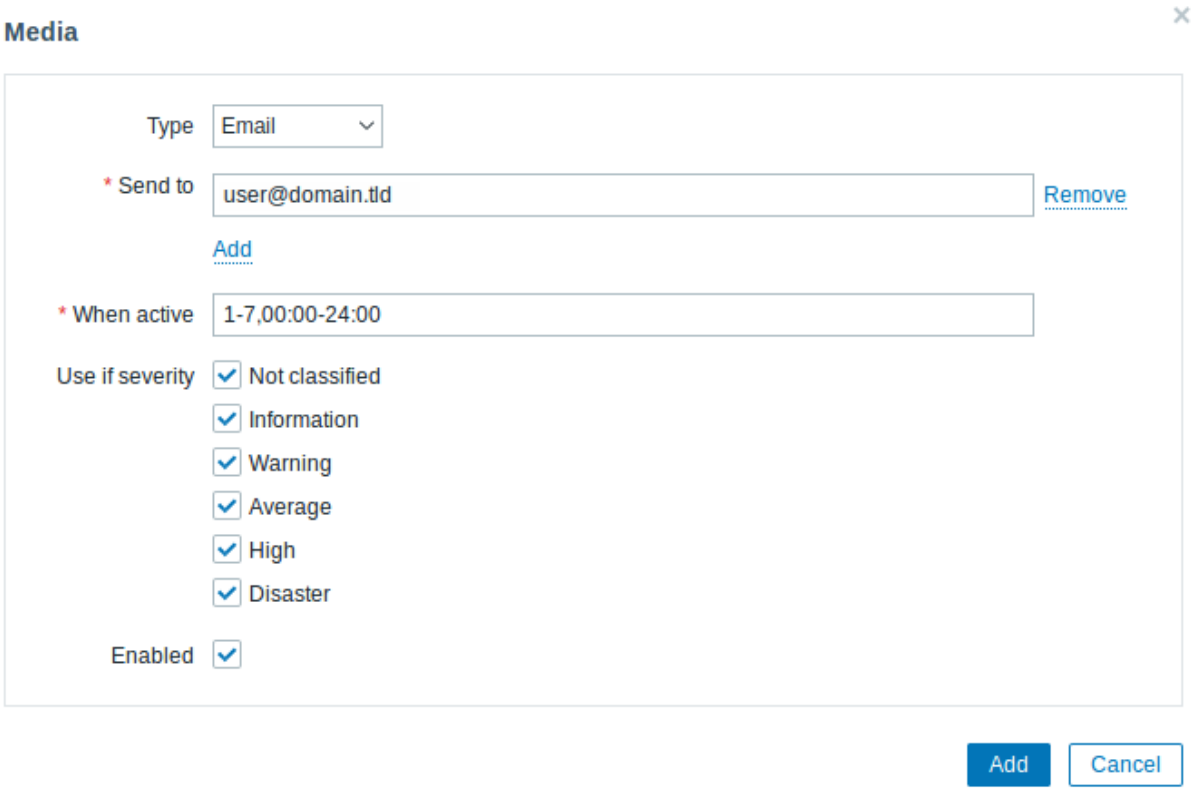


Pamiętaj, że niektóre pozycje nie mają danych i mają stan *Not supported*. Dzieje się tak, ponieważ Zabbix nie może znaleźć prawidłowych liczników wydajności w określonym magazynie danych, ponieważ nie są one włączone w monitorowanym środowisku VMware.

Skonfiguruj alerty o problemach

Zabbix może powiadamiać Cię o problemach z infrastrukturą za pomocą różnych metod. Ten przewodnik przedstawia podstawowe kroki konfiguracji wysyłania alertów e-mail.

1. Przejdź do *Ustawienia użytkownika → Profil*, przełącz się na kartę *Media* i dodaj swój adres e-mail.



2. Postępuj zgodnie z przewodnikiem Otrzymywanie powiadomienia o problemie.

Następnym razem, gdy Zabbix wykryje problem, powinieneś otrzymać alert e-mail.

Zobacz także

- Tworzenie pozycji — jak rozpocząć monitorowanie dodatkowych metryk.
- Eskalacje problemów — jak tworzyć wieloetapowe scenariusze alertów (np. najpierw wysłać wiadomość do administratora systemu, a następnie, jeśli problem nie zostanie rozwiązany w ciągu 45 minut, wysłać wiadomość do kierownika centrum danych).
- Monitorowanie maszyn wirtualnych — dodatkowe informacje o monitorowaniu VMware (proces zbierania danych, opcje konfiguracji serwera, wskazówki dotyczące rozwiązywania problemów itp.).
- Klucze pozycji monitorowania VMware — pełna lista metryk VMware, które można monitorować za pomocą Zabbix.
- Szablon *VMware* — dodatkowe informacje o szablonie *VMware*.
- Szablon *VMware FQDN* — dodatkowe informacje o szablonie *VMware FQDN*.

6 Monitoruj ruch sieciowy za pomocą Zabbix

Wprowadzenie Ta strona przeprowadzi Cię przez kroki wymagane do rozpoczęcia podstawowego monitorowania ruchu sieciowego za pomocą Zabbix.

Dla kogo jest ten przewodnik

Ten przewodnik jest przeznaczony dla nowych użytkowników Zabbix i zawiera minimalny zestaw kroków wymaganych do włączenia podstawowego monitorowania ruchu sieciowego. Jeśli szukasz opcji zaawansowanego dostosowywania lub potrzebujesz bardziej zaawansowanej konfiguracji, zobacz sekcję Konfiguracja podręcznika Zabbix.

Wymagania wstępne

Przed kontynuowaniem tego przewodnika należy pobrać i zainstalować Zabbix serwer, Zabbix frontend oraz Zabbix agent zgodnie z instrukcjami dla używanego systemu operacyjnego. Należy pamiętać, że Zabbix agent powinien zostać zainstalowany na maszynie, która wymaga monitorowania ruchu sieciowego. Może to być ten sam host, na którym zainstalowany jest Zabbix serwer, lub inny host.

Ten przewodnik zawiera instrukcje dotyczące konfiguracji monitorowania ruchu sieciowego interfejsu *eth0* na oddzielnej maszynie o nazwie *Remote host*.

Konfiguracja Zabbix do monitorowania Agent Zabbix może zbierać metryki w trybie aktywnym lub pasywnym (jednocześnie). Więcej informacji można znaleźć w sekcji Pasywne i aktywne kontrole agenta. W tym przewodniku zostanie opisane monitorowanie za pomocą kontroli pasywnych.

Konfigurowanie agenta Zabbix

1. Otwórz plik konfiguracyjny agenta na maszynie, na której agent jest zainstalowany (domyślnie ścieżka to */usr/local/etc/zabbix_agentd.conf*):

```
sudo vi /usr/local/etc/zabbix_agentd.conf
```

2. Dodaj adres IP lub nazwę DNS swojego serwera Zabbix do parametru *Server*. Na przykład:

```
Server=192.0.2.22
```

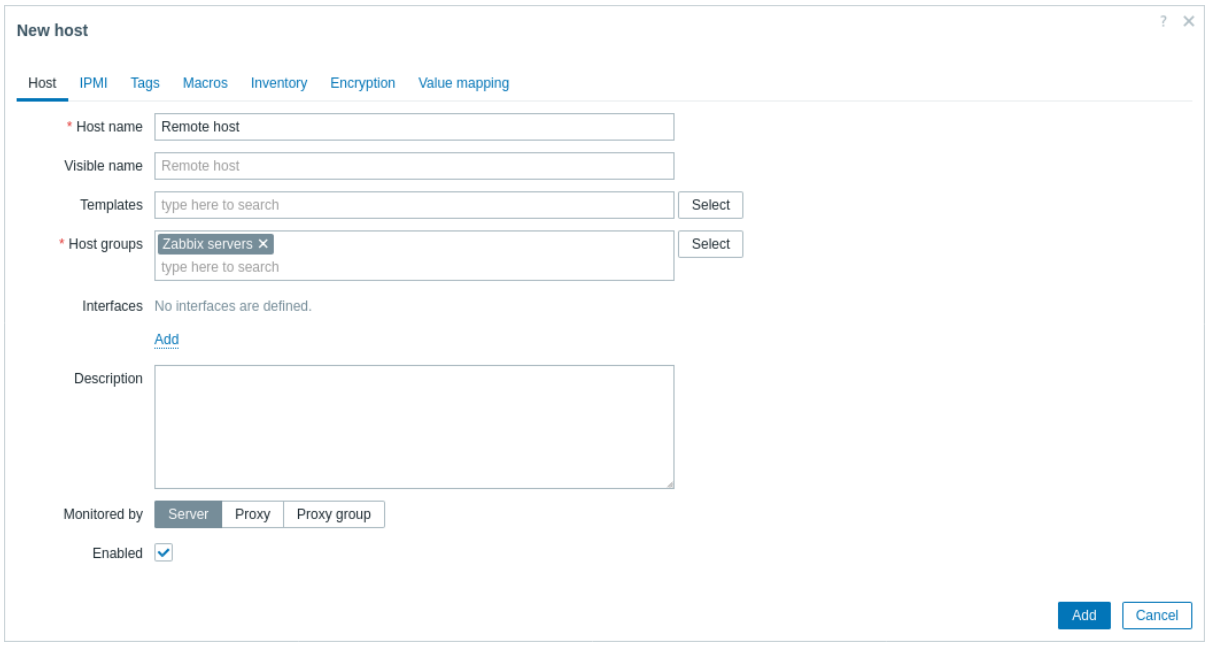
3. Uruchom ponownie agenta Zabbix:

```
systemctl restart zabbix-agent
```

Frontend Zabbix

1. Zaloguj się do frontend Zabbix.

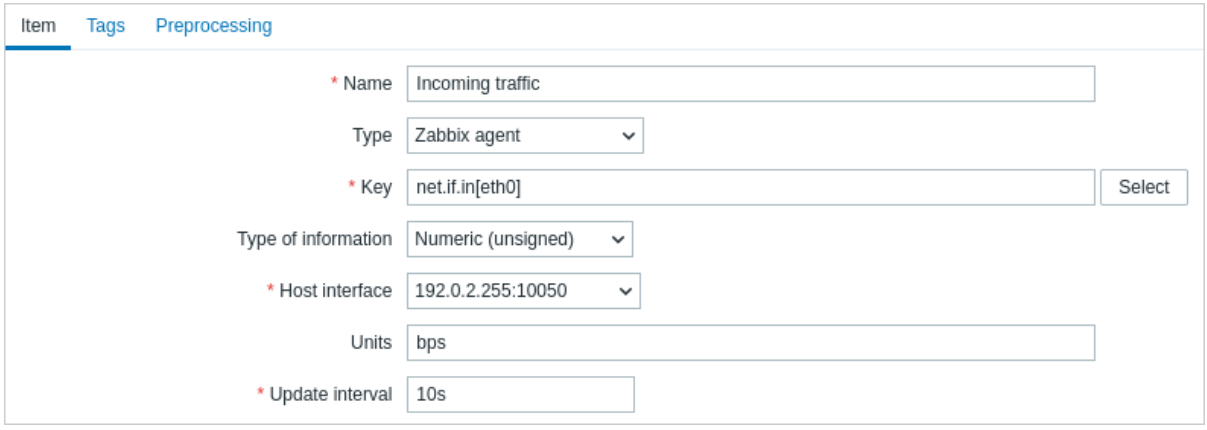
2. Utwórz hosta w interfejsie webowym Zabbix, podając adres IP lub nazwę DNS komputera, na którym zainstalowano agent.



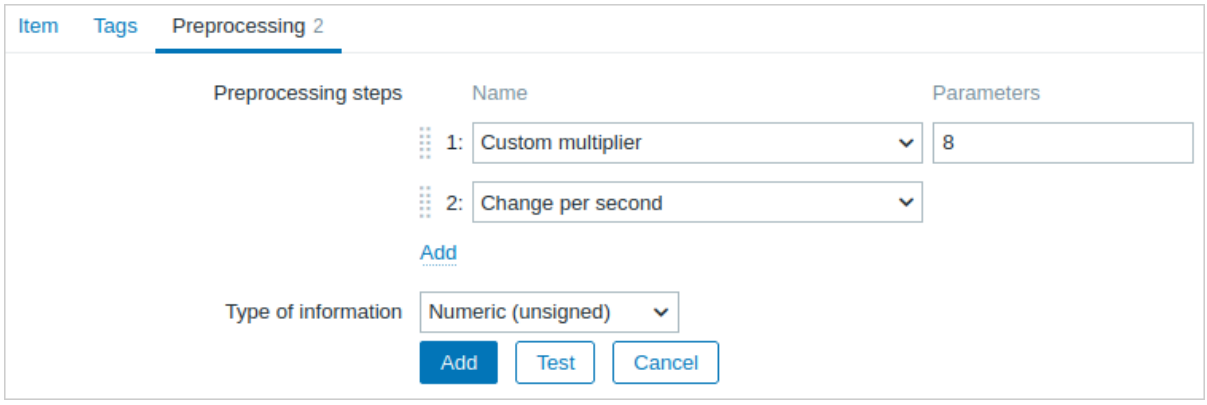
Tworzenie pozycji Postępuj zgodnie z instrukcjami dotyczącymi tworzenia pozycji, aby dodać pozycje do monitorowania ruchu, a mianowicie:

- Ruch przychodzący
- Ruch wychodzący
- Całkowity ruch

Prosta konfiguracja pozycji monitorującej ruch przychodzący będzie wyglądać następująco:

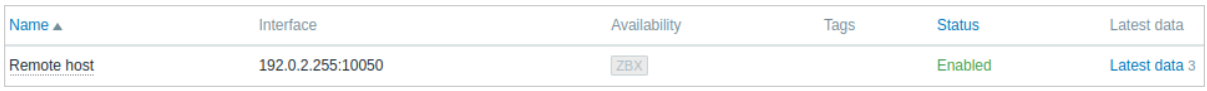


Aby zebrane dane nadawały się do praktycznego wykorzystania, podczas tworzenia pozycji możesz skonfigurować kilka kroków przetwarzania wstępnego. W tym przypadku mogą to być mnożenie przez 8 (aby przeliczyć bajty na bity) oraz prezentacja jako zmiana na sekundę.

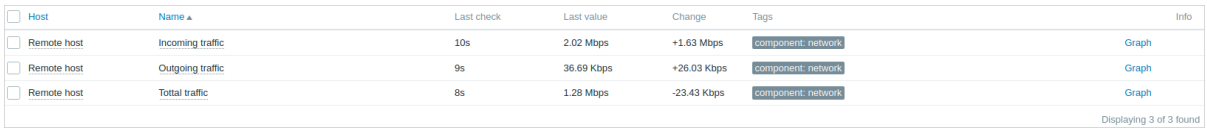


Wyświetlanie zebranych danych Gratulacje! Na tym etapie Zabbix już monitoruje ruch w Twojej sieci.

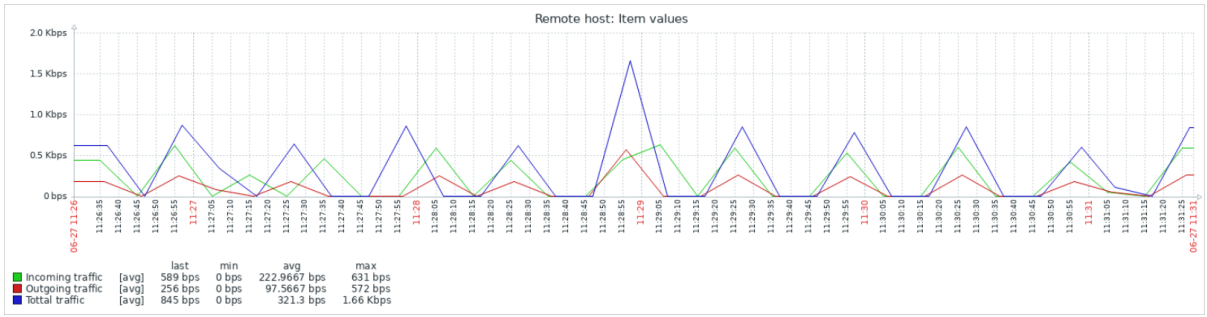
Aby wyświetlić zebrane metryki, otwórz sekcję menu *Monitoring → Hosts* i kliknij *Latest data* w wierszu hosta.



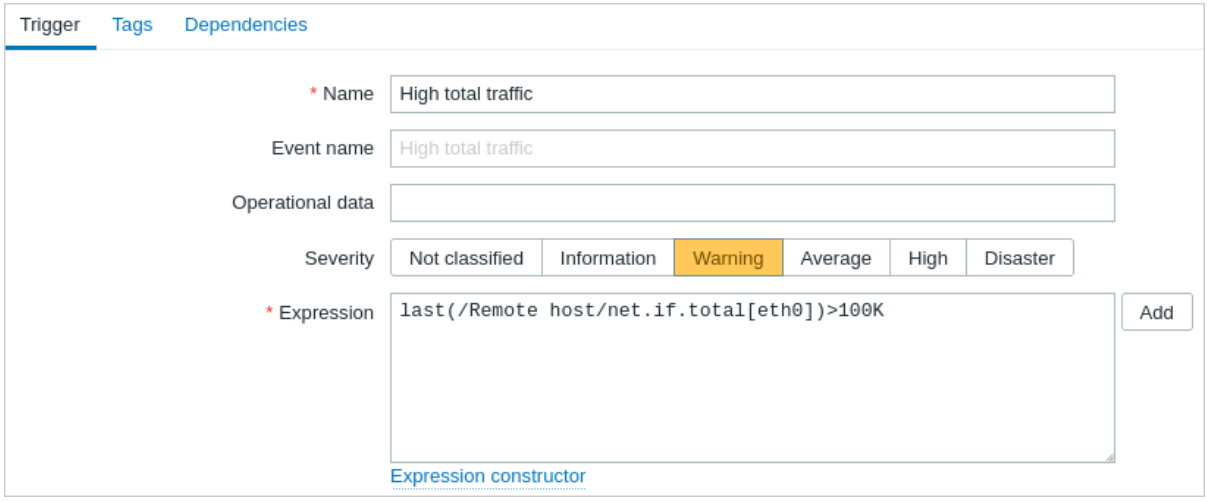
Zobaczysz dane o ruchu.



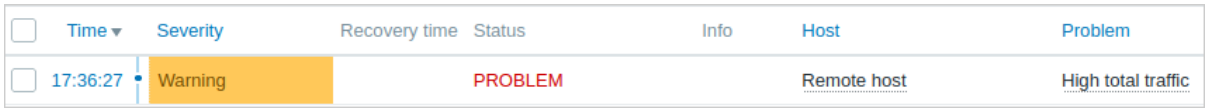
Wyświetlanie wykresów Zebrane dane mogą być wyświetlane jako wykresy. Aby je wyświetlić, w sekcji *Najnowsze dane* kliknij *Wykres* w wierszu danej pozycji lub wybierz wymagane pozycje i kliknij *Wyświetl wykres* poniżej.



Konfiguracja wyzwalaczy Możesz skonfigurować wyzwalacze, aby wykrywać nieprawidłowy ruch sieciowy. Zapoznaj się z instrukcjami dotyczącymi konfigurowania wyzwalacza i dodaj wyzwalacz sygnalizujący, że całkowity ruch jest zbyt wysoki, na przykład:



Teraz spraw, aby ruch przekroczył próg ustawiony w wyrażeniu wyzwalacza, a następnie przejdź do *Monitoring* → *Problems*, aby sprawdzić, czy problem jest tam wyświetlany.



Konfiguracja alertów o problemach Istnieje kilka sposobów otrzymywania powiadomień o problemie. Najpopularniejszym z nich jest e-mail, dlatego postępuj zgodnie z instrukcjami konfiguracji powiadomienia o problemie przez e-mail. Możesz także wybrać inne typy mediów, które będą używane do dostarczania powiadomień.

Zobacz także:

- Eskalacje problemów — jak tworzyć wieloetapowe scenariusze alertów (np. najpierw wysłać wiadomość do administratora systemu, a następnie, jeśli problem nie zostanie rozwiązany w ciągu 45 minut, wysłać wiadomość do kierownika centrum danych).
- Potwierdzanie problemów — jak wskazać, że problem jest znany, dodawać komentarze dotyczące jego rozwiązywania, tłumić lub zamykać problem.
- Monitorowanie systemu Linux za pomocą agent Zabbix — jak rozpocząć podstawowe monitorowanie najważniejszych pozycji przez podłączenie wstępnie skonfigurowanego szablon.

7 Monitoruj ruch sieciowy za pomocą aktywnych kontroli

Wprowadzenie Ta strona przeprowadzi Cię przez kroki wymagane do rozpoczęcia podstawowego monitorowania ruchu sieciowego za pomocą Zabbix z użyciem aktywnych kontroli.

Dla kogo jest ten przewodnik

Ten przewodnik jest przeznaczony dla nowych użytkowników Zabbix i zawiera minimalny zestaw kroków wymaganych do włączenia podstawowego monitorowania ruchu sieciowego przy użyciu aktywnych kontroli. Jeśli szukasz opcji zaawansowanego dostosowywania lub potrzebujesz bardziej zaawansowanej konfiguracji, zobacz sekcję Configuration podręcznika Zabbix.

Wymagania wstępne

Przed kontynuowaniem tego przewodnika należy pobrać i zainstalować serwer Zabbix, frontend Zabbix oraz agent Zabbix zgodnie z instrukcjami dla używanego systemu operacyjnego. Należy pamiętać, że agent Zabbix powinien zostać zainstalowany na maszynie, która wymaga monitorowania ruchu sieciowego. Może to być ten sam host, na którym zainstalowany jest serwer Zabbix, lub inny host.

Ten przewodnik zawiera instrukcje dotyczące konfiguracji monitorowania ruchu sieciowego interfejsu *eth0* na oddzielnej maszynie o nazwie *Remote host*.

Konfiguracja Zabbix do monitorowania Agent Zabbix może zbierać metryki w trybie aktywnym lub pasywnym (jednocześnie). Więcej informacji można znaleźć w sekcji Pasywne i aktywne kontrole agenta. W tym przewodniku zostanie opisane monitorowanie za pomocą **aktywnych kontroli**.

Konfigurowanie agenta Zabbix

1. Otwórz plik konfiguracyjny agenta na maszynie, na której agent jest zainstalowany.

Jeśli używasz Zabbix agent:

```
sudo vi /etc/zabbix/zabbix_agentd.conf
```

Jeśli używasz Zabbix agent 2:

```
sudo vi /etc/zabbix/zabbix_agent2.conf
```

2. Dodaj adres IP lub nazwę DNS (oraz opcjonalny port) swojego serwera Zabbix do parametru ServerActive. Na przykład:

```
ServerActive=192.0.2.0:10051
```

Agent Zabbix użyje tego adresu do połączenia z portem trappera serwera Zabbix (domyślnie: 10051) i zażądania danych konfiguracyjnych dla aktywnych kontroli.

3. Zdefiniuj parametr Hostname, który musi odpowiadać nazwie hosta zdefiniowanej w frontendzie Zabbix. W naszym przykładzie jest to:

```
Hostname=Remote host
```

Wartość Hostname musi się zgadzać, ponieważ w przypadku aktywnych kontroli agent Zabbix używa jej do pobrania z serwera poprawnej konfiguracji hosta. Dokładniej mówiąc, agent inicjuje połączenie z serwerem i identyfikuje się za pomocą wartości Hostname. Następnie serwer dostarcza konfigurację monitorowania dla tego hosta. Jeśli te wartości będą się różnić, agent nie otrzyma odpowiedniej konfiguracji, co spowoduje brak metryk lub problemy z monitorowaniem.

4. Uruchom ponownie agenta Zabbix.

Jeśli używasz Zabbix agent:

```
systemctl restart zabbix-agent
```

Jeśli używasz Zabbix agent 2:

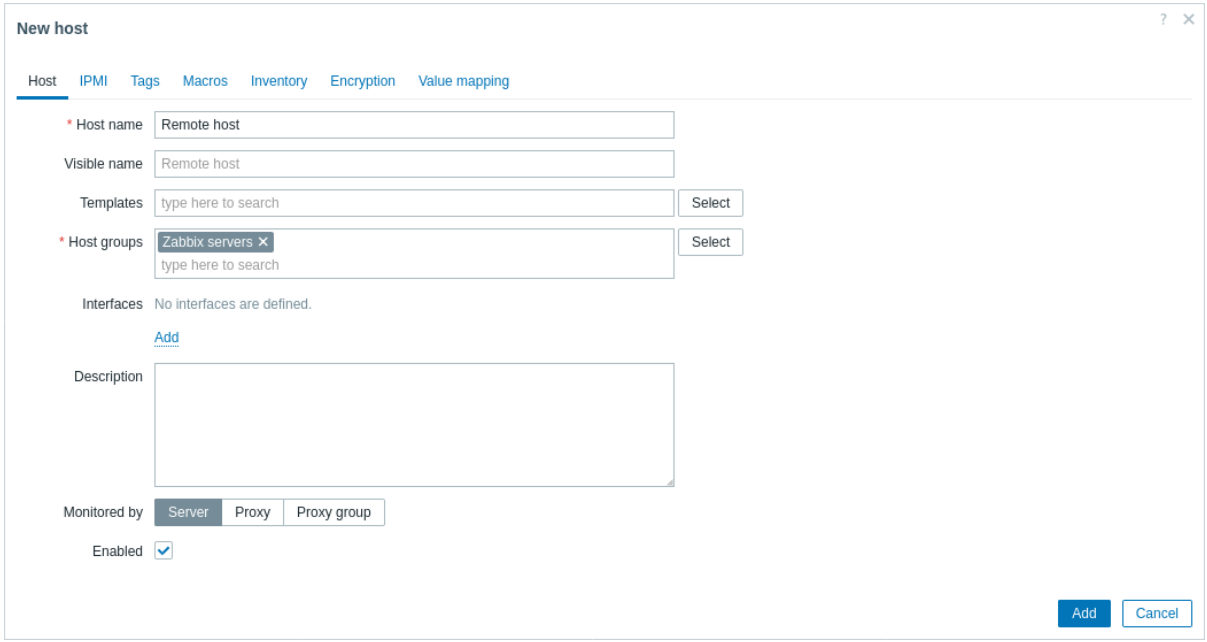
```
systemctl restart zabbix-agent2
```

Zabbix frontend

1. Zaloguj się do Zabbix frontend.

2. Utwórz host w interfejsie webowym Zabbix.

- W polu *Host name* wprowadź nazwę hosta (np. „Remote host”), która odpowiada wartości parametru Hostname zdefiniowanej wcześniej w pliku konfiguracyjnym agent.
- W polu *Host groups* wpisz lub wybierz grupę hostów (np. „Zabbix servers”).
- Pozostaw *Interfaces* niezdefiniowane; interfejs nie jest wymagany dla aktywnych testów, ponieważ agent inicjuje połączenie z serwerem, zamiast nasłuchiwać połączenia od serwera.

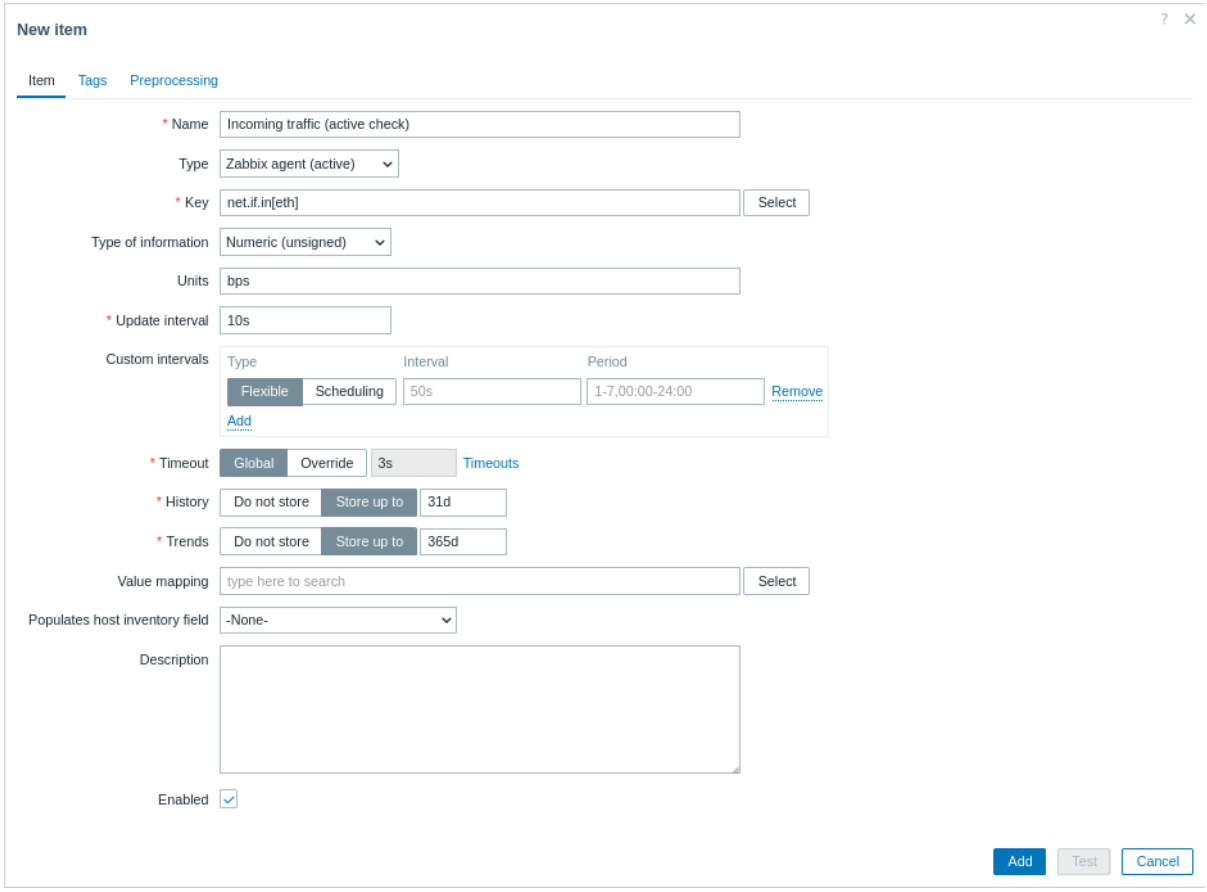


3. Kliknij *Add*, aby dodać hosta. Ten host będzie reprezentował monitorowaną maszynę z systemem Linux.

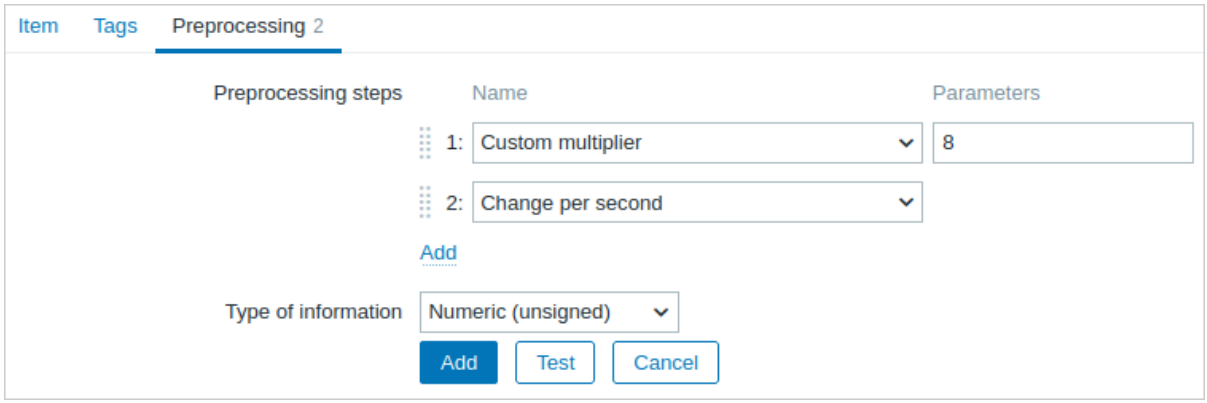
Tworzenie pozycji Postępuj zgodnie z instrukcjami dotyczącymi tworzenia pozycji, aby dodać pozycje do monitorowania ruchu, a mianowicie:

- Ruch przychodzący
- Ruch wychodzący
- Całkowity ruch

Prosta konfiguracja pozycji monitorowania ruchu przychodzącego z aktywnym sprawdzaniem wyglądałaby następująco:

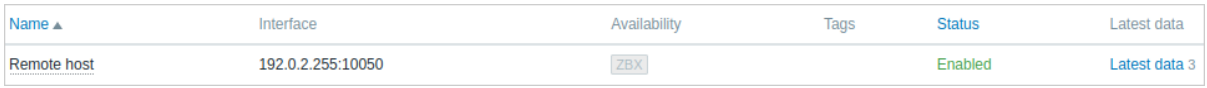


Aby zebrane dane nadawały się do praktycznego wykorzystania, podczas tworzenia pozycji można ustawić kilka kroków przetwarzania wstępnego. W podanym przypadku może to być mnożenie przez 8 (aby przeliczyć bajty na bity) oraz prezentacja jako zmiana na sekundę.

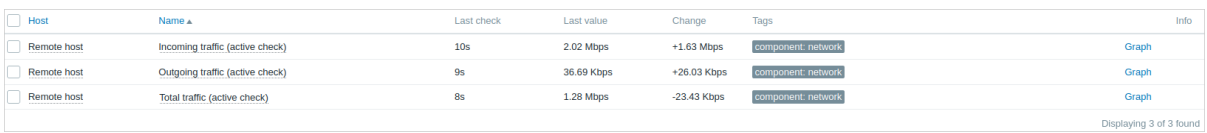


Wyświetlanie zebranych danych Gratulacje! Na tym etapie Zabbix monitoruje już ruch sieciowy.

Aby wyświetlić zebrane metryki, otwórz sekcję menu *Monitoring → Hosts* i kliknij *Latest data* w wierszu hosta.



Zobaczysz dane dotyczące ruchu.



Zobacz także:

- Wyświetlanie wykresów - jak wyświetlać zebrane dane w postaci wykresów.
- Konfigurowanie wyzwalaczy - jak skonfigurować wyzwalacze do wykrywania nietypowego ruchu sieciowego.
- Konfigurowanie alertów o problemach - jak skonfigurować powiadomienia o sytuacjach problemowych.

- Eskalacje problemów - jak tworzyć wieloetapowe scenariusze alertów (np. najpierw wysłać wiadomość do administratora systemu, a następnie, jeśli problem nie zostanie rozwiązany w ciągu 45 minut, wysłać wiadomość do kierownika centrum danych).
- Potwierdzanie problemów - jak wskazać, że problem jest znany, dodawać komentarze dotyczące jego rozwiązania, tłumić lub zamykać problem.
- Monitorowanie systemu Linux za pomocą Zabbix agent - jak rozpocząć podstawowe monitorowanie najważniejszych pozycji przez podłączenie wstępnie skonfigurowanego szablonu.
- Instalacja z pakietów - jak zainstalować komponenty Zabbix przy użyciu oficjalnych pakietów RPM i DEB dla różnych dystrybucji Linuksa, zapewniając dostęp do najnowszych funkcji i poprawek błędów.

8 Monitorowanie stron internetowych za pomocą pozycji przeglądarki

Wprowadzenie

Ta strona przeprowadzi Cię przez kroki wymagane do rozpoczęcia podstawowego monitorowania stron internetowych za pomocą pozycji przeglądarkowych.

Dla kogo jest ten przewodnik

Ten przewodnik jest przeznaczony dla nowych użytkowników Zabbix i zawiera minimalny zestaw kroków wymaganych do włączenia podstawowego monitorowania stron internetowych za pomocą pozycji przeglądarkowych. Jeśli szukasz opcji zaawansowanego dostosowania lub potrzebujesz bardziej zaawansowanej konfiguracji, zobacz stronę Pozycje przeglądarkowe lub sekcję Konfiguracja podręcznika Zabbix.

Wymagania wstępne

Przed kontynuowaniem tego przewodnika należy pobrać i zainstalować serwer Zabbix oraz frontend Zabbix zgodnie z instrukcjami dla używanego systemu operacyjnego.

W zależności od środowiska niektóre kroki w tym przewodniku mogą się nieznacznie różnić. Ten przewodnik opiera się na środowisku działającym pod kontrolą Ubuntu.

Konfiguracja WebDriver

Pozycje przeglądarki wymagają frameworka automatyzacji (Selenium Server lub zwykłego WebDriver, na przykład ChromeDriver) jako punktu końcowego testów web, który steruje przeglądarką i wchodzi z nią w interakcję, wykonując polecenia testowe, takie jak klikanie przycisków lub wprowadzanie tekstu. W tym przewodniku jako przykład zostanie użyty Selenium Server z Chrome w kontenerze Docker.

Zakłada się, że Docker jest już skonfigurowany. Ten przewodnik nie obejmuje konfiguracji Dockera. Instrukcje instalacji można znaleźć tutaj: Install Docker Engine on Ubuntu.

1. Uruchom Selenium Server z Chrome w kontenerze Docker z następującymi opcjami:

- **docker run --name browser** — uruchamia nowy kontener Docker o nazwie „browser”;
- **-p 4444:4444** — mapuje port 4444 na twoim hoście na port 4444 w kontenerze (jest to port używany przez Selenium Server do przyjmowania poleceń);
- **-p 7900:7900** — mapuje port 7900 na twoim hoście na port 7900 w kontenerze (jest to port używany przez serwer Virtual Network Computing (VNC), umożliwiający zdalne wyświetlanie GUI przeglądarki; wymaga klienta VNC);
- **--shm-size=”2g”** — przydziela kontenerowi 2 GB pamięci współdzielonej (jest to ważne dla prawidłowego działania Chrome, ponieważ może on wymagać znacznej ilości pamięci współdzielonej, aby uniknąć awarii);
- **-d** — uruchamia kontener w trybie odłączonym, co oznacza, że będzie działał w tle;
- **selenium/standalone-chrome:latest** — określa obraz Docker do użycia; w tym przypadku jest to najnowsza wersja Selenium Server with Chrome.

```
docker run --name browser \
-p 4444:4444 \
-p 7900:7900 \
--shm-size="2g" \
-d selenium/standalone-chrome:latest
```

2. Upewnij się, że kontener Docker `browser` działa i jest dostępny.

- Pobierz adres IP kontenera (w tym przykładzie 192.0.2.1):

```
ip addr

### 1: lo: <LOOPBACK,UP,LOWER_UP>
```

```
###     ...
### 3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> ...
###     inet 192.0.2.1/16 brd 192.0.255.255 scope global docker0
###     ...
```

- Przetestuj połączenie z kontenerem za pomocą Ncat:

```
nc -zv 192.0.2.1 4444

### Connection to 192.0.2.1 4444 port [tcp/*] succeeded!
```

- Pobierz zawartość strony internetowej z Selenium Server za pomocą curl:

```
curl -L 192.0.2.1:4444

### <!DOCTYPE html>
### <html lang="en">
###
### <head>
###   <meta charset="utf-8"/>
###   <link href="favicon.svg" rel="icon" type="image/svg">
###   <meta content="width=device-width, initial-scale=1" name="viewport"/>
###   <link href="logo192.png" rel="apple-touch-icon"/>
###   <link href="manifest.json" rel="manifest"/>
###   <title>Selenium Grid</title>
### </head>
###
### <body>
### ...
```

Note:
W celu rozwiązywania problemów zapoznaj się z Docker documentation.

Skonfiguruj serwer Zabbix

Pozycje przeglądarki są wykonywane i przetwarzane przez procesy Zabbix *browser poller*, które należy włączyć, dostosowując parametr konfiguracji serwera StartBrowserPollers. Dodatkowo parametr WebDriverURL powinien wskazywać wcześniej skonfigurowany endpoint testów webowych.

Domyślnie parametr StartBrowserPollers jest ustawiony na 1, dlatego wystarczy określić endpoint testów webowych.

1. Otwórz plik konfiguracyjny serwera Zabbix.

```
vi /etc/zabbix/zabbix_server.conf
```

2. Odszukaj i ustaw parametr WebDriverURL w pliku konfiguracyjnym serwera Zabbix:

```
##### Option: WebDriverURL
###WebDriver interface HTTP[S] URL. For example http://localhost:4444 used with Selenium WebDriver standal
###
### Mandatory: no
### Default:
### WebDriverURL=

WebDriverURL=192.0.2.1:4444
```

3. Uruchom ponownie serwer Zabbix.

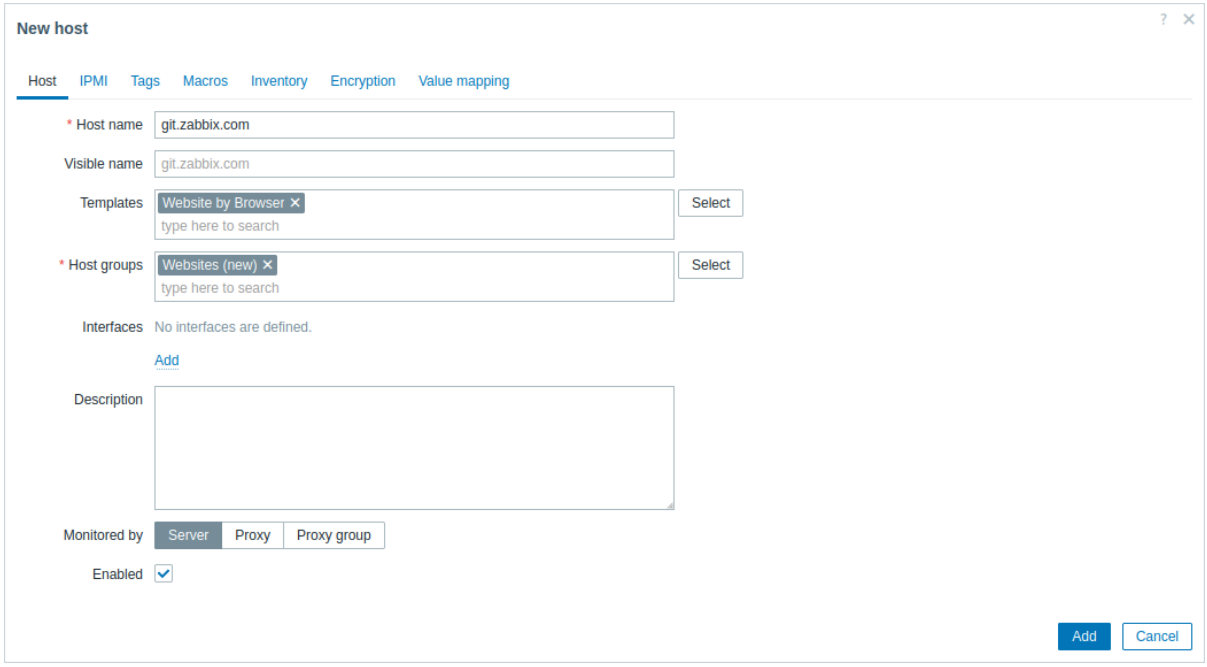
```
systemctl restart zabbix-server
```

Konfiguracja frontendu Zabbix

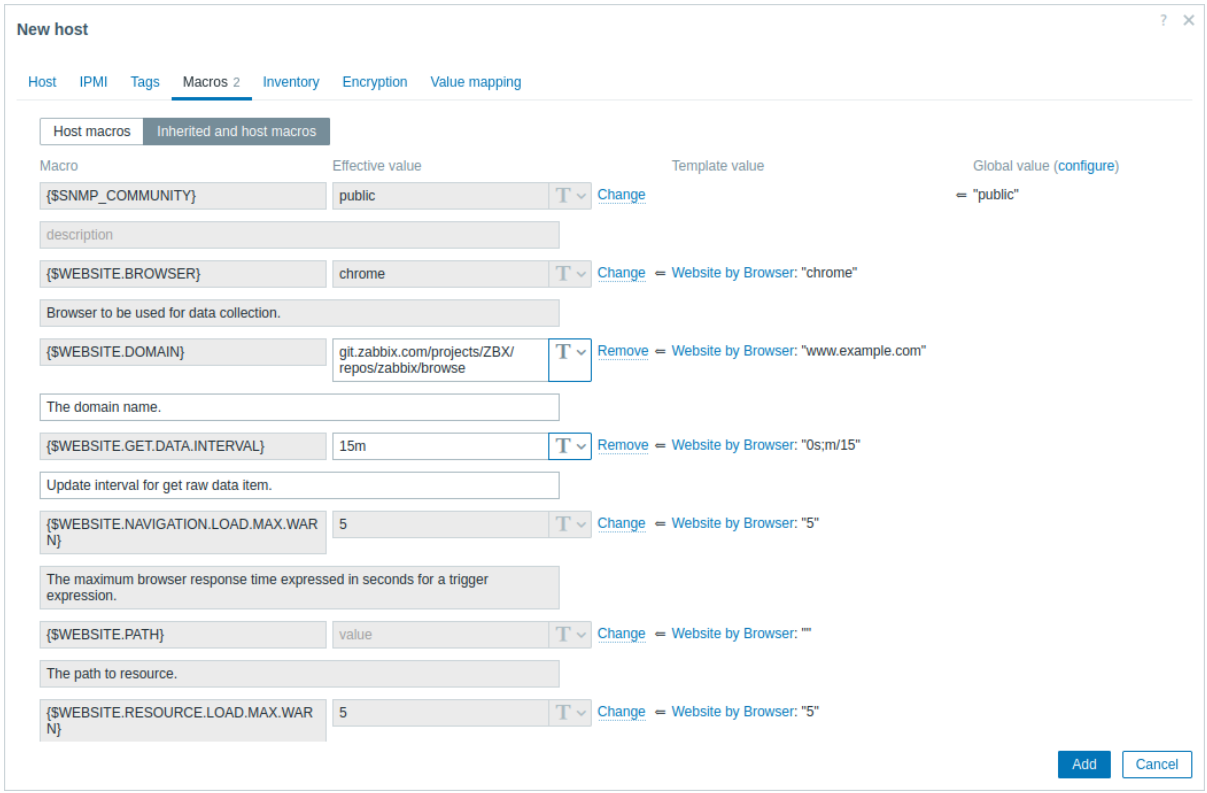
1. Zaloguj się do frontendu Zabbix.

2. Utwórz hosta w interfejsie webowym Zabbix:

- W polu *Host name* wprowadź nazwę hosta (na przykład „git.zabbix.com”).
- W polu *Templates* wpisz lub wybierz szablon „Website by Browser”. Więcej informacji o tym szablonie znajdziesz tutaj: Website by Browser.
- W polu *Host groups* wpisz lub wybierz grupę hostów (na przykład nową grupę hostów „Websites”).



- Na karcie *Macros* przełącz się na *Inherited and host macros*, odszukaj następujące makra i kliknij *Change* obok wartości makra, aby je zaktualizować:
  - {$WEBSITE.DOMAIN} - Nazwa domeny (na przykład git.zabbix.com/projects/ZBX/repos/zabbix/browse)
  - {$WEBSITE.GET.DATA.INTERVAL} - Interwał aktualizacji danych pozycji (na przykład 15m)

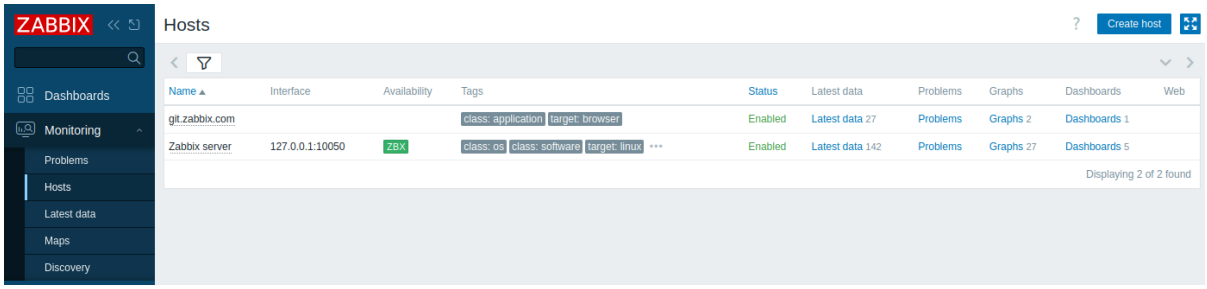


3. Kliknij przycisk *Add*, aby utworzyć hosta. Ten host będzie reprezentował witrynę internetową, którą chcesz monitorować.

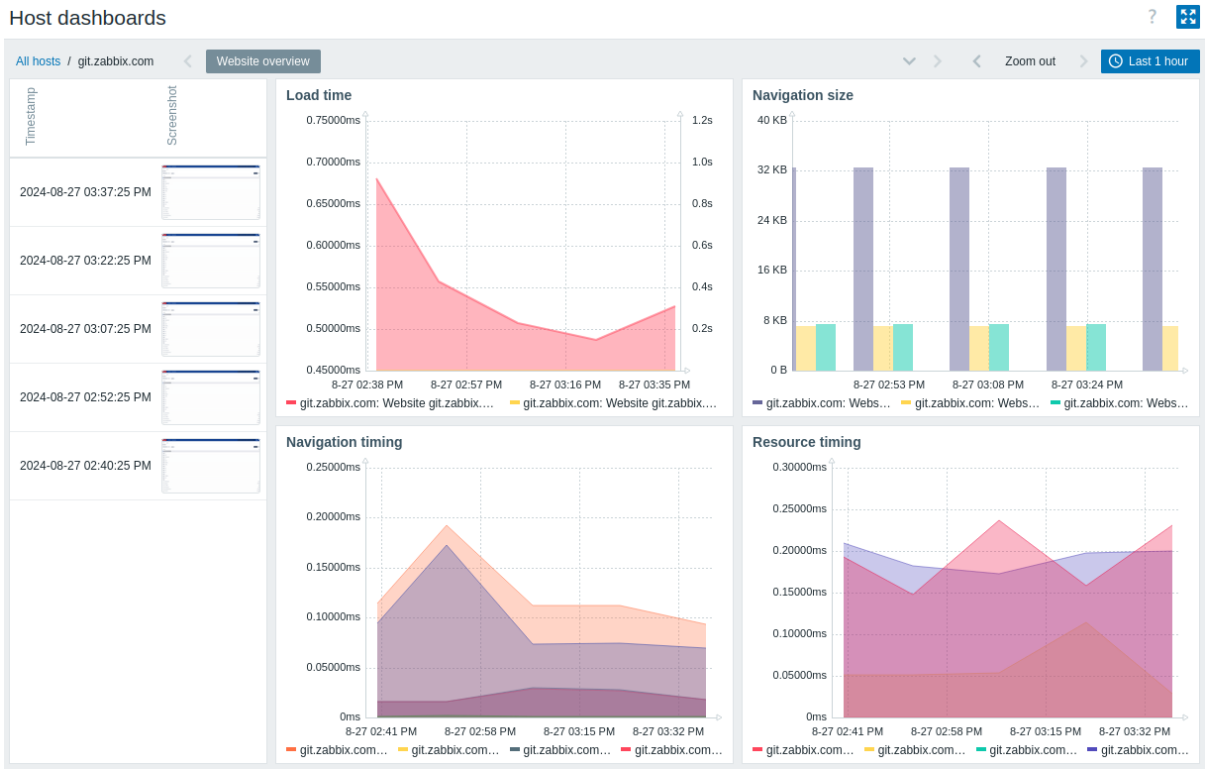
Wyświetlanie zebranych metryk

Gratulacje! Na tym etapie Zabbix monitoruje już wskazaną przez Ciebie witrynę internetową.

Aby wyświetlić zebrane metryki, przejdź do sekcji menu *Monitoring → Hosts* i kliknij *Dashboards* obok hosta.



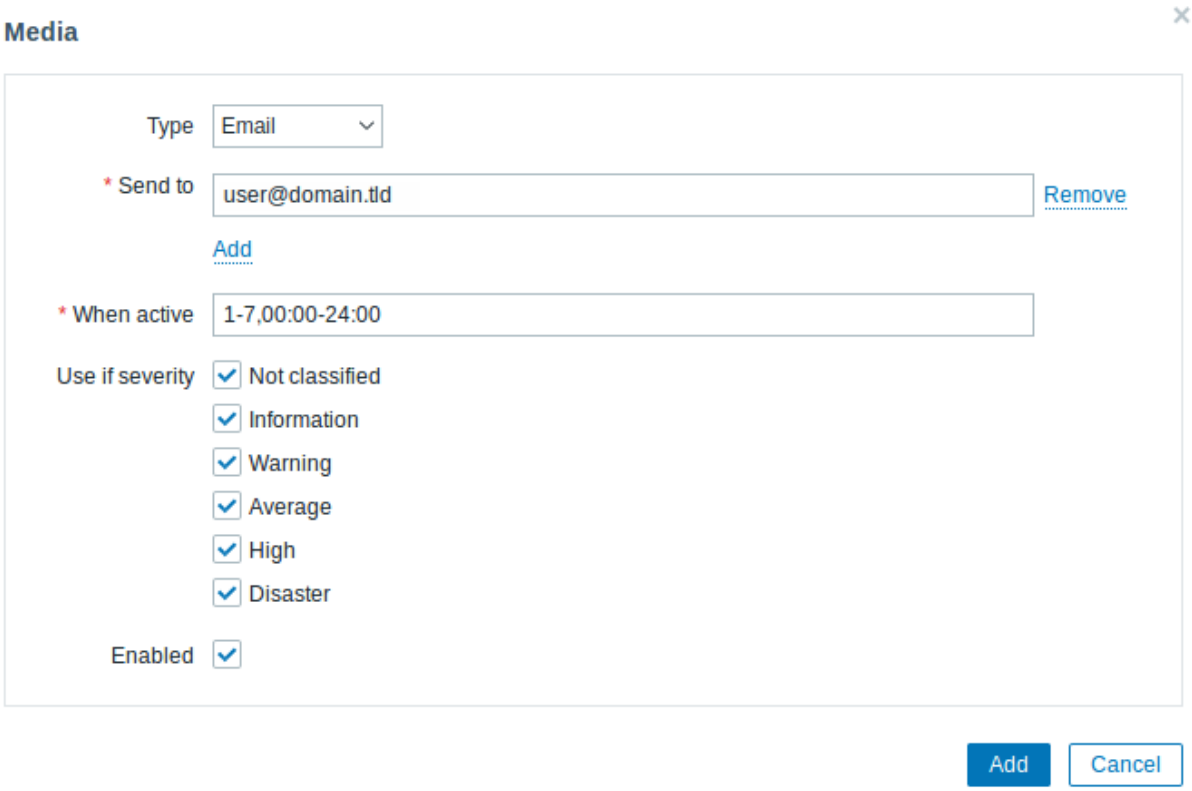
Ta czynność przeniesie Cię do pulpitu hosta (skonfigurowanego na poziomie szablonu) z najważniejszymi metrykami zebranymi z witryny internetowej.



Skonfiguruj alerty o problemach

Zabbix może powiadamiać Cię o problemach z infrastrukturą na wiele sposobów. Ten przewodnik przedstawia podstawowe kroki konfiguracji wysyłania alertów e-mail.

1. Przejdź do *Ustawienia użytkownika* → *Profil*, przejdź do zakładki *Media* i dodaj swój adres e-mail.



2. Postępuj zgodnie z przewodnikiem Otrzymywanie powiadomienia o problemie.

Następnym razem, gdy Zabbix wykryje problem, powinieneś otrzymać alert e-mail.

Przetestuj swoją konfigurację

Aby przetestować swoją konfigurację, możemy zasymulować rzeczywisty problem, aktualizując konfigurację hosta w Zabbix frontend.

1. Otwórz konfigurację hosta swojej witryny internetowej w Zabbix.

2. Przejdź do zakładki *Macros* i wybierz *Inherited and host macros*.

3. Kliknij *Change* obok, na przykład, wcześniej skonfigurowanej wartości makra {$WEBSITE.DOMAIN} i ustaw nieprawidłową nazwę domeny (na przykład /git.zabbix.com/projects/ZBX/repos/zabbix/browse).

4. Kliknij *Update*, aby zaktualizować konfigurację hosta.

5. Po chwili Zabbix wykryje problem „Failed to get JSON of the requested website", ponieważ nie będzie mógł połączyć się z określoną witryną internetową. Problem pojawi się w *Monitoring → Problems*.



Jeśli alerty są skonfigurowane, otrzymasz również powiadomienie o problemie.

6. Zmień wartość makra z powrotem na poprzednią, aby rozwiązać problem i kontynuować monitorowanie witryny internetowej.

Zobacz także

- Tworzenie pozycji - jak rozpocząć monitorowanie dodatkowych metryk.
- Eskalacje problemów - jak tworzyć wieloetapowe scenariusze alertów (np. najpierw wysłać wiadomość do administratora systemu, a następnie, jeśli problem nie zostanie rozwiązany w ciągu 45 minut, wysłać wiadomość do kierownika centrum danych).
- Pozycje przeglądarki - jak skonfigurować pozycje przeglądarki.
- Szablon Website by Browser - dodatkowe informacje o szablonie *Website by Browser*.

9 Monitorowanie certyfikatów stron internetowych za pomocą agent Zabbix 2 (pasywnie)

Wprowadzenie

Ten przewodnik zawiera kompleksowy przegląd sposobu konfiguracji i monitorowania certyfikatów SSL/TLS przy użyciu klucza `web.certificate.get` w Zabbix agent 2. Został opracowany, aby uprościć monitorowanie certyfikatów dla pojedynczych lub wielu witryn internetowych, zapewniając administratorom możliwość szybkiego identyfikowania potencjalnych problemów, takich jak wygasłe lub nieprawidłowe certyfikaty.

Dla kogo jest ten przewodnik

Ten przewodnik jest przeznaczony dla nowych użytkowników Zabbix i zawiera minimalny zestaw kroków wymaganych do włączenia podstawowego monitorowania certyfikatów stron internetowych. Jeśli szukasz opcji zaawansowanego dostosowywania lub potrzebujesz bardziej zaawansowanej konfiguracji, zobacz sekcję Configuration w podręczniku Zabbix.

Wymagania wstępne

Przed przystąpieniem do tego przewodnika należy pobrać i zainstalować serwer Zabbix, frontend Zabbix oraz agent Zabbix 2 zgodnie z instrukcjami dla używanego systemu operacyjnego. W tym samouczku założono, że zarówno serwer Zabbix, jak i agent są zainstalowane na tej samej maszynie; dlatego w konfiguracji użyto `127.0.0.1`.

Skonfiguruj Zabbix agent 2

1. Otwórz plik konfiguracyjny Zabbix agent (domyślna ścieżka: `/etc/zabbix/zabbix_agent2.conf`):

```
sudo vi /etc/zabbix/zabbix_agent2.conf
```

2. Ustaw parametr Server na 127.0.0.1, ponieważ agent i serwer działają na tej samej maszynie:

```
Server=127.0.0.1
```

3. Zapisz plik i uruchom ponownie usługę Zabbix agent 2:

```
sudo systemctl restart zabbix-agent2
```

4. Po zakończeniu instalacji i konfiguracji Zabbix agent 2 przetestuj jego dostępność za pomocą:

```
zabbix_get -s 127.0.0.1 -k web.certificate.get[<website_DNS_name>]
```

Zabbix agent 2 domyślnie zawiera wtyczkę WebCertificate, więc nie jest wymagana osobna instalacja ani konfiguracja.

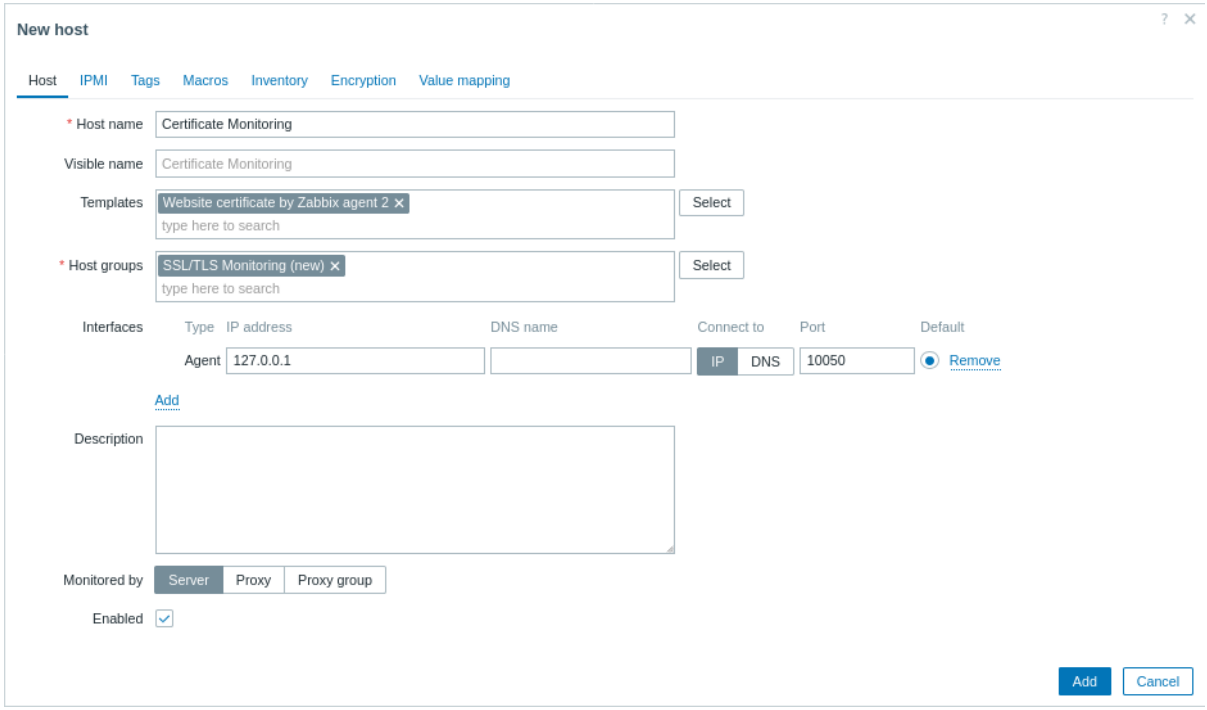
Konfiguracja frontendu Zabbix

1. Zaloguj się do frontendu Zabbix.

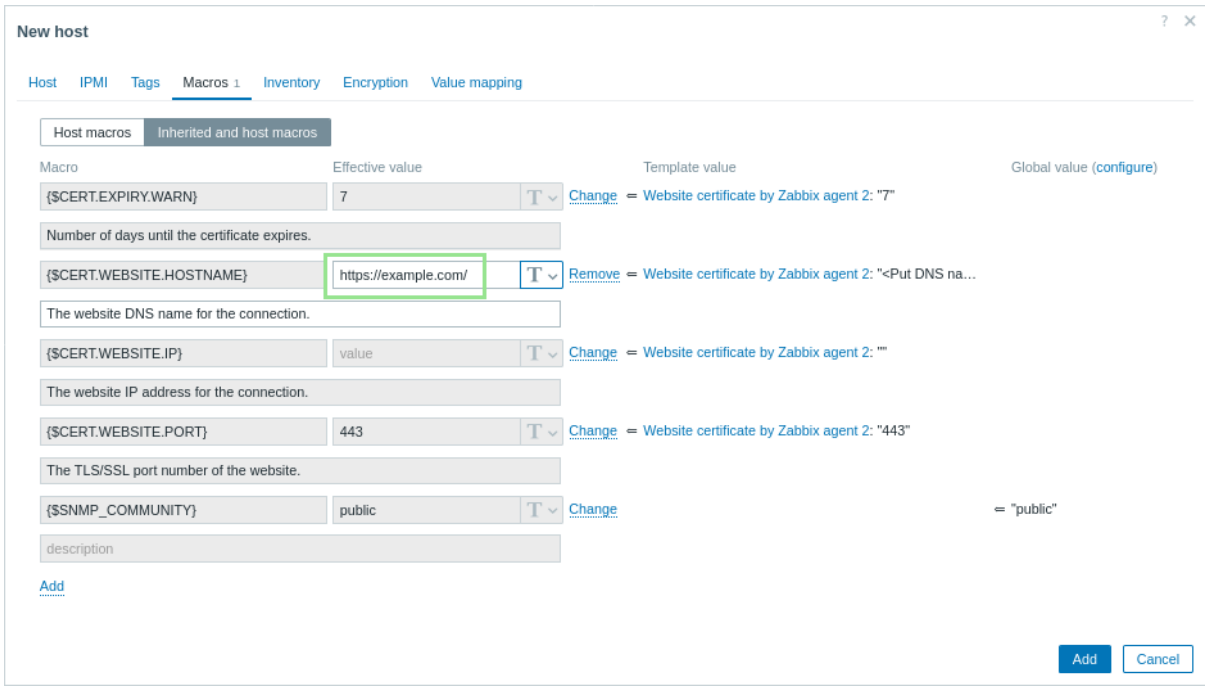
2. Przejdź do *Monitoring* > *Hosts*.

3. Kliknij istniejący host, na którym chcesz monitorować certyfikaty stron internetowych, lub utwórz host, jeśli to konieczne:

- W polu *Host name* wprowadź nazwę hosta (np. „Certificate Monitoring”).
- W polu *Templates* wpisz lub wybierz szablon „Website certificate by Zabbix agent 2”, który zostanie podłączony do hosta.
- W polu *Host groups* wpisz lub wybierz grupę hostów (np. „SSL/TLS Monitoring”).
- W polu *Interfaces* dodaj interfejs typu „Agent” i określ adres IP. W tym przykładzie użyto adresu „127.0.0.1”.



- Na karcie *Macros* przełącz się na *Inherited and host macros*, odszukaj następujące makra i kliknij *Change* obok wartości makra, aby ją zaktualizować:
  - `{$CERT.WEBSITE.HOSTNAME}` — jako wartość wprowadź żądaną nazwę DNS strony internetowej.



4. Kliknij *Add*, aby dodać host.

Aby monitorować wiele stron internetowych, możesz podać rozdzieloną przecinkami listę ich nazw hostów w makrze `{$CERT.WEBSITE.HOSTN`. Opcjonalnie możesz również podać rozdzieloną przecinkami listę portów w makrze `{$CERT.WEBSITE.PORT}`, gdzie każdy port odpowiada odpowiedniej nazwie hosta zgodnie z kolejnością. Na przykład, aby monitorować example.com i example.org na porcie 8443:

- `{$CERT.WEBSITE.HOSTNAME}`: example.com,example.org
- `{$CERT.WEBSITE.PORT}`: 443,8443

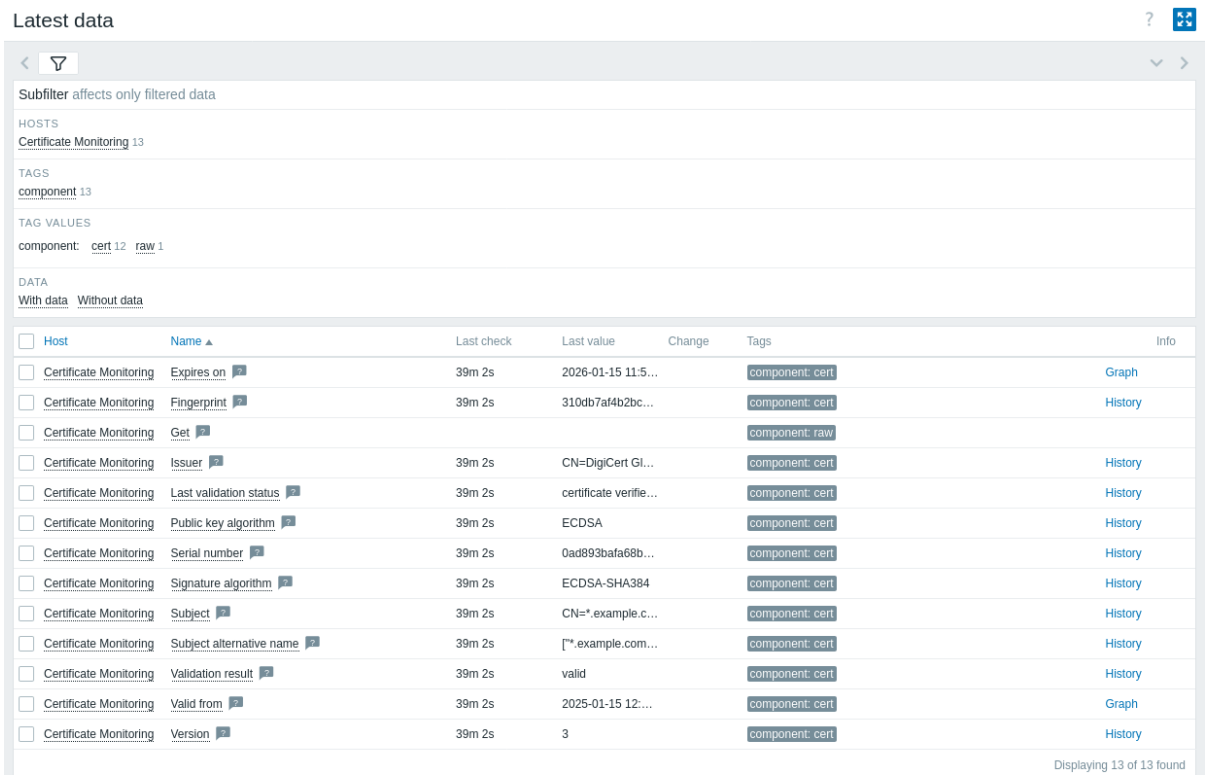
Dla każdej strony internetowej określonej w makrze `{$CERT.WEBSITE.HOSTNAME}` Zabbix utworzy odpowiedni zestaw pozycji i wyzwalaczy. Umożliwia to indywidualne monitorowanie i alertowanie dla certyfikatu SSL każdej strony internetowej.

Host	Name ▲	Last check	Last value
Certificate Monitoring	Get data	11m 16s	{"error":{"message…
Certificate Monitoring	[example.com]: Expires on	11m 6s	2026-01-15 11:59:…
Certificate Monitoring	[example.com]: Fingerprint	11m 6s	310db7af4b2bc90…
Certificate Monitoring	[example.com]: Get		
Certificate Monitoring	[example.com]: Issuer	11m 6s	CN=DigiCert Glob…
Certificate Monitoring	[example.com]: Last validation status	11m 6s	certificate verified …
Certificate Monitoring	[example.com]: Public key algorithm	11m 6s	ECDSA
Certificate Monitoring	[example.com]: Serial number	11m 6s	0ad893bafa68b0b…
Certificate Monitoring	[example.com]: Signature algorithm	11m 6s	ECDSA-SHA384
Certificate Monitoring	[example.com]: Subject	11m 6s	CN=*.example.co…
Certificate Monitoring	[example.com]: Subject alternative name	11m 6s	["*.example.com","…
Certificate Monitoring	[example.com]: Validation result	11m 6s	valid
Certificate Monitoring	[example.com]: Valid from	11m 6s	2025-01-15 12:00:…
Certificate Monitoring	[example.com]: Version	11m 6s	3
Certificate Monitoring	[example.org]: Expires on	10m 52s	2026-01-15 11:59:…
Certificate Monitoring	[example.org]: Fingerprint	10m 52s	3b451cfce915637…
Certificate Monitoring	[example.org]: Get		
Certificate Monitoring	[example.org]: Issuer	10m 52s	CN=DigiCert Glob…
Certificate Monitoring	[example.org]: Last validation status	10m 52s	certificate verified …
Certificate Monitoring	[example.org]: Public key algorithm	10m 52s	ECDSA
Certificate Monitoring	[example.org]: Serial number	10m 52s	0722a749b558476…
Certificate Monitoring	[example.org]: Signature algorithm	10m 52s	ECDSA-SHA384
Certificate Monitoring	[example.org]: Subject	10m 52s	CN=*.example.org…
Certificate Monitoring	[example.org]: Subject alternative name	10m 52s	["*.example.org","e…
Certificate Monitoring	[example.org]: Validation result	10m 52s	valid
Certificate Monitoring	[example.org]: Valid from	10m 52s	2025-01-15 12:00:…

Wyświetlanie zebranych metryk

Gratulacje! Na tym etapie Zabbix monitoruje już wybrany certyfikat WWW.

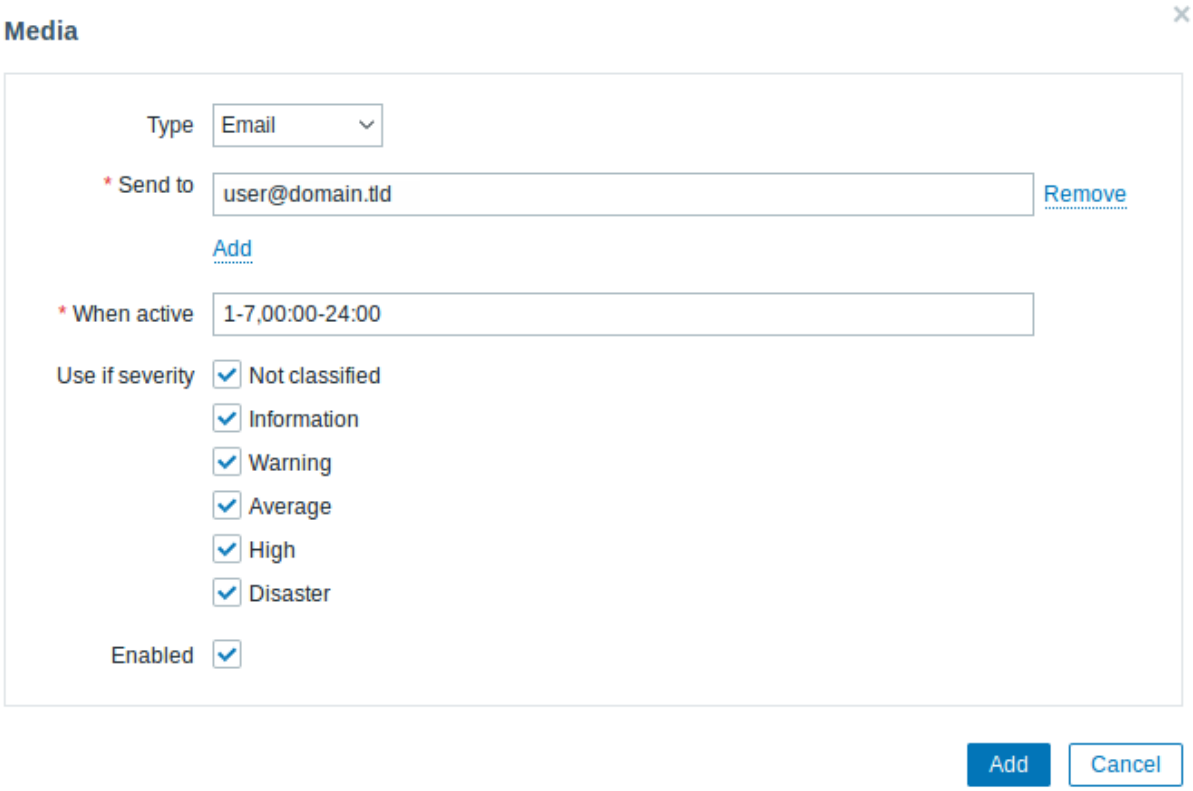
Aby wyświetlić zebrane metryki, przejdź do sekcji menu *Monitoring > Hosts* i kliknij *Latest data* obok hosta, aby wyświetlić na liście wszystkie najnowsze zebrane metryki, takie jak data wygaśnięcia, wystawca i podmiot.



Skonfiguruj alerty o problemach

Zabbix może powiadamiać Cię o problemach z infrastrukturą. Ten przewodnik zawiera podstawowe kroki konfiguracji wysyłania alertów e-mail.

1. Przejdź do *Ustawienia użytkownika > Profil*, przełącz się na kartę *Media* i dodaj swój adres e-mail.



2. Postępuj zgodnie z przewodnikiem Otrzymywanie powiadomienia o problemie.

Następnym razem, gdy Zabbix wykryje problem, powinieneś otrzymać alert e-mail.

Przetestuj swoją konfigurację

Aby przetestować swoją konfigurację, możemy zasymulować rzeczywisty problem, aktualizując konfigurację hosta w Zabbix frontend.

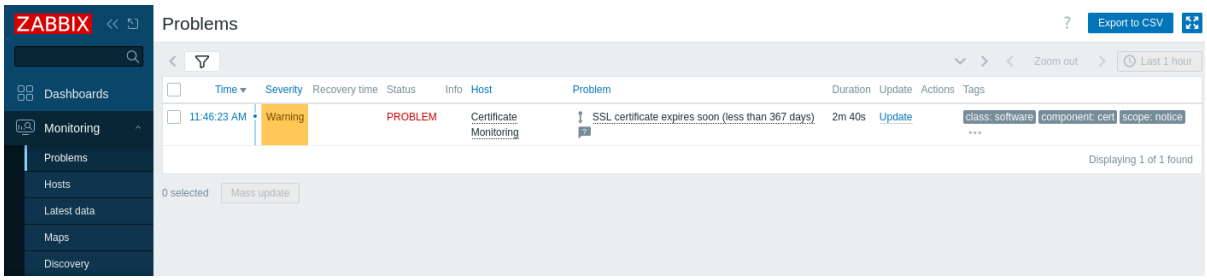
1. Otwórz konfigurację swojego hosta „Certificate Monitoring” w Zabbix.

2. Przejdź do zakładki *Macros* i wybierz *Inherited and host macros*.

3. Kliknij *Change* obok wcześniej skonfigurowanej wartości makra `{$CERT.EXPIRY.WARN}` i ustaw bardzo dużą liczbę dni (więcej niż 365 dni powinno wystarczyć), aby otrzymać ostrzeżenie przed wygaśnięciem certyfikatu.

4. Kliknij *Update*, aby zaktualizować konfigurację hosta.

5. Za chwilę Zabbix wykryje problem „SSL certificate expires soon” wraz z liczbą dni pozostałych do wygaśnięcia. Problem pojawi się w *Monitoring > Problems*.



Jeśli alerty są skonfigurowane, otrzymasz również powiadomienie o problemie.

6. Zmień wartość makra z powrotem na poprzednią, aby rozwiązać problem i kontynuować monitorowanie wartości certyfikatu.

Zobacz także

- Zabbix agent 2 - zawiera listę kluczy pozycji.
- Szablon *Website certificate by Zabbix agent 2* - dodatkowe informacje o szablonie *Website certificate by Zabbix agent 2*.
- Szablon *Website certificate by Zabbix agent 2 active* - dodatkowe informacje o szablonie *Website certificate by Zabbix agent 2 active*.
- Monitorowanie stron internetowych za pomocą pozycji Browser - jak rozpocząć podstawowe monitorowanie stron internetowych za pomocą pozycji Browser.

10 Monitorowanie przełącznika sieciowego lub routera za pomocą Zabbix

Wprowadzenie Ten przewodnik przeprowadzi Cię przez kroki wymagane do rozpoczęcia podstawowego monitorowania przełącznika sieciowego lub routera przy użyciu Zabbix. Jako przykład użyto routera Cisco, jednak procedura ma zastosowanie do każdego urządzenia sieciowego z włączoną obsługą SNMP.

Dla kogo jest ten przewodnik

Ten przewodnik jest przeznaczony dla nowych użytkowników Zabbix oraz administratorów sieci, którzy chcą szybko włączyć podstawowe monitorowanie urządzeń sieciowych. Jeśli potrzebujesz zaawansowanego dostosowania lub rozszerzonych opcji konfiguracji, zapoznaj się ze stroną SNMP agent lub sekcją Konfiguracja podręcznika Zabbix.

Wymagania wstępne

Przed kontynuowaniem upewnij się, że masz:

- Zainstalowane Zabbix serwer i Zabbix frontend: zainstaluj je zgodnie z instrukcjami dla swojego systemu operacyjnego (zobacz Instalacja z pakietów oraz Instalacja interfejsu webowego).
- Zainstalowany Zabbix agent, jeśli monitorujesz lokalne metryki sieciowe.
- Urządzenie z włączonym SNMP: przełącznik sieciowy lub router (na przykład router Cisco) z włączonym SNMP.
- Zainstalowane pliki MIB: instalacja plików MIB umożliwia Zabbix tłumaczenie numerycznych OID na czytelne dla człowieka nazwy i opisy. Bez prawidłowej obsługi MIB możesz widzieć jedynie wartości numeryczne, co utrudnia konfigurację pozycji i rozwiązywanie problemów.

Aby zainstalować pliki MIB w Ubuntu:

1. Zainstaluj pakiet do pobierania MIB:

```
sudo apt-get update
sudo apt-get install snmp-mibs-downloader
```

Jeśli musisz dodać pliki MIB specyficzne dla dostawcy (np. od Cisco, Juniper), umieść je w odpowiednim katalogu MIB:

- W systemach opartych na Linuksie typowe lokalizacje to /usr/share/snmp/mibs/ lub /usr/local/share/snmp/mibs/.
- W instalacjach Zabbix pliki MIB mogą być przechowywane w /var/lib/zabbix/mibs/.

Upewnij się, że zmienna środowiskowa MIBDIRS lub plik snmp.conf zawiera prawidłową ścieżkę.

Aby sprawdzić, czy system rozpoznaje nowe pliki MIB, użyj:

```
snmptranslate -IR -On <MIB-NAME>::<object>
```

Szczegółowe instrukcje znajdziesz w dokumentacji swojej biblioteki SNMP:

- Cisco MIBs
- Juniper MIBs

2. Edytuj `/etc/snmp/snmp.conf` i zakomentuj linię zaczynającą się od `mibs :`, aby umożliwić systemowi załadowanie wszystkich dostępnych plików MIB.

3. Zweryfikuj to, uruchamiając `snmpwalk` (na przykład `snmpwalk -v 2c -c <your_community_string> <device_IP>`), i sprawdź, czy OID są wyświetlane z opisowymi nazwami.

W zależności od środowiska niektóre kroki w tym przewodniku mogą się nieznacznie różnić. Ten przewodnik opiera się na środowisku działającym pod kontrolą Ubuntu oraz monitorowanym urządzeniu sieciowym Cisco Catalyst 3750V2-24FS.

Zakłada się, że urządzenie sieciowe jest już fizycznie zainstalowane i podłączone.

Skonfiguruj urządzenie sieciowe (przykład routera Cisco) Aby monitorowanie przez SNMP było możliwe, musisz skonfigurować urządzenie sieciowe tak, aby zezwalało na zapytania SNMP. Poniższy przykład dotyczy SNMPv2 i nie uwzględnia istniejących ustawień. Uwaga: zastosowanie tych poleceń może nadpisać bieżące konfiguracje SNMP.

W przypadku routera Cisco konfiguracja zazwyczaj obejmuje kroki opisane poniżej.

Przykład SNMPv2 1. Włącz SNMP i ustaw ciąg community.

Zaloguj się do konsoli routera Cisco i przejdź do trybu konfiguracji:

```
configure terminal
```

Następnie włącz SNMP, podając ciąg community tylko do odczytu. Na przykład:

```
snmp-server community <your_community_string> RO
```

Zastąp `<your_community_string>` swoim bezpiecznym ciągiem community. Uwaga: opcja RO (Read-Only) umożliwia SNMP pobieranie danych z urządzenia, ale uniemożliwia wprowadzanie jakichkolwiek zmian konfiguracyjnych.

Ze względów bezpieczeństwa zaleca się ograniczenie dostępu SNMP wyłącznie do niezbędnych urządzeń. Aby uzyskać dalsze wskazówki dotyczące konfigurowania list kontroli dostępu (ACL), zapoznaj się z oficjalną dokumentacją Cisco.

2. Zapisz konfigurację.

Zapisz zmiany, aby ustawienia SNMP zostały zachowane po ponownym uruchomieniu:

```
write memory
```

Przykład SNMPv3 SNMPv3 zapewnia zwiększone bezpieczeństwo dzięki uwierzytelnianiu i szyfrowaniu. Jego konfiguracja jest bezpieczniejsza niż w przypadku SNMPv2 i powinna zostać zweryfikowana z dokumentacją właściwą dla danego urządzenia.

1. Utwórz grupę SNMP.

Skonfiguruj grupę SNMPv3 z włączoną prywatnością (szyfrowaniem):

```
configure terminal
snmp-server group <your_group> v3 priv
```

2. Utwórz użytkownika SNMP.

Dodaj użytkownika SNMPv3 z uwierzytelnianiem i prywatnością. Zastąp symbole zastępcze żądanymi wartościami:

```
snmp-server user <your_user> <your_group> v3 auth md5 <auth_password> priv aes 128 <priv_password>
```

3. Zapisz konfigurację:

```
write memory
```

Aby uzyskać więcej informacji lub instrukcje dotyczące konkretnego modelu, możesz skorzystać z zewnętrznych samouczków konfiguracji Cisco SNMP. Ten przewodnik przedstawia jednak podstawowe kroki umożliwiające włączenie monitorowania SNMP.

Konfiguracja frontendu Zabbix

Utwórz host w frontendzie Zabbix 1. Zaloguj się do frontendu Zabbix.

2. Dodaj nowy host.

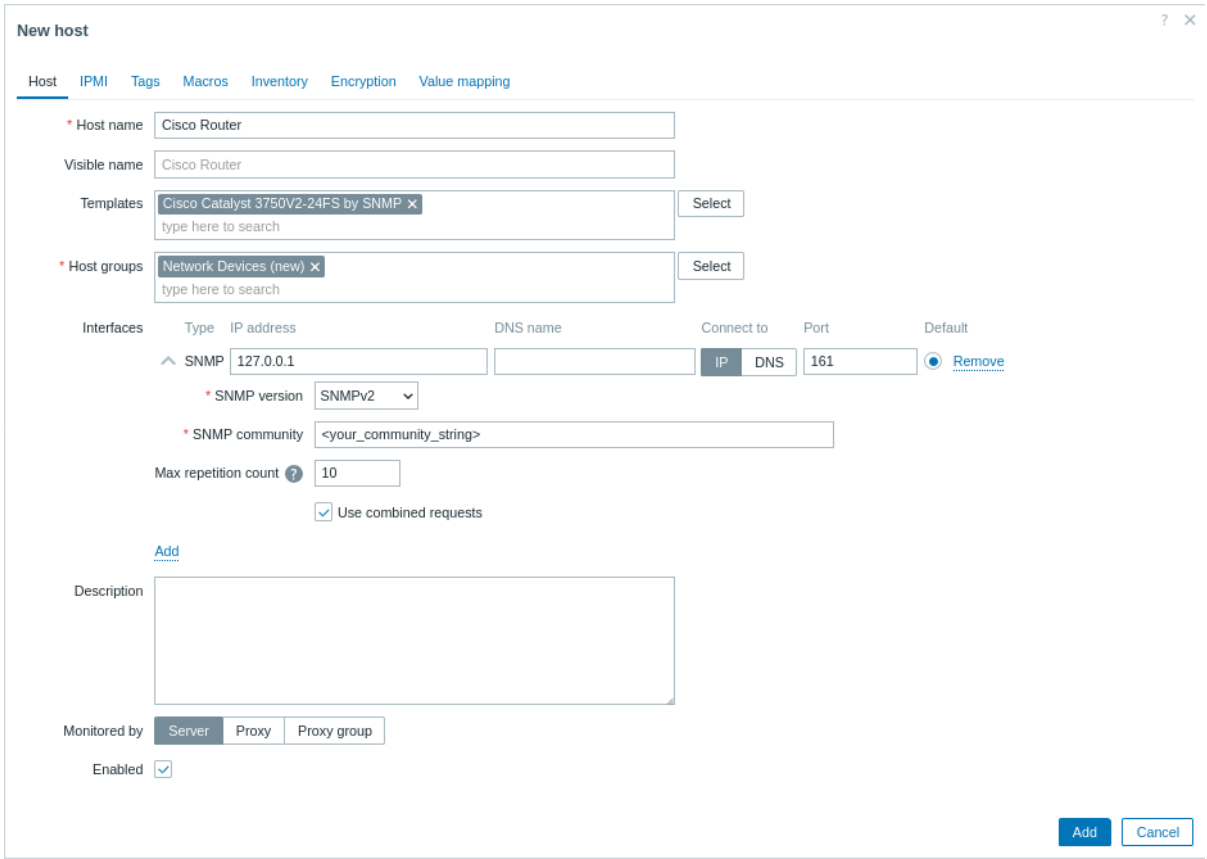
Przejdź do *Data collection* > *Hosts* i kliknij *Create host*.

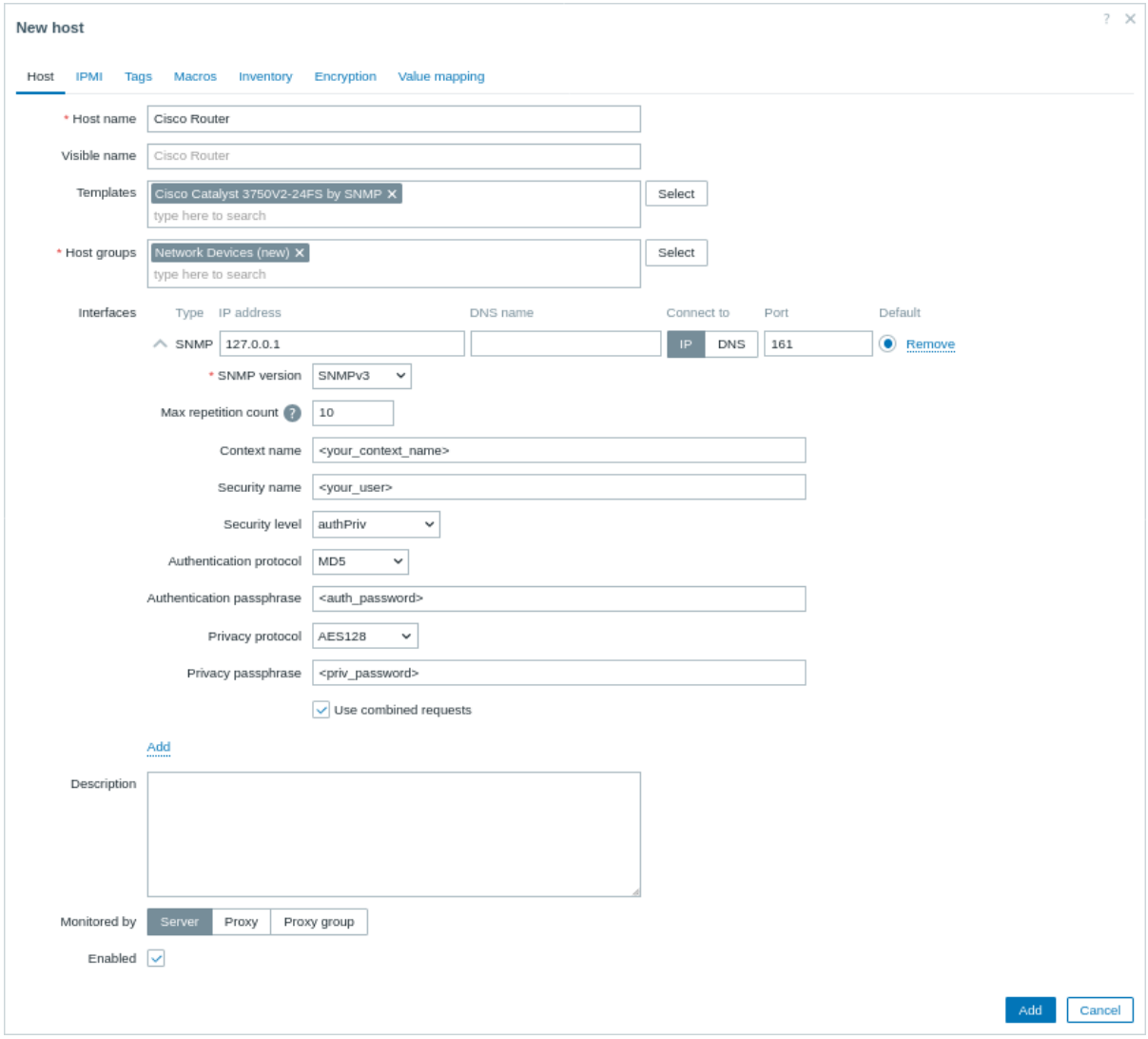
- *Host name*: wprowadź nazwę swojego urządzenia (np. „Cisco Router”).
- Host groups: wybierz istniejącą grupę lub utwórz nową grupę, taką jak „Network Devices”.
- Interfaces:
  - Kliknij *Add* w sekcji Interfaces.
  - Wybierz *SNMP* jako typ interfejsu.
  - Wprowadź adres IP lub nazwę DNS swojego routera Cisco.
  - Ustaw domyślny port SNMP (zwykle 161).
  - Użyj menu rozwijanego, aby wybrać odpowiednią wersję SNMP (np. SNMPv2).
  - Dla SNMPv1/v2 wprowadź community string w polu *SNMP community*. W przypadku SNMPv3 zostaniesz poproszony o podanie dodatkowych poświadczeń (*Context name*, *Security name* i *Security level* itp.).

3. Podłącz szablony

W polu *Templates* wybierz szablon SNMP, który najlepiej pasuje do Twojego urządzenia. Zabbix udostępnia szereg gotowych szablonów SNMP dla wielu rodzin urządzeń. Na przykład, jeśli monitorujesz urządzenie Cisco, wybierz szablon odpowiadający systemowi operacyjnemu lub modelowi Twojego urządzenia (taki jak Cisco IOS SNMP lub Cisco Catalyst 3750<model urządzenia> SNMP).

4. Kliknij *Add*, aby zapisać host.

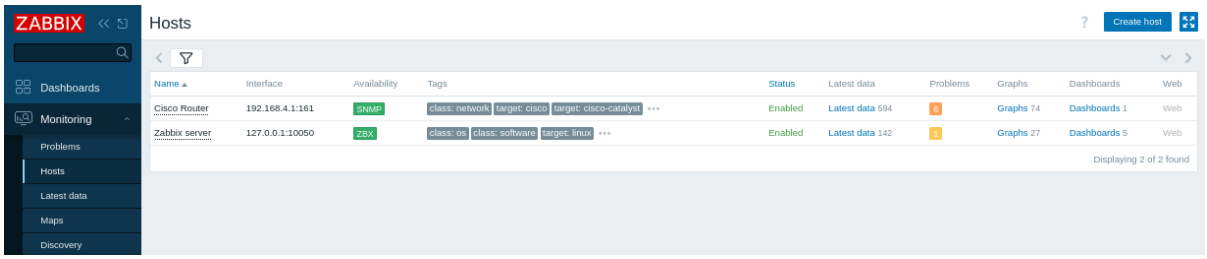




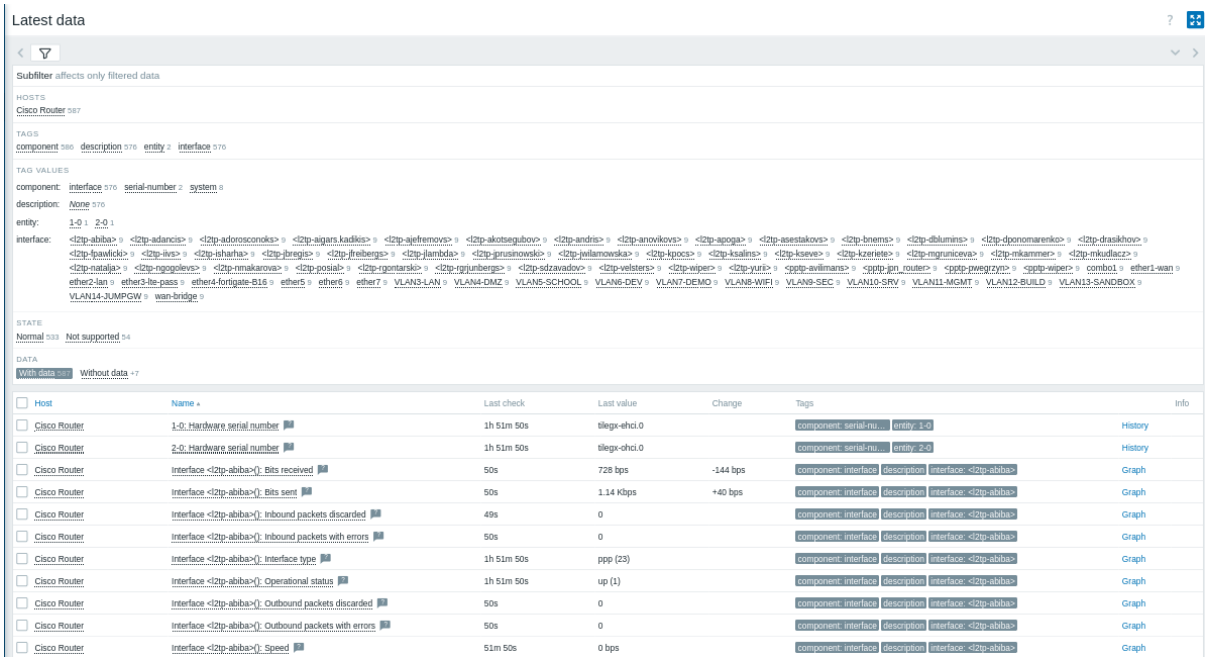
Wyświetlanie zebranych metryk Gratulacje! Zabbix jest teraz skonfigurowany do monitorowania Twojego urządzenia sieciowego.

Najnowsze dane:

- Przejdź do Monitoring > Latest data w frontendzie Zabbix.



- Wybierz host „Cisco Router” (lub wykryte hosty), aby wyświetlić metryki, takie jak czas działania sprzętu i sieci, utrata pakietów ICMP, ping, czas odpowiedzi itp.



- Wykresy i ekrany:

Aby zwizualizować dane wydajności, kliknij *Graphs* obok pozycji SNMP, aby zobaczyć szczegółowe metryki.

Jako kolejny krok możesz:

- Dodać niestandardowe pozycje SNMP, aby monitorować dodatkowe metryki.
- Skonfigurować alerty problemów, aby otrzymywać powiadomienia o potencjalnych problemach.

Tworzenie pozycji SNMP Gdy host jest już skonfigurowany, możesz utworzyć pozycje do monitorowania określonych metryk. Uwaga: ten krok jest opcjonalny, jeśli używasz szablonu, ponieważ szablony zawierają już domyślne zestawy pozycji.

1. Zidentyfikuj OID SNMP:

Użyj polecenia `snmpwalk`, aby wyświetlić listę dostępnych OID-ów na swoim urządzeniu. Na przykład:

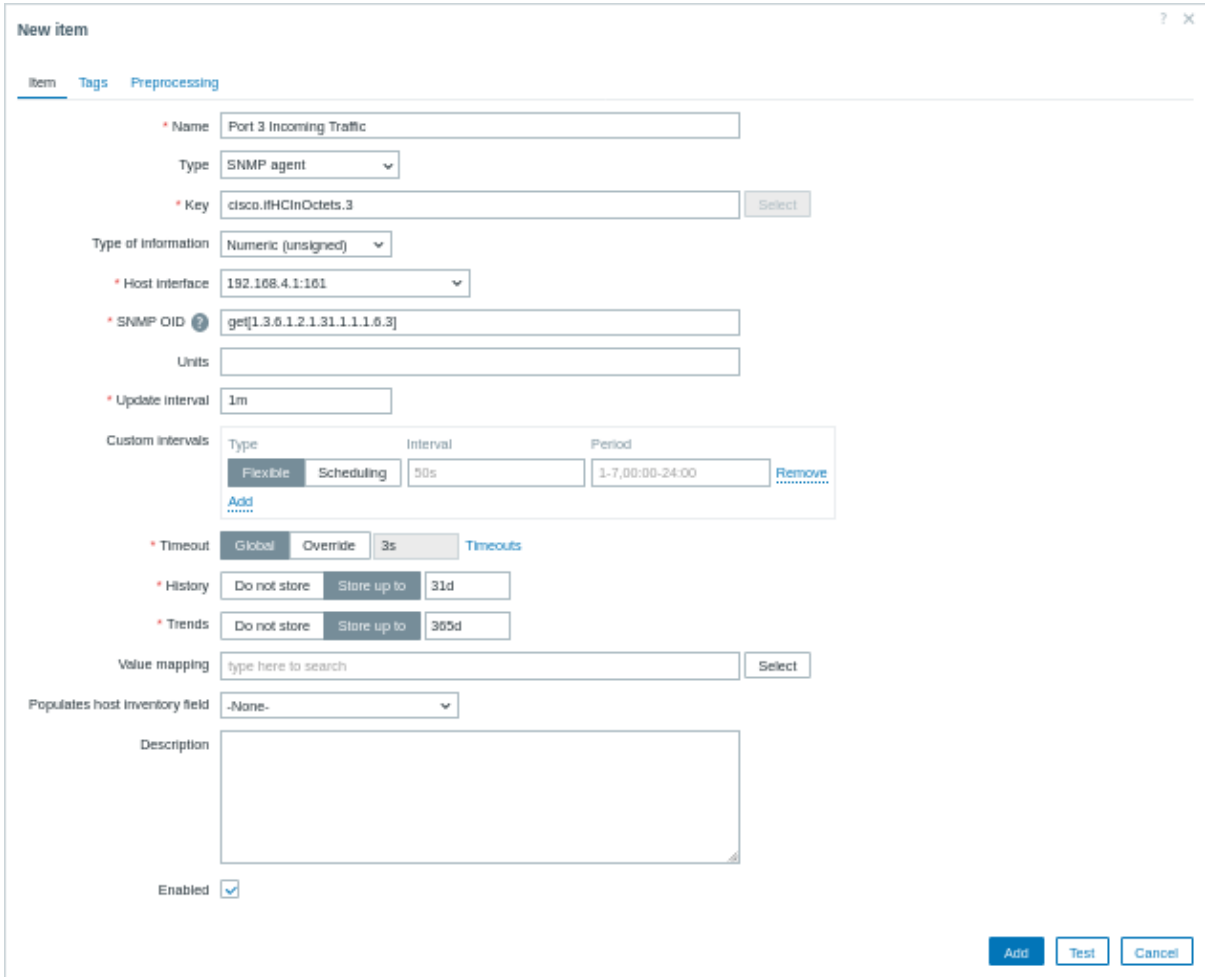
```
snmpwalk -v 2c -c <your_community_string> <device_IP> .
```

Znajdź OID dla metryki, którą chcesz monitorować (na przykład IF-MIB::ifHCInOctets.3 dla ruchu przychodzącego na porcie 3). Aby uzyskać numeryczny OID, możesz użyć:

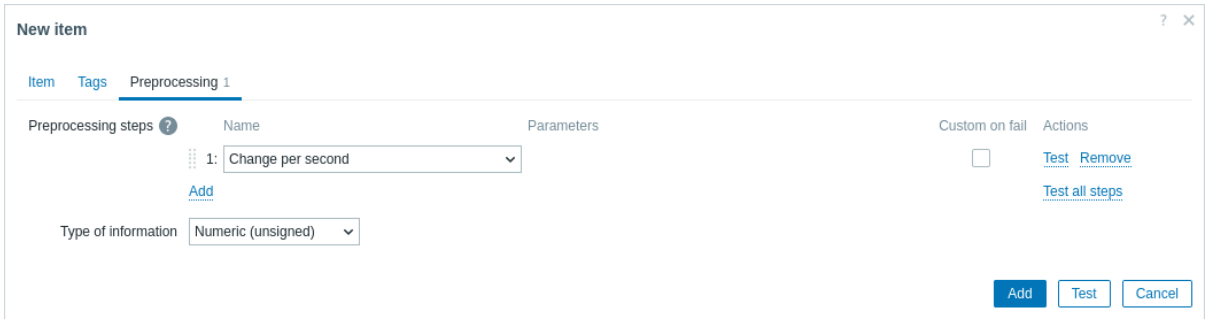
```
snmpget -v 2c -c <your_community_string> -On <device_IP> IF-MIB::ifHCInOctets.3
```

2. Utwórz pozycję SNMP:

- Przejdź do *Data collection* > *Hosts* i kliknij kartę *Items* dla swojego hosta SNMP, a następnie kliknij *Create item*.
- *Name*: wprowadź opisową nazwę (np. „Ruch przychodzący na porcie 3”).
- *Type*: wybierz *SNMP agent*.
- *Key*: podaj znaczący klucz (np. `cisco.ifHCInOctets.3`).
- *Host interface*: upewnij się, że wybrany jest interfejs SNMP.
- *SNMP OID*: wprowadź OID, używając jednego z obsługiwanych formatów, na przykład:
  - `get[1.3.6.1.2.1.31.1.1.1.6.3]` dla pojedynczej wartości;
  - `walk[1.3.6.1.2.1.31.1.1.1.6.3]` do asynchronicznego pobrania poddrzewa wartości.



- *Preprocessing* (w razie potrzeby): jeśli pozycja zwraca licznik skumulowany (taki jak ruch na interfejsie), przejdź do karty *Preprocessing* i dodaj krok przetwarzania wstępnego, taki jak „Zmiana na sekundę”, aby obliczyć tempo.



Aby pobrać wiele wartości w jednej transakcji SNMP, możesz podać kilka OID-ów, używając składni `walk[OID1,OID2,...]`.

Tłumaczenie OID-ów między nazwami numerycznymi a MIB Podczas pracy z SNMP może być konieczna konwersja między numerycznymi OID-ami a odpowiadającymi im nazwami MIB. Takie tłumaczenie ułatwia identyfikację metryk i rozwiązywanie problemów.

- Tłumaczenie nazwy MIB na numeryczny OID: użyj polecenia `snmptranslate` z opcją `-On`. Na przykład, aby przetłumaczyć nazwę MIB `IF-MIB::ifHCInOctets.3` na jej numeryczny OID, uruchom:

```
snmptranslate -On IF-MIB::ifHCInOctets.3
```

To polecenie może zwrócić:

```
.1.3.6.1.2.1.31.1.1.1.6.3
```

- Tłumaczenie numerycznego OID-a na jego nazwę MIB: użyj polecenia `snmptranslate` z opcją `-IR` (lub `-m ALL`), aby odwrócić tłumaczenie. Na przykład, aby przetłumaczyć numeryczny OID `.1.3.6.1.2.1.31.1.1.1.6.3` z powrotem na jego nazwę MIB, uruchom:

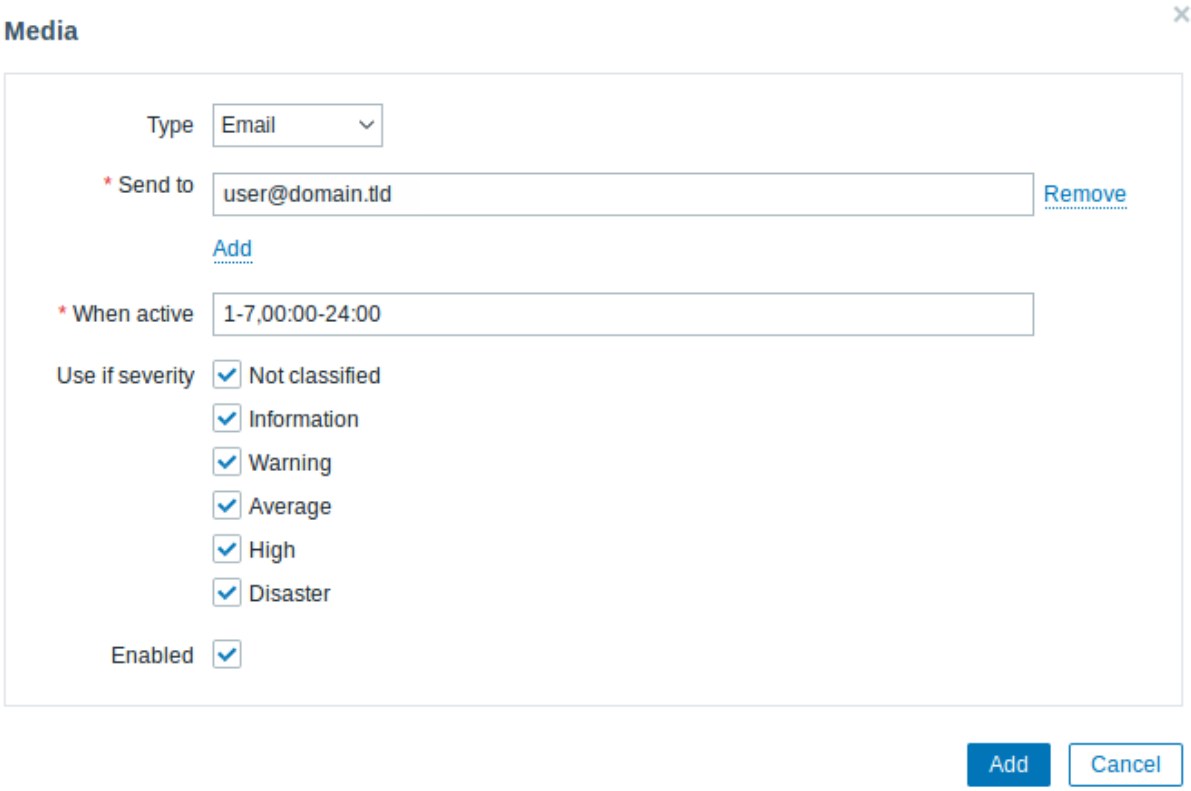
```
snmptranslate -IR -On .1.3.6.1.2.1.31.1.1.1.6.3
```

To polecenie może zwrócić:

```
IF-MIB::ifHCInOctets.3
```

Konfiguracja alertów o problemach Ten przewodnik zawiera podstawowe kroki konfiguracji wysyłania alertów e-mail.

1. Przejdź do *User settings > Profile*, przełącz się na kartę *Media* i dodaj swój adres e-mail.

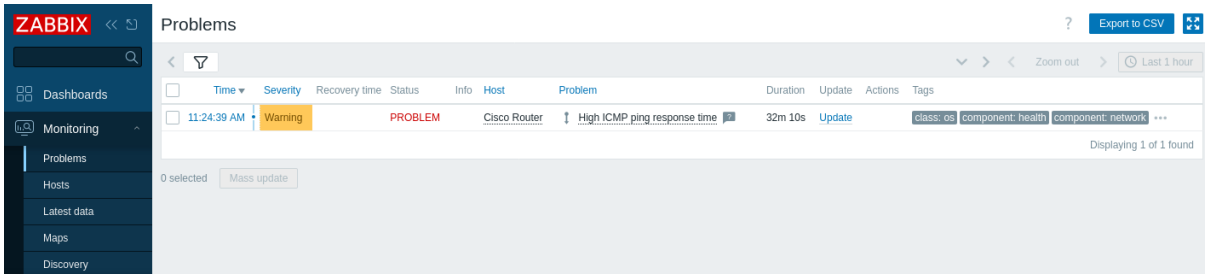


2. Postępuj zgodnie z przewodnikiem Receiving a problem notification.

Następnym razem, gdy Zabbix wykryje problem, powinieneś otrzymać alert e-mail.

Przetestuj swoją konfigurację Aby upewnić się, że Zabbix prawidłowo wykrywa problemy z wydajnością sieci, zasymuluj rzeczywisty problem, zwiększając próg czasu odpowiedzi ICMP ping.

1. Otwórz konfigurację swojego hosta „Cisco Router” w Zabbix.
2. Przejdź do zakładki *Macros* i wybierz *Inherited and host macros*.
3. Znajdź makro `{$ICMP_RESPONSE_TIME_WARN}` (lub podobne makro progu czasu odpowiedzi).
4. Ustaw bardzo niską wartość (np. 0.001), aby wyzwolić alert, gdy odpowiedź ping przekroczy tę wartość.
5. Kliknij *Update*, aby zastosować zmiany.
6. Poczekaj chwilę, aż Zabbix wykryje zasymulowany problem.
7. Przejdź do *Monitoring > Problems*, aby sprawdzić, czy pojawił się alert (np. „High ICMP ping response time”).



Jeśli alerty są skonfigurowane, powinieneś również otrzymać powiadomienie o problemie.

8. Przywróć pierwotną wartość makra i kliknij *Update*, aby zapisać zmiany.
9. Potwierdź, że problem został rozwiązany i zniknął z sekcji *Problems*.

Rozwiązywanie problemów z monitorowaniem SNMP Jeśli zauważysz, że ikona SNMP w frontendzie Zabbix jest CZERWONA lub nie są zbierane żadne dane, wypróbuj następujące kroki:

1. Sprawdź łączność SNMP.

Dla SNMPv2 uruchom następujące polecenie z serwera Zabbix:

```
snmpwalk -v 2c -c <community_string> <device_IP> .
```

To polecenie weryfikuje, czy urządzenie odpowiada na zapytania SNMP.

W przypadku SNMPv3 podaj odpowiednie poświadczenia SNMPv3:

```
snmpwalk -v3 -u <your_user> -l authPriv -a MD5 -A <auth_password> -x AES -X <priv_password> <device_IP> .
```

To weryfikuje, czy poświadczenia SNMPv3 są poprawne oraz czy urządzenie odpowiada w sposób bezpieczny.

2. Upewnij się, że pliki MIB są zainstalowane i włączone zgodnie z opisem w wymaganiach wstępnych. Aby to potwierdzić, następujące polecenie nie powinno zwracać błędu podczas odpytywania urządzenia sieciowego:

```
snmpwalk -v 2c -c <your_community_string> <device_IP> ifInOctets
```

Powinno to zwrócić przetłumaczone OID bez błędów.

3. Potwierdź, że wersja SNMP i poświadczenia skonfigurowane w Zabbix odpowiadają tym ustawionym na urządzeniu. Na przykład sprawdź ustawienia SNMP w konfiguracji hosta Zabbix i porównaj je z konfiguracją urządzenia. Na urządzeniu Cisco możesz sprawdzić ustawienia SNMP, uruchamiając:

```
show running-config | include snmp
```

To pozwala upewnić się, że community string (dla SNMPv2) lub dane użytkownika SNMPv3 są poprawne.

4. Zweryfikuj, że SNMP jest poprawnie włączone na urządzeniu sieciowym. Na routerze Cisco zaloguj się do konsoli i uruchom:

```
show running-config | include snmp
```

To polecenie wyświetla aktywną konfigurację SNMP i pomaga potwierdzić, że SNMP jest poprawnie skonfigurowane.

5. Upewnij się, że żadne zapory sieciowe ani problemy sieciowe nie blokują ruchu SNMP (zwykle na porcie 161) między serwerem Zabbix a urządzeniem. Możesz przetestować łączność za pomocą:

nc -zv <device_IP> 161

`nc -zv` sprawdza, czy port 161 jest otwarty i nasłuchuje na urządzeniu.

Dodatkowo, jeśli używasz UFW w Ubuntu, sprawdź stan zapory:

```
sudo ufw status
```

Lub, w przypadku iptables:

```
sudo iptables -L -n
```

6. Przejrzyj pliki dziennika serwera Zabbix pod kątem błędów związanych z SNMP, aby pomóc w ustaleniu przyczyny problemu:

```
tail -f /tmp/zabbix_server.log
```

`tail -f` pozwala monitorować aktualizacje dziennika w czasie rzeczywistym.

Zobacz także:

- Tworzenie pozycji - dowiedz się, jak dodawać dodatkowe metryki.
- Agent SNMP - dodatkowe informacje o monitorowaniu SNMP w Zabbix.
- Standaryzowane szablony dla urządzeń sieciowych - informacje o dostępnych szablonach SNMP.
- Odkrywanie OID-ów SNMP - dodatkowe informacje o wykrywaniu SNMP na przełączniku.
- Konfigurowanie reguły wykrywania sieci - dodatkowe informacje o tym, jak skonfigurować regułę wykrywania sieci używaną przez Zabbix do wykrywania hostów i usług.

11 Monitorowanie dziennika zdarzeń Windows przy użyciu aktywnych kontroli

Wprowadzenie

Ten przewodnik wyjaśnia, jak monitorować dzienniki zdarzeń systemu Windows w Zabbix przy użyciu aktywnych kontroli. Korzystając z kluczy pozycji specyficznych dla systemu Windows w Zabbix, można zbierać i analizować krytyczne zdarzenia (takie jak nieudane próby logowania, błędy systemowe itp.) w czasie rzeczywistym.

Dla kogo jest ten przewodnik

Ten przewodnik jest przeznaczony dla nowych użytkowników Zabbix oraz administratorów sieci, którzy chcą monitorować dzienniki zdarzeń systemu Windows. Informacje o zaawansowanych opcjach konfiguracji można znaleźć w dokumentacji kluczy pozycji specyficznych dla systemu Windows.

Wymagania wstępne

Przed kontynuowaniem należy pobrać i zainstalować serwer Zabbix oraz frontend Zabbix zgodnie z instrukcjami dla używanego systemu operacyjnego. Należy również pobrać i zainstalować agent Zabbix na komputerze z systemem Windows, który ma być monitorowany.

Skonfiguruj agent Zabbix do monitorowania dziennika zdarzeń systemu Windows

1. Otwórz `zabbix_agentd.conf` (domyślna ścieżka: `C:\Program Files\Zabbix Agent\zabbix_agentd.conf`) na swoim hoście Windows i upewnij się, że parametr ServerActive jest ustawiony na adres IP twojego serwera Zabbix, a parametr Hostname odpowiada nazwie hosta, która zostanie zdefiniowana w frontend Zabbix. Umożliwia to agentowi żądanie aktywnych kontroli dla swojego hosta i od określonego serwera Zabbix. Na przykład:

```
ServerActive=192.0.2.0
Hostname=MyWindowsHost
```

2. Uruchom ponownie usługę agent Zabbix, aby zastosować zmiany:

```
net stop "Zabbix Agent" && net start "Zabbix Agent"
```

3. Sprawdź, czy host Windows działa:

- Upewnij się, że usługa agent Zabbix działa na hoście Windows.
- Sprawdź, czy host Windows może połączyć się z serwerem Zabbix na porcie 10051. Aby przetestować łączność z hosta Windows, otwórz PowerShell i uruchom następujące polecenie:

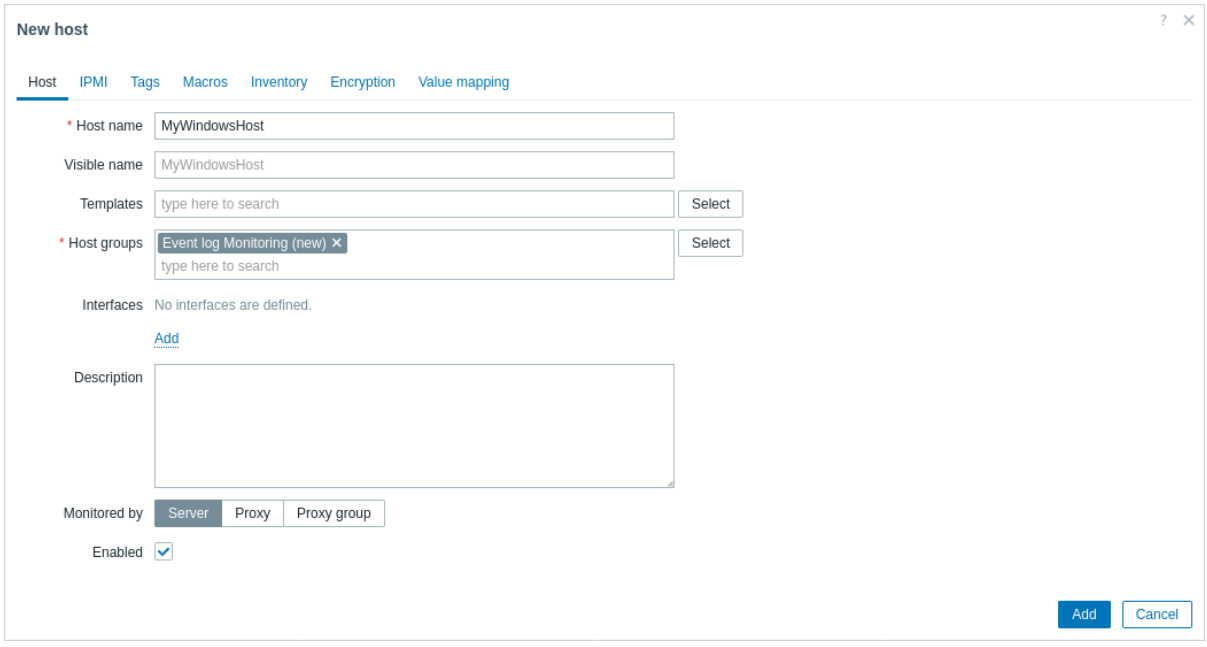
```
Test-NetConnection -ComputerName <Zabbix-server-IP> -Port 10051
```

Konfiguracja frontend Zabbix

1. Przejdź do *Data collection* > *Hosts* i utwórz hosta:

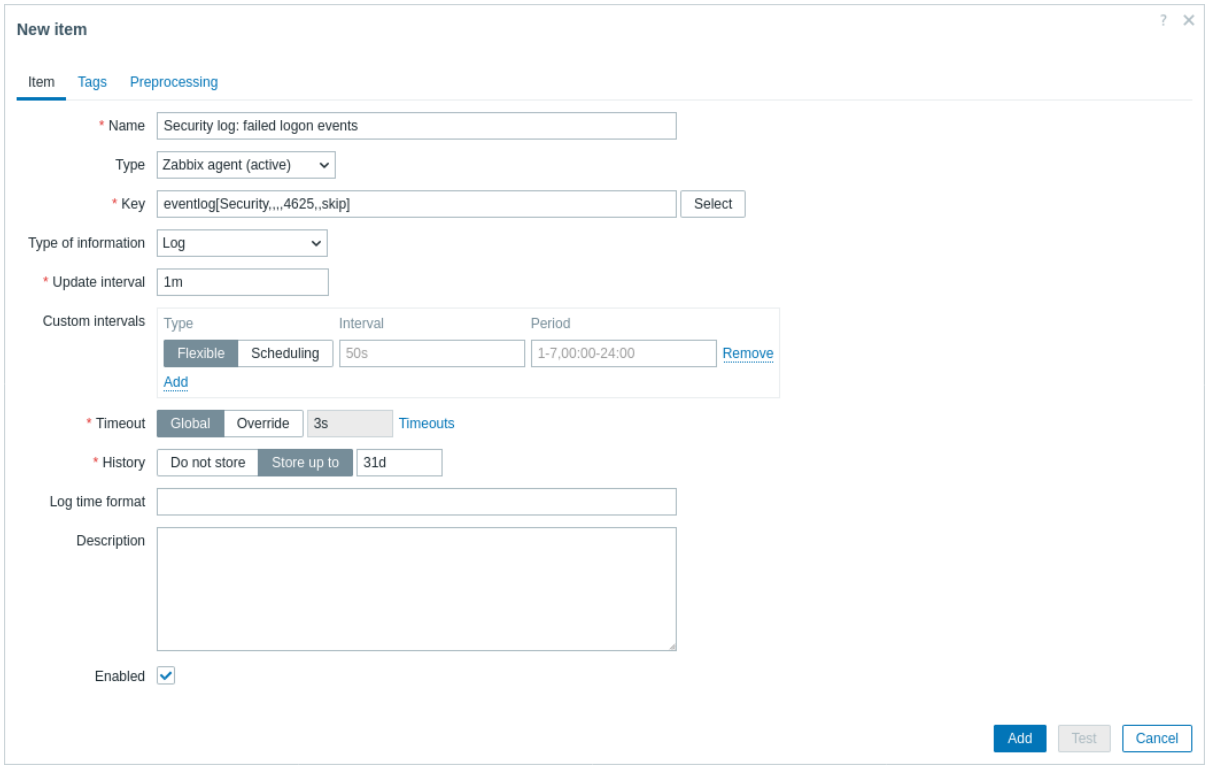
- W polu *Host name* wprowadź nazwę hosta (np. „MyWindowsHost”).
- W polu *Host groups* wpisz lub wybierz grupę hostów (np. „Event log Monitoring”).
- Naciśnij *Add*, aby zapisać skonfigurowanego hosta.

Note:
W polu *Templates* możesz dodać szablon „Windows by Zabbix agent active”, aby ułatwić rozwiązywanie problemów przez obserwowanie, czy inne aktywne pozycje na tym samym hoście są aktualizowane.



2. Utwórz nową pozycję z następującymi parametrami:

- W polu *Name* wprowadź opisową nazwę pozycji (np. „Security log: failed logon events”).
- Z listy rozwijanej *Type* wybierz „Zabbix agent (active)” (wymagane do monitorowania dziennika zdarzeń).
- W polu *Key* użyj klucza pozycji eventlog. Na przykład, aby monitorować nieudane próby logowania (Event ID: 4625) w dzienniku Security i ignorować wpisy starsze niż ostatnie sprawdzenie pozycji (przy użyciu parametru `skip`), wprowadź następujący klucz pozycji: `eventlog[Security,,,,4625,,skip]`
- Z listy rozwijanej *Type of information* wybierz „Log”.



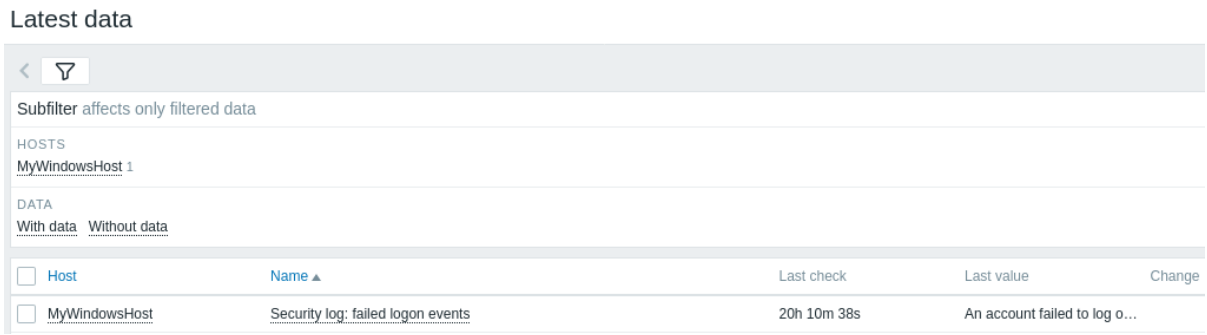
3. Kliknij *Add*, aby zapisać pozycję.

Testowanie i przegląd zebranych metryk

Gratulacje! Zabbix jest teraz skonfigurowany do zbierania dzienników zdarzeń systemu Windows. Aby sprawdzić, czy dzienniki zdarzeń są zbierane, możesz przetestować pozycję „Security log: failed logon events”, wylogowując się ze swojego konta Windows i próbując zalogować się przy użyciu nieprawidłowych poświadczeń.

Następnie wyświetl zebrane dzienniki w Zabbix frontend:

1. Przejdź do *Monitoring* > *Latest data* w Zabbix frontend.



2. Odfiltruj dane według hosta „MyWindowsHost” w polu *Name*.

3. Kliknij *History*, aby wyświetlić zarejestrowane wartości dziennika.

MyWindowsHost: Security log: failed logon events

Timestamp	Local time	Source	Severity	Event ID	Value
2025-04-07 11:13:11 PM	2025-04-07 11:12:19 PM	Microsoft-Windows-Security-Auditing	Failure Audit	4625	An account failed to log on. Subject: Security ID: NT AUTHORITY\SYSTEM Account Name: DESKTOP-NNEM26U$ Account Domain: WORKGROUP Logon ID: 0x3E7 Logon Type: 2 Account For Which Logon Failed: Security ID: NULL SID Account Name: Admin Account Domain: DESKTOP-NNEM26U Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A

4. Jeśli wartości dziennika nie są widoczne, przejdź do sekcji Rozwiązywanie problemów w tym przewodniku.

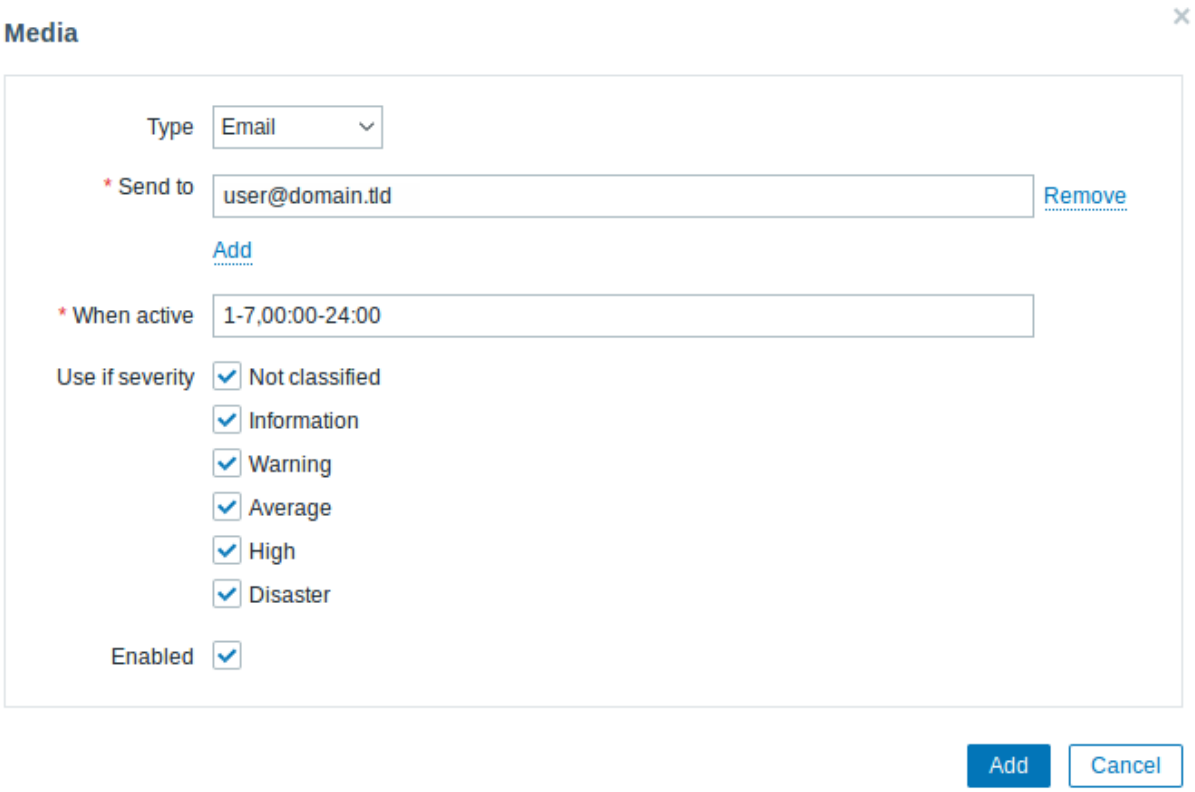
Konfiguracja alertów o problemach

Ten przewodnik zawiera podstawowe kroki konfiguracji wysyłania alertów e-mail.

1. Przejdź do **Zbieranie danych > Hosty**, aby zdefiniować wyzwalacz, który uruchomi się, gdy pozycja dziennika zdarzeń zarejestruje interesujący Cię wzorzec. Na przykład, aby wykrywać nieudane próby logowania w dzienniku Security, użyj funkcji find():

find(/MyWindowsHost/eventlog[Security,,,4625,skip],10m,"like","Logon failed")

2. Przejdź do *Ustawienia użytkownika > Profil*, otwórz kartę *Media* i dodaj swój adres e-mail.



3. Postępuj zgodnie z przewodnikiem Otrzymywanie powiadomienia o problemie.

Następnym razem, gdy Zabbix wykryje problem, powinieneś otrzymać alert e-mail.

Rozwiązywanie problemów

Jeśli napotkasz problemy ze zbieraniem lub wyświetlaniem dzienników zdarzeń systemu Windows, skorzystaj z poniższych wskazówek, aby zidentyfikować i rozwiązać typowe problemy:

1. Na serwerze Zabbix (Linux) wyświetl reguły iptables za pomocą następującego polecenia:

```
sudo iptables -L -n
```

i sprawdź, czy istnieje reguła ACCEPT dla portu TCP 10051.

2. Upewnij się, że klucz `eventlog[...]` używa dokładnej nazwy dziennika (z uwzględnieniem wielkości liter), identyfikatora zdarzenia, trybu (np. skip) oraz innych parametrów dokładnie tak, jak pokazano w kluczach pozycji specyficznych dla systemu Windows.

Zobacz także:

- Tworzenie pozycji — dowiedz się, jak dodawać dodatkowe metryki.
- Agent Zabbix w systemie Microsoft Windows — szczegółowe instrukcje instalacji.
- Monitorowanie systemu Windows za pomocą agenta Zabbix — kompleksowy przewodnik dotyczący konfiguracji podstawowego monitorowania maszyn z systemem Windows przy użyciu agenta Zabbix.
- Klucze pozycji specyficzne dla systemu Windows — szczegółowe informacje o kluczach pozycji specyficznych dla systemu Windows obsługiwanych przez agentów Zabbix, w tym o kluczach do monitorowania dziennika zdarzeń.
- Monitorowanie plików dziennika — instrukcje dotyczące konfiguracji Zabbix do scentralizowanego monitorowania i analizy plików dziennika, mające zastosowanie również do dzienników zdarzeń systemu Windows.

Czym jest Zabbix

Zabbix został stworzony przez Alexeia Vladisheva i obecnie jest aktywnie rozwijany oraz wspierany przez Zabbix SIA.

Zabbix to rozproszone rozwiązanie monitorujące klasy korporacyjnej typu open source.

Zabbix to oprogramowanie monitorujące liczne parametry sieci oraz stan i integralność serwerów, maszyn wirtualnych, aplikacji, usług, baz danych, stron internetowych, chmury i nie tylko. Zabbix wykorzystuje elastyczny mechanizm powiadomień, który umożliwia użytkownikom konfigurowanie alertów e-mail dla praktycznie każdego zdarzenia. Pozwala to na szybką reakcję na problemy serwera. Zabbix oferuje doskonałe funkcje raportowania i wizualizacji danych w oparciu o przechowywane dane. Dzięki temu Zabbix idealnie nadaje się do planowania pojemności.

Zabbix obsługuje zarówno odpytywanie, jak i trapowanie. Wszystkie raporty i statystyki Zabbix, a także parametry konfiguracyjne, są dostępne przez oparty na sieci frontend. Oparty na sieci frontend zapewnia, że stan sieci i kondycja serwerów mogą być oceniane z dowolnego miejsca. Przy prawidłowej konfiguracji Zabbix może odgrywać ważną rolę w monitorowaniu infrastruktury IT. Dotyczy to w równym stopniu małych organizacji z kilkoma serwerami, jak i dużych firm z wieloma serwerami.

Zabbix jest bezpłatny. Zabbix jest tworzony i rozpowszechniany na licencji AGPL-3.0. Oznacza to, że jego kod źródłowy jest swobodnie rozpowszechniany i dostępny publicznie.

Dostępne jest wsparcie komercyjne, świadczone przez firmę Zabbix i jej partnerów na całym świecie.

Dowiedz się więcej o funkcjach Zabbix.

Użytkownicy Zabbix Wiele organizacji różnej wielkości na całym świecie polega na Zabbix jako podstawowej platformie monitoringu.

Architektura Zabbix składa się z kilku głównych komponentów oprogramowania. Ich zadania opisano poniżej.

Serwer

Serwer Zabbix jest centralnym komponentem, do którego agenty raportują informacje o dostępności, integralności oraz statystyki. Serwer jest centralnym repozytorium, w którym przechowywane są wszystkie dane konfiguracyjne, statystyczne i operacyjne.

Przechowywanie w bazie danych

Wszystkie informacje konfiguracyjne, a także dane gromadzone przez Zabbix, są przechowywane w bazie danych.

Interfejs webowy

Aby zapewnić łatwy dostęp do Zabbix z dowolnego miejsca i z dowolnej platformy, udostępniany jest interfejs oparty na technologii web. Interfejs jest częścią serwera Zabbix i zwykle (choć niekoniecznie) działa na tej samej fizycznej maszynie co serwer.

Proxy

Zabbix proxy może zbierać dane o wydajności i dostępności w imieniu serwera Zabbix. Proxy jest opcjonalną częścią wdrożenia Zabbix; może jednak być bardzo korzystny do rozłożenia obciążenia pojedynczego serwera Zabbix.

Agent

Agenty Zabbix są wdrażane na monitorowanych celach, aby aktywnie monitorować lokalne zasoby i aplikacje oraz raportować zebrane dane do serwera Zabbix. Od wersji Zabbix 4.4 dostępne są dwa typy agentów: Zabbix agent (lekkie rozwiązanie, obsługiwane na wielu platformach, napisane w C) oraz Zabbix agent 2 (dodatkowo elastyczny, łatwo rozszerzalny za pomocą wtyczek, napisany w Go).

Przepływ danych Ponadto ważne jest, aby zrobić krok wstecz i przyjrzeć się ogólnemu przepływowi danych w Zabbix. Aby utworzyć pozycja, która zbiera dane, należy najpierw utworzyć host. Przechodząc na drugi koniec spektrum Zabbix, aby utworzyć wyzwalacz, trzeba najpierw mieć pozycja. Aby utworzyć akcję, trzeba mieć wyzwalacz. Zatem jeśli chcesz otrzymać alert, że obciążenie CPU jest zbyt wysokie na *Serwerze X*, musisz najpierw utworzyć wpis hosta dla *Serwera X*, następnie pozycja do monitorowania jego CPU, potem wyzwalacz, który aktywuje się, jeśli obciążenie CPU jest zbyt wysokie, a na końcu akcję, która wyśle Ci wiadomość e-mail. Choć może się wydawać, że to wiele kroków, przy użyciu szablonów wcale tak nie jest. Jednak dzięki takiej konstrukcji możliwe jest utworzenie bardzo elastycznej konfiguracji.

Funkcje Zabbix to wysoce zintegrowane rozwiązanie do monitorowania sieci, oferujące wiele funkcji w jednym pakiecie.

Zbieranie danych

- sprawdzanie dostępności i wydajności
- obsługa SNMP (zarówno trapów, jak i odpytywania), IPMI, JMX, monitorowania VMware
- kontrole niestandardowe
- zbieranie wymaganych danych w niestandardowych interwałach
- realizowane przez serwer/proxy oraz przez agenty

Elastyczne definicje progów

- można definiować bardzo elastyczne progi problemów, zwane wyzwalaczami, odwołujące się do wartości z bazy danych backendu

Wysoce konfigurowalne alertowanie

- wysyłanie powiadomień można dostosować pod kątem harmonogramu eskalacji, odbiorcy i typu nośnika
- powiadomienia mogą być bardziej zrozumiałe i pomocne dzięki użyciu zmiennych makr
- automatyczne akcje obejmują polecenia zdalne

Tworzenie wykresów w czasie rzeczywistym

- monitorowane pozycje są natychmiast przedstawiane na wykresach przy użyciu wbudowanej funkcji tworzenia wykresów

Możliwości monitorowania stron WWW

- Zabbix może śledzić ścieżkę symulowanych kliknięć myszą na stronie WWW i sprawdzać jej działanie oraz czas odpowiedzi

Rozbudowane opcje wizualizacji

- możliwość tworzenia niestandardowych wykresów, które mogą łączyć wiele pozycji w jednym widoku
- mapy sieci
- pokazy slajdów w stylu przeglądu pulpitu
- raporty
- widok monitorowanych zasobów na wysokim poziomie (biznesowym)

Przechowywanie danych historycznych

- dane przechowywane w bazie danych
- konfigurowalna historia
- wbudowana procedura housekeeping

Łatwa konfiguracja

- dodawanie monitorowanych urządzeń jako hostów
- hosty są obejmowane monitorowaniem po dodaniu do bazy danych
- stosowanie szablonów do monitorowanych urządzeń

Użycie szablonów

- grupowanie kontroli w szablonach
- szablony mogą dziedziczyć po innych szablonach

Wykrywanie sieci

- automatyczne wykrywanie urządzeń sieciowych
- autorejestracja agenta
- wykrywanie systemów plików, interfejsów sieciowych i OID-ów SNMP

Szybki interfejs WWW

- frontend oparty na WWW w PHP
- dostępny z dowolnego miejsca
- umożliwia intuicyjną nawigację przez klikanie
- dziennik audytu

Zabbix API

- Zabbix API zapewnia programowalny interfejs do Zabbix na potrzeby masowych operacji, integracji z oprogramowaniem firm trzecich i innych zastosowań.

System uprawnień

- bezpieczne uwierzytelnianie użytkowników
- niektórzy użytkownicy mogą być ograniczeni do określonych widoków

W pełni funkcjonalny i łatwo rozszerzalny agent

- wdrażany na monitorowanych celach
- może być wdrażany zarówno w systemach Linux, jak i Windows

Demony binarne

- napisane w C, dla wysokiej wydajności i małego zużycia pamięci
- łatwe do przenoszenia

Gotowość do złożonych środowisk

- zdalne monitorowanie jest łatwe dzięki użyciu Zabbix proxy

Słownik W tej sekcji możesz poznać znaczenie niektórych terminów powszechnie używanych w Zabbix.

host

- dowolne fizyczne lub wirtualne urządzenie, aplikacja, usługa lub dowolny inny logicznie powiązany zbiór monitorowanych parametrów.

host group

- logiczne grupowanie hostów. Grupy hostów są używane podczas przypisywania praw dostępu do hostów dla różnych grup użytkowników.

item

- konkretny fragment danych, który chcesz otrzymywać z hosta, metryka danych.

value preprocessing

- przekształcenie otrzymanej wartości metryki przed zapisaniem jej do bazy danych.

trigger

- wyrażenie logiczne definiujące próg problemu i używane do „oceny” danych otrzymywanych w pozycjach.

Gdy otrzymane dane są powyżej progu, wyzwalacze przechodzą ze stanu „Ok” do stanu „Problem”. Gdy otrzymane dane są poniżej progu, wyzwalacze pozostają w stanie „Ok” lub do niego wracają.

template

- zestaw encji (pozycji, wyzwalaczy, wykresów, reguł wykrywania niskiego poziomu, scenariuszy WWW) gotowych do zastosowania do jednego lub kilku hostów.

Zadaniem szablonów jest przyspieszenie wdrażania zadań monitorowania na hoście, a także ułatwienie stosowania masowych zmian w zadaniach monitorowania. Szablony są łączone bezpośrednio z poszczególnymi hostami.

template group

- logiczne grupowanie szablonów. Grupy szablonów są używane podczas przypisywania praw dostępu do szablonów dla różnych grup użytkowników.

event

- pojedyncze wystąpienie czegoś, co zasługuje na uwagę, takiego jak zmiana stanu wyzwalacza lub wykrycie/automatyczna rejestracja agenta.

event tag

- wstępnie zdefiniowany znacznik zdarzenia. Może być używany w korelacji zdarzeń, granulacji uprawnień itp.

event correlation

- metoda elastycznego i precyzyjnego korelowania problemów z ich rozwiązaniem.

Na przykład możesz zdefiniować, że problem zgłoszony przez jeden wyzwalacz może zostać rozwiązany przez inny wyzwalacz, który może nawet używać innej metody zbierania danych.

problem

- wyzwalacz znajdujący się w stanie „Problem".

problem update

- opcje zarządzania problemem udostępniane przez Zabbix, takie jak dodanie komentarza, potwierdzenie, zmiana ważności lub ręczne zamknięcie.

action

- wstępnie zdefiniowany sposób reagowania na zdarzenie.

Akcja składa się z operacji (np. wysłania powiadomienia) oraz warunków (*kiedy* operacja jest wykonywana)

escalation

- niestandardowy scenariusz wykonywania operacji w ramach akcji; sekwencja wysyłania powiadomień/wykonywania zdalnych poleceń.

macro

- symbol zastępczy zmiennej, który jest rozwijany do określonej wartości w zależności od kontekstu.

media

- środek dostarczania powiadomień; kanał dostarczania.

notification

- wiadomość o jakimś zdarzeniu wysłana do użytkownika za pośrednictwem wybranego kanału mediów.

remote command

- wstępnie zdefiniowane polecenie, które jest automatycznie wykonywane na monitorowanym hoście po spełnieniu określonego warunku.

web scenario

- jedno lub kilka żądań HTTP służących do sprawdzenia dostępności witryny internetowej.

frontend

- interfejs WWW dostarczany z Zabbix.

dashboard

- konfigurowalna sekcja interfejsu WWW wyświetlająca podsumowania i wizualizacje ważnych informacji w jednostkach wizualnych zwanych widżetami.

widget

- jednostka wizualna wyświetlająca informacje określonego rodzaju i źródła (podsumowanie, mapa, wykres, zegar itp.), używana na pulpicie.

Zabbix API

- Zabbix API umożliwia używanie protokołu JSON RPC do tworzenia, aktualizowania i pobierania obiektów Zabbix (takich jak hosty, pozycje, wykresy i inne) lub wykonywania dowolnych innych niestandardowych zadań.

Zabbix server

- *centralny proces oprogramowania Zabbix, który wykonuje monitorowanie, współdziała z proxy Zabbix i agentami, oblicza wyzwalacze, wysyła powiadomienia; centralne repozytorium danych.*

Zabbix proxy

- *proces, który może zbierać dane w imieniu serwera Zabbix, przejmując część obciążenia przetwarzania z serwera.*

Zabbix agent

- *proces wdrożony na monitorowanych celach w celu aktywnego monitorowania lokalnych zasobów i aplikacji.*

Zabbix agent 2

- *nowa generacja agenta Zabbix do aktywnego monitorowania lokalnych zasobów i aplikacji, umożliwiająca używanie niestandardowych wtyczek do monitorowania.*

> **Attention:**
> Ponieważ Zabbix agent 2 współdzieli znaczną część funkcjonalności z Zabbix agent, termin „Zabbix agent" w dokumentacji oznacza oba - Zabbix agent i Zabbix agent 2, jeśli zachowanie funkcjonalne jest takie samo. Zabbix agent 2 jest wymieniany osobno tylko wtedy, gdy jego funkcjonalność się różni.

encryption

- *obsługa szyfrowanej komunikacji między komponentami Zabbix (serwer, proxy, agent, narzędzia zabbix_sender i zabbix_get)* z użyciem protokołu Transport Layer Security (TLS).

agent autoregistration

- *zautomatyzowany proces, w którym agent Zabbix sam rejestruje się* jako host i rozpoczyna monitorowanie.

network discovery

- *zautomatyzowane wykrywanie urządzeń sieciowych*.

low-level discovery

- *zautomatyzowane wykrywanie encji niskiego poziomu na określonym urządzeniu* (np. systemów plików, interfejsów sieciowych itp.).

low-level discovery rule

- *zestaw definicji do zautomatyzowanego wykrywania encji niskiego poziomu* na urządzeniu.

item prototype

- *metryka z określonymi parametrami jako zmiennymi, gotowa do wykrywania niskiego poziomu*. Po wykryciu niskiego poziomu zmienne są automatycznie zastępowane rzeczywistymi wykrytymi parametrami, a metryka automatycznie rozpoczyna zbieranie danych.

trigger prototype

- *wyzwalacz z określonymi parametrami jako zmiennymi, gotowy do wykrywania niskiego poziomu*. Po wykryciu niskiego poziomu zmienne są automatycznie zastępowane rzeczywistymi wykrytymi parametrami, a wyzwalacz automatycznie rozpoczyna ocenę danych.

Prototypy niektórych innych encji Zabbix są również używane w wykrywaniu niskiego poziomu - prototypy wykresów, prototypy hostów, prototypy grup hostów.

Zabbix Cloud

Zabbix Cloud

Poznaj dostępne opcje konfiguracji i mechanizmy kontroli dostępu dla organizacji oraz węzłów w Zabbix Cloud.

Konfiguracja i zarządzanie Zabbix Cloud

Rozpocznij korzystanie z Zabbix Cloud Instrukcje krok po kroku, które pomogą szybko uruchomić instancję Zabbix Cloud, w tym przeprowadzić wstępną konfigurację i podłączyć monitorowane urządzenia.

Konfiguracja węzła Dowiedz się, jak skonfigurować węzeł Zabbix Cloud, koncentrując się na dostępie, obsłudze danych i ustawieniach zasobów.

Dodawanie użytkowników Dowiedz się, jak dodawać użytkowników i przypisywać im role w organizacji Zabbix Cloud oraz jej węzłach.

Dowiedz się więcej o Zabbix Cloud

Zabbix Cloud a on-premises Porównaj różnice w zarządzaniu, skalowalności i utrzymaniu między tymi dwoma wdrożeniami i dowiedz się, które z nich może najpłynniej wspierać Twój przepływ pracy.

Poznaj Zabbix Cloud Zapoznaj się z przeglądem Zabbix Cloud, w tym z jego kluczowymi funkcjami, korzyściami oraz tym, co obejmuje subskrypcja. Odpowiedzi na często zadawane pytania dotyczące konfiguracji i użytkowania znajdziesz w FAQ.

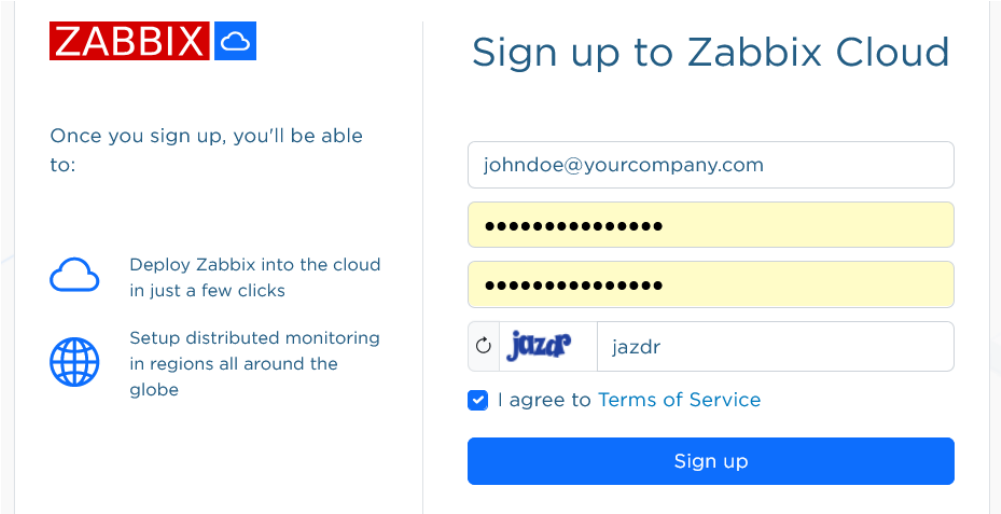
Wdróż Zabbix w chmurze

Aby uruchomić Zabbix w chmurze, wykonaj następujące kroki:

- Zaloguj się lub zarejestruj na cloud.zabbix.com
- Utwórz węzeł chmurowy
- Rozpocznij korzystanie z Zabbix w chmurze

Logowanie lub rejestracja Możesz zalogować się na cloud.zabbix.com przy użyciu istniejącego konta Google, GitHub lub Microsoft.

Alternatywnie przejdź do strony rejestracji, aby utworzyć konto.



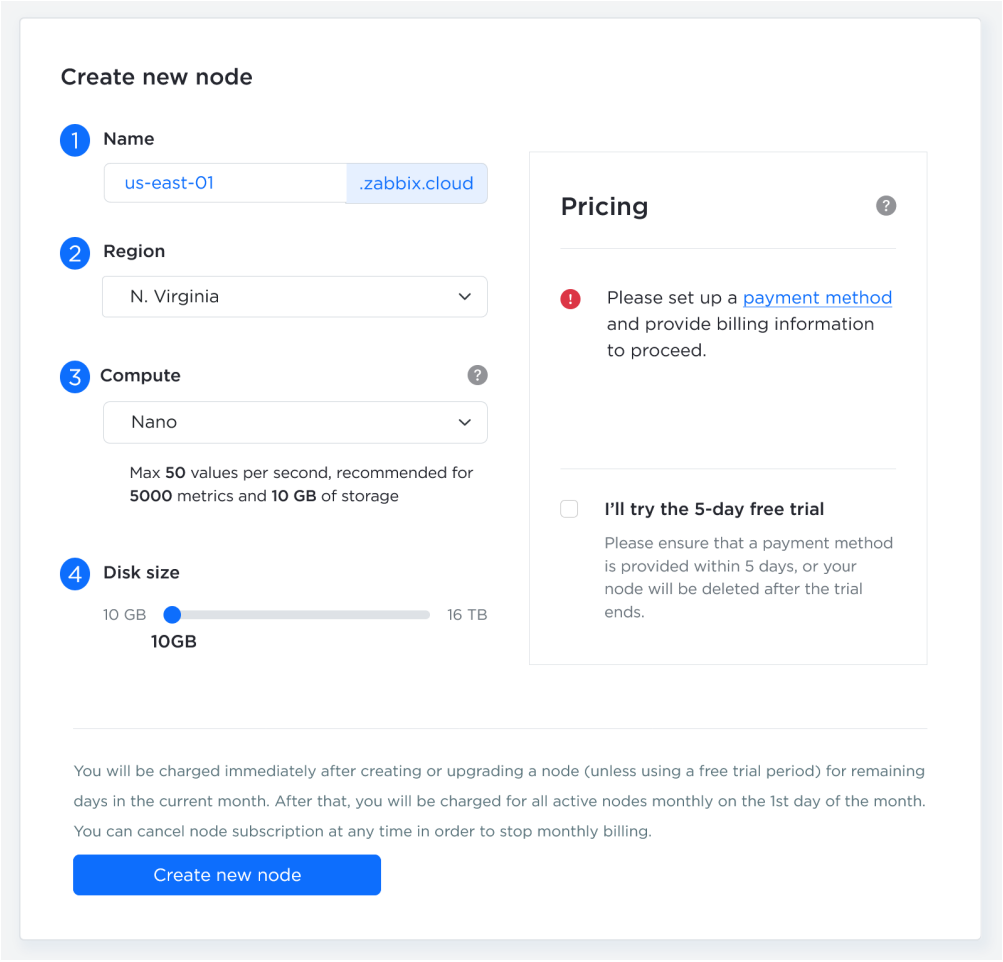
Po rejestracji otrzymasz w wiadomości e-mail potwierdzenie utworzenia nowego konta.

Przejdź do cloud.zabbix.com, aby się zalogować. Podczas logowania zostaniesz poproszony o jednorazowe hasło. Hasło to zostanie wysłane do Ciebie w wiadomości e-mail.

Tworzenie węzła chmurowego Węzeł chmurowy to instancja Zabbix działająca w chmurze. Obejmuje ona serwer Zabbix, bazę danych oraz frontend webowy.

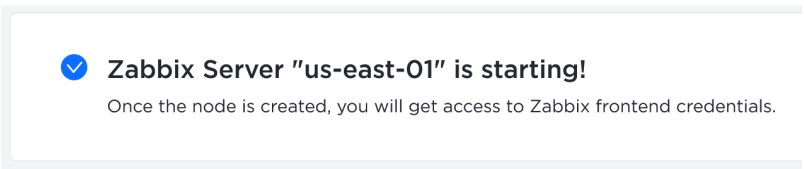
Po zalogowaniu zobaczysz, że dla Twojego konta domyślnie istnieje już organizacja *Private*. Domyślną organizację możesz później zmienić.

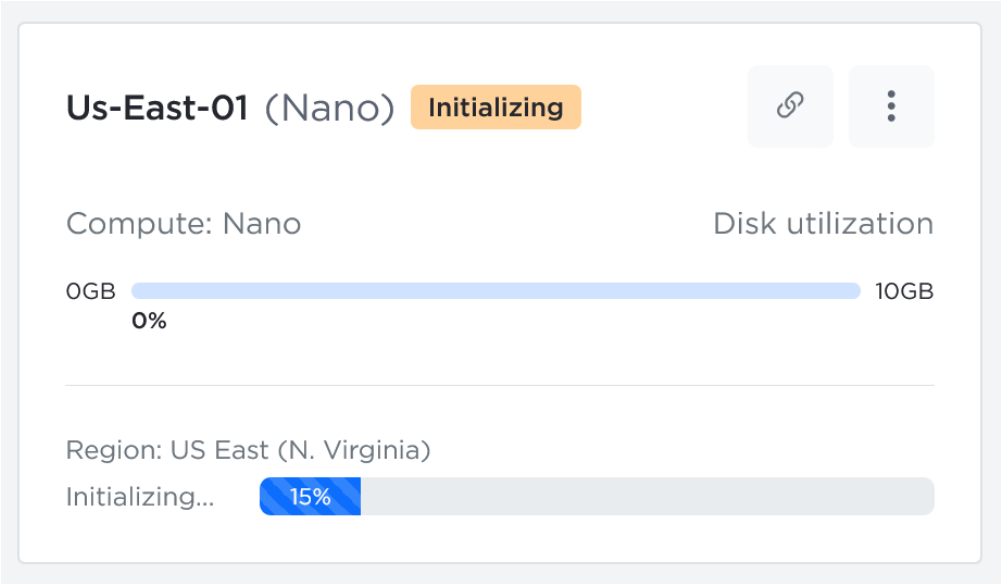
Kliknij *Create New Node*. Otworzy się formularz konfiguracji węzła.

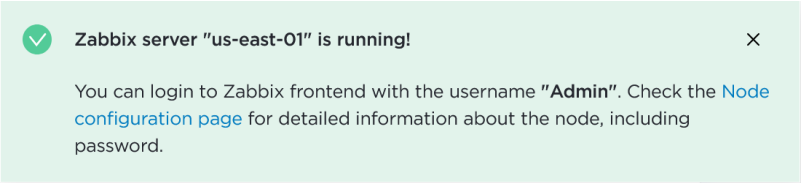


Parametr	Opis
Name	Wybierz unikalną nazwę węzła. Nazwa węzła tworzy unikalny adres URL serwera/frontendu chmurowego w formacie `<your-name>.zabbix.cloud`.
Region	Wybierz najbliższą lokalizację centrum danych, aby zminimalizować opóźnienia sieciowe.
Compute	Wybierz moc obliczeniową dla węzła. Aby określić, jaki poziom zasobów jest potrzebny, zobacz szczegóły cenowe. W razie potrzeby zawsze możesz później zwiększyć zasoby. Przed utworzeniem węzła innego niż próbny wymagane będzie skonfigurowanie metody płatności. Dodaj informacje rozliczeniowe w menu *Billing*. Dostępny jest 5-dniowy **bezpłatny okres próbny** umożliwiający wypróbowanie węzła poziomu *Nano*. W okresie próbnym nie zostaniesz obciążony opłatami, jednak po jego zakończeniu węzeł zostanie usunięty, jeśli nie zostanie przekształcony w węzeł płatny.
Disk size	Suwak domyślnie ustawiony jest na zalecane minimum zależne od poziomu. Zwiększ tę wartość, jeśli przechowujesz duże ilości historii lub trendów. Pamiętaj, że większe dyski wiążą się z wyższymi miesięcznymi kosztami oraz że nie możesz samodzielnie zmniejszyć rozmiaru dysku — aby go zmniejszyć, musisz skontaktować się z pomocą techniczną.

Po wypełnieniu formularza kliknij *Create New Node*. Podczas inicjalizacji węzła wyświetlany jest odpowiedni komunikat, a sam węzeł jest już widoczny w sekcji Organizations.





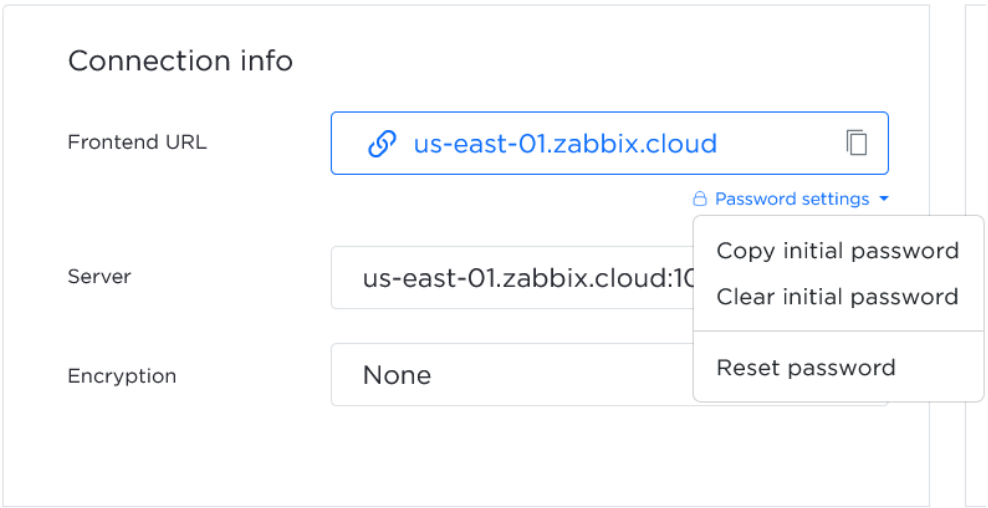


Rozpocznij korzystanie z Zabbix

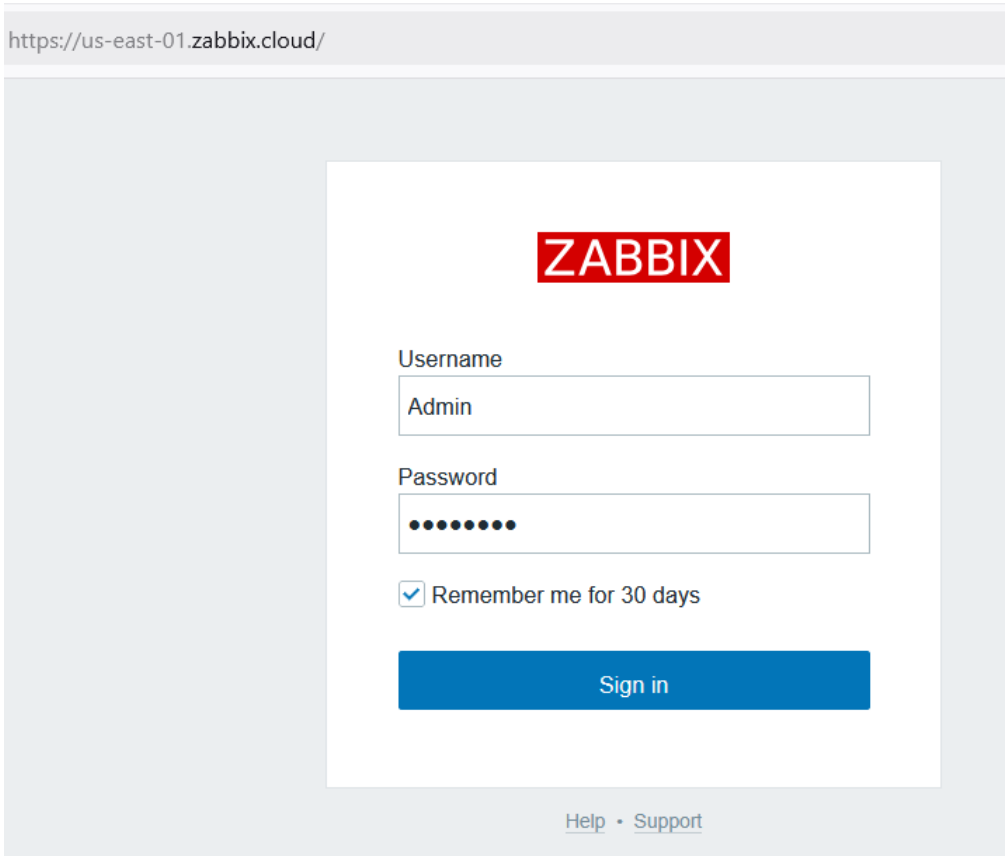
Gdy status węzła zmieni się z *Initializing* na *Running*, możesz zalogować się do frontend Zabbix.

Aby uzyskać dostęp do początkowego hasła frontend, kliknij utworzony węzeł.

Zostaniesz przeniesiony do ustawień węzła (przegląd, filtry dostępu, szyfrowanie, kopie zapasowe itp.). W sekcji **Connection info** kliknij *Password settings* i wybierz *Copy initial password* z listy rozwijanej.



Kliknij adres URL frontend, aby otworzyć frontend Zabbix (`us-east-01.zabbix.cloud`).



Zaloguj się, używając następujących danych logowania:

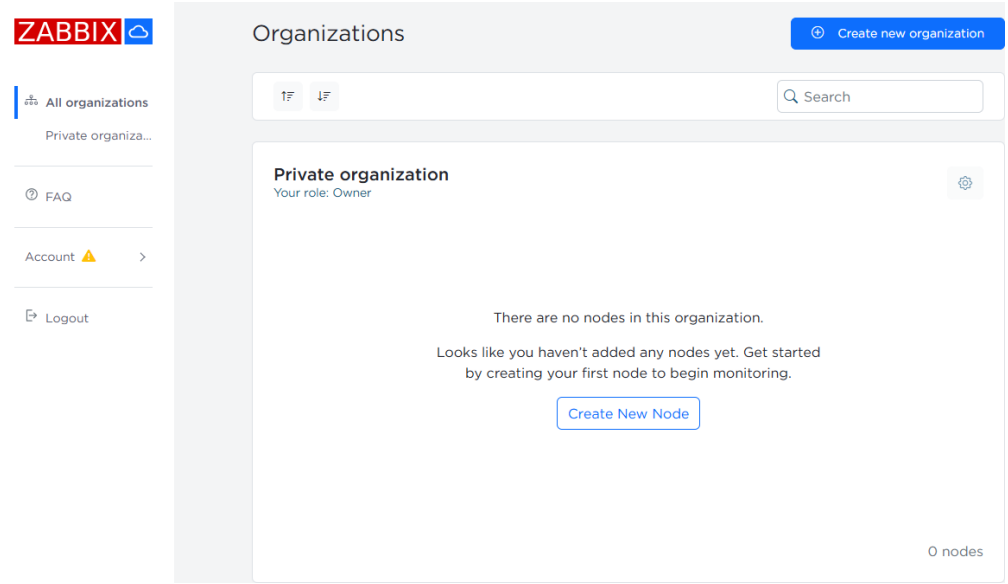
- *Username* - `Admin`
- *Password* - podaj początkowe hasło (np. HzTG9t7Y)

Aby rozpocząć monitorowanie, musisz zdefiniować filtry dostępu — adres IP lub adresy, którym wolno łączyć się z serwerem chmurowym Zabbix. Należy zdefiniować co najmniej jeden.

Zarządzanie organizacją Organizacja jest kontenerem dla jednego lub większej liczby węzłów. Organizacje pomagają również porządkować zasoby i delegować obowiązki, takie jak:

- Zarządzanie węzłami
- Rozliczenia

Po zalogowaniu do Zabbix Cloud wyświetlana jest strona *Wszystkie organizacje*. Domyślnie dla Twojego konta tworzona jest prywatna organizacja.



Jako właściciel tej organizacji możesz zarządzać użytkownikami, administratorami, węzłami oraz nazwą organizacji. Kliknij przycisk

ustawień  , aby uzyskać dostęp do opcji zarządzania.

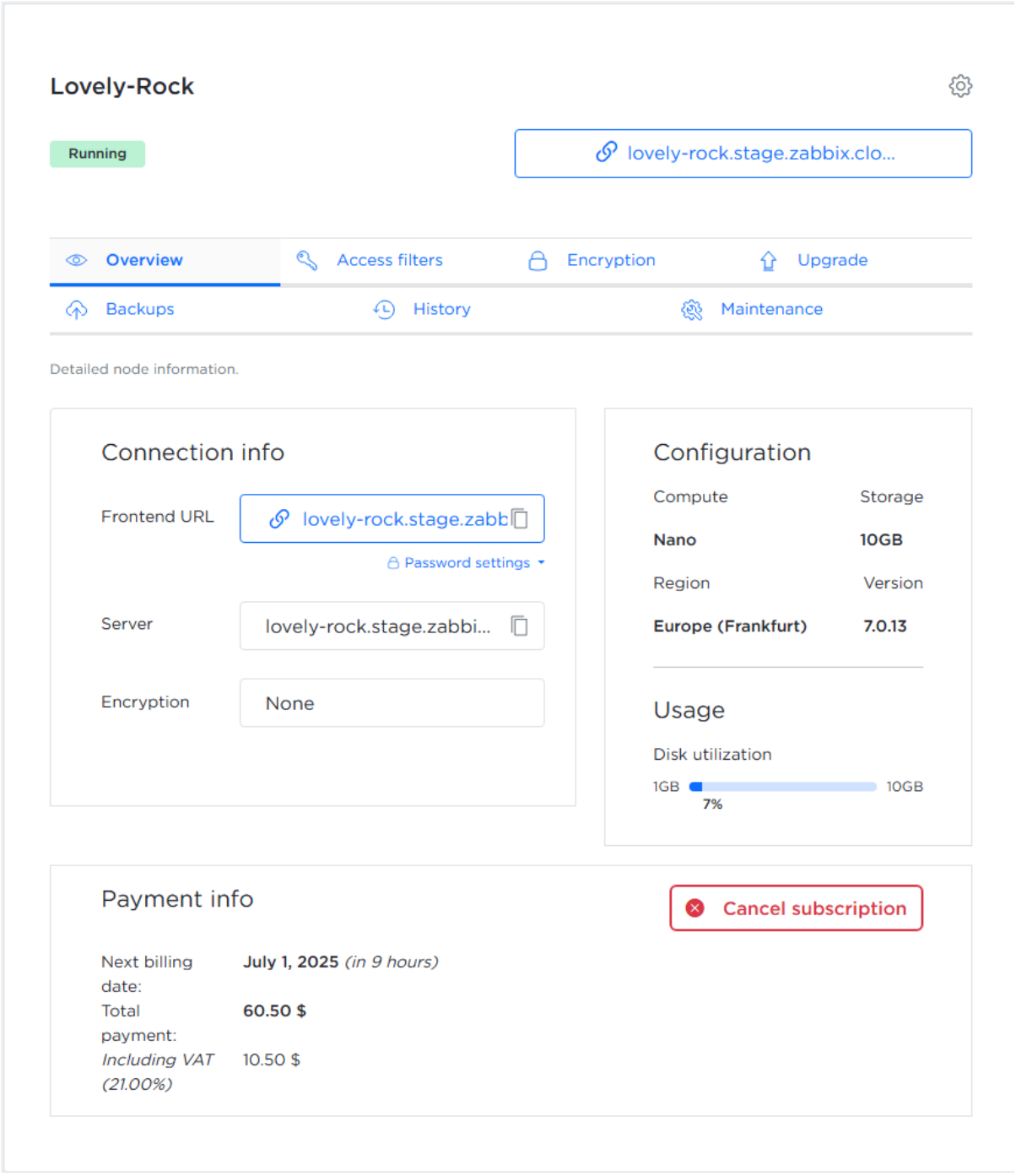
Konfiguracja węzła

Przegląd

Aby uzyskać dostęp do strony konfiguracji węzła, kliknij węzeł w sekcji *All organizations*, z poziomu menu organizacji lub użyj linku *Node configuration page* wyświetlanego po uruchomieniu węzła.

W widoku konfiguracji węzła każda karta umożliwia zarządzanie określonym aspektem węzła:

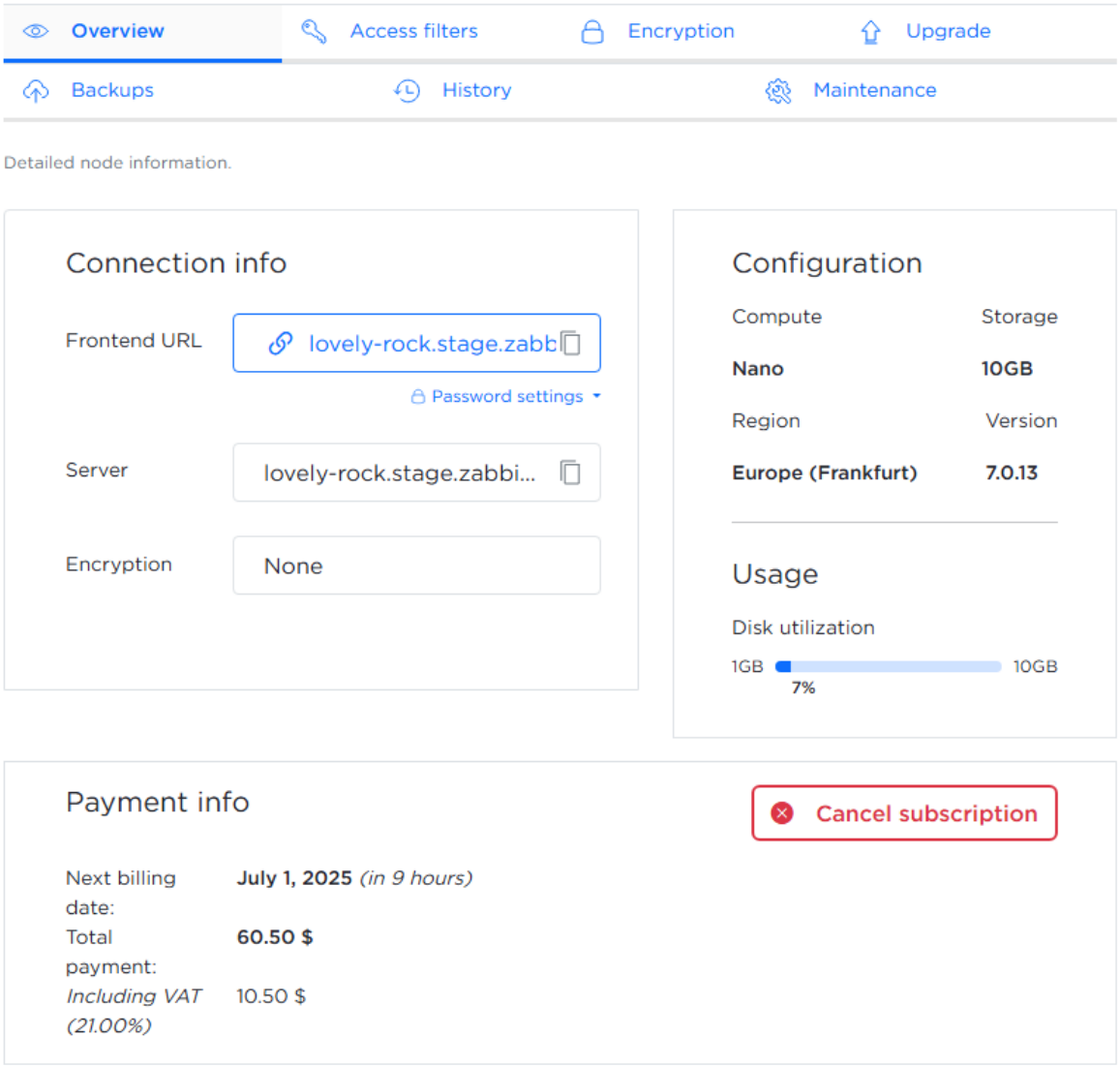
- Przegląd — wyświetlanie szczegółów węzła, otwieranie jego frontend oraz zarządzanie użytkownikami węzła.
- Filtry dostępu — kontrola dostępu według adresu IP lub podsieci.
- Szyfrowanie — konfiguracja TLS przez przesyłanie certyfikatów, kluczy i opcjonalnych list CRL.
- Kopie zapasowe — tworzenie, przywracanie i usuwanie migawek węzła; wyświetlanie terminu następnej zaplanowanej kopii zapasowej.
- Historia — ustawianie okresów retencji dla dzienników audytu, historii i trendów, z predefiniowanymi jednostkami oraz limitem aktualizacji 3 razy dziennie.
- Konserwacja — definiowanie cotygodniowych okien konserwacyjnych według strefy czasowej, dnia i godziny.
- Aktualizacja — skalowanie zasobów obliczeniowych/pamięci masowej lub zarządzanie statusem wersji próbnej/płatności.



Note:
Niektóre karty mogą być niedostępne w zależności od typu użytkownika, który wyświetla stronę, oraz statusu węzła (wersja próbna/niepróbna).

Karta Przegląd

Karta *Przegląd* zawiera szczegółowe informacje o węźle.



Jest podzielona na trzy sekcje:

Informacje o połączeniu:

- Klikalny adres URL frontend z opcją kopiowania do schowka
- Ustawienia hasła
- Bieżąca metoda szyfrowania

Konfiguracja i użycie:

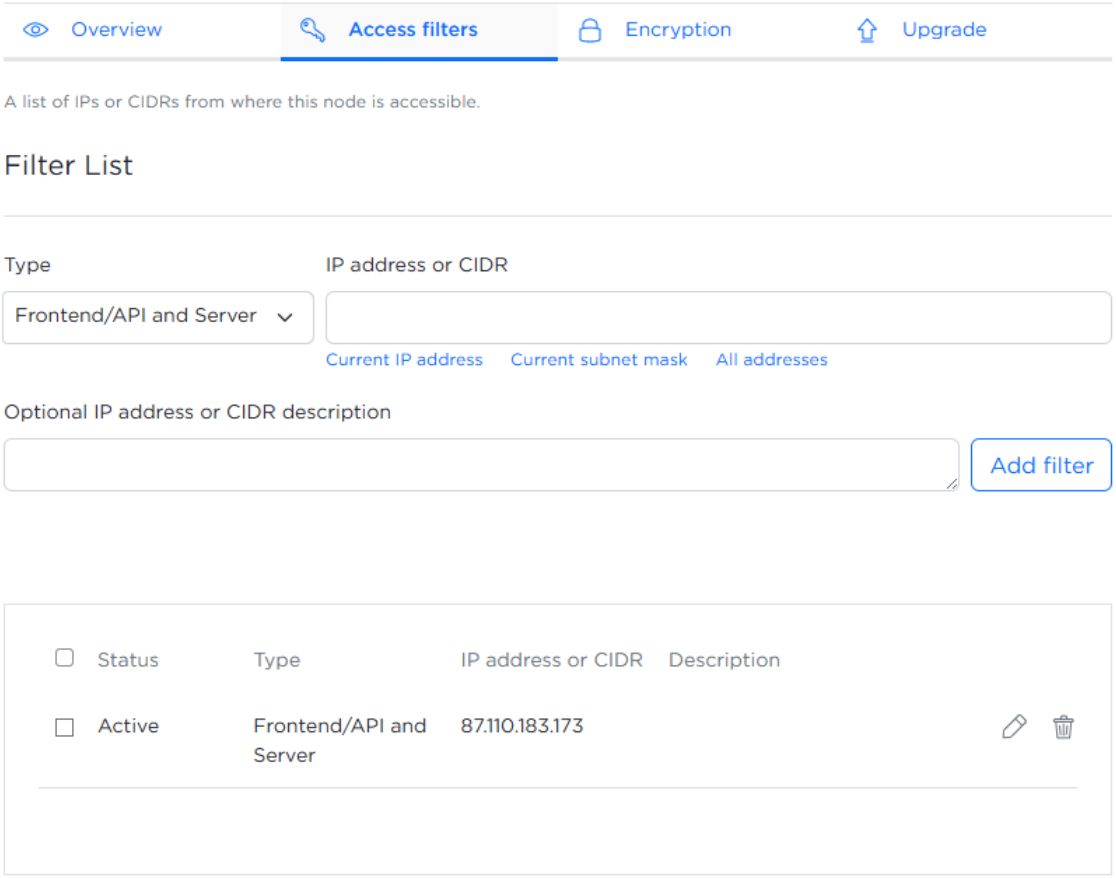
- Poziom mocy obliczeniowej, maksymalna przestrzeń dyskowa, region
- Wersja komponentów Zabbix
- Wykorzystanie dysku

Informacje o węźle/Informacje o płatności:

- Data wygaśnięcia (dla węzłów testowych i przedpłaconych)
- Po zakończeniu inicjalizacji węzła wyświetlany jest przycisk zależny od kontekstu, w zależności od typu węzła: - *Przejdź na plan płatny* - dostępne dla węzłów w bezpłatnym okresie próbnym - *Anuluj subskrypcję* - dostępne dla płatnych węzłów z aktywną subskrypcją - *Ponownie zasubskrybuj plan płatny* - wyświetlane, jeśli subskrypcja została anulowana - Dla węzłów przedpłaconych nie jest wyświetlany żaden przycisk akcji, ponieważ mają długi okres ważności i nie można ich anulować

Karta filtrów dostępu

Karta *Filtry dostępu* umożliwia ograniczenie dostępu do węzła Zabbix na podstawie adresu IP lub podsieci.



Aby skonfigurować filtr dostępu, uzupełnij następujące pola:

- *Typ* — użyj listy rozwijanej, aby wybrać, który komponent Zabbix ma zostać ograniczony: tylko frontend/API, tylko serwer lub oba.
- *Adres IP lub CIDR* — wprowadź adres IP lub CIDR ręcznie albo uzupełnij pole automatycznie, wybierając odpowiednią opcję.
- *Opcjonalny opis adresu IP lub CIDR* — dodaj opcjonalny opis dla każdego adresu IP lub podsieci.

Po uzupełnieniu pól kliknij *Dodaj filtr*.
Dodane filtry pojawią się w poniższej tabeli, zawierającej status, typ, adres IP lub podsieć oraz opis.

Warning:
Podczas inicjalizacji węzła filtr dostępu dla użytego adresu IP jest tworzony automatycznie. Jeśli później połączysz się z innego adresu IP lub z innej sieci, musisz dodać ten adres tutaj, w przeciwnym razie dostęp zostanie zablokowany.

Możesz:

- — edytować filtr.
- — usunąć filtr lub wiele filtrów za pomocą pól wyboru.

Karta Szyfrowanie

Karta *Szyfrowanie* umożliwia skonfigurowanie TLS encryption między komponentami Zabbix przez przesłanie wymaganych plików certyfikatów.

Aby włączyć bezpieczną komunikację z użyciem certyfikatów, wybierz *CERTIFICATE* i prześlij z komputera następujące pliki:

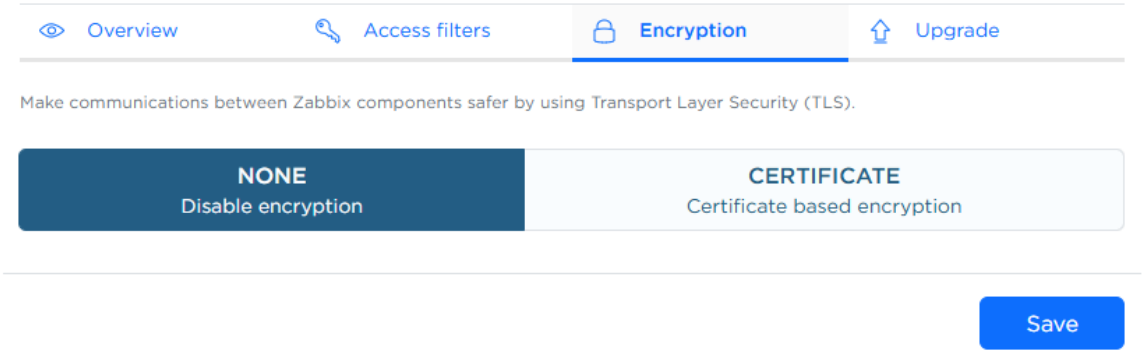
- *Certyfikaty głównego urzędu certyfikacji (Root CA)* — używane do weryfikacji autentyczności certyfikatów drugiej strony. Kliknij *Choose file* i wybierz plik zawierający zaufane certyfikaty głównego urzędu certyfikacji (zwykle plik `.crt` lub `.pem`, zakodowany w formacie PEM).

- *Łańcuch certyfikatów* — reprezentuje łańcuch zaufania dla własnego certyfikatu.
  Kliknij *Choose file* i wybierz plik zakodowany w formacie PEM (np. `.crt` lub `.pem`), który zawiera Twój certyfikat oraz wszystkie pośrednie certyfikaty CA.

- *Klucz prywatny* — klucz prywatny odpowiadający Twojemu certyfikatowi.
  Kliknij *Choose file* i wybierz plik `.key` zakodowany w formacie PEM.

- *Unieważnione certyfikaty* (opcjonalnie) — jeśli utrzymujesz listę unieważnionych certyfikatów (CRL), kliknij *Choose file* i wybierz plik CRL, aby wskazać certyfikaty, które nie powinny być już uznawane za zaufane.

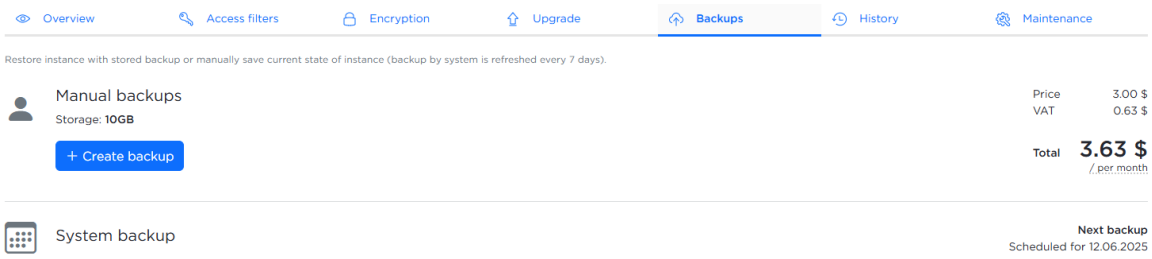
Po wybraniu plików kliknij *Save*. Pliki zostaną przesłane, zweryfikowane i zastosowane do skonfigurowania szyfrowania TLS między komponentami Zabbix.



Karta Kopie zapasowe

Karta *Kopie zapasowe* umożliwia przeglądanie, tworzenie, przywracanie i usuwanie kopii zapasowych węzła Zabbix.

Możesz przywrócić instancję z dowolnej zapisanej kopii zapasowej lub w dowolnym momencie utworzyć nową ręczną kopię zapasową.
Karta pokazuje również datę następnej zaplanowanej kopii zapasowej.



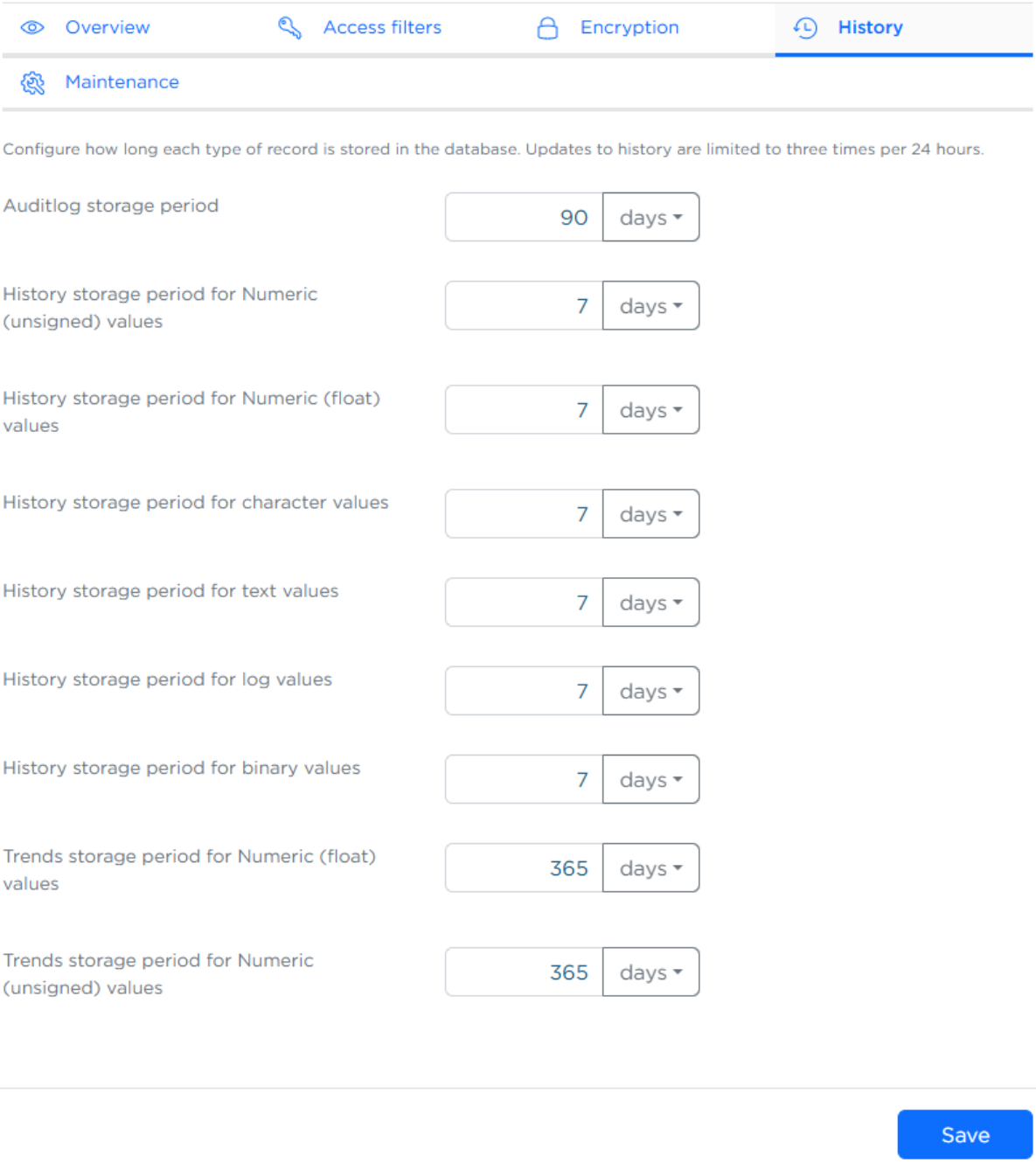
Aby utworzyć kopię zapasową:

1. Kliknij przycisk *Create backup*.
2. W wyskakującym oknie wprowadź opcjonalny opis.
3. Kliknij *Create*, aby potwierdzić.

Warning:
Dodatkowe kopie zapasowe są rozliczane miesięcznie na podstawie wykorzystania przestrzeni dyskowej.

Karta Historia

Karta *Historia* umożliwia skonfigurowanie, jak długo przechowywane są różne typy danych historycznych.



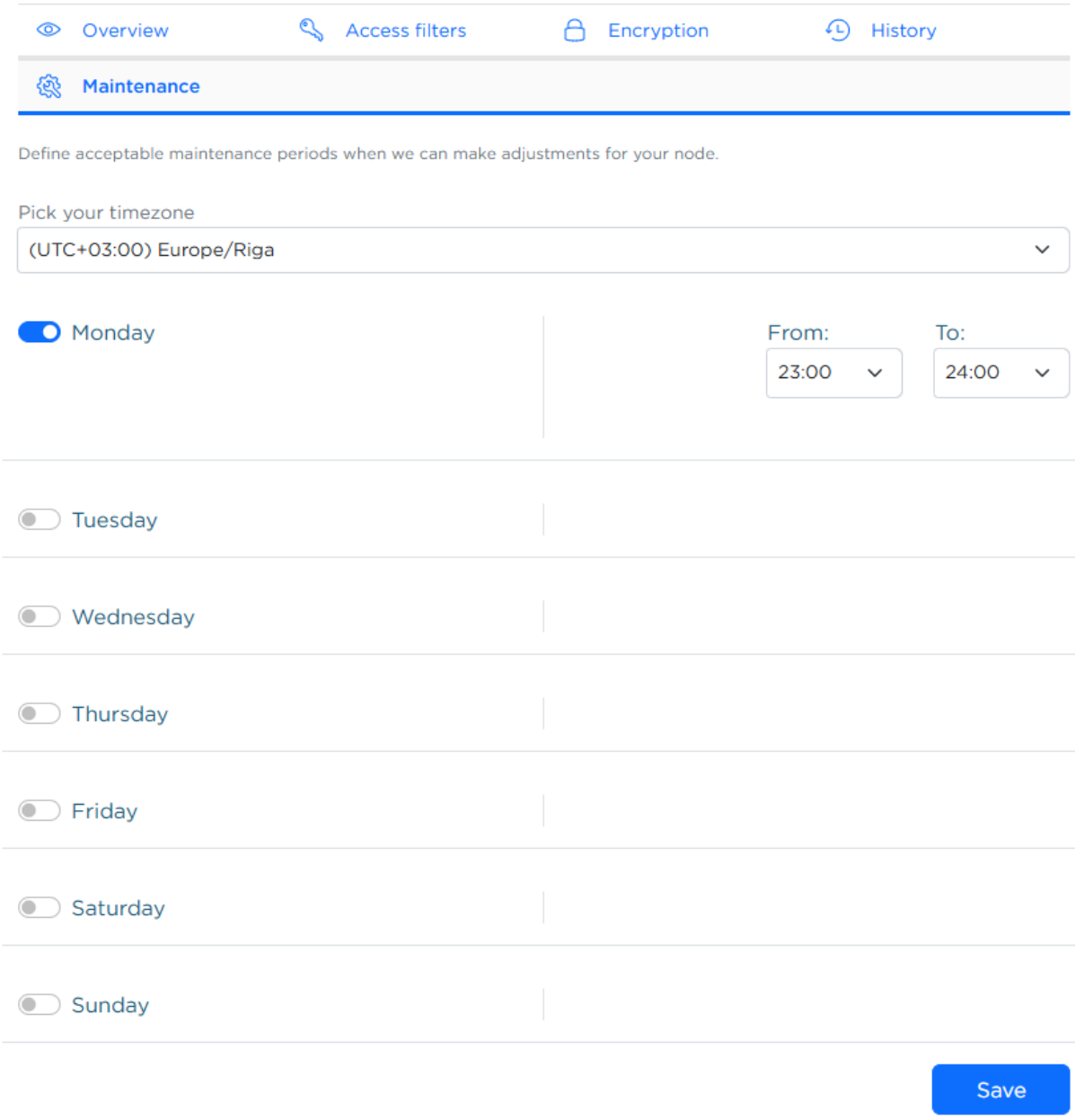
Możesz ustawić okres przechowywania dla każdego typu danych (np. dane liczbowe, tekst, logi) oraz wybrać jednostkę (dni, miesiące, lata). Zmiany można wprowadzać maksymalnie trzy razy w ciągu 24 godzin.

Po zaktualizowaniu wartości kliknij *Zapisz*, aby zastosować zmiany.

Warning:
Dłuższe okresy przechowywania mogą zwiększyć wykorzystanie przestrzeni dyskowej i mogą wpływać na wydajność. Zaleca się konfigurowanie okresów przechowywania na podstawie rzeczywistych danych i potrzeb analitycznych.
 Zabbix Cloud używa partycjonowania bazy danych do zarządzania przechowywaniem danych zamiast tradycyjnego mechanizmu housekeeping w Zabbix. Umożliwia to szybsze działanie i bardziej przewidywalną obsługę retencji danych.

Karta Konserwacja

Karta *Konserwacja* umożliwia zdefiniowanie akceptowalnych okien konserwacyjnych, w których na węźle mogą być wykonywane aktualizacje lub dostosowania.

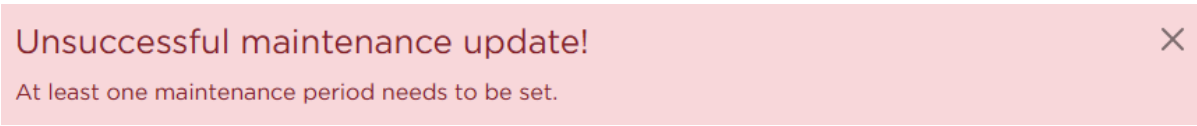


Należy:

- Wybrać strefę czasową z listy rozwijanej.
- Wybrać co najmniej jeden dzień i jedno godzinne okno konserwacyjne.

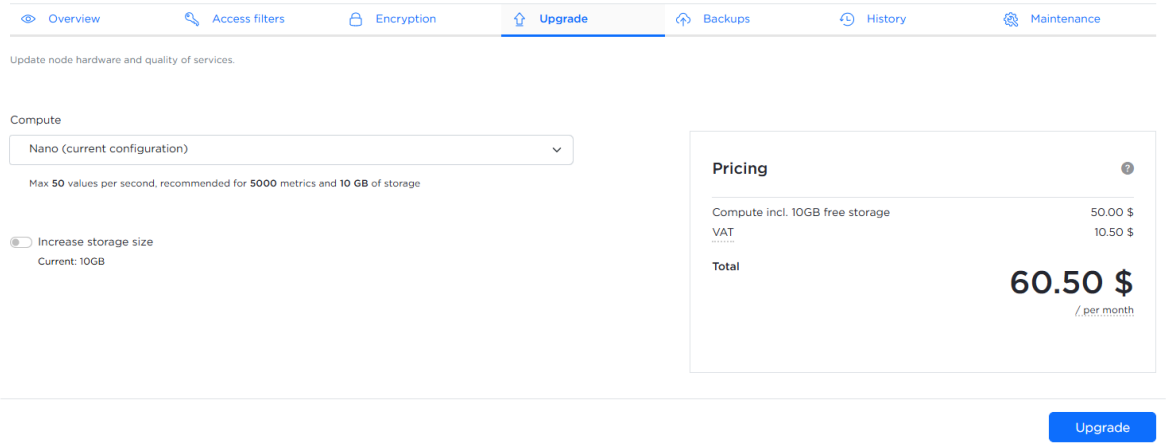
Kliknij *Zapisz*, aby zastosować zmiany.

Jeśli nie zostanie wybrany żaden dzień ani okno czasowe, zostanie wyświetlony błąd.



Karta Upgrade

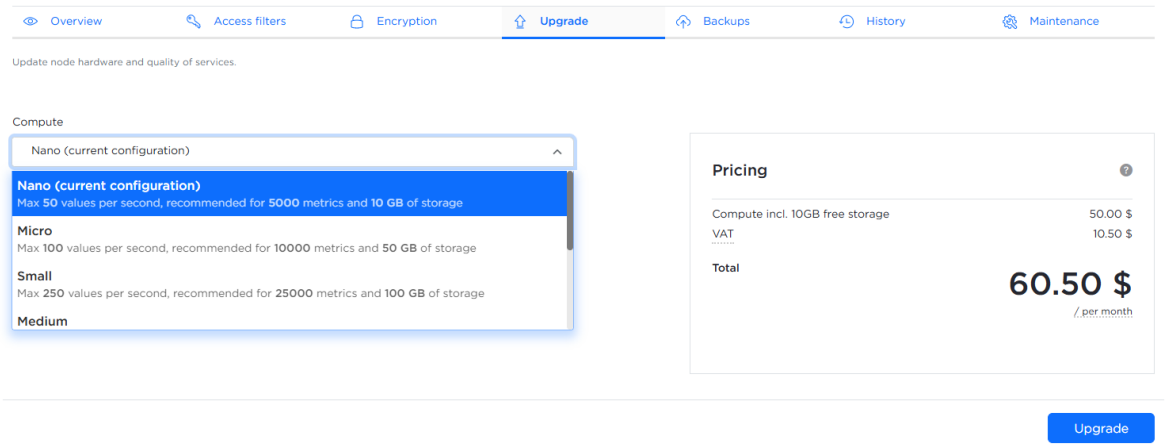
Karta *Upgrade* umożliwia skalowanie zasobów węzła lub zarządzanie jego subskrypcją.



Możesz zwiększyć poziom mocy obliczeniowej lub rozmiar dysku — pamiętaj, że rozmiar dysku można zwiększyć tylko raz na 24 godziny i nie można go zmniejszyć za pomocą interfejsu użytkownika (w przypadku próśb o zmniejszenie pojemności skontaktuj się ze wsparciem Zabbix).
Węzły w okresie próbnym można przekształcić w płatne subskrypcje.

Aby zwiększyć poziom mocy obliczeniowej:

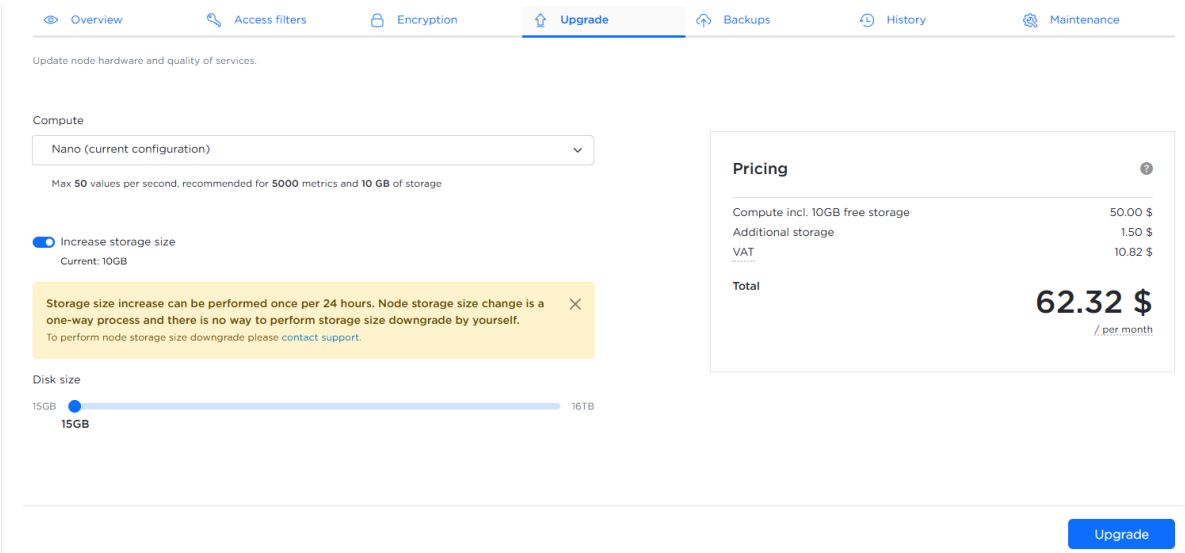
1. Kliknij listę rozwijaną *Compute*.



2. Wybierz żądaną konfigurację.
3. Kliknij przycisk *Upgrade*.

Aby zwiększyć rozmiar dysku:

1. Kliknij przycisk opcji *Increase storage size*.
2. Ustaw suwak *Disk size* na żądaną wartość.



3. Kliknij przycisk *Upgrade*.

Note:
Zaktualizowana całkowita cena miesięczna jest wyświetlana w tabeli *Pricing* przed potwierdzeniem zmian.

Dodawanie użytkowników

Wprowadzenie

Poniższe przykłady opisują, jak dodawać użytkowników do organizacji i węzłów.

Note:
Kopiowanie, czyszczenie i resetowanie hasła frontend może być wykonywane wyłącznie przez właściciela.

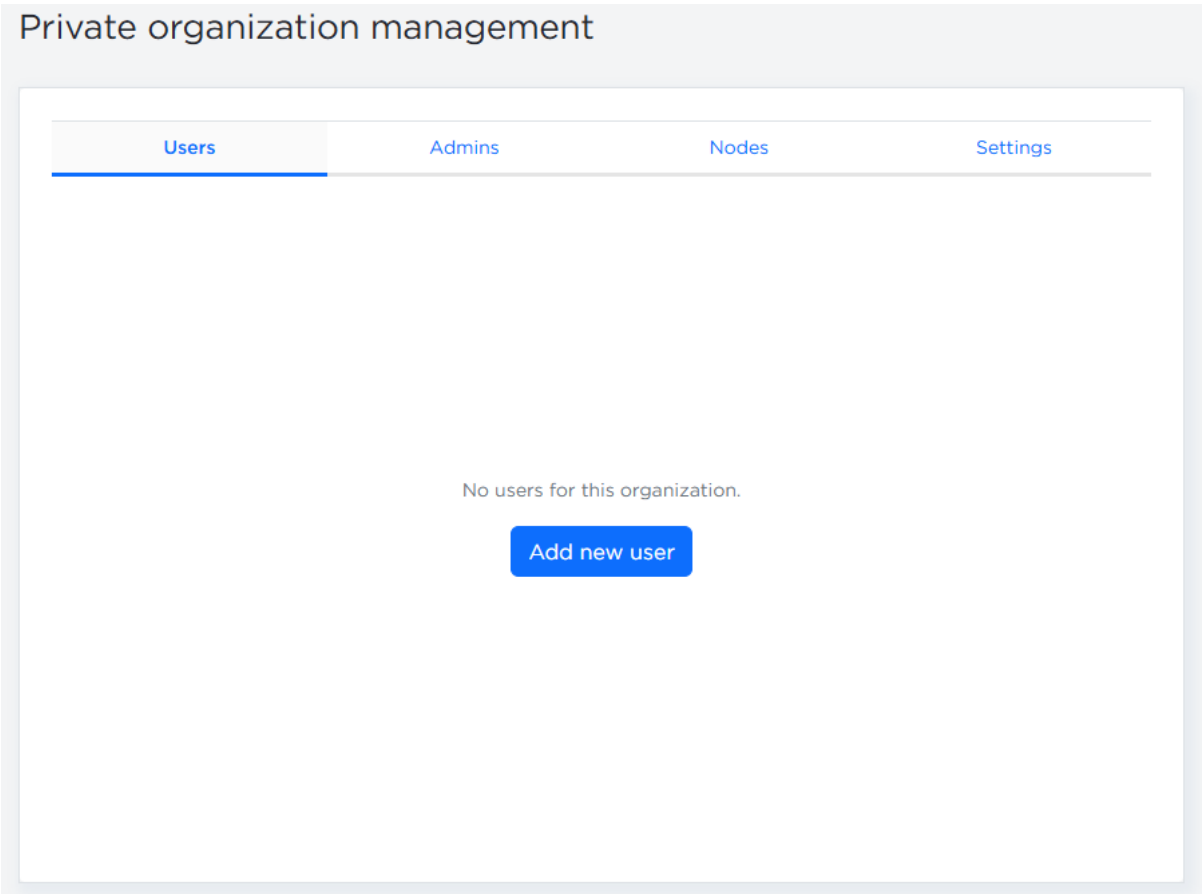
Dodawanie użytkowników do organizacji

Podobnie jak użytkownicy w Zabbix, możesz tworzyć użytkowników w Zabbix Cloud i przypisywać im role, aby kontrolować, co mogą robić w organizacji i jej węzłach.

Aby dodać użytkowników do swojej organizacji:

1. Otwórz stronę *All organizations*.

2. Kliknij przycisk ustawień wybranej organizacji, aby przejść do jej menu zarządzania.



3. Na karcie *Users* lub *Admins* kliknij *Add new user*.

4. Wprowadź adres e-mail użytkownika i wybierz rolę: *Administrator* lub *User*.

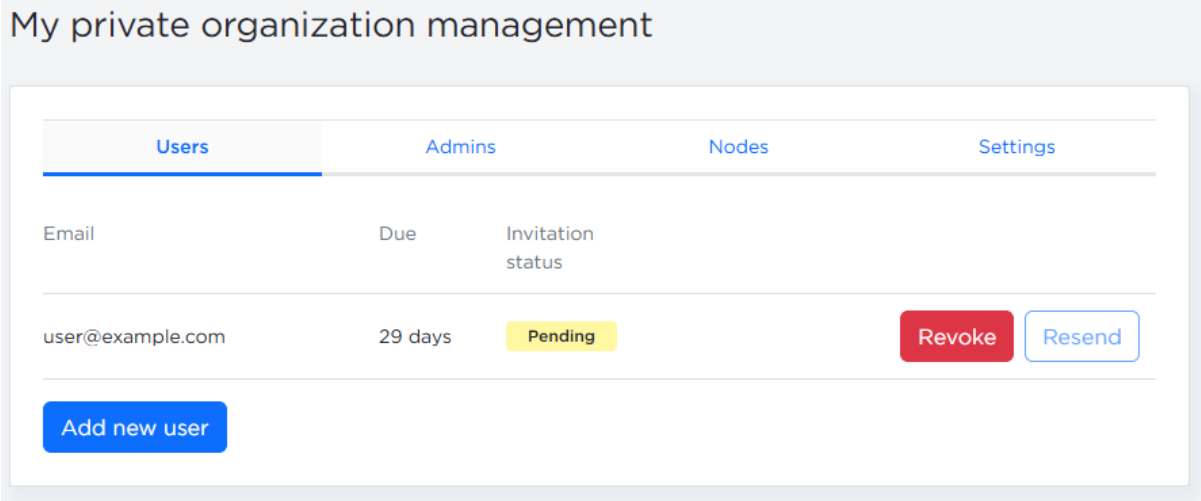
Pamiętaj, że wybranie roli *User* dodaje użytkownika do organizacji, ale nie nadaje dostępu do żadnych węzłów.

Każda rola zapewnia inny poziom dostępu:

- **User** — może uzyskiwać dostęp do przypisanych mu węzłów i wykonywać zadania konfiguracyjne, które nie generują opłat, na przykład:
  - Zarządzać filtrami dostępu
  - Konfigurować szyfrowanie
  - Ustawiać okresy przechowywania historii/trendów
  - Planować okresy konserwacji
- **Administrator** — ma wszystkie uprawnienia roli User i może również wykonywać działania, które mogą generować opłaty, na przykład:
  - Tworzyć i przywracać kopie zapasowe
  - Zwiększać lub zmniejszać zasoby węzła (warstwę obliczeniową i rozmiar dysku)
  - Anulować subskrypcje
- **Owner** — ma pełną kontrolę nad organizacją. Oprócz wszystkich uprawnień roli Administrator, Owner może:
  - Tworzyć i usuwać węzły
  - Dodawać lub usuwać użytkowników i administratorów
  - Zmieniać nazwę organizacji lub ją usuwać
  - Zarządzać danymi rozliczeniowymi

> **Attention:**
> Metoda płatności Owner jest obciążana za wszystkie usługi. Jeśli wymagane jest potwierdzenie bankowe, Owner musi autoryzować transakcję, nawet jeśli została zainicjowana przez Administratora.

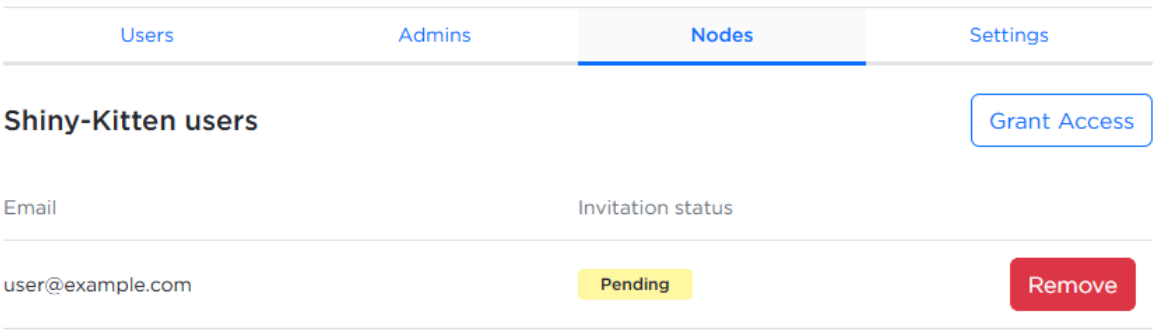
Zaproszony użytkownik zostanie dodany ze statusem *Pending*.
Możesz cofnąć zaproszenie lub wysłać je ponownie (ponowne wysłanie jest dostępne raz na 10 minut — przycisk będzie wyłączony po osiągnięciu tego limitu).



Dodawanie użytkowników do węzłów

Aby dodać użytkownika do węzła:

1. Przejdź do zakładki *Nodes*.
2. Kliknij *Grant Access*.
3. Wybierz z listy rozwijanej użytkownika dodanego do organizacji.
4. Kliknij *Grant access*.



Alternatywnie możesz nadać dostęp z okna *Node configuration*:

1. Kliknij przycisk ustawień  .
2. Wybierz *Add user*.
3. Wybierz użytkownika i kliknij *Grant access*.

Zaproszeni użytkownicy muszą zaakceptować zaproszenie, tworząc konto Zabbix Cloud przy użyciu tego samego adresu e-mail, na który wysłano zaproszenie. Jeśli użytkownik ma już konto Zabbix Cloud przypisane do tego adresu e-mail, musi się zalogować i potwierdzić zaproszenie. Zaproszenia są powiązane z konkretnym adresem e-mail i nie mogą zostać zaakceptowane z innego konta.

Kluczowe różnice w Zabbix Cloud

Tabela porównawcza Chociaż większość funkcjonalności pokrywa się między lokalnymi instalacjami Zabbix a węzłami chmurowymi, istnieją również różnice. Poniżej przedstawiono zbiorczą tabelę porównawczą. W kolejnych sekcjach szczegółowo opisano wybrane pozycje.

Funkcja / Aspekt	Zabbix Cloud	Zabbix lokalnie
Cykl wydań	Zgodny z wydaniami LTS releases	Wybierasz własną wersję Zabbix (stabilną, beta, niestandardowe buildy)
Łatwość użycia	Platforma gotowa do użycia, w pełni zarządzana przez Zabbix	Wymaga instalacji, konfiguracji i utrzymania
Łatanie podatności	Automatyczne aktualizacje systemu operacyjnego/Zabbix	Ręczne aktualizacje wykonywane przez użytkownika
Certyfikat HTTPS	Ważny certyfikat dostępny od razu po uruchomieniu (bez Let's Encrypt)	Domyślnie samopodpisany (można skonfigurować Let's Encrypt lub inne CA)
Wydajność DB (INSERT/UPDATE/SELECT)	Automatyczne partycjonowanie dla maksymalnej szybkości; brak długotrwałych operacji DELETE	Ręczne partycjonowanie i czyszczenie (możliwe długie transakcje DELETE)
Dostrajanie wydajności	Wstępnie dostrojone przez zespół Zabbix Cloud (brak changelogów)	Pełna widoczność i kontrola nad parametrami dostrajania
Kontrola zapory sieciowej	Zarządzana przez zespół Zabbix Cloud; porty GUI/trapper nie są publicznie wystawione	Pełna kontrola nad regułami zapory i ekspozycją portów
Izolacja i ochrona DB	Wysoki poziom izolacji, brak bezpośredniego dostępu do DB/SSH	Zależy od Twojej sieci i zabezpieczeń hosta
Wysoka dostępność (HA)	Działa na platformie chmurowej o wysokiej dostępności, proxy Zabbix mogą być używane dla większej odporności zbierania danych	HA zarządzane przez użytkownika
Pułapki SNMP	Tylko przez dedykowany proxy (brak odbiornika pułapek z HA/balansowaniem obciążenia)	Bezpośrednio lub przez proxy, możliwe HA/balansowanie obciążenia
Odpytywanie SNMP	Trudne bez proxy (każde urządzenie wymaga NAT/niestandardowego portu)	Natywne odpytywanie SNMP; proxy opcjonalny
Ustawienia retencji	Historia/Trendy/Audyt tylko przez UI (bez API ani pliku konfiguracyjnego)	Konfigurowalne w pliku konfiguracyjnym serwera Zabbix lub przez API
Niestandardowe skrypty	`AlertScriptsPath`, `ExternalScripts`, frontend i moduły społeczności nie są obsługiwane	W pełni obsługiwane (ścieżka skryptów, moduły, integracje)
Monitorowanie ODBC	Tylko PostgreSQL (sterownik `{postgresql}`); wtyczka MariaDB obecna jako placeholder	ODBC dla PostgreSQL, MySQL, Oracle itd. - w pełni konfigurowalne
Ograniczanie wywołań ODBC	Niemożliwe (`StartODBCPollers=1` tylko; ciężkie synchroniczne zapytania blokują inną pracę)	W pełni dostrajana liczba pollerów i harmonogramowanie
Przesyłanie certyfikatu SAML	Nieobsługiwane	Obsługiwane przez UI lub API
Raporty cykliczne	Należy samodzielnie utworzyć nośnik Email (nośnik skryptowy nie jest obsługiwany)	Obsługuje zarówno nośnik skryptowy, jak i Email od razu po uruchomieniu

Funkcja / Aspekt	Zabbix Cloud	Zabbix lokalnie
Interfejs hosta dla aktywnych testów	Adres IP przydzielany przez platformę (tworzony automatycznie)	Interfejsy zarządzane przez Ciebie; adresy IP pod Twoją kontrolą

Różnice funkcjonalne Pułapki SNMP

Pułapki SNMP są obsługiwane wyłącznie przez dedykowany proxy Zabbix. Jeśli wymagane jest monitorowanie pułapek SNMP, nie można używać automatycznego równoważenia obciążenia ani wysokiej dostępności dla proxy, ponieważ pułapki SNMP muszą być wysyłane na pojedynczy adres IP.

Odpytywanie SNMP

Bez proxy odpytywanie SNMP wymaga, aby każde urządzenie było udostępnione przez NAT i niestandardowe porty.

Ustawienia retencji

Okresy retencji historii, trendów i dziennika audytu można konfigurować w chmurze wyłącznie za pośrednictwem interfejsu webowego. Tych ustawień nie można konfigurować za pomocą `zabbix_server.conf` ani przez API.

Ręczne nadpisywanie historii dla poszczególnych pozycji nie jest obsługiwane (partycjonowanie jest kontrolowane globalnie). Adresy URL węzłów chmurowych nie akceptują tych samych parametrów zapytania co instalacje lokalne.

Własne skrypty

Następujące typy własnych skryptów nie są obsługiwane przez Zabbix Cloud:

- Skrypty alertów (`AlertScriptsPath`)
- Skrypty zewnętrzne (`ExternalScripts`)
- Skrypty frontend na serwerze Zabbix

Nie można instalować modułów frontend opracowanych przez społeczność.

Monitorowanie ODBC

Zabbix Cloud obsługuje monitorowanie ODBC tylko dla PostgreSQL. Użyj oficjalnego szablonu ODBC Zabbix i zdefiniuj connection string w szablonie, używając:

```
Driver={postgresql}
```

Wtyczka MariaDB jest również zainstalowana, ale obecnie nie działa. Jeśli jest używana, zdefiniuj:

```
Driver={mysql}
```

Attention:
Nie jest znana żadna działająca konfiguracja dla Oracle MySQL 8.0 w Zabbix Cloud. Chociaż proste zapytania (takie jak `SELECT 1`) mogą się powieść, bardziej złożone zapytania zwracają `SQL_ERROR`.

 Nie ma możliwości ograniczenia wywołań ODBC (`StartODBCPollers=1` only). Intensywne synchroniczne raportowanie może wpływać na wydajność, a jednocześnie może być uruchomione tylko pojedyncze `SELECT`.

Dostęp do infrastruktury

Zabbix Cloud nie zapewnia dostępu SSH do bazowych węzłów ani nie zezwala na bezpośrednie połączenia z bazą danych (na przykład do portu 3306). Wszystkie działania związane z konfiguracją, monitorowaniem i rozwiązywaniem problemów muszą być wykonywane za pośrednictwem interfejsu użytkownika chmury lub API, co zapewnia, że warstwy systemu operacyjnego i bazy danych pozostają odizolowane i zabezpieczone.

Interfejs aktywnych kontroli

Aktywne kontrole w chmurze automatycznie tworzą interfejs hosta z adresem IP niezwiązanym z lokalną siecią. Domyślnie ten adres IP może być zewnętrzny. Aby zachować spójność, po utworzeniu możesz ręcznie usunąć lub dostosować interfejs hosta.

Przesyłanie certyfikatu SAML

Uwierzytelnianie SAML nie jest obsługiwane, ponieważ niewielu dostawców akceptuje niezaszyfrowane lub niepodpisane komunikaty SAML.

Zaplanowane raporty

Domyślny typ mediów *Cloud Email* używa transportu skryptowego i nie może być używany do zaplanowanych raportów. Aby wysyłać raporty pocztą e-mail:

1. Utwórz nowy typ mediów Email.

2. Przypisz medium e-mail do swojego użytkownika w *Ustawienia użytkownika* > *Media*.
3. Wybierz ten typ mediów podczas konfigurowania zaplanowanych raportów.

Centrum dewelopera

Centrum deweloperskie

Rozpocznij tworzenie niestandardowych rozszerzeń dla Zabbix, korzystając ze wskazówek dotyczących modułów, widżetów i wtyczek.

Twórz na Zabbix

Moduły frontend Przewodniki i materiały referencyjne dotyczące tworzenia niestandardowych modułów, które rozszerzają lub modyfikują frontend Zabbix, aby dostosować go do konkretnych przypadków użycia.

Widgety Omówienie struktury i logiki widgetów wraz z instrukcjami tworzenia niestandardowych elementów pulpitu dostosowanych do Twoich potrzeb.

Wtyczki Przegląd sposobu tworzenia i zarządzania wtyczkami Zabbix w celu rozszerzenia funkcjonalności lub integracji z systemami zewnętrznymi.

Pluginy

Przegląd Niestandardowe wtyczki rozszerzają funkcjonalność agenta Zabbix 2. Są kompilowane osobno, ale używają pakietu współdzielonego z agentem Zabbix 2.

Każda wtyczka jest pakietem *Go*, który definiuje strukturę i implementuje jeden lub kilka interfejsów wtyczki (*Exporter*, *Configurator*, *Runner*).

Przejdź do:

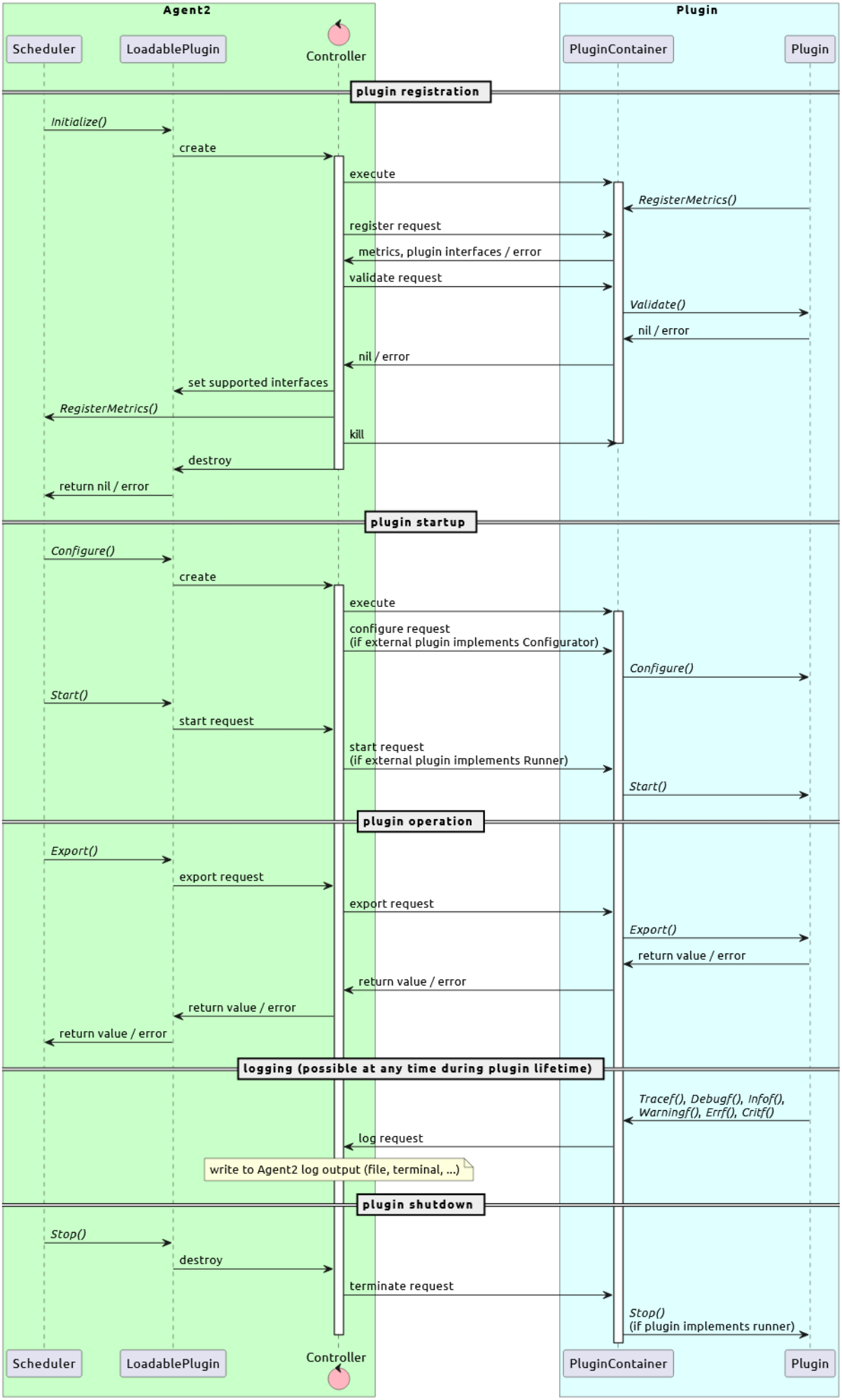
- Napisz swoją pierwszą wtyczkę
- Interfejsy wtyczek

Zobacz także:

- Przykładowa wtyczka dla agenta Zabbix 2

Schemat połączenia Agent Zabbix 2 łączy się dwukierunkowo z wtyczkami za pomocą gniazd UNIX w systemie Linux i nazwanych potoków w systemie Windows.

Poniższy diagram połączeń ilustruje proces komunikacji między agentem Zabbix 2 a wtyczką oraz proces zbierania metryk.


Agent2
Plugin
Scheduler
LoadablePlugin
Controller
PluginContainer
Plugin
plugin registration
Initialize()
create
execute
RegisterMetrics()
register request
metrics, plugin interfaces / error
validate request
Validate()
nil / error
nil / error
set supported interfaces
RegisterMetrics()
kill
destroy
return nil / error
plugin startup
Configure()
create
execute
configure request
(if external plugin implements Configurator)
Configure()
Start()
start request
start request
(if external plugin implements Runner)
Start()
plugin operation
Export()
export request
export request
Export()
return value / error
return value / error
return value / error
return value / error
logging (possible at any time during plugin lifetime)
Tracef(), Debugf(), Infof(),
Warningf(), Errf(), Critf()
log request
write to Agent2 log output (file, terminal, ...)
plugin shutdown
Stop()
destroy
terminate request
Stop()
(if plugin implements runner)
Scheduler
LoadablePlugin
Controller
PluginContainer
Plugin

What you'll create This is ste-by-step tutorial for creating a simple loadable plugin named **MyIP**. This plugin will implement a single item key (`myip`) returning the external IP address of the Zabbix agent host.

Step 1: Setup

1. A plugin is a standard Go module. Start by initializing the `go.mod` file in the plugin directory to track plugin dependencies:

```
cd path/to/plugins/myip # Switch to your plugin directory
go mod init myip
```

2. Install the mandatory dependency Zabbix Go SDK (`golang.zabbix.com/sdk`):

```
go get golang.zabbix.com/sdk@$LATEST_COMMIT_HASH
```

Replace `$LATEST_COMMIT_HASH` with the latest `HEAD` commit hash from the `golang.zabbix.com/sdk` repository in the appropriate release branch. For example:

```
go get golang.zabbix.com/sdk@af85407
```

Note that `golang.zabbix.com/sdk` versioning is currently not supported, but this may change in the future.

Additional dependencies can be installed as needed using `go get`.

3. Create an empty `main.go` file for the plugin source code:

```
touch main.go
```

Now the initial setup is complete, and the plugin is ready for development.

Step 2: Plugin structure The `golang.zabbix.com/sdk` module, installed in the previous step, provides the necessary framework for plugin development and ensures all plugins have a consistent structure.

1. Set up basic execution flow.

Start by defining the main execution flow of the plugin. Add the following code to `main.go`:

```
package main

func main() {
    err := run()
    if err != nil {
        panic(err)
    }
}

func run() error {
    return nil
}
```

This establishes the basic execution flow for the plugin. The run function will later contain the core logic of the plugin.

2. Explore the plugin interfaces.

A Zabbix agent 2 plugin shall be represented by a struct that implements interfaces from the `golang.zabbix.com/sdk/plugin` package:

- *Accessor* - defines essential methods all plugins must implement, such as setting the plugin name and handling item key timeouts.
- One or more of the following functional plugin interfaces:
  - *Exporter* - performs a poll and returns a value (or values), nothing, or an error; often used alongside the *Collector* interface.
  - *Collector* - manages the periodic collection of data.
  - *Runner* - defines plugin startup and shutdown procedures.
  - *Watcher* - allows to implement independent metric polling, bypassing the agent's internal scheduler; useful for trap-based or event-driven monitoring.
  - *Configurator* - defines how the plugin reads and applies its configuration settings.

You can either implement these interfaces yourself or use the default ones provided by the Zabbix Go SDK, modifying them as needed. This tutorial uses the default implementations.

3. Create the plugin struct.

Now, import the *plugin* package and create a `myIP` struct that embeds the `plugin.Base` struct:

```
import "golang.zabbix.com/sdk/plugin"

type myIP struct {
    plugin.Base
}
```

The myIP struct currently satisfies the Accessor interface. A method for implementing one of the functional plugin interfaces, the `Exporter`, will be added later in the tutorial.

Step 3: Define item keys Your plugin needs the item keys to collect data and provide it to Zabbix server or proxy.

1. Import *errs* package for error handling:

```
import "golang.zabbix.com/sdk/errs"
```

2. Register item keys using the `plugin.RegisterMetrics()` function within the `run()` function:

```
func run() error {
    p := &myIP{}

    // Register the `myip` item key.
    err := plugin.RegisterMetrics(
        p,
        "MyIP",                          // Plugin name
        "myip",                          // Item key name
        "Returns the host's IP address.", // Item key description
    )
    if err != nil {
        return errs.Wrap(err, "failed to register metrics")
    }

    return nil
}
```

To register several item keys, repeat the parameters *metric name* and *description* for each metric. For example:

```
plugin.RegisterMetrics(&impl, "Myip", "metric.one", "Metric one description.", "metric.two", "Metric two d
```

Step 4: Set up the handler The handler facilitates communication between the agent and the plugin.

1. Import the *container* package:

```
import "golang.zabbix.com/sdk/plugin/container"
```

2. Indise the `run()` function add code to create and set up a handler:

```
func run() error {
    p := &myIP{}

    // Register the `myip` item key.
    err := plugin.RegisterMetrics(
        p,
        "MyIP",                          // Plugin name
        "myip",                          // Item key name
        "Returns the host's IP address.", // Item key description
    )
    if err != nil {
        return errs.Wrap(err, "failed to register metrics")
    }

    // Create a new handler.
    h, err := container.NewHandler("MyIP") // Plugin name
    if err != nil {
        return errs.Wrap(err, "failed to create new handler")
    }
```

```
    // Setup logging to forward logs from the plugin to the agent.
    // Available via p.Logger.Infof, p.Logger.Debugf, etc.
    p.Logger = h

    // Start plugin execution.
    // Blocks until a termination request is received from the agent.
    err = h.Execute()
    if err != nil {
        return errs.Wrap(err, "failed to execute plugin handler")
    }

    return nil
}
```

Step 5: Implement data collection Data collection is done via the Exporter interface, which describes the `Export` method:

```
func Export(
  key string,             // The item key to collect.
  params []string,        // Arguments passed to the item key (`myip[arg1, arg2]`).
  context ContextProvider // Metadata about the item key data collection.
) (any, error)
```

1. Import the required packages for HTTP requests and response reading:

```
import (
    "io"
    "net/http"
)
```

2. Implement the `Export` method for the `myIP` struct:

```
func (p *myIP) Export(
    key string, params []string, context plugin.ContextProvider,
) (any, error) {
    // The plugin can use different data collection logic based on the `key` parameter.
    // This implementation only verifies that the provided `key` is supported.
    if key != "myip" {
        return nil, errs.Errorf("unknown item key %q", key)
    }

    // The log will get forwarded to the agent 2 log.
    p.Infof(
        "received request to handle %q key with %d parameters",
        key,
        len(params),
    )

    // Collect the data and return it.

    resp, err := http.Get("https://api.ipify.org")
    if err != nil {
        return nil, errs.Wrap(err, "failed to get IP address")
    }

    defer resp.Body.Close()

    body, err := io.ReadAll(resp.Body)
    if err != nil {
        return nil, errs.Wrap(err, "failed to read response body")
    }

    return string(body), nil
}
```

Step 6: Build and configure the plugin

1. To build the plugin, run:

```
go mod tidy
go build
```

This should create an executable `myip` in the current directory.

2. Configure Zabbix agent 2 to use the plugin:

```
echo "Plugins.MyIP.System.Path=$PATH_TO_THE_MYIP_PLUGIN_EXECUTABLE" > /etc/zabbix_agent2.d/plugins.d/myip.
```

Replace `$PATH_TO_THE_MYIP_PLUGIN_EXECUTABLE` with the path to the `myip` created in step 5.

The plugin name in the configuration parameter name (*MyIP* in this tutorial) must match the plugin name defined in the *plugin.RegisterMetrics()* function.

3. To test the plugin and its `myip` item, run:

```
zabbix_agent2 -c /etc/zabbix_agent2.conf -t myip
```

The output should contain an external IP address of your host and look similar to this:

```
myip                                          [s|192.0.2.0]
```

With that, you have created a simple loadable plugin for Zabbix agent 2. Congrats!

```go
package main

import (
    "io"
    "net/http"

    "golang.zabbix.com/sdk/errs"
    "golang.zabbix.com/sdk/plugin"
    "golang.zabbix.com/sdk/plugin/container"
)

var _ plugin.Exporter = (*myIP)(nil)

type myIP struct {
    plugin.Base
}

func main() {
    err := run()
    if err != nil {
        panic(err)
    }
}

func run() error {
    p := &myIP{}

    // Register the `myip` item key.
    err := plugin.RegisterMetrics(
        p,
        "MyIP",                             // Plugin name
        "myip",                             // Item key name
        "Returns the host's IP address.", // Item key description
    )
    if err != nil {
        return errs.Wrap(err, "failed to register metrics")
    }

    // Create a new handler.
```

```
    h, err := container.NewHandler("MyIP") // Plugin name
    if err != nil {
        return errs.Wrap(err, "failed to create new handler")
    }

    // Setup logging to forward logs from the plugin to the agent.
    // Available via p.Logger.Infof, p.Logger.Debugf, etc.
    p.Logger = h

    // Start plugin execution.
    // Blocks until a termination request from the agent is received.
    err = h.Execute()
    if err != nil {
        return errs.Wrap(err, "failed to execute plugin handler")
    }

    return nil
}

func (p *myIP) Export(
    key string, params []string, context plugin.ContextProvider,
) (any, error) {
    // The plugin can use different data collection logic based on the `key` parameter.
    // This implementation only verifies that the provided `key` is supported.
    if key != "myip" {
        return nil, errs.Errorf("unknown item key %q", key)
    }

    // The log will get forwarded to the agent 2 log.
    p.Infof(
        "received request to handle %q key with %d parameters",
        key,
        len(params),
    )

    // Collect the data and return it.

    resp, err := http.Get("https://api.ipify.org")
    if err != nil {
        return nil, errs.Wrap(err, "failed to get IP address")
    }

    defer resp.Body.Close()

    body, err := io.ReadAll(resp.Body)
    if err != nil {
        return nil, errs.Wrap(err, "failed to read response body")
    }

    return string(body), nil
}
```

Complete source code

Interfejsy wtyczek

Ta sekcja opisuje dostępne interfejsy wtyczek.

plugin.Exporter *Exporter* to najprostszy interfejs, który wykonuje badanie, zwraca wartość (wartości), nic lub błąd. Akceptuje przygotowany klucz elementu, parametry i kontekst. Dostęp do wszystkich innych interfejsów wtyczek jest wyłączny i żadna

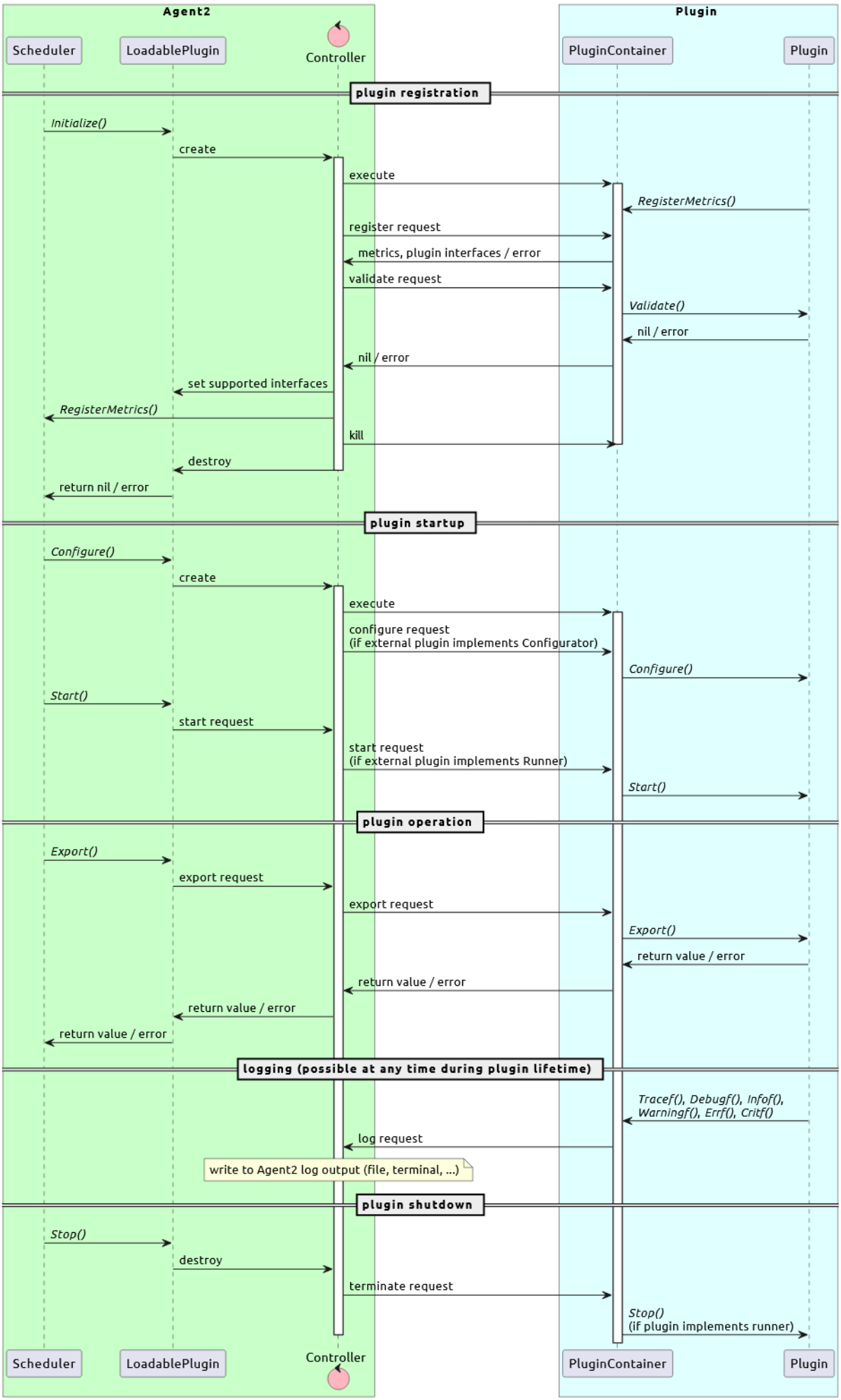
metoda nie może zostać wywołana, jeśli wtyczka wykonuje już zadanie. Ponadto istnieje limit maksymalnie 100 równoczesnych wywołań *Export()* dla wtyczki, który można zmniejszyć zgodnie z wymaganiami dla każdej wtyczki.

plugin.Configurator Interfejs *Configurator* udostępnia parametry konfiguracji wtyczki z plików konfiguracyjnych agenta Zabbix 2.

plugin.Runner Interfejs *Runner* zapewnia możliwości do wykonywania inicjalizacji, gdy wtyczka jest uruchamiana (aktywowana) i deinicjalizacji, gdy wtyczka jest zatrzymywana (dezaktywowana). Na przykład wtyczka może uruchomić/zatrzymać jakąś w tle *goroutine*, implementując interfejs Runner.

Connection diagram Zabbix agent 2 connects bidirectionally to the plugins using UNIX sockets on Linux and Named Pipes on Windows.

The connection diagram below illustrates the communication process between Zabbix agent 2 and a loadable plugin and the metrics collection process.


Agent2
Plugin
Scheduler
LoadablePlugin
Controller
PluginContainer
Plugin
plugin registration
Initialize()
create
execute
RegisterMetrics()
register request
metrics, plugin interfaces / error
validate request
Validate()
nil / error
nil / error
set supported interfaces
RegisterMetrics()
kill
destroy
return nil / error
plugin startup
Configure()
create
execute
configure request
(if external plugin implements Configurator)
Configure()
Start()
start request
start request
(if external plugin implements Runner)
Start()
plugin operation
Export()
export request
export request
Export()
return value / error
return value / error
return value / error
return value / error
logging (possible at any time during plugin lifetime)
Tracef(), Debugf(), Infof(),
Warningf(), Errf(), Critf()
log request
write to Agent2 log output (file, terminal, ...)
plugin shutdown
Stop()
destroy
terminate request
Stop()
(if plugin implements runner)
Scheduler
LoadablePlugin
Controller
PluginContainer
Plugin

Biblioteka Python dla Zabbix

zabbix_utils to oficjalna biblioteka Pythona dla Zabbix.

Za pomocą zabbix_utils możesz:

- Używać API Zabbix do zarządzania obiektami Zabbix (tworzyć hosty, aktualizować pozycje, pobierać zdarzenia itp.).
- Zbierać dane z agent Zabbix (podobnie jak za pomocą Zabbix get).
- Wysyłać dane do serwer Zabbix lub proxy (podobnie jak za pomocą Zabbix sender).

Biblioteka obsługuje zarówno synchroniczne, jak i asynchroniczne wykonywanie skryptów, co pozwala jej obsługiwać zarówno proste przepływy pracy, jak i zakrojone na szeroką skalę operacje równoległe, takie jak masowe zbieranie danych, eksport zbiorczy, przetwarzanie alertów oraz efektywne skalowanie systemu.

Biblioteka jest zgodna z obsługiwanymi wersjami serwer Zabbix oraz nowoczesnymi wydaniami Pythona.

Aby rozpocząć, zainstaluj bibliotekę, a następnie skorzystaj z przewodnika szybki start.

Instalacja

zabbix_utils można zainstalować przy użyciu dowolnej z metod opisanych poniżej.

Wymagania:

- Zabbix 6.0 lub nowszy (testowano na 6.0, 7.0, 7.2, 7.4)
- Python 3.8 lub nowszy (testowano na 3.8–3.13)
- asynchroniczny framework HTTP aiohttp (wymagany tylko w trybie asynchronicznym)

Python Package Index (PyPI)

Jest to najczęściej stosowana metoda w większości środowisk:

```
pip install zabbix_utils
pip install zabbix_utils[async] # Tylko dla obsługi async
```

Repozytorium Zabbix

Użyj tej metody, jeśli wolisz zarządzać zależnościami za pomocą menedżera pakietów swojego systemu.

Pobierz pakiety Zabbix dla swojej dystrybucji Linuksa, a następnie uruchom poniższe polecenia.

W systemie RHEL i pochodnych:

```
dnf install python3-zabbix-utils
dnf install epel-release # Tylko dla obsługi async
dnf install python3-aiohttp # Tylko dla obsługi async
```

W systemach Debian/Ubuntu i pochodnych:

```
apt install python3-zabbix-utils
apt install python3-aiohttp # Tylko dla obsługi async
```

Źródło (GitHub)

Użyj tej metody, jeśli preferujesz najnowszą wersję rozwojową:

```
git clone https://github.com/zabbix/python-zabbix-utils
cd python-zabbix-utils/
pip install -r requirements.txt # Tylko dla obsługi asynchronicznej
python3 setup.py install
```

Aby zainstalować zależności wymagane dla trybu asynchronicznego, możesz także użyć jednej z metod opisanych powyżej.

Przewodnik szybkiego startu

Po zainstalowaniu zabbix_utils możesz używać go w swoim skrypcie.

Ten przewodnik szybkiego startu pokazuje, jak:

- Pobierać nazwę hosta z Zabbix agent.
- Tworzyć host i pozycja typu trapper za pomocą Zabbix API.
- Wysyłać wartość do pozycji.

Przewodnik przedstawia skrypt krok po kroku, wyjaśniając każdą część w miarę jej wprowadzania. Na końcu strony znajduje się kompletny skrypt.

W przewodniku założono również, że Twój serwer Zabbix, agent i API działają lokalnie.

Pobieranie nazwy hosta z Zabbix agent

Zacznij od pobrania nazwy hosta systemu, na którym działa Zabbix agent. Ta nazwa hosta będzie potrzebna do utworzenia hosta przy użyciu Zabbix API.

1. Zaimportuj klasę `Getter` z zabbix_utils. Ta klasa działa podobnie jak Zabbix get i umożliwia żądanie danych z Zabbix agent.

2. Utwórz instancję `Getter`, która łączy się z lokalnym Zabbix agent pod adresem `127.0.0.1` na porcie `10050`.

3. Wywołaj metodę `get()` na instancji `Getter`, aby zażądać nazwy hosta z Zabbix agent.

- Metoda `get()` przyjmuje klucz pozycji jako parametr i wysyła żądanie do Zabbix agent o tę pozycję.
- Metoda `get()` zwraca obiekt, a nazwa hosta jest przechowywana w atrybucie `value` tego obiektu.
- `system.hostname` to wbudowany klucz Zabbix agent, który zwraca nazwę hosta.

```
from zabbix_utils import Getter

agent = Getter(host='127.0.0.1', port=10050)
hostname = agent.get('system.hostname').value
```

Połącz się i zaloguj do Zabbix API

Następnie połącz się z Zabbix API. Pozwoli to Twojemu skryptowi zarządzać obiektami Zabbix, takimi jak hosty i pozycje.

1. Zaimportuj klasę `ZabbixAPI` z zabbix_utils.

2. Utwórz instancję `ZabbixAPI` i podaj adres URL swojego interfejsu webowego Zabbix.

3. Wywołaj metodę `login()` na instancji `ZabbixAPI` i podaj swoją nazwę użytkownika oraz hasło. Konto musi mieć uprawnienie do uzyskiwania dostępu do Zabbix API.

4. Wywołaj metodę `logout()`, aby zamknąć sesję po zakończeniu operacji API.

```
from zabbix_utils import ZabbixAPI

api = ZabbixAPI(url='127.0.0.1/zabbix')
api.login(user='Admin', password='zabbix')

### API operations go here

api.logout()
```

Utwórz host w Zabbix

Teraz, gdy masz nazwę hosta z Zabbix agent i jesteś połączony z Zabbix API, możesz utworzyć nowy host w Zabbix.

1. Wywołaj metodę API `host.create()` na instancji `ZabbixAPI` i podaj szczegóły hosta:

- `host` — ustaw na zmienną `hostname` zawierającą nazwę hosta pobraną z Zabbix agent.
- `interfaces` — zawiera szczegóły połączenia dla Zabbix agent uruchomionego na hoście.
- `groups` — zawiera co najmniej jedną grupę hostów, do której host powinien należeć.

2. Ponieważ Zabbix API zwraca ID nowo utworzonego hosta, zapisz to ID w zmiennej `host_id` do późniejszego użycia.

3. Wyświetl komunikat potwierdzający, że host został utworzony.

```
api.host.create(
    host=hostname,
    interfaces=[{
        'type': 1,
        'main': 1,
        'useip': 1,
        'ip': '127.0.0.1',
```

```
        'dns': '',
        'port': '10050',
    }],
    groups=[{'groupid': '2'}]
)

host_id = host['hostids'][0]

print(f"Host '{hostname}' created with ID {host_id}")
```

Utwórz nową pozycję w Zabbix

Po utworzeniu hosta możesz dodać do niego pozycję.

1. Zdefiniuj unikalny klucz dla pozycji, która ma zostać utworzona.

2. Wywołaj metodę `item.create()` na instancji `ZabbixAPI` i podaj szczegóły pozycji:

- `hostid` - ustaw na zmienną `host_id` zawierającą ID hosta, który został właśnie utworzony.
- `name` - nazwa pozycji.
- `key_` - ustaw na zmienną `item_key`, którą właśnie zdefiniowano.
- `type` - ustaw na 2 (pozycja trapper); jest to wymagane do odbierania wartości wysyłanych ze skryptu w kolejnych krokach.
- `value_type` - ustaw na 3 (numeric unsigned), czyli typ danych przechowywanych przez tę pozycję.

3. Ponieważ Zabbix API zwraca ID nowo utworzonej pozycji, zapisz to ID w zmiennej `item_id` do późniejszego użycia.

4. Wyświetl komunikat potwierdzający utworzenie pozycji.

```
item_key = 'app.myservice.heartbeat'

item = api.item.create(
    hostid=host_id,
    name='App heartbeat',
    key_=item_key,
    type=2,
    value_type=3,
)

item_id = item['itemids'][0]

print(f"Item '{item_key}' created with ID {item_id}")
```

Wyślij wartość do hosta

Teraz, gdy utworzyłeś host i pozycję, możesz wysłać do niej dane.

1. Zaimportuj klasę `time` i odczekaj kilka sekund przed wysłaniem danych. Dzięki temu Zabbix w pełni przetworzy nowy host i pozycję.

2. Zaimportuj klasę `Sender` z zabbix_utils. Ta klasa działa podobnie jak Zabbix sender i umożliwia skryptowi wysyłanie danych do Zabbix.

3. Utwórz instancję `Sender`, która łączy się z lokalnym serwerem Zabbix pod adresem `127.0.0.1` na porcie `10051`.

4. Wywołaj metodę `send_value()` na instancji `Sender`, aby wysłać wartość do pozycji hosta, i podaj następujące szczegóły:

- `hostname` — ustaw na zmienną `hostname` zawierającą nazwę hosta pobraną z Zabbix agent.
- `item_key` — ustaw na zmienną `item_key`, którą właśnie wcześniej zdefiniowałeś w skrypcie.
- `1` — wartość do wysłania.

4. Wyświetl komunikat potwierdzający, że wartość została wysłana.

```
import time
time.sleep(10)

from zabbix_utils import Sender

sender = Sender(server='127.0.0.1', port=10051)

response = sender.send_value(hostname, item_key, 1)
```

```
print(f"Sender response: {response}")
```

Po pomyślnym wykonaniu tego kodu powinien zostać wyświetlony komunikat o powodzeniu informujący, że Zabbix odebrał wartość:

```
Sender response: {"processed": 1, "failed": 0, "total": 1, "time": "0.000151", "chunk": 1}
```

Teraz możesz również sprawdzić wartość w interfejsie webowym Zabbix (*Monitoring* > *Latest data*).

Kompletny skrypt

Poniżej znajduje się kompletny skrypt, który łączy wszystkie kroki: pobranie nazwy hosta, utworzenie hosta i pozycji przy użyciu Zabbix API oraz wysłanie danych do Zabbix.

```
import time
from zabbix_utils import Getter, ZabbixAPI, Sender

### Pobierz nazwę hosta z Zabbix agent
agent = Getter(host='127.0.0.1', port=10050)
hostname = agent.get('system.hostname').value

### Połącz z Zabbix API i zaloguj się
api = ZabbixAPI(url='127.0.0.1/zabbix')
api.login(user='Admin', password='zabbix')

### Utwórz host w Zabbix
host = api.host.create(
    host=hostname,
    interfaces=[{
        'type': 1,
        'main': 1,
        'useip': 1,
        'ip': '127.0.0.1',
        'dns': '',
        'port': '10050',
    }],
    groups=[{'groupid': '2'}]
)

host_id = host['hostids'][0]

print(f"Host '{hostname}' created with ID {host_id}")

### Utwórz pozycję w Zabbix
item_key = 'app.myservice.heartbeat'

item = api.item.create(
    hostid=host_id,
    name='App heartbeat',
    key_=item_key,
    type=2,
    value_type=3
)

item_id = item['itemids'][0]

print(f"Item '{item_key}' created with ID {item_id}")

### Wyloguj się z API
api.logout()

### Poczekaj, aż Zabbix przetworzy nowy host
time.sleep(10)

### Wyślij wartość do hosta
sender = Sender(server='127.0.0.1', port=10051)
```

```
response = sender.send_value(hostname, item_key, 1)

print(f"Sender response: {response}")
```

Korzystanie z API Zabbix

zabbix_utils umożliwia korzystanie z API Zabbix do zarządzania obiektami Zabbix, w tym tworzenia hostów, aktualizowania pozycji, pobierania zdarzeń i nie tylko.

Żądania API mogą być wykonywane w trybie synchronicznym lub asynchronicznym:

- W trybie synchronicznym skrypt Python wysyła żądanie i czeka na odpowiedź przed kontynuowaniem działania, co jest odpowiednie dla prostych, sekwencyjnych i przewidywalnych operacji.
- W trybie asynchronicznym skrypt wysyła żądania bez oczekiwania na każdą odpowiedź, umożliwiając równoległe wykonywanie innych operacji; jest to bardziej efektywne w przypadku wolnych żądań lub dużych partii danych.

Przykłady na tej stronie koncentrują się na trybie synchronicznym, chociaż tryb asynchroniczny opiera się na podobnych wzorcach. Dodatkowe przykłady są dostępne w repozytorium GitHub zabbix_utils.

Import

Aby używać zabbix_utils do pracy z API Zabbix, zaimportuj klasę `ZabbixAPI` w swoim skrypcie:

```
from zabbix_utils import ZabbixAPI
```

> **Note:**
> Jeśli już używasz biblioteki Python społeczności, zazwyczaj możesz zastąpić ten import przez `ZabbixAPI` z zabbix_utils.

Logowanie

Przed wykonywaniem żądań API należy utworzyć instancję `ZabbixAPI` i zalogować się do Zabbix API.

Wybierz metodę, która najlepiej odpowiada sposobowi zarządzania poświadczeniami. Możesz użyć nazwy użytkownika i hasła lub tokenów API.

Podczas inicjalizacji

Podczas tworzenia instancji `ZabbixAPI` możesz od razu podać adres URL interfejsu webowego Zabbix oraz swoje dane uwierzytelniające:

```
### Nazwa użytkownika i hasło:
api = ZabbixAPI(url="127.0.0.1/zabbix", user="Admin", password="zabbix")

### Token API:
api = ZabbixAPI(url="127.0.0.1/zabbix", token="your_api_token")
```

Jeśli wolisz pogrupować parametry połączenia, możesz przekazać je jako słownik Pythona i rozpakować go za pomocą składni argumentów nazwanych Pythona:

```
ZABBIX_AUTH = {
    "url": "127.0.0.1/zabbix",
    "user": "Admin",
    "password": "zabbix"
}

api = ZabbixAPI(**ZABBIX_AUTH)
```

Używanie `login()`

Możesz najpierw utworzyć instancję `ZabbixAPI`, podając tylko URL interfejsu webowego Zabbix, a następnie użyć metody `login()` ze swoimi poświadczeniami:

```
### Nazwa użytkownika i hasło:
api = ZabbixAPI(url="127.0.0.1/zabbix")
api.login(user="Admin", password="zabbix")

### Token API:
```

```
api = ZabbixAPI(url="127.0.0.1/zabbix")
api.login(token="your_api_token")
```

Używanie zmiennych środowiskowych

Możesz najpierw zapisać swoje dane uwierzytelniające jako zmienne środowiskowe, na przykład przy użyciu terminala:

```
### Nazwa użytkownika i hasło:
export ZABBIX_USER="Admin"
export ZABBIX_PASSWORD="zabbix"

### Token:
export ZABBIX_TOKEN="your_api_token"
```

Następnie, jeśli uruchomisz swój skrypt z tej samej sesji terminala, instancja `ZabbixAPI` w skrypcie wymaga jedynie adresu URL interfejsu webowego Zabbix:

```
api = ZabbixAPI(url="127.0.0.1/zabbix")
```

Możesz również zapisać adres URL w zmiennej środowiskowej:

```
### Nazwa użytkownika i hasło:
export ZABBIX_USER="Admin"
export ZABBIX_PASSWORD="zabbix"
export ZABBIX_URL="https://127.0.0.1/zabbix"

### Token:
export ZABBIX_TOKEN="your_api_token"
export ZABBIX_URL="https://127.0.0.1/zabbix"
```

Gdy adres URL i dane uwierzytelniające są już ustawione jako zmienne środowiskowe, instancja `ZabbixAPI` w skrypcie nie wymaga już żadnych argumentów:

```
api = ZabbixAPI()
```

Wylogowanie

Jeśli zalogowano się przy użyciu nazwy użytkownika i hasła, po zakończeniu operacji API należy wywołać metodę `logout()`:

```
from zabbix_utils import ZabbixAPI

api = ZabbixAPI(url="127.0.0.1/zabbix")
api.login(user="Admin", password="zabbix")

### API actions go here

api.logout()
```

> **Note:**
> Wywołanie metody `logout()` nie jest wymagane podczas używania tokenów API.

Żądania API

Po zalogowaniu możesz wykonywać dowolne żądania API, wywołując metody opisane w opisie metod API Zabbix.

Metody API są wywoływane przy użyciu następującego formatu:

```
api_instance.zabbix_object.method(parameters)
```

> **Note:**
> Niektóre nazwy metod lub obiektów API Zabbix używają słów, które są słowami zastrzeżonymi w Pythonie (np. `import`). Aby uniknąć błędów Pythona, podczas używania ich w Pythonie dodaj podkreślenie do nazwy metody lub obiektu (np. `api.configuration.import_`).

Na przykład, aby wyświetlić listę hostów za pomocą `host.get`:

```
### 1. Importuj ZabbixAPI z zabbix_utils:
from zabbix_utils import ZabbixAPI
```

```
### 2. Utwórz instancję ZabbixAPI i zaloguj się:
api = ZabbixAPI(url="127.0.0.1/zabbix")
api.login(user="Admin", password="zabbix")

### 3. Pobierz hosty pasujące do filtra:
hosts = api.host.get(
    filter={
        "host": [
            "Zabbix server",
            "Linux server"
        ]
    }
)

### 4. Iteruj po zwróconych hostach i wyświetl szczegóły każdego hosta:
for host in hosts:
    print(host)

### 5. Wyloguj się z API, aby zamknąć sesję:
api.logout()
```

Tryb asynchroniczny

Tryb asynchroniczny pozwala skryptowi wysyłać żądania API bez czekania na zakończenie każdego z nich. Może to zwiększyć wydajność skryptu, gdy musi on wykonać wiele żądań API lub gdy niektóre żądania zajmują dużo czasu.

Podczas korzystania z trybu asynchronicznego występują istotne różnice w porównaniu z trybem synchronicznym:

- Zaimportuj moduł `asyncio` języka Python (należy najpierw zainstalować wymagane zależności).
- Zaimportuj `AsyncZabbixAPI` zamiast `ZabbixAPI`.
- Napisz kod wewnątrz funkcji `async`.
- Używaj `await` podczas wywoływania metod API, w tym `login()` i `logout()`.

> **Attention:**
> Podczas tworzenia instancji `AsyncZabbixAPI` nie można zalogować się podczas inicjalizacji.

Na przykład, aby wyświetlić listę hostów za pomocą `host.get` w trybie asynchronicznym:

```
### 1. Zaimportuj asyncio dla trybu asynchronicznego oraz AsyncZabbixAPI z zabbix_utils:
import asyncio
from zabbix_utils import AsyncZabbixAPI

### 2. Zdefiniuj główną funkcję async, w której będą wykonywane wszystkie operacje API:
async def main():

    # 3. Utwórz instancję AsyncZabbixAPI i zaloguj się (wymaga await):
    api = AsyncZabbixAPI(url="127.0.0.1")
    await api.login(user="User", password="zabbix")

    # 4. Pobierz hosty pasujące do filtra (wymaga await):
    hosts = await api.host.get(
        filter={
            "host": [
                "Zabbix server",
                "Linux server"
            ]
        }
    )

    # 5. Iteruj po zwróconych hostach i wypisz szczegóły każdego hosta:
    for host in hosts:
        print(host)

    # 6. Wyloguj się z API, aby zamknąć sesję (wymaga await):
```

```
    await api.logout()

### 7. Uruchom główną funkcję async main() przy użyciu pętli zdarzeń asyncio:
asyncio.run(main())
```

Przykłady

Poniższe przykłady pokazują typowe zadania API Zabbix z użyciem biblioteki zabbix_utils.

Dodatkowe przykłady są dostępne w katalogu `examples` repozytorium GitHub zabbix_utils.

Zbieranie danych z agenta Zabbix

Przegląd

zabbix_utils umożliwia zbieranie danych z Zabbix agent (podobnie jak Zabbix get).

Dane mogą być zbierane w trybie synchronicznym lub asynchronicznym:

- W trybie synchronicznym skrypt Python wysyła żądanie i czeka na dane przed kontynuowaniem działania, co jest odpowiednie dla prostych, sekwencyjnych i przewidywalnych operacji.
- W trybie asynchronicznym skrypt wysyła żądania bez oczekiwania na każdą odpowiedź, umożliwiając równoległe wykonywanie innych operacji; jest to bardziej wydajne w przypadku wolnych żądań lub dużych partii danych.

Przykłady na tej stronie koncentrują się na trybie synchronicznym, chociaż tryb asynchroniczny opiera się na podobnych wzorcach. Dodatkowe przykłady są dostępne w repozytorium GitHub zabbix_utils.

Import

Aby używać `zabbix_utils` do zbierania wartości pozycji, zaimportuj klasę `Getter` w swoim skrypcie Python:

```
from zabbix_utils import Getter
```

Dane żądania

Aby zażądać wartości pozycji:

1. Utwórz instancję `Getter`, podając adres IP i port swojego agenta Zabbix.
2. Wywołaj metodę `get()` na instancji `Getter`, podając klucz pozycji, którą chcesz pobrać.

Na przykład, aby zażądać danych dla pozycji `system.uname`:

```
agent = Getter(host='192.0.2.0', port=10050)
response = agent.get('system.uname')
```

Używanie niestandardowego adresu IP

Jeśli serwer uruchamiający skrypt ma wiele adresów IP, możesz określić `source_ip`, którego `Getter` ma używać podczas łączenia się z Zabbix agent:

```
agent = Getter(
    host='192.0.2.0',
    port=10050,
    source_ip='10.10.7.1'
)
```

Używanie timeout

Możesz ustawić `timeout` odpowiedzi dla `Getter`, aby kontrolować, jak długo skrypt powinien czekać na odpowiedź od agent Zabbix, zanim zrezygnuje:

```
agent = Getter(
    host='192.0.2.0',
    port=10050,
    timeout=30
)
```

Używanie szyfrowania

`Getter` nie zawiera wbudowanej obsługi szyfrowania, ale można ją zapewnić, tworząc wrapper z użyciem bibliotek zewnętrznych:

```
def psk_wrapper(sock, tls):
    # ...
    # Implementacja wrappera TLS PSK dla gniazda
    # ...

agent = Getter(
    host='192.0.2.0',
    port=10050,
    socket_wrapper=psk_wrapper
)
```

Odpowiedź

Odpowiedź z Zabbix agent jest przetwarzana przez bibliotekę i zwracana jako obiekt `AgentResponse`:

```
print(response)
### {
###     "error": null,
###     "raw": "Linux zabbix_server 5.15.0-3.60.5.1.el9uek.x86_64",
###     "value": "Linux zabbix_server 5.15.0-3.60.5.1.el9uek.x86_64"
### }

print(response.value)
### Linux zabbix_server 5.15.0-3.60.5.1.el9uek.x86_64

print(response.error)
### None
```

Tryb asynchroniczny

Tryb asynchroniczny pozwala skryptowi zbierać wartości bez oczekiwania na nadejście każdej z nich. Może to zwiększyć wydajność skryptu, gdy musi on zebrać wiele wartości lub gdy zebranie niektórych wartości zajmuje dużo czasu.

Podczas korzystania z trybu asynchronicznego występują istotne różnice w porównaniu z trybem synchronicznym:

- Zaimportuj moduł `asyncio` języka Python (najpierw musisz zainstalować wymagane zależności).
- Zaimportuj `AsyncGetter` zamiast `Getter`.
- Napisz kod wewnątrz funkcji `async`.
- Użyj `await` podczas wywoływania metody `get()`.

Na przykład, aby pobrać pojedynczą wartość przy użyciu trybu asynchronicznego:

```
### 1. Import asyncio for asynchronous mode, and AsyncGetter from zabbix_utils:
import asyncio
from zabbix_utils import AsyncGetter

### 2. Define the main async function where all data requests will be executed:
async def main():
    agent = AsyncGetter(host='192.0.2.0', port=10050)

    # 3. Fetch the system.uname value from Zabbix agent (must await):
    response = await agent.get('system.uname')

    # 4. Print the value returned by Zabbix agent:
    print(response.value)

### 5. Run the async main() function using asyncio's event loop:
asyncio.run(main())
```

Wysyłanie danych do serwera lub proxy Zabbix

zabbix_utils umożliwia wysyłanie wartości pozycji do pozycji trapper na serwer lub proxy Zabbix (podobnie jak Zabbix sender).

Możesz wysłać pojedynczą wartość, wiele wartości, a nawet kierować dane do wielu klastrów Zabbix.

Dane mogą być wysyłane w trybie synchronicznym lub asynchronicznym:

- W trybie synchronicznym skrypt Python wysyła wartości i czeka na odpowiedź przed kontynuowaniem działania; jest to odpowiednie rozwiązanie dla prostych, sekwencyjnych i przewidywalnych operacji.
- W trybie asynchronicznym skrypt wysyła wartości bez oczekiwania na każdą odpowiedź, umożliwiając równoległe wykonywanie innych operacji; jest to bardziej efektywne w przypadku wolnych żądań lub dużych partii danych.

Przykłady na tej stronie koncentrują się na trybie synchronicznym, chociaż tryb asynchroniczny opiera się na podobnych wzorcach. Dodatkowe przykłady są dostępne w repozytorium GitHub zabbix_utils.

Import

Aby używać `zabbix_utils` do wysyłania wartości pozycji, zaimportuj klasę `Sender` w swoim skrypcie:

```
from zabbix_utils import Sender
```

Aby wysyłać wiele wartości, możesz również zaimportować klasę `ItemValue`:

```
from zabbix_utils import Sender, ItemValue
```

Wyślij pojedynczą wartość

Aby wysłać wartość pozycji:

1. Utwórz instancję `Sender`, podając adres IP i port swojego serwera lub proxy Zabbix.
2. Wywołaj metodę `send_value()` na instancji `Sender`, używając następującego formatu:

```
sender_instance.send_value('host', 'item.key', 'value', optional_timestamp, optional_nanoseconds)
```

Na przykład, aby wysłać 1 do pozycji trapper `service.status` na hoście `Linux server`:

```
sender = Sender(server='127.0.0.1', port=10051)
response = sender.send_value('Linux server', 'service.status', 1)
```

Używanie niestandardowego adresu IP

Jeśli serwer uruchamiający skrypt ma wiele adresów IP, możesz określić `source_ip`, którego `Sender` ma używać podczas wysyłania wartości do serwera Zabbix lub proxy:

```
sender = Sender(
    server='127.0.0.1',
    port=10051,
    source_ip='10.10.7.1'
)
```

Używanie timeout

Możesz ustawić `timeout` odpowiedzi dla `Sender`, aby kontrolować, jak długo skrypt powinien czekać na odpowiedź z serwera Zabbix lub proxy, zanim zrezygnuje:

```
sender = Sender(
    server='127.0.0.1',
    port=10051,
    timeout=30
)
```

Używanie pliku konfiguracyjnego agent

Możesz pozwolić, aby zabbix_utils odczytywał parametry `Server` lub `ServerActive` z lokalnego pliku konfiguracyjnego Zabbix agent lub agent 2. W takich przypadkach nie musisz określać parametrów połączenia podczas tworzenia instancji `Sender`:

```
sender = Sender(
    use_config=True,
    config_path='/etc/zabbix/zabbix_agent2.conf'
)
```

Attention:
Jeśli `ServerActive` zawiera jeden lub więcej klastrów Zabbix z wieloma instancjami serwer, `Sender` wysyła dane do pierwszego dostępnego serwer w każdym klastrze. Jeśli `ServerActive` nie jest ustawiony, używany jest adres z `Server` z domyślnym portem (10051).

Używanie szyfrowania

Sender nie zawiera wbudowanej obsługi szyfrowania, ale można ją zapewnić, tworząc opakowanie przy użyciu bibliotek zewnętrznych:

```
def psk_wrapper(sock, tls):
    # ...
    # Implementacja opakowania TLS PSK dla gniazda
    # ...

sender = Sender(
    server='127.0.0.1',
    port=10051,
    socket_wrapper=psk_wrapper
)
```

Odpowiedź dla pojedynczej wartości

Odpowiedź zwrócona przez serwer Zabbix lub proxy jest przetwarzana przez bibliotekę i zwracana jako obiekt TrapperResponse:

```
print(response)
### {"processed": 1, "failed": 0, "total": 1, "time": "0.000123", "chunk": 1}

print(response.processed)
### 1

print(response.failed)
### 0

print(response.total)
### 1
```

Tryb asynchroniczny

Tryb asynchroniczny pozwala skryptowi Python wysyłać wartości bez oczekiwania na odpowiedź z serwera Zabbix lub proxy. Może to zwiększyć wydajność skryptu, gdy musi on wysłać wiele wartości albo gdy wysłanie niektórych wartości zajmuje dużo czasu.

Podczas korzystania z trybu asynchronicznego występuje kilka istotnych różnic w porównaniu z trybem synchronicznym:

- Zaimportuj moduł asyncio języka Python (najpierw należy zainstalować wymagane zależności).
- Zaimportuj AsyncSender zamiast Sender.
- Napisz kod wewnątrz funkcji async.
- Użyj await podczas wywoływania metody send_value().

Na przykład, aby wysłać pojedynczą wartość w trybie asynchronicznym:

```
### 1. Import asyncio for asynchronous mode, and AsyncSender from zabbix_utils:
import asyncio
from zabbix_utils import AsyncSender

### 2. Define the main async function where all data sending operations (must await) will be executed:
async def main():
    sender = AsyncSender(server='127.0.0.1', port=10051)
    response = await sender.send_value('Linux server', 'service.status', 1)

    # 3. Print the response returned by Zabbix server or proxy:
    print(response)

### 4. Run the async main() function using asyncio's event loop:
asyncio.run(main())
```

Wysyłanie wielu wartości

Aby wysłać wiele wartości:

1. Przygotuj tablicę obiektów ItemValue, z których każdy używa tego samego formatu co metoda send_value().
2. Utwórz instancję Sender, podając adres IP i port serwera lub proxy Zabbix.
3. Wywołaj metodę send() (zamiast send_value()) na instancji Sender, przekazując tablicę obiektów z wartościami do wysłania.

Na przykład, aby wysłać pięć wartości do różnych hostów:

```
items = [
    ItemValue('server-de', 'service.status', 'up', 1770887205, 100),
    ItemValue('server-fr', 'service.status', 'up', 1770887205, 100),
    ItemValue('server-uk', 'service.status', 'up', 1770887205, 100),
    ItemValue('server-nl', 'service.status', 'up', 1770887205, 100),
    ItemValue('server-pl', 'service.status', 'up', 1770887205, 100),
]

sender = Sender(server='127.0.0.1', port=10051)
response = sender.send(items)
```

Używanie niestandardowego rozmiaru fragmentu

Jeśli chcesz wysłać więcej wartości, niż pozycja trapper może przyjąć w pojedynczym żądaniu, możesz podzielić je na fragmenty.

Domyślnie rozmiar fragmentu wynosi 250 wartości. Możesz go zmienić, ustawiając parametr `chunk_size` podczas tworzenia instancji `Sender`.

Na przykład, aby wysłać pięć wartości w trzech fragmentach (2-2-1), ustaw parametr `chunk_size` na 2:

```
items = [
    ItemValue('server-de', 'service.status', 'up'),
    ItemValue('server-fr', 'service.status', 'up'),
    ItemValue('server-uk', 'service.status', 'up'),
    ItemValue('server-nl', 'service.status', 'up'),
    ItemValue('server-pl', 'service.status', 'up'),
]

sender = Sender(server='127.0.0.1', port=10051, chunk_size=2)
response = sender.send(items)
```

Wysyłanie wartości do wielu klastrów Zabbix

Aby wysyłać wartości do wielu klastrów Zabbix:

1. Przygotuj tablicę klastrów Zabbix. Jeśli klaster ma wiele węzłów, wartość zostanie wysłana do pierwszego **dostępnego** węzła każdego klastra.
2. Utwórz obiekt `Sender`, podając tablicę klastrów Zabbix.
3. Wywołaj metodę `send_value()` na instancji `Sender`, używając tego samego formatu jak w metodzie `send_value()`.

Na przykład, aby wysłać wartość do pierwszego dostępnego węzła w każdym klastrze:

```
zabbix_clusters = [
    ['zabbix.cluster1.node1', 'zabbix.cluster1.node2:10051'],
    ['zabbix.cluster2.node1:10051', 'zabbix.cluster2.node2', 'zabbix.cluster2.node3']
]

sender = Sender(clusters=zabbix_clusters)
response = sender.send_value('Linux server', 'service.status', 1)
```

Odpowiedź dla wielu wartości

Domyślnie `Sender` zwraca zagregowany wynik wysyłania wartości dla wszystkich hostów lub klastrów:

```
print(response)
### {"processed": 2, "failed": 0, "total": 2, "time": "0.000108", "chunk": 2}
```

Jeśli potrzebujesz bardziej szczegółowych informacji, możesz sprawdzić wyniki dla każdego klastra i każdego fragmentu za pomocą atrybutu `response.details`:

```
print(response)
### {"processed": 2, "failed": 0, "total": 2, "time": "0.000108", "chunk": 2}

if response.failed == 0:
    print(f"Wartość została wysłana pomyślnie w {response.time}")
else:
    print(response.details)
    # {
    #     127.0.0.1:10051: [
```

```
    #         {
    #             "processed": 1,
    #             "failed": 0,
    #             "total": 1,
    #             "time": "0.000051",
    #             "chunk": 1
    #         }
    #     ],
    #     zabbix.example.local:10051: [
    #         {
    #             "processed": 1,
    #             "failed": 0,
    #             "total": 1,
    #             "time": "0.000057",
    #             "chunk": 1
    #         }
    #     ]
    # }

    for node, chunks in response.details.items():
        for resp in chunks:
            print(f"Przetworzono {resp.processed} z {resp.total} na {node.address}:{node.port}")
            # Przetworzono 1 z 1 na 127.0.0.1:10051
            # Przetworzono 1 z 1 na zabbix.example.local:10051
```

Rejestrowanie debugowania

Aby rozwiązywać problemy podczas pracy z Zabbix API, zbierania danych z Zabbix agent lub wysyłania danych do Zabbix serwer lub proxy, można włączyć rejestrowanie debugowania.

Biblioteka zabbix_utils używa standardowego modułu `logging` języka Python.

Aby wyświetlać szczegółowe komunikaty debugowania z biblioteki:

1. Zaimportuj do skryptu moduł `logging` języka Python.
2. Skonfiguruj system rejestrowania tak, aby wyprowadzał komunikaty w czytelnym formacie, i ustaw poziom rejestrowania na DEBUG.

```
import logging
from zabbix_utils import Getter

logging.basicConfig(
    format=u'[%(asctime)s] %(levelname)s %(message)s',
    level=logging.DEBUG
)

agent = Getter(host='127.0.0.1', port=10050)
resp = agent.get('system.uname')

print(resp.value)
```

Po włączeniu rejestrowania debugowania wyświetlane są szczegółowe informacje o żądaniach i odpowiedziach, na przykład:

```
[2023-10-01 12:00:01,587] DEBUG Content of the packet: b'ZBXD\x01\x0c\x00\x00\x00\x00\x00\x00\x00system.un
[2023-10-01 12:00:01,722] DEBUG Zabbix response header: b'ZBXD\x01C\x00\x00\x00C\x00\x00\x00'
[2023-10-01 12:00:01,723] DEBUG Zabbix response body: Linux test_server 5.15.0-3.60.5.1.el9uek.x86_64
[2023-10-01 12:00:01,724] DEBUG Response from [127.0.0.1:10050]: Linux test_server 5.15.0-3.60.5.1.el9uek.
Linux test_server 5.15.0-3.60.5.1.el9uek.x86_64
```

Moduły

Co to jest moduł frontendowy PHP?

- Moduł to jednostka posiadająca unikalny identyfikator, nazwę, opis, autora i inne pola zdefiniowane w pliku manifestu, wraz z PHP, JavaScript i innymi plikami znajdującymi się w jednym katalogu w katalogu *modules* instalacji frontendu Zabbix (na przykład *zabbix/ui/modules*).
- Moduł powinien spełniać proste zasady aby zapewnić poprawne działanie.
- Moduł musi zostać zainstalowany (rozpakowany) i włączony w interfejsie frontendu przez administratora.

Do czego można wykorzystać moduł

- Dodawanie nowych funkcjonalności poprzez niestandardowe sekcje frontendu;
- Tworzenie niestandardowych typów widgetów dashboardu (zobacz moduły widgetów);
- Zastąpienie lub rozszerzenie istniejącej funkcjonalności.

Do czego nie można wykorzystać modułu

- Rejestracja nowej metody API lub modyfikacja istniejącej.

Jak działają moduły

- Włączony moduł jest uruchamiany przy każdym żądaniu HTTP, przed wykonaniem kodu akcji.
- Moduł zarejestruje nowe akcje lub zdefiniuje na nowo istniejące.
- Moduł doda nowe sekcje front-endu i usunie lub zdefiniuje na nowo istniejące.
- Moduł będzie podłączał się do zdarzeń front-endu, takich jak onBeforeAction i onTerminate, jeśli będzie to konieczne.
- Żądana akcja jest ostatecznie wykonywana przez uruchomienie kodu akcji - domyślnego lub zdefiniowanego w module.

Gdzie dalej Niezależnie od tego, czy wolisz uczyć się poprzez działanie, czy najpierw przeczytać wytyczne, te strony zawierają informacje i kroki wymagane do zbudowania własnych modułów:

- Samouczki krok po kroku dotyczące pisania pierwszego modułu
- Struktura pliku modułu
- Szczegóły modułu widżetu
- Przykłady modułów do ponownego wykorzystania

Struktura plików modułu

Cały kod związany z modułem jest przechowywany w pojedynczym katalogu wewnątrz katalogu **modules** instalacji frontendu Zabbix (na przykład *zabbix/ui/modules*).

```
example_module_directory/ (wymagane)
   manifest.json (wymagane) Metadane i definicja akcji.
   Module.php Inicjalizacja modułu i obsługa zdarzeń.
   actions/   pliki kontrolera akcji.
       SomethingView.php
       SomethingCreate.php
       SomethingDelete.php
       data_export/
           ExportAsXml.php
           ExportAsExcel.php
   views/   pliki widoków.
       example.something.view.php
       example.something.delete.php
   assets/   wszelkie dodatkowe pliki do wykorzystania w widokach. Należy określić w pliku manifest.json.
       js/   skrypty JavaScript używane w widokach.
           example.something.view.js.php
       css/   pliki CSS używane w widokach.
           example.something.css
        image.png   obraz do użycia w widokach.
        example.something.file   dowolny plik do użycia w widokach.
```

Drzewo plików modułów

Tworzenie modułu Przykładowy proces tworzenia modułu składa się z następujących kroków (jeśli jest dostępny, kliknij nazwę pliku lub folderu, aby wyświetlić dodatkowe szczegóły dotyczące kroku):

1. Utwórz nowy katalog dla modułu w **zabbix/ui/modules/**.
2. Dodaj plik manifest.json z metadanymi modułu.
3. Utwórz folder *views* i zdefiniuj widok(y) modułu.
4. Utwórz folder *actions* i zdefiniuj akcję(y) modułu.
5. Utwórz plik Module.php (lub Widget.php dla widżetów pulpitu) i zdefiniuj reguły inicjalizacji i obsługi reguł.
6. Utwórz folder *assets* dla plików JavaScript (umieść w *assets/js*), stylów CSS (umieść w *assets/css*) lub innych dodatkowych plików.
7. Upewnij się, że określiłeś wymagane widoki, akcje i pliki zasobów w pliku manifest.json.
8. Zarejestruj moduł w interfejsie użytkownika Zabbix i zacznij go używać.

Note:
Możesz zarejestrować i włączyć moduł zaraz po utworzeniu pliku manifest.json. Po włączeniu modułu możesz natychmiast wyświetlić podgląd wszystkich zmian wprowadzonych do plików modułu, odświeżając interfejs użytkownika Zabbix.

manifest.json

Każdy moduł wymaga pliku manifest.json. Plik musi znajdować się w głównym katalogu (na przykład *zabbix/ui/modules/module_name/manifest*

Jako minimum plik manifest.json powinien określać następujące pola:

```
{
    "manifest_version": 2.0,
    "id": "my_ip_address",
    "name": "My IP Address",
    "namespace": "MyIPAddress",
    "version": "1.0"
}
```

Parametry obsługiwane w **manifest.json** (kliknij nazwę parametry, aby zobaczyć szczegółowy opis):

Parametr	Opis	Wymagane
manifest_version	Wersja modułu manifestu.	Tak
id	Unikalny identyfikator modułu.	
name	Nazwa modułu, która będzie wyświetlana w sekcji Administracja.	
namespace	Przestrzeń nazw PHP dla klas modułów.	
version	Wersja modułu.	
type	Typ modułu. Dla widgetu musi być ustawiony jako *widget*	Tak dla widgetów, w przeciwnym razie nie
widget	Konfiguracja widgetu. Używany tylko dla widgetów.	
actions	Akcje umożliwiające rejestrację w module.	
assets	Style CSS i pliki JavaScript do uwzględnienia.	No
author	Autor modułu.	
config	Domyślne wartości niestandardowych opcji modułów .	
description	Opis modułu.	
url	Link do opisu modułu.	

manifest_version

Wersja manifestu modułu. Obecnie obsługiwana wersja to **2.0**.

Typ: Double

Przykład:

```
"manifest_version": 2.0
```

ID

Identyfikator modułu. Musi być unikalny. Aby uniknąć przyszłych konfliktów w nazewnictwie, zaleca się używanie przedrostków dla modułów (nazwa autora, firmy lub jakakolwiek inna). Na przykład, jeśli moduł jest przykładem lekcji, a nazwa modułu to ”Mój moduł”, wówczas identyfikatorem będzie ”przykład_mój_moduł”.

Typ: String

Przykład:

```
"id": "przykład_mój_moduł"
```

name

Nazwa modułu, która będzie wyświetlana w sekcji Administracja.

Typ: String

Przykład:

```
"name": "My module"
```

namespace

Przestrzeń nazw PHP dla klas modułów.

Typ: String

Przykład:

```
"namespace": "ClockWidget"
```

version

Wersja modułu. Wersja zostanie wyświetlona w sekcji Administracja.

Typ: String

Przykład:

```
"version": "1.0"
```

type

Typ modułu. Wymagane w przypadku widgetów i musi być równe ”widget”.

Typ: String

Domyślne: ”module”

Przykład:

```
"type": "widget"
```

działania

Akcje do zarejestrowania w module. Wymagane jest zdefiniowanie klucza obiektu *class* dla każdej akcji, pozostałe klucze akcji są opcjonalne.

Typ: Obiekt

Obsługiwane klucze obiektu, jeśli *typ* to *module*:

- **write.your.action.name** (obiekt) - nazwa akcji, należy zapisać małymi literami [a-z], oddzielając słowa kropkami. Obsługuje klucze:
  - **class** (string; wymagane) - nazwa klasy akcji.
  - **layout** (string) - układ akcji. Obsługiwane wartości: *layout.json*, *layout.htmlpage* (domyślnie), *null*.
  - **view** (string) - widok akcji.

Przykład:

```
"actions": {
    "moduł.example.list": {
        "class": "ExampleList",
        "view": "example.list",
        "layout": "layout.htmlpage"
        }
    }
```

Obsługiwane klucze obiektu, jeśli *type* to *widget*:

- **widget.{id}.view** (object) - nazwa pliku i klasy dla widoku widgetu. Zamień **{id}** na wartość id widżetu (na przykład *widget.example_clock.view*). Obsługuje klucze:

    - **class** (string; wymagane) - nazwa klasy akcji dla trybu widoku widgetu w celu rozszerzenia domyślnej klasy CControllerDashboardWidgetView. Plik źródłowy klasy musi znajdować się w katalogu *actions*.
    - **view** (string) - widok widżetu. Musi znajdować się w katalogu *views*. Jeśli plik widoku to *widget.view.php*, co jest wartością domyślną, można pozostawić pustą wartość. Jeśli używasz innej nazwy, podaj ją tutaj.
- **widget.{id}.edit** (object) - nazwa pliku widoku konfiguracji widgetu. Zamień **{id}** na wartość id widżetu (na przykład *widget.example_clock.edit*). Obsługuje klucze:
    - **class** (string; wymagane) - nazwa klasy akcji dla trybu widoku konfiguracji widgetu. Plik źródłowy klasy musi znajdować się w katalogu *actions*.
    - **view** (string) - widok konfiguracji widgetu. Musi znajdować się w katalogu *views*. Jeśli plik widoku to *widget.edit.php*, co jest wartością domyślną, można pozostawić pustą wartość. Jeśli używasz innej nazwy, podaj ją tutaj.

Przykład:

```
"actions": {
    "widget.tophosts.view": {
        "class": "WidgetView"
    },
    "widget.tophosts.column.edit": {
        "class": "ColumnEdit",
        "view": "column.edit",
        "layout": "layout.json"
    }
}
```

assets

Style CSS i pliki JavaScript do uwzględnienia.

Typ: Object

Obsługiwane klucze obiektów:

- **css** (tablica) - pliki CSS do dołączenia. Pliki muszą znajdować się w katalogu *assets/css*.
- **js** (tablica) - pliki JavaScript do dołączenia. Pliki muszą znajdować się w katalogu *assets/js*.

Przykład:

```
"assets": {
    "css": ["widget.css"],
    "js": ["class.widget.js"]
}
```

author

Autor modułu. Autor zostanie wyświetlony w sekcji Administracja.

Typ: String

Przykład:

```
"author": "John Smith"
```

konfiguracja

Domyślne wartości opcji modułu. Obiekt może zawierać dowolne klucze niestandardowe. Jeśli podane, wartości te zostaną zapisane do bazy danych podczas rejestracji modułu. Nowe zmienne dodane później zostaną zapisane przy pierwszym wywołaniu. Po zapisaniu, wartości zmiennych można zmieniać wyłącznie bezpośrednio w bazie danych.

Typ: Obiekt

Przykład:

```
„config”: {
    "username": "Administrator",
    "password": "",
    "auth_url": "https://example.com/auth"
}
```

description

Opis modułu.

Typ: String

Przykład:

```
"description": "To jest widget zegara."
```

widget

Konfiguracja widgetu. Używana, jeśli *type* jest ustawiony na *widget*.

Typ: Object

Obsługiwane klucze obiektu:

- **name** (string) - używana na liście widgetów oraz jako domyślny nagłówek. Jeśli jest pusta, zostanie użyty parametr „name” z modułu.
- **size** (object) - domyślne wymiary widgetu. Obsługuje klucze:
  - *width* (integer) - domyślna szerokość widgetu.
  - *height* (integer) - domyślna wysokość widgetu.
- **form_class** (string) - klasa z formularzem pól widgetu. Musi znajdować się w katalogu *includes*. Jeśli klasą jest *WidgetForm.php*, oczekiwana domyślnie, ten parametr może zostać pominięty. W przypadku użycia innej nazwy należy ją tutaj określić.
- **js_class** (string) - nazwa klasy JavaScript dla trybu widoku widgetu, rozszerzającej domyślną klasę CWidget. Klasa zostanie załadowana wraz z pulpitem. Plik źródłowy klasy musi znajdować się w katalogu assets/js. Zobacz także: assets.
- **use_time_selector** (boolean) - określa, czy widget wymaga selektora czasu pulpitu. Obsługiwane wartości: *true*, *false* (domyślnie).
- **refresh_rate** (integer) - częstotliwość odświeżania widgetu w sekundach (domyślnie: 60).

Przykład:

```
"widget": {
    "name": "",
    "size": {
        "width": 12,
        "height": 5
    },
    "form_class": "WidgetForm",
    "js_class": "CWidget",
    "use_time_selector": false,
    "refresh_rate": 60
}
```

url

Link do opisu modułu. W przypadku widżetów ten link zostanie otwarty po kliknięciu ikony pomocy ? w oknie Dodaj widżet lub Edytuj widżet. Jeśli nie określono **url**, kliknięcie ikony pomocy spowoduje otwarcie strony ogólnej Widżety pulpitu nawigacyjnego.

Typ: Łańcuch znaków

Przykład:

```
"url": "http://example.com"
```

Akcje

Za ’logikę biznesową’ modułu odpowiadają akcje. Akcja zwykle składa się z controller i action view.

Moduł może:

- Wywołać akcje, które są już zdefiniowane w interfejsie frontowym Zabbix.
- Zastąpić akcje domyślne akcjami niestandardowymi.
- Zdefiniować zupełnie nowe akcje.

Aby zastąpić domyślne zachowanie akcji jakimś niestandardowym zachowaniem, zdefiniuj akcję o tej samej nazwie w konfiguracji modułu. Kiedy akcja zostanie wywołana, zamiast domyślnej akcji Zabbix’a zostanie wykonana akcja modułu.

Pliki akcji powinny być przechowywane w folderze *akcje*. Akcje muszą być określone w pliku manifest.json.

Kontroler

Przepływ pracy kontrolera akcji:

1. Sprawdź, czy wszystkie parametry przekazane w żądaniu HTTP są prawidłowe:

- Wywołaj metodę *checkInput()* kontrolera;
- Użyj reguł walidacji zdefiniowanych w CNewValidator.php;
- Wywołaj metodę *validateInput()*.

2. Sprawdź uprawnienia użytkownika.

3. Przygotuj dane zgodnie z przekazanymi parametrami: jeśli *checkInput()* zwróci true, Zabbix wywoła metodę *doAction()* kontrolera.

4. Przygotuj tablicę **$data** dla widoku. Użyj *CControllerResponseData* oraz metody *setResponse()*, aby zapisać odpowiedź w tablicy **$data**.

Przykład:

```
/**
 * Validate input parameters.
 *
 * @return bool
 */
protected function checkInput(): bool {
    $ret = $this->validateInput([
        'status' => 'in '.implode(',', [HOST_STATUS_MONITORED, HOST_STATUS_NOT_MONITORED])
    ]);

    if (!$ret) {
        $this->setResponse(new CControllerResponseFatal());
    }

    return $ret;
}

/**
 * Check user permissions.
 *
 * @return bool
 */
protected function checkPermissions() {
    return $this->getUserType() >= USER_TYPE_ZABBIX_ADMIN;
}

/**
 * Execute action and generate response object.
 */
protected function do Action(): void {
    $data = [
        'hosts_count' => API::Host()->get([
            'countOutput' => true,
            'filter' => [
                'status' => $this->getInput('status')
            ]
        ])
    ];

    $this->setResponse(new CControllerResponseData($data));
}
```

Note:
Pełną listę dostępnych klas kontrolerów w Zabbix można zobaczyć w kodzie źródłowym.

Widoki

Plik widoku odbiera dane z kontrolera, a następnie przygotowuje ich wygląd w HTML.

> **Note:**
> Definiowanie widoku(-ów) dla modułu frontend jest opcjonalne, chyba że moduł jest widgetem.
> Widgety pulpitu wymagają co najmniej dwóch widoków: jednego dla trybu edycji i jednego dla trybu podglądu (powinny być przechowywane w katalogu *views*).

W widoku można używać predefiniowanych klas HTML Zabbix (z */zabbix/ui/include/classes/html*), a także dodawać nowe klasy HTML i CSS. Nowe klasy powinny być przechowywane w folderze *assets* modułu.

Przykład:

```
...
(new CColHeader(_('Name')))
```

Spowoduje to dodanie nowej nazwy kolumny *Name* oraz nadanie stylu górnemu wierszowi tabeli tak jak na innych stronach Zabbix.

Widok akcji

To jest plik referencyjny do definiowania widoku akcji.

```
<?php declare(strict_types = 1);

/**
* @var CView $this
*/

$this->includeJsFile('example.something.view.js.php');

(new CWidget())
    ->setTitle(_('Something view'))
    ->addItem(new CDiv($data['name']))
    ->addItem(new CPartial('module.example.something.reusable', [
        'contacts' => $data['contacts']
    ]))
    ->show();
```

Aktywa

Folder *assets* może zawierać dowolne pliki i podfoldery, które nie należą do innych katalogów. Możesz go używać do:

- Styli JavaScript (muszą znajdować się w *assets/js*);
- Styli CSS (muszą znajdować się w *assets/css*);
- Obrazów;
- Czcionek;
- Wszystkiego innego, co chcesz uwzględnić.

assets/js

Katalog *assets/js* jest zastrzeżony i powinien zawierać wyłącznie pliki JavaScript. Aby widget mógł używać tych plików, określ je w pliku *manifest.json*.

Na przykład:

```
"assets": {
    "js": ["class.widget.js"]
}
```

assets/css

Katalog *assets/css* jest zastrzeżony i powinien zawierać wyłącznie pliki stylu CSS. Aby widget mógł używać tych plików, określ je w pliku *manifest.json*.

Na przykład:

```
"assets": {
    "css": ["mywidget.css"]
}
```

Style CSS

Pliki CSS mogą zawierać niestandardowy atrybut „theme” w celu zdefiniowania innego stylu dla określonych motywów frontendu.

Dostępne motywy i ich wartości atrybutów:

- **Niebieski** - [theme='blue-theme']
- **Ciemny** - [theme='dark-theme']
- **Jasny o wysokim kontraście** - [theme='hc-light']
- **Ciemny o wysokim kontraście** - [theme='hc-dark']

Przykład:

```
.widget {
    background-color: red;
}

[theme='dark-theme'] .widget {
    background-color: gren;
}
```

Zarejestruj nowy moduł

Ta sekcja wyjaśnia jak dodać nowy moduł do frontendu Zabbix.

Wymagania wstępne Przed kontynuowaniem upewnij się, że:

- Moduł znajduje się w katalogu *moduły* (modules) instalacji front-endu Zabbix (na przykład *zabbix/ui/modules*).
- Moduł ma co najmniej podstawową wersję pliku manifest.json.
- Masz dostęp do sekcji menu Administracja w Zabbix (wymaga roli użytkownika Super administrator).

> **Note:**
> The frontend will not install or even recognize incompatible modules.

Dodawanie modułu Otwórz stronę *Administracja* → *Ogólne* → *Moduły* i naciśnij *Skanuj katalog*.



Znajdź swój moduł na liście i aktywuj go.

Aby aktywować moduł, naciśnij hiperłącze *Wyłączony* - stan modułu zmieni się na *Włączony*.

Po naciśnięciu na nazwę modułu można wyświetlić dodatkowe informacje o module, takie jak autor, wersja czy krótki opis (jeśli został zdefiniowany w manifeście).

Podgląd widżetu Moduły widżetów po dodaniu stają się natychmiast widoczne na liście widżetów pulpitu.

Możesz otworzyć pulpit, przełączyć się do trybu edycji i dodać widżet do pulpitu jak zwykle.

Po wprowadzeniu zmian w widżecie odśwież pulpit, aby zobaczyć, jak widżet wygląda po najnowszych aktualizacjach.

Widżety

Widżety to moduły front-endu Zabbix używane w pulpitach nawigacyjnych. O ile nie zaznaczono inaczej, wszystkie wytyczne dotyczące modułów mają zastosowanie również do widżetów.

Jednak widżet różni się znacząco od modułu. Aby zbudować widżet:

- określ typ "widget" w pliku manifest.json ("type": "widget");
- uwzględnij co najmniej dwa widoki: jeden dla trybu prezentacji widżetu i jeden dla trybu konfiguracji widżetu (example.widget.view.php i example.widget.edit.php);
- i kontroler dla prezentacji widżetu (WidgetView.php);
- użyj i rozszerz domyślne klasy widżetów.

Konfiguracja

Konfiguracja widżetu jest częścią modułu widżetu, która pozwala użytkownikowi definiować ustawienia widżetu dla prezentacja. Ta strona opisuje klasy, które mogą być użyte do stworzenia formularza konfiguracji widżetu z niestandardowymi polami.

Widżet

Główna klasa widżetu, rozszerzająca bazową klasę wszystkich widżetów pulpitu - *CWidget*. Wymagana do nadpisania domyślnego zachowania widżetu.

Klasa Widget powinna znajdować się w katalogu głównym widżetu (na przykład, zabbix/ui/modules/my_custom_widget).

Przykład Widget.php

```
<?php

namespace Modules\MyCustomWidget;

use Zabbix\Core\CWidget;

class Widget extends CWidget {

    public const MY_CONSTANT = 0;

    public function getTranslationStrings(): array {
        return [
            'class.widget.js' => [
                'No data' => _('No data')
            ]
        ];
    }
}
```

WidgetForm

Klasa *WidgetForm* rozszerza domyślną klasę *CWidgetForm* i zawiera zestaw pól *CWidgetField*, które są wymagane do zdefiniowania struktury przechowywania konfiguracji widgetu w bazie danych oraz obsługi walidacji danych wejściowych.

Klasa *WidgetForm* powinna znajdować się w katalogu *includes*. Jeśli klasa ma inną nazwę, należy ją określić w parametrze *widget/form_class* w pliku *manifest.json*.

Przykład pliku includes/WidgetForm.php

```
<?php

namespace Modules\MyCustomWidget\Includes;

use Modules\MyCustomWidget\Widget;

use Zabbix\Widgets\{
    CWidgetField,
    CWidgetForm
};

use Zabbix\Widgets\Fields\{
    CWidgetFieldMultiSelectItem,
    CWidgetFieldTextBox,
    CWidgetFieldColor
};


class WidgetForm extends CWidgetForm {

    public const DEFAULT_COLOR_PALETTE = [
        'FF465C', 'B0AF07', '0EC9AC', '524BBC', 'ED1248', 'D1E754', '2AB5FF', '385CC7', 'EC1594', 'BAE37D'
        '6AC8FF', 'EE2B29', '3CA20D', '6F4BBC', '00A1FF', 'F3601B', '1CAE59', '45CFDB', '894BBC', '6D6D6D'
    ];
```

```
    public function addFields(): self {
        return $this
            ->addField(
                (new CWidgetFieldMultiSelectItem('itemid', _('Item')))
                    ->setFlags(CWidgetField::FLAG_NOT_EMPTY | CWidgetField::FLAG_LABEL_ASTERISK)
                    ->setMultiple(false)
            )
            ->addField(
                new CWidgetFieldTextBox('description', _('Description'))
            )
            ->addField(
                (new CWidgetFieldColor('chart_color', _('Color')))->setDefault('FF0000')
            );
    }
}
```

CWidgetFormView

Klasa *CWidgetFormView* jest wymagana do określenia logiki prezentacji pól zdefiniowanych w klasie *WidgetForm*, określając ich wygląd i zachowanie podczas renderowania w widoku konfiguracji.

Klasa *CWidgetFormView* obsługuje następujące metody:

- *addField()* - przyjmuje jako parametr instancję klasy *CWidgetFieldView*; każda klasa *CWidgetField* ma odpowiadającą jej klasę *CWidgetFieldView* do użycia w widoku konfiguracji widgetu.
- *addFieldset()* - przyjmuje instancję klasy *CWidgetFieldsGroupView*, która łączy pola w zwijany kontener.
- *addFieldsGroup()* - przyjmuje instancję *CWidgetFormFieldsetCollapsibleView*, która wizualnie (za pomocą obramowania) łączy pola w grupę.
- *includeJsFile()* - umożliwia dodanie pliku JavaScript do widoku konfiguracji widgetu.
- *addJavaScript()* - umożliwia dodanie osadzonego kodu JavaScript, który zostanie wykonany natychmiast po załadowaniu widoku konfiguracji widgetu.

Klasa *CWidgetFormView* powinna znajdować się w katalogu *views*.

Przykład views/widget.edit.php

```
<?php

/**
 * Widok formularza mojego niestandardowego widgetu.
 *
 * @var CView $this
 * @var array $data
 */

use Modules\MyCustomWidget\Includes\WidgetForm;

(new CWidgetFormView($data))
    ->addField(
        (new CWidgetFieldMultiSelectItemView($data['fields']['itemid']))->setPopupParameter('numeric', tru
    )
    ->addFieldset(
        (new CWidgetFormFieldsetCollapsibleView(_('Konfiguracja zaawansowana')))
            ->addField(
                new CWidgetFieldTextBoxView($data['fields']['description'])
            )
            ->addField(
                new CWidgetFieldColorView($data['fields']['chart_color'])
            )
    )
    ->includeJsFile('widget.edit.js.php')
    ->addJavaScript('my_custom_widget_form.init('.json_encode([
        'color_palette' => WidgetForm::DEFAULT_COLOR_PALETTE
    ]).');')
    ->show();
```

JavaScript

Klasa JavaScript może być użyta do dodania dynamicznego zachowania i interaktywności do widoku konfiguracji widżetu. Na przykład, można zainicjować selektor kolorów, zdefiniowany w klasie *CWidgetFormView*.

Klasa JavaScript powinna zostać załadowana wraz z formularzem, dlatego należy odwołać się do niej w klasie *CWidgetFormView* za pomocą metod *includeJsFile()* i *addJavaScript()*.

W poniższym przykładzie instancja klasy singleton jest natychmiast tworzona i przechowywana pod nazwą *window.my_custom_widget_form*. W ten sposób otwarcie formularza po raz drugi spowoduje ponowne utworzenie instancji.

Klasa JavaScript powinna znajdować się w katalogu *views*.

views/widget.edit.js.php example

```
<?php

use Modules\MyCustomWidget\Widget;

?>

window.my_custom_widget_form = new class {

    init({color_palette}) {
        colorPalette.setThemeColors(color_palette);

        for (const colorpicker of jQuery('.<?= ZBX_STYLE_COLOR_PICKER ?> input')) {
            jQuery(colorpicker).colorpicker();
        }

        const overlay = overlays_stack.getById('widget_properties');

        for (const event of ['overlay.reload', 'overlay.close']) {
            overlay.$dialogue[0].addEventListener(event, () => { jQuery.colorpicker('hide'); });
        }
    }
};
```

CWidgetField

Klasa *CWidgetField* jest klasą bazową, po której dziedziczą wszystkie klasy pól formularza (*CWidgetFieldCheckBox*, *CWidgetFieldTextArea*, *CWidgetFieldRadioButtonList* itd.). Klasy rozszerzające *CWidgetField* odpowiadają za odbieranie, zapisywanie i walidację wartości konfiguracji widżetu.

Dostępne są następujące klasy *CWidgetField*.

CWidgetField class	Database field type	Description
CWidgetFieldCheckBox	int32	Pojedyncze pole wyboru.
CWidgetFieldCheckBoxList	array of int32	Wiele pól wyboru w ramach jednego pola konfiguracyjnego.
CWidgetFieldColor	string	Pole wyboru koloru.
CWidgetFieldDatePicker	string	Pole wyboru daty.
CWidgetFieldHostPatternSelect	string	Pole wielokrotnego wyboru umożliwiające wybranie jednego lub wielu hostów. Obsługuje definiowanie wzorców nazw hostów (zostaną wybrane wszystkie pasujące hosty).
CWidgetFieldIntegerBox	int32	Pole do wprowadzania liczby całkowitej. Może być używane do konfiguracji wartości minimalnych i maksymalnych.
CWidgetFieldLatLng	string	Pole tekstowe umożliwiające wprowadzenie szerokości geograficznej, długości geograficznej i poziomu powiększenia mapy, oddzielonych przecinkami.
CWidgetFieldMultiSelectActionID		Pole wielokrotnego wyboru do wybierania akcji (z listy akcji zdefiniowanych w *Alerts → Actions*).
CWidgetFieldMultiSelectGraphID		Pole wielokrotnego wyboru do wybierania wykresów niestandardowych.
CWidgetFieldMultiSelectGraphIDPrototype		Pole wielokrotnego wyboru do wybierania prototypów wykresów niestandardowych.
CWidgetFieldMultiSelectGroupID		Pole wielokrotnego wyboru do wybierania grup hostów.
CWidgetFieldMultiSelectHostID		Pole wielokrotnego wyboru do wybierania hostów.

CWidgetField class	Database field type	Description
CWidgetFieldMultiSelectItem	ID	Pole wielokrotnego wyboru do wybierania pozycji.
CWidgetFieldMultiSelectItemPattern	ID	Pole wielokrotnego wyboru do wybierania wzorców pozycji.
CWidgetFieldMultiSelectItemPrototype	ID	Pole wielokrotnego wyboru do wybierania prototypów pozycji.
CWidgetFieldMultiSelectMap	ID	Pole wielokrotnego wyboru do wybierania map.
CWidgetFieldMultiSelectMediaType	ID	Pole wielokrotnego wyboru do wybierania typów mediów.
CWidgetFieldMultiSelectOverrideHost	ID	Pole wielokrotnego wyboru do wybierania źródła danych (pulpitu lub innego widżetu) zawierającego host, dla którego widżet może wyświetlać dane.
CWidgetFieldMultiSelectService	ID	Pole wielokrotnego wyboru do wybierania usług.
CWidgetFieldMultiSelectSla	ID	Pole wielokrotnego wyboru do wybierania SLA.
CWidgetFieldMultiSelectUser	ID	Pole wielokrotnego wyboru do wybierania użytkowników.
CWidgetFieldNumericBox	string	Pole do wprowadzania liczby zmiennoprzecinkowej.
CWidgetFieldRadioButtonList	int32	Grupa przycisków opcji składająca się z jednego lub większej liczby przycisków opcji.
CWidgetFieldRangeControl	int32	Suwak do wybierania wartości typu całkowitego.
CWidgetFieldReference	string	Tworzy unikalny identyfikator tego widżetu na pulpicie. Jest używany do odwoływania się do tego widżetu z innych widżetów.
CWidgetFieldSelect	int32	Rozwijane pole wyboru.
CWidgetFieldSeverities	array of int32	*CWidgetFieldCheckBoxList* z predefiniowanymi poziomami ważności wyzwalaczy.
CWidgetFieldTags	array of (string, int32, string)	Umożliwia skonfigurowanie jednego lub wielu wierszy filtra tagów.
CWidgetFieldTextArea	string	Obszar tekstowy do wprowadzania tekstu wielowierszowego.
CWidgetFieldTextBox	string	Pole tekstowe do wprowadzania tekstu jednowierszowego.
CWidgetFieldTimePeriod	array of string	Pole wyboru okresu czasu.
CWidgetFieldTimeZone	string	Lista rozwijana ze strefami czasowymi.
CWidgetFieldThresholds	array of (string, string)	Umożliwia skonfigurowanie par kolorów i liczb.
CWidgetFieldUrl	string	Pole tekstowe umożliwiające wprowadzanie adresów URL.

Następujące klasy *CWidgetField* zostały utworzone dla konkretnych widżetów. Klasy te mają bardzo specyficzne zastosowania, ale w razie potrzeby mogą być również używane ponownie.

CWidgetField class	Database field type	Description
CWidgetFieldColumnsList	array of (multiple mixed)	Dla widżetu *Top hosts*. Tworzy tabelę z niestandardowymi kolumnami dozwolonych typów.
CWidgetFieldNavTree	string	Dla widżetu *Map navigation tree*. Zastępuje widok widżetu w trybie edycji drzewem wyboru map.

Prezentacja

Ta strona opisuje komponenty, których można użyć do utworzenia widoku prezentacji widżetu. Widok prezentacji widżetu to część widżetu, która odbiera dane zgodnie z jego konfiguracją i wyświetla je na pulpicie nawigacyjnym w kontenerze.

Widok prezentacji składa się z trzech części:

- Widget action
- Widok widżetu
- JavaScript

Akcja widgetu

Klasa akcji widgetu (*WidgetView*) zawiera metody operacji na widgetach w trybie widoku prezentacji. Większość akcji widgetów używa domyślnej klasy kontrolera *CControllerDashboardWidgetView* i/lub ją rozszerza.

Klasa akcji widgetu powinna znajdować się w katalogu *actions* i być określona w parametrze *actions* (*actions/widget.{id}.view/class*) w pliku *manifest.json*.

Przykład actions/WidgetView.php (zaimplementowany w natywnym widżecie Zabbix *Informacje o systemie*)

```
class WidgetView extends CControllerDashboardWidgetView {

    protected function doAction(): void {
```

```
        $this->setResponse(new CControllerResponseData([
            'name' => $this->getInput('name', $this->widget->getDefaultName()),
            'system_info' => CSystemInfoHelper::getData(),
            'info_type' => $this->fields_values['info_type'],
            'user_type' => CWebUser::getType(),
            'user' => [
                'debug_mode' => $this->getDebugMode()
            ]
        ]));
    }
}
```

Widok widgetu

Klasa widoku widgetu (*CWidgetView*) odpowiada za budowanie widoku prezentacji widgetu.

Klasa widoku widgetu powinna znajdować się w katalogu *views*. Jeśli plik zawierający klasę widoku widgetu ma inną nazwę niż domyślna (*widget.view.php*), należy ją określić w parametrze *actions* pliku *manifest.json* (*actions/widget.{id}.view/view*).

Przykład views/widget.view.php

```
<?php

/**
 * Mój niestandardowy widok widgetu.
 *
 * @var CView $this
 * @var array $data
 */

(new CWidgetView($data))
    ->addItem(
        new CTag('h1', true, $data['name'])
    )
    ->show();
```

JavaScript

Klasa JavaScript odpowiada za określanie zachowania widżetu, takiego jak aktualizowanie danych widżetu, zmiana rozmiaru widżetu, wyświetlanie elementów widżetu itp.

Wszystkie operacje JavaScript używają i/lub rozszerzają bazową klasę JavaScript wszystkich widżetów pulpitu - *CWidget*. Klasa *CWidget* zawiera zestaw metod z domyślną implementacją zachowania widżetu. W zależności od złożoności widżetu metody te mogą być używane bez zmian lub rozszerzane.

Klasa *CWidget* zawiera następujące metody:

- Metody definiujące cykl życia widżetu: *onInitialize()*, *onStart()*, *onActivate()*, *onDeactivate()*, *onDestroy()*, *onEdit()*.
- Metody obsługujące aktualizację i wyświetlanie danych widżetu: *promiseUpdate()*, *getUpdateRequestData()*, *processUpdateResponse(response)*, *processUpdateErrorResponse(error)*, *setContents(response)*.
- Metody modyfikujące wygląd widżetu: *onResize()*, *hasPadding()*.

Klasa JavaScript powinna znajdować się w katalogu *assets/js* i być określona w parametrze *assets* (*assets/js*) w pliku *manifest.json*.

Metody cyklu życia

Metody cyklu życia widżetu są wywoływane przez pulpit nawigacyjny oraz na różnych etapach cyklu życia widżetu podczas jego istnienia w pulpicie nawigacyjnym.

Metoda ***onInitialize()*** definiuje początkowy stan i/lub wartości widżetu, bez wykonywania jakichkolwiek manipulacji HTML lub danymi. Metoda ta jest wywoływana, gdy tworzony jest widżet (tworzona jest instancja obiektu widżetu), zazwyczaj poprzez dodanie widżetu do strony pulpitu nawigacyjnego lub załadowanie strony pulpitu nawigacyjnego.

Przykład:

```
onInitialize() {
    this._time_offset = 0;
    this._interval_id = null;
    this._clock_type = CWidgetClock.TYPE_ANALOG;
    this._time_zone = null;
```

```
    this._show_seconds = true;
    this._time_format = 0;
    this._tzone_format = 0;
    this._show = [];
    this._has_contents = false;
    this._is_enabled = true;
}
```

Metoda ***onStart()*** definiuje strukturę HTML widgetu, bez wykonywania jakiejkolwiek manipulacji danymi. Ta metoda jest wywoływana przed pierwszą aktywacją strony pulpitu, czyli zanim pulpit i jego widgety zostaną w pełni wyświetlone użytkownikowi.

Przykład:

```
onStart() {
    this._events.resize = () => {
        const padding = 25;
        const header_height = this._view_mode === ZBX_WIDGET_VIEW_MODE_HIDDEN_HEADER
            ? 0
            : this._header.offsetHeight;

        this._target.style.setProperty(
            '--content-height',
            `${this._cell_height * this._pos.height - padding * 2 - header_height}px`
        );
    }
}
```

Metoda ***onActivate()*** uaktywnia widget i czyni go interaktywnym poprzez włączenie niestandardowych detektorów zdarzeń (służących do reagowania na działania użytkownika) oraz zainicjowanie cyklu aktualizacji widgetu (aby utrzymywać jego zawartość na bieżąco). Ta metoda jest wywoływana po aktywacji strony pulpitu, czyli gdy zostanie ona w pełni wyświetlona w interfejsie użytkownika.

Należy pamiętać, że przed wywołaniem metody *onActivate()* widget znajduje się w stanie nieaktywnym (`WIDGET_STATE_INACTIVE`). Po pomyślnym wywołaniu widget przechodzi do stanu aktywnego (`WIDGET_STATE_ACTIVE`). W stanie aktywnym widget reaguje na działania, nasłuchuje zdarzeń, okresowo aktualizuje swoją zawartość i może współdziałać z innymi widgetami.

Przykład:

```
onActivate() {
    this._startClock();

    this._resize_observer = new ResizeObserver(this._events.resize);
    this._resize_observer.observe(this._target);
}
```

Metoda ***onDeactivate()*** zatrzymuje wszelką aktywność i interaktywność widżetu przez dezaktywację niestandardowych nasłuchiwaczy zdarzeń oraz zatrzymanie cyklu aktualizacji widżetu. Ta metoda jest wywoływana, gdy strona pulpitu jest dezaktywowana, to znaczy po przełączeniu na inną stronę lub usunięciu, albo gdy widżet zostanie usunięty ze strony pulpitu.

Należy pamiętać, że przed wywołaniem metody *onDeactivate()* widżet znajduje się w stanie aktywnym (`WIDGET_STATE_ACTIVE`). Po pomyślnym wywołaniu widżet przechodzi do stanu nieaktywnego (`WIDGET_STATE_INACTIVE`).

Przykład:

```
onDeactivate() {
    this._stopClock();
    this._resize_observer.disconnect();
}
```

Metoda ***onDestroy()*** wykonuje zadania porządkowe przed usunięciem widgetu z dashboardu, co może obejmować zamknięcie połączenia z bazą danych ustanowionego podczas inicjalizacji widgetu, usunięcie danych tymczasowych w celu zwolnienia pamięci systemowej i uniknięcia wycieków zasobów, wyrejestrowanie detektorów zdarzeń związanych ze zdarzeniami zmiany rozmiaru lub kliknięciami przycisków, aby zapobiec niepotrzebnej obsłudze zdarzeń i wyciekom pamięci itd. Ta metoda jest wywoływana, gdy widget lub strona dashboardu, która go zawiera, zostaje usunięta.

Należy pamiętać, że przed wywołaniem metody *onDestroy()* widget w stanie aktywnym (`WIDGET_STATE_ACTIVE`) jest zawsze dezaktywowany przez wywołanie metody *onDeactivate()*.

Przykład:

```
onDestroy() {
    if (this._filter_widget) {
        this._filter_widget.off(CWidgetMap.WIDGET_NAVTREE_EVENT_MARK, this._events.mark);
        this._filter_widget.off(CWidgetMap.WIDGET_NAVTREE_EVENT_SELECT, this._events.select);
    }
}
```

Metoda ***onEdit()*** definiuje wygląd i zachowanie widżetu, gdy pulpit przechodzi w tryb edycji. Ta metoda jest wywoływana, gdy pulpit przechodzi w tryb edycji, zazwyczaj gdy użytkownik użyje przycisku *Edytuj* widżetu lub przycisku *Edytuj pulpit* na pulpicie.

Przykład:

```
onEdit() {
    this._deactivateGraph();
}
```

Metoda procesu aktualizacji

Metoda procesu aktualizacji widżetu są odpowiedzialne za pobieranie zaktualizowanych danych z serwera Zabbix lub dowolnego innego źródła danych i wyświetlanie ich w widżecie.

Metoda ***promiseUpdate()*** inicjuje proces aktualizacji danych przez pobieranie danych, zazwyczaj za pomocą żądań web lub wywołań API. Ta metoda jest wywoływana, gdy strona pulpitu jest wyświetlana, a następnie okresowo, aż strona pulpitu zostanie przełączona na inną stronę pulpitu.

Poniżej przedstawiono przykład domyślnej implementacji metody *promiseUpdate()* używanej przez większość natywnych widgetów Zabbix. W domyślnej implementacji metoda *promiseUpdate()* stosuje ogólny wzorzec pobierania danych z serwera. Tworzy nowy obiekt `Curl` z odpowiednim adresem URL i parametrami żądania, wysyła żądanie POST za pomocą metody *fetch()* z obiektem danych zbudowanym przez metodę *getUpdateRequestData()*, a następnie odpowiednio przetwarza odpowiedź (lub odpowiedź błędu) za pomocą *processUpdateResponse(response)* lub *processUpdateErrorResponse(error)*. Ta implementacja jest odpowiednia dla większości widgetów, ponieważ zazwyczaj pobierają one dane w formacie JSON i obsługują je w spójny sposób.

```
promiseUpdate() {
    const curl = new Curl('zabbix.php');

    curl.setArgument('action', `widget.${this._type}.view`);

    return fetch(curl.getUrl(), {
        method: 'POST',
        headers: {'Content-Type': 'application/json'},
        body: JSON.stringify(this.getUpdateRequestData()),
        signal: this._update_abort_controller.signal
    })
        .then((response) => response.json())
        .then((response) => {
            if ('error' in response) {
                this.processUpdateErrorResponse(response.error);

                return;
            }

            this.processUpdateResponse(response);
        });
    }
```

Metoda ***getUpdateRequestData()*** przygotowuje dane żądania do serwera na potrzeby aktualizacji widżetu, zbierając różne właściwości i odpowiadające im wartości (identyfikatory widżetu, ustawienia filtrów, zakresy czasu itp.) ze stanu i konfiguracji widżetu, a następnie tworząc obiekt danych reprezentujący informacje wymagane do wysłania do serwera w żądaniu aktualizacji. Ta metoda jest wywoływana wyłącznie jako część domyślnej metody *promiseUpdate()*, czyli podczas procesu aktualizacji widżetu.

Domyślna implementacja:

```
getUpdateRequestData() {
    return {
        templateid: this._dashboard.templateid ?? undefined,
        dashboardid: this._dashboard.dashboardid ?? undefined,
        widgetid: this._widgetid ?? undefined,
```

```
        name: this._name !== '' ? this._name : undefined,
        fields: Object.keys(this._fields).length > 0 ? this._fields : undefined,
        view_mode: this._view_mode,
        edit_mode: this._is_edit_mode ? 1 : 0,
        dynamic_hostid: this._dashboard.templateid !== null || this.supportsDynamicHosts()
            ? (this._dynamic_hostid ?? undefined)
            : undefined,
        ...this._contents_size
    };
}
```

Metoda ***processUpdateResponse(response)*** obsługuje odpowiedź otrzymaną z serwera po żądaniu aktualizacji i, jeśli proces aktualizacji zakończył się powodzeniem i bez błędów, czyści dane widżetu oraz wyświetla nową zawartość za pomocą metody *setContents()*. Ta metoda jest wywoływana wyłącznie jako część domyślnej metody *promiseUpdate()*, czyli podczas procesu aktualizacji widżetu.

Domyślna implementacja:

```
processUpdateResponse(response) {
    this._setHeaderName(response.name);

    this._updateMessages(response.messages);
    this._updateInfo(response.info);
    this._updateDebug(response.debug);

    this.setContents(response);
}
```

Metoda ***processUpdateErrorResponse(error)*** obsługuje odpowiedź otrzymaną z serwera po żądaniu aktualizacji, jeśli odpowiedź zawiera błąd, i wyświetla komunikat/-y o błędzie. Ta metoda jest wywoływana wyłącznie jako część domyślnej metody *promiseUpdate()*, czyli podczas procesu aktualizacji widżetu.

Domyślna implementacja:

```
processUpdateErrorResponse(error) {
    this._updateMessages(error.messages, error.title);
}
```

Metoda ***setContents(response)*** wyświetla zawartość widżetu, jeśli proces aktualizacji widżetu zakończył się pomyślnie i bez błędów, co może obejmować manipulowanie elementami DOM, aktualizowanie komponentów interfejsu użytkownika, stosowanie stylów lub formatowania itp. Ta metoda jest wywoływana wyłącznie jako część domyślnej metody *processUpdateResponse(response)*, czyli podczas obsługi odpowiedzi otrzymanej z serwera po żądaniu aktualizacji.

Domyślna implementacja:

```
setContents(response) {
    this._body.innerHTML = response.body ?? '';
}
```

Metoda modyfikacji prezentacji

Metoda modyfikacji prezentacji widżetu jest odpowiedzialna za modyfikację wyglądu widżetu.

Metoda ***onResize()*** odpowiada za dostosowanie elementów wizualnych widgetu do nowego rozmiaru widgetu, co może obejmować zmianę rozmieszczenia elementów, dostosowanie wymiarów elementów, obcinanie tekstu, implementację lazy loading w celu poprawy responsywności podczas zmiany rozmiaru itp. Ta metoda jest wywoływana, gdy widget zmienia rozmiar, na przykład gdy użytkownik ręcznie zmienia rozmiar widgetu lub gdy zmieniany jest rozmiar okna przeglądarki.

Przykład:

```
onResize() {
    if (this.getState() === WIDGET_STATE_ACTIVE) {
        this._startUpdating();
    }
}
```

Metoda ***hasPadding()*** odpowiada za zastosowanie pionowego dopełnienia 8 px u dołu widżetu, gdy jest on skonfigurowany tak, aby wyświetlać nagłówek. Ta metoda jest wywoływana po aktywowaniu strony pulpitu, czyli gdy staje się ona stroną wyświetlaną w interfejsie użytkownika.

Implementacja domyślna:

```
hasPadding() {
    return this.getViewMode() !== ZBX_WIDGET_VIEW_MODE_HIDDEN_HEADER;
}
```

W przypadku niektórych widżetów konieczne jest wykorzystanie całej dostępnej przestrzeni widżetu do skonfigurowania na przykład niestandardowego koloru tła. Poniżej przedstawiono przykład implementacji metody *hasPadding()* używanej w natywnym widżecie Zabbix *Wartość pozycji*.

```
hasPadding() {
    return false;
}
```

Poradniki

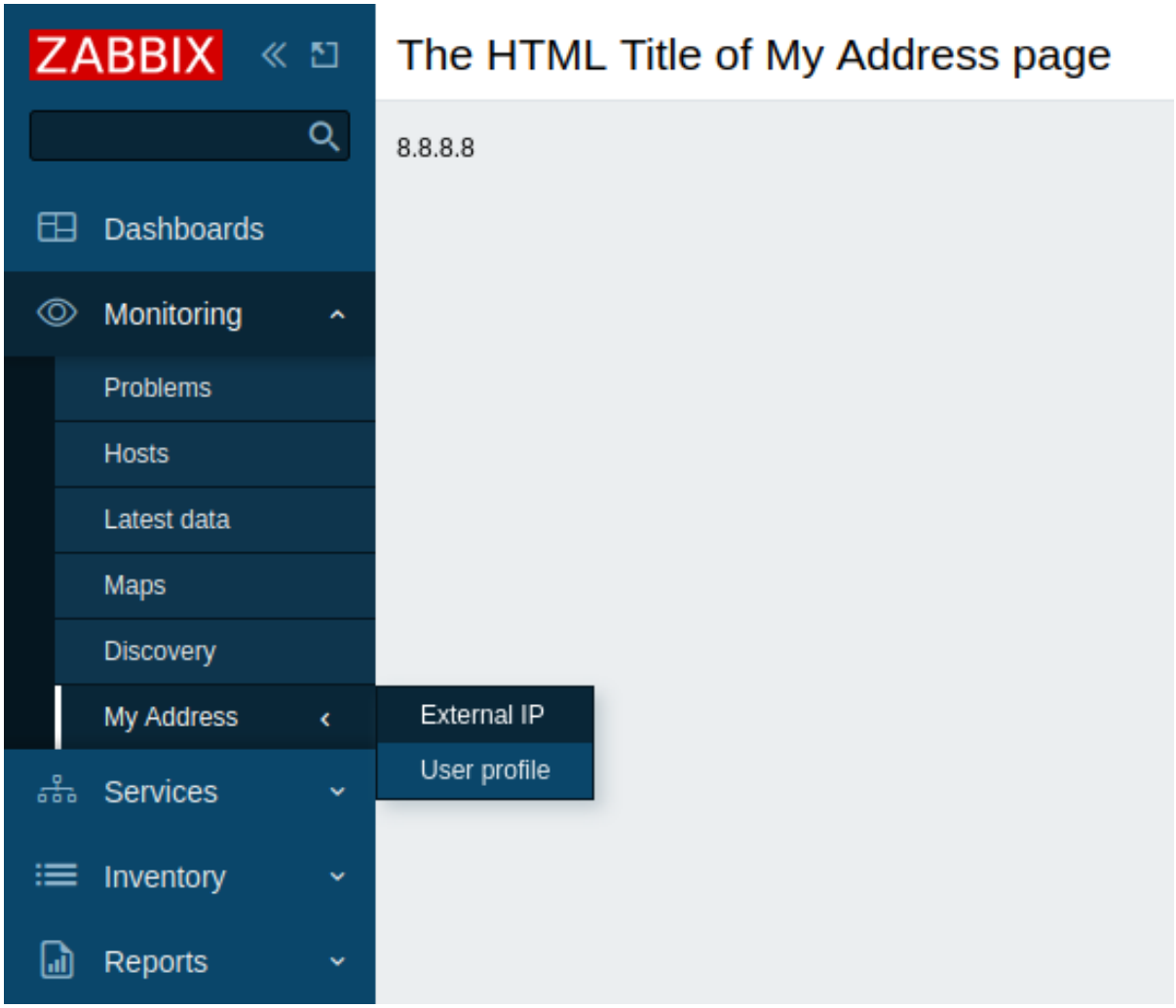
Ta sekcja zawiera praktyczne instrukcje krok po kroku, które pokazują, jak stworzyć własny moduł oraz widżet w Zabbix.

Utwórz moduł (samouczek)

To jest samouczek krok po kroku, który pokazuje, jak utworzyć prosty moduł front-endu Zabbix. Możesz pobrać wszystkie pliki tego modułu jako archiwum ZIP: MyAddress.zip.

Co zbudujesz

Podczas tego samouczka najpierw zbudujesz moduł front-end, który dodaje nową sekcję menu *Mój adres*, a następnie przekonwertujesz go na bardziej zaawansowany moduł front-end, który wysyła żądanie HTTP do *https://api.seeip.org* i wyświetla odpowiedź — adres IP Twojego komputera — na nowej stronie w nowo utworzonej sekcji menu *Mój adres*. Oto jak będzie wyglądał ukończony moduł:



Część I - Podstawowy moduł

Dodaj pusty moduł do frontendu Zabbix

1. Utwórz katalog *MyAddress* w katalogu *modules* instalacji frontendu Zabbix (na przykład *zabbix/ui/modules*).
2. Utwórz plik *manifest.json* z podstawowymi metadanymi modułu (zobacz opis obsługiwanych parametrów).

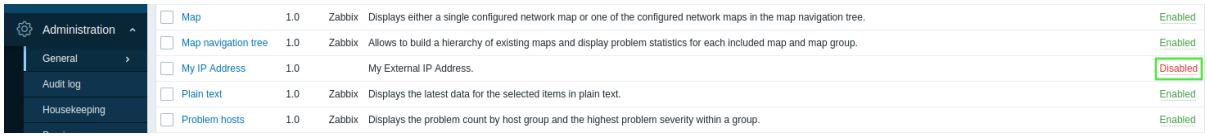
ui/modules/MyAddress/manifest.json

```
{
"manifest_version": 2.0,
"id": "my-address",
"name": "My IP Address",
"version": "1.0",
"namespace": "MyAddress",
"description": "My External IP Address."
}
```

3. W interfejsie użytkownika Zabbix przejdź do sekcji *Administracja* → *Ogólne* → *Moduły* i kliknij przycisk *Skanuj katalog*.



4. Znajdź nowy moduł *My IP Address* na liście i kliknij hiperłącze „Wyłączony”, aby zmienić status modułu z „Wyłączony” na „Włączony” (jeśli nie widzisz swojego modułu na liście, sprawdź uprawnienia).



Moduł jest teraz zarejestrowany w frontendzie. Jednak nie jest jeszcze widoczny, ponieważ nadal musisz zdefiniować funkcjonalność modułu. Po dodaniu zawartości do katalogu modułu, natychmiast zobaczysz zmiany w frontendzie Zabbix po odświeżeniu strony.

Utwórz sekcję menu

1. Utwórz plik *Module.php* w katalogu *MyAddress*.

Ten plik implementuje nową klasę *Module*, która rozszerza domyślną klasę *CModule*. Klasa *Module* wstawi nową sekcję menu *My Address* do menu głównego.

Metoda *setAction()* określa akcję, która zostanie wykonana po kliknięciu sekcji menu. Na początek możesz użyć wstępnie zdefiniowanej akcji *userprofile.edit*, która otworzy stronę *User profile*. W części III tego samouczka dowiesz się, jak utworzyć niestandardową akcję.

ui/modules/MyAddress/Module.php

```
<?php

namespace Modules\MyAddress;

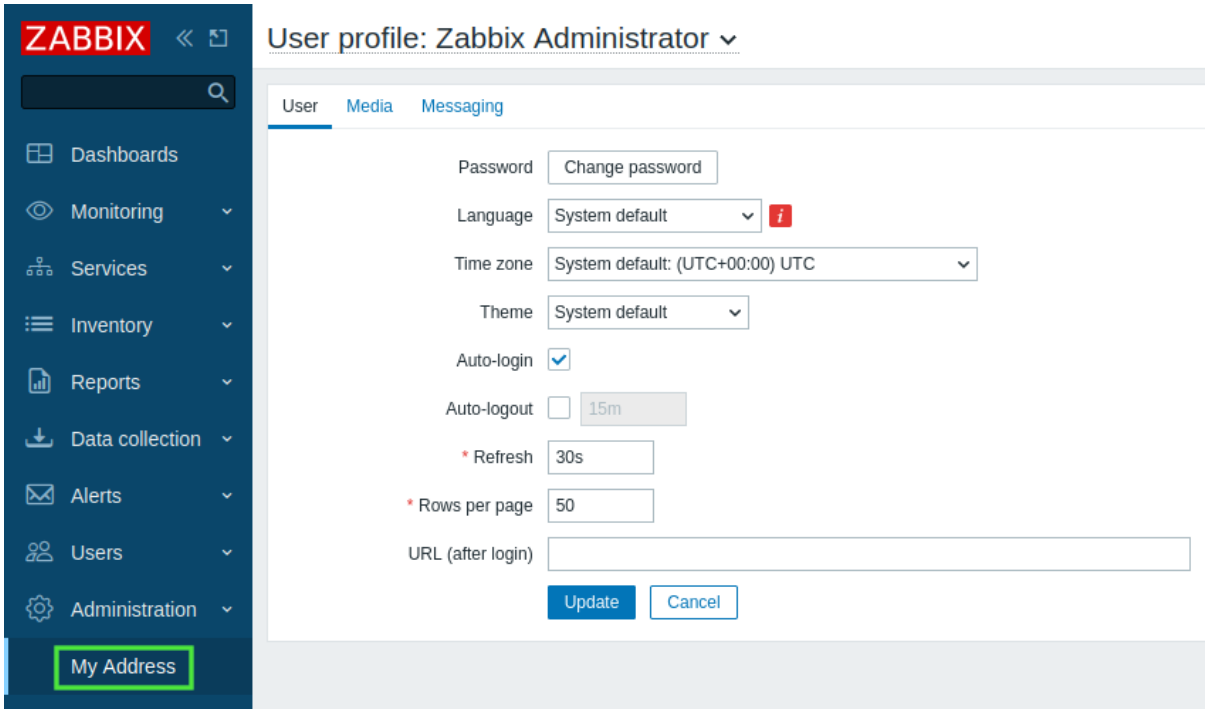
use Zabbix\Core\CModule,
APP,
CMenuItem;

class Module extends CModule {

public function init(): void {
APP::Component()->get('menu.main')
->add((new CMenuItem(_('My Address')))
->setAction('userprofile.edit'));
}
}
```

Note:
Możesz zastąpić `'userprofile.edit'` innymi akcjami, na przykład `'charts.view'` (otwiera niestandardowe wykresy), `'problems.view'` (otwiera *Monitorowanie* → *Problemy*) lub `'report.status'` (otwiera raport *Informacje o systemie*).

3. Odśwież interfejs użytkownika Zabbix. Na dole głównego menu Zabbix znajduje się teraz nowa sekcja *My address*. Kliknij *My address*, aby otworzyć stronę *User profile*.



Część II - Zmiana lokalizacji sekcji menu

W tej części przeniesiesz sekcję menu *My address* do sekcji *Monitorowanie*, a następnie dodasz do niej zagnieżdżone menu. W rezultacie użytkownicy będą mogli uzyskać dostęp do dwóch stron podmenu z sekcji menu *Monitorowanie* → *My address*.

1. Otwórz i edytuj plik *Module.php*.

ui/modules/MyAddress/Module.php

```
<?php

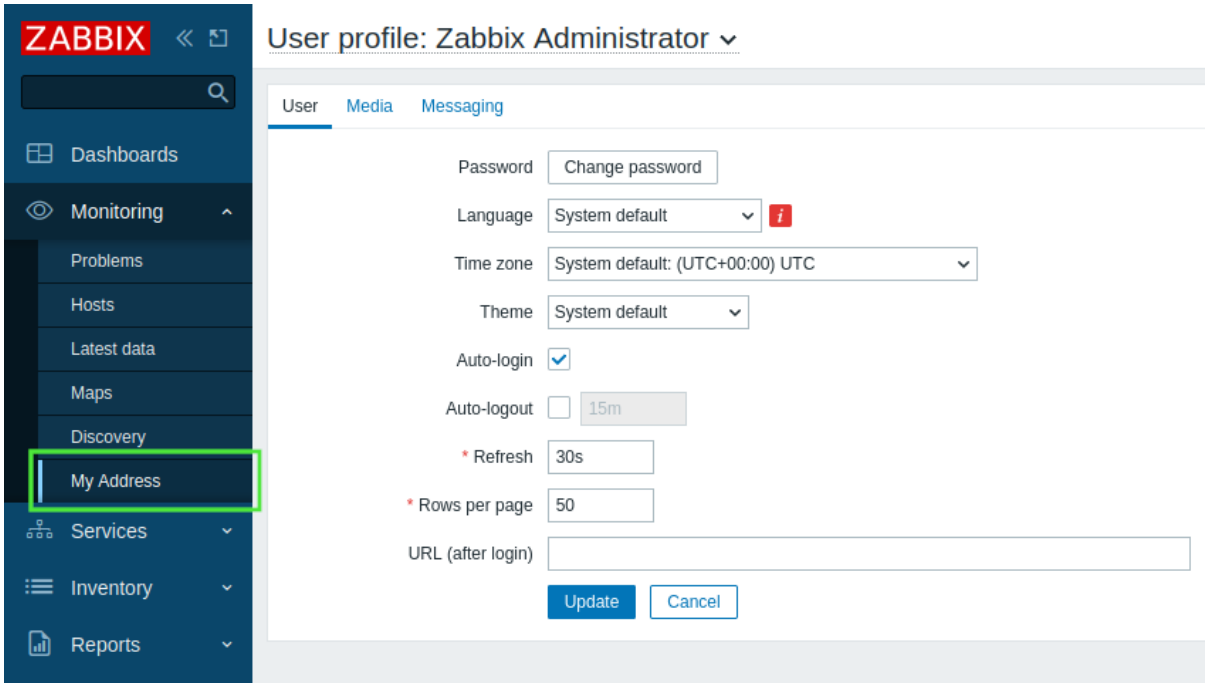
namespace Modules\MyAddress;

use Zabbix\Core\CModule,
APP,
CMenuItem;

class Module extends CModule {

public function init(): void {
APP::Component()->get('menu.main')
->findOrAdd(_('Monitoring'))
->getSubmenu()
->insertAfter(_('Discovery'),
(new CMenuItem(_('My Address')))->setAction('userprofile.edit')
);
}
}
```

2. Odśwież interfejs użytkownika Zabbix. Rozwiń sekcję menu *Monitoring* i zauważ, że sekcja *My address* znajduje się teraz poniżej sekcji *Odkrywanie*.



3. Aby dodać zagnieżdżone strony do sekcji menu *Mój adres*, otwórz i edytuj ponownie plik *Module.php*.

Ten krok tworzy dwie podsekcje:

- *Zewnętrzny adres IP*, który wykonuje nową akcję 'my.address', która zostanie zdefiniowana w kolejnych krokach;
- *Profil użytkownika*, który wykonuje wstępnie zdefiniowaną akcję 'userprofile.edit', aby otworzyć stronę *Profil użytkownika*.

Należy pamiętać, że w przypadku zagnieżdżonego menu należy użyć klasy *CMenu* oprócz klas użytych w poprzednich krokach.

ui/modules/MyAddress/Module.php

```
<?php

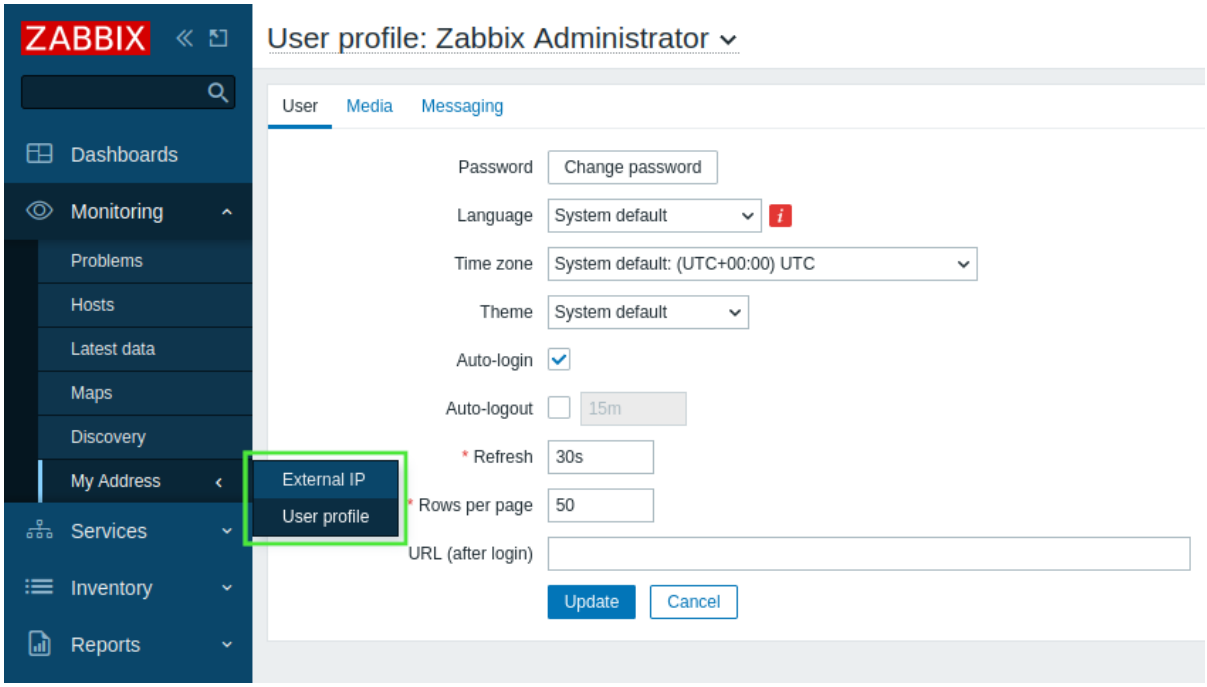
namespace Modules\MyAddress;

użyj Zabbix\Core\CModule,
APP,
CMenu,
CMenuItem;

class Module extends CModule {

public function init(): void {
APP::Component()->get('menu.main')
->findOrAdd(_('Monitoring'))
->getSubmenu()
->insertAfter(_('Discovery'),
(new CMenuItem(_('Mój adres')))->setSubMenu(
new CMenu([
(new CMenuItem(_('Zewnętrzny adres IP')))->setAction('my.address'),
(new CMenuItem(_('Profil użytkownika')))->setAction('userprofile.edit')
])
)
);
}
}
```

4. Odśwież frontend Zabbix. Zauważ, że sekcja menu *Mój adres* zawiera teraz menu trzeciego poziomu z dwiema stronami - *Zewnętrzny adres IP* i *Profil użytkownika*.



Część III - Akcja modułu

Akcja jest implementowana w dwóch plikach - *actions/MyAddress.php* i *views/my.address.php*. Plik ***actions/MyAddress.php*** zajmuje się implementacją logiki biznesowej, podczas gdy plik ***views/my.address.php*** odpowiada za widok.

1. Utwórz katalog *actions* w katalogu *MyAddress*.
2. Utwórz plik *MyAddress.php* w katalogu *actions*.

Logika akcji zostanie zdefiniowana w klasie *MyAddress*. Ta klasa akcji zaimplementuje cztery funkcje: *init()*, *checkInput()*, *checkPermissions()* i *doAction()*. Frontend Zabbix wywołuje funkcję *doAction()*, gdy żądana jest akcja. Ta funkcja odpowiada za logikę biznesową modułu.

> **Attention:**
> Dane muszą być zorganizowane jako tablica asocjacyjna. Tablica może być wielowymiarowa i może zawierać dowolne dane oczekiwane przez widok.

ui/modules/MyAddress/actions/MyAddress.php

```
<?php

namespace Modules\MyAddress\Actions;

use CController,
CControllerResponseData;

class MyAddress extends CController {

public function init(): void {
$this->disableCsrfValidation();
}

protected function checkInput(): bool {
return true;
}

protected function checkPermissions(): bool {
return true;
}

protected function doAction(): void {
$data = ['my-ip' => file_get_contents("https://api.seeip.org")];
$response = new CControllerResponseData($data);
```

```
$this->setResponse($response);
}
}
```

3. Utwórz nowy katalog *views* w katalogu *MyAddress*.
4. Utwórz plik *my.address.php* w katalogu *views* i zdefiniuj widok modułu.

Należy zauważyć, że zmienna `$data` jest dostępna w widoku bez jej konkretnego definiowania. Framework automatycznie przekazuje tablicę asocjacyjną do widoku.

ui/modules/MyAddress/views/my.address.php

```
<?php

(new CHtmlPage())
->setTitle(_('Tytuł HTML strony My Address'))
->addItem(new CDiv($data['my-ip']))
->show();
```

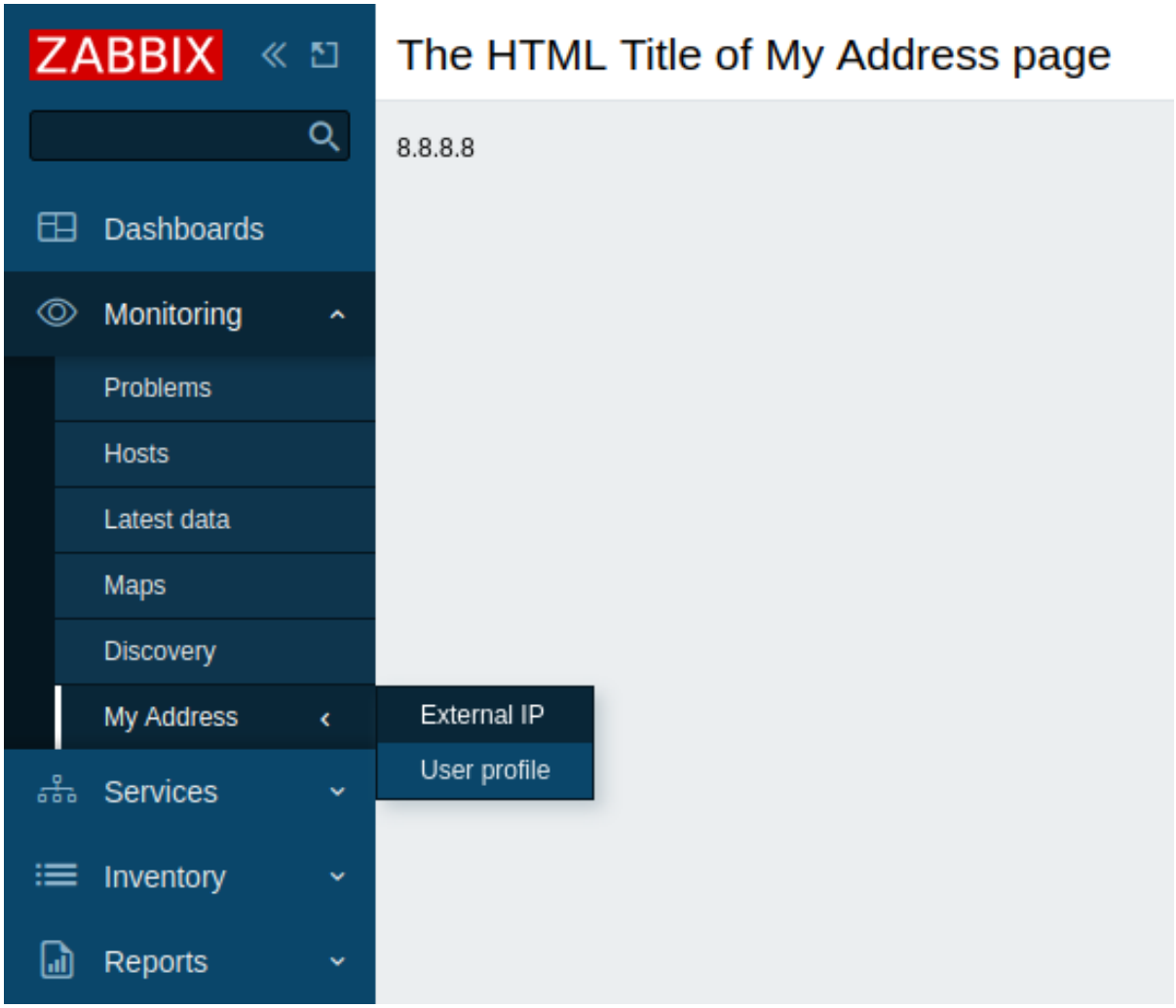
5. Akcja modułu musi zostać zarejestrowana w pliku *manifest.json*. Otwórz *manifest.json* i dodaj nowy obiekt `actions`, który zawiera:

- klucz akcji z nazwą akcji zapisaną małymi literami (a-z) i słowami oddzielonymi kropkami (na przykład `my.address`);
- nazwę klasy akcji (`MyAddress`) jako wartość klucza `class` obiektu `my.address`;
- nazwę widoku akcji (`my.address`) jako wartość klucza `view` obiektu `my.address`.

ui/modules/MyAddress/manifest.json

```
{
"manifest_version": 2.0,
"id": "my-address",
"name": "My IP Address",
"version": "1.0",
"namespace": "MyAddress",
"description": "My External IP Address.",
"actions": {
"my.address": {
"class": "MyAddress",
"view": "my.address"
}
}
}
```

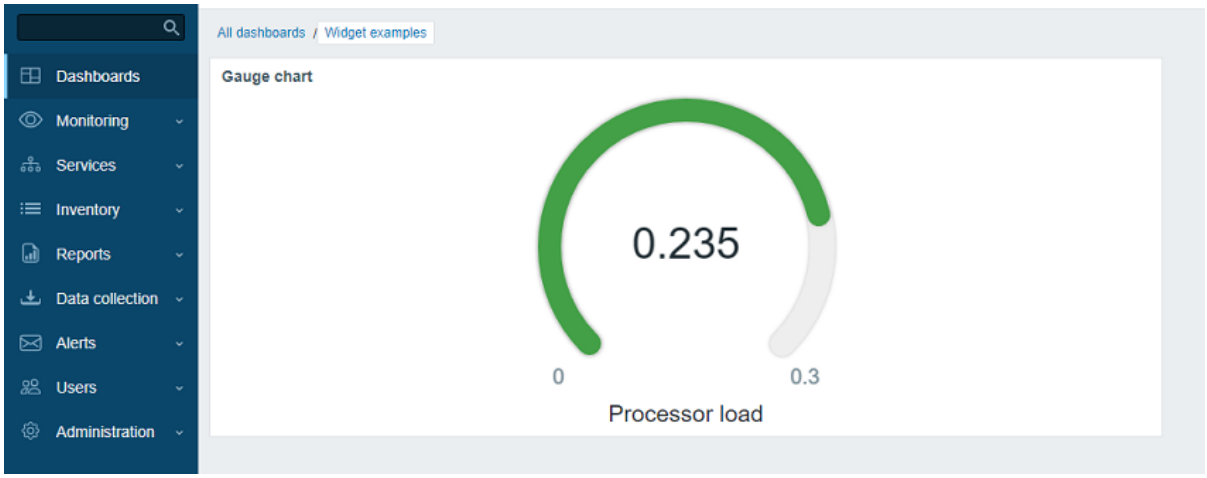
6. Odśwież interfejs użytkownika Zabbix. Kliknij *Mój adres → Zewnętrzny adres IP*, aby zobaczyć adres IP swojego komputera.



Utwórz widżet (samouczek)

To jest samouczek pokazujący krok po kroku, jak utworzyć prosty widget pulpitu nawigacyjnego. Możesz pobrać wszystkie pliki tego widgetu w postaci archiwum ZIP: lesson_gauge_chart.zip.

Co zbudujesz Podczas tego samouczka najpierw zbudujesz podstawowy widżet „Hello, world!", a następnie przekonwertujesz go na bardziej zaawansowany widżet, który wyświetla wartość pozycji jako wykres wskaźnikowy. Oto jak będzie wyglądał gotowy widżet:



Część I - "Witaj, świecie!" W tej sekcji dowiesz się, jak utworzyć minimalną wymaganą liczbę elementów widgetu i dodać nowy widget do frontendu Zabbix.

Dodawanie pustego widgetu do frontend Zabbix

1. Utwórz katalog *lesson_gauge_chart* w katalogu *modules* swojej instalacji frontend Zabbix (na przykład *zabbix/ui/modules*).

Note:
Wszystkie niestandardowe widgety są traktowane jako moduły zewnętrzne i muszą być dodawane do katalogu *modules* instalacji frontend Zabbix (na przykład *zabbix/ui/modules*). Katalog *zabbix/ui/widgets* jest zarezerwowany dla wbudowanych widgetów Zabbix i jest aktualizowany razem z interfejsem Zabbix UI.

2. Utwórz plik *manifest.json* z podstawowymi metadanymi widgetu (zobacz opis obsługiwanych parametrów).

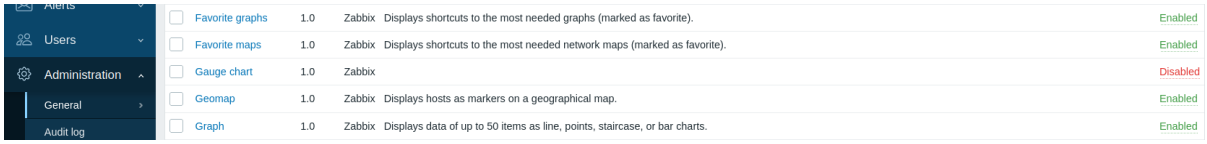
ui/modules/lesson_gauge_chart/manifest.json

```
{
    "manifest_version": 2.0,
    "id": "lesson_gauge_chart",
    "type": "widget",
    "name": "Gauge chart",
    "namespace": "LessonGaugeChart",
    "version": "1.1",
    "author": "Zabbix"
}
```

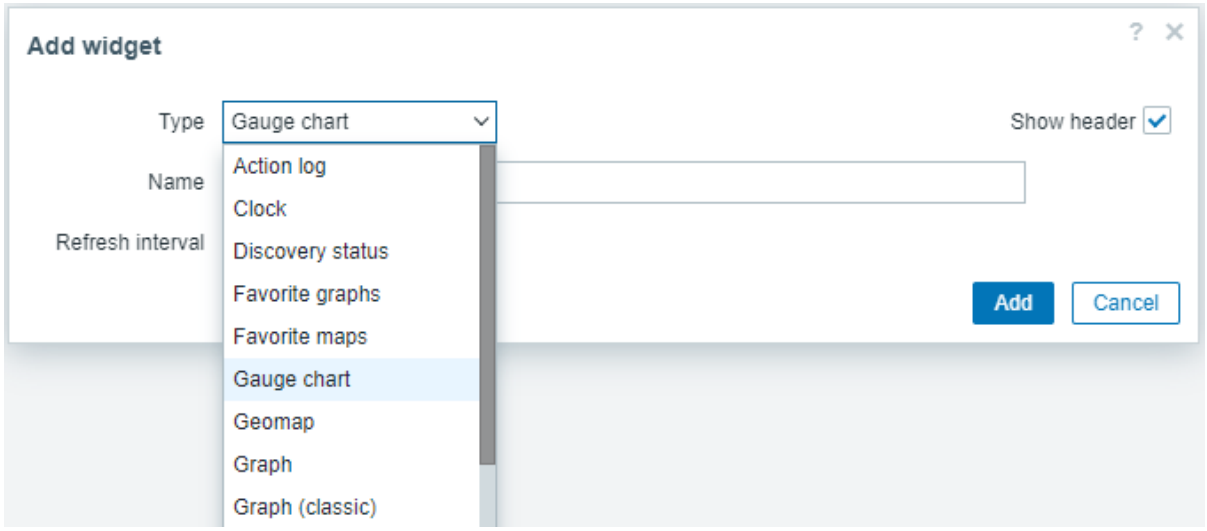
3. W frontend Zabbix przejdź do sekcji *Administration* → *General* → *Modules* i kliknij przycisk *Scan directory*.



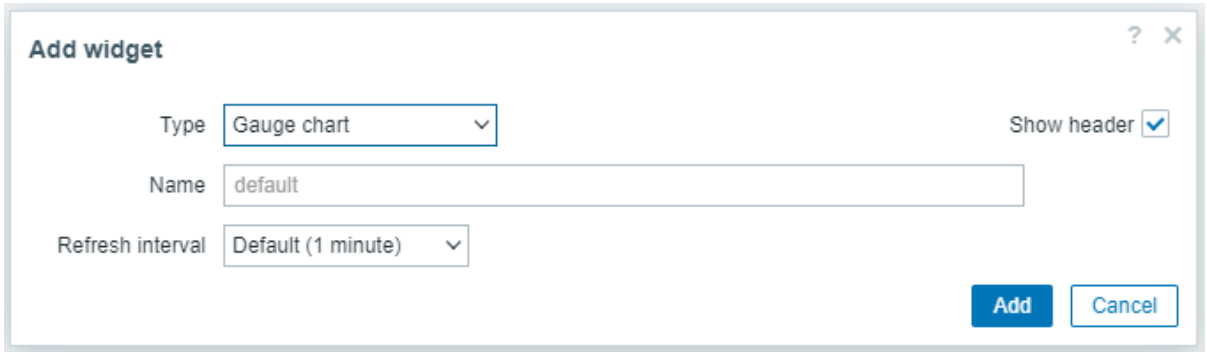
4. Odszukaj na liście nowy moduł *Gauge chart* i kliknij hiperłącze "Disabled", aby zmienić status modułu z "Disabled" na "Enabled" (jeśli moduł nie jest widoczny na liście, zobacz sekcję troubleshooting).



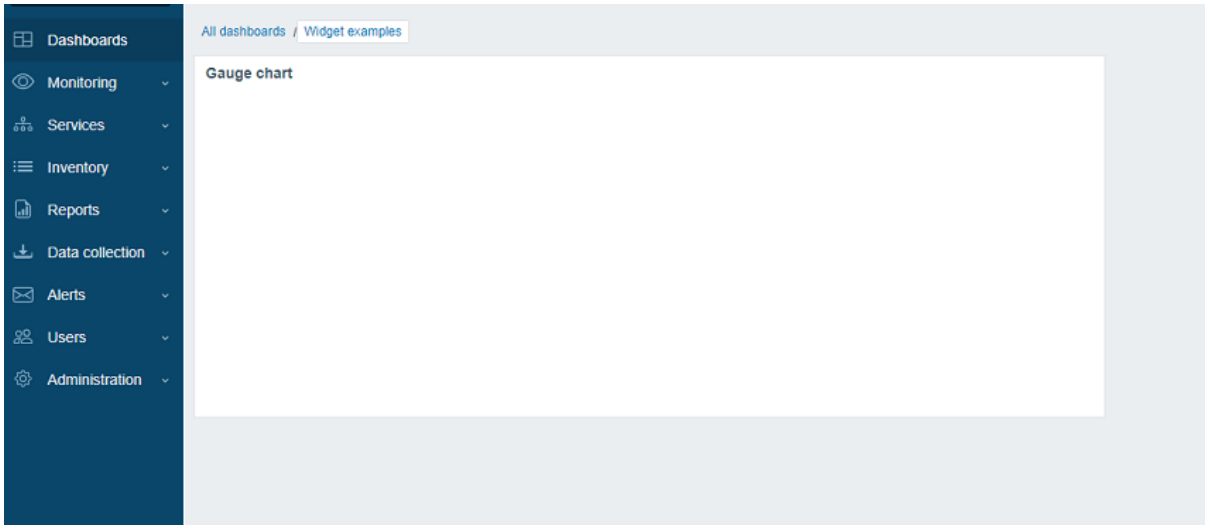
5. Otwórz dashboard, przełącz go w tryb edycji i dodaj nowy widget. W polu *Type* wybierz "Gauge chart".



6. Na tym etapie konfiguracja widgetu *Gauge chart* zawiera tylko wspólne pola widgetu *Name* i *Refresh interval*. Kliknij *Add*, aby dodać widget do dashboardu.



7. Na dashboardzie powinien pojawić się pusty widget. Kliknij *Save changes* w prawym górnym rogu, aby zapisać dashboard.



Dodawanie widoku widgetu

Note:
Plik **widoku** widgetu powinien znajdować się w katalogu *views* (w tym samouczku: *ui/modules/lesson_gauge_chart/views/*). Jeśli plik ma domyślną nazwę *widget.view.php*, nie trzeba go rejestrować w pliku *manifest.json*. Jeśli plik ma inną nazwę, należy ją określić w sekcji *actions/widget.lesson_gauge_chart.view* pliku manifest.json.

1. Utwórz katalog *views* w katalogu *lesson_gauge_chart*.
2. Utwórz plik *widget.view.php* w katalogu *views*.

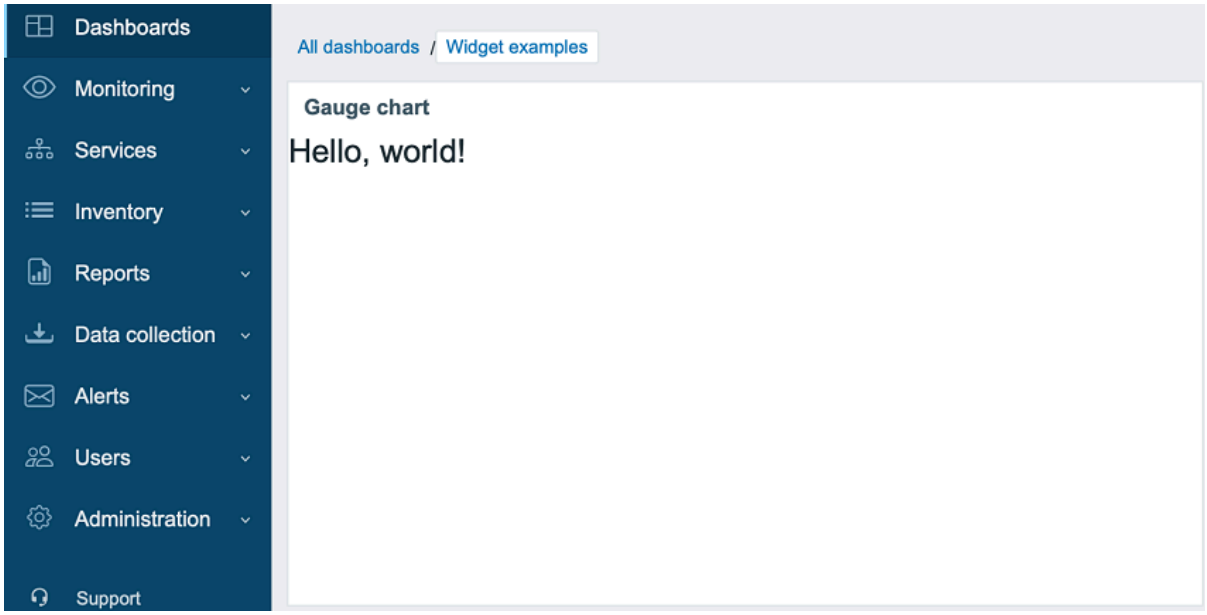
ui/modules/lesson_gauge_chart/views/widget.view.php

```
<?php

/**
 * Widok widgetu wykresu wskaźnikowego.
 *
 * @var CView $this
 * @var array $data
 */

(new CWidgetView($data))
    ->addItem(
        new CTag('h1', true, 'Hello, world!')
    )
    ->show();
```

3. Odśwież pulpit. Widget *Gauge chart* wyświetla teraz „Hello, world!”.



Część II - Wykres wskaźnikowy Dodawanie ustawień do widoku konfiguracji i używanie ich w widoku widgetu

W tej sekcji dowiesz się, jak dodać pole konfiguracji widgetu i wyświetlić wprowadzaną wartość w widoku widgetu jako tekst.

Konfiguracja widgetu składa się z formularza (*Zabbix\Widgets\CWidgetForm*) oraz widoku formularza widgetu (*widget.edit.php*). Aby dodać pola (*Zabbix\Widgets\CWidgetField*), należy utworzyć klasę *WidgetForm*, która będzie rozszerzać *Zabbix\Widgets\CWidgetForm*.

Formularz zawiera zestaw pól (*Zabbix\Widgets\CWidgetField*) różnych typów, które są używane do walidacji wartości wprowadzanych przez użytkownika. Pole formularza (*Zabbix\Widgets\CWidgetField*) dla każdego typu elementu wejściowego konwertuje wartość do jednolitego formatu, aby można ją było przechowywać w bazie danych.

> **Note:**
> Plik **form** widgetu powinien znajdować się w katalogu *includes* (w tym samouczku: *ui/modules/lesson_gauge_chart/includes/*). Jeśli plik ma domyślną nazwę *WidgetForm.php*, nie trzeba go rejestrować w pliku *manifest.json*. Jeśli plik ma inną nazwę, należy ją określić w sekcji *widget/form_class* pliku manifest.json.

1. Utwórz nowy katalog *includes* w katalogu *lesson_gauge_chart*.
2. Utwórz plik *WidgetForm.php* w katalogu *includes*.

ui/modules/lesson_gauge_chart/includes/WidgetForm.php

```
<?php

namespace Modules\LessonGaugeChart\Includes;

use Zabbix\Widgets\CWidgetForm;

class WidgetForm extends CWidgetForm {
}
```

3. Dodaj pole *Description* do formularza konfiguracji widgetu. Jest to zwykłe pole tekstowe, w którym użytkownik może wprowadzić dowolny zestaw znaków. Możesz do tego użyć klasy *CWidgetFieldTextBox*.

ui/modules/lesson_gauge_chart/includes/WidgetForm.php

```
<?php

namespace Modules\LessonGaugeChart\Includes;

use Zabbix\Widgets\CWidgetForm;

use Zabbix\Widgets\Fields\CWidgetFieldTextBox;

class WidgetForm extends CWidgetForm {

    public function addFields(): self {
```

```
        return $this
            ->addField(
                new CWidgetFieldTextBox('description', _('Description'))
            );
    }
}
```

4. W katalogu *views* utwórz plik widoku konfiguracji widgetu *widget.edit.php* i dodaj widok dla nowego pola *Description*. Dla klasy pola *CWidgetFieldTextBox* widokiem jest *CWidgetFieldTextBoxView.*

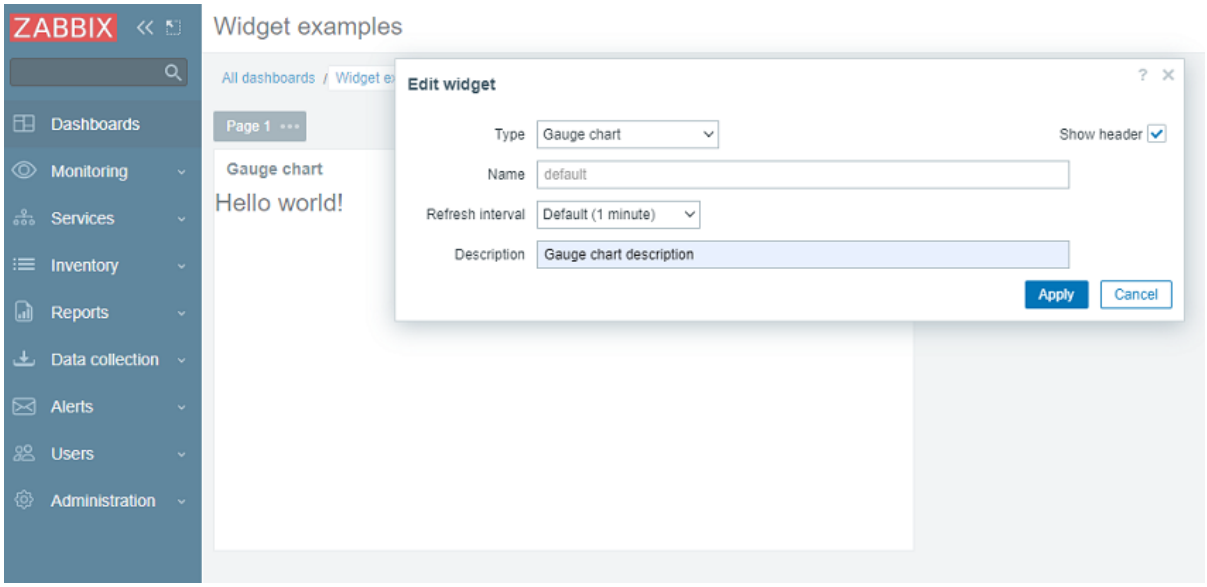
ui/modules/lesson_gauge_chart/views/widget.edit.php

```
<?php

/**
 * Gauge chart widget form view.
 *
 * @var CView $this
 * @var array $data
 */

(new CWidgetFormView($data))
    ->addField(
        new CWidgetFieldTextBoxView($data['fields']['description'])
    )
    ->show();
```

5. Przejdź do pulpitu i kliknij ikonę koła zębatego w widżecie, aby otworzyć formularz konfiguracji widgetu.
6. Formularz konfiguracji widgetu zawiera teraz nowe pole tekstowe *Description*. Wprowadź dowolną wartość, na przykład *Gauge chart description*.



7. Kliknij *Apply* w formularzu konfiguracji widgetu. Następnie kliknij *Save changes* w prawym górnym rogu, aby zapisać pulpit. Zwróć uwagę, że nowy opis nie jest nigdzie widoczny, a widget nadal wyświetla „Hello, world!”.

Aby nowy opis pojawił się w widżecie, wartość pola *Description* musi zostać pobrana z bazy danych i przekazana do widoku widgetu. W tym celu należy utworzyć klasę akcji.

8. Utwórz nowy katalog *actions* w katalogu *lesson_gauge_chart*.
9. Utwórz plik *WidgetView.php* w katalogu *actions*. Klasa akcji *WidgetView* będzie rozszerzać klasę *CControllerDashboardWidgetView*.

Wartości pól konfiguracji widgetu są przechowywane we właściwości **$fields_values** klasy akcji.

ui/modules/lesson_gauge_chart/actions/WidgetView.php

```
<?php
```

```php
namespace Modules\LessonGaugeChart\Actions;

use CControllerDashboardWidgetView,
    CControllerResponseData;

class WidgetView extends CControllerDashboardWidgetView {

    protected function doAction(): void {
        $this->setResponse(new CControllerResponseData([
            'name' => $this->getInput('name', $this->widget->getName()),
            'description' => $this->fields_values['description'],
            'user' => [
                'debug_mode' => $this->getDebugMode()
            ]
        ]));
    }
}
```

10. Otwórz plik *manifest.json* i zarejestruj *WidgetView* jako klasę akcji w sekcji *actions/widget.lesson_gauge_chart.view*.

ui/modules/lesson_gauge_chart/manifest.json

```
{
    "manifest_version": 2.0,
    "id": "lesson_gauge_chart",
    "type": "widget",
    "name": "Gauge chart",
    "namespace": "LessonGaugeChart",
    "version": "1.0",
    "author": "Zabbix",
    "actions": {
        "widget.lesson_gauge_chart.view": {
            "class": "WidgetView"
        }
    }
}
```

11. Teraz możesz użyć wartości pola opisu, zawartej w *$data['description']*, w widoku widgetu. Otwórz plik *views/widget.view.php* i zastąp statyczny tekst „Hello, world!" wartością *$data['description']*.

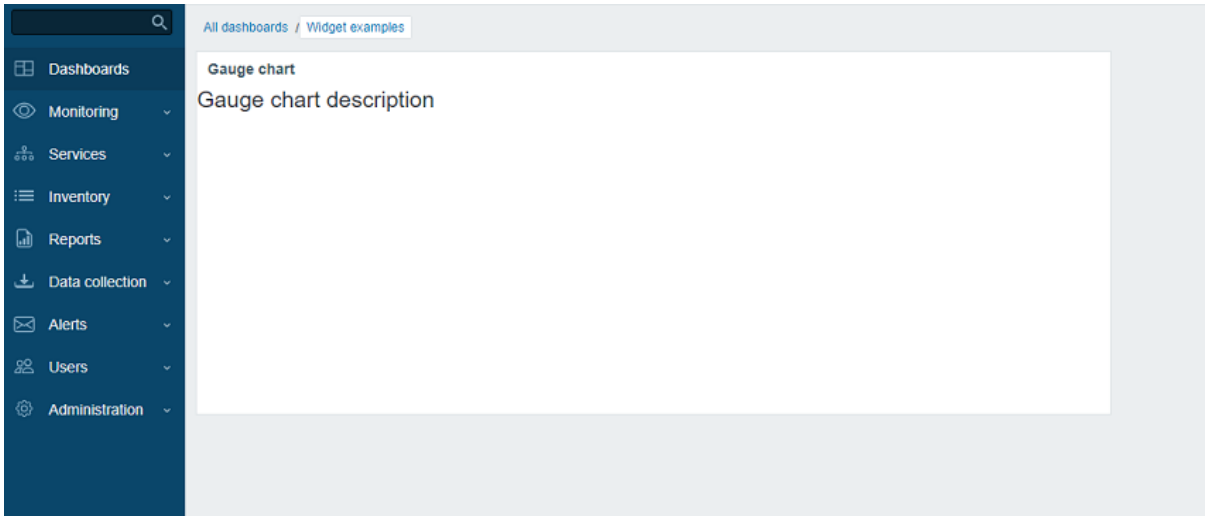
ui/modules/lesson_gauge_chart/views/widget.view.php

```php
<?php

/**
 * Gauge chart widget view.
 *
 * @var CView $this
 * @var array $data
 */

(new CWidgetView($data))
    ->addItem(
        new CTag('h1', true, $data['description'])
    )
    ->show();
```

12. Odśwież stronę pulpitu. Powinien teraz być widoczny tekst opisu widgetu zamiast „Hello, world!".



Pobieranie wartości pozycji przez API

Widget powinien wyświetlać ostatnią wartość pozycji wybranej przez użytkownika. W tym celu należy dodać możliwość wyboru pozycji w konfiguracji widgetu.

W tej sekcji dowiesz się, jak dodać pole wyboru pozycji do formularza widgetu oraz jak dodać wizualną część tego pola do widoku konfiguracji. Następnie kontroler widgetu będzie mógł pobrać dane pozycji i jej wartość za pomocą żądania API. Po odebraniu wartość będzie mogła zostać wyświetlona w widoku widgetu.

1. Otwórz plik *includes/WidgetForm.php* i dodaj pole *CWidgetFieldMultiSelectItem*. Pozwoli to na wybór pozycji w formularzu konfiguracji.

ui/modules/lesson_gauge_chart/includes/WidgetForm.php

```
<?php

namespace Modules\LessonGaugeChart\Includes;

use Zabbix\Widgets\{
    CWidgetField,
    CWidgetForm
};

use Zabbix\Widgets\Fields\{
    CWidgetFieldMultiSelectItem,
    CWidgetFieldTextBox
};

/**
 * Formularz widgetu wykresu wskaźnikowego.
 */
class WidgetForm extends CWidgetForm {

    public function addFields(): self {
        return $this
            ->addField(
                (new CWidgetFieldMultiSelectItem('itemid', _('Item')))
                    ->setFlags(CWidgetField::FLAG_NOT_EMPTY | CWidgetField::FLAG_LABEL_ASTERISK)
                    ->setMultiple(false)
            )
            ->addField(
                new CWidgetFieldTextBox('description', _('Description'))
            );
    }
}
```

2. Otwórz plik *views/widget.edit.php* i dodaj wizualny komponent pola do widoku konfiguracji.

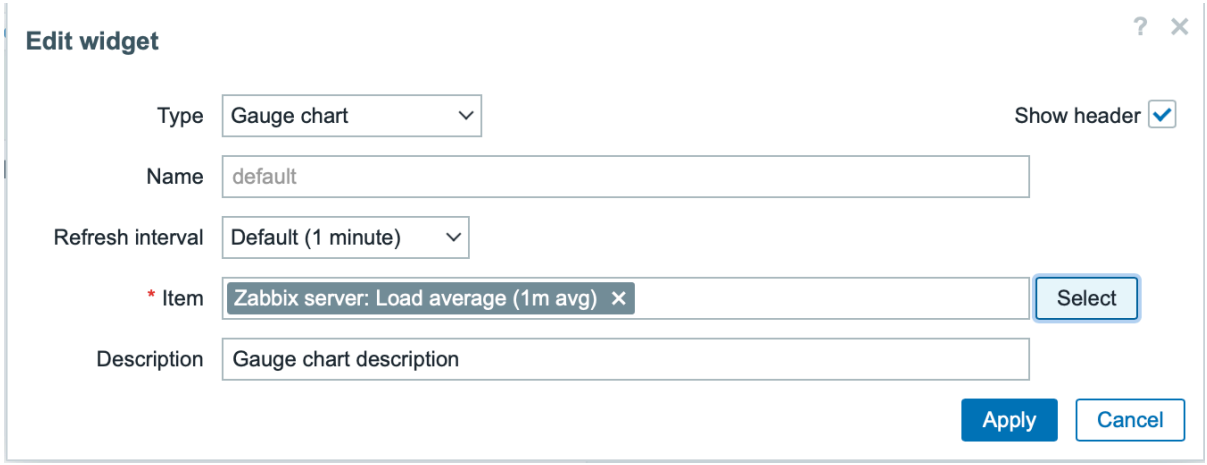
ui/modules/lesson_gauge_chart/views/widget.edit.php

```php
<?php

/**
 * Widok formularza widgetu wykresu wskaźnikowego.
 *
 * @var CView $this
 * @var array $data
 */

(new CWidgetFormView($data))
    ->addField(
        new CWidgetFieldMultiSelectItemView($data['fields']['itemid'])
    )
    ->addField(
        new CWidgetFieldTextBoxView($data['fields']['description'])
    )
    ->show();
```

3. Wróć do pulpitu i kliknij ikonę koła zębatego w widżecie, aby otworzyć formularz konfiguracji widgetu.
4. Formularz konfiguracji widgetu zawiera teraz nowe pole wejściowe *Item*. Wybierz host "Zabbix server" oraz pozycję "Load average (1m avg)".



5. Kliknij *Apply* w formularzu konfiguracji widgetu. Następnie kliknij *Save changes* w prawym górnym rogu, aby zapisać pulpit.
6. Otwórz i zmodyfikuj plik *actions/WidgetView.php*.

Od tej chwili ID pozycji będzie dostępne w kontrolerze widgetu w *$this->fields_values['itemid']*. Metoda kontrolera *doAction()* pobiera dane pozycji (nazwę, typ wartości, jednostki) za pomocą metody API *item.get* oraz ostatnią wartość pozycji za pomocą metody API *history.get*.

ui/modules/lesson_gauge_chart/actions/WidgetView.php

```php
<?php

namespace Modules\LessonGaugeChart\Actions;

use API,
    CControllerDashboardWidgetView,
    CControllerResponseData;

class WidgetView extends CControllerDashboardWidgetView {

    protected function doAction(): void {
        $db_items = API::Item()->get([
            'output' => ['itemid', 'value_type', 'name', 'units'],
            'itemids' => $this->fields_values['itemid'],
            'webitems' => true,
            'filter' => [
                'value_type' => [ITEM_VALUE_TYPE_UINT64, ITEM_VALUE_TYPE_FLOAT]
            ]
```

```
        ]);

        $value = null;

        if ($db_items) {
            $item = $db_items[0];

            $history = API::History()->get([
                'output' => API_OUTPUT_EXTEND,
                'itemids' => $item['itemid'],
                'history' => $item['value_type'],
                'sortfield' => 'clock',
                'sortorder' => ZBX_SORT_DOWN,
                'limit' => 1
            ]);

            if ($history) {
                $value = convertUnitsRaw([
                    'value' => $history[0]['value'],
                    'units' => $item['units']
                ]);
            }
        }

        $this->setResponse(new CControllerResponseData([
            'name' => $this->getInput('name', $this->widget->getName()),
            'value' => $value,
            'description' => $this->fields_values['description'],
            'user' => [
                'debug_mode' => $this->getDebugMode()
            ]
        ]));
    }
}
```

7. Otwórz plik *views/widget.view.php* i dodaj wartość pozycji do widoku widgetu.

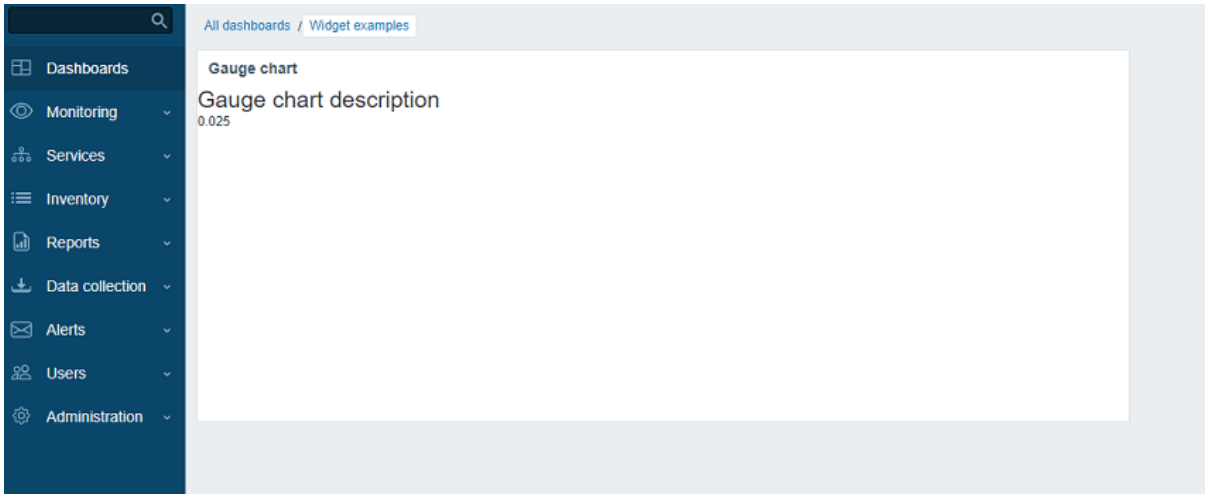
ui/modules/lesson_gauge_chart/views/widget.view.php

```
<?php

/**
 * Widok widgetu wykresu wskaźnikowego.
 *
 * @var CView $this
 * @var array $data
 */

(new CWidgetView($data))
    ->addItem([
        new CTag('h1', true, $data['description']),
        new CDiv($data['value'] !== null ? $data['value']['value'] : _('No data'))
    ])
    ->show();
```

8. Odśwież stronę pulpitu. Widget wyświetli najnowszą wartość pozycji.



Dodawanie zaawansowanych ustawień konfiguracji do widoku konfiguracji

W tej sekcji dowiesz się, jak dodać rozwijaną/zwijaną sekcję *Zaawansowana konfiguracja* z opcjonalnymi parametrami, takimi jak kolor, wartości minimalna i maksymalna, jednostki oraz pole *Opis* utworzone wcześniej.

1. Utwórz plik *Widget.php* w głównym katalogu widgetu *lesson_gauge_chart*, aby utworzyć nową klasę *Widget*.

Klasa *Widget* będzie rozszerzać klasę bazową *CWidget*, aby dodać/zastąpić domyślne ustawienia widgetu (w tym przypadku — tłumaczenia). JavaScript podany poniżej wyświetla ciąg „Brak danych” w przypadku braku danych. Ciąg „Brak danych” jest obecny w plikach tłumaczeń interfejsu Zabbix.

Jeśli istnieją jakiekolwiek stałe widgetu, zaleca się również określenie ich w klasie *Widget*.

ui/modules/lesson_gauge_chart/Widget.php

```
<?php

namespace Modules\LessonGaugeChart;

use Zabbix\Core\CWidget;

class Widget extends CWidget {

    public const UNIT_AUTO = 0;
    public const UNIT_STATIC = 1;

    public function getTranslationStrings(): array {
        return [
            'class.widget.js' => [
                'No data' => _('No data')
            ]
        ];
    }
}
```

2. Otwórz *includes/WidgetForm.php* i dodaj nowe pola *Kolor* (selektor koloru), *Min* (pole numeryczne), *Max* (pole numeryczne) oraz *Jednostki* (lista wyboru), a także zdefiniuj domyślną paletę kolorów dla selektora koloru, aby można było jej użyć w kolejnych krokach.

ui/modules/lesson_gauge_chart/includes/WidgetForm.php

```
<?php

namespace Modules\LessonGaugeChart\Includes;

use Modules\LessonGaugeChart\Widget;

use Zabbix\Widgets\{
    CWidgetField,
    CWidgetForm
};
```

```
use Zabbix\Widgets\Fields\{
    CWidgetFieldColor,
    CWidgetFieldMultiSelectItem,
    CWidgetFieldNumericBox,
    CWidgetFieldSelect,
    CWidgetFieldTextBox
};

/**
 * Formularz widgetu wykresu wskaźnikowego.
 */
class WidgetForm extends CWidgetForm {

    public const DEFAULT_COLOR_PALETTE = [
        'FF465C', 'B0AF07', '0EC9AC', '524BBC', 'ED1248', 'D1E754', '2AB5FF', '385CC7', 'EC1594', 'BAE37D',
        '6AC8FF', 'EE2B29', '3CA20D', '6F4BBC', '00A1FF', 'F3601B', '1CAE59', '45CFDB', '894BBC', '6D6D6D'
    ];

    public function addFields(): self {
        return $this
            ->addField(
                (new CWidgetFieldMultiSelectItem('itemid', _('Item')))
                    ->setFlags(CWidgetField::FLAG_NOT_EMPTY | CWidgetField::FLAG_LABEL_ASTERISK)
                    ->setMultiple(false)
            )
            ->addField(
                (new CWidgetFieldColor('chart_color', _('Color')))->setDefault('FF0000')
            )
            ->addField(
                (new CWidgetFieldNumericBox('value_min', _('Min')))
                    ->setDefault(0)
                    ->setFlags(CWidgetField::FLAG_NOT_EMPTY | CWidgetField::FLAG_LABEL_ASTERISK)
            )
            ->addField(
                (new CWidgetFieldNumericBox('value_max', _('Max')))
                    ->setDefault(100)
                    ->setFlags(CWidgetField::FLAG_NOT_EMPTY | CWidgetField::FLAG_LABEL_ASTERISK)
            )
            ->addField(
                (new CWidgetFieldSelect('value_units', _('Units'), [
                    Widget::UNIT_AUTO => _x('Auto', 'history source selection method'),
                    Widget::UNIT_STATIC => _x('Static', 'history source selection method')
                ]))->setDefault(Widget::UNIT_AUTO)
            )
            ->addField(
                (new CWidgetFieldTextBox('value_static_units'))
            )
            ->addField(
                new CWidgetFieldTextBox('description', _('Description'))
            );
    }
}
```

3. Otwórz *views/widget.edit.php* i dodaj wizualne komponenty pól do widoku konfiguracji.

ui/modules/lesson_gauge_chart/views/widget.edit.php

```
<?php

/**
 * Widok formularza widgetu wykresu wskaźnikowego.
 *
 * @var CView $this
```

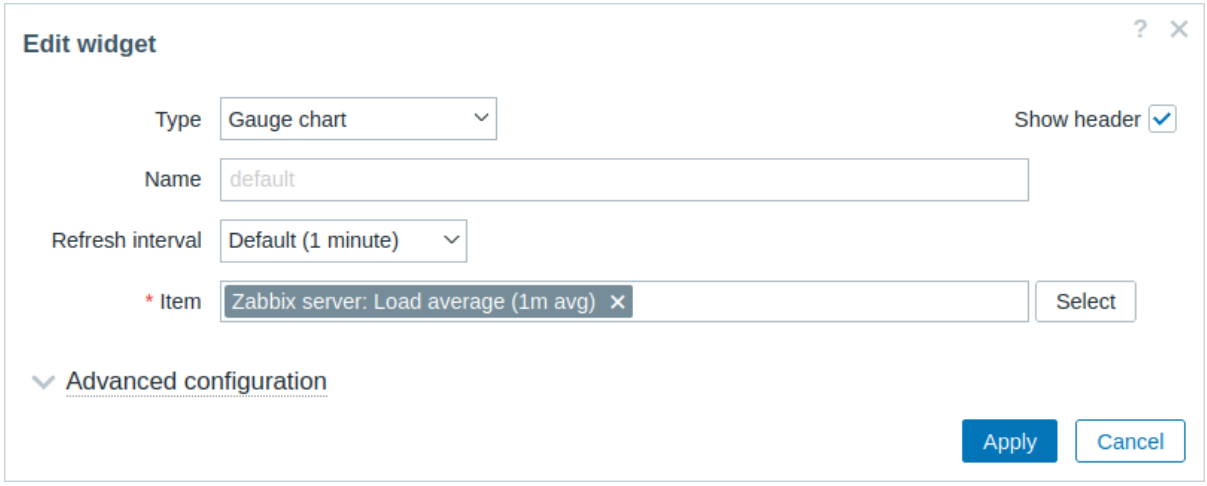
```
 * @var array $data
 */

$lefty_units = new CWidgetFieldSelectView($data['fields']['value_units']);
$lefty_static_units = (new CWidgetFieldTextBoxView($data['fields']['value_static_units']))
    ->setPlaceholder(_('value'))
    ->setWidth(ZBX_TEXTAREA_TINY_WIDTH);

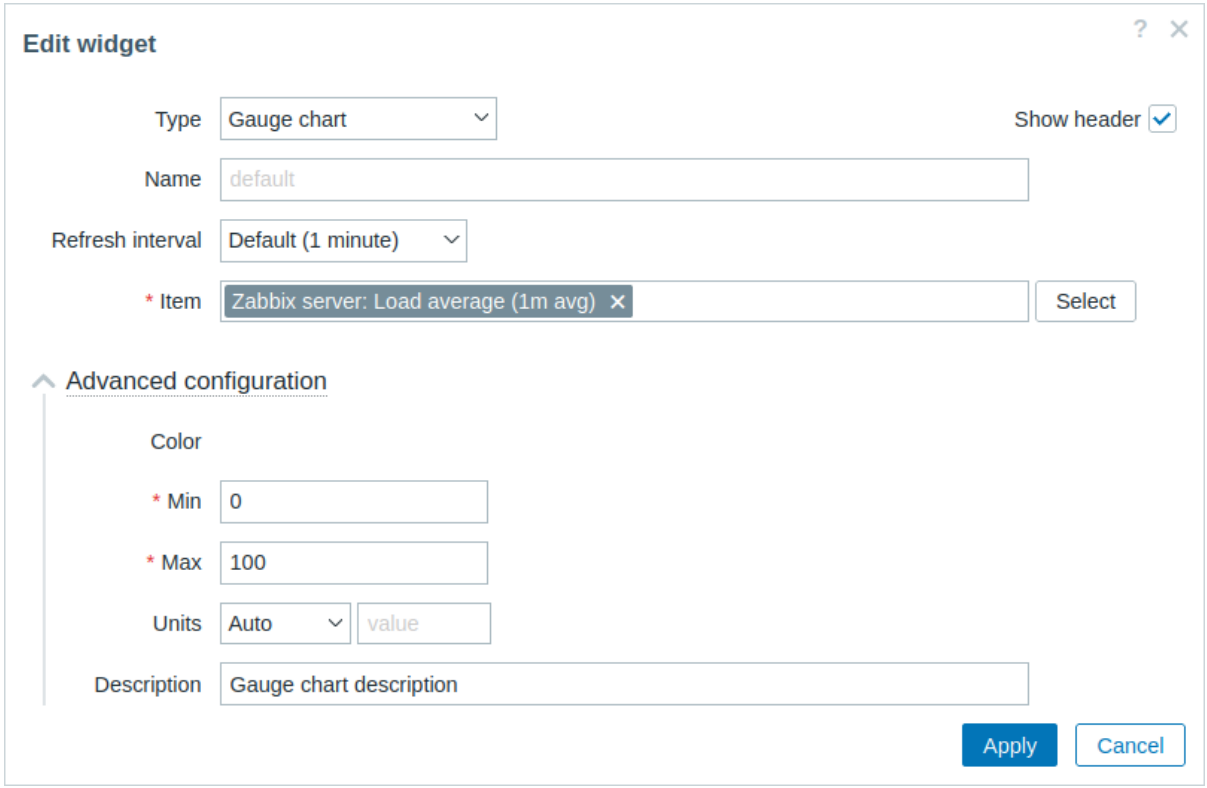
(new CWidgetFormView($data))
    ->addField(
        (new CWidgetFieldMultiSelectItemView($data['fields']['itemid']))
            ->setPopupParameter('numeric', true)
    )
    ->addFieldset(
        (new CWidgetFormFieldsetCollapsibleView(_('Advanced configuration')))
            ->addField(
                new CWidgetFieldColorView($data['fields']['chart_color'])
            )
            ->addField(
                new CWidgetFieldNumericBoxView($data['fields']['value_min'])
            )
            ->addField(
                new CWidgetFieldNumericBoxView($data['fields']['value_max'])
            )
            ->addItem([
                $lefty_units->getLabel(),
                (new CFormField([
                    $lefty_units->getView()->addClass(ZBX_STYLE_FORM_INPUT_MARGIN),
                    $lefty_static_units->getView()
                ]))
            ])
            ->addField(
                new CWidgetFieldTextBoxView($data['fields']['description'])
            )
    )
    ->show();
```

Note:
Metoda *addField()* klasy *CWidgetFormView* przyjmuje ciąg klasy CSS jako drugi parametr.

4. Wróć do pulpitu, przełącz się w tryb edycji i kliknij ikonę koła zębatego w widżecie, aby otworzyć formularz konfiguracji widgetu. Formularz konfiguracji widgetu zawiera teraz nową rozwijaną/zwijaną sekcję *Zaawansowana konfiguracja*.



5. Rozwiń sekcję *Zaawansowana konfiguracja*, aby zobaczyć dodatkowe pola konfiguracji widgetu. Zwróć uwagę, że pole *Kolor* nie ma jeszcze selektora koloru. Dzieje się tak dlatego, że selektor koloru musi zostać zainicjowany za pomocą JavaScript, który zostanie dodany w następnej sekcji — *Dodawanie JavaScript do widgetu*.



Dodawanie JavaScript do widgetu

W tej sekcji dowiesz się, jak dodać wykres wskaźnikowy (gauge chart) — utworzony przy użyciu JavaScript — który pokazuje, czy najnowsza wartość jest prawidłowa, czy zbyt wysoka/zbyt niska.

1. Utwórz plik *widget.edit.js.php* w katalogu *views*.

JavaScript będzie odpowiadał za inicjalizację selektora kolorów w widoku konfiguracji.

ui/modules/lesson_gauge_chart/views/widget.edit.js.php

```
<?php

use Modules\LessonGaugeChart\Widget;

?>

window.widget_lesson_gauge_chart_form = new class {

    init({color_palette}) {
        this._unit_select = document.getElementById('value_units');
        this._unit_value = document.getElementById('value_static_units');

        this._unit_select.addEventListener('change', () => this.updateForm());

        colorPalette.setThemeColors(color_palette);

        for (const colorpicker of jQuery('.<?= ZBX_STYLE_COLOR_PICKER ?> input')) {
            jQuery(colorpicker).colorpicker();
        }

        const overlay = overlays_stack.getById('widget_properties');

        for (const event of ['overlay.reload', 'overlay.close']) {
            overlay.$dialogue[0].addEventListener(event, () => { jQuery.colorpicker('hide'); });
        }

        this.updateForm();
    }
```

```
    updateForm() {
        this._unit_value.disabled = this._unit_select.value == <?= Widget::UNIT_AUTO ?>;
    }
};
```

2. Otwórz *views/widget.edit.php* i dodaj plik *widget.edit.js.php* z kodem JavaScript do widoku konfiguracji. Aby to zrobić, użyj metody *includeJsFile()*. Aby dodać osadzony kod JavaScript, użyj metody *addJavaScript()*.

ui/modules/lesson_gauge_chart/views/widget.edit.php

```
<?php

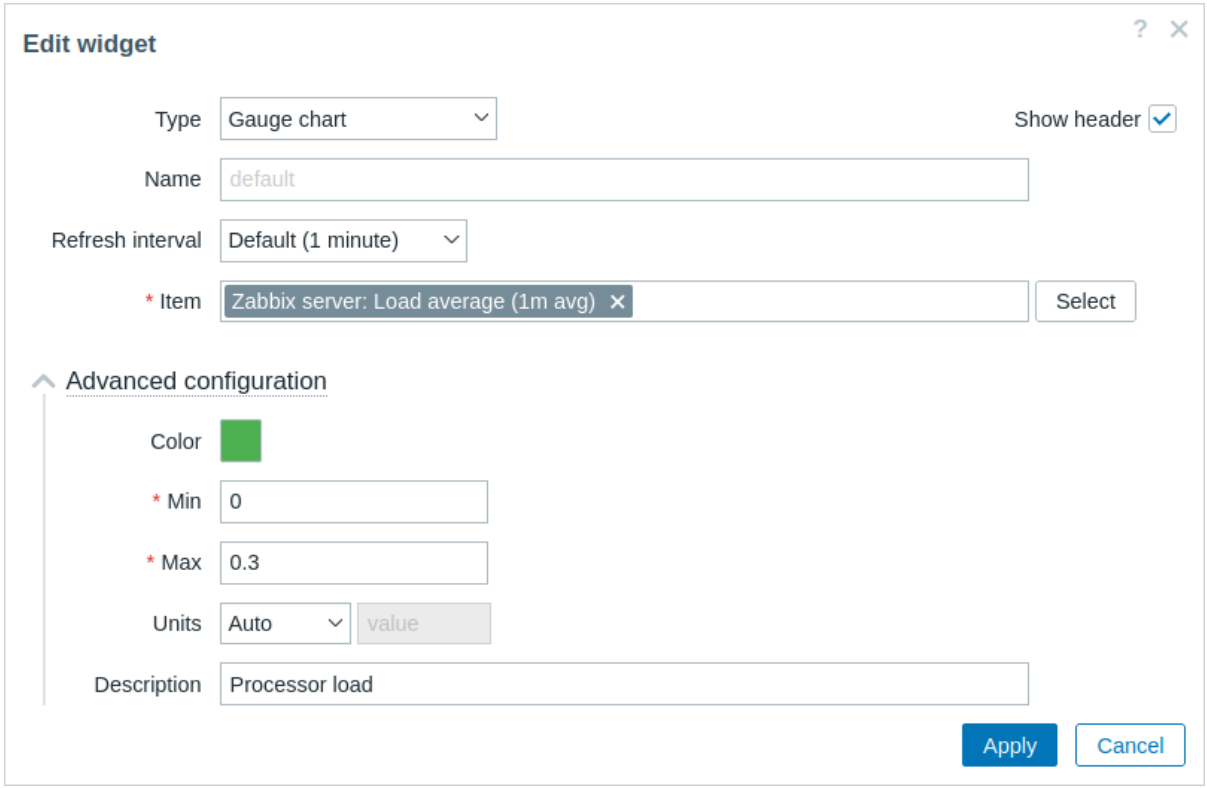
/**
 * Widok formularza widgetu wykresu wskaźnikowego.
 *
 * @var CView $this
 * @var array $data
 */

use Modules\LessonGaugeChart\Includes\WidgetForm;

$lefty_units = new CWidgetFieldSelectView($data['fields']['value_units']);
$lefty_static_units = (new CWidgetFieldTextBoxView($data['fields']['value_static_units']))
    ->setPlaceholder(_('value'))
    ->setWidth(ZBX_TEXTAREA_TINY_WIDTH);

(new CWidgetFormView($data))
    ->addField(
        (new CWidgetFieldMultiSelectItemView($data['fields']['itemid']))
            ->setPopupParameter('numeric', true)
    )
    ->addFieldset(
        (new CWidgetFormFieldsetCollapsibleView(_('Advanced configuration')))
            ->addField(
                new CWidgetFieldColorView($data['fields']['chart_color'])
            )
            ->addField(
                new CWidgetFieldNumericBoxView($data['fields']['value_min'])
            )
            ->addField(
                new CWidgetFieldNumericBoxView($data['fields']['value_max'])
            )
            ->addItem([
                $lefty_units->getLabel(),
                (new CFormField([
                    $lefty_units->getView()->addClass(ZBX_STYLE_FORM_INPUT_MARGIN),
                    $lefty_static_units->getView()
                ]))
            ])
            ->addField(
                new CWidgetFieldTextBoxView($data['fields']['description'])
            )
    )
    ->includeJsFile('widget.edit.js.php')
    ->addJavaScript('widget_lesson_gauge_chart_form.init('.json_encode([
        'color_palette' => WidgetForm::DEFAULT_COLOR_PALETTE
    ], JSON_THROW_ON_ERROR).');')
    ->show();
```

3. Wróć do pulpitu, kliknij ikonę koła zębatego w widżecie, aby otworzyć formularz konfiguracji widgetu. Następnie rozwiń sekcję *Advanced configuration*, aby zobaczyć zainicjalizowany selektor kolorów. Wypełnij pola wartościami i wybierz kolor dla wykresu wskaźnikowego.



4. Kliknij *Apply* w formularzu konfiguracji widgetu. Następnie kliknij *Save changes* w prawym górnym rogu, aby zapisać pulpit.
5. Otwórz *actions/WidgetView.php* i zaktualizuj kontroler.

Właściwość **$this->fields_values** zawiera teraz wartości wszystkich pól z sekcji *Advanced configuration*. Uzupełnij kontroler, aby umożliwić przekazywanie konfiguracji i wartości wybranej pozycji do widoku widgetu.

ui/modules/lesson_gauge_chart/actions/WidgetView.php

```
<?php

namespace Modules\LessonGaugeChart\Actions;

use API,
    CControllerDashboardWidgetView,
    CControllerResponseData;

class WidgetView extends CControllerDashboardWidgetView {

    protected function doAction(): void {
        $db_items = API::Item()->get([
            'output' => ['itemid', 'value_type', 'name', 'units'],
            'itemids' => $this->fields_values['itemid'],
            'webitems' => true,
            'filter' => [
                'value_type' => [ITEM_VALUE_TYPE_UINT64, ITEM_VALUE_TYPE_FLOAT]
            ]
        ]);

        $history_value = null;

        if ($db_items) {
            $item = $db_items[0];

            $history = API::History()->get([
                'output' => API_OUTPUT_EXTEND,
                'itemids' => $item['itemid'],
                'history' => $item['value_type'],
                'sortfield' => 'clock',
                'sortorder' => ZBX_SORT_DOWN,
```

```
                'limit' => 1
            ]);

            if ($history) {
                $history_value = convertUnitsRaw([
                    'value' => $history[0]['value'],
                    'units' => $item['units']
                ]);
            }
        }

        $this->setResponse(new CControllerResponseData([
            'name' => $this->getInput('name', $this->widget->getName()),
            'history' => $history_value,
            'fields_values' => $this->fields_values,
            'user' => [
                'debug_mode' => $this->getDebugMode()
            ]
        ]));
    }
}
```

6. Otwórz i zmodyfikuj *views/widget.view.php*.

Musisz utworzyć kontener dla wykresu wskaźnikowego, który narysujesz w kolejnych krokach, oraz kontener dla opisu.

Aby przekazać wartości do JavaScript jako obiekt JSON, użyj metody *setVar()*.

ui/modules/lesson_gauge_chart/views/widget.view.php

```
<?php

/**
 * Widok widgetu wykresu wskaźnikowego.
 *
 * @var CView $this
 * @var array $data
 */

(new CWidgetView($data))
    ->addItem([
        (new CDiv())->addClass('chart'),
        $data['fields_values']['description']
            ? (new CDiv($data['fields_values']['description']))->addClass('description')
            : null
    ])
    ->setVar('history', $data['history'])
    ->setVar('fields_values', $data['fields_values'])
    ->show();
```

7. Utwórz nowy katalog *assets* w katalogu *lesson_gauge_chart*. Ten katalog będzie używany do przechowywania JavaScript, CSS oraz potencjalnie innych zasobów, takich jak czcionki lub obrazy.
8. Dla JavaScript widoku widgetu utwórz katalog *js* w katalogu *assets*.
9. Utwórz plik *class.widget.js* w katalogu *assets/js*.

Ta klasa JavaScript widgetu będzie rozszerzać bazową klasę JavaScript wszystkich widgetów pulpitu — *CWidget*.

Pulpit opiera się na poprawnej implementacji widgetu i przekazuje do niego wszystkie istotne informacje poprzez wywoływanie odpowiednich metod JavaScript. Pulpit oczekuje również, że widget będzie generował zdarzenia, gdy wystąpi jakaś interakcja. Dlatego klasa *CWidget* zawiera zestaw metod z domyślną implementacją zachowania widgetu, które można dostosować przez rozszerzenie tej klasy.

W tym przypadku konieczne jest pewne dostosowanie, dlatego zostanie zaimplementowana własna logika dla następujących aspektów działania widgetu:

- inicjalizacja widgetu, która odpowiada za zdefiniowanie początkowego stanu widgetu (zobacz metodę *onInitialize()*);

- wyświetlanie zawartości widgetu (to znaczy rysowanie wykresu wskaźnikowego), jeśli proces aktualizacji widgetu zakończył się powodzeniem i bez błędów (zobacz metodę *processUpdateResponse(response)* oraz powiązane metody *_resizeChart()* i *_updatedChart()*)
- zmiana rozmiaru widgetu (zobacz metodę *onResize()* oraz powiązaną metodę *_resizeChart()*)

W przypadku innych aspektów widgetu wykresu wskaźnikowego zostanie użyta domyślna implementacja zachowania widgetu. Aby dowiedzieć się więcej o metodach JavaScript klasy *CWidget*, zobacz: JavaScript.

Ponieważ ten kod JavaScript jest wymagany dla widoku widgetu, powinien być ładowany wraz ze stroną pulpitu. Aby włączyć ładowanie JavaScript, musisz zaktualizować parametry *assets/js* oraz *js_class* w pliku ***manifest.json***, jak pokazano w kroku 10.

ui/modules/lesson_gauge_chart/assets/js/class.widget.js

```
class WidgetLessonGaugeChart extends CWidget {

    static UNIT_AUTO = 0;
    static UNIT_STATIC = 1;

    onInitialize() {
        super.onInitialize();

        this._refresh_frame = null;
        this._chart_container = null;
        this._canvas = null;
        this._chart_color = null;
        this._min = null;
        this._max = null;
        this._value = null;
        this._last_value = null;
        this._units = '';
    }

    processUpdateResponse(response) {
        if (response.history === null) {
            this._value = null;
            this._units = '';
        }
        else {
            this._value = Number(response.history.value);
            this._units = response.fields_values.value_units == WidgetLessonGaugeChart.UNIT_AUTO
                ? response.history.units
                : response.fields_values.value_static_units;
        }

        this._chart_color = response.fields_values.chart_color;
        this._min = Number(response.fields_values.value_min);
        this._max = Number(response.fields_values.value_max);

        super.processUpdateResponse(response);
    }

    setContents(response) {
        if (this._canvas === null) {
            super.setContents(response);

            this._chart_container = this._body.querySelector('.chart');
            this._chart_container.style.height =
                `${this._getContentsSize().height - this._body.querySelector('.description').clientHeight}
            this._canvas = document.createElement('canvas');

            this._chart_container.appendChild(this._canvas);

            this._resizeChart();
        }
```

```
        this._updatedChart();
    }

    onResize() {
        super.onResize();

        if (this._state === WIDGET_STATE_ACTIVE) {
            this._resizeChart();
        }
    }

    _resizeChart() {
        const ctx = this._canvas.getContext('2d');
        const dpr = window.devicePixelRatio;

        this._canvas.style.display = 'none';
        const size = Math.min(this._chart_container.offsetWidth, this._chart_container.offsetHeight);
        this._canvas.style.display = '';

        this._canvas.width = size * dpr;
        this._canvas.height = size * dpr;

        ctx.scale(dpr, dpr);

        this._canvas.style.width = `${size}px`;
        this._canvas.style.height = `${size}px`;

        this._refresh_frame = null;

        this._updatedChart();
    }

    _updatedChart() {
        if (this._last_value === null) {
            this._last_value = this._min;
        }

        const start_time = Date.now();
        const end_time = start_time + 400;

        const animate = () => {
            const time = Date.now();

            if (time <= end_time) {
                const progress = (time - start_time) / (end_time - start_time);
                const smooth_progress = 0.5 + Math.sin(Math.PI * (progress - 0.5)) / 2;
                let value = this._value !== null ? this._value : this._min;
                value = (this._last_value + (value - this._last_value) * smooth_progress - this._min) / (t

                const ctx = this._canvas.getContext('2d');
                const size = this._canvas.width;
                const char_weight = size / 12;
                const char_shadow = 3;
                const char_x = size / 2;
                const char_y = size / 2;
                const char_radius = (size - char_weight) / 2 - char_shadow;

                const font_ratio = 32 / 100;

                ctx.clearRect(0, 0, size, size);

                ctx.beginPath();
```

```
                ctx.shadowBlur = char_shadow;
                ctx.shadowColor = '#bbb';
                ctx.strokeStyle = '#eee';
                ctx.lineWidth = char_weight;
                ctx.lineCap = 'round';
                ctx.arc(char_x, char_y, char_radius, Math.PI * 0.749, Math.PI * 2.251, false);
                ctx.stroke();

                ctx.beginPath();
                ctx.strokeStyle = `#${this._chart_color}`;
                ctx.lineWidth = char_weight - 2;
                ctx.lineCap = 'round';
                ctx.arc(char_x, char_y, char_radius, Math.PI * 0.75,
                    Math.PI * (0.75 + (1.5 * Math.min(1, Math.max(0, value)))), false
                    );
                ctx.stroke();

                ctx.shadowBlur = 2;
                ctx.fillStyle = '#1f2c33';
                ctx.font = `${(char_radius * font_ratio)|0}px Arial`;
                ctx.textAlign = 'center';
                ctx.textBaseline = 'middle';
                ctx.fillText(`${this._value !== null ? this._value : t('No data')}${this._units}`,
                    char_x, char_y, size - char_shadow * 4 - char_weight * 2
                );

                ctx.fillStyle = '#768d99';
                ctx.font = `${(char_radius * font_ratio * .5)|0}px Arial`;
                ctx.textBaseline = 'top';

                ctx.textAlign = 'left';
                ctx.fillText(`${this._min}${this._min != '' ? this._units : ''}`,
                    char_weight * .75, size - char_weight * 1.25, size / 2 - char_weight
                );

                ctx.textAlign = 'right';
                ctx.fillText(`${this._max}${this._max != '' ? this._units : ''}`,
                    size - char_weight * .75, size - char_weight * 1.25, size / 2 - char_weight
                );

                requestAnimationFrame(animate);
            }
            else {
                this._last_value = this._value;
            }
        };

        requestAnimationFrame(animate);
    }
}
```

10. Otwórz *manifest.json* i dodaj:

- nazwę pliku (*class.widget.js*) do tablicy w sekcji *assets/js*;
- nazwę klasy (*WidgetLessonGaugeChart*) do parametru *js_class* w sekcji *widget*.

Klasa *WidgetLessonGaugeChart* będzie teraz automatycznie ładowana wraz z pulpitem.

ui/modules/lesson_gauge_chart/manifest.json

```
{
    "manifest_version": 2.0,
    "id": "lesson_gauge_chart",
    "type": "widget",
    "name": "Gauge chart",
```

```
    "namespace": "LessonGaugeChart",
    "version": "1.0",
    "author": "Zabbix",
    "actions": {
        "widget.lesson_gauge_chart.view": {
            "class": "WidgetView"
        }
    },
    "widget": {
        "js_class": "WidgetLessonGaugeChart"
    },
    "assets": {
        "js": ["class.widget.js"]
    }
}
```

Dodawanie stylów CSS do widgetu

W tej sekcji dowiesz się, jak dodać niestandardowe style CSS, aby widget wyglądał bardziej atrakcyjnie.

1. Dla stylów widgetu utwórz nowy katalog *css* w katalogu *assets*.
2. Utwórz plik *widget.css* w katalogu *assets/css*. Aby nadać styl elementom widgetu, użyj selektora *div.dashboard-widget-{widget id}*. Aby skonfigurować CSS dla całego widgetu, użyj selektora *form.dashboard-widget-{widget id}*

ui/modules/lesson_gauge_chart/assets/css/widget.css

```
div.dashboard-widget-lesson_gauge_chart {
    display: grid;
    grid-template-rows: 1fr;
    padding: 0;
}

div.dashboard-widget-lesson_gauge_chart .chart {
    display: grid;
    align-items: center;
    justify-items: center;
}

div.dashboard-widget-lesson_gauge_chart .chart canvas {
    background: white;
}

div.dashboard-widget-lesson_gauge_chart .description {
    padding-bottom: 8px;
    font-size: 1.750em;
    line-height: 1.2;
    text-align: center;
}

.dashboard-grid-widget-hidden-header div.dashboard-widget-lesson_gauge_chart .chart {
    margin-top: 8px;
}
```

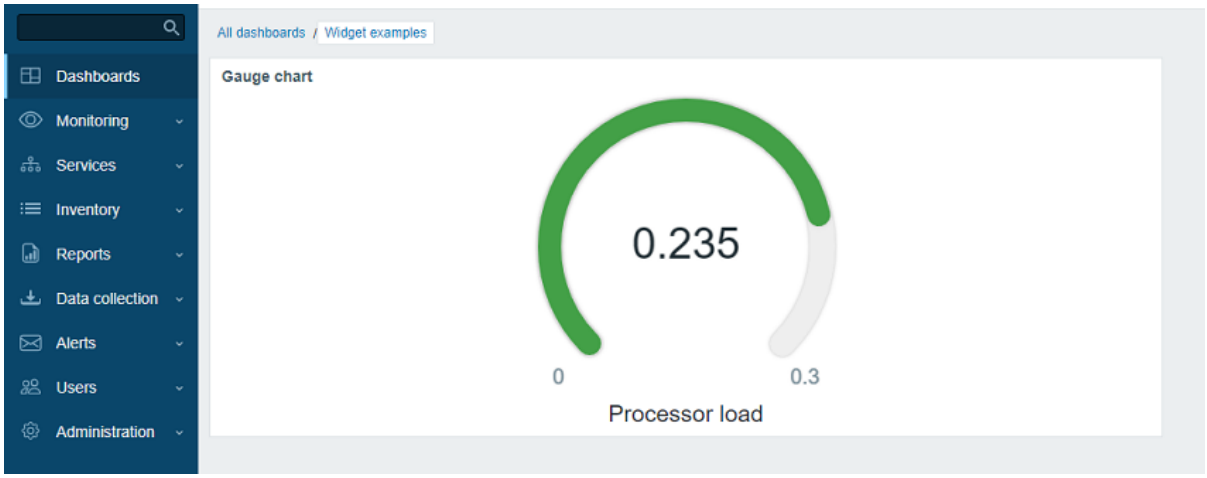
3. Otwórz plik *manifest.json* i dodaj nazwę pliku CSS (*widget.css*) do tablicy w sekcji *assets/css*. Umożliwi to wczytanie stylów CSS zdefiniowanych w pliku *widget.css* wraz ze stroną pulpitu.

ui/modules/lesson_gauge_chart/manifest.json

```
{
    "manifest_version": 2.0,
    "id": "lesson_gauge_chart",
    "type": "widget",
    "name": "Gauge chart",
    "namespace": "LessonGaugeChart",
    "version": "1.0",
    "author": "Zabbix",
```

```
    "actions": {
        "widget.lesson_gauge_chart.view": {
            "class": "WidgetView"
        }
    },
    "widget": {
        "js_class": "WidgetLessonGaugeChart"
    },
    "assets": {
        "css": ["widget.css"],
        "js": ["class.widget.js"]
    }
}
```

4. Odśwież stronę pulpitu, aby zobaczyć gotową wersję widgetu.



Przykłady

Ta sekcja zawiera pliki przykładowych modułów i widgetów, których możesz użyć jako podstawy do tworzenia własnych modułów.

Aby użyć modułu:

1. Pobierz archiwum ZIP.
2. Rozpakuj zawartość do oddzielnego katalogu w katalogu *modules* Twojej instalacji frontowej Zabbix (na przykład *zabbix/ui/modules*).
3. Zarejestruj moduł w interfejsie frontu Zabbix.

Przykład modułu Podczas tworzenia grupy hostów, przyznaj uprawnienia do odczytu skonfigurowanym grupom użytkowników - hg_auto_perm.zip

Przykłady widgetów

- Minimalny widget - widget_min.zip
- Widget ”Hello, world” wykorzystujący wyłącznie CSS - hello_world_css.zip
- Widget ”Hello, world” wykorzystujący wyłącznie JavaScript - hello_world_js.zip
- Widget ”Hello, world” wykorzystujący PHP - hello_world_php.zip

Jako przykładów możesz także użyć natywnych widgetów Zabbix’a.

Zmiany w tworzeniu rozszerzeń

Ta strona zawiera listę wszystkich zmian (jeśli występują) dotyczących tworzenia niestandardowych rozszerzeń Zabbix.

Strony podręcznika Zabbix

Dokumentacja referencyjna narzędzi i usług Zabbix wiersza poleceń, zawierająca listę dostępnych poleceń, opcji i przykładów użycia.

zabbix_agent2

Sekcja: Polecenia do zarządzania systemem (8)
Zaktualizowano: 2019-01-29
Indeks Wróć do głównej zawartości

NAZWA

zabbix_agent2 - Zabbix agent 2

SKŁADNIA

zabbix_agent2 [**-c** *config-file*]
zabbix_agent2 [**-c** *config-file*] [**-v**] **-p**
zabbix_agent2 [**-c** *config-file*] [**-v**] **-t** *item-key*
zabbix_agent2 [**-c** *config-file*] **-R** *runtime-option*
zabbix_agent2 [**-c** *config-file*] **-T**
zabbix_agent2 -h
zabbix_agent2 -V

OPIS

zabbix_agent2 jest aplikacją do monitorowania parametrów różnych usług.

OPCJE

-c, **--config** *plik-konfiguracyjny*
Określa alternatywny*plik-konfiguracji* zamiast domyślnego.

-R, **--runtime-control** *opcja-kontroli-działania*
Wykonuje funkcje administracyjne zależnie od podanej *opcji-kontroli-działania*.

Opcje kontroli w czasie działania: userparameter_reload
Przeładuj parametry użytkownika z pliku konfiguracyjnego

log_level_increase
Zwiększ poziom logowania

log_level_decrease
Zmniejsz poziom logowania

help
Wyświetl listę dostępnych opcji kontroli w czasie działania

metrics
Wyświetl listę dostępnych metryk

version
Wyświetl wersję

-p, **--print**
Wyświetl znane pozycje i zakończ działanie. Dla każdej pozycji używane są albo domyślne wartości ogólne, albo podawane są

specyficzne wartości domyślne do testowania. Te wartości domyślne są wymienione w nawiasach kwadratowych jako parametry klucza pozycji. Zwracane wartości są ujęte w nawiasy kwadratowe i poprzedzone typem zwracanej wartości, oddzielonym znakiem pionowej kreski. Dla parametrów użytkownika typ to zawsze **t**, ponieważ agent nie może określić wszystkich możliwych wartości zwracanych. Pozycje wyświetlane jako działające nie mają gwarancji działania z serwera Zabbix ani przez zabbix_get podczas odpytywania uruchomionego demona agent, ponieważ uprawnienia lub środowisko mogą być inne. Typy zwracanych wartości to:

d
Liczba z częścią dziesiętną.

m
Nieobsługiwane. Może to być spowodowane odpytywaniem pozycji, która działa tylko w trybie aktywnym, jak pozycja monitorowania logu, albo pozycji wymagającej wielu zebranych wartości. Problemy z uprawnieniami lub nieprawidłowe parametry użytkownika również mogą skutkować stanem nieobsługiwanym.

s
Tekst. Maksymalna długość nie jest ograniczona.

t
Tekst. Tak samo jak **s**.

u
Nieujemna liczba całkowita.

-t, **--test** *item-key*
Przetestuj pojedynczą pozycję i zakończ działanie. Opis danych wyjściowych znajduje się w **--print**.

-v, **--verbose**
Włącz szczegółowe dane wyjściowe podczas testowania pozycji lub wyświetlania znanych pozycji.

-T, **--test-config**
Sprawdź poprawność pliku konfiguracyjnego i zakończ działanie.

-h, **--help**
Wyświetl tę pomoc i zakończ działanie.

-V, **--version**
Wyświetl informacje o wersji i zakończ działanie.

PLIKI

/usr/local/etc/zabbix_agent2.conf
Domyślna lokalizacja pliku konfiguracyjnego Zabbix agent 2 (jeśli nie została zmodyfikowana podczas kompilacji).

ZOBACZ TAKŻE

Dokumentacja https://www.zabbix.com/manuals

zabbix_agentd(8), **zabbix_get**(8), **zabbix_js**(8), **zabbix_proxy**(8), **zabbix_sender**(8), **zabbix_server**(8)

Indeks

NAZWA

SKŁADNIA

OPIS

OPCJE

PLIKI

ZOBACZ TAKŻE

AUTOR

Ten dokument został utworzony: 14:07:57 GMT, 22 listopada 2021

zabbix_agentd

Sekcja: Polecenia do zarządzania systemem (8)
Zaktualizowano: 2019-01-29
Index Wróć do głównej zawartości

Nazwa

zabbix_agentd - Demon agenta Zabbix

SKŁADNIA

zabbix_agentd [**-c** *plik-konfiguracyjny*]
zabbix_agentd [**-c** *plik-konfiguracyjny*] **-p**
zabbix_agentd [**-c** *plik-konfiguracyjny*] **-t** *klucz-pozycji*
zabbix_agentd [**-c** *plik-konfiguracyjny*] **-R** *opcja-kontroli-działania*
zabbix_agentd [**-c** *config-file*] **-T**
zabbix_agentd -h
zabbix_agentd -V

OPIS

zabbix_agentd jest demonem monitorującym różne parametry serwera.

OPCJE

-c, **--config** *plik-konfiguracyjny*
Użyj alternatywnego *pliku-konfiguracji* zamiast domyślnego.

-f, **--foreground**
Uruchom agenta Zabbix jako proces pierwszoplanowy.

-R, **--runtime-control** *opcja-kontroli-działania*
Wykonaj funkcje administracyjne zależnie od podanej *opcji-kontroli-działania*.

Opcje kontroli w czasie działania userparameter_reload
Przeładuj parametry użytkownika z pliku konfiguracyjnego

log_level_increase[=*target*]
Zwiększ poziom logowania; jeśli target nie jest określony, dotyczy wszystkich procesów

log_level_decrease[=*target*]
Zmniejsz poziom logowania; jeśli target nie jest określony, dotyczy wszystkich procesów

Cele sterowania poziomem logowania *process-type*
Wszystkie procesy określonego typu (active checks, collector, listener)

process-type,N
Typ procesu i numer (np. listener,3)

pid
Identyfikator procesu, do 65535. Dla większych wartości określ cel jako ”process-type,N”

-p, **--print**
Wyświetl znane pozycje i zakończ. Dla każdej pozycji używane są albo ogólne wartości domyślne, albo dostarczane są specyficzne wartości domyślne do testów. Te wartości domyślne są wymienione w nawiasach kwadratowych jako parametry klucza pozycji. Zwracane wartości są ujęte w nawiasy kwadratowe i poprzedzone typem zwracanej wartości, oddzielonym znakiem pionowej kreski. Dla parametrów użytkownika typ to zawsze **t**, ponieważ agent nie może określić wszystkich możliwych wartości zwracanych. Pozycje wyświetlane jako działające nie mają gwarancji działania z serwera Zabbix ani z zabbix_get podczas odpytywania działającego demona agent, ponieważ uprawnienia lub środowisko mogą być inne. Typy zwracanych wartości to:

d
Liczba z częścią dziesiętną.

m
Nieobsługiwane. Może to być spowodowane odpytywaniem pozycji, która działa tylko w trybie aktywnym, jak pozycja monitorowania logu, albo pozycji wymagającej wielu zebranych wartości. Problemy z uprawnieniami lub nieprawidłowe parametry użytkownika również mogą skutkować stanem nieobsługiwanym.

s
Tekst. Maksymalna długość nie jest ograniczona.

t
Tekst. Tak samo jak **s**.

u
Nieujemna liczba całkowita.

-t, **--test** *item-key*
Przetestuj pojedynczą pozycję i zakończ. Opis danych wyjściowych znajduje się przy **--print**.

-T, **--test-config**
Zweryfikuj plik konfiguracyjny i zakończ.

-h, **--help**
Wyświetl tę pomoc i zakończ.

-V, **--version**
Wyświetl informacje o wersji i zakończ.

PLIKI

/usr/local/etc/zabbix_agentd.conf
Domyślna lokalizacja pliku konfiguracyjnego Zabbix agent (jeśli nie została zmieniona podczas kompilacji).

ZOBACZ TAKŻE

Dokumentacja https://www.zabbix.com/manuals

zabbix_agent2(8), **zabbix_get**(1), **zabbix_js**(1), **zabbix_proxy**(8), **zabbix_sender**(1), **zabbix_server**(8)

Indeks

NAZWA

SKŁADNIA

OPIS

OPCJE

PLIKI

ZOBACZ TAKŻE

AUTOR

Ten dokument został utworzony: 20:50:13 GMT, 22 listopada 2021

zabbix_get

Sekcja: Polecenia użytkownika (1)
Aktualizacja: 2022-01-06
Index Powrót do głównego spisu treści

NAME

zabbix_get - narzędzie Zabbix get

SKŁADNIA

zabbix_get -s *nazwa-hosta-lub-IP* [**-p** *numer-portu*] [**-I** *adres-IP*] [**-t** *limit-czasu*] **-k** *klucz-pozycji*
zabbix_get -s *nazwa-hosta-lub-IP* [**-p** *numer-portu*] [**-I** *adres-IP*] [**-t** *limit-czasu*] **--tls-connect cert --tls-ca-file** *plik-CA* [**--tls-crl-file** *plik-CRL*] [**--tls-agent-cert-issuer** *wystawca-certyfikatu] [**--tls-agent-cert-subject** podmiot-certyfikatu*] **--tls-cert-file** plik-certyfikatu* **--tls-key-file** *plik-klucza* [**--tls-cipher13** *ciąg-szyfru*] [**--tls-cipher** *ciąg-szyfru*] **-k** *klucz-pozycji*
zabbix_get -s *nazwa-hosta-lub-IP* [**-p** *numer-portu*] [**-I** *adres-IP*] [**-t** *limit-czasu*] **--tls-connect psk --tls-psk-identity** *identyfikator-PSK* **--tls-psk-file** *plik-PSK* [**--tls-cipher13** *ciąg-szyfru*] [**--tls-cipher** *ciąg-szyfru*] **-k** *klucz-pozycji*
zabbix_get -h
zabbix_get -V

OPIS

zabbix_get to narzędzie wiersza poleceń służące do pobierania danych z Zabbix agent.

OPCJE

-s, **--host** *nazwa-hosta-lub-IP*
Określ nazwę hosta lub adres IP hosta.

-p, **--port** *numer-portu*
Określ numer portu agent działającego na hoście.
Wartość domyślna to 10050.

-I, **--source-address** *adres-IP*
Określ źródłowy adres IP.

-t, **--timeout** *sekundy*
Określ limit czasu.
Prawidłowy zakres: 1-600 sekund (domyślnie: 30)

-k, **--key** *klucz-pozycji*
Określ klucz pozycji, dla której ma zostać pobrana wartość.

-P, **--protocol** *wartość*
Protokół używany do komunikacji z agent.
Wartości:

auto połącz przy użyciu protokołu JSON, w razie niepowodzenia przełącz się i ponów próbę z użyciem protokołu tekstowego (domyślnie)

json połącz przy użyciu protokołu JSON

plaintext połącz przy użyciu protokołu tekstowego, w którym wysyłany jest tylko klucz pozycji (wydania 6.4.x i starsze)

--tls-connect *wartość*
Sposób połączenia z agent.
Wartości:

nieszyfrowane
połącz bez szyfrowania (domyślnie)

psk
połącz przy użyciu TLS i klucza współdzielonego

cert
połącz przy użyciu TLS i certyfikatu

--tls-ca-file *CA-file*
Pełna ścieżka do pliku zawierającego certyfikaty nadrzędnego urzędu certyfikacji (CA) do weryfikacji certyfikatu strony zdalnej.

--tls-crl-file *CRL-file*
Pełna ścieżka do pliku zawierającego unieważnione certyfikaty.

--tls-agent-cert-issuer *cert-issuer*
Dozwolony wystawca certyfikatu agenta.

--tls-agent-cert-subject *cert-subject*
Dozwolony podmiot certyfikatu agenta.

--tls-cert-file *cert-file*
Pełna ścieżka do pliku zawierającego certyfikat lub łańcuch certyfikatów.

--tls-key-file *key-file*
Pełna ścieżka do pliku zawierającego klucz prywatny.

--tls-psk-identity *PSK-identity*
Ciąg tożsamości PSK.

--tls-psk-file *PSK-file*
Pełna ścieżka do pliku zawierającego klucz współdzielony.

--tls-cipher13 *cipher-string*
Ciąg szyfrów dla OpenSSL 1.1.1 lub nowszego dla TLS 1.3.
Zastępuje domyślne kryteria wyboru zestawu szyfrów.
Ta opcja nie jest dostępna, jeśli wersja OpenSSL jest niższa niż 1.1.1.

--tls-cipher *cipher-string*
Ciąg priorytetów GnuTLS (dla TLS 1.2 i nowszych) lub ciąg szyfrów OpenSSL
(tylko dla TLS 1.2).
Zastępuje domyślne kryteria wyboru zestawu szyfrów.

-h, **--help**
Wyświetl tę pomoc i zakończ.

-V, **--version**
Wyświetl informacje o wersji i zakończ.

PRZYKŁADY

zabbix_get -s 127.0.0.1 -p 10050 -k ”system.cpu.load[all,avg1]”
zabbix_get -s 127.0.0.1 -p 10050 -k ”system.cpu.load[all,avg1]” --tls-connect cert --tls-ca-file /home/zabbix/zabbix_ca_file --tls-agent-cert-issuer ”CN=Signing CA,OU=IT operations,O=Example Corp,DC=example,DC=com” --tls-agent-cert-subject ”CN=server1,OU=IT operations,O=Example Corp,DC=example,DC=com” --tls-cert-file /home/zabbix/zabbix_get.crt --tls-key-file /home/zabbix/zabbix_get.key
zabbix_get -s 127.0.0.1 -p 10050 -k ”system.cpu.load[all,avg1]” --tls-connect psk --tls-psk-identity ”PSK ID Zabbix agentd” --tls-psk-file /home/zabbix/zabbix_agentd.psk

ZOBACZ TAKŻE

Dokumentacja https://www.zabbix.com/manuals

zabbix_agentd(8), **zabbix_proxy**(8), **zabbix_sender**(1), **zabbix_server**(8), **zabbix_js**(1), **zabbix_agent2**(8), **zabbix_web_service**(8)

Indeks

NAZWA

SKŁADNIA

OPIS

OPCJE

PRZYKŁADY

ZOBACZ TAKŻE

AUTOR

Ten dokument został utworzony: 08:42:29 GMT, 11 czerwca 2021

zabbix_js

Sekcja: Polecenia użytkownika (1)
Aktualizacja: 2022-01-06
Index Powrót do głównego spisu treści

NAZWA

zabbix_js - narzędzie Zabbix JS

SKŁADNIA

zabbix_js -s *plik-skryptu* **-p** *parametry-wejściowe* [**-l** *poziom-logowania*] [**-t** *limit-czasu*]
zabbix_js -s *plik-skryptu* **-i** *plik-parametry-wejściowe* [**-l** *poziom-logowania*] [**-t** *limit-czasu*]
zabbix_js -h
zabbix_js -V

OPIS

zabbix_js to narzędzie wiersza poleceń, które może być używane do testowania osadzonych skryptów.

OPCJE

-s, **--script** *script-file*
Określ nazwę pliku skryptu do wykonania. Jeśli jako nazwę pliku podano '-', skrypt zostanie odczytany ze standardowego wejścia.

-p, **--param** *input-param*
Określ parametr wejściowy.

-i, **--input** *input-file*
Określ nazwę pliku parametru wejściowego. Jeśli jako nazwę pliku podano '-', dane wejściowe zostaną odczytane ze standardowego wejścia.

-w, **--webdriver** *url*
Określ adres URL webdrivera.

-l, **--loglevel** *log-level*
Określ poziom logowania.

-t, **--timeout** *timeout*
Określ limit czasu w sekundach. Prawidłowy zakres: 1-600 sekund (domyślnie: 10)

-h, **--help**
Wyświetl tę pomoc i zakończ działanie.

-V, **--version**
Wyświetl informacje o wersji i zakończ działanie.

PRZYKŁADY

zabbix_js -s script-file.js -p example

ZOBACZ TAKŻE

Dokumentacja https://www.zabbix.com/manuals

zabbix_agent2(8), **zabbix_agentd**(8), **zabbix_get**(1), **zabbix_proxy**(8), **zabbix_sender**(1), **zabbix_server**(8)

Indeks

NAZWA

SKŁADNIA

OPIS

OPCJE

PRZYKŁADY

ZOBACZ TAKŻE

Ten dokument został utworzony: 21:23:35 GMT, 18 marca 2020

zabbix_proxy

Sekcja: Polecenia do zarządzania systemem (8)
Zaktualizowano: 2020-09-04
Indeks Wróc do głównej zawartości

NAZWA

zabbix_proxy - Demon Zabbix proxy

SKŁADNIA

zabbix_proxy [**-c** *plik-konfiguracyjny*]
zabbix_proxy [**-c** *plik-konfiguracyjny*] **-R** *opcja-kontroli-działania*
zabbix_proxy [**-c** *config-file*] **-T**
zabbix_proxy -h
zabbix_proxy -V

OPIS

zabbix_proxy jest demonem, który zbiera dane monitoringu z urządzeń i wysyła je do serwera Zabbix.

OPCJE

-c, **--config** *plik-konfiguracyjny*
Użyj alternatywnego *pliku-konfiguracji* zamiast domyślnego.

-f, **--foreground**
Uruchom Zabbix proxy jako proces pierwszoplanowy.

-R, **--runtime-control** *opcja-kontroli-działania*
Wykonaj funkcje administracyjne zależnie od podanej *opcji-kontroli-działania*.

Opcje kontroli w czasie działania config_cache_reload
Przeładuj pamięć podręczną konfiguracji. Ignorowane, jeśli pamięć podręczna jest obecnie ładowana. Aktywny proxy Zabbix połączy się z serwerem Zabbix i zażąda danych konfiguracyjnych. Domyślny plik konfiguracyjny (o ile nie podano opcji **-c**) zostanie użyty do znalezienia pliku PID, a sygnał zostanie wysłany do procesu wskazanego w pliku PID.

snmp_cache_reload
Przeładuj pamięć podręczną SNMP. Należy pamiętać, że Zabbix buforuje mapowania EngineID→IP dla SNMPv3 i może automatycznie ponownie używać EngineID, aby zmniejszyć narzut odpytywania.

housekeeper_execute
Uruchom housekeeper. Ignorowane, jeśli housekeeper jest obecnie wykonywany.

diaginfo[=*section*]
Zapisz w logu wewnętrzne informacje diagnostyczne określonej sekcji. Sekcją może być *historycache*, *preprocessing*, *locks*. Domyślnie zapisywane są informacje diagnostyczne wszystkich sekcji.

log_level_increase[=*target*]
Zwiększ poziom logowania; jeśli target nie zostanie określony, dotyczy to wszystkich procesów.

log_level_decrease[=*target*]
Zmniejsz poziom logowania; jeśli target nie zostanie określony, dotyczy to wszystkich procesów.

Cele sterowania poziomem logowania *process-type*
Wszystkie procesy określonego typu (menedżer dostępności, browser poller, synchronizator konfiguracji, nadawca danych, menedżer wykrywania, synchronizator historii, housekeeper, http poller, icmp pinger, menedżer ipmi, ipmi poller, java poller, odbc poller, poller, agent poller, http agent poller, snmp poller, menedżer przetwarzania wstępnego, self-monitoring, snmp trapper, menedżer zadań, trapper, unreachable poller, kolektor vmware)

process-type,N
Typ procesu i numer (np. poller,3)

pid
Identyfikator procesu, do 65535. Dla większych wartości określ cel jako „process-type,N”

Cele sterowania profilowaniem

process-type
Wszystkie procesy określonego typu (synchronizator konfiguracji, nadawca danych, menedżer wykrywania, synchronizator historii, housekeeper, http poller, menedżer przetwarzania wstępnego, icmp pinger, menedżer ipmi, ipmi poller, java poller, poller, agent poller, http agent poller, snmp poller, self-monitoring, snmp trapper, menedżer zadań, trapper, unreachable poller, kolektor vmware, history poller, menedżer dostępności, odbc poller)

process-type,N
Typ procesu i numer (np. history syncer,1)

pid
Identyfikator procesu, do 65535. Dla większych wartości określ cel jako „process-type,N”

scope
Zakres profilowania (rwlock, mutex, processing) może być używany z typem procesu (np. history syncer,1,processing)

-T, **--test-config**
Sprawdź poprawność pliku konfiguracyjnego i zakończ.

-h, **--help**
Wyświetl tę pomoc i zakończ.

-V, **--version**
Wyświetl informacje o wersji i zakończ.

PLIKI

/usr/local/etc/zabbix_proxy.conf
Domyślna lokalizacja pliku konfiguracyjnego proxy Zabbix (jeśli nie została zmodyfikowana podczas kompilacji).

ZOBACZ TAKŻE

Dokumentacja https://www.zabbix.com/manuals

zabbix_agentd(8), **zabbix_get**(1), **zabbix_sender**(1), **zabbix_server**(8), **zabbix_js**(1), **zabbix_agent2**(8)

Indeks

NAZWA

SKŁADNIA

OPIS

OPCJE

PLIKI

ZOBACZ TAKŻE

AUTOR

Ten dokument został utworzony: 16:12:22 GMT, 04 września 2020

zabbix_sender

Sekcja: Polecenia użytkownika (1)
Zaktualizowano: 2021-06-01
Indeks Powrót do głównego spisu treści

NAME

zabbix_sender - narzędzie Zabbix sender

SKŁADNIA

zabbix_sender [**-v**] **-z** *serwer* [**-p** *port*] [**-I** *adres-IP*] [**-t** *limit-czasu*] **-s** *host* **-k** *klucz* **-o** *wartość*
zabbix_sender [**-v**] **-z** *serwer* [**-p** *port*] [**-I** *adres-IP*] [**-t** *limit-czasu*] [**-s** *host*] [**-T**] [**-N**] [**-r**] [**-g**] **-i** *plik-wejściowy*
zabbix_sender [**-v**] **-c** *plik-konfiguracyjny* [**-z** *serwer*] [**-p** *port*] [**-I** *adres-IP*] [**-t** *limit-czasu*] [**-s** *host*] **-k** *klucz* **-o** *wartość*
zabbix_sender [**-v**] **-c** *plik-konfiguracyjny* [**-z** *serwer*] [**-p** *port*] [**-I** *adres-IP*] [**-t** *limit-czasu*] [**-s** *host*] [**-T**] [**-N**] [**-r**] [**-g**] **-i** *plik-wejściowy*
zabbix_sender [**-v**] **-z** *serwer* [**-p** *port*] [**-I** *adres-IP*] [**-t** *limit-czasu*] **-s** *host* **--tls-connect cert --tls-ca-file** *plik-CA* [**--tls-crl-file** *plik-CRL*] [**--tls-server-cert-issuer** *wystawca-certyfikatu*] [**--tls-server-cert-subject** *podmiot-certyfikatu*] **--tls-cert-file** *plik-certyfikatu* **--tls-key-file** *plik-klucza* [**--tls-cipher13** *ciąg-szyfrów*] [**--tls-cipher** *ciąg-szyfrów*] **-k** *klucz* **-o** *wartość*
zabbix_sender [**-v**] **-z** *serwer* [**-p** *port*] [**-I** *adres-IP*] [**-t** *limit-czasu*] [**-s** *host*] **--tls-connect cert --tls-ca-file** *plik-CA* [**--tls-crl-file** *plik-CRL*] [**--tls-server-cert-issuer** *wystawca-certyfikatu*] [**--tls-server-cert-subject** *podmiot-certyfikatu*] **--tls-cert-file** *plik-certyfikatu* **--tls-key-file** *plik-klucza* [**--tls-cipher13** *ciąg-szyfrów*] [**--tls-cipher** *ciąg-szyfrów*] [**-T**] [**-N**] [**-r**] [**-g**] **-i** *plik-wejściowy*
zabbix_sender [**-v**] **-c** *plik-konfiguracyjny* [**-z** *serwer*] [**-p** *port*] [**-I** *adres-IP*] [**-t** *limit-czasu*] [**-s** *host*] **--tls-connect cert --tls-ca-file** *plik-CA* [**--tls-crl-file** *plik-CRL*] [**--tls-server-cert-issuer** *wystawca-certyfikatu*] [**--tls-server-cert-subject** *podmiot-certyfikatu*] **--tls-cert-file** *plik-certyfikatu* **--tls-key-file** *plik-klucza* [**--tls-cipher13** *ciąg-szyfrów*] [**--tls-cipher** *ciąg-szyfrów*] **-k** *klucz* **-o** *wartość*
zabbix_sender [**-v**] **-c** *plik-konfiguracyjny* [**-z** *serwer*] [**-p** *port*] [**-I** *adres-IP*] [**-t** *limit-czasu*] [**-s** *host*] **--tls-connect cert --tls-ca-file** *plik-CA* [**--tls-crl-file** *plik-CRL*] [**--tls-server-cert-issuer** *wystawca-certyfikatu*] [**--tls-server-cert-subject** *podmiot-certyfikatu*] **--tls-cert-file** *plik-certyfikatu* **--tls-key-file** *plik-klucza* [**--tls-cipher13** *ciąg-szyfrów*] [**--tls-cipher** *ciąg-szyfrów*] [**-T**] [**-N**] [**-r**] [**-g**] **-i** *plik-wejściowy*
zabbix_sender [**-v**] **-z** *serwer* [**-p** *port*] [**-I** *adres-IP*] [**-t** *limit-czasu*] **-s** *host* **--tls-connect psk --tls-psk-identity** *tożsamość-PSK* **--tls-psk-file** *plik-PSK* [**--tls-cipher13** *ciąg-szyfrów*] [**--tls-cipher** *ciąg-szyfrów*] **-k** *klucz* **-o** *wartość*
zabbix_sender [**-v**] **-z** *serwer* [**-p** *port*] [**-I** *adres-IP*] [**-t** *limit-czasu*] [**-s** *host*] **--tls-connect psk --tls-psk-identity** *tożsamość-PSK* **--tls-psk-file** *plik-PSK* [**--tls-cipher13** *ciąg-szyfrów*] [**--tls-cipher** *ciąg-szyfrów*] [**-T**] [**-N**] [**-r**] [**-g**] **-i** *plik-wejściowy*
zabbix_sender [**-v**] **-c** *plik-konfiguracyjny* [**-z** *serwer*] [**-p** *port*] [**-I** *adres-IP*] [**-t** *limit-czasu*] [**-s** *host*] **--tls-connect psk --tls-psk-identity** *tożsamość-PSK* **--tls-psk-file** *plik-PSK* [**--tls-cipher13** *ciąg-szyfrów*] [**--tls-cipher** *ciąg-szyfrów*] **-k** *klucz* **-o** *wartość*
zabbix_sender [**-v**] **-c** *plik-konfiguracyjny* [**-z** *serwer*] [**-p** *port*] [**-I** *adres-IP*] [**-t** *limit-czasu*] [**-s** *host*] **--tls-connect psk --tls-psk-identity** *tożsamość-PSK* **--tls-psk-file** *plik-PSK* [**--tls-cipher13** *ciąg-szyfrów*] [**--tls-cipher** *ciąg-szyfrów*] [**-T**] [**-N**] [**-r**] [**-g**] **-i** *plik-wejściowy*
zabbix_sender -h
zabbix_sender -V

DESCRIPTION

zabbix_sender jest narzędziem linii poleceń, który wysyła dane do serwera Zabbix lub proxy. Na serwerze Zabbix należy utworzyć pozycję **Trapper Zabbix** z odpowiednim kluczem. Należy pamiętać, że zwrócone będą akceptowane tylko z hostów określonych w polu **Dopuszczalne hosty** dla tej pozycji.

OPCJE

-c, **--config** *config-file*
Użyj *config-file*. **Zabbix sender** odczytuje szczegóły serwera z pliku konfiguracji agentd. Domyślnie **Zabbix sender** nie odczytuje żadnego pliku konfiguracyjnego. Obsługiwane są tylko parametry **Hostname**, **ServerActive**, **SourceIP**, **TLSConnect**, **TLSCAFile**, **TLSCRLFile**, **TLSServerCertIssuer**, **TLSServerCertSubject**, **TLSCertFile**, **TLSKeyFile**, **TLSPSKIdentity** oraz **TLSPSKFile**.
Hostname zdefiniowany za pomocą parametru **HostnameItem** nie zostanie pobrany; w takim przypadku nazwę hosta należy podać w wierszu poleceń (zobacz opcję -s).
Wszystkie adresy zdefiniowane w parametrze konfiguracyjnym **ServerActive** agenta są używane do wysyłania danych. Jeśli wysyłanie partii danych do jednego adresu zakończy się niepowodzeniem, kolejne partie nie będą wysyłane na ten adres.

-z, **--zabbix-server** *server*
Nazwa hosta lub adres IP serwera Zabbix. Jeśli host jest monitorowany przez proxy, należy użyć nazwy hosta proxy lub jego adresu IP. W przypadku użycia razem z **--config** nadpisuje wpisy parametru **ServerActive** określone w pliku konfiguracji agentd.

-p, **--port** *port*
Określ numer portu trappera serwera Zabbix działającego na serwerze. Wartość domyślna to 10051. W przypadku użycia razem z **--config** nadpisuje wpisy portu parametru **ServerActive** określone w pliku konfiguracji agentd.

-I, **--source-address** *IP-address*
Określ źródłowy adres IP. W przypadku użycia razem z **--config** nadpisuje parametr **SourceIP** określony w pliku konfiguracji agentd.

-t, **--timeout** *seconds*
Określ limit czasu. Prawidłowy zakres: 1-300 sekund (domyślnie: 60)

-s, **--host** *host*
Określ nazwę hosta, do którego należy pozycja (zgodnie z rejestracją w frontendzie Zabbix). Adres IP hosta ani nazwa DNS nie zadziałają. W przypadku użycia razem z **--config** nadpisuje parametr **Hostname** określony w pliku konfiguracji agentd.

-k, **--key** *key*
Określ klucz pozycji, do której ma zostać wysłana wartość.

-o, **--value** *value*
Określ wartość pozycji.

-i, **--input-file** *input-file*
Wczytaj wartości z pliku wejściowego. Podaj **-** jako **<input-file>**, aby odczytywać wartości ze standardowego wejścia. Każdy wiersz pliku zawiera wpisy rozdzielone białymi znakami: **<hostname> <key> <value>**. Każda wartość musi być określona w osobnym wierszu. Każdy wiersz musi zawierać 3 wpisy rozdzielone białymi znakami: **<hostname> <key> <value>**, gdzie „hostname” to nazwa monitorowanego hosta zarejestrowana w frontendzie Zabbix, „key” to klucz docelowej pozycji, a „value” — wartość do wysłania. Podaj **-** jako **<hostname>**, aby użyć nazwy hosta z pliku konfiguracji agenta lub z argumentu **--host**.

Przykład wiersza pliku wejściowego:

”Linux DB3” db.connections 43

Typ wartości musi być poprawnie ustawiony w konfiguracji pozycji we frontendzie Zabbix.
Zabbix sender wyśle do 250 wartości w jednym połączeniu.
Limit rozmiaru dla wysyłania wartości z pliku wejściowego zależy od rozmiaru opisanego w protokole komunikacyjnym Zabbix.
Zawartość pliku wejściowego musi być zakodowana w UTF-8.
Wszystkie wartości z pliku wejściowego są wysyłane sekwencyjnie, od góry do dołu.
Wpisy muszą być sformatowane zgodnie z następującymi zasadami:

- Obsługiwane są wpisy ujęte i nieujęte w cudzysłów.
- Znakiem cytowania jest podwójny cudzysłów.
- Wpisy zawierające białe znaki muszą być ujęte w cudzysłów.
- Znaki podwójnego cudzysłowu i ukośnika odwrotnego wewnątrz wpisu ujętego w cudzysłów muszą być poprzedzone ukośnikiem odwrotnym.
- Escaping nie jest obsługiwany we wpisach nieujętych w cudzysłów.
- Sekwencje ucieczki znaku nowej linii (\n) są obsługiwane w ciągach ujętych w cudzysłów.
- Sekwencje ucieczki znaku nowej linii są usuwane z końca wpisu.

-T, **--with-timestamps**
Ta opcja może być używana tylko razem z opcją **--input-file**.

Każdy wiersz pliku wejściowego musi zawierać 4 wpisy rozdzielone białymi znakami: **<hostname> <key> <timestamp> <value>**.
Znacznik czasu powinien być podany w formacie Unix timestamp. Jeśli docelowa pozycja ma wyzwalacze odwołujące się do niej, wszystkie znaczniki czasu muszą być w kolejności rosnącej, w przeciwnym razie obliczanie zdarzeń nie będzie poprawne.

Przykład wiersza pliku wejściowego:

”Linux DB3” db.connections 1429533600 43

Więcej szczegółów można znaleźć przy opcji **--input-file**.

Jeśli wartość ze znacznikiem czasu zostanie wysłana dla hosta, który znajduje się w konserwacji typu „brak danych”, to ta wartość zostanie odrzucona; jednak możliwe jest wysłanie wartości ze znacznikiem czasu dla wygasłego okresu konserwacji i zostanie ona zaakceptowana.

-N, **--with-ns**
Ta opcja może być używana tylko razem z opcją **--with-timestamps**.

Każdy wiersz pliku wejściowego musi zawierać 5 wpisów rozdzielonych białymi znakami: **<hostname> <key> <timestamp> <ns> <value>**.

Przykład wiersza pliku wejściowego:

”Linux DB3” db.connections 1429533600 7402561 43

Więcej szczegółów można znaleźć przy opcji **--input-file**.

-r, **--real-time**
Wysyłaj wartości pojedynczo natychmiast po ich odebraniu. Może to być używane podczas odczytu ze standardowego wejścia.

-g, **--group**
Grupuj wartości według hostów i wysyłaj je do każdego hosta w osobnej partii.

--tls-connect *value*
Sposób połączenia z serwerem lub proxy. Wartości:

unencrypted
połącz bez szyfrowania (domyślnie)

psk
połącz za pomocą TLS oraz klucza współdzielonego

cert
połącz za pomocą TLS oraz certyfikatu

--tls-ca-file *plik-CA*
Pełna ścieżka do pliku zawierającego certyfikaty urzędu certyfikacji dla weryfikacji certyfikatów równorzędnych.

--tls-crl-file *plik-CRL*
Pełna ścieżka do pliku zawierającego unieważnione certyfikaty.

--tls-server-cert-issuer *wystawca-certyfikatu*
Dozwolony wystawca certyfikatu.

--tls-server-cert-subject *podmiot-certyfikatu*
Dozwolony podmiot certyfikatu.

--tls-cert-file *plik-certyfikatu*
Pełna ścieżka do pliku zawierającego certyfikat lub łańcuch certyfikatów.

--tls-key-file *klucz-prywatny*
Pełna ścieżka do pliku zawierającego klucz prywatny.

--tls-psk-identity *identyfikator-PSK*
Ciąg znaków identyfikatora PSK.

--tls-psk-file *plik-PSK*
Pełna ścieżka do pliku zawierającego klucz współdzielony.

--tls-cipher13 *ciąg-szyfru*
Ciąg szyfru dla OpenSSL 1.1.1 lub nowszego dla TLS 1.3. Zastępuje domyślne kryteria wyboru zestawu szyfrów. Ta opcja nie jest dostępna, jeżeli wersja OpenSSL jest starsza niż 1.1.1.

--tls-cipher *ciąg-szyfru*
Łańcuch priorytetów GnuTLS (dla TLS 1.2 i nowszych) lub łańcuch szyfrujący OpenSSL (tylko dla TLS 1.2). Zastępuje domyślne kryteria wyboru zestawu szyfrów.

-v, **--verbose**
Tryb szczegółowy, **-vv** dla jeszcze więcej szczegółów.

-h, **--help**
Wypisuje tę pomoc i kończy działanie.

-V, **--version**
Wypisuje informacje o wersji i kończy działanie.

KOD POWROTU

Kod powrotu jest równy 0 jeżeli wartości zostały wysłane i wszystkie z nich zostały pomyślnie przetworzone przez serwer. Jeśli dane zostały wysłane, ale przetwarzanie chociaż jednej z nich nie powiodło się, kod powrotu wynosi 2. Jeśli wysyłanie danych nie powiodło się, kod powrotu jest równy 1.

PRZYKŁADY

zabbix_sender -c /etc/zabbix/zabbix_agentd.conf -k mysql.queries -o 342.45

Wysyła **342.45** jako wartość dla pozycji **mysql.queries** monitorowanego hosta. Używa monitorowanego hosta i serwer Zabbix zdefiniowanego w pliku konfiguracyjnym agenta.

zabbix_sender -c /etc/zabbix/zabbix_agentd.conf -s ”Monitorowany Host” -k mysql.queries -o 342.45

Wysyła **342.45** jako wartość dla pozycji **mysql.queries** dla hosta **Monitorowany Host** na serwer Zabbix zdefiniowany w pliku konfiguracyjnym agenta.

zabbix_sender -z 192.168.1.113 -i data_values.txt

Wysyła wartości z pliku **data_values.txt** do serwera Zabbix o adresie IP **192.168.1.113**. Nazwy hostów i klucze są zdefiniowane w pliku.

echo ”- hw.serial.number 1287872261 SQ4321ASDF” | zabbix_sender -c /usr/local/etc/zabbix_agentd.conf -T -i -

Wysyła wartość ze znacznikiem czasu z wiersza poleceń do serwera Zabbix określonego w pliku konfiguracyjnym agenta. Myślnik w danych wejściowych wskazuje, że nazwa hosta powinna być pobrana również z tego samego pliku konfiguracyjnego.

echo ’”Zabbix server” trapper.item ””’ | zabbix_sender -z 192.168.1.113 -p 10000 -i -

Wysyła pustą wartość pozycji do serwera Zabbix z adresem IP **192.168.1.113** na porcie **10000** z wiersza poleceń. Puste wartości musza być zawarte w podwójnych cudzysłowach.

zabbix_sender -z 192.168.1.113 -s ”Monitorowany Host” -k mysql.queries -o 342.45 --tls-connect cert --tls-ca-file /home/zabbix/zabbix_ca_file --tls-cert-file /home/zabbix/zabbix_agentd.crt --tls-key-file /home/zabbix/zabbix_agentd.key

Wysyła **342.45** jako wartość dla pozycji **mysql.queries** dla hosta **Monitorowany Host** do serwera o adresie IP **192.168.1.113** używając TLS razem z certyfikatem.

zabbix_sender -z 192.168.1.113 -s ”Monitorowany Host” -k mysql.queries -o 342.45 --tls-connect psk --tls-psk-identity ”PSK ID Zabbix agentd” --tls-psk-file /home/zabbix/zabbix_agentd.psk

Wysyła **342.45** jako wartość dla pozycji **mysql.queries** dla hosta **Monitorowany Host** do serwera o adresie IP **192.168.1.113** używając TLS razem z kluczem współdzielonym (PSK).

ZOBACZ TAKŻE

Dokumentacja https://www.zabbix.com/manuals

zabbix_agentd(8), **zabbix_get**(1), **zabbix_proxy**(8), **zabbix_server**(8), **zabbix_js**(1), **zabbix_agent2**(8), **zabbix_web_service**(8)

Indeks

NAZWA

STRESZCZENIE

OPIS

OPCJE

STATUS WYJŚCIA

PRZYKŁADY

ZOBACZ TAKŻE

AUTOR

Ten dokument został utworzony: 08:42:39 GMT, 11 czerwca 2021 r.

zabbix_server

Sekcja: Polecenia do zarządzania systemem (8)
Zaktualizowano: 2020-09-04
Indeks Wróć do głównej zawartości

NAME

zabbix_server - Demon serwera Zabbix

SKŁADNIA

zabbix_server [**-c** *config-file*]
zabbix_server [**-c** *config-file*] **-R** *runtime-option*
zabbix_server [**-c** *config-file*] **-T**
zabbix_server -h
zabbix_server -V

OPIS

zabbix_server jest głównym demonem oprogramowania Zabbix.

OPCJE

-c, **--config** *config-file*
Użyj alternatywnego pliku *config-file* zamiast domyślnego.

-f, **--foreground**
Uruchom serwer Zabbix na pierwszym planie.

-R, **--runtime-control** *runtime-option*
Wykonaj funkcje administracyjne zgodnie z opcją *runtime-option*.

-T, **--test-config**
Zweryfikuj plik konfiguracyjny i zakończ działanie.

-h, **--help**
Wyświetl tę pomoc i zakończ działanie.

-V, **--version**
Wyświetl informacje o wersji i zakończ działanie.

Przykłady uruchamiania serwera Zabbix z parametrami wiersza poleceń:

```
zabbix_server -c /usr/local/etc/zabbix_server.conf
zabbix_server --help
zabbix_server -V
```

KONTROLA W CZASIE DZIAŁANIA

Opcje kontroli w czasie działania:

config_cache_reload
Przeładuj pamięć podręczną konfiguracji. Ignorowane, jeśli pamięć podręczna jest obecnie ładowana. Do znalezienia pliku PID zostanie użyty domyślny plik konfiguracyjny (chyba że podano opcję **-c**), a sygnał zostanie wysłany do procesu wskazanego w pliku PID.

snmp_cache_reload
Przeładuj pamięć podręczną SNMP, wyczyść właściwości SNMP (engine time, engine boots, engine id, credentials) dla wszystkich hostów. Należy pamiętać, że Zabbix buforuje mapowania SNMPv3 EngineID→IP i może automatycznie ponownie używać EngineID, aby zmniejszyć narzut odpytywania.

housekeeper_execute
Uruchom housekeeper. Ignorowane, jeśli housekeeper jest obecnie wykonywany.

trigger_housekeeper_execute
Uruchom housekeeper wyzwalaczy (usuń problemy dla usuniętych wyzwalaczy). Ignorowane, jeśli housekeeper wyzwalaczy dla usług jest obecnie wykonywany.

diaginfo[=*section*]
Zapisz w logu wewnętrzne informacje diagnostyczne dla określonej sekcji. Sekcją może być *historycache*, *preprocessing*, *alerting*, *lld*, *valuecache*, *locks*. Domyślnie zapisywane są informacje diagnostyczne dla wszystkich sekcji.

ha_status
Zapisz w logu stan klastra wysokiej dostępności (HA).

ha_remove_node[=*target*]
Usuń węzeł wysokiej dostępności (HA), określony przez nazwę lub ID. Pamiętaj, że aktywne/zapasowe węzły nie mogą zostać usunięte.

ha_set_failover_delay[=*delay*]
Ustaw opóźnienie przełączenia awaryjnego wysokiej dostępności (HA). Obsługiwane są sufiksy czasu, np. 10s, 1m.

proxy_config_cache_reload[=*target*] Przeładuj pamięć podręczną konfiguracji proxy.

secrets_reload
Przeładuj sekrety z Vault.

service_cache_reload
Przeładuj pamięć podręczną menedżera usług.

prof_enable[=*target*]
Włącz profilowanie. Wpływa na wszystkie procesy, jeśli target nie został określony. Włączone profilowanie dostarcza szczegółów o wszystkich rwlockach/mutexach według nazw funkcji.

prof_disable[=*target*]
Wyłącz profilowanie. Wpływa na wszystkie procesy, jeśli target nie został określony.

log_level_increase[=*target*]
Zwiększ poziom logowania; wpływa na wszystkie procesy, jeśli target nie został określony

log_level_decrease[=*target*]
Zmniejsz poziom logowania; wpływa na wszystkie procesy, jeśli target nie został określony

Cele sterowania poziomem logowania *process-type*
Wszystkie procesy określonego typu (alerter, menedżer alertów, menedżer dostępności, browser poller, configuration syncer, worker configuration syncer, menedżer connectorów, worker connectora, menedżer wykrywania, escalator, menedżer HA, history poller, history syncer, housekeeper, http poller, icmp pinger, internal poller, menedżer IPMI, ipmi poller, java poller, odbc poller,

poller, agent poller, http agent poller, snmp poller, menedżer przetwarzania wstępnego, menedżer grup proxy, proxy poller, self-monitoring, menedżer usług, snmp trapper, menedżer zadań, timer, trapper, unreachable poller, vmware collector)

process-type,N
Typ procesu i numer (np. poller,3)

pid
Identyfikator procesu, do 65535. Dla większych wartości określ cel jako ”process-type,N”

Cele sterowania profilowaniem

process-type
Wszystkie procesy określonego typu (alerter, menedżer alertów, menedżer dostępności, browser poller, configuration syncer, worker configuration syncer, menedżer connectorów, worker connectora, menedżer wykrywania, escalator, menedżer HA, history poller, history syncer, housekeeper, http poller, icmp pinger, internal poller, menedżer IPMI, ipmi poller, java poller, odbc poller, poller, agent poller, http agent poller, snmp poller, menedżer przetwarzania wstępnego, menedżer grup proxy, proxy poller, self-monitoring, menedżer usług, snmp trapper, menedżer zadań, timer, trapper, unreachable poller, vmware collector)

process-type,N
Typ procesu i numer (np. history syncer,1)

pid
Identyfikator procesu, do 65535. Dla większych wartości określ cel jako ”process-type,N”

scope
Zakres profilowania (rwlock, mutex, processing) może być używany z typem procesu (np. history syncer,1,processing)

PLIKI

/usr/local/etc/zabbix_server.conf
Domyślna lokalizacja pliku konfiguracyjnego serwera Zabbix (jeśli nie została zmodyfikowana podczas kompilacji).

ZOBACZ TAKŻE

Dokumentacja https://www.zabbix.com/manuals

zabbix_agentd(8), **zabbix_get**(1), **zabbix_proxy**(8), **zabbix_sender**(1), **zabbix_js**(1), **zabbix_agent2**(8)

Indeks

NAZWA

SKŁADNIA

OPIS

OPCJE

PLIKI

ZOBACZ TAKŻE

AUTOR

Ten dokument został utworzony: 16:12:14 GMT, 04 września 2020

zabbix_web_service

Sekcja: Polecenia konserwacyjne (8)
Zaktualizowano: 2019-01-29
Index Powrót do głównego spisu treści

NAZWA

zabbix_web_service — usługa internetowa Zabbix

SKŁADNIA

zabbix_web_service [**-c** *config-file*]
zabbix_web_service [**-c** *config-file*] **-T**
zabbix_web_service -h
zabbix_web_service -V

OPIS

zabbix_web_service jest aplikacją do świadczenia usług internetowych dla komponentów Zabbix.

OPCJE

-c, **--config** *config-file*
Użyj alternatywnego pliku *config-file* zamiast domyślnego.

-T, **--test-config**
Sprawdź poprawność pliku konfiguracyjnego i zakończ działanie.

-h, **--help**
Wyświetl tę pomoc i zakończ działanie.

-V, **--version**
Wyświetl informacje o wersji i zakończ działanie.

PLIKI

/usr/local/etc/zabbix_web_service.conf
Domyślna lokalizacja pliku konfiguracyjnego dla Zabbix web service (jeżeli nie zostało to zmodyfikowane podczas komplikacji).

ZOBACZ TAKŻE

Dokumentacja https://www.zabbix.com/manuals

zabbix_agentd(8), **zabbix_get**(1), **zabbix_proxy**(8), **zabbix_sender**(1), **zabbix_server**(8), **zabbix_js**(1), **zabbix_agent2**(8)

Indeks

NAZWA

SKŁADNIA

OPIS

OPCJE

PLIKI

ZOBACZ TAKŻE

AUTOR

Ten dokument został stworzony o: 12:58:30 GMT, 11 czerwca, 2021

Informacja o prawach autorskich

Dokumentacja Zabbix NIE jest rozpowszechniana na licencji AGPL-3.0. Korzystanie z dokumentacji Zabbix podlega następującym warunkom:

Możesz utworzyć drukowaną kopię tej dokumentacji wyłącznie do własnego użytku osobistego. Konwersja do innych formatów jest dozwolona, o ile rzeczywista treść nie zostanie w żaden sposób zmieniona ani zredagowana. Nie wolno publikować ani rozpowszechniać tej dokumentacji w żadnej formie ani na żadnym nośniku, chyba że rozpowszechniasz dokumentację w sposób podobny do

tego, w jaki rozpowszechnia ją Zabbix (to znaczy elektronicznie do pobrania na stronie internetowej Zabbix) albo na nośniku USB lub podobnym, pod warunkiem jednak, że dokumentacja jest rozpowszechniana razem z oprogramowaniem na tym samym nośniku. Jakiekolwiek inne wykorzystanie, takie jak jakiekolwiek rozpowszechnianie drukowanych kopii lub wykorzystanie tej dokumentacji, w całości lub w części, w innej publikacji, wymaga uprzedniej pisemnej zgody upoważnionego przedstawiciela Zabbix. Zabbix zastrzega sobie wszelkie prawa do tej dokumentacji, które nie zostały wyraźnie przyznane powyżej.