### Contents

**Zabbix Manual**

<table>
<thead>
<tr>
<th>1. Introduction</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Manual structure</td>
<td>5</td>
</tr>
<tr>
<td>2 What is Zabbix</td>
<td>6</td>
</tr>
<tr>
<td>3 Zabbix features</td>
<td>6</td>
</tr>
<tr>
<td>4 Zabbix overview</td>
<td>7</td>
</tr>
<tr>
<td>5 What’s new in Zabbix 4.0.0</td>
<td>8</td>
</tr>
<tr>
<td>6 What’s new in Zabbix 4.0.1</td>
<td>32</td>
</tr>
<tr>
<td>7 What’s new in Zabbix 4.0.2</td>
<td>33</td>
</tr>
<tr>
<td>8 What’s new in Zabbix 4.0.3</td>
<td>33</td>
</tr>
<tr>
<td>9 What’s new in Zabbix 4.0.4</td>
<td>34</td>
</tr>
<tr>
<td>10 What’s new in Zabbix 4.0.5</td>
<td>34</td>
</tr>
<tr>
<td>11 What’s new in Zabbix 4.0.6</td>
<td>35</td>
</tr>
<tr>
<td>12 What’s new in Zabbix 4.0.7</td>
<td>36</td>
</tr>
<tr>
<td>13 What’s new in Zabbix 4.0.8</td>
<td>37</td>
</tr>
<tr>
<td>14 What’s new in Zabbix 4.0.9</td>
<td>37</td>
</tr>
<tr>
<td>15 What’s new in Zabbix 4.0.10</td>
<td>37</td>
</tr>
<tr>
<td>16 What’s new in Zabbix 4.0.11</td>
<td>38</td>
</tr>
<tr>
<td>17 What’s new in Zabbix 4.0.12</td>
<td>39</td>
</tr>
<tr>
<td>18 What’s new in Zabbix 4.0.13</td>
<td>39</td>
</tr>
<tr>
<td>19 What’s new in Zabbix 4.0.14</td>
<td>39</td>
</tr>
<tr>
<td>20 What’s new in Zabbix 4.0.15</td>
<td>40</td>
</tr>
<tr>
<td>21 What’s new in Zabbix 4.0.16</td>
<td>40</td>
</tr>
<tr>
<td>22 What’s new in Zabbix 4.0.17</td>
<td>41</td>
</tr>
<tr>
<td>23 What’s new in Zabbix 4.0.18</td>
<td>41</td>
</tr>
<tr>
<td>24 What’s new in Zabbix 4.0.19</td>
<td>41</td>
</tr>
<tr>
<td>25 What’s new in Zabbix 4.0.20</td>
<td>42</td>
</tr>
<tr>
<td>26 What’s new in Zabbix 4.0.21</td>
<td>42</td>
</tr>
<tr>
<td>27 What’s new in Zabbix 4.0.22</td>
<td>42</td>
</tr>
<tr>
<td>28 What’s new in Zabbix 4.0.23</td>
<td>42</td>
</tr>
<tr>
<td>29 What’s new in Zabbix 4.0.24</td>
<td>42</td>
</tr>
<tr>
<td>30 What’s new in Zabbix 4.0.25</td>
<td>43</td>
</tr>
<tr>
<td>31 What’s new in Zabbix 4.0.26</td>
<td>43</td>
</tr>
<tr>
<td>32 What’s new in Zabbix 4.0.27</td>
<td>43</td>
</tr>
<tr>
<td>33 What’s new in Zabbix 4.0.28</td>
<td>43</td>
</tr>
<tr>
<td>34 What’s new in Zabbix 4.0.29</td>
<td>43</td>
</tr>
<tr>
<td>35 What’s new in Zabbix 4.0.30</td>
<td>44</td>
</tr>
<tr>
<td>36 What’s new in Zabbix 4.0.31</td>
<td>44</td>
</tr>
<tr>
<td>37 What’s new in Zabbix 4.0.32</td>
<td>44</td>
</tr>
<tr>
<td>38 What’s new in Zabbix 4.0.33</td>
<td>44</td>
</tr>
<tr>
<td>39 What’s new in Zabbix 4.0.34</td>
<td>44</td>
</tr>
<tr>
<td>40 What’s new in Zabbix 4.0.35</td>
<td>44</td>
</tr>
<tr>
<td>41 What’s new in Zabbix 4.0.36</td>
<td>44</td>
</tr>
<tr>
<td>42 What’s new in Zabbix 4.0.37</td>
<td>44</td>
</tr>
<tr>
<td>43 What’s new in Zabbix 4.0.38</td>
<td>45</td>
</tr>
<tr>
<td>44 What’s new in Zabbix 4.0.39</td>
<td>45</td>
</tr>
</tbody>
</table>

2. Definitions

3. Zabbix processes

1 Server
1 Login and configuring user ........................ 125
2 New host .................................... 129
3 New item .................................. 130
4 New trigger .................................. 133
5 Receiving problem notification ................. 135
6 New template ................................ 139

6 Zabbix appliance ................................ 141
7. Configuration ................................. 144
   1 Hosts and host groups ..................... 149
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zabbix manpages</td>
<td>1354</td>
</tr>
<tr>
<td>zabbix_agentd</td>
<td>1354</td>
</tr>
<tr>
<td>NAME</td>
<td>1354</td>
</tr>
<tr>
<td>SYNOPSIS</td>
<td>1354</td>
</tr>
<tr>
<td>DESCRIPTION</td>
<td>1354</td>
</tr>
<tr>
<td>OPTIONS</td>
<td>1355</td>
</tr>
<tr>
<td>FILES</td>
<td>1355</td>
</tr>
<tr>
<td>SEE ALSO</td>
<td>1356</td>
</tr>
<tr>
<td>AUTHOR</td>
<td>1356</td>
</tr>
<tr>
<td>Index</td>
<td>1356</td>
</tr>
<tr>
<td>zabbix_get</td>
<td>1356</td>
</tr>
<tr>
<td>NAME</td>
<td>1356</td>
</tr>
<tr>
<td>SYNOPSIS</td>
<td>1356</td>
</tr>
<tr>
<td>DESCRIPTION</td>
<td>1356</td>
</tr>
<tr>
<td>OPTIONS</td>
<td>1356</td>
</tr>
<tr>
<td>EXAMPLES</td>
<td>1357</td>
</tr>
<tr>
<td>SEE ALSO</td>
<td>1358</td>
</tr>
<tr>
<td>AUTHOR</td>
<td>1358</td>
</tr>
<tr>
<td>Index</td>
<td>1358</td>
</tr>
<tr>
<td>zabbix_proxy</td>
<td>1358</td>
</tr>
<tr>
<td>NAME</td>
<td>1358</td>
</tr>
<tr>
<td>SYNOPSIS</td>
<td>1358</td>
</tr>
<tr>
<td>DESCRIPTION</td>
<td>1358</td>
</tr>
<tr>
<td>OPTIONS</td>
<td>1358</td>
</tr>
<tr>
<td>FILES</td>
<td>1359</td>
</tr>
<tr>
<td>SEE ALSO</td>
<td>1359</td>
</tr>
<tr>
<td>AUTHOR</td>
<td>1359</td>
</tr>
<tr>
<td>Index</td>
<td>1359</td>
</tr>
<tr>
<td>zabbix_sender</td>
<td>1360</td>
</tr>
<tr>
<td>NAME</td>
<td>1360</td>
</tr>
<tr>
<td>SYNOPSIS</td>
<td>1360</td>
</tr>
<tr>
<td>DESCRIPTION</td>
<td>1360</td>
</tr>
<tr>
<td>OPTIONS</td>
<td>1360</td>
</tr>
<tr>
<td>EXIT STATUS</td>
<td>1362</td>
</tr>
<tr>
<td>EXAMPLES</td>
<td>1362</td>
</tr>
<tr>
<td>SEE ALSO</td>
<td>1363</td>
</tr>
<tr>
<td>AUTHOR</td>
<td>1363</td>
</tr>
<tr>
<td>Index</td>
<td>1363</td>
</tr>
<tr>
<td>zabbix_server</td>
<td>1364</td>
</tr>
<tr>
<td>NAME</td>
<td>1364</td>
</tr>
<tr>
<td>SYNOPSIS</td>
<td>1364</td>
</tr>
<tr>
<td>DESCRIPTION</td>
<td>1364</td>
</tr>
<tr>
<td>OPTIONS</td>
<td>1364</td>
</tr>
<tr>
<td>FILES</td>
<td>1365</td>
</tr>
<tr>
<td>SEE ALSO</td>
<td>1365</td>
</tr>
<tr>
<td>AUTHOR</td>
<td>1365</td>
</tr>
<tr>
<td>Index</td>
<td>1365</td>
</tr>
</tbody>
</table>
Zabbix Manual

Welcome to the user manual for Zabbix software. These pages are created to help users successfully manage their monitoring tasks with Zabbix, from the simple to the more complex.

Copyright notice

Zabbix documentation is NOT distributed under a GPL license. Use of Zabbix documentation is subject to the following terms:

You may create a printed copy of this documentation solely for your own personal use. Conversion to other formats is allowed as long as the actual content is not altered or edited in any way. You shall not publish or distribute this documentation in any form or on any media, except if you distribute the documentation in a manner similar to how Zabbix disseminates it (that is, electronically for download on a Zabbix web site) or on a USB or similar medium, provided however that the documentation is disseminated together with the software on the same medium. Any other use, such as any dissemination of printed copies or use of this documentation, in whole or in part, in another publication, requires the prior written consent from an authorized representative of Zabbix. Zabbix reserves any and all rights to this documentation not expressly granted above.

1. Introduction

Please use the sidebar to access content in the Introduction section.

1 Manual structure

Structure

The content of this Zabbix 4.0 manual is divided into sections and subsections to provide easy access to particular subjects of interest.

When you navigate to respective sections, make sure that you expand section folders to reveal full content of what is included in subsections and individual pages.

Cross-linking between pages of related content is provided as much as possible to make sure that relevant information is not missed by the users.

Sections

Introduction provides general information about current Zabbix software. Reading this section should equip you with some good reasons to choose Zabbix.

Zabbix concepts explain the terminology used in Zabbix and provides details on Zabbix components.

Installation and Quickstart sections should help you to get started with Zabbix. Zabbix appliance is an alternative for getting a quick taster of what it is like to use Zabbix.

Configuration is one of the largest and more important sections in this manual. It contains loads of essential advice about how to set up Zabbix to monitor your environment, from setting up hosts to getting essential data to viewing data to configuring notifications and remote commands to be executed in case of problems.

IT services section details how to use Zabbix for a high-level overview of your monitoring environment.

Web monitoring should help you learn how to monitor the availability of web sites.

Virtual machine monitoring presents a how-to for configuring VMware environment monitoring.

Maintenance, Regular expressions, Event acknowledgment and XML export/import are further sections that reveal how to use these various aspects of Zabbix software.

Discovery contains instructions for setting up automatic discovery of network devices, active agents, file systems, network interfaces, etc.

Distributed monitoring deals with the possibilities of using Zabbix in larger and more complex environments.

Encryption helps explaining the possibilities of encrypting communications between Zabbix components.

Web interface contains information specific for using the web interface of Zabbix.

API section presents details of working with Zabbix API.

Detailed lists of technical information are included in Appendixes. This is where you will also find a FAQ section.
2 What is Zabbix

Overview

Zabbix was created by Alexei Vladishev, and currently is actively developed and supported by Zabbix SIA.

Zabbix is an enterprise-class open source distributed monitoring solution.

Zabbix is software that monitors numerous parameters of a network and the health and integrity of servers, virtual machines, applications, services, databases, websites, the cloud and more. Zabbix uses a flexible notification mechanism that allows users to configure e-mail based alerts for virtually any event. This allows a fast reaction to server problems. Zabbix offers excellent reporting and data visualization features based on the stored data. This makes Zabbix ideal for capacity planning.

Zabbix supports both polling and trapping. All Zabbix reports and statistics, as well as configuration parameters, are accessed through a web-based frontend. A web-based frontend ensures that the status of your network and the health of your servers can be assessed from any location. Properly configured, Zabbix can play an important role in monitoring IT infrastructure. This is equally true for small organizations with a few servers and for large companies with a multitude of servers.

Zabbix is free of cost. Zabbix is written and distributed under the GPL General Public License version 2. It means that its source code is freely distributed and available for the general public.

Commercial support is available and provided by Zabbix Company and its partners around the world.

Learn more about Zabbix features.

Users of Zabbix

Many organizations of different size around the world rely on Zabbix as a primary monitoring platform.

3 Zabbix features

Overview

Zabbix is a highly integrated network monitoring solution, offering a multiplicity of features in a single package.

Data gathering

• availability and performance checks
• support for SNMP (both trapping and polling), IPMI, JMX, VMware monitoring
• custom checks
• gathering desired data at custom intervals
• performed by server/proxy and by agents

Flexible threshold definitions

• you can define very flexible problem thresholds, called triggers, referencing values from the backend database

Highly configurable alerting

• sending notifications can be customized for the escalation schedule, recipient, media type
• notifications can be made meaningful and helpful using macro variables
• automatic actions include remote commands

Real-time graphing

• monitored items are immediately graphed using the built-in graphing functionality

Web monitoring capabilities

• Zabbix can follow a path of simulated mouse clicks on a web site and check for functionality and response time

Extensive visualization options

• ability to create custom graphs that can combine multiple items into a single view
• network maps
• custom screens and slide shows for a dashboard-style overview
• reports
• high-level (business) view of monitored resources

Historical data storage
• data stored in a database
• configurable history
• built-in housekeeping procedure

**Easy configuration**
• add monitored devices as hosts
• hosts are picked up for monitoring, once in the database
• apply templates to monitored devices

**Use of templates**
• grouping checks in templates
• templates can inherit other templates

**Network discovery**
• automatic discovery of network devices
• agent auto registration
• discovery of file systems, network interfaces and SNMP OIDs

**Fast web interface**
• a web-based frontend in PHP
• accessible from anywhere
• you can click your way through
• audit log

**Zabbix API**
• Zabbix API provides programmable interface to Zabbix for mass manipulations, 3rd party software integration and other purposes.

**Permissions system**
• secure user authentication
• certain users can be limited to certain views

**Full featured and easily extensible agent**
• deployed on monitoring targets
• can be deployed on both Linux and Windows

**Binary daemons**
• written in C, for performance and small memory footprint
• easily portable

**Ready for complex environments**
• remote monitoring made easy by using a Zabbix proxy

4 Zabbix overview

Architecture
Zabbix consists of several major software components. Their responsibilities are outlined below.

**Server**
Zabbix server is the central component to which agents report availability and integrity information and statistics. The server is the central repository in which all configuration, statistical and operational data are stored.

**Database storage**
All configuration information as well as the data gathered by Zabbix is stored in a database.

**Web interface**
For an easy access to Zabbix from anywhere and from any platform, the web-based interface is provided. The interface is part of Zabbix server, and usually (but not necessarily) runs on the same physical machine as the one running the server.

**Proxy**
**Zabbix proxy** can collect performance and availability data on behalf of Zabbix server. A proxy is an optional part of Zabbix deployment; however, it may be very beneficial to distribute the load of a single Zabbix server.

**Agent**

**Zabbix agents** are deployed on monitoring targets to actively monitor local resources and applications and report the gathered data to Zabbix server.

**Data flow**

In addition it is important to take a step back and have a look at the overall data flow within Zabbix. In order to create an item that gathers data you must first create a host. Moving to the other end of the Zabbix spectrum you must first have an item to create a trigger. You must have a trigger to create an action. Thus if you want to receive an alert that your CPU load is too high on Server X you must first create a host entry for Server X followed by an item for monitoring its CPU, then a trigger which activates if the CPU is too high, followed by an action which sends you an email. While that may seem like a lot of steps, with the use of templating it really isn’t. However, due to this design it is possible to create a very flexible setup.

### 5 What’s new in Zabbix 4.0.0

**Improved dashboards**  Dashboard have seen further improvements in the new version to make them more appealing visually, more versatile and flexible to the user needs.

To achieve the new look and functionality, the following developments have been made:

- A new more versatile SVG-based **graph widget** has been added, while the classic design graph widget is also still available
- Widgets no longer contain a footer displaying widget details (e.g. the Updated: hh:mm:ss message about the time they were updated), achieving a much cleaner look of the dashboards. Note that:
  - In the Problems widget the message “N of M problems are shown” will still be displayed if there are more problems than can be displayed according to the Show lines setting
  - Digital clock will no longer be displayed in the Clock widget footer
- In the new **Kiosk** mode, widgets only can be displayed with no headers at all
- A new Global view dashboard is now shipped with the default Zabbix dataset, replacing the main Dashboard of the previous version
- Another default dashboard has been added that focuses on displaying Zabbix server performance: **Zabbix server health**
This dashboard is shared with the Zabbix administrators group only, by default.

**Retrieve metrics immediately**  Retrieving a new value for an item (metric) in Zabbix has always been cyclic and based on configured update intervals. While for many items the update intervals are quite short, there are others (including low-level discovery rules) for which the update intervals are quite long, so in real life situations there may be a need to retrieve a new value quicker - to pick up changes in discoverable resources, for example.

This is now made possible in the new Zabbix version by means of a Check now button that is available in two locations:

- **Configuration form** of an existing item or discovery rule.
- **List of items or discovery rules**: select the required entities and click on Check now.

**Attention:**

When checking for a new value, the configuration cache is not updated, thus the values will not reflect very recent changes to item/discovery rule configuration. Therefore, it is also not possible to check for a new value for an item/rule that has been created just now.
New HTTP item type  A new HTTP item type has been introduced allowing data polling using the HTTP/HTTPS protocol. Trapping is also possible using Zabbix sender or Zabbix sender protocol.

For more details see **HTTP agent** item type.

**New templates**  New templates are available for monitoring some IBM, Dell, HP, Cisco UCS and Supermicro Aten hardware:

- Template Server IBM IMM SNMPv1/2
- Template Server Dell iDRAC SNMPv2
- Template Server HP iLO SNMPv2
- Template Server Supermicro Aten SNMPv2
- Template Server Cisco UCS SNMPv2

These templates are part of the default Zabbix dataset for new installations. If you are upgrading from previous versions, you can download the latest templates from the Zabbix Git repository. Then, while in Configuration → Templates you can import them manually into Zabbix. If templates with the same names already exist, the Delete missing options should be checked when importing to achieve a clean import. This way the old items that are no longer in the updated template will be removed (note that it will mean losing history of these old items).

**Item prototypes can depend on regular items**  Zabbix 3.4 introduced dependent items (and dependent item prototypes) that can extract data from the bulk metrics gathered by a master item. Previously, however, item prototypes could only depend on another item prototype from the same low-level discovery rule. This limitation has now been lifted. An item prototype can depend on either another prototype or a regular item from the same host.
When selecting the master item for the prototype there are now two buttons in the frontend - one for selecting a regular master item and another for selecting a prototype master item.

**Low-level discovery macros in item preprocessing**  
Low-level discovery macros now can be used in item preprocessing steps for item prototypes.

User macros and user macros with context can be used in item preprocessing steps for regular items and item prototypes.

**Substring extraction of low-level discovery macro value**  
Macro functions are now supported with low-level discovery macros, allowing to extract a certain part of the macro value using a regular expression.

For example, you may want to extract the customer name and interface number from the following LLD macro for the purposes of event tagging:

```
{#IFALIAS}=customername_1
```

To do so, the `regsub` macro function can be used with the macro in the event tag value field of a trigger prototype:

```
Tags

Customer

{{#IFALIAS}.regsub(".*_([0-9]+)", \1)}

Interface

{{#IFALIAS}.regsub(".*_([0-9]+)", \2)}
```

For more information on macro function syntax, see: [Macro functions](#).

Macro functions are supported in all locations where low-level discovery macros can be used, except for low-level discovery rule filter.

**Host maintenance on trigger level**  
Host maintenance now can be limited to the triggers/services with the corresponding tags:
Required tags can be specified when configuring maintenance periods. If specified, host maintenance will be activated and notifications will be suppressed only for triggers/problems with the corresponding tags, while for all other triggers of the specified hosts problem reporting in the frontend and problem notifications will remain active.

Related changes

With host maintenance flexibility extended to trigger/service level, some maintenance-related options have been renamed or added:

<table>
<thead>
<tr>
<th>New naming</th>
<th>Old naming</th>
<th>Affected location</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show suppressed problems</td>
<td>Show hosts in maintenance</td>
<td>Filter option in Monitoring → Problems</td>
<td>Display problems which would otherwise be suppressed (not shown) because of host maintenance.</td>
</tr>
<tr>
<td>Pause operations for</td>
<td>Pause operations while in</td>
<td>Configuration option in action</td>
<td>Delay execution of operations until host maintenance ends.</td>
</tr>
<tr>
<td>suppressed problems</td>
<td>maintenance</td>
<td>operations</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>New naming</td>
<td>Old naming</td>
<td>Affected location</td>
<td>Function</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------</td>
<td>----------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Problem is suppressed</td>
<td>Maintenance status</td>
<td>Action condition</td>
<td>Yes - execute action if problem is suppressed</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>No - do not execute action if problem is</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>suppressed</td>
</tr>
</tbody>
</table>

**Single sign-on using webserver**  
Single sign-on to the frontend using solutions like Kerberos, NTLM and others has been made possible by adding new HTTP authentication options.

HTTP authentication has now gained a dedicated tab in the Authentication form in which you may define whether to send non-authenticated users to the Zabbix login page or to the HTTP login page, specify case-sensitive/case-insensitive login and remove the domain name from the sent user credentials.

![Authentication form with HTTP settings](image)

Case-sensitive/case-insensitive login option has also been added to LDAP authentication details.

See also: Authentication

In a related development, an LDAP frontend access option has been added for user group configuration.

**More flexible active agent auto-registration**  
Previously auto-registration was run only once, which did not offer much flexibility for cases when something on the host is changed. In the new version, auto-registration is rerun if host metadata (HostMetadata, HostMetadataItem parameters in agent configuration) is changed.

This allows to adapt monitoring based on the nature of changes on the host. To make such a more flexible approach work, auto-registration actions now support additional operations:

- remove host
- enable host
- remove from host group
- unlink from template

**MySQL 8.0 supported**  
Support for MySQL 8.0 has been added.

**Date-based indices setup for Elasticsearch**  
In order to properly scale history data in Elasticsearch, multiple indices per data type are required. It is now possible to set up such date-based indices. For more details, see Elasticsearch setup.

**More secure connections for proxies**  
It is now possible to configure connections for both active and passive proxies in a more secure way:

- The allowed address range for an active proxy can be limited. When configuring an active proxy in the frontend, there is a new field called Proxy address. If specified then active proxy requests will only be accepted from this list of IP addresses/DNS names of the active proxy.
The Server parameter in passive proxy configuration, which previously was ignored, is now mandatory. The passive proxy will reject an address that is not listed in the Server parameter.

**Problem severity can be changed** Problem severity previously always depended on the severity of the underlying trigger and could not be changed. Now problem severity in the event table is a separate field and can be updated. Even though the original value is based on the trigger severity, it can be updated using the problem update screen.

**Working with problems** Problem update screen

The problem update screen is a reworked version of the acknowledgment screen of the previous Zabbix versions.

Besides renaming, the following changes have been made:

- Problem severity can now be changed on the event level
- Each problem update action can be done separately:
  - You may leave a comment on the problem without acknowledging
  - You may acknowledge a problem without commenting
  - You may manually close a problem without acknowledging, commenting, etc.
- You may define the scope for each of the actions that follow: Change severity, Acknowledge, Close problem.
- The history list contains more symbolic information on the activities so far

Other changes
• The problem severity displayed is now event-level severity and will change if updated in the following locations:
  - Monitoring → Problems (and the corresponding dashboard widgets and screen elements)
  - Monitoring → Overview (and the corresponding dashboard widgets and screen elements)
  - Host group issues and Host issues screen elements
• The content of what is displayed in the Actions column of Monitoring → Problems has been expanded. Previously it only had textual information about the course of actions. Now all information is symbolic (icons) and, besides actions, also displays information on such activities as commenting and changing problem severity. When you roll the mouse over the icons, popups are displayed with more details about each activity.
• Previously in event details there were separate blocks for acknowledgments, message and remote command actions. Now all activities on the problem are displayed in one block and symbolic icons are used for each stage of the problem life cycle, including entries for problem generation and resolution times.
• Acknowledgment operations in actions have been renamed to Update operations
• Event acknowledgment is now always enabled (the on/off checkbox in Administration → General (GUI option in dropdown) has been removed)
• Macros have been updated:
  - {ACK.DATE} renamed to {EVENT.UPDATE.DATE}
  - {ACK.TIME} renamed to {EVENT.UPDATE.TIME}
  - {ACK.MESSAGE} renamed to {EVENT.UPDATE.MESSAGE}
  - {EVENT.ACK.HISTORY} renamed to {EVENT.UPDATE.HISTORY}
  - {EVENT.UPDATE.ACTION} added
  - {EVENT.SEVERITY} added
  - {EVENT.NSEVERITY} added
• Default messages for operations, recovery operations and update operations have been changed to reflect the updated macros

New graph widget A new graph widget for the dashboards has been introduced providing a more modern and versatile way of visualizing data collected by Zabbix. The new widget uses vector technique to draw the image and serves as a platform for multiple new visualization features that were not available using the existing image drawing approach.

![New graph widget](image)

For more information see dashboard widgets.

The graph widget supported before can still be used and is now renamed to Graph (classic).

Time selector redesign The time period selector has been redesigned with the aim of providing users a one-click opportunity to select often required periods.
It is also possible to zoom out the selected period (increase it two times or by 50% in both directions), to move the period back and forth, and select a more specific date from the date picker.

The following locations benefit from the redesign:

- Monitoring → Dashboard (graph widget)
- Monitoring → Problems (with History selected in the filter)
- Monitoring → Web (in scenario details)
- Monitoring → Latest data (item graph, item history, ad-hoc graph, templated screens)
- Monitoring → Graphs
- Monitoring → Screens
- Monitoring → Screens (slideshows)
- Reports → Availability report
- Reports → Triggers top 100
- Reports → Audit
- Reports → Action log

See also: Time period selector

**Kiosk mode for frontend pages** In the new Kiosk mode for frontend pages only the page content is displayed. Thus, for example, in dashboards only the widgets are displayed.

Kiosk mode is accessible by clicking on the button when already in fullscreen mode. Kiosk mode is supported for all pages where fullscreen mode is supported.

**Compact view of problems** A Compact view mode has been added in Monitoring → Problems allowing to maximize the amount of problems that can be seen at the same time:
To activate the compact view mode, select the respective option in the filter.

Two more new options are available in the problem filter:

- Highlight whole row allows to highlight the full row of unresolved problems using the problem severity color. This option is available in the standard blue and dark themes; it is not available in the high-contrast themes.
- Show timeline allows to display/hide the visual timeline. This checkbox has also been added to the Problems dashboard widget configuration. Note that this option is not available when Compact view is selected.

**Monitoring → Triggers removed** With Monitoring → Problems becoming the go-to section when needing to see the current problems, it has been decided to remove the Triggers section from the Monitoring menu.

Note that trigger status as such can now be viewed in Configuration → Hosts → Triggers (in the new Value column), while trigger descriptions can be accessed from the Trigger context menu and are opened in a popup window.

**Inventory macro support in event tags** `{INVENTORY*}` macros are now supported in event tags used for trigger-based event correlation.

Expansion of inventory macros in event tags allows to correlate events (i.e. problems and their resolution), for example, by data-center location, responsible system administrator, rack number and any other inventory item provided, thus giving administrators even more automation possibilities.

**Preventing unit conversion flexibly** Specifying a unit for an item in Zabbix results in a multiplier prefix being added - for example, an incoming value ‘2048’ with unit ‘B’ would be displayed as ‘2KB’. The unit blacklist for which such conversion was prevented in previous Zabbix versions was hardcoded and consisted of ms, rpm, RPM, %.

In the new version, any unit can be prevented from being converted by using a `!` prefix, for example `!B`. To better illustrate how this conversion works with and without the blacklisting, see the following examples of values and units:

```
1024 !B → 1024 B
1024 B → 1 KB
61 !s → 61 s
61 s → 1m 1s
0 !uptime → 0 uptime
```
Even though the previous unit blacklist also still works, it is now deprecated, so the correct way to prevent conversion for these units is now !ms, !rpm, !RPM, !%.

**Multiple emails in one user media**  Multiple e-mail addresses can now be specified in one user media entry.

If multiple e-mail addresses are specified this way, one e-mail will be sent to all the specified recipients.

**Real-time export of events, values, trends**  Real-time export of trigger events, item values and trends in a newline-delimited JSON format is possible by specifying the new ExportDir parameter in server configuration. Another new parameter - ExportFileSize may be used to determine the maximum size of an individual export file.

See also: Real-time export of events, values, trends

**Tag-based permissions**  User groups form has been completed with a new Tag filter tab that allows to set tag-based permissions for user groups to see problems filtered by tag name and its value:

This change applies to the “User groups” form in Administration → User groups.

**Compression for server-proxy communication**  All communications between Zabbix server and all proxies, and vice versa are now unconditionally compressed. Compression lowers the bandwidth requirements and improves data transfer speed.

The Administration → Proxies form is extended with an additional column named “Compression”.

---

0 uptime → 00:00:00
0 !! → 0 !
0 ! → 0
Zlib library is required for compression support.

**Improved database down messages**  Database down messages have been improved to provide more details about the occurred problem. Database down message from now on consists of the following content:

[MySQL|PostgreSQL|Oracle|IBM DB2] database <DB Name> [on <DB Host>:<DB Port>] is not available: <error message depending on the type of DBMS (database)>

<DB Host> is not added to the message if it is defined as an empty value and <DB Port> is not added if it is the default value ("0").

**Use of "not" keyword**  Use of "not" keyword in Custom expression field and in a Discovery rule filter drop down is now supported.

This change applies to the Event correlation rules form in Configuration → Event correlation, Actions form in Configuration → Actions and Discovery rule filter.

**Items**  New items

- **vfs.dir.count** agent item has been added to recursively count all entries in the given directory.

Updated items

- **vm.memory.size** agent item now supports a slab parameter.
- The following agent items now support new mode values:
  - **net.if.total** - overruns (fifo) and compressed
  - **net.if.in** - overruns (fifo), frame, compressed and multicast
  - **net.if.out** - overruns (fifo)/, collisions (colls), carrier and compressed
- For **logrt** and **logrt.count** items, a copytruncate log file rotation option has been added.
- The following values are now supported in Boolean to decimal transformation for **Item value preprocessing** : ok, master, err, slave.
- **zabbix[rcache,<cache>,<mode>]** and **zabbix[wcache,<cache>,<mode>]** internal items now support a pused mode, returning the use percentage of the respective buffer.

JMX monitoring
Zabbix Java gateway now supports working with custom MBeans returning non-primitive data types, which override the `toString()` method.

External script argument wrapping

When running an external script, the script arguments are now wrapped in single quotes `' instead of double quotes `"`. This change allows Zabbix to pass more characters in external check parameters, for example, the `$` sign.

Searching IPMI sensor by full name

In the IPMI sensor field for IPMI items it is now also possible to specify a search for the full name, by using a `name:` prefix before the value.

**Triggers**  Time triggers processed by history syncers

The processing of time-based trigger functions such as `nodata()`, `date()`, `dayofmonth()`, `dayofweek()`, `time()` and `now()` has been moved from timer processes to history syncers.

While previously all time-based triggers were recalculated at the same time, creating peak loads every 30 seconds, now the time-based trigger processing is evenly spread within those 30 seconds.

The output of history syncer and timer processes has been updated accordingly.

Now:

```
zabbix_server: history syncer #3 [processed 0 values, 0 triggers in 0.000005 sec, idle 1 sec]
zabbix_server: timer #1 [updated 0 hosts, suppressed 0 events in 0.000472 sec, idle 59 sec]
```

Before:

```
zabbix_server: history syncer #4 [synced 35 items in 0.166198 sec, idle 5 sec]
zabbix_server: timer #1 [processed 3 triggers, 0 events in 0.007867 sec, 0 maint.periods in 0.005677 sec, idle 30 sec]
```

**Miscellaneous**

- Regular expressions and global regular expressions are now supported in the parameter values of the `logsource` trigger function.

**Frontend**  Mandatory fields marked

Mandatory fields in all Zabbix frontend forms are now marked with a red asterisk.

Keyboard navigation

- All interactive elements (except maps) can now be accessed by pressing the Tab key;
- Popups can now be opened, worked with and closed by keyboard;
- Context menu options can now be navigated by keyboard arrows. Pressing Esc will close the whole context menu, while pressing Enter will activate the selected option.
- Year, month and date can be selected by keyboard in the redesigned date picker.

Date picker redesign

The date picker has been redesigned to allow selecting year, month and date by keyboard.
It is possible to navigate between the blocks of year/month/date using Tab and Shift+Tab. Keyboard arrows or arrow buttons allow to select the desired value. Pressing Enter (or clicking on the desired value) activates the choice.

Selecting time has been removed from the date picker as that is part of the redesigned time selector. The Done button is also removed, because the selected date is now activated immediately. The Now button has also been removed.

Color picker redesign

The color picker has been redesigned and offers a larger palette of colors to pick from:
Popup windows replaced by overlay dialogs

All popups that were opened in new windows are now opened as overlay dialogs across the frontend.
Additionally, a Cancel button has been added to these windows.

Filtering

More flexible problem filtering by tags

More flexibility has been added to problem filtering by event tag name and value:
• Calculation types for tag filter conditions have been added - And/Or and Or
• In tag filtering exact (case-sensitive) and similar (case-insensitive) string match is possible
• The number of displayed tags can be selected - from completely hiding the Tags column to the maximum of three tags (in the new Show tags field)
• The mode of displaying tags can be selected - by full name, shortened name or value name only (in the new Tag name field)
• The order in which tags are displayed with the problem can be defined, as a comma-separated list (in the new Tag display priority field)

These changes apply to the filter in Monitoring → Problems and to the Problems dashboard widget.

Similar changes are made to the filter in Configuration → Hosts → Triggers excluding Show tags, Tag name and Tag display priority fields.

Host list

You can now filter hosts depending on whether they are monitored by Zabbix server or Zabbix proxy. If filtering by proxy, it is also possible to specify the proxy or proxies.

By default Any is selected and the auto-complete field Proxy is not visible. When selecting Proxy, a new auto-complete field with Proxy label becomes visible in the filter.

Item list

You can now filter items depending on whether they are:

• Regular items - created manually or from a template
• Discovered items - created by low-level discovery
Trigger value shown in trigger configuration list

Trigger value (OK/Problem) is now displayed in the trigger configuration list, in the new Value column:

Renamed operators

Condition operators have been renamed and unified everywhere in the frontend:

<table>
<thead>
<tr>
<th>New</th>
<th>Old</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equals</td>
<td>=, Equal, Exactly</td>
</tr>
<tr>
<td>Does not equal</td>
<td>&lt;&gt;</td>
</tr>
<tr>
<td>Is greater than or equals</td>
<td>&gt;=</td>
</tr>
<tr>
<td>Is less than or equals</td>
<td>&lt;=</td>
</tr>
<tr>
<td>Contains</td>
<td>Like</td>
</tr>
<tr>
<td>Does not contain</td>
<td>Not like</td>
</tr>
</tbody>
</table>

Renamed widgets, screen elements and reports

The following elements have been renamed:
Multiple item support in plain text widget

It is now possible to add multiple items during Plain text widget configuration:

![Edit widget](image)

* Items location option has also been added to choose the way how information in the widget may be displayed:

| < | | < | | < |

Event status color adjustment

![Trigger displaying options](image)
A new Use custom event status colors option has been added in Administration → General → Trigger displaying options. This option allows to turn on the customization of colors for acknowledged/unacknowledged problems.

Changes in “Host mass update” form

New checkbox Remove host groups and auto-complete field added. From now users are able to remove specific host groups from hosts. In case hosts are already in selected groups, then hosts will be removed from these groups. In case hosts are not in selected groups, nothing will added or removed. In case same host groups are replaced and removed at the same time, hosts are actually left without groups.

Changes in “User media” form

Trigger severity active blocks are now styled in severity colors while inactive blocks have the same color as table background color.

This change applies to the “Media” tab in Administration → Users → User properties form and User profile configuration form.

Twin boxes replaced with auto-select

|<| |<| ![|]|

From now some of the forms are much more user-friendly and compact. Twin box controls are now removed and replaced with auto-select.

This change applies to the following configuration forms:

- Configuration → Hosts → Create/Edit host and Configuration;
- Configuration → Host groups → Create/Edit host group;
- Configuration → Maintenance → Create/Edit maintenance period → Hosts & Groups tab;
- Configuration → Templates → Create/Edit template;
- Administration → User groups → //Create/Edit user group //;
- Administration → Proxies → Create/Edit proxy.

Improved widget configuration

When adding a new widget to a dashboard or editing an existing one, change of widget type opens a form with default values set for all fields depending on the type of newly selected widget.

Graph visual improvements in a widget
Graph display in widgets has been enhanced. A generated graph is now occupying the maximum possible space allowing more information to be displayed.

Frontend top bar menu improvements

A new Support button redirecting to Zabbix official support page is now added to Zabbix frontend top bar menu:

Accessibility

Several improvements have been made to Zabbix frontend in order to make it usable with assistive technologies and generally more friendly for visually-impaired people.

High-contrast themes

Two new high-contrast themes have been added for Zabbix frontend:

- High-contrast light
- High-contrast dark

Within this development, default colors for graphs in the dark themes have also been updated:

- When creating a new graph in the dark theme, there will be a higher contrast of colors for items added to the graph (already created graphs are not affected).
- When viewing simple graphs in the dark theme, colors for items will be in higher contrast.

Screen reader-friendly features

- Top-level navigation and user-level content is now readable by screenreader.
- The dashboard and all widgets in view mode (except for the map navigation tree) are now readable by screenreader.
- It is now possible to view graph values as text in a table so that it can be read with a screen reader. This functionality is implemented for custom graphs and ad-hoc graphs.

Readable summary in maps

A hidden “aria-label” property has been added to maps allowing map information to be read with a screen reader. Both general map description and individual element description is available, in the following format:

- for map description: <Map name>, <* of * items in problem state>, <* problems in total>.
- for describing one element with one problem: <Element type>, Status <Element status>, <Element name>, <Problem description>.
- for describing one element with multiple problems: <Element type>, Status <Element status>, <Element name>, <* problems>.
• for describing one element without problems: `<Element type>`, Status `<Element status>`, `<Element name>`.

For example, this description is available:

`Local network, 1 of 6 elements in problem state, 1 problem in total. Host, Status problem, My host, Free disk space is ... servers. Host, Status ok, Server 1. Host, Status ok, Server 2. Host, Status ok, Server 3. Host, Status ok, Server 4. ` for the following map:

![Map of network elements](image)

Icons for notification type

Corresponding icons and colouring have been added at the beginning of frontend notifications to indicate whether the message is about success, failure or warning.

<p>| | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>

These changes allow the actual message to be on a white background, improving overall readability.

Green background removed

Green background has been removed:

• for resolved problems in the severity column in Monitoring → Problems/Triggers and the corresponding dashboard widget

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>

• for devices that are up in Monitoring → Discovery

Discovery status details

Discovery status details in Monitoring → Discovery are now displayed as text inside the cell, instead of a pop-up that’s visible upon mouse over.

---

In Zabbix 4.0.0

Before Zabbix 4.0.0
In addition, green colouring is removed from cells with uptime, while red remains in the cells with downtime.

Configurable session cookie name

The session cookie name that Zabbix frontend uses for internal authentication is now configurable in ZBX_SESSION_NAME of the frontend definitions.

Host column always displayed

The host column is now always displayed even if only one host is selected in:

- Monitoring → Latest data
- Monitoring → Web
- Reports → Availability

The benefits of this change are:

- The host menu in the latest data page is now always available with links to useful options
- It is clear which host is displayed when using a screenreader

Miscellaneous

- The allowed character limit has been raised from 63 to 255 ASCII characters for fields containing DNS names. The affected forms are host configuration and passive proxy configuration.
- When importing maps (Monitoring → Maps → Import button) the Create new option for importing images is now checked by default:
Macros

- \{ITEM.VALUE\}, \{ITEM.LASTVALUE\} are now supported in the URL field of trigger configuration.

Daemons Validity to avoid proxy/agent data duplication

Session tokens have been added to incoming proxy/agent data along with virtual IDs that are assigned to incoming values. The value ID is a simple ascending counter, unique within one data session (identified by the session token). This ID is used to discard duplicate values that might be sent in poor connectivity environments. For more details on the protocols, see:

- Server-proxy data exchange protocol
- Active agent checks

Data without session token will be accepted without validation for duplicate values, ensuring backwards compatibility.

Miscellaneous

- Command line arguments that exceed 2KB are now supported in proc.num and proc.mem checks on AIX platform.

Performance Server performance

Zabbix server performance has been improved by replacing semaphores with pthread mutexes and read-write locks.

Problem name generation

Problem and event names previously were generated on the fly in the frontend and on server side based on the respective trigger name with all the macros expanded. That lead to severe performance issues and also made it impossible to see historical information about problems if the trigger name had changed.

Now problem and event names are stored directly in the ‘events’ and ‘problem’ tables at the moment when an event is generated for a problem or recovery. Zabbix frontend can search and query the respective tables directly. This change leads to a better separation of triggers and problems, improves performance, especially that of the frontend and maintains historical problem names. However, the size of problem/events tables is now larger.

Note that for internal events the name contains an error message why an object changed its state; upon recovery no name is used. For discovery and auto-registration events no name is used.

A new \{EVENT.NAME\} macro is supported, returning the event/problem name with macros resolved.

See also the upgrade notes for:

- Related macro changes
- Related API method changes

Logging

- Zabbix Java gateway logs are now easier to read, as exception stack trace is no longer available in error and warning level messages.

API improvements From now on user.checkAuthentication method contains additional parameter “extend”.

See also

- Template changes
6 What’s new in Zabbix 4.0.1

URL parameters for fullscreen/kiosk modes

Fullscreen and kiosk modes in supported frontend pages can now be activated using URL parameters. For example, in dashboards:

- `/zabbix.php?action=dashboard.view&fullscreen=1` - activate fullscreen mode
- `/zabbix.php?action=dashboard.view&kiosk=1` - activate kiosk mode
- `/zabbix.php?action=dashboard.view&fullscreen=0` - activate normal mode

Filtering

Host filtering based on linked templates

Hosts can now be filtered based on the template that they are linked to. Multiple templates can be specified.

This functionality may be useful to filter hosts and then mass update their properties (including the template linkage).

Template filtering based on linked templates

Templates can now be filtered based on the templates that are directly linked to it. Multiple directly linked templates can be specified.

Item improvements

The following items that were previously supported only on AIX LPAR of type “Shared”, now are also supported on “Dedicated”:

- `system.stat[cpu,ec]` (with “Dedicated” always returns 100 (percent))
- `system.stat[cpu,pc]`
- `system.stat[ent]`

See `system.stat[]` in agent items for more details.

Daemon improvements

- Support of OpenSSL 1.1.1 has been added.
7 What's new in Zabbix 4.0.2

License update for linking with OpenSSL

Exception has been added to the license giving permission that the code of Zabbix is linked with the OpenSSL project OpenSSL library (see README file in Zabbix source code).

Daemon improvements

- Daemons and commandline utilities when showing version information (with `-V` option) now also display the crypto library version.

Frontend improvements

- Cookie names and values are now properly URI-encoded.
- HTTP agent items are now also listed in Administration → Queue.
- Radio buttons now immediately display the correct color when in focus and clicked on.

Previously they would first turn dark blue, before displaying the correct color when out of focus.

Macros

- Host macros: `{HOST.HOST}`, `{HOST.NAME}`, `{HOST.IP}`, `{HOST.DNS}`, `{HOST.CONN}` are now supported in trapper/HTTP agent item “Allowed hosts” field in the frontend (also "trapper_hosts" property in API).

See also

- Template changes

8 What's new in Zabbix 4.0.3

Displaying latest values of problem triggers

Latest values of items in trigger expressions that caused a problem can now be seen in Monitoring → Problems and in the Problems and Problems by severity dashboard widgets if configured.

In Monitoring → Problems, latest item values are an additional column if the Show latest values checkbox is marked in the filter.

In the Problems dashboard widget, latest item values are an additional column if the Show latest values checkbox is marked in the widget configuration.

In the Problems by severity dashboard widget, latest value column is added in the problem detail popup if the Show latest values checkbox is marked in the widget configuration.

Frontend improvements

- If the Check now request is performed from the item list for items that do not support it (template items, active agent items, etc.), a corresponding error message is now displayed. Previously it would display a ‘Request sent successfully’ message even though the functionality would not work for these items.

Item changes

* `''vmware.hv.discovery''` item for VMware hypervisor discovery now returns two [[:manual:vm_monitoring/discovery|d...}
9 What's new in Zabbix 4.0.4

Items
A new regex_excl_dir parameter has been added to vfs.dir.count[] and vfs.dir.size[] agent items allowing to exclude the whole content of a subdirectory from the results.

Graphs
Previously, two data points were needed for a line/staircase graph to draw a line in an SVG graph. Now, if there's only one data point it is drawn as point regardless of draw type. The point size is calculated from line width, but it cannot be smaller than 3 pixels, even if line width is less.

LDAP authentication with anonymous bind
Anonymous bind is now supported in LDAP authentication.

10 What's new in Zabbix 4.0.5

Remote monitoring of Zabbix stats
It is now possible to make some internal metrics of Zabbix server and proxy accessible remotely by another Zabbix instance or a third party tool. This can be useful so that supporters/service providers can monitor their client Zabbix servers/proxies remotely or, in organizations where Zabbix is not the main monitoring tool, that Zabbix internal metrics can be monitored by a third party system in an umbrella-monitoring setup.

Zabbix internal stats are exposed to a configurable set of addresses listed in the new ‘StatsAllowedIP’ server/proxy parameter. Requests will be accepted only from these addresses.

To configure querying of internal stats on another Zabbix instance, you may use two new items:

- `zabbix[stats,<ip>,<port>]` internal item - for direct remote queries of Zabbix server/proxy. <ip> and <port> are used to identify the target instance.
- `zabbix.stats[<ip>,<port>]` agent item - for agent-based remote queries of Zabbix server/proxy. <ip> and <port> are used to identify the target instance.

To make sure that the target instance allows querying it by the external instance, list the address of the external instance in the ‘StatsAllowedIP’ parameter on the target instance.

These items gather statistics in bulk and return a JSON which can be used as the master item for dependent items that get their data from. A selected set of internal metrics (i.e. not all) is returned by either of these two items.

There are also another two new items allowing to specifically remotely query internal queue stats:

- `zabbix[stats,<ip>,<port>,queue,<from>,<to>]` internal item - for direct internal queue queries to remote Zabbix server/proxy
- `zabbix.stats[<ip>,<port>,queue,<from>,<to>]` agent item - for agent-based internal queue queries to remote Zabbix server/proxy

For more details, see:

- Remote monitoring of Zabbix stats
- Internal items
- Zabbix agent items

New templates
New templates are also available for remote Zabbix server or proxy internal metric monitoring:

- Template App Remote Zabbix server
- Template App Remote Zabbix proxy

Note that in order to use a template for remote monitoring of multiple external instances, a separate host is required for each external instance monitoring.
**11 What’s new in Zabbix 4.0.6**

Windows MSI agent packages

Windows MSI installer packages for Zabbix Windows agent are available for download.

Date and time on hover in graph widget

Date and time is now also displayed, in addition to displaying item values, when hovering over a point in time in the graph widget. Note that this is the date and time of the point in graph, not of the actual values. However, this change still allows to know more precisely when something (e.g. a peak) happened:

![Graph with date and time](image)

Item changes

- A ‘mode’ parameter has been added to the `vmware.eventlog[]` item key, used in monitoring VMware environments, allowing to optionally specify skipping of older log data. See also: [Template changes](#).
- Support of IPv6 addresses has been added to the first parameter of the `net.dns[]` Zabbix agent item.

Frontend changes

- The Info column is now also displayed in the item list for template items. Previously it was only displayed in the host item list.
- The Trigger menu is now also accessible by clicking on the trigger information in the event detail page:
12 What's new in Zabbix 4.0.7

Frontend

Global search

The global search field in the top-right corner has been improved. Starting to type in it will show all hosts with matching strings in any part of the name, not only in the beginning of the name as before.

![Global search example](image)

The global search field can now also match the technical name to the visible name of the host. In this case the matching visible name is listed as an option, but not highlighted:

![Global search example](image)

Discovery rule filtering

A filter has been added for discovery rule filtering in Monitoring → Discovery. The filter replaces the dropdown from previous Zabbix versions. If you start typing the name in the filter, all matching enabled discovery rules will be listed for selection.

![Discovery rule filter example](image)

More than one discovery rule can be selected now.
Copying items, triggers, graphs

The form for item/trigger/graph copying to other targets has been changed:

- The Target type field is now a radio button type, instead of a dropdown;
- The Target field allows to multiselect, rather than displaying all possible targets in what could be an endless list. Starting to type in the Target field will show all available corresponding targets.

13 What's new in Zabbix 4.0.8

Custom headers in web scenarios/HTTP checks

The length of custom header value fields has been increased from 255 to 1000 characters.

Frontend

Human readable time in Plain text widget

When displaying time in the Plain text dashboard widget, it is now displayed in a human readable form.

Daemons

Warnings about incompatible versions

Warnings are now being logged if incompatible Zabbix daemon versions are used.

Windows agent compilation revision

Generating a Windows file properties revision number has been added for agent compilation on MS Windows. It follows a \{b\}\{t\}\{nn\} format where:

- \{b\} - source (1 - feature or release, 2 - tag)
- \{t\} - type (1 - alpha, 2 - beta, 3 - release candidate, 4 - release)
- \{nn\} - sequence number for the ‘type’

For example:

<table>
<thead>
<tr>
<th>Tag</th>
<th>Branch</th>
<th>Version</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.8</td>
<td>Zabbix 4.0.8</td>
<td>4.0.8.2400</td>
<td></td>
</tr>
<tr>
<td></td>
<td>release/4.0</td>
<td>Zabbix 4.0.8rc3</td>
<td>4.0.8.1303</td>
</tr>
<tr>
<td></td>
<td>feature/ZBX-16074</td>
<td>Zabbix 4.0.8rc1</td>
<td>4.0.8.1301</td>
</tr>
</tbody>
</table>

14 What’s new in Zabbix 4.0.9

This minor version does not have any functional changes.

15 What's new in Zabbix 4.0.10

VMware datastore discovery

VMware datastore discovery has been moved from hypervisor level to vCenter level. As a result datastores are discovered and datastore info is collected only once for each datastore instead of one time per each hypervisor.
Within this development the following new items have been added:

- vmware.datastore.discovery[<url>]
- vmware.datastore.hv.list[<url>,<datastore>]
- vmware.datastore.read[<url>,<datastore>,<mode>]
- vmware.datastore.write[<url>,<datastore>,<mode>]
- vmware.datastore.size[<url>,<datastore>,<mode>]
- vmware.hv.datastore.list[<url>,<uuid>]

For more information on the added items, see: [VMware monitoring item keys](#)

**Item changes**

**web.page.get, web.page.perf, web.page.regexp** agent items now along with hostname also support URL as the first parameter, allowing to specify both HTTP and HTTPS protocols. As a prerequisite of SSL (HTTPS) functionality, the agent should be compiled with cURL support. Previously, only domain name or IP address was allowed in the first parameter and there was no support for HTTPS protocol.

Additionally, Unicode is now supported in the hostnames of these items (Punycode support was added).

**Configuration parameters**

The **LoadModule** server/proxy/agent parameter now supports specifying relative or absolute path to the module.

**Maintenance icon in host list**

An orange wrench icon 🛠️ next to the host status now indicates that this host is in maintenance in Configuration → Hosts. Maintenance details are displayed when the mouse pointer is positioned over the icon:

<table>
<thead>
<tr>
<th>Status</th>
<th>Availability</th>
<th>Agent encry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>ZBX</td>
<td>SNMP</td>
</tr>
</tbody>
</table>

Previously, an orange In maintenance string was displayed as status instead of the icon.

**Regular expressions**

The Filesystems for discovery global regular expression has been updated to include “apfs”.

### 16 What’s new in Zabbix 4.0.11

**Full JSONPath functionality supported**

Full support of JSONPath functionality has been added in item value preprocessing.

**Item history**

Global housekeeper settings no longer override item-level history/trends settings in the case when keeping history/trends is entirely disabled on the item level.

In addition, if previously disabling item history/trends had to be specified by entering ‘0’ as the storage period value, now the same can be done using a dedicated radio button.
Manual closing of problems

When updating a problem, the checkbox for closing a problem is now available if the Allow manual close option is checked in trigger configuration for at least one of the selected problems. Only those problems will be closed that are allowed to be closed when clicking on Update. Already closed problems will not be closed repeatedly. If no problem is manually closeable, the checkbox is disabled.

Previously, closing a problem in this way was only possible if the Allow manual close option was checked in trigger configuration for each selected problem. If at least one problem was not manually closeable, the checkbox was disabled.

Similarly, when changing problem severity the relevant checkbox is now available if at least one selected problem is read-writable. Previously each selected problem had to be read-writable, otherwise the checkbox was disabled.

Global notifications

Several improvements have been made to global notification messages and sounds:

• Notifications are synchronized across tabs and windows. Any changes to the list of notifications are immediately rendered into other tabs.
• Notification timeout is calculated since the first rendering time of the notification.
• The Display OK triggers for setting is now applied to recovery type notifications. That becomes relevant if it is shorter than the regular problem notification message timeout thus the notification disappears sooner.
• Default audio clips are now in MP3 (it used to be wave files). An embedded media player is not used any more (it was used for Internet Explorer only), so now, in case of custom audio files, you must be sure that your browser can play them (or just use the MP3 format).
• The sound tends to follow the focused tab/window, except when Play sound is set to 'Once'.
• When Play sound is set to 'Once' it will not replay the sound on page reload.
• In case of several notifications, the sound of the most severe or the most recent notification is played.
• There is now an icon next to each snoozed notification.
• It is possible to snooze a whole list of notifications of High severity and be assured to receive an alarm when an Average severity notification arrives, meanwhile keeping the notification list with all event links open.
• If you snooze a notification in problem state, it will not play audio when the particular problem becomes resolved.
• Regardless of how many tabs are opened the server is polled by only one of them, reducing server load. Additionally the server response traffic is minimized, by not containing the message body and title in response, if the client receives the same notification ID.
• Recovery of a crashed tab is implemented. Any tab that is still able to execute JavaScript will detect a crashed tab and would continue to be the one who polls server. In case of a slow connection and heavy page load during the request, any other tab would continue to poll for notifications. Thus with a notification timeout (30 seconds) and a performed request (40 seconds) one can be assured that no notifications will miss the eye if there is another tab..
• Slide animations are improved. Fade out will happen when all remaining notifications reach the message timeout at once, else the consecutive slide-up transition is applied.
• Updated user settings, such as the timeout and audiofile, are applied to the list of notifications dynamically.

Increased proxy-server limit per connection

Limit per connection has been increased from 128MB to 1GB packet size (ZBX_MAX_RECV_DATA_SIZE constant).

Working with English perfcounters on Windows

It is now possible to work with exclusively English names of Windows performance counters, regardless of the locale, using the new items/parameters:

• perf_counter_en Windows agent item
• PerfCounterEn Windows agent parameter

Note that these items will only work on Windows Server 2008/Vista and above.
Cisco UCS server template

A Cisco UCS server monitoring template - Template Server Cisco UCS SNMPv2 has been added.

It will be available in Configuration → Templates in new installations. If you are upgrading from previous versions, you can find this template in the templates directory of the downloaded latest Zabbix version. Then, while in Configuration → Templates you can import it manually into Zabbix.

Macros

A new \{EVENT.RECOVERY.NAME\} macro is supported, returning the recovery event name.

\{TRIGGER.ID\} macro is now supported in trigger tag values. It may be useful for identifying triggers created from trigger prototypes and, for example, suppressing problems from these triggers during maintenance.

JSONPath preprocessing

Quoted numeric values are now accepted by the JSONPath aggregate functions (sum, min, max, etc.) in item value preprocessing. It means that the values are converted from string type to numeric if aggregation is required.

Acknowledged problems in trigger overview

The icon that indicates an acknowledged problem in Monitoring → Overview now is displayed only if all problems or resolved problems of the trigger are acknowledged. Previously it was enough for the last problem to be acknowledged.

20 What’s new in Zabbix 4.0.15

Problem export to CSV

Export to CSV in Monitoring → Problems now exports problems from all pages, not just the selected page. Filter settings are still obeyed.

Guest user disabled

The "guest" user is now disabled by default in new installations.

Guest user info

In previous versions, when logged in as guest, there was no way to tell what user you were logged in as, because the profile icon was hidden for the guest user. In the new version a slightly different version of the profile icon is displayed when you are logged in as guest - 🅰️. This icon is not clickable and does not lead to the user profile. When the mouse is positioned over it, info is displayed with the name ‘guest’ to suggest the currently logged user.

21 What’s new in Zabbix 4.0.16

Import option to remove existing template linkage

During host or template import it is now possible to update template linkage using the Delete missing option. If using this option any template linkage that does not also exist in the import file will be deleted from the existing host/template along with all entities inherited from these unlinked templates (items, triggers, etc).
By default this option is unchecked and before it is possible to mark this checkbox a warning message is displayed that all inherited entities may be lost as a result.

22 What's new in Zabbix 4.0.17

New items
A new `vfs.fs.get` agent item has been added that returns a JSON with filesystem data including such details as the mountpoint name, mountpoint type, filesystem size and inode metrics.

See a working example of how this item can be used in discovery.

Cannot support audio notification notice
“Cannot support notification audio for this device.” message will be displayed when notification sounds on the device cannot be played.

23 What's new in Zabbix 4.0.18

libssh support
Support of the libssh library (starting from version 0.6.0) has been added. Previously only libssh2 was supported for SSH checks.

DB character set and collation check
A check for the correct character set and collation is now performed on the database, database tables and table fields during the initial frontend installation. If the check fails a warning message is displayed.

A warning message is also displayed in Reports → System information.

See also instructions for changing database character set and collation in MySQL.

Internal events can be disabled
Internal events will not be created, if all internal actions for them are disabled --- this can be useful for reducing the amount of event records and controlling the size of the event tables. See more information.

24 What's new in Zabbix 4.0.19

Log items
Two new options have been added to the `log`, `log.count`, `logrt` and `logrt.count` items:

- mtime-reread - non-unique records, reread file if its modification time changes but size does not
- mtime-noreread - non-unique records, do not reread file if its modification time changes but size does not
For log and log.count items these options have been added as a new <options> parameter, e.g.
\texttt{log[file, regexp, encoding, maxlines, mode, output, maxdelay, options]}

For logrt and logrt.count these options have been added to the already existing <options> parameter.

**JSONPath**

Zabbix implementation of **JSONPath** now supports the extraction of matching element names with a ~ suffix. It returns the name of the matched object or an index in string format of the matched array item.

**Encryption**

User-configured ciphersuites are now supported for GnuTLS and OpenSSL.

25 What's new in Zabbix 4.0.20

**Use of relative URLs**

Relative paths are now allowed in a URL field.

26 What's new in Zabbix 4.0.21

**Cache size configuration parameter**

The maximum value of the CacheSize configuration parameter for Zabbix server/proxy has been increased from 8GB to 64GB.

27 What's new in Zabbix 4.0.22

**Modification time ignored in log, log.count items**

File modification time is now ignored in log and log.count items.

**Enhanced URL widget security**

The URL dashboard widget and the URL screen element now put retrieved URL content into the sandbox. By default, all sandbox restrictions are enabled. It is possible to modify sandbox attribute settings in the defines.inc.php file, however turning sandboxing off is not recommended for security reasons. To learn more about the sandbox attribute, please see the sandbox section of the iframe HTML element description.

28 What's new in Zabbix 4.0.23

**VMware datacenter discovery**

A new \texttt{vmware.dc.discovery[url]} item returns a JSON containing \{#DATACENTER\} and \{#DATACENTERID\} properties.

**Host information in VMware event log**

The information returned by the \texttt{vmware.eventlog[url, mode]} item now contains information about the source host, if such information is detected in the log.

29 What's new in Zabbix 4.0.24

This minor version contains no functional changes.
30 What's new in Zabbix 4.0.25

Aggregate item helper
The item key selector for aggregate items in the frontend now lists all available aggregate keys (grpavg,grpmax,grpmin,grpsum) and their descriptions.

Second precision for age/duration macros
Several built-in macros returning age/duration now return the value with down-to-a-second precision:

- `{DISCOVERY.DEVICE.UPTIME}`
- `{DISCOVERY.SERVICE.UPTIME}`
- `{EVENT.AGE}`

Previously these macros returned values with down-to-a-minute precision.

31 What's new in Zabbix 4.0.26

This minor version contains no functional changes.

32 What's new in Zabbix 4.0.27

Disabled autocomplete attribute for sensitive fields
To avoid potential exposure of data, the autocomplete attribute is now turned off for many fields containing sensitive information, such as a user's password for logging into Zabbix, pre-shared keys (PSK), macro values, usernames and passwords used for data collection by various items and hosts, SNMPv3 authentication and privacy passphrases, passwords for media types; SSL key password and HTTP proxy fields used in web scenarios and HTTP items; usernames, passwords and key passphrases in remote commands. This setting shall prevent most browsers from using autocompletion in the affected fields.

Protection against user enumeration attacks
To make sure an attacker may not guess valid user names because temporary account blocking after consecutive failed login attempts is only applied to existing user names, the account blocking is now also enforced if non-existing user names are used.

To further obscure the possibility of such attacks, a unified generic message is now displayed for all problems related to incorrect login:

Incorrect user name or password or account is temporarily blocked.

33 What's new in Zabbix 4.0.28

Custom multiplier preprocessing step
Custom multiplier preprocessing step now accepts strings with macros (a macro must resolve as an integer or a floating-point number).

Java gateway property file
A new zabbix.properties configuration parameter allows to specify a property file, which can be used to set additional properties in such a way that they are not visible on a command line or to overwrite existing ones.

34 What's new in Zabbix 4.0.29

This minor version does not have any functional changes.
35 What's new in Zabbix 4.0.30

This minor version does not have any functional changes.

36 What's new in Zabbix 4.0.31

This minor version does not have any functional changes.

37 What's new in Zabbix 4.0.32

Web scenario fields

The maximum field size has been increased from 255 to 2000 characters in the web scenario variables and web scenario step variables and post fields.

38 What's new in Zabbix 4.0.33

This minor version does not have any functional changes.

39 What's new in Zabbix 4.0.34

Frontend

If Zabbix web interface is opened in one of the languages available on the Zabbix website, clicking the Support link will open the Support page in the appropriate language. For all other languages, including English, the Support page will be opened in English.

Items

The `vmware.eventlog[]` item for VMware monitoring, when used with the 'skip' option, e.g. `vmware.eventlog[<url>,skip]` now behaves differently after being recreated (i.e. previous item removed, new one created with a different internal ID) - now the internal events cache is reset and only new events are read. Previously, the skip option would not be enforced in this scenario.

40 What's new in Zabbix 4.0.35

This minor version does not have any functional changes.

41 What's new in Zabbix 4.0.36

This minor version does not have any functional changes.

42 What's new in Zabbix 4.0.37

Security

Vulnerability to CVE-2021-42550 has been fixed. As an additional security measure it is recommended to check permissions to the `/etc/zabbix/zabbix_java_gateway_logback.xml` file and set it read-only, if write permissions are available for the “zabbix” user.
What's new in Zabbix 4.0.38

This minor version does not have any functional changes.

What's new in Zabbix 4.0.39

SourceIP support in LDAP simple checks  SourceIP support has been added to LDAP simple checks. Note that with OpenLDAP, version 2.6.1 or above is required.

2. Definitions

Overview  In this section you can learn the meaning of some terms commonly used in Zabbix.

Definitions  host
- a networked device that you want to monitor, with IP/DNS.

host group
- a logical grouping of hosts; it may contain hosts and templates. Hosts and templates within a host group are not in any way linked to each other. Host groups are used when assigning access rights to hosts for different user groups.

item
- a particular piece of data that you want to receive off of a host, a metric of data.

value preprocessing
- a transformation of received metric value before saving it to the database.

trigger
- a logical expression that defines a problem threshold and is used to "evaluate" data received in items.

When received data are above the threshold, triggers go from 'Ok' into a 'Problem' state. When received data are below the threshold, triggers stay in/return to an 'Ok' state.

event
- a single occurrence of something that deserves attention such as a trigger changing state or a discovery/agent auto-registration taking place.

event tag
- a pre-defined marker for the event. It may be used in event correlation, permission granulation, etc.

event correlation
- a method of correlating problems to their resolution flexibly and precisely.

For example, you may define that a problem reported by one trigger may be resolved by another trigger, which may even use a different data collection method.

problem
- a trigger that is in "Problem" state.

problem update
- problem management options provided by Zabbix, such as adding comment, acknowledging, changing severity or closing manually.

action
- a predefined means of reacting to an event.

An action consists of operations (e.g. sending a notification) and conditions (when the operation is carried out)
escalation
- a custom scenario for executing operations within an action; a sequence of sending notifications/executing remote commands.

media
- a means of delivering notifications; delivery channel.

notification
- a message about some event sent to a user via the chosen media channel.

remote command
- a pre-defined command that is automatically executed on a monitored host upon some condition.

template
- a set of entities (items, triggers, graphs, screens, applications, low-level discovery rules, web scenarios) ready to be applied to one or several hosts.

The job of templates is to speed up the deployment of monitoring tasks on a host; also to make it easier to apply mass changes to monitoring tasks. Templates are linked directly to individual hosts.

application
- a grouping of items in a logical group.

web scenario
- one or several HTTP requests to check the availability of a web site.

frontend
- the web interface provided with Zabbix.

dashboard
- customizable section of the web interface displaying summaries and visualizations of important information in visual units called widgets.

widget
- visual unit displaying information of a certain kind and source (a summary, a map, a graph, the clock, etc.), used in the dashboard.

Zabbix API
- Zabbix API allows you to use the JSON RPC protocol to create, update and fetch Zabbix objects (like hosts, items, graphs and others) or perform any other custom tasks.

Zabbix server
- a central process of Zabbix software that performs monitoring, interacts with Zabbix proxies and agents, calculates triggers, sends notifications; a central repository of data.

Zabbix agent
- a process deployed on monitoring targets to actively monitor local resources and applications.

Zabbix proxy
- a process that may collect data on behalf of Zabbix server, taking some processing load off of the server.

encryption
- support of encrypted communications between Zabbix components (server, proxy, agent, zabbix_sender and zabbix_get utilities) using Transport Layer Security (TLS) protocol.

network discovery
- automated discovery of network devices.

low-level discovery
- automated discovery of low-level entities on a particular device (e.g. file systems, network interfaces, etc.).

low-level discovery rule
- set of definitions for automated discovery of low-level entities on a device.

item prototype
- a metric with certain parameters as variables, ready for low-level discovery. After low-level discovery the variables are automatically substituted with the real discovered parameters and the metric automatically starts gathering data.

**trigger prototype**

- a trigger with certain parameters as variables, ready for low-level discovery. After low-level discovery the variables are automatically substituted with the real discovered parameters and the trigger automatically starts evaluating data.

Prototypes of some other Zabbix entities are also in use in low-level discovery - graph prototypes, host prototypes, host group prototypes, application prototypes.

**agent auto-registration**

- automated process whereby a Zabbix agent itself is registered as a host and started to monitor.

### 3. Zabbix processes

Please use the sidebar to access content in the Zabbix process section.

#### 1 Server

**Overview**

Zabbix server is the central process of Zabbix software.

The server performs the polling and trapping of data, it calculates triggers, sends notifications to users. It is the central component to which Zabbix agents and proxies report data on availability and integrity of systems. The server can itself remotely check networked services (such as web servers and mail servers) using simple service checks.

The server is the central repository in which all configuration, statistical and operational data is stored, and it is the entity in Zabbix that will actively alert administrators when problems arise in any of the monitored systems.

The functioning of a basic Zabbix server is broken into three distinct components; they are: Zabbix server, web frontend and database storage.

All of the configuration information for Zabbix is stored in the database, which both the server and the web frontend interact with. For example, when you create a new item using the web frontend (or API) it is added to the items table in the database. Then, about once a minute Zabbix server will query the items table for a list of the items which are active that is then stored in a cache within the Zabbix server. This is why it can take up to two minutes for any changes made in Zabbix frontend to show up in the latest data section.

**Running server**

If installed as package

Zabbix server runs as a daemon process. The server can be started by executing:

```shell
shell> service zabbix-server start
```

This will work on most of GNU/Linux systems. On other systems you may need to run:

```shell
shell> /etc/init.d/zabbix-server start
```

Similarly, for stopping/restarting/viewing status, use the following commands:

```shell
shell> service zabbix-server stop
shell> service zabbix-server restart
shell> service zabbix-server status
```

**Start up manually**

If the above does not work you have to start it manually. Find the path to the zabbix_server binary and execute:

```shell
shell> zabbix_server
```

You can use the following command line parameters with Zabbix server:

- `--config <file>` path to the configuration file (default is /usr/local/etc/zabbix_server.conf)
- `--foreground` run Zabbix server in foreground
- `--runtime-control <option>` perform administrative functions
Examples of running Zabbix server with command line parameters:

shell> zabbix_server -c /usr/local/etc/zabbix_server.conf
shell> zabbix_server --help
shell> zabbix_server -V

Runtime control

Runtime control options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>config_cache_reload</td>
<td>Reload configuration cache. Ignored if cache is being currently loaded.</td>
<td></td>
</tr>
<tr>
<td>housekeeper_execute</td>
<td>Start the housekeeping procedure. Ignored if the housekeeping procedure is currently in progress.</td>
<td></td>
</tr>
<tr>
<td>log_level_increase[=&lt;target&gt;]</td>
<td>Increase log level, affects all processes if target is not specified.</td>
<td></td>
</tr>
<tr>
<td>log_level_decrease[=&lt;target&gt;]</td>
<td>Decrease log level, affects all processes if target is not specified.</td>
<td></td>
</tr>
</tbody>
</table>

Example of using runtime control to reload the server configuration cache:

shell> zabbix_server -c /usr/local/etc/zabbix_server.conf -R config_cache_reload

Example of using runtime control to trigger execution of housekeeper:

shell> zabbix_server -c /usr/local/etc/zabbix_server.conf -R housekeeper_execute

Examples of using runtime control to change log level:

Increase log level of all processes:

shell> zabbix_server -c /usr/local/etc/zabbix_server.conf -R log_level_increase

Increase log level of second poller process:

shell> zabbix_server -c /usr/local/etc/zabbix_server.conf -R log_level_increase=poller,2

Increase log level of process with PID 1234:

shell> zabbix_server -c /usr/local/etc/zabbix_server.conf -R log_level_increase=1234

Decrease log level of all http poller processes:

shell> zabbix_server -c /usr/local/etc/zabbix_server.conf -R log_level_decrease="http poller"

Process user

Zabbix server is designed to run as a non-root user. It will run as whatever non-root user it is started as. So you can run server as any non-root user without any issues.

If you will try to run it as ‘root’, it will switch to a hardcoded ‘zabbix’ user, which must be present on your system. You can only run server as ‘root’ if you modify the ‘AllowRoot’ parameter in the server configuration file accordingly.

If Zabbix server and agent are run on the same machine it is recommended to use a different user for running the server than for running the agent. Otherwise, if both are run as the same user, the agent can access the server configuration file and any Admin level user in Zabbix can quite easily retrieve, for example, the database password.
Configuration file

See the configuration file options for details on configuring zabbix_server.

Start-up scripts

The scripts are used to automatically start/stop Zabbix processes during system’s start-up/shutdown. The scripts are located under directory misc/init.d.

Server process types

- alert manager - manager of alerter tasks
- alerter - process for sending notifications
- configuration syncer - process for managing in-memory cache of configuration data
- discoverer - process for discovery of devices
- escalator - process for escalation of actions
- history syncer - history DB writer
- housekeeper - process for removal of old historical data
- http poller - web monitoring poller
- icmp pinger - poller for icmp ping checks
- ipmi manager - IPMI poller manager
- ipmi poller - poller for IPMI checks
- java poller - poller for Java checks
- poller - normal poller for passive checks
- preprocessing manager - manager of preprocessing tasks
- preprocessing worker - process for data preprocessing
- proxy poller - poller for passive proxies
- self-monitoring - process for collecting internal server statistics
- snmp trapper - trapper for SNMP traps
- task manager - process for remote execution of tasks requested by other components (e.g. close problem, acknowledge problem, check item value now, remote command functionality)
- timer - timer for processing maintenances
- trigger - trigger for active checks, traps, proxy communication
- unreachable poller - poller for unreachable devices
- vmware collector - VMware data collector responsible for data gathering from VMware services

The server log file can be used to observe these process types.

Various types of Zabbix server processes can be monitored using the zabbix[process,<type>,<mode>,<state>] internal item.

Supported platforms

Due to the security requirements and mission-critical nature of server operation, UNIX is the only operating system that can consistently deliver the necessary performance, fault tolerance and resilience. Zabbix operates on market leading versions.

Zabbix server is tested on the following platforms:

- Linux
- Solaris
- AIX
- HP-UX
- Mac OS X
- FreeBSD
- OpenBSD
- NetBSD
- SCO Open Server
- Tru64/OSF1

Note: Zabbix may work on other Unix-like operating systems as well.

Locale

Note that the server requires a UTF-8 locale so that some textual items can be interpreted correctly. Most modern Unix-like systems have a UTF-8 locale as default, however, there are some systems where that may need to be set specifically.
Overview

Zabbix agent is deployed on a monitoring target to actively monitor local resources and applications (hard drives, memory, processor statistics, etc.).

The agent gathers operational information locally and reports data to Zabbix server for further processing. In case of failures (such as a hard disk running full or a crashed service process), Zabbix server can actively alert the administrators of the particular machine that reported the failure.

Zabbix agents are extremely efficient because of use of native system calls for gathering statistical information.

Passive and active checks

Zabbix agents can perform passive and active checks.

In a passive check the agent responds to a data request. Zabbix server (or proxy) asks for data, for example, CPU load, and Zabbix agent sends back the result.

Active checks require more complex processing. The agent must first retrieve a list of items from Zabbix server for independent processing. Then it will periodically send new values to the server.

Whether to perform passive or active checks is configured by selecting the respective monitoring item type. Zabbix agent processes items of type 'Zabbix agent' or 'Zabbix agent (active)'.

Supported platforms

Zabbix agent is supported on the following platforms:

- Windows (all desktop and server versions since XP)
- Linux (also available in distribution packages)
- macOS
- IBM AIX
- FreeBSD
- OpenBSD
- Solaris

Agent on UNIX-like systems

Zabbix agent on UNIX-like systems is run on the host being monitored.

Installation

See the package installation section for instructions on how to install Zabbix agent as package.

Alternatively see instructions for manual installation if you do not want to use packages.

Attention:

In general, 32bit Zabbix agents will work on 64bit systems, but may fail in some cases.

If installed as package

Zabbix agent runs as a daemon process. The agent can be started by executing:

```sh
cshell> service zabbix-agent start
```

This will work on most of GNU/Linux systems. On other systems you may need to run:

```sh
cshell> /etc/init.d/zabbix-agent start
```

Similarly, for stopping/restarting/viewing status of Zabbix agent, use the following commands:

```sh
shell> service zabbix-agent stop
shell> service zabbix-agent restart
shell> service zabbix-agent status
```

Start up manually

If the above does not work you have to start it manually. Find the path to the zabbix_agentd binary and execute:

```sh
cshell> zabbix_agentd
```
Agent on Windows systems

Zabbix agent on Windows runs as a Windows service.

Preparation

Zabbix agent is distributed as a zip archive. After you download the archive you need to unpack it. Choose any folder to store Zabbix agent and the configuration file, e.g.

C:\zabbix

Copy bin\zabbix_agentd.exe and conf\zabbix_agentd.conf files to c:\zabbix.

Edit the c:\zabbix\zabbix_agentd.conf file to your needs, making sure to specify a correct “Hostname” parameter.

Installation

After this is done use the following command to install Zabbix agent as Windows service:

C:\> c:\zabbix\zabbix_agentd.exe -c c:\zabbix\zabbix_agentd.conf -i

Now you should be able to configure “Zabbix agent” service normally as any other Windows service.

See more details on installing and running Zabbix agent on Windows.

Other agent options

It is possible to run multiple instances of the agent on a host. A single instance can use the default configuration file or a configuration file specified in the command line. In case of multiple instances each agent instance must have its own configuration file (one of the instances can use the default configuration file).

The following command line parameters can be used with Zabbix agent:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNIX and Windows agent</td>
<td>Path to the configuration file.</td>
</tr>
<tr>
<td>-c --config &lt;config-file&gt;</td>
<td>You may use this option to specify a configuration file that is not the default one.</td>
</tr>
<tr>
<td></td>
<td>On UNIX, default is /usr/local/etc/zabbix_agentd.conf or as set by compile-time variables --sysconfdir or --prefix.</td>
</tr>
<tr>
<td></td>
<td>On Windows, default is c:\zabbix_agentd.conf</td>
</tr>
<tr>
<td>-p --print</td>
<td>Print known items and exit.</td>
</tr>
<tr>
<td></td>
<td>Note: To return user parameter results as well, you must specify the configuration file (if it is not in the default location).</td>
</tr>
<tr>
<td>-t --test &lt;item key&gt;</td>
<td>Test specified item and exit.</td>
</tr>
<tr>
<td></td>
<td>Note: To return user parameter results as well, you must specify the configuration file (if it is not in the default location).</td>
</tr>
<tr>
<td>-h --help</td>
<td>Display help information</td>
</tr>
<tr>
<td>-V --version</td>
<td>Display version number</td>
</tr>
<tr>
<td>UNIX agent only</td>
<td>Perform administrative functions. See runtime control.</td>
</tr>
<tr>
<td>-R --runtime-control &lt;option&gt;</td>
<td></td>
</tr>
<tr>
<td>Windows agent only</td>
<td>Use multiple agent instances (with -i,-d,-s,-x functions).</td>
</tr>
<tr>
<td>-m --multiple-agents</td>
<td>To distinguish service names of instances, each service name will include the Hostname value from the specified configuration file.</td>
</tr>
<tr>
<td>Windows agent only (functions)</td>
<td>Install Zabbix Windows agent as service</td>
</tr>
<tr>
<td>-i --install</td>
<td>Uninstall Zabbix Windows agent service</td>
</tr>
<tr>
<td>-d --uninstall</td>
<td>Start Zabbix Windows agent service</td>
</tr>
<tr>
<td>-s --start</td>
<td>Stop Zabbix Windows agent service</td>
</tr>
<tr>
<td>-x --stop</td>
<td></td>
</tr>
</tbody>
</table>

Specific examples of using command line parameters:

- printing all built-in agent items with values
- testing a user parameter with “mysql.ping” key defined in the specified configuration file
- installing a “Zabbix Agent” service for Windows using the default path to configuration file c:\zabbix_agentd.conf
- installing a “Zabbix Agent [Hostname]” service for Windows using the configuration file zabbix_agentd.conf located in the same folder as agent executable and make the service name unique by extending it by Hostname value from the config file
shell> zabbix_agentd --print
shell> zabbix_agentd -t "mysql.ping" -c /etc/zabbix/zabbix_agentd.conf
shell> zabbix_agentd.exe -i
shell> zabbix_agentd.exe -i -m -c zabbix_agentd.conf

Runtime control

With runtime control options you may change the log level of agent processes.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Target</th>
</tr>
</thead>
</table>
| log_level_increase[=<target>] | Increase log level. If target is not specified, all processes are affected. | Target can be specified as:  
  process type - all processes of specified type (e.g., listener)  
  process type,N - process type and number (e.g., listener,3)  
  pid - process identifier (1 to 65535). For larger values specify target as 'process-type,N'. |
| log_level_decrease[=<target>] | Decrease log level. If target is not specified, all processes are affected. | |

Examples:

- increasing log level of all processes
- increasing log level of the third listener process
- increasing log level of process with PID 1234
- decreasing log level of all active check processes

shell> zabbix_agentd -R log_level_increase
shell> zabbix_agentd -R log_level_increase=listener,3
shell> zabbix_agentd -R log_level_increase=1234
shell> zabbix_agentd.exe -R log_level_decrease="active checks"

Note:
Runtime control is not supported on OpenBSD, NetBSD and Windows.

Agent process types

- active checks - process for performing active checks
- collector - process for data collection
- listener - process for listening to passive checks

The agent log file can be used to observe these process types.

Process user

Zabbix agent on UNIX is designed to run as a non-root user. It will run as whatever non-root user it is started as. So you can run agent as any non-root user without any issues.

If you will try to run it as 'root', it will switch to a hardcoded 'zabbix' user, which must be present on your system. You can only run agent as 'root' if you modify the 'AllowRoot' parameter in the agent configuration file accordingly.

Configuration file

For details on configuring Zabbix agent see the configuration file options for zabbix_agentd or Windows agent.

Locale

Note that the agent requires a UTF-8 locale so that some textual agent items can return the expected content. Most modern Unix-like systems have a UTF-8 locale as default, however, there are some systems where that may need to be set specifically.

Exit code

Before version 2.2 Zabbix agent returned 0 in case of successful exit and 255 in case of failure. Starting from version 2.2 and higher Zabbix agent returns 0 in case of successful exit and 1 in case of failure.
Overview

Zabbix proxy is a process that may collect monitoring data from one or more monitored devices and send the information to the Zabbix server, essentially working on behalf of the server. All collected data is buffered locally and then transferred to the Zabbix server the proxy belongs to.

Deploying a proxy is optional, but may be very beneficial to distribute the load of a single Zabbix server. If only proxies collect data, processing on the server becomes less CPU and disk I/O hungry.

A Zabbix proxy is the ideal solution for centralized monitoring of remote locations, branches and networks with no local administrators.

Zabbix proxy requires a separate database.

Attention:
Note that databases supported with Zabbix proxy are SQLite, MySQL and PostgreSQL. Using Oracle or IBM DB2 is at your own risk and may contain some limitations as, for example, in return values of low-level discovery rules.

See also: Using proxies in a distributed environment

Running proxy

If installed as package

Zabbix proxy runs as a daemon process. The proxy can be started by executing:

shell> service zabbix-proxy start

This will work on most of GNU/Linux systems. On other systems you may need to run:

shell> /etc/init.d/zabbix-proxy start

Similarly, for stopping/restarting/viewing status of Zabbix proxy, use the following commands:

shell> service zabbix-proxy stop
shell> service zabbix-proxy restart
shell> service zabbix-proxy status

Start up manually

If the above does not work you have to start it manually. Find the path to the zabbix_proxy binary and execute:

shell> zabbix_proxy

You can use the following command line parameters with Zabbix proxy:

-c --config <file>                  path to the configuration file
-f --foreground run Zabbix proxy in foreground
-R --runtime-control <option>       perform administrative functions
-h --help give this help
-V --version display version number

Note:
Runtime control is not supported on OpenBSD and NetBSD.

Examples of running Zabbix proxy with command line parameters:

shell> zabbix_proxy -c /usr/local/etc/zabbix_proxy.conf
shell> zabbix_proxy --help
shell> zabbix_proxy -V

Runtime control

Runtime control options:
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>config_cache_reload</td>
<td>Reload configuration cache. Ignored if cache is being currently loaded. The Zabbix proxy will connect to the Zabbix server and request configuration data.</td>
<td></td>
</tr>
<tr>
<td>housekeeper_execute</td>
<td>Start the housekeeping procedure. Ignored if the housekeeping procedure is currently in progress.</td>
<td></td>
</tr>
</tbody>
</table>

**log_level_increase[=⟨target⟩]**

Increase log level, affects all processes if target is not specified.

**log_level_decrease[=⟨target⟩]**

Decrease log level, affects all processes if target is not specified.

Example of using runtime control to reload the proxy configuration cache:

```shell
shell> zabbix_proxy -c /usr/local/etc/zabbix_proxy.conf -R config_cache_reload
```

Example of using runtime control to trigger execution of housekeeper:

```shell
shell> zabbix_proxy -c /usr/local/etc/zabbix_proxy.conf -R housekeeper_execute
```

Examples of using runtime control to change log level:

Increase log level of all processes:

```shell
shell> zabbix_proxy -c /usr/local/etc/zabbix_proxy.conf -R log_level_increase
```

Increase log level of second poller process:

```shell
shell> zabbix_proxy -c /usr/local/etc/zabbix_proxy.conf -R log_level_increase=poller,2
```

Increase log level of process with PID 1234:

```shell
shell> zabbix_proxy -c /usr/local/etc/zabbix_proxy.conf -R log_level_increase=1234
```

Decrease log level of all http poller processes:

```shell
shell> zabbix_proxy -c /usr/local/etc/zabbix_proxy.conf -R log_level_decrease="http poller"
```

Process user

Zabbix proxy is designed to run as a non-root user. It will run as whatever non-root user it is started as. So you can run proxy as any non-root user without any issues.

If you will try to run it as 'root', it will switch to a hardcoded 'zabbix' user, which must be present on your system. You can only run proxy as 'root' if you modify the 'AllowRoot' parameter in the proxy configuration file accordingly.

Configuration file

See the configuration file options for details on configuring zabbix_proxy.

Proxy process types

- configuration syncer - process for managing in-memory cache of configuration data
- data sender - proxy data sender
- discoverer - process for discovery of devices
- heartbeat sender - proxy heartbeat sender
- history syncer - history DB writer
- housekeeper - process for removal of old historical data
- http poller - web monitoring poller
- icmp pinger - poller for icmp ping checks
- ipmi manager - IPMI pollermanager
- ipmi poller - poller for IPMI checks
- java poller - poller for Java checks
- poller - normal poller for passive checks
• self-monitoring - process for collecting internal server statistics
• snmp trapper - trapper for SNMP traps
• task manager - process for remote execution of tasks requested by other components (e.g. close problem, acknowledge problem, check item value now, remote command functionality)
• trapper - trapper for active checks, traps, proxy communication
• unreachable poller - poller for unreachable devices
• vmware collector - VMware data collector responsible for data gathering from VMware services

The proxy log file can be used to observe these process types.

Various types of Zabbix proxy processes can be monitored using the `zabbix[process,<type>,<mode>,<state>]` internal item.

Supported platforms

Zabbix proxy runs on the same list of server#supported platforms as Zabbix server.

Locale

Note that the proxy requires a UTF-8 locale so that some textual items can be interpreted correctly. Most modern Unix-like systems have a UTF-8 locale as default, however, there are some systems where that may need to be set specifically.

4 Java gateway

Overview

Native support for monitoring JMX applications exists in the form of a Zabbix daemon called “Zabbix Java gateway”, available since Zabbix 2.0. Zabbix Java gateway is a daemon written in Java. To find out the value of a particular JMX counter on a host, Zabbix server queries Zabbix Java gateway, which uses the JMX management API to query the application of interest remotely. The application does not need any additional software installed, it just has to be started with `-Dcom.sun.management.jmxremote` option on the command line.

Java gateway accepts incoming connection from Zabbix server or proxy and can only be used as a “passive proxy”. As opposed to Zabbix proxy, it may also be used from Zabbix proxy (Zabbix proxies cannot be chained). Access to each Java gateway is configured directly in Zabbix server or proxy configuration file, thus only one Java gateway may be configured per Zabbix server or Zabbix proxy. If a host will have items of type JMX agent and items of other type, only the JMX agent items will be passed to Java gateway for retrieval.

When an item has to be updated over Java gateway, Zabbix server or proxy will connect to the Java gateway and request the value, which Java gateway in turn retrieves and passes back to the server or proxy. As such, Java gateway does not cache any values.

Zabbix server or proxy has a specific type of processes that connect to Java gateway, controlled by the option `StartJavaPollers`. Internally, Java gateway starts multiple threads, controlled by the `START_POLLERS` option. On the server side, if a connection takes more than `Timeout` seconds, it will be terminated, but Java gateway might still be busy retrieving value from the JMX counter. To solve this, there is the `TIMEOUT` option in Java gateway that allows to set timeout for JMX network operations.

Zabbix server or proxy will try to pool requests to a single JMX target together as much as possible (affected by item intervals) and send them to the Java gateway in a single connection for better performance.

It is suggested to have `StartJavaPollers` less than or equal to `START_POLLERS`, otherwise there might be situations when no threads are available in the Java gateway to service incoming requests; in such a case Java gateway uses ThreadPoolExecutor.CallerRunsPolicy, meaning that the main thread will service the incoming request and temporarily will not accept any new requests.

Getting Java gateway

You can install Java gateway either from the sources or packages downloaded from Zabbix website.

Using the links below you can access information how to get and run Zabbix Java gateway, how to configure Zabbix server (or Zabbix proxy) to use Zabbix Java gateway for JMX monitoring, and how to configure Zabbix items in Zabbix frontend that correspond to particular JMX counters.
1 Setup from sources

Overview

If installed from sources, the following information will help you in setting up Zabbix Java gateway.

Overview of files

If you obtained Java gateway from sources, you should have ended up with a collection of shell scripts, JAR and configuration files under $PREFIX/sbin/zabbix_java. The role of these files is summarized below.

- bin/zabbix-java-gateway-$VERSION.jar: Java gateway JAR file itself.
- lib/logback-core-0.9.27.jar, lib/logback-classic-0.9.27.jar, lib/slf4j-api-1.6.1.jar, lib/android-json-4.3_r3.1.jar: Dependencies of Java gateway: Logback, SLF4J, and Android JSON library.
- shutdown.sh, startup.sh: Convenience scripts for starting and stopping Java gateway.
- settings.sh: Configuration file that is sourced by startup and shutdown scripts above.

Configuring and running Java gateway

By default, Java gateway listens on port 10052. If you plan on running Java gateway on a different port, you can specify that in settings.sh script. See the description of Java gateway configuration file for how to specify this and other options.

Warning: Port 10052 is not IANA registered.

Once you are comfortable with the settings, you can start Java gateway by running the startup script:

$ ./startup.sh

Likewise, once you no longer need Java gateway, run the shutdown script to stop it:

$ ./shutdown.sh

Note that unlike server or proxy, Java gateway is lightweight and does not need a database.

Configuring server for use with Java gateway

With Java gateway up and running, you have to tell Zabbix server where to find Zabbix Java gateway. This is done by specifying JavaGateway and JavaGatewayPort parameters in the server configuration file. If the host on which JMX application is running is monitored by Zabbix proxy, then you specify the connection parameters in the proxy configuration file instead.

JavaGateway=192.168.3.14
JavaGatewayPort=10052

By default, server does not start any processes related to JMX monitoring. If you wish to use it, however, you have to specify the number of pre-forked instances of Java pollers. You do this in the same way you specify regular pollers and trappers.

StartJavaPollers=5

Do not forget to restart server or proxy, once you are done with configuring them.

Debugging Java gateway

In case there are any problems with Java gateway or an error message that you see about an item in the frontend is not descriptive enough, you might wish to take a look at Java gateway log file.
By default, Java gateway logs its activities into /tmp/zabbix_java.log file with log level “info”. Sometimes that information is not enough and there is a need for information at log level “debug”. In order to increase logging level, modify file lib/logback.xml and change the level attribute of <root> tag to “debug”:

```
<root level="debug">
    <appender-ref ref="FILE" />
</root>
```

Note that unlike Zabbix server or Zabbix proxy, there is no need to restart Zabbix Java gateway after changing logback.xml file - changes in logback.xml will be picked up automatically. When you are done with debugging, you can return the logging level to “info”.

If you wish to log to a different file or a completely different medium like database, adjust logback.xml file to meet your needs. See Logback Manual for more details.

Sometimes for debugging purposes it is useful to start Java gateway as a console application rather than a daemon. To do that, comment out PID_FILE variable in settings.sh. If PID_FILE is omitted, startup.sh script starts Java gateway as a console application and makes Logback use lib/logback-console.xml file instead, which not only logs to console, but has logging level “debug” enabled as well.

Finally, note that since Java gateway uses SLF4J for logging, you can replace Logback with the framework of your choice by placing an appropriate JAR file in lib directory. See SLF4J Manual for more details.

JMX monitoring

See JMX monitoring page for more details.

### 2 Setup from RHEL/CentOS packages

Overview

If installed from RHEL/CentOS packages, the following information will help you in setting up Zabbix Java gateway.

Configuring and running Java gateway

Configuration parameters of Zabbix Java gateway may be tuned in the file:

```
/etc/zabbix/zabbix_java_gateway.conf
```

For more details, see Zabbix Java gateway configuration parameters. To start Zabbix Java gateway:

```
# service zabbix-java-gateway restart
```

To automatically start Zabbix Java gateway on boot:

RHEL 7 and later:

```
# systemctl enable zabbix-java-gateway
```

RHEL prior to 7:

```
# chkconfig --level 12345 zabbix-java-gateway on
```

Configuring server for use with Java gateway

With Java gateway up and running, you have to tell Zabbix server where to find Zabbix Java gateway. This is done by specifying JavaGateway and JavaGatewayPort parameters in the server configuration file. If the host on which JMX application is running is monitored by Zabbix proxy, then you specify the connection parameters in the proxy configuration file instead.

```
JavaGateway=192.168.3.14
JavaGatewayPort=10052
```

By default, server does not start any processes related to JMX monitoring. If you wish to use it, however, you have to specify the number of pre-forked instances of Java pollers. You do this in the same way you specify regular pollers and trappers.

```
StartJavaPollers=5
```

Do not forget to restart server or proxy, once you are done with configuring them.

Debugging Java gateway

Zabbix java gateway log file is:

```
/var/log/zabbix/zabbix_java_gateway.log
```
If you like to increase the logging, edit the file:

/etc/zabbix/zabbix_java_gateway_logback.xml

and change level="info" to "debug" or even "trace" (for deep troubleshooting):

```xml
<configuration scan="true" scanPeriod="15 seconds">
  [...]
  <root level="info">
    <appender-ref ref="FILE" />
  </root>
</configuration>
```

JMX monitoring

See JMX monitoring page for more details.

### 3 Setup from Debian/Ubuntu packages

**Overview**

If installed from Debian/Ubuntu packages, the following information will help you in setting up Zabbix Java gateway.

Configuring and running Java gateway

Java gateway configuration may be tuned in the file:

/etc/zabbix/zabbix_java_gateway.conf

For more details, see Zabbix Java gateway configuration parameters.

To start Zabbix Java gateway:

```
# service zabbix-java-gateway restart
```

To automatically start Zabbix Java gateway on boot:

```
# systemctl enable zabbix-java-gateway
```

Configuring server for use with Java gateway

With Java gateway up and running, you have to tell Zabbix server where to find Zabbix Java gateway. This is done by specifying JavaGateway and JavaGatewayPort parameters in the server configuration file. If the host on which JMX application is running is monitored by Zabbix proxy, then you specify the connection parameters in the proxy configuration file instead.

```
JavaGateway=192.168.3.14
JavaGatewayPort=10052
```

By default, server does not start any processes related to JMX monitoring. If you wish to use it, however, you have to specify the number of pre-forked instances of Java pollers. You do this in the same way you specify regular pollers and trappers.

```
StartJavaPollers=5
```

Do not forget to restart server or proxy, once you are done with configuring them.

Debugging Java gateway

Zabbix Java gateway log file is:

/var/log/zabbix/zabbix_java_gateway.log

If you like to increase the logging, edit the file:

/etc/zabbix/zabbix_java_gateway_logback.xml

and change level="info" to "debug" or even "trace" (for deep troubleshooting):

```xml
<configuration scan="true" scanPeriod="15 seconds">
  [...]
  <root level="info">
    <appender-ref ref="FILE" />
  </root>
</configuration>
```
5 Sender

Overview
Zabbix sender is a command line utility that may be used to send performance data to Zabbix server for processing. The utility is usually used in long running user scripts for periodical sending of availability and performance data.

For sending results directly to Zabbix server or proxy, a trapper item type must be configured.

Running Zabbix sender
An example of running Zabbix UNIX sender:

```
shell> cd bin
shell> ./zabbix_sender -z zabbix -s "Linux DB3" -k db.connections -o 43
```

where:
- `z` - Zabbix server host (IP address can be used as well)
- `s` - technical name of monitored host (as registered in Zabbix frontend)
- `k` - item key
- `o` - value to send

**Attention:**
Options that contain whitespaces, must be quoted using double quotes.

Zabbix sender can be used to send multiple values from an input file. See the Zabbix sender manpage for more information.

Zabbix sender accepts strings in UTF-8 encoding (for both UNIX-like systems and Windows) without byte order mark (BOM) first in the file.

Zabbix sender on Windows can be run similarly:

```
zabbix_sender.exe [options]
```

Since Zabbix 1.8.4, zabbix_sender realtime sending scenarios have been improved to gather multiple values passed to it in close succession and send them to the server in a single connection. A value that is not further apart from the previous value than 0.2 seconds can be put in the same stack, but maximum pooling time still is 1 second.

**Note:**
Zabbix sender will terminate if invalid (not following parameter=value notation) parameter entry is present in the specified configuration file.

6 Get

Overview
Zabbix get is a command line utility which can be used to communicate with Zabbix agent and retrieve required information from the agent.

The utility is usually used for the troubleshooting of Zabbix agents.

Running Zabbix get
An example of running Zabbix get under UNIX to get the processor load value from the agent:

```
shell> cd bin
shell> ./zabbix_get -s 127.0.0.1 -p 10050 -k system.cpu.load[all,avg1]
```

Another example of running Zabbix get for capturing a string from a website:

```
shell> cd bin
shell> ./zabbix_get -s 192.168.1.1 -p 10050 -k "web.page.regexp[www.example.com,\,\,\,"USA: ([a-zA-Z0-9.-]+)\"]"
```
Note that the item key here contains a space so quotes are used to mark the item key to the shell. The quotes are not part of the item key; they will be trimmed by the shell and will not be passed to Zabbix agent.

Zabbix get accepts the following command line parameters:

- `--host <host name or IP>` Specify host name or IP address of a host.
- `--port <port number>` Specify port number of agent running on the host. Default is 10050.
- `--source-address <IP address>` Specify source IP address.
- `--key <item key>` Specify key of item to retrieve value of.
- `--help` Give this help.
- `--version` Display version number.

See also [Zabbix get manpage](https://zabbix.com/documentation) for more information.

Zabbix get on Windows can be run similarly:

```bash
zabbix_get.exe [options]
```

### 4. Installation

Please use the sidebar to access content in the Installation section.

#### 1 Getting Zabbix

**Overview**

There are four ways of getting Zabbix:

- Install it from the [distribution packages](https://zabbix.com/documentation)
- Download the latest source archive and compile it yourself
- Install it from the [containers](https://zabbix.com/documentation)
- Download the [virtual appliance](https://zabbix.com/documentation)

To download the latest distribution packages, pre-compiled sources or the virtual appliance, go to the Zabbix download page, where direct links to latest versions are provided.

**Getting Zabbix source code**

There are several ways of getting Zabbix source code:

- You can [download](https://zabbix.com/documentation) the released stable versions from the official Zabbix website
- You can [download](https://zabbix.com/documentation) nightly builds from the official Zabbix website developer page
- You can get the latest development version from the Git source code repository system:
  - The primary location of the full repository is at [https://git.zabbix.com/scm/zbx/zabbix.git](https://git.zabbix.com/scm/zbx/zabbix.git)
  - Master and supported releases are also mirrored to Github at [https://github.com/zabbix/zabbix](https://github.com/zabbix/zabbix)

A Git client must be installed to clone the repository. The official commandline Git client package is commonly called `git` in distributions. To install, for example, on Debian/Ubuntu, run:

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

To grab all Zabbix source, change to the directory you want to place the code in and execute:

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

#### 2 Requirements

**Hardware**

**Memory**

Zabbix requires both physical and disk memory. 128 MB of physical memory and 256 MB of free disk space could be a good starting point. However, the amount of required disk memory obviously depends on the number of hosts and parameters that are being monitored. If you’re planning to keep a long history of monitored parameters, you should be thinking of at least a couple of...
gigabytes to have enough space to store the history in the database. Each Zabbix daemon process requires several connections to a database server. Amount of memory allocated for the connection depends on configuration of the database engine.

**Note:**
The more physical memory you have, the faster the database (and therefore Zabbix) works.

**CPU**

Zabbix and especially Zabbix database may require significant CPU resources depending on number of monitored parameters and chosen database engine.

**Other hardware**

A serial communication port and a serial GSM modem are required for using SMS notification support in Zabbix. USB-to-serial converter will also work.

**Examples of hardware configuration**

The table provides several examples of hardware configurations:

<table>
<thead>
<tr>
<th>Name</th>
<th>Platform</th>
<th>CPU/Memory</th>
<th>Database</th>
<th>Monitored hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small</td>
<td>CentOS Virtual Appliance</td>
<td>2 CPU cores/2GB</td>
<td>MySQL InnoDB</td>
<td>100</td>
</tr>
<tr>
<td>Medium</td>
<td>CentOS</td>
<td>4 CPU cores/8GB</td>
<td>MySQL InnoDB</td>
<td>500</td>
</tr>
<tr>
<td>Large</td>
<td>RedHat Enterprise Linux</td>
<td>8 CPU cores/16GB</td>
<td>RAID10 MySQL InnoDB or PostgreSQL</td>
<td>&gt;1000</td>
</tr>
<tr>
<td>Very large</td>
<td>RedHat Enterprise Linux</td>
<td>8 CPU cores/16GB</td>
<td>Fast RAID10 MySQL InnoDB or PostgreSQL</td>
<td>&gt;10000</td>
</tr>
</tbody>
</table>

**Note:**
Actual configuration depends on the number of active items and refresh rates very much (see database size section of this page for details). It is highly recommended to run the database on a separate box for large installations.

**Supported platforms**

Due to security requirements and mission-critical nature of monitoring server, UNIX is the only operating system that can consistently deliver the necessary performance, fault tolerance and resilience. Zabbix operates on market leading versions.

Zabbix is tested on the following platforms:

- Linux
- IBM AIX
- FreeBSD
- NetBSD
- OpenBSD
- HP-UX
- Mac OS X
- Solaris
- Windows: all desktop and server versions since XP (Zabbix agent only)

**Note:**
Zabbix may work on other Unix-like operating systems as well.

**Attention:**
Zabbix disables core dumps if compiled with encryption and does not start if system does not allow disabling of core dumps.

**Software**

Zabbix is built around a modern Apache web server, leading database engines, and PHP scripting language.

**Database management system**
<table>
<thead>
<tr>
<th>Software</th>
<th>Version</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>MySQL</td>
<td>5.0.3 - 8.0.x</td>
<td>Required if MySQL is used as Zabbix backend database. InnoDB engine is required. MariaDB also works with Zabbix. For MySQL we recommend using the C API (libmysqlclient) library for building server/proxy. For MariaDB we recommend using the MariaDB Connector/C library for building server/proxy.</td>
</tr>
<tr>
<td>Oracle</td>
<td>10g or later</td>
<td>Required if Oracle is used as Zabbix backend database.</td>
</tr>
<tr>
<td>PostgreSQL</td>
<td>8.1 or later</td>
<td>Required if PostgreSQL is used as Zabbix backend database. It is suggested to use at least PostgreSQL 8.3, which introduced much better VACUUM performance.</td>
</tr>
<tr>
<td>IBM DB2</td>
<td>9.7 or later</td>
<td>Required if IBM DB2 is used as Zabbix backend database.</td>
</tr>
<tr>
<td>SQLite</td>
<td>3.3.5 or later</td>
<td>SQLite is only supported with Zabbix proxies. Required if SQLite is used as Zabbix proxy database.</td>
</tr>
</tbody>
</table>

**Attention:**
IBM DB2 support is experimental!

Frontend

The following software is required to run Zabbix frontend:

<table>
<thead>
<tr>
<th>Software</th>
<th>Version</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache</td>
<td>1.3.12 or later</td>
<td>PHP 8.0 is not supported.</td>
</tr>
<tr>
<td>PHP</td>
<td>5.4.0 or later</td>
<td>PHP GD extension must support PNG images (--with-png-dir), JPEG (--with-jpeg-dir) images and FreeType 2 (--with-freetype-dir).</td>
</tr>
<tr>
<td>PHP extensions:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>gd</td>
<td>2.0 or later</td>
<td>php-bcmath (--enable-bcmath)</td>
</tr>
<tr>
<td>bcmath</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ctype</td>
<td></td>
<td>php-ctype (--enable-ctype)</td>
</tr>
<tr>
<td>libXML</td>
<td>2.6.15 or later</td>
<td>php-xml or php5-dom, if provided as a separate package by the distributor.</td>
</tr>
<tr>
<td>xmlreader</td>
<td></td>
<td>php-xmireader, if provided as a separate package by the distributor.</td>
</tr>
<tr>
<td>xmlwriter</td>
<td></td>
<td>php-xmlwriter, if provided as a separate package by the distributor.</td>
</tr>
<tr>
<td>session</td>
<td></td>
<td>php-session, if provided as a separate package by the distributor.</td>
</tr>
<tr>
<td>sockets</td>
<td></td>
<td>php-net-socket (--enable-sockets). Required for user script support.</td>
</tr>
<tr>
<td>mbstring</td>
<td></td>
<td>php-mbstring (--enable-mbstring)</td>
</tr>
<tr>
<td>gettext</td>
<td></td>
<td>php-gettext (--with-gettext). Required for translations to work.</td>
</tr>
<tr>
<td>ldap</td>
<td></td>
<td>php-ldap. Required only if LDAP authentication is used in the frontend.</td>
</tr>
<tr>
<td>ibm_db2</td>
<td></td>
<td>Required if IBM DB2 is used as Zabbix backend database.</td>
</tr>
</tbody>
</table>
Software | Version | Comments
---|---|---
mysqli | | Required if MySQL is used as Zabbix backend database.
oici8 | | Required if Oracle is used as Zabbix backend database.
pgresql | | Required if PostgreSQL is used as Zabbix backend database.

**Note:**
Zabbix may work on previous versions of Apache, MySQL, Oracle, and PostgreSQL as well.

**Attention:**
For other fonts than the default DejaVu, PHP function `imagerotate` might be required. If it is missing, these fonts might be rendered incorrectly when a graph is displayed. This function is only available if PHP is compiled with bundled GD, which is not the case in Debian and other distributions.

Web browser on client side
Cookies and Java Script must be enabled.

The latest stable versions of Google Chrome, Mozilla Firefox, Microsoft Internet Explorer and Opera are supported. Other browsers (Apple Safari, Konqueror) may work with Zabbix as well.

**Warning:**
The same origin policy for iFrames is implemented, which means that Zabbix cannot be placed in frames on a different domain.

Still, pages placed into a Zabbix frame will have access to Zabbix frontend (through JavaScript) if the page that is placed in the frame and Zabbix frontend are on the same domain. A page like `http://secure-zabbix.com/cms/page.html`, if placed into screens or dashboards on `http://secure-zabbix.com/zabbix/`, will have full JS access to Zabbix.

Server
Mandatory requirements are needed always. Optional requirements are needed for the support of the specific function.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>libpcre</td>
<td>Mandatory</td>
<td>PCRE library is required for Perl Compatible Regular Expression (PCRE) support. The naming may differ depending on the GNU/Linux distribution, for example ‘libpcre3’ or ‘libpcre1’. Note that you need exactly PCRE (v8.x); PCRE2 (v10.x) library is not used.</td>
</tr>
<tr>
<td>libevent</td>
<td></td>
<td>Required for bulk metric support and IPMI monitoring. Version 1.4 or higher. Note that for Zabbix proxy this requirement is optional; it is needed for IPMI monitoring support.</td>
</tr>
<tr>
<td>libpthread</td>
<td></td>
<td>Required for mutex and read-write lock support.</td>
</tr>
<tr>
<td>zlib</td>
<td></td>
<td>Required for compression support.</td>
</tr>
<tr>
<td>OpenIPMI</td>
<td>Optional</td>
<td>Required for IPMI support.</td>
</tr>
<tr>
<td>libssh2 or libssh</td>
<td></td>
<td>Required for SSH checks. Version 1.0 or higher (libssh2); 0.6.0 or higher (libssh). libssh is supported since Zabbix 4.0.18.</td>
</tr>
<tr>
<td>fping</td>
<td></td>
<td>Required for ICMP ping items.</td>
</tr>
</tbody>
</table>
### Zabbix Dependencies

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>libcurl</td>
<td></td>
<td>Required for web monitoring, VMware monitoring, SMTP authentication, web.page. <em>Zabbix agent items</em>, HTTP agent items and Elasticsearch (if used). Version 7.28.0 or higher is recommended. Libcurl version requirements: - SMTP authentication: version 7.20.0 or higher - Elasticsearch: version 7.28.0 or higher</td>
</tr>
<tr>
<td>libiksemel</td>
<td></td>
<td>Required for Jabber support.</td>
</tr>
<tr>
<td>libxml2</td>
<td></td>
<td>Required for VMware monitoring and XML XPath preprocessing.</td>
</tr>
<tr>
<td>net-snmp</td>
<td></td>
<td>Required for SNMP support.</td>
</tr>
<tr>
<td>GnuTLS, OpenSSL, LibreSSL or mbed TLS</td>
<td></td>
<td>Required when using encryption.</td>
</tr>
</tbody>
</table>

### Agent Dependencies

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>libpcre</td>
<td>Mandatory</td>
<td>PCRE library is required for Perl Compatible Regular Expression (PCRE) support. The naming may differ depending on the GNU/Linux distribution, for example 'libpcre3' or 'libpcre1'. Note that you need exactly PCRE (v8.x); PCRE2 (v10.x) library is not used.</td>
</tr>
<tr>
<td>GnuTLS, OpenSSL, LibreSSL or mbed TLS</td>
<td>Optional</td>
<td>Required when using encryption. On Microsoft Windows systems OpenSSL 1.1.1 or later is required.</td>
</tr>
</tbody>
</table>

### Java gateway

If you obtained Zabbix from the source repository or an archive, then the necessary dependencies are already included in the source tree.

If you obtained Zabbix from your distribution’s package, then the necessary dependencies are already provided by the packaging system.

In both cases above, the software is ready to be used and no additional downloads are necessary.

If, however, you wish to provide your versions of these dependencies (for instance, if you are preparing a package for some Linux distribution), below is the list of library versions that Java gateway is known to work with. Zabbix may work with other versions of these libraries, too.

The following table lists JAR files that are currently bundled with Java gateway in the original code:

<table>
<thead>
<tr>
<th>Library</th>
<th>License</th>
<th>Website</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>logback-core-1.2.3.jar</td>
<td>EPL 1.0, LGPL 2.1</td>
<td><a href="http://logback.qos.ch/">http://logback.qos.ch/</a></td>
<td>Tested with 0.9.27, 1.0.13, 1.1.1 and 1.2.3.</td>
</tr>
<tr>
<td>logback-classic-1.2.3.jar</td>
<td>EPL 1.0, LGPL 2.1</td>
<td><a href="http://logback.qos.ch/">http://logback.qos.ch/</a></td>
<td>Tested with 0.9.27, 1.0.13, 1.1.1 and 1.2.3.</td>
</tr>
<tr>
<td>slf4j-api-1.7.30.jar</td>
<td>MIT License</td>
<td><a href="http://www.slf4j.org/">http://www.slf4j.org/</a></td>
<td>Tested with 1.6.1, 1.6.6, 1.7.6 and 1.7.30.</td>
</tr>
<tr>
<td>android-json-4.3_r3.1.jar</td>
<td>Apache License 2.0</td>
<td><a href="https://android.googlesource.com/platform/libcore/+master/json">https://android.googlesource.com/platform/libcore/+master/json</a></td>
<td>Tested with 2.3.3_r1.1 and 4.3_r3.1. See src/zabbix_java/lib/README for instructions on creating a JAR file.</td>
</tr>
</tbody>
</table>

Java gateway compiles and runs with Java 1.6 and above. It is recommended that those who provide a precompiled version of the gateway for others use Java 1.6 for compilation, so that it runs on all versions of Java up to the latest one.

Default port numbers

---

64
The following table lists default port numbers that Zabbix components listen on:

<table>
<thead>
<tr>
<th>Zabbix component</th>
<th>Port number</th>
<th>Protocol</th>
<th>Type of connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zabbix agent</td>
<td>10050</td>
<td>TCP</td>
<td>on demand</td>
</tr>
<tr>
<td>Zabbix server</td>
<td>10051</td>
<td>TCP</td>
<td>on demand</td>
</tr>
<tr>
<td>Zabbix proxy</td>
<td>10051</td>
<td>TCP</td>
<td>on demand</td>
</tr>
<tr>
<td>Zabbix Java gateway</td>
<td>10052</td>
<td>TCP</td>
<td>on demand</td>
</tr>
</tbody>
</table>

Database size

Zabbix configuration data require a fixed amount of disk space and do not grow much.

Zabbix database size mainly depends on these variables, which define the amount of stored historical data:

- Number of processed values per second

This is the average number of new values Zabbix server receives every second. For example, if we have 3000 items for monitoring with refresh rate of 60 seconds, the number of values per second is calculated as 3000/60 = 50.

It means that 50 new values are added to Zabbix database every second.

- Housekeeper settings for history

Zabbix keeps values for a fixed period of time, normally several weeks or months. Each new value requires a certain amount of disk space for data and index.

So, if we would like to keep 30 days of history and we receive 50 values per second, total number of values will be around 

\[(30\times24\times3600)\times50 = 129.600.000\], or about 130M of values.

Depending on the database engine used, type of received values (floats, integers, strings, log files, etc), the disk space for keeping a single value may vary from 40 bytes to hundreds of bytes. Normally it is around 90 bytes per value for numeric items. In our case, it means that 130M of values will require 130M \(\times 90\) bytes = 10.9GB of disk space.

Note:
The size of text/log item values is impossible to predict exactly, but you may expect around 500 bytes per value.

- Housekeeper setting for trends

Zabbix keeps a 1-hour max/min/avg/count set of values for each item in the table trends. The data is used for trending and long period graphs. The one hour period cannot be customized.

Zabbix database, depending on database type, requires about 90 bytes per each total. Suppose we would like to keep trend data for 5 years. Values for 3000 items will require \(3000\times24\times365\times90 = 2.2GB\) per year, or \(11GB\) for 5 years.

- Housekeeper settings for events

Each Zabbix event requires approximately 250 bytes of disk space. It is hard to estimate the number of events generated by Zabbix daily. In the worst case scenario, we may assume that Zabbix generates one event per second.

For each recovered event an event_recovery record is created. Normally most of events will be recovered so we can assume one event_recovery record per event. That means additional 80 bytes per event.

Optionally events can have tags, each tag record requiring approximately 100 bytes of disk space. The number of tags per event (#tags) depends on configuration. So each will need an additional #tags * 100 bytes of disk space.

It means that if we want to keep 3 years of events, this would require \(3\times365\times24\times3600\times(250+80+\#tags*100) = \sim 30GB + \#tags*100\) disk space.

Note:
1. More when having non-ASCII event names, tags and values.
2. The size approximations are based on MySQL and might be different for other databases.

The table contains formulas that can be used to calculate the disk space required for Zabbix system:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Formula for required disk space (in bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zabbix configuration</td>
<td>Fixed size. Normally 10MB or less.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Formula for required disk space (in bytes)</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>History</td>
<td>days*(items/refresh rate)<em>24</em>3600*bytes</td>
</tr>
<tr>
<td></td>
<td>items : number of items</td>
</tr>
<tr>
<td></td>
<td>days : number of days to keep history</td>
</tr>
<tr>
<td></td>
<td>refresh rate : average refresh rate of items</td>
</tr>
<tr>
<td></td>
<td>bytes : number of bytes required to keep single value, depends on database engine, normally ~90 bytes.</td>
</tr>
<tr>
<td>Trends</td>
<td>days*(items/3600)<em>24</em>3600*bytes</td>
</tr>
<tr>
<td></td>
<td>items : number of items</td>
</tr>
<tr>
<td></td>
<td>days : number of days to keep history</td>
</tr>
<tr>
<td></td>
<td>bytes : number of bytes required to keep single trend, depends on database engine, normally ~90 bytes.</td>
</tr>
<tr>
<td>Events</td>
<td>days<em>events</em>24<em>3600</em>bytes</td>
</tr>
<tr>
<td></td>
<td>events : number of event per second. One (1) event per second in worst case scenario.</td>
</tr>
<tr>
<td></td>
<td>days : number of days to keep history</td>
</tr>
<tr>
<td></td>
<td>bytes : number of bytes required to keep single trend, depends on database engine, normally ~330 + average number of tags per event * 100 bytes.</td>
</tr>
</tbody>
</table>

So, the total required disk space can be calculated as:

**Configuration + History + Trends + Events**

The disk space will NOT be used immediately after Zabbix installation. Database size will grow then it will stop growing at some point, which depends on housekeeper settings.

**Time synchronization**

It is very important to have precise system time on server with Zabbix running. **ntpd** is the most popular daemon that synchronizes the host’s time with the time of other machines. It’s strongly recommended to maintain synchronized system time on all systems Zabbix components are running on.

**Best practices for secure Zabbix setup**

**Overview**

This section contains best practices that should be observed in order to set up Zabbix in a secure way.

The practices contained here are not required for the functioning of Zabbix. They are recommended for better security of the system.

**Access control**

**Principle of least privilege**

The principle of least privilege should be used at all times for Zabbix. This principle means that user accounts (in Zabbix frontend) or process user (for Zabbix server/proxy or agent) have only those privileges that are essential to perform intended functions. In other words, user accounts at all times should run with as few privileges as possible.

**Attention:**

Giving extra permissions to ‘zabbix’ user will allow it to access configuration files and execute operations that can compromise the overall security of the infrastructure.

When implementing the least privilege principle for user accounts, Zabbix **frontend user types** should be taken into account. It is important to understand that while a “Admin” user type has less privileges than “Super Admin” user type, it has administrative permissions that allow managing configuration and execute custom scripts.

**Note:**

Some information is available even for non-privileged users. For example, while Administration → Scripts is not available for non-Super Admins, scripts themselves are available for retrieval by using Zabbix API. Limiting script permissions and not adding sensitive information (like access credentials, etc) should be used to avoid exposure of sensitive information available in global scripts.

**Secure user for Zabbix agent**

In the default configuration, Zabbix server and Zabbix agent processes share one ‘zabbix’ user. If you wish to make sure that the agent cannot access sensitive details in server configuration (e.g. database login information), the agent should be run as a different user:
1. Create a secure user
2. Specify this user in the agent configuration file (‘User’ parameter)
3. Restart the agent with administrator privileges. Privileges will be dropped to the specified user.

Revoke write access to SSL configuration file in Windows

Zabbix Windows agent compiled with OpenSSL will try to reach the SSL configuration file in c:\openssl-64bit. The "openssl-64bit" directory on disk C: can be created by non-privileged users.

So for security hardening, it is required to create this directory manually and revoke write access from non-admin users.

Please note that the directory names will be different on 32-bit and 64-bit versions of Windows.

Cryptography

Setting up SSL for Zabbix frontend

On RHEL/Centos, install mod_ssl package:

```
yum install mod_ssl
```

Create directory for SSL keys:

```
mkdir -p /etc/httpd/ssl/private
chmod 700 /etc/httpd/ssl/private
```

Create SSL certificate:

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/httpd/ssl/private/apache-selfsigned.key -out /etc/httpd/ssl/apache-selfsigned.crt
```

Fill out the prompts appropriately. The most important line is the one that requests the Common Name. You need to enter the domain name that you want to be associated with your server. You can enter the public IP address instead if you do not have a domain name. We will use example.com in this article.

```
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 []:
```

Edit Apache SSL configuration:

```
/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
```

Restart the Apache service to apply the changes:

```
systemctl restart httpd.service
```

Web server hardening

Enabling Zabbix on root directory of URL

Add a virtual host to Apache configuration and set permanent redirect for document root to Zabbix SSL URL. Do not forget to replace example.com with the actual name of the server.

```
/etc/httpd/conf/httpd.conf
```

```
#Add lines

<VirtualHost *:*
  ServerName example.com
  Redirect permanent / https://example.com
</VirtualHost>
```

Restart the Apache service to apply the changes:

```
systemctl restart httpd.service
```
Enabling HTTP Strict Transport Security (HSTS) on the web server

**HSTS** is enforced by Zabbix frontend in versions 4.0.0 - 4.0.2.

Starting with **4.0.3** to protect Zabbix frontend against protocol downgrade attacks, we recommend to enable **HSTS** policy on the web server.

For example, to enable HSTS policy for your Zabbix frontend in Apache configuration:

/etc/httpd/conf/httpd.conf

add the following directive to your virtual host's configuration:

```html
<VirtualHost *:443>
    Header set Strict-Transport-Security "max-age=31536000"
</VirtualHost>
```

Restart the Apache service to apply the changes:

```bash
systemctl restart httpd.service
```

Disabling web server information exposure

It is recommended to disable all web server signatures as part of the web server hardening process. The web server is exposing software signature by default:

```
Response Headers

Cache-Control: no-store, no-cache, must-revalidate
Connection: Keep-Alive
Content-Encoding: gzip
Content-Length: 1160
Content-Type: text/html; charset=UTF-8
Keep-Alive: timeout=5, max=100
Pragma: no-cache
Server: Apache/2.4.18 (Ubuntu)
```

The signature can be disabled by adding two lines to the Apache (used as an example) configuration file:

```bash
ServerSignature Off
ServerTokens Prod
```

PHP signature (X-Powered-By HTTP header) can be disabled by changing the php.ini configuration file (signature is disabled by default):

```bash
expose_php = Off
```

Web server restart is required for configuration file changes to be applied.

Additional security level can be achieved by using the **mod_security** (package libapache2-mod-security2) with Apache. **mod_security** allows to remove server signature instead of only removing version from server signature. Signature can be altered to any value by changing "SecServerSignature" to any desired value after installing **mod_security**.

Please refer to documentation of your web server to find help on how to remove/change software signatures.

Disabling default web server error pages

It is recommended to disable default error pages to avoid information exposure. Web server is using built-in error pages by default:
Default error pages should be replaced/removed as part of the web server hardening process. The "ErrorDocument" directive can be used to define a custom error page/text for Apache web server (used as an example).

Please refer to documentation of your web server to find help on how to replace/remove default error pages.

Removing web server test page

It is recommended to remove the web server test page to avoid information exposure. By default, web server webroot contains a test page called index.html (Apache2 on Ubuntu is used as an example):

![Apache2 Ubuntu Default Page](image)

The test page should be removed or should be made unavailable as part of the web server hardening process.

Set X-Frame-Options HTTP response header

By default, Zabbix is configured with X-Frame-Options HTTP response header set to SAMEORIGIN, meaning that content can only be loaded in a frame that has the same origin as the page itself.

Zabbix frontend elements that pull content from external URLs (namely, the URL dashboard widget) display retrieved content in a sandbox with all sandboxing restrictions enabled.

These settings enhance the security of the Zabbix frontend and provide protection against XSS and clickjacking attacks. Super Admins can modify iframe sandboxing and X-Frame-Options HTTP response header parameters as needed. Please carefully weigh the risks and benefits before changing default settings. Turning sandboxing or X-Frame-Options off completely is not recommended.

Hiding the file with list of common passwords

To increase the complexity of password brute force attacks, it is suggested to limit access to the file /data/top_passwords.txt by modifying web server configuration. This file contains a list of the most common and context-specific passwords, and is used to prevent users from setting such passwords if Avoid easy-to-guess passwords parameter is enabled in the password policy.

For example, on NGINX file access can be limited by using the location directive:

```
location = /data/top_passwords.txt {
    deny all;
    return 404;
}
```

On Apache - by using .htaccess file:

```
<Files "top_passwords.txt">
    Order Allow,Deny
    Deny from all
</Files>
```
3 Installation from sources

You can get the very latest version of Zabbix by compiling it from the sources.

A step-by-step tutorial for installing Zabbix from the sources is provided here.

1 Installing Zabbix daemons

1 Download the source archive

Go to the Zabbix download page and download the source archive. Once downloaded, extract the sources, by running:

```
$ tar -zxvf zabbix-4.0.0.tar.gz
```

**Note:** Enter the correct Zabbix version in the command. It must match the name of the downloaded archive.

2 Create user account

For all of the Zabbix daemon processes, an unprivileged user is required. If a Zabbix daemon is started from an unprivileged user account, it will run as that user.

However, if a daemon is started from a 'root' account, it will switch to a 'zabbix' user account, which must be present. To create such a user account (in its own group, "zabbix"),

on a RedHat-based system, run:

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

on a Debian-based system, run:

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

**Attention:**

Zabbix processes do not need a home directory, which is why we do not recommend creating it. However, if you are using some functionality that requires it (e. g. store MySQL credentials in $HOME/.my.cnf) you are free to create it using the following commands.

On RedHat-based systems, run:
```
mkdir -m u=rwx,g=rwx,o= -p /usr/lib/zabbix
chown zabbix:zabbix /usr/lib/zabbix
```

On Debian-based systems, run:
```
mkdir -m u=rwx,g=rwx,o= -p /var/lib/zabbix
chown zabbix:zabbix /var/lib/zabbix
```

A separate user account is not required for Zabbix frontend installation.

If Zabbix server and agent are run on the same machine it is recommended to use a different user for running the server than for running the agent. Otherwise, if both are run as the same user, the agent can access the server configuration file and any Admin level user in Zabbix can quite easily retrieve, for example, the database password.
3 Create Zabbix database

For Zabbix server and proxy daemons, as well as Zabbix frontend, a database is required. It is not needed to run Zabbix agent.

SQL scripts are provided for creating database schema and inserting the dataset. Zabbix proxy database needs only the schema while Zabbix server database requires also the dataset on top of the schema.

Having created a Zabbix database, proceed to the following steps of compiling Zabbix.

4 Configure the sources

When configuring the sources for a Zabbix server or proxy, you must specify the database type to be used. Only one database type can be compiled with a server or proxy process at a time.

To see all of the supported configuration options, inside the extracted Zabbix source directory run:

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

To configure the sources for a Zabbix server and agent, you may run something like:

```
./configure --enable-server --enable-agent --with-mysql --enable-ipv6 --with-net-snmp --with-libcurl --with-libxml2 --with-openipmi
```

**Note:**

For virtual machine monitoring --with-libcurl and --with-libxml2 configuration options are required; --with-libcurl is also required for SMTP authentication and web.page.* Zabbix agent items. Note that cURL 7.20.0 or higher is required with the --with-libcurl configuration option.

To configure the sources for a Zabbix server (with PostgreSQL etc.), you may run:

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

To configure the sources for a Zabbix proxy (with SQLite etc.), you may run:

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

To configure the sources for a Zabbix agent, you may run:

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

You may use the --enable-static flag to statically link libraries. If you plan to distribute compiled binaries among different servers, you must use this flag to make these binaries work without required libraries. Note that --enable-static does not work under Solaris.

**Attention:**

Using --enable-static option is not recommended when building server.

In order to build the server statically you must have a static version of every external library needed. There is no strict check for that in configure script.

**Attention:**

If ./configure fails due to missing libraries or some other circumstance, please take a look at the config.log file for more detailed error description. For example, if we have missing libssl, the error message may be misleading:

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

But, if we look at config.log, it has a more detailed description for configuration failure:

```
/usr/bin/ld: cannot find -lssl
/usr/bin/ld: cannot find -lcrypto
```
Command-line utilities `zabbix_get` and `zabbix_sender` are compiled if `--enable-agent` option is used.

Add optional path to the MySQL configuration file `--with-mysql=/<path_to_the_file>/mysql_config` to select the desired MySQL client library when there is a need to use one that is not located in the default location. It is useful when there are several versions of MySQL installed or MariaDB installed alongside MySQL on the same system.

Use `--with-ibm-db2` flag to specify location of the CLI API.

Use `--with-oracle` flag to specify location of the OCI API.

For encryption support see [Compiling Zabbix with encryption support](#).

See also: [known issues](#) with compiling Zabbix agent on HP-UX.

5 Make and install everything

If installing from git, it is required to run first:

```shell
$ make dbschema
```

This step should be run as a user with sufficient permissions (commonly ‘root’, or by using `sudo`).

Running `make install` will by default install the daemon binaries (`zabbix_server`, `zabbix_agentd`, `zabbix_proxy`) in `/usr/local/sbin` and the client binaries (`zabbix_get`, `zabbix_sender`) in `/usr/local/bin`.

To specify a different location than `/usr/local`, use a `--prefix` key in the previous step of configuring sources, for example `--prefix=/home/zabbix`. In this case daemon binaries will be installed under `<prefix>/sbin`, while utilities under `<prefix>/bin`. Man pages will be installed under `<prefix>/share`.

6 Review and edit configuration files

• edit the Zabbix agent configuration file `/usr/local/etc/zabbix_agentd.conf`

You need to configure this file for every host with `zabbix_agentd` installed.

You must specify the Zabbix server IP address in the file. Connections from other hosts will be denied.

• edit the Zabbix server configuration file `/usr/local/etc/zabbix_server.conf`

You must specify the database name, user and password (if using any).

The rest of the parameters will suit you with their defaults if you have a small installation (up to ten monitored hosts). You should change the default parameters if you want to maximize the performance of Zabbix server (or proxy) though.

• if you have installed a Zabbix proxy, edit the proxy configuration file `/usr/local/etc/zabbix_proxy.conf`

You must specify the server IP address and proxy hostname (must be known to the server), as well as the database name, user and password (if using any).

With SQLite the full path to database file must be specified; DB user and password are not required.

7 Start up the daemons

Run `zabbix_server` on the server side.

```shell
shell> zabbix_server
```
Note:
Make sure that your system allows allocation of 36MB (or a bit more) of shared memory, otherwise the server may not start and you will see "Cannot allocate shared memory for <type of cache>." in the server log file. This may happen on FreeBSD, Solaris 8.
See the "See also" section at the bottom of this page to find out how to configure shared memory.

Run zabbix_agentd on all the monitored machines.

```
shell> zabbix_agentd
```

Note:
Make sure that your system allows allocation of 2MB of shared memory, otherwise the agent may not start and you will see "Cannot allocate shared memory for collector." in the agent log file. This may happen on Solaris 8.

If you have installed Zabbix proxy, run zabbix_proxy.

```
shell> zabbix_proxy
```

2 Installing Zabbix web interface

Copying PHP files

Zabbix frontend is written in PHP, so to run it a PHP supported webserver is needed. Installation is done by simply copying the PHP files from frontends/php to the webserver HTML documents directory.

Common locations of HTML documents directories for Apache web servers include:

- `/usr/local/apache2/htdocs` (default directory when installing Apache from source)
- `/srv/www/htdocs` (OpenSUSE, SLES)
- `/var/www/html` (Debian, Ubuntu, Fedora, RHEL, CentOS)

It is suggested to use a subdirectory instead of the HTML root. To create a subdirectory and copy Zabbix frontend files into it, execute the following commands, replacing the actual directory:

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

If planning to use any other language than English, see Installation of additional frontend languages for instructions.

Note:
In Zabbix 4.0.8 (only) the web server user requires write permissions to the assets directory.

Installing frontend

Step 1

In your browser, open Zabbix URL: http://<server_ip_or_name>/zabbix

You should see the first screen of the frontend installation wizard.
Step 2

Make sure that all software prerequisites are met.

<table>
<thead>
<tr>
<th>Pre-requisite</th>
<th>Minimum value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PHP version</td>
<td>5.4.0</td>
<td></td>
</tr>
<tr>
<td>PHP memory_limit option</td>
<td>128MB</td>
<td>In php.ini: memory_limit = 128M</td>
</tr>
<tr>
<td>PHP post_max_size option</td>
<td>16MB</td>
<td>In php.ini: post_max_size = 16M</td>
</tr>
<tr>
<td>PHP upload_max_filesize option</td>
<td>2MB</td>
<td>In php.ini: upload_max_filesize = 2M</td>
</tr>
<tr>
<td>PHP max_execution_time option</td>
<td>300 seconds (values 0 and -1 are allowed)</td>
<td>In php.ini: max_execution_time = 300</td>
</tr>
<tr>
<td>PHP max_input_time option</td>
<td>300 seconds (values 0 and -1 are allowed)</td>
<td>In php.ini: max_input_time = 300</td>
</tr>
<tr>
<td>PHP session.auto_start option</td>
<td>must be disabled</td>
<td>In php.ini: session.auto_start = 0</td>
</tr>
<tr>
<td>Pre-requisite</td>
<td>Minimum value</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Database support</td>
<td>One of: MySQL, Oracle, PostgreSQL, IBM DB2</td>
<td>One of the following modules must be installed: mysql, oci8, pgsq1, ibm_db2</td>
</tr>
<tr>
<td>bcmath</td>
<td></td>
<td>php-bcmath</td>
</tr>
<tr>
<td>mbstring</td>
<td></td>
<td>php-mbstring</td>
</tr>
<tr>
<td>PHP mbstring.func_overload option</td>
<td>must be disabled</td>
<td>In php.ini: mbstring.func_overload = 0</td>
</tr>
<tr>
<td>PHP always_populate_raw_post_data</td>
<td>must be disabled</td>
<td>Required only for PHP versions 5.6.0 or newer.</td>
</tr>
<tr>
<td>option</td>
<td></td>
<td>In php.ini: always_populate_raw_post_data = -1</td>
</tr>
<tr>
<td>sockets</td>
<td></td>
<td>php-net-socket. Required for user script support.</td>
</tr>
<tr>
<td>gd</td>
<td>2.0 or higher</td>
<td>php-gd. PHP GD extension must support PNG images (--with-png-dir), JPEG (--with-jpeg-dir) images and FreeType 2 (--with-freetype-dir).</td>
</tr>
<tr>
<td>libxml</td>
<td>2.6.15</td>
<td>php-xml or php5-dom</td>
</tr>
<tr>
<td>xmlwriter</td>
<td></td>
<td>php-xmlwriter</td>
</tr>
<tr>
<td>xmlreader</td>
<td></td>
<td>php-xmireader</td>
</tr>
<tr>
<td>ctype</td>
<td></td>
<td>php-ctype</td>
</tr>
<tr>
<td>session</td>
<td></td>
<td>php-session</td>
</tr>
<tr>
<td>gettext</td>
<td></td>
<td>php-gettext</td>
</tr>
</tbody>
</table>

Since Zabbix 2.2.1, the PHP gettext extension is not a mandatory requirement for installing Zabbix. If gettext is not installed, the frontend will work as usual, however, the translations will not be available.

Optional pre-requisites may also be present in the list. A failed optional prerequisite is displayed in orange and has a Warning status. With a failed optional pre-requisite, the setup may continue.

**Attention:**
If there is a need to change the Apache user or user group, permissions to the session folder must be verified. Otherwise Zabbix setup may be unable to continue.

Step 3
Enter details for connecting to the database. Zabbix database must already be created.
Step 4

Enter Zabbix server details.

Entering a name for Zabbix server is optional, however, if submitted, it will be displayed in the menu bar and page titles.

Step 5

Review a summary of settings.
Step 6

Download the configuration file and place it under conf/ in the webserver HTML documents subdirectory where you copied Zabbix PHP files to.
Step 7

Finish the installation.

Step 8

Zabbix frontend is ready! The default user name is **Admin**, password **zabbix**.

Proceed to **getting started with Zabbix**.

3 Installing Java gateway

It is required to install Java gateway only if you want to monitor JMX applications. Java gateway is lightweight and does not require a database.
To install from sources, first download and extract the source archive.

To compile Java gateway, run the `./configure` script with `--enable-java` option. It is advisable that you specify the `--prefix` option to request installation path other than the default `/usr/local`, because installing Java gateway will create a whole directory tree, not just a single executable.

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

To compile and package Java gateway into a JAR file, run `make`. Note that for this step you will need `javac` and `jar` executables in your path.

```
$ make
```

Now you have a `zabbix-java-gateway-$VERSION.jar` file in `src/zabbix_java/bin`. If you are comfortable with running Java gateway from `src/zabbix_java` in the distribution directory, then you can proceed to instructions for configuring and running Java gateway. Otherwise, make sure you have enough privileges and run `make install`.

```
$ make install
```

Proceed to setup for more details on configuring and running Java gateway.

### Building Windows agent binaries with/without TLS

#### Overview

This section demonstrates how to build Windows agent binaries from sources with or without TLS.

#### Compiling OpenSSL

The following steps will help you to compile OpenSSL from sources on MS Windows 10 (64-bit).

1. For compiling OpenSSL you will need on Windows machine:
   1. C compiler (e.g. VS 2017 RC),
   2. NASM [https://www.nasm.us/](https://www.nasm.us/),
   3. Perl (e.g. Strawberry Perl from [http://strawberryperl.com/](http://strawberryperl.com/)),
   4. Perl module Text::Template (cpan Text::Template).
2. Get OpenSSL sources from [https://www.openssl.org/](https://www.openssl.org/). OpenSSL 1.1.1 is used here.
3. Unpack OpenSSL sources, for example, in E:\openssl-1.1.1.
4. Open a command line window e.g. the x64 Native Tools Command Prompt for VS 2017 RC.
5. Go to the OpenSSL source directory, e.g. E:\openssl-1.1.1.
   1. Verify that NASM can be found:
      ```
      e:\openssl-1.1.1> nasm --version
      NASM version 2.13.01 compiled on May 1 2017
      ```
6. Configure OpenSSL, for example:
      ```
      e:\openssl-1.1.1> perl E:\openssl-1.1.1\Configure VC-WIN64A no-shared no-capieng no-gost no-dgram no-dtls1-method no-dtls1_2-method --api=1.1.0 --prefix=C:\OpenSSL-Win64-111-static
      ```
      - Note the option ‘no-shared’: if ‘no-shared’ is used then the OpenSSL static libraries libcrypto.lib and libssl.lib will be ‘self-sufficient’ and resulting Zabbix binaries will include OpenSSL in themselves, no need for external OpenSSL DLLs. Advantage: Zabbix binaries can be copied to other Windows machines without OpenSSL libraries. Disadvantage: when a new OpenSSL bugfix version is released, Zabbix agent needs to be recompiled and reinstalled.
      - If ‘no-shared’ is not used, then the static libraries libcrypto.lib and libssl.lib will be using OpenSSL DLLs at runtime. Advantage: when a new OpenSSL bugfix version is released, probably you can upgrade only OpenSSL DLLs, without recompiling Zabbix agent. Disadvantage: copying Zabbix agent to another machine requires copying OpenSSL DLLs, too.
7. Compile OpenSSL, run tests, install:
      ```
      e:\openssl-1.1.1> nmake
      e:\openssl-1.1.1> nmake test
      All tests successful.
      Files=152, Tests=1152, 501 wallclock secs ( 0.67 usr + 0.61 sys = 1.28 CPU) Result: PASS
      e:\openssl-1.1.1> nmake install_sw
      ```
      *install_sw* installs only software components (i.e. libraries, header files, but no documentation). If you want everything, use “nmake install”.

#### Compiling PCRE

1. Download the PCRE (not PCRE2) library (new mandatory library since Zabbix 4.0) from [http://pcre.org/](http://pcre.org/).
2. Extract to directory E:\pcre-8.41.
3. Install CMake from [https://cmake.org/download/](https://cmake.org/download/), during install select: and ensure that cmake\bin is on your path (tested version 3.9.4).
4. Create a new, empty build directory, preferably a subdirectory of the source dir. For example, E:\pcre-8.41\build.
5. Open a commandline window e.g. the x64 Native Tools Command Prompt for VS 2017 and from that shell environment run cmake-gui. Do not try to start Cmake from the Windows Start menu, as this can lead to errors.
6. Enter E:\pcre-8.41 and E:\pcre-8.41\build for the source and build directories, respectively.
7. Hit the "Configure" button.
When specifying the generator for this project select "NMake Makefiles".

Create a new, empty install directory. For example, E:\pcre-8.41-install.

The GUI will then list several configuration options. Make sure the following options are selected:
- PCRE_SUPPORT_UNICODE_PROPERTIES ON
- PCRE_SUPPORT_UTF ON
- CMAKE_INSTALL_PREFIX E:\pcre-8.41-install

Hit "Configure" again. The adjacent "Generate" button should now be active.

Hit "Generate".

In the event that errors do occur, it is recommended that you delete the CMake cache before attempting to repeat the CMake build process. In the CMake GUI, the cache can be deleted by selecting "File > Delete Cache".

The build directory should now contain a usable build system - Makefile.

Open a commandline window e.g. the x64 Native Tools Command Prompt for VS 2017 and navigate to the Makefile mentioned above.

Run NMake command: E:\pcre-8.41\build nmake install

Compiling Zabbix

The following steps will help you to compile Zabbix from sources on MS Windows 10 (64-bit). When compiling Zabbix with/without TLS support the only significant difference is in step 4.

Support for OpenSSL 1.1.1 was added in 4.0.1, some additional fixes - in 4.0.2rc1.

1. On a Linux machine check out the source from git:

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

   $ cd zabbix

   $ git checkout 4.0.22 -b 4.0.22 # replace 4.0.22 with the latest release available

   $ ./bootstrap.sh

   $ ./configure --enable-agent --enable-ipv6 --prefix=`pwd`

   $ make dbschema

   $ make dist

2. Copy and unpack the archive, e.g. zabbix-4.0.2.tar.gz, on a Windows machine.

3. Let’s assume that sources are in e:\zabbix-4.0.2. Open a commandline window e.g. the x64 Native Tools Command Prompt for VS 2017 RC. Go to E:\zabbix-4.0.2\build\win32\project.

   - without TLS: E:\zabbix-4.0.2\build\win32\project> nmake /K PCREINCDIR=E:\pcre-8.41-install\include PCRELIBDIR=E:\pcre-8.41-install\lib
   - with TLS: E:\zabbix-4.0.2\build\win32\project> nmake /K -f Makefile_get TLS=openssl TLSINCDIR=C:\OpenSSL-Win64-111-static\include PCREINCDIR=E:\pcre-8.41-install\include PCRELIBDIR=E:\pcre-8.41-install\lib

5. New binaries are located in e:\zabbix-4.0.2\bin\win64. Since OpenSSL was compiled with 'no-shared' option, Zabbix binaries contain OpenSSL within themselves and can be copied to other machines that do not have OpenSSL.

Compiling Zabbix with LibreSSL

The process is similar to compiling with OpenSSL, but you need to make small changes in files located in the build\win32\project directory:

* In "Makefile_tls" delete "'/DHAVE_OPENSSL_WITH_PSK'". i.e. find

   CFLAGS = $(CFLAGS) /DHAVE_OPENSSL /DHAVE_OPENSSL_WITH_PSK</code>

   and replace it with

   CFLAGS = $(CFLAGS)

   /DHAVE_OPENSSL

* In "Makefile_common.inc" add "'/NODEFAULTLIB:LIBCMT'" i.e. find

   /MANIFESTUAC:"level='asInvoker' uiAccess='false'" /DYNAMICBASE:NO /PDB:$(TARGETDIR)$(TARGETNAME).pdb</code>

   and replace it with

   /MANIFESTUAC:"level='asInvoker' uiAccess='false'" /DYNAMICBASE:NO /PDB:$(TARGETDIR)$\$(TARGETNAME)\$/\$(TARGETNAME).pdb

   /NODEFAULTLIB:LIBCMT

4 Installation from packages

From Zabbix official repository

Zabbix SIA provides official RPM and DEB packages for:

- Red Hat Enterprise Linux/CentOS
- Debian/Ubuntu/Raspbian
- SUSE Linux Enterprise Server
Package files are available at repo.zabbix.com. Yum and apt repositories are also available on the server.

A step-by-step tutorial for installing Zabbix from packages is provided in sub-pages of this section.

Note, that though some OS distributions (in particular, Debian-based distributions) provide their own Zabbix packages, these packages are not supported by Zabbix. Zabbix packages provided by 3rd parties can be out of date and may lack the latest features and bug fixes. It is recommended to use only official packages from repo.zabbix.com. If you have previously used unofficial Zabbix packages, see notes about upgrading Zabbix packages from OS repositories.

### 1 Red Hat Enterprise Linux/CentOS

**Overview**

Official Zabbix 4.0 LTS packages for Red Hat Enterprise Linux, CentOS, and Oracle Linux are available on Zabbix website. Packages are available with either MySQL/PostgreSQL database and Apache web server support.

Zabbix agent packages and utilities Zabbix get and Zabbix sender are available on Zabbix Official Repository for RHEL 8, RHEL 7, RHEL 6, and RHEL 5.

Zabbix Official Repository provides fping, iksemel and libssh2 packages as well. These packages are located in the non-supported directory.

**Adding Zabbix repository**

Install the repository configuration package. This package contains yum (software package manager) configuration files.

**RHEL 7:**

```bash
# rpm -Uvh https://repo.zabbix.com/zabbix/4.0/rhel/7/x86_64/zabbix-release-4.0-1.el7.noarch.rpm
```

**RHEL 6:**

```bash
# rpm -Uvh https://repo.zabbix.com/zabbix/4.0/rhel/6/x86_64/zabbix-release-4.0-1.el6.noarch.rpm
```

**RHEL 5:**

```bash
# rpm -Uvh https://repo.zabbix.com/zabbix/4.0/rhel/5/x86_64/zabbix-release-4.0-1.noarch.rpm
```

**Frontend installation prerequisites**

Zabbix frontend requires additional packages not available in basic installation. You need to enable repository of optional rpms in the system you will run Zabbix frontend on:

**RHEL 7:**

```bash
# yum-config-manager --enable rhel-7-server-optional-rpms
```

**Server/proxy/frontend installation**

To install Zabbix server (available for RHEL 7, deprecated on RHEL 6) with MySQL support:

```bash
# yum install zabbix-server-mysql
```

To install Zabbix proxy with MySQL support:

```bash
# yum install zabbix-proxy-mysql
```

To install Zabbix frontend (available for RHEL 7, deprecated on RHEL 6) with MySQL support:

```bash
# yum install zabbix-web-mysql
```

Substitute ‘mysql’ in the commands with ‘pgsql’ to use PostgreSQL, or with ‘sqlite3’ to use SQLite3 (proxy only).

**Creating database**

For Zabbix server and proxy daemons a database is required. It is not needed to run Zabbix agent.

**Warning:**

Separate databases are needed for Zabbix server and Zabbix proxy; they cannot use the same database. Therefore, if they are installed on the same host, their databases must be created with different names!

Create the database using the provided instructions for MySQL or PostgreSQL.

**Importing data**

Now import initial schema and data for the server with MySQL:

```bash
[81]```
You will be prompted to enter your newly created database password.

With PostgreSQL:

```
# zcat /usr/share/doc/zabbix-server-pgsql*/create.sql.gz | sudo -u zabbix psql zabbix
```

For proxy, import initial schema:

```
# zcat /usr/share/doc/zabbix-proxy-pgsql*/schema.sql.gz | sudo -u zabbix psql zabbix
```

For proxy with PostgreSQL (or SQLite):

```
# zcat /usr/share/doc/zabbix-proxy-pgsql*/schema.sql.gz | sudo -u zabbix psql zabbix
# zcat /usr/share/doc/zabbix-proxy-sqlite3*/schema.sql.gz | sqlite3 zabbix.db
```

Configure database for Zabbix server/proxy

Edit `zabbix_server.conf` (and `zabbix_proxy.conf`) to use their respective databases. For example:

```
# vi /etc/zabbix/zabbix_server.conf
DBHost=localhost
DBName=zabbix
DBUser=zabbix
DBPassword=<password>
```

In DBPassword use Zabbix database password for MySQL; PostgreSQL user password for PostgreSQL.

Use DBHost= with PostgreSQL. You might want to keep the default setting DBHost=localhost (or an IP address), but this would make PostgreSQL use a network socket for connecting to Zabbix. See SELinux configuration below for instructions.

Starting Zabbix server process

It’s time to start Zabbix server process:

```
# service zabbix-server start
```

and make it start at system boot:

RHEL 7 and later:

```
# systemctl enable zabbix-server
```

RHEL prior to 7:

```
# chkconfig --level 12345 zabbix-server on
```

Substitute ‘zabbix-server’ with ‘zabbix-proxy’ if you are installing Zabbix proxy.

Zabbix frontend configuration

For RHEL 7 and later the Apache configuration file for Zabbix frontend is located in `/etc/httpd/conf.d/zabbix.conf`.

If you use RHEL 6 please read the section about using Zabbix frontend on RHEL 6 on how to configure the frontend.

Some PHP settings are already configured. But it’s necessary to uncomment the “date.timezone” setting and set the right timezone for you.

```
php_value max_execution_time 300
php_value memory_limit 128M
php_value post_max_size 16M
php_value upload_max_filesize 2M
php_value max_input_time 300
php_value max_input_vars 10000
php_value always_populate_raw_post_data -1
# php_value date.timezone Europe/Riga
```

Now you are ready to proceed with frontend installation steps which will allow you to access your newly installed Zabbix.

Note that a Zabbix proxy does not have a frontend; it communicates with Zabbix server only.

**Note:**

Zabbix official repository provides fping, iksemel, libssh2 packages as well. These packages are located in the non-supported directory.

SELinux configuration
Having SELinux status enabled in enforcing mode, you need to execute the following commands to enable communication between Zabbix frontend and server:

RHEL 7 and later:

```
# setsebool -P httpd_can_connect_zabbix on
```

If the database is accessible over network (including 'localhost' in case of PostgreSQL), you need to allow Zabbix frontend to connect to the database too:

```
# setsebool -P httpd_can_network_connect_db on
```

RHEL prior to 7:

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

As frontend and SELinux configuration is done, you need to restart Apache web server:

```
# service httpd restart
```

Zabbix frontend and server on RHEL 6

Zabbix frontend on RHEL 6 is not supported because of PHP version. Since Zabbix 3.0 the requirements are to have PHP 5.4.0 or later while RHEL 6 latest version is 5.3.3.

In most cases Zabbix server and frontend are installed on the same machine. When upgrading 2.2 to 3.0 Zabbix server will perform database upgrade and frontend will stop working. There is no way to roll back the database changes so users will be forced to upgrade PHP using 3rd party packages. This is why Zabbix server is also deprecated on RHEL 6.

If you still want to use Zabbix frontend on RHEL 6 and upgraded your PHP using 3rd party packages you would need to enable zabbix-deprecated repository first:

- open file /etc/yum.repos.d/zabbix.repo
- find section [zabbix-deprecated]
- set enabled=1
- save the file

You will have to do some more manual configuration. This is because we cannot identify the Apache version required for your PHP which makes it impossible for us to provide proper Apache configuration for Zabbix frontend. We have included 2 Apache configuration files to our zabbix-web package, one for Apache 2.2 and another for 2.4, which you would need to integrate with the Apache configuration yourself:

- httpd22-example.conf
- httpd24-example.conf

To get the full path to the files execute:

```
$ rpm -ql zabbix-web | grep example.conf
```

Agent installation

To install the agent, run:

```
# yum install zabbix-agent
```

To start the agent, run:

```
# service zabbix-agent start
```

If you want to run Zabbix agent as root, see here.

Java gateway installation

It is required to install Java gateway only if you want to monitor JMX applications. Java gateway is lightweight and does not require a database.

Once the required repository is added, you can install Zabbix Java gateway by running:

```
# yum install zabbix-java-gateway
```

Proceed to setup for more details on configuring and running Java gateway.

Installing debuginfo packages

::: noteclassic Debuginfo packages are currently available for RHEL/CentOS versions 7, 6 and 5. ::: To enable debuginfo repository edit /etc/yum.repos.d/zabbix.repo file. Change enabled=0 to enabled=1 for zabbix-debuginfo repository.
[zabbix-debuginfo]
name=Zabbix Official Repository debuginfo - $basearch
baseurl=http://repo.zabbix.com/zabbix/4.0/rhel/7/$basearch/debuginfo/
enabled=0
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-ZABBIX-A14FE591
gpgcheck=1

This will allow you to install the zabbix-debuginfo package.

# yum install zabbix-debuginfo

This single package contains debug information for all binary Zabbix components.

2 Debian/Ubuntu/Raspbian

Overview

Official Zabbix 4.0 LTS packages for Debian, Ubuntu, and Raspberry Pi OS (Raspbian) are available on Zabbix website.

Packages are available with either MySQL/PostgreSQL database and Apache web server support.

Adding Zabbix repository

Install the repository configuration package. This package contains apt (software package manager) configuration files.

For Debian 10, run the following commands:

Note! For Debian 9, substitute ‘buster’ with ‘stretch’ in the commands. For Debian 8, substitute ‘buster’ with ‘jessie’ in the commands.

# wget https://repo.zabbix.com/zabbix/4.0/debian/pool/main/z/zabbix-release/zabbix-release_4.0-2+buster_all.deb
# dpkg -i zabbix-release_4.0-2+buster_all.deb
# apt update

For Ubuntu 20.04 (focal), run the following commands:

# wget https://repo.zabbix.com/zabbix/4.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_4.0-3+focal_all.deb
# dpkg -i zabbix-release_4.0-3+focal_all.deb
# apt update

• For Ubuntu 18.04, substitute ‘focal’ with ‘bionic’ in the commands.
• For Ubuntu 16.04, substitute ‘focal’ with ‘xenial’ in the commands.
• For Ubuntu 14.04, substitute ‘focal’ with ‘trusty’ in the commands.

For Raspbian, run the following commands:

# wget https://repo.zabbix.com/zabbix/4.0/raspbian/pool/main/z/zabbix-release/zabbix-release_4.0-2+buster_all.deb
# dpkg -i zabbix-release_4.0-2+buster_all.deb
# apt update

Server/proxy/frontend installation

To install Zabbix server with MySQL support:

# apt install zabbix-server-mysql

To install Zabbix proxy with MySQL support:

# apt install zabbix-proxy-mysql

To install Zabbix frontend:

# apt install zabbix-frontend-php

Substitute ‘mysql’ in the commands with ‘pgsql’ to use PostgreSQL, or with ‘sqlite3’ to use SQLite3 (proxy only).

Creating database

For Zabbix server and proxy daemons a database is required. It is not needed to run Zabbix agent.

Warning:
Separate databases are needed for Zabbix server and Zabbix proxy; they cannot use the same database. Therefore, if they are installed on the same host, their databases must be created with different names!

Create the database using the provided instructions for MySQL or PostgreSQL.
Importing data

Now import initial schema and data for the server with MySQL:

```bash
# zcat /usr/share/doc/zabbix-server-mysql/create.sql.gz | mysql -uzabbix -p zabbix
```

You will be prompted to enter your newly created database password.

With PostgreSQL:

```bash
# zcat /usr/share/doc/zabbix-server-pgsql/create.sql.gz | sudo -u zabbix psql zabbix
```

For proxy, import initial schema:

```bash
# zcat /usr/share/doc/zabbix-proxy-mysql/schema.sql.gz | mysql -uzabbix -p zabbix
```

For proxy with PostgreSQL (or SQLite):

```bash
# zcat /usr/share/doc/zabbix-proxy-pgsql/schema.sql.gz | sudo -u zabbix psql zabbix
# zcat /usr/share/doc/zabbix-proxy-sqlite3/schema.sql.gz | sqlite3 zabbix.db
```

Configure database for Zabbix server/proxy

Edit `zabbix_server.conf` (and `zabbix_proxy.conf`) to use their respective databases. For example:

```bash
# vi /etc/zabbix/zabbix_server.conf
DBHost=localhost
DBName=zabbix
DBUser=zabbix
DBPassword=<password>
```

In `DBPassword` use Zabbix database password for MySQL; PostgreSQL user password for PostgreSQL.

Use `DBHost` with PostgreSQL. You might want to keep the default setting `DBHost=localhost` (or an IP address), but this would make PostgreSQL use a network socket for connecting to Zabbix. Refer to the respective section for RHEL/CentOS for instructions.

Starting Zabbix server process

It’s time to start Zabbix server process and make it start at system boot:

```
# service zabbix-server start
# update-rc.d zabbix-server enable
```

Substitute ‘zabbix-server’ with ‘zabbix-proxy’ to start Zabbix proxy process.

SELinux configuration

Refer to the respective section for RHEL/CentOS.

As frontend and SELinux configuration is done, you need to restart Apache web server:

```
# service apache2 restart
```

Frontend configuration

Apache configuration file for Zabbix frontend is located in `/etc/apache2/conf-enabled/zabbix.conf`. Some PHP settings are already configured. But it’s necessary to uncomment the “date.timezone” setting and set the right timezone for you.

```
php_value max_execution_time 300
php_value memory_limit 128M
php_value post_max_size 16M
php_value upload_max_filesize 2M
php_value max_input_time 300
php_value max_input_vars 10000
php_value always_populate_raw_post_data -1
# php_value date.timezone Europe/Riga
```

Now you are ready to proceed with frontend installation steps which will allow you to access your newly installed Zabbix.

Note that a Zabbix proxy does not have a frontend; it communicates with Zabbix server only.

Agent installation

To install the agent, run

```
# apt install zabbix-agent
```

To start the agent, run:
# service zabbix-agent start

If you want to run Zabbix agent as root, see [here](#).  

Java gateway installation

It is required to install [Java gateway](#) only if you want to monitor JMX applications. Java gateway is lightweight and does not require a database.

Once the required repository is added, you can install Zabbix Java gateway by running:

# apt install zabbix-java-gateway

Proceed to [setup](#) for more details on configuring and running Java gateway.

### 3 Windows agent installation from MSI

Overview

Zabbix Windows agent can be installed from Windows MSI installer packages (32-bit or 64-bit) available for [download](#).

The Zabbix get and sender utilities can also be installed, either together with Zabbix agent or separately.

32-bit package cannot be installed on a 64-bit Windows.

All packages come with TLS support, however, configuring TLS is optional.

Both UI and command-line based installation is supported.

Installation steps

To install, double-click the downloaded MSI file.
Accept the license to proceed to the next step.
Specify the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>Specify host name.</td>
</tr>
<tr>
<td>Zabbix server IP/DNS</td>
<td>Specify IP/DNS of Zabbix server.</td>
</tr>
<tr>
<td>Agent listen port</td>
<td>Specify agent listen port (10050 by default).</td>
</tr>
<tr>
<td>Server or Proxy for active checks</td>
<td>Specify IP/DNS of Zabbix server/proxy for active agent checks.</td>
</tr>
<tr>
<td>Remote commands</td>
<td>Mark the checkbox to enable remote commands.</td>
</tr>
<tr>
<td>Enable PSK</td>
<td>Mark the checkbox to enable TLS support via pre-shared keys.</td>
</tr>
<tr>
<td>Add agent location to the PATH</td>
<td>Add agent location to the PATH variable.</td>
</tr>
</tbody>
</table>
Enter pre-shared key identity and value. This step is only available if you checked Enable PSK in the previous step.
Select Zabbix components to install - Zabbix agent daemon, Zabbix sender, Zabbix get.
Zabbix components along with the configuration file will be installed in a Zabbix Agent folder in Program Files. zabbix_agentd.exe will be set up as Windows service with automatic startup.
Command-line based installation

Supported parameters

The following set of parameters is supported by created MSIs:

<table>
<thead>
<tr>
<th>Number</th>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>LOGTYPE</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>LOGFILE</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>ENABLEREMOTECOMMANDS</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>SERVER</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>LISTENPORT</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>SERVERACTIVE</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>HOSTNAME</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>TIMEOUT</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>TLSCONNECT</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>TLSACCEPT</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>TLSPSKIDENTITY</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>TLSPSKFILE</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>TLSPSKVALUE</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>TLSCAFILE</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>TLSCRLFILE</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>TLSSERVERCERTISSUER</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>TLSSERVERCERTSUBJECT</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>TLSCERTFILE</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>TLSKEYFILE</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>INSTALLFOLDER</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>ENABLEPATH</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>SKIP</td>
<td>SKIP=fw - do not install firewall exception rule</td>
</tr>
<tr>
<td>Number</td>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>23</td>
<td>ADDPROGRAM</td>
<td>A comma-delimited list of programs to install. Possible values: AgentProgram, GetProgram, SenderProgram. E.g., ADDPROGRAM=AgentProgram,GetProgram</td>
</tr>
<tr>
<td>24</td>
<td>ADDLOCAL</td>
<td>A comma-delimited list of programs to install. Possible values: AgentProgram, GetProgram, SenderProgram. E.g., ADDLOCAL=AgentProgram,SenderProgram</td>
</tr>
<tr>
<td>25</td>
<td>CONF</td>
<td>Specify path to custom configuration file, e.g., CONF=c:\full\path\to\user.conf</td>
</tr>
</tbody>
</table>

To install you may run, for example:

```
SET INSTALLFOLDER=C:\Program Files\za

msiexec /i*v log.txt /i zabbix_agent-4.0.6-x86.msi /qn^  
LOGTYPE=file^  
LOGFILE="%INSTALLFOLDER%\za.log"^  
ENABLEREMOCON=1^  
SERVER=192.168.6.76^  
LISTENPORT=12345^  
SERVERACTIVE=:1^  
HOSTNAME=myHost^  
TLS_CONNECT=psk^  
TLS_ACCEPT=psk^  
TLSPSKIDENTITY=MyPSKID^  
TLSPSKFILE="%INSTALLFOLDER%\mykey.psk"^  
TSLCAFILE="c:\temp\f.txt1"^  
TLSRLFILE="c:\temp\f.txt2"^  
TSSLSERVERCERTISSUER="My CA"^  
TSSLSERVERCERTSUBJECT="My Cert"^  
TLS_CERTFILE="c:\temp\f.txt5"^  
TLSKEYFILE="c:\temp\f.txt6"^  
ENABLEPATH=1^  
INSTALLFOLDER="%INSTALLFOLDER%"^  
SKIP=fw^  
```

or

```
msiexec /i*v log.txt /i zabbix_agent-4.0.6-x86.msi /qn^  
SERVER=192.168.6.76^  
TLS_CONNECT=psk^  
TLS_ACCEPT=psk^  
TLSPSKIDENTITY=MyPSKID^  
TLSPSKVALUE=1f87b595725ac58dd977beef14b97461a7c1045b9a1c963065002c5473194952^  
```

If both TLSPSKFILE and TLSPSKVALUE are passed, then TLSPSKVALUE will be written to TLSPSKFILE.

## 4 Mac OS agent installation from PKG

### Overview

Zabbix Mac OS agent can be installed from PKG installer packages available for download. Versions with or without encryption are available.

### Installing agent

The agent can be installed using the graphical user interface or from the command line, for example:

```
sudo installer -pkg zabbix_agent-4.0.44-macos-amd64-openssl.pkg -target /
```

Make sure to use the correct Zabbix package version in the command. It must match the name of the downloaded package.

### Running agent
The agent will start automatically after installation or restart.

You may edit the configuration file at \texttt{/usr/local/etc/zabbix/zabbix_agentd.conf} if necessary.

To start the agent manually, you may run:

\texttt{sudo launchctl start com.zabbix.zabbix_agentd}

To stop the agent manually:

\texttt{sudo launchctl stop com.zabbix.zabbix_agentd}

During upgrade, the existing configuration file is not overwritten. Instead a new \texttt{zabbix_agentd.conf.NEW} file is created to be used for reviewing and updating the existing configuration file, if necessary. Remember to restart the agent after manual changes to the configuration file.

Troubleshooting and removing agent

This section lists some useful commands that can be used for troubleshooting and removing Zabbix agent installation.

See if Zabbix agent is running:

\texttt{ps aux | grep zabbix_agentd}

See if Zabbix agent has been installed from packages:

\texttt{$ pkgutil --pkgs | grep zabbix}

com.zabbix.pkg.ZabbixAgent

See the files that were installed from the installer package (note that the initial / is not displayed in this view):

\texttt{$ 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

Stop Zabbix agent if it was launched with launchctl:

\texttt{sudo launchctl unload /Library/LaunchDaemons/com.zabbix.zabbix_agentd.plist}

Remove files (including configuration and logs) that were installed with installer package:

\texttt{sudo rm -f /Library/LaunchDaemons/com.zabbix.zabbix_agentd.plist}

\texttt{sudo rm -f /usr/local/sbin/zabbix_agentd}

\texttt{sudo rm -f /usr/local/bin/zabbix_get}

\texttt{sudo rm -f /usr/local/bin/zabbix_sender}

\texttt{sudo rm -rf /usr/local/etc/zabbix}

\texttt{sudo rm -rf /var/logs/zabbix}

Forget that Zabbix agent has been installed:

\texttt{sudo pkgutil --forget com.zabbix.pkg.ZabbixAgent}

5 Installation from containers

\textbf{Docker} Zabbix provides Docker images for each Zabbix component as portable and self-sufficient containers to speed up deployment and update procedure.

Zabbix components come with MySQL and PostgreSQL database support, Apache2 and Nginx web server support. These images are separated into different images.

Docker base images

Zabbix components are provided on Ubuntu, Alpine Linux and CentOS base images:

<table>
<thead>
<tr>
<th>Image</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>alpine</td>
<td>3.11</td>
</tr>
</tbody>
</table>
All images are configured to rebuild latest images if base images are updated.

**Attention:**
Zabbix Docker Appliance image is decommissioned since 4.0.19 and will not be available for newer releases. Please use a separate Docker image for each component instead of the all-in-one solution.

Docker file sources

Everyone can follow Docker file changes using the Zabbix official repository on github.com. You can fork the project or make your own images based on official Docker files.

Structure

All Zabbix components are available in the following Docker repositories:

- **Zabbix agent** - zabbix/zabbix-agent
- **Zabbix server**
  - Zabbix server with MySQL database support - zabbix/zabbix-server-mysql
  - Zabbix server with PostgreSQL database support - zabbix/zabbix-server-pgsql
- **Zabbix web-interface**
  - Zabbix web-interface based on Apache2 web server with MySQL database support - zabbix/zabbix-web-apache-mysql
  - Zabbix web-interface based on Apache2 web server with PostgreSQL database support - zabbix/zabbix-web-apache-pgsql
  - Zabbix web-interface based on Nginx web server with MySQL database support - zabbix/zabbix-web-nginx-mysql
  - Zabbix web-interface based on Nginx web server with PostgreSQL database support - zabbix/zabbix-web-nginx-pgsql
- **Zabbix proxy**
  - Zabbix proxy with SQLite3 database support - zabbix/zabbix-proxy-sqlite3
  - Zabbix proxy with MySQL database support - zabbix/zabbix-proxy-mysql
- **Zabbix Java Gateway** - zabbix/zabbix-java-gateway

Additionally there is SNMP trap support. It is provided as additional repository (zabbix/zabbix-snmprtraps) based on Alpine Linux, CentOS 7 and Ubuntu 18.04. It could be linked with Zabbix server and Zabbix proxy.

Versions

Each repository of Zabbix components contains the following tags:

- latest - latest stable version of a Zabbix component based on Alpine Linux image
- alpine-latest - latest stable version of a Zabbix component based on Alpine Linux image
- ubuntu-latest - latest stable version of a Zabbix component based on Ubuntu image
- alpine-4.0-latest - latest minor version of a Zabbix 4.0 component based on Alpine Linux image
- ubuntu-4.0-latest - latest minor version of a Zabbix 4.0 component based on Ubuntu image
- alpine-4.0.* - different minor versions of a Zabbix 4.0 component based on Alpine Linux image, where * is the minor version of Zabbix component
- ubuntu-4.0.* - different minor versions of a Zabbix 4.0 component based on Ubuntu image, where * is the minor version of Zabbix component

Usage

Environment variables

All Zabbix component images provide environment variables to control configuration. These environment variables are listed in each component repository. These environment variables are options from Zabbix configuration files, but with different naming method. For example, ZBX_LOGSLOWQUERIES is equal to LogSlowQueries from Zabbix server and Zabbix proxy configuration files.

**Attention:**
Some of configuration options are not allowed to change. For example, PIDFile and LogType.

Some of components have specific environment variables, which do not exist in official Zabbix configuration files:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ubuntu</td>
<td>18.04 (bionic)</td>
<td></td>
</tr>
<tr>
<td>centos</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>Environment Variable</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DB_SERVER_HOST</td>
<td>Server</td>
<td>This variable is IP or DNS name of MySQL or PostgreSQL server. By default, value is mysql-server or postgres-server for MySQL or PostgreSQL respectively.</td>
</tr>
<tr>
<td>DB_SERVER_PORT</td>
<td>Server</td>
<td>This variable is port of MySQL or PostgreSQL server. By default, value is ’3306’ or ’5432’ respectively.</td>
</tr>
<tr>
<td>MYSQL_USER</td>
<td>Server</td>
<td>MySQL database user. By default, value is ‘zabbix’.</td>
</tr>
<tr>
<td>MYSQL_PASSWORD</td>
<td>Server</td>
<td>MySQL database password. By default, value is ‘zabbix’.</td>
</tr>
<tr>
<td>MYSQL_DATABASE</td>
<td>Server</td>
<td>Zabbix database name. By default, value is ‘zabbix’ for Zabbix server and ‘zabbix_proxy’ for Zabbix proxy.</td>
</tr>
<tr>
<td>POSTGRES_USER</td>
<td>Server</td>
<td>PostgreSQL database user.</td>
</tr>
<tr>
<td>POSTGRES_PASSWORD</td>
<td>Server</td>
<td>PostgreSQL database password.</td>
</tr>
<tr>
<td>POSTGRES_DB</td>
<td>Server</td>
<td>Zabbix database name. By default, value is ‘zabbix’ for Zabbix server and ‘zabbix_proxy’ for Zabbix proxy.</td>
</tr>
<tr>
<td>PHP_TZ</td>
<td>Web-interface</td>
<td>Timezone in PHP format. Full list of supported timezones are available on <a href="https://php.net">php.net</a>. By default, value is ‘Europe/Riga’.</td>
</tr>
<tr>
<td>ZBX_SERVER_NAME</td>
<td>Web interface</td>
<td>Visible Zabbix installation name in right top corner of the web interface. By default, value is ‘Zabbix Docker’</td>
</tr>
<tr>
<td>ZBX_JAVAGATEWAY_ENABLE</td>
<td>Server</td>
<td>Enables communication with Zabbix Java gateway to collect Java related checks. By default, value is “false”</td>
</tr>
<tr>
<td>ZBX_ENABLE_SNMP_TRAPS</td>
<td>Server</td>
<td>Enables SNMP trap feature. It requires <code>zabbix-snmptaps</code> instance and shared volume <code>/var/lib/zabbix/snmptaps</code> to Zabbix server or Zabbix proxy.</td>
</tr>
</tbody>
</table>

**Volumes**

The images allow to use some mount points. These mount points are different and depend on Zabbix component type:

<table>
<thead>
<tr>
<th>Volume</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zabbix agent</td>
<td>The volume allows to include *.conf files and extend Zabbix agent using the <code>UserParameter</code> feature</td>
</tr>
<tr>
<td>/etc/zabbix/zabbix_agentd.d</td>
<td>The volume allows to load additional modules and extend Zabbix agent using the <code>LoadModule</code> feature</td>
</tr>
<tr>
<td>/var/lib/zabbix/modules</td>
<td>The volume is used to store TLS-related files. These file names are specified using <code>ZBX_TLSCAFILE</code>, <code>ZBX_TLSCRLFILE</code>, <code>ZBX_TLSKEY_FILE</code> and <code>ZBX_TLSPSKFILE</code> environment variables</td>
</tr>
<tr>
<td>Zabbix server</td>
<td>The volume is used for custom alert scripts. It is the <code>AlertScriptsPath</code> parameter in <code>zabbix_server.conf</code></td>
</tr>
</tbody>
</table>
The volume is used by external checks. It is the ExternalScripts parameter in zabbix_server.conf.

The volume allows to load additional modules and extend Zabbix server using the LoadModule feature.

The volume is used to store TLS related files. These file names are specified using ZBX_TLS_CERTFILE, ZBX_TLS_CRL_FILE, ZBX_TLS_KEY_FILE and ZBX_TLS_PSK_FILE environment variables.

The volume is used as location of SSL client certificate files for client authentication. It is the SSLCertLocation parameter in zabbix_server.conf.

The volume is used as location of SSL private key files for client authentication. It is the SSLSKeyLocation parameter in zabbix_server.conf.

The volume is used as location of certificate authority (CA) files for SSL server certificate verification. It is the SSLCertLocation parameter in zabbix_proxy.conf.

The volume is used as location of snmptraps.log file. It could be shared by zabbix-snmptraps container and inherited using the volumes_from Docker option while creating a new instance of Zabbix server. SNMP trap processing feature could be enabled by using shared volume and switching the ZBX_ENABLE_SNMP_TRAPS environment variable to 'true'.

The volume allows to add new MIB files. It does not support subdirectories, all MIBs must be placed in /var/lib/zabbix/mibs.

The volume is used by external checks. It is the ExternalScripts parameter in zabbix_proxy.conf.

The volume allows to store database files on external devices. Supported only for Zabbix proxy with SQLite.

The volume allows to load additional modules and extend Zabbix server using the LoadModule feature.

The volume is used to store TLS related files. These file names are specified using ZBX_TLS_CERTFILE, ZBX_TLS_CRL_FILE, ZBX_TLS_KEY_FILE and ZBX_TLS_PSK_FILE environment variables.

The volume is used as location of SSL client certificate files for client authentication. It is the SSLCertLocation parameter in zabbix_proxy.conf.

The volume is used as location of SSL private key files for client authentication. It is the SSLSKeyLocation parameter in zabbix_proxy.conf.

The volume is used as location of certificate authority (CA) files for SSL server certificate verification. It is the SSLCertLocation parameter in zabbix_proxy.conf.

The volume is used as location of snmptraps.log file. It could be shared by zabbix-snmptraps container and inherited using the volumes_from Docker option while creating a new instance of Zabbix server. SNMP trap processing feature could be enabled by using shared volume and switching the ZBX_ENABLE_SNMP_TRAPS environment variable to 'true'.

The volume allows to add new MIB files. It does not support subdirectories, all MIBs must be placed in /var/lib/zabbix/mibs.

The volume allows to enable HTTPS for Zabbix web interface. The volume must contain the two ssl.crt and ssl.key files prepared for Apache2 SSL connections.

The volume allows to enable HTTPS for Zabbix web interface. The volume must contain the two ssl.crt and ssl.key files prepared for Apache2 SSL connections.
The volume allows to enable HTTPS for Zabbix web interface. The volume must contain the two ssl.crt, ssl.key files and dbparam.pem prepared for Nginx SSL connections.

Zabbix snmptraps
/var/lib/zabbix/snmptraps
The volume contains the snmptraps.log log file named with received SNMP traps.

/var/lib/zabbix/mibs
The volume allows to add new MIB files. It does not support subdirectories, all MIBs must be placed in /var/lib/zabbix/mibs.

For additional information use Zabbix official repositories in Docker Hub.

Usage examples

**Example 1**
The example demonstrates how to run Zabbix server with MySQL database support, Zabbix web interface based on the Nginx web server and Zabbix java gateway.

1. Create network dedicated for Zabbix component containers:

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

2. Start empty MySQL server instance

   # 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:8.0 
   --character-set-server=utf8 --collation-server=utf8_bin 
   --default-authentication-plugin=mysql_native_password

3. Start Zabbix java gateway instance

   # docker run --name zabbix-java-gateway -t 
   --network=zabbix-net 
   --restart unless-stopped 
   -d zabbix/zabbix-java-gateway:alpine-4.0-latest

4. Start Zabbix server instance and link the instance with created MySQL server instance

   # 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-4.0-latest

Note:
Zabbix server instance exposes 10051/TCP port (Zabbix trapper) to host machine.

5. Start Zabbix web interface and link the instance with created MySQL server and Zabbix server instances

   # 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"
**Example 2**

The example demonstrates how to run Zabbix server with PostgreSQL database support, Zabbix web interface based on the Nginx web server and SNMP trap feature.

1. Create network dedicated for Zabbix component containers:
   
   ```bash
   # docker network create --subnet 172.20.0.0/16 --ip-range 172.20.240.0/20 zabbix-net
   ```

2. Start empty PostgreSQL server instance
   
   ```bash
   # 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. Start Zabbix snmptraps instance
   
   ```bash
   # 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
   --restart unless-stopped
   -d zabbix/zabbix-snmptraps:alpine-4.0-latest
   ```

   **Note:**
   Zabbix snmptrap instance exposes the 162/UDP port (SNMP traps) to host machine.

4. Start Zabbix server instance and link the instance with created PostgreSQL server instance
   
   ```bash
   # 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
   --volumes-from zabbix-snmptraps
   --restart unless-stopped
   -d zabbix/zabbix-server-pgsql:alpine-4.0-latest
   ```

   **Note:**
   Zabbix server instance exposes the 10051/TCP port (Zabbix trapper) to host machine.

5. Start Zabbix web interface and link the instance with created PostgreSQL server and Zabbix server instances
   
   ```bash
   # 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 \
-v /etc/ssl/nginx:/etc/ssl/nginx:ro \
--restart unless-stopped \
-d zabbix/zabbix-web-nginx-pgsql:alpine-4.0-latest

**Note:**
Zabbix web interface instance exposes the 443/TCP port (HTTPS) to host machine. Directory /etc/ssl/nginx must contain certificate with required name.

**Docker Compose**
Zabbix provides compose files also for defining and running multi-container Zabbix components in Docker. These compose files are available in Zabbix docker official repository on github.com: [https://github.com/zabbix/zabbix-docker](https://github.com/zabbix/zabbix-docker).

These compose files are added as examples, they are overloaded. For example, they contain proxies with MySQL and SQLite3 support.

There are a few different versions of compose files:

<table>
<thead>
<tr>
<th>File name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>docker-compose_v3_alpine_mysql_latest.yaml</td>
<td>The compose file runs the latest version of Zabbix 4.0 components on Alpine Linux with MySQL database support.</td>
</tr>
<tr>
<td>docker-compose_v3_alpine_mysql_local.yaml</td>
<td>The compose file locally builds the latest version of Zabbix 4.0 and runs Zabbix components on Alpine Linux with MySQL database support.</td>
</tr>
<tr>
<td>docker-compose_v3_alpine_pgsql_latest.yaml</td>
<td>The compose file runs the latest version of Zabbix 4.0 components on Alpine Linux with PostgreSQL database support.</td>
</tr>
<tr>
<td>docker-compose_v3_alpine_pgsql_local.yaml</td>
<td>The compose file locally builds the latest version of Zabbix 4.0 and runs Zabbix components on Alpine Linux with PostgreSQL database support.</td>
</tr>
<tr>
<td>docker-compose_v3_centos_mysql_latest.yaml</td>
<td>The compose file runs the latest version of Zabbix 4.0 components on CentOS 7 with MySQL database support.</td>
</tr>
<tr>
<td>docker-compose_v3_centos_mysql_local.yaml</td>
<td>The compose file locally builds the latest version of Zabbix 4.0 and runs Zabbix components on CentOS 7 with MySQL database support.</td>
</tr>
<tr>
<td>docker-compose_v3_centos_pgsql_latest.yaml</td>
<td>The compose file runs the latest version of Zabbix 4.0 components on CentOS 7 with PostgreSQL database support.</td>
</tr>
<tr>
<td>docker-compose_v3_centos_pgsql_local.yaml</td>
<td>The compose file locally builds the latest version of Zabbix 4.0 and runs Zabbix components on CentOS 7 with PostgreSQL database support.</td>
</tr>
<tr>
<td>docker-compose_v3_ubuntu_mysql_latest.yaml</td>
<td>The compose file runs the latest version of Zabbix 4.0 components on Ubuntu 18.04 with MySQL database support.</td>
</tr>
<tr>
<td>docker-compose_v3_ubuntu_mysql_local.yaml</td>
<td>The compose file locally builds the latest version of Zabbix 4.0 and runs Zabbix components on Ubuntu 18.04 with MySQL database support.</td>
</tr>
<tr>
<td>docker-compose_v3_ubuntu_pgsql_latest.yaml</td>
<td>The compose file runs the latest version of Zabbix 4.0 components on Ubuntu 18.04 with PostgreSQL database support.</td>
</tr>
<tr>
<td>docker-compose_v3_ubuntu_pgsql_local.yaml</td>
<td>The compose file locally builds the latest version of Zabbix 4.0 and runs Zabbix components on Ubuntu 18.04 with PostgreSQL database support.</td>
</tr>
</tbody>
</table>

**Attention:**
Available Docker compose files support version 3 of Docker Compose.

**Storage**
Compose files are configured to support local storage on a host machine. Docker Compose will create a zbx_env directory in the folder with the compose file when you run Zabbix components using the compose file. The directory will contain the same structure as described above in the *Volumes* section and directory for database storage.

There are also volumes in read-only mode for `/etc/localtime` and `/etc/timezone` files.
Environment files

In the same directory with compose files on github.com you can find files with default environment variables for each component in compose file. These environment files are named like .env_<type of component>.

Examples

**Example 1**

```
# git checkout 4.0
# docker-compose -f ./docker-compose_v3_alpine_mysql_latest.yaml up -d
```

The command will download latest Zabbix 4.0 images for each Zabbix component and run them in detach mode.

**Attention:**

Do not forget to download .env_<type of component> files from github.com official Zabbix repository with compose files.

**Example 2**

```
# git checkout 4.0
# docker-compose -f ./docker-compose_v3_ubuntu_mysql_local.yaml up -d
```

The command will download base image Ubuntu 18.04 (bionic), then build Zabbix 4.0 components locally and run them in detach mode.

6 Upgrade procedure

Overview

This section provides upgrade information for Zabbix **4.0**:

- using packages:
  - for Red Hat Enterprise Linux/CentOS
  - for Debian/Ubuntu

- using sources

Direct upgrade to Zabbix 4.0.x is possible from Zabbix **3.4.x**, **3.2.x**, **3.0.x**, **2.4.x**, **2.2.x** and **2.0.x**. For upgrading from earlier versions consult Zabbix documentation for 2.0 and earlier.

Upgrade from packages

Overview

This section provides the steps required for a successful upgrade using official RPM and DEB packages provided by Zabbix for:

- Red Hat Enterprise Linux/CentOS
- Debian/Ubuntu

Zabbix packages from OS repositories

Often, OS distributions (in particular, Debian-based distributions) provide their own Zabbix packages. Note, that these packages are not supported by Zabbix, they are typically out of date and lack the latest features and bug fixes. Only the packages from repo.zabbix.com are officially supported.

If you are upgrading from packages provided by OS distributions (or had them installed at some point), follow this procedure to switch to official Zabbix packages:

1. Always uninstall the old packages first.
2. Check for residual files that may have been left after deinstallation.
3. Install official packages following installation instructions provided by Zabbix.

Never do a direct update, as this may result in a broken installation.
Overview

This section provides the steps required for a successful upgrade from Zabbix 3.4.x to Zabbix 4.0.x using official Zabbix packages for Red Hat Enterprise Linux/CentOS.

While upgrading Zabbix agents is not mandatory (but recommended), Zabbix server and proxies must be of the same major version. Therefore, in a server-proxy setup, Zabbix server and all proxies have to be stopped and upgraded.

To minimize downtime and data loss during the upgrade, it is recommended to stop and upgrade Zabbix server and then stop, upgrade and start Zabbix proxies one after another. When all proxies are upgraded, start Zabbix server. During the Zabbix server downtime, running proxies will keep collecting and storing data and will pass the data to Zabbix server when the server is up and running. Any notifications for problems during Zabbix server downtime will be generated only after the upgraded server is started.

Note that with SQLite database on proxies, history data from proxies before the upgrade will be lost, because SQLite database upgrade is not supported and the SQLite database file has to be manually removed. When proxy is started for the first time and the SQLite database file is missing, proxy creates it automatically.

Depending on database size the database upgrade to version 4.0 may take a long time.

Warning:
Before the upgrade make sure to read the relevant upgrade notes!

The following upgrade notes are available:

<table>
<thead>
<tr>
<th>Upgrade from</th>
<th>Read full upgrade notes</th>
<th>Most important changes between versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.4.x</td>
<td>For 4.0</td>
<td>'libpthread' and 'zlib' libraries now mandatory; Support for plain text protocol dropped and header is mandatory; Pre-1.4 version Zabbix agents are no longer supported; The Server parameter in passive proxy configuration now mandatory</td>
</tr>
<tr>
<td>3.2.x</td>
<td>For 3.4 For 4.0</td>
<td>SQLite support as backend database dropped for Zabbix server/frontend; Perl Compatible Regular Expressions (PCRE) supported instead of POSIX extended; 'libpcre' and 'libevent' libraries mandatory for Zabbix server; Exit code checks added for user parameters, remote commands and system.run[] items without the 'nowait' flag as well as Zabbix server executed scripts; Zabbix java gateway has to be upgraded to support new functionality</td>
</tr>
<tr>
<td>3.0.x LTS</td>
<td>For 3.2 For 3.4 For 4.0</td>
<td>Database upgrade may be slow, depending on the history table size</td>
</tr>
</tbody>
</table>

You may also want to check the requirements for 4.0.

Note:
It may be handy to run two parallel SSH sessions during the upgrade, executing the upgrade steps in one and monitoring the server/proxy logs in another. For example, run `tail -f zabbix_server.log` or `tail -f zabbix_proxy.log` in the second SSH session showing you the latest log file entries and possible errors in real time. This can be critical for production instances.

Upgrade procedure

1 Stop Zabbix processes

Stop Zabbix server to make sure that no new data is inserted into database.

```
# systemctl stop zabbix-server
```

If upgrading the proxy, stop proxy too.

```
# systemctl stop zabbix-proxy
```
Attention:

It is known to be possible to upgrade the server only and have older and unupgraded proxies report data to a newer server (the proxies can’t refresh their configuration though). This approach, however, is not recommended and not supported by Zabbix and choosing it is entirely at your own risk.

2 Back up the existing Zabbix database

This is a very important step. Make sure that you have a backup of your database. It will help if the upgrade procedure fails (lack of disk space, power off, any unexpected problem).

3 Back up configuration files, PHP files and Zabbix binaries

Make a backup copy of Zabbix binaries, configuration files and the PHP file directory.

Configuration files:

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

PHP files and Zabbix binaries:

# cp -R /usr/share/zabbix/ /opt/zabbix-backup/
# cp -R /usr/share/doc/zabbix-* /opt/zabbix-backup/

4 Update repository configuration package

To proceed with the upgrade your current repository package has to be updated.

# rpm -Uvh https://repo.zabbix.com/zabbix/4.0/rhel/7/x86_64/zabbix-release-4.0-1.el7.noarch.rpm

5 Upgrade Zabbix components

To upgrade Zabbix components you may run something like:

# yum upgrade zabbix-server-mysql zabbix-web-mysql zabbix-agent

If using PostgreSQL, substitute mysql with pgsql in the command. If upgrading the proxy, substitute server with proxy in the command.

6 Review component configuration parameters

See the upgrade notes for details on mandatory changes.

7 Start Zabbix processes

Start the updated Zabbix components.

# systemctl start zabbix-server
# systemctl start zabbix-proxy
# systemctl start zabbix-agent

8 Clear web browser cookies and cache

After the upgrade you may need to clear web browser cookies and web browser cache for the Zabbix web interface to work properly.

Upgrading between minor versions

It is possible to upgrade between minor versions of 4.0.x (for example, from 4.0.1 to 4.0.3). Upgrading between minor versions is easy.

To execute Zabbix minor version upgrade it is required to run:

$ sudo yum upgrade 'zabbix-*'

To execute Zabbix server minor version upgrade run:

$ sudo yum upgrade 'zabbix-server-*'

To execute Zabbix agent minor version upgrade run:

$ sudo yum upgrade 'zabbix-agent-*'

Note that you may also use ‘update’ instead of ‘upgrade’ in these commands. While ‘upgrade’ will delete obsolete packages, ‘update’ will preserve them.
Overview

This section provides the steps required for a successful upgrade from Zabbix 3.4.x to Zabbix 4.0.x using official Zabbix packages for Debian/Ubuntu.

While upgrading Zabbix agents is not mandatory (but recommended), Zabbix server and proxies must be of the same major version. Therefore, in a server-proxy setup, Zabbix server and all proxies have to be stopped and upgraded.

To minimize downtime and data loss during the upgrade, it is recommended to stop and upgrade Zabbix server and then stop, upgrade and start Zabbix proxies one after another. When all proxies are upgraded, start Zabbix server. During the Zabbix server downtime, running proxies will keep collecting and storing data and will pass the data to Zabbix server when the server is up and running. Any notifications for problems during Zabbix server downtime will be generated only after the upgraded server is started.

Note that with SQLite database on proxies, history data from proxies before the upgrade will be lost, because SQLite database upgrade is not supported and the SQLite database file has to be manually removed. When proxy is started for the first time and the SQLite database file is missing, proxy creates it automatically.

Depending on database size the database upgrade to version 4.0 may take a long time.

### Warning:
Before the upgrade make sure to read the relevant upgrade notes!

The following upgrade notes are available:

<table>
<thead>
<tr>
<th>Upgrade from</th>
<th>Read full upgrade notes</th>
<th>Important notes/changes between versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.4.x</td>
<td>For 4.0</td>
<td>'libpthread' and 'zlib' libraries now mandatory; Support for plain text protocol dropped and header is mandatory; Pre-1.4 version Zabbix agents are no longer supported; The Server parameter in passive proxy configuration now mandatory</td>
</tr>
<tr>
<td>3.2.x</td>
<td>Also for 3.4</td>
<td>SQLite support as backend database dropped for Zabbix server/frontend; Perl Compatible Regular Expressions (PCRE) supported instead of POSIX extended; 'libpcre' and 'libevent' libraries mandatory for Zabbix server; Exit code checks added for user parameters, remote commands and system.run[] items without the 'nowait' flag as well as Zabbix server executed scripts; Zabbix Java gateway has to be upgraded to support new functionality</td>
</tr>
<tr>
<td>3.0.x</td>
<td>Also for 3.2</td>
<td>Database upgrade may be slow, depending on the history table size</td>
</tr>
</tbody>
</table>

You may also want to check the requirements for 4.0.

### Note:
It may be handy to run two parallel SSH sessions during the upgrade, executing the upgrade steps in one and monitoring the server/proxy logs in another. For example, run `tail -f zabbix_server.log` or `tail -f zabbix_proxy.log` in the second SSH session showing you the latest log file entries and possible errors in real time. This can be critical for production instances.

#### Upgrade procedure

1. Stop Zabbix processes

Stop Zabbix server to make sure that no new data is inserted into database.

```
# service zabbix-server stop
```

If upgrading Zabbix proxy, stop proxy too.

```
# service zabbix-proxy stop
```
**Attention:** It is known to be possible to upgrade the server only and have older and unupgraded proxies report data to a newer server (the proxies can’t refresh their configuration though). This approach, however, is not recommended and not supported by Zabbix and choosing it is entirely at your own risk.

2 Back up the existing Zabbix database

This is a very important step. Make sure that you have a backup of your database. It will help if the upgrade procedure fails (lack of disk space, power off, any unexpected problem).

3 Back up configuration files, PHP files and Zabbix binaries

Make a backup copy of Zabbix binaries, configuration files and the PHP file directory.

Configuration files:

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

PHP files and Zabbix binaries:

```shell
# cp -R /usr/share/zabbix/ /opt/zabbix-backup/
# cp -R /usr/share/doc/zabbix-* /opt/zabbix-backup/
```

4 Update repository configuration package

To proceed with the update your current repository package has to be uninstalled.

```shell
# rm -Rf /etc/apt/sources.list.d/zabbix.list
Then install the new repository configuration package.
```

On **Debian 9** run:

```shell
# wget https://repo.zabbix.com/zabbix/4.0/debian/pool/main/z/zabbix-release/zabbix-release_4.0-2+stretch_all.deb
# dpkg -i zabbix-release_4.0-2+stretch_all.deb
```

On **Debian 8** run:

```shell
# wget https://repo.zabbix.com/zabbix/4.0/debian/pool/main/z/zabbix-release/zabbix-release_4.0-2+jessie_all.deb
# dpkg -i zabbix-release_4.0-2+jessie_all.deb
```

On **Ubuntu 18.04** run:

```shell
# wget https://repo.zabbix.com/zabbix/4.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_4.0-2+bionic_all.deb
# dpkg -i zabbix-release_4.0-2+bionic_all.deb
```

On **Ubuntu 16.04** run:

```shell
# wget https://repo.zabbix.com/zabbix/4.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_4.0-2+xenial_all.deb
# dpkg -i zabbix-release_4.0-2+xenial_all.deb
```

On **Ubuntu 14.04** run:

```shell
# wget https://repo.zabbix.com/zabbix/4.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_4.0-2+trusty_all.deb
# dpkg -i zabbix-release_4.0-2+trusty_all.deb
```

Update the repository information.

```shell
# apt-get update
```

5 Upgrade Zabbix components

To upgrade Zabbix components you may run something like:

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

If using PostgreSQL, substitute mysql with pgsql in the command. If upgrading the proxy, substitute server with proxy in the command.

6 Review component configuration parameters

See the upgrade notes for details on mandatory changes.

For new optional parameters, see the What’s new section.

7 Start Zabbix processes
Start the updated Zabbix components.

# service zabbix-server start
# service zabbix-proxy start
# service zabbix-agent start

8 Clear web browser cookies and cache

After the upgrade you may need to clear web browser cookies and web browser cache for the Zabbix web interface to work properly.

Upgrade between minor versions

It is possible to upgrade minor versions of 4.0.x (for example, from 4.0.1 to 4.0.3). It is easy.

To upgrade Zabbix minor version please run:

$ sudo apt install --only-upgrade 'zabbix.*'

To upgrade Zabbix server minor version please run:

$ sudo apt install --only-upgrade 'zabbix-server.*'

To upgrade Zabbix agent minor version please run:

$ sudo apt install --only-upgrade 'zabbix-agent.*'

Upgrade from sources

Overview

This section provides the steps required for a successful upgrade from Zabbix 3.4.x to Zabbix 4.0.x using official Zabbix sources.

While upgrading Zabbix agents is not mandatory (but recommended), Zabbix server and proxies must be of the same major version. Therefore, in a server-proxy setup, Zabbix server and all proxies have to be stopped and upgraded.

To minimize downtime and data loss during the upgrade, it is recommended to stop and upgrade Zabbix server and then stop, upgrade and start Zabbix proxies one after another. When all proxies are upgraded, start Zabbix server. During the Zabbix server downtime, running proxies will keep collecting and storing data and will pass the data to Zabbix server when the server is up and running. Any notifications for problems during Zabbix server downtime will be generated only after the upgraded server is started.

Attention:

It is known to be possible to start the upgraded server and have older and unupgraded proxies report data to a newer server (the proxies can’t refresh their configuration though). This approach, however, is not recommended and not supported by Zabbix and choosing it is entirely at your own risk.

Note that with SQLite database on proxies, history data from proxies before the upgrade will be lost, because SQLite database upgrade is not supported and the SQLite database file has to be manually removed. When proxy is started for the first time and the SQLite database file is missing, proxy creates it automatically.

Depending on database size the database upgrade to version 4.0 may take a long time.

Warning:

Before the upgrade make sure to read the relevant upgrade notes!

The following upgrade notes are available:

<table>
<thead>
<tr>
<th>Upgrade from</th>
<th>Read full upgrade notes</th>
<th>Important notes/changes between versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.4.x</td>
<td>For 4.0</td>
<td>'libpthread' and 'zlib' libraries now mandatory; Support for plain text protocol dropped and header is mandatory; Pre-1.4 version Zabbix agents are no longer supported; The Server parameter in passive proxy configuration now mandatory</td>
</tr>
<tr>
<td>Upgrade from</td>
<td>Read full upgrade notes</td>
<td>Important notes/changes between versions</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>3.2.x</td>
<td>Also for 3.4</td>
<td>SQLite support as backend database dropped for Zabbix server/frontend; Perl Compatible Regular Expressions (PCRE) supported instead of POSIX extended; ‘libpcre’ and ‘libevent’ libraries mandatory for Zabbix server; Exit code checks added for user parameters, remote commands and system.run[] items without the ‘nowait’ flag as well as Zabbix server executed scripts; Zabbix Java gateway has to be upgraded to support new functionality</td>
</tr>
<tr>
<td>3.0.x</td>
<td>Also for 3.2</td>
<td>Database upgrade may be slow, depending on the history table size</td>
</tr>
<tr>
<td>2.4.x</td>
<td>Also for 3.0</td>
<td>Minimum required PHP version upped from 5.3.0 to 5.4.0 LogFile agent parameter must be specified</td>
</tr>
<tr>
<td>2.2.x</td>
<td>Also for 2.4</td>
<td>Node-based distributed monitoring removed</td>
</tr>
<tr>
<td>2.0.x</td>
<td>Also for 2.2</td>
<td>Minimum required PHP version upped from 5.1.6 to 5.3.0; Case-sensitive MySQL database required for proper server work; character set utf8 and utf8_bin collation is required for Zabbix server to work properly with MySQL database. See database creation scripts. ‘mysqli’ PHP extension required instead of ‘mysql’</td>
</tr>
</tbody>
</table>

You may also want to check the requirements for 4.0.

**Note:**

It may be handy to run two parallel SSH sessions during the upgrade, executing the upgrade steps in one and monitoring the server/proxy logs in another. For example, run `tail -f zabbix_server.log` or `tail -f zabbix_proxy.log` in the second SSH session showing you the latest log file entries and possible errors in real time. This can be critical for production instances.

Server upgrade process

1 Stop server

Stop Zabbix server to make sure that no new data is inserted into database.

2 Back up the existing Zabbix database

This is a very important step. Make sure that you have a backup of your database. It will help if the upgrade procedure fails (lack of disk space, power off, any unexpected problem).

3 Back up configuration files, PHP files and Zabbix binaries

Make a backup copy of Zabbix binaries, configuration files and the PHP file directory.

4 Install new server binaries

Use these instructions to compile Zabbix server from sources.

5 Review server configuration parameters

See the upgrade notes for details on mandatory changes.

For new optional parameters, see the What’s new section.

6 Start new Zabbix binaries

Start new binaries. Check log files to see if the binaries have started successfully.

Zabbix server will automatically upgrade the database. When starting up, Zabbix server reports the current (mandatory and optional) and required database versions. If the current mandatory version is older than the required version, Zabbix server automatically executes the required database upgrade patches. The start and progress level (percentage) of the database upgrade is written to the Zabbix server log file. When the upgrade is completed, a “database upgrade fully completed” message is written to the log file. If any of the upgrade patches fail, Zabbix server will not start. Zabbix server will also not start if the current mandatory database version is newer than the required one. Zabbix server will only start if the current mandatory database version corresponds to the required mandatory version.
Before you start the server:

- Make sure the database user has enough permissions (create table, drop table, create index, drop index)
- Make sure you have enough free disk space.

7 Install new Zabbix web interface

The minimum required PHP version is 5.4.0. Update if needed and follow [installation instructions](#).

8 Clear web browser cookies and cache

After the upgrade you may need to clear web browser cookies and web browser cache for the Zabbix web interface to work properly.

Proxy upgrade process

1 Stop proxy

Stop Zabbix proxy.

2 Back up configuration files and Zabbix proxy binaries

Make a backup copy of the Zabbix proxy binary and configuration file.

3 Install new proxy binaries

Use these [instructions](#) to compile Zabbix proxy from sources.

4 Review proxy configuration parameters

There are no mandatory changes in this version to proxy parameters. For new optional parameters, see the What’s new section.

5 Start new Zabbix proxy

Start the new Zabbix proxy. Check log files to see if the proxy has started successfully.

Zabbix proxy will automatically upgrade the database. Database upgrade takes place similarly as when starting Zabbix server.

Agent upgrade process

1 Stop agent

Stop Zabbix agent.

2 Back up configuration files and Zabbix agent binaries

Make a backup copy of the Zabbix agent binary and configuration file.

3 Install new agent binaries

Use these [instructions](#) to compile Zabbix agent from sources.

Alternatively, you may download pre-compiled Zabbix agents from the Zabbix download page.

4 Review agent configuration parameters

There are no mandatory changes in this version to agent parameters.

5 Start new Zabbix agent

Start the new Zabbix agent. Check log files to see if the agent has started successfully.

Upgrade between minor versions

When upgrading between minor versions of 4.0.x (for example from 4.0.1 to 4.0.3) it is required to execute the same actions for server/proxy/agent as during the upgrade between major versions. The only difference is that when upgrading between minor versions no changes to the database are made.
Proxy startup with MySQL 8.0.0-8.0.17

zabbix_proxy on MySQL versions 8.0.0-8.0.17 fails with the following “access denied” error:

[Z3001] connection to database 'zabbix' failed: [1227] Access denied; you need (at least one of) the SUPER, SYSTEM_VARIABLES_ADMIN or SESSION_VARIABLES_ADMIN privilege(s) for this operation.

That is due to MySQL 8.0.0 starting to enforce special permissions for setting session variables. However, in 8.0.18 this behavior was removed: As of MySQL 8.0.18, setting the session value of this system variable is no longer a restricted operation.

The workaround is based on granting additional privileges to the zabbix user:

For MySQL versions 8.0.14 - 8.0.17:

grant SESSION_VARIABLES_ADMIN on *.* to 'zabbix'@'localhost';

For MySQL versions 8.0.0 - 8.0.13:

grant SYSTEM_VARIABLES_ADMIN on *.* to 'zabbix'@'localhost';

Upgrade with MariaDB 10.2.1 and before

Upgrading Zabbix may fail if database tables were created with MariaDB 10.2.1 and before, because in those versions the default row format is compact. This can be fixed by changing the row format to dynamic (see also ZBX-17690).

NetBSD 8.0 and newer

Various Zabbix processes may randomly crash on startup on the NetBSD versions 8.X and 9.X. That is due to the too small default stack size (4MB), which must be increased by running:

ulimit -s 10240

For more information, please see the related problem report: ZBX-18275.

Global event correlation

Events may not get correlated correctly if the time interval between the first and second event is very small, i.e. half a second and less.

IPMI checks

IPMI checks will not work with the standard OpenIPMI library package on Debian prior to 9 (stretch) and Ubuntu prior to 16.04 (xenial). To fix that, recompile OpenIPMI library with OpenSSL enabled as discussed in ZBX-6139.

SSH checks

• Some Linux distributions like Debian, Ubuntu do not support encrypted private keys (with passphrase) if the libssh2 library is installed from packages. Please see ZBX-4850 for more details.

• When using libssh 0.9.x on CentOS 8 with OpenSSH 8 SSH checks may occasionally report “Cannot read data from SSH server”. This is caused by a libssh issue (more detailed report). The error is expected to have been fixed by a stable libssh 0.9.5 release. See also ZBX-17756 for details.

• Using the pipe “|” in the SSH script may lead to a “Cannot read data from SSH server” error. In this case it is recommended to upgrade the libssh library version. See also ZBX-21337 for details.

ODBC checks

• MySQL unixODBC driver should not be used with Zabbix server or Zabbix proxy compiled against MariaDB connector library and vice versa, if possible it is also better to avoid using the same connector as the driver due to an upstream bug. Suggested setup:

PostgreSQL, SQLite or Oracle connector → MariaDB or MySQL unixODBC driver MariaDB connector → MariaDB unixODBC driver
MySQL connector → MySQL unixODBC driver

See ZBX-7665 for more information and available workarounds.

• XML data queried from Microsoft SQL Server may get truncated in various ways on Linux and UNIX systems.

• It has been observed that using ODBC checks for monitoring Oracle databases using various versions of Oracle Instant Client for Linux causes Zabbix server to crash. See also: ZBX-18402, ZBX-20803.
If using FreeTDS UnixODBC driver, you need to prepend a ‘SET NOCOUNT ON’ statement to an SQL query (for example, 
```
SET NOCOUNT ON
DECLARE @strsql NVARCHAR(max)
SET @strsql = ....
```
). Otherwise, database monitor item in Zabbix will fail to retrieve the information with an error “SQL query returned empty result”.
See [ZBX-19917](#) for more information.

Incorrect request method parameter in items

The request method parameter, used only in HTTP checks, may be incorrectly set to ‘1’, a non-default value for all items as a result of upgrade from a pre-4.0 Zabbix version. For details on how to fix this situation, see [ZBX-19308](#).

Web monitoring and HTTP agent

Zabbix server leaks memory on CentOS 6, CentOS 7 and possibly other related Linux distributions due to an [upstream bug](#) when “SSL verify peer” is enabled in web scenarios or HTTP agent. Please see [ZBX-10486](#) for more information and available workarounds.

Simple checks

There is a bug in [fping](#) versions earlier than v3.10 that mishandles duplicate echo replay packets. This may cause unexpected results for `icmpping`, `icmppingloss`, `icmppingsec` items. It is recommended to use the latest version of [fping](#). Please see [ZBX-11726](#) for more details.

SNMP checks

If the OpenBSD operating system is used, a use-after-free bug in the Net-SNMP library up to the 5.7.3 version can cause a crash of Zabbix server if the SourceIP parameter is set in the Zabbix server configuration file. As a workaround, please do not set the SourceIP parameter. The same problem applies also for Linux, but it does not cause Zabbix server to stop working. A local patch for the net-snmp package on OpenBSD was applied and will be released with OpenBSD 6.3.

SNMP data spikes

Spikes in SNMP data have been observed that may be related to certain physical factors like voltage spikes in the mains. See [ZBX-14318](#) more details.

SNMP traps

The "net-snmp-perl" package, needed for SNMP traps, has been removed in RHEL/CentOS 8.0-8.2; re-added in RHEL 8.3.

So if you are using RHEL 8.0-8.2, the best solution is to upgrade to RHEL 8.3; if you are using CentOS 8.0-8.2, you may wait for CentOS 8.3 or use a package from EPEL.

Please also see [ZBX-17192](#) for more information.

Alerter process crash in CentOS/RHEL 7

Instances of a Zabbix server alerter process crash have been encountered in Centos/RHEL 7. Please see [ZBX-10461](#) for details.

Compiling Zabbix agent on HP-UX

If you install the PCRE library from a popular HP-UX package site [http://hpux.connect.org.uk](http://hpux.connect.org.uk), for example from file `pcre-8.42-ia64_64-11.31.depot`, you get only the 64-bit version of the library installed in the `/usr/local/lib/hpux64` directory.

In this case, for successful agent compilation customized options need to be used for the “configure” script, e.g.:

```
CFLAGS="-DD64" ./configure --enable-agent --with-libpcre-include=/usr/local/include --with-libpcre-lib=/usr/local/lib/hpux64
```

Flipping frontend locales

It has been observed that frontend locales may flip without apparent logic, i.e. some pages (or parts of pages) are displayed in one language while other pages (or parts of pages) in a different language. Typically the problem may appear when there are several users, some of whom use one locale, while others use another.

A known workaround to this is to disable multithreading in PHP and Apache.

The problem is related to how setting the locale works in PHP: locale information is maintained per process, not per thread. So in a multi-thread environment, when there are several projects run by same Apache process, it is possible that the locale gets changed in another thread and that changes how data can be processed in the Zabbix thread.

For more information, please see related problem reports:

- [ZBX-10911](#) (Problem with flipping frontend locales)
- [ZBX-16297](#) (Problem with number processing in graphs using the `bcddiv` function of BC Math functions)

Compatibility issue with PHP 7.0

It has been observed that with PHP 7.0 importing a template with web monitoring triggers may fail due to incorrectly added double quotes to the web monitoring items in the trigger expressions. The issue goes away when upgrading PHP to 7.1.
PHP 7.3 opcache configuration

If "opcache" is enabled in the PHP 7.3 configuration, Zabbix frontend may show a blank screen when loaded for the first time. This is a registered PHP bug. To work around this, please set the "opcache.optimization_level" parameter to 0x7FFFBFDF in the PHP configuration (php.ini file).

Graphs

Changes to Daylight Saving Time (DST) result in irregularities when displaying X axis labels (date duplication, date missing, etc).

Log file monitoring

10g[] and 10g[] items repeatedly reread log file from the beginning if file system is 100% full and the log file is being appended (see ZBX-10884 for more information).

Slow MySQL queries

Zabbix server generates slow SELECT queries in case of non-existing values for items. This issue is known to occur in MySQL 5.6/5.7 versions (for an extended discussion, see ZBX-10652), and, in specific cases, may also occur in later MySQL versions. A workaround to this is disabling the index_condition_pushdown or prefer_ordering_index optimizer in MySQL. Note, however, that this workaround may not fix all issues related to slow queries.

MariaDB row size error

Prior to MariaDB 10.2.26, 10.3.17, and 10.4.7, MariaDB didn’t properly calculate the row sizes while executing DDL, so “unsafe” tables could be created, even with innodb_strict_mode=ON set. This was fixed by MDEV-19292. As a side effect, tables that could be created in previous versions may get rejected after the latest releases.

Suggested database changes for existing 4.0 installations:

```
shell> mysql -uroot -p<password>
mysql> alter table `host_inventory` modify `name` varchar(128) default '' not null, modify `alias` varchar(128) default '' not null, modify `os` varchar(128) default '' not null, modify `os_short` varchar(128) default '' not null;
```

Suggested database changes for new 4.0 installations:

```
shell> mysql -uroot -p<password>
mysql> set global innodb_strict_mode='OFF';
```

Perform database creation as usual and fix schema after:

```
shell> mysql -uroot -p<password>
mysql> alter table `host_inventory` modify `name` varchar(128) default '' not null, modify `alias` varchar(128) default '' not null, modify `os` varchar(128) default '' not null, modify `os_short` varchar(128) default '' not null;
mysql> set global innodb_strict_mode='ON';
```

API

The output parameter does not work properly with the history.get method (fixed in 4.0.11).

API login

A large number of open user sessions can be created when using custom scripts with the user.login method without a following user.logout.

IPv6 address issue in SNMPv3 traps

Due to a net-snmp bug, IPv6 address may not be correctly displayed when using SNMPv3 in SNMP traps. For more details and a possible workaround, see ZBX-14541.

IE11 issue with map resizing in dashboard widgets

Maps, in Internet Explorer 11, are cut off on the right side if the map content is larger than the dashboard widget area (instead of being resized proportionately). This is intentional because of an IE11-related issue with proper resizing of SVG images.

Zabbix agent checks on Windows

Non-existing DNS entries in a Server parameter of Zabbix agent configuration file (zabbix_agentd.conf) may increase Zabbix agent response time on Windows. This happens because Windows DNS caching daemon doesn’t cache negative responses for IPv4 addresses. However, for IPv6 addresses negative responses are cached, so a possible workaround to this is disabling IPv4 on the host.

MySQL custom error codes

If Zabbix is used with MySQL installation on Azure, an unclear error message [9002] Some errors occurred may appear in Zabbix logs. This generic error text is sent to Zabbix server or proxy by the database. To get more information about the cause of the error, check Azure logs.

Known issues in 4.0.0
• Fullscreen mode for the dashboards cannot be accessed with the respective URL parameter: `/zabbix.php?action=dashboard.view&fullscreen=1`. Fixed in 4.0.1.

• When filtering triggers in Monitoring → Overview (Triggers), trigger severity instead of problem severity is taken into account. Known issues in 4.0.0, 4.0.1

• Upgrade to 4.0.0 and 4.0.1 from Zabbix 3.0 does not replace `{TRIGGER.NAME}` macros to `{EVENT.NAME}` macros like it should. Fixed for 4.0.2.

Known issues in 4.0.0 - 4.0.2

• If the Check now request is performed from the item list for items that do not support it (template items, active agent items, etc.), a 'Request sent successfully' message is displayed even though the functionality does not work for these items. Fixed in 4.0.3, by displaying a corresponding error message.

Known issues in 4.0.2

• Parent host group selection does not work in the following locations:
  - Monitoring → Problems filter
  - Monitoring → Dashboard widgets with host group selection:
  - Reports → Triggers top 100 filter

Known issues in 4.0.0 - 4.0.3

• Time suffixes do not work in constants of calculated item formulas. Fixed in 4.0.4.

• Negative problem duration affects the total result in SLA calculation or Availability report, making it incorrect. Fixed in 4.0.4.

Known issues in 4.0.3

• If an item is deleted that has a low-level discovery created trigger, the trigger is not deleted. This leads to "orphaned" problems (with no item/host) being displayed in the problem view. Similarly, if an item is deleted that has low-level discovery created dependent item, the dependent item is not deleted. Fixed in 4.0.4.

Known issues starting with 4.0.3

• Failed login attempt message has been changed to display only the first 39 characters of a stored IP address as that's the character limit in the database field. That means that IPv6 IP addresses longer than 39 characters will be shown incompletely.

Known issues in 4.0.0 - 4.0.5

• net.dns[] Zabbix agent item does not support IPv6 addresses in its first parameter. Fixed in 4.0.6.

Slow event info retrieval with older MySQL databases

Zabbix 4.0 installations with MySQL 5.X and 8.0.19 might run a slow query when retrieving problem/event information from the database. In particular, this affects the Problems by severity widget, event.get and problem.get API methods. To improve performance of SQL statements, apply the patch provided in ZBX-18080 (available for Zabbix 4.0.26 and newer).

Known issues in 4.0.6, 4.0.7

• IPMI pollers are unable to process more than 60 items per minute. Fixed in 4.0.8.

• You may encounter the issue of 100% CPU usage by IPMI pollers if using OpenIPMI version 2.0.26 and above. Fixed in 4.0.8.

Known issues in 4.0.8

• This version requires write permissions to the assets directory for the web server user. This requirement, however, would break those installations of the frontend where the web server has no write permissions to the document root (see ZBX-16180 for details). As a result, this requirement is rolled back in 4.0.9.

Known issues in 4.0.0 - 4.0.15

• High memory usage has been observed during process startup with SQLite 3.7.17 on Centos/RHEL 7. The startup process has been improved in 4.0.16 to avoid similar issues with other databases as well. See ZBX-9084 for more details.

8 Template changes

This page lists all changes to the stock templates that are shipped with Zabbix.

Note that upgrading to the latest Zabbix version will not automatically upgrade the templates used. It is suggested to modify the templates in existing installations by:

• Downloading the latest templates from the Zabbix Git repository:
• Then, while in Configuration → Templates you can import them manually into Zabbix. If templates with the same names
already exist, the Delete missing options should be checked when importing to achieve a clean import. This way the old
items that are no longer in the updated template will be removed (note that it will mean losing history of these old items).

Changes in 4.0.0  New templates

New templates are available for monitoring some IBM, Dell, HP, Cisco UCS and Supermicro Aten hardware:

• Template Server IBM IMM SNMPv1/2
• Template Server Dell iDRAC SNMPv2
• Template Server HP iLO SNMPv2
• Template Server Supermicro Aten SNMPv2
• Template Server Cisco UCS SNMPv2

These templates are part of the default Zabbix dataset for new installations. If you are upgrading from previous versions, you can
import these templates manually.

Improved naming style

Naming style of groups and applications has been improved for some out-of-the-box templates.

Positional macros removed

 Deprecated positional macros have been removed from item names in standard templates.

Server/proxy template

The default Zabbix server/proxy templates (Template App Zabbix Server, Template App Zabbix Proxy) have been changed.

While some items have been renamed, there are also some completely new items:

• Number of processed character values per second
• Number of processed log values per second
• Number of processed not supported values per second
• Number of processed numeric (float) values per second
• Number of processed numeric (unsigned) values per second
• Number of processed text values per second

The following items are new and replace some old ones:

• Zabbix configuration cache, % used - replaces Zabbix configuration cache, % free
• Zabbix history index cache, % used - replaces Zabbix history index cache, % free
• Zabbix history write cache, % used - replaces Zabbix history write cache, % free
• (in server template only) Zabbix trend write cache, % used - replaces Zabbix trend write cache, % free
• (in server template only) Zabbix value cache, % used - replaces Zabbix value cache, % free

The trigger expressions using the replaced items have been updated accordingly.

Changes in 4.0.2  OS Linux template

Two new items have been added to Template_OS_Linux:

• CPU guest time - the time spent running a virtual CPU for guest operating systems
• CPU guest nice time - the time spent running a niced guest (virtual CPU for guest operating systems)

The CPU utilization graph has been updated to include these two items.

Changes in 4.0.3  Tomcat template

Template App Apache Tomcat JMX has been updated:

• support for recent Tomcat versions has been added
• the following macros have been defined: {$PROTOCOL_HANDLER_HTTP}, {$PROTOCOL_HANDLERHTTPS}, {$PROTOCOL- COL_HANDLER_AJP}

Changes in 4.0.5  New templates

New templates are available for remote monitoring of Zabbix server or proxy internal metrics from an external instance:

• Template App Remote Zabbix server
• Template App Remote Zabbix proxy

Note that in order to use a template for remote monitoring of multiple external instances, a separate host is required for each
external instance monitoring.
Changes in 4.0.6  VMware template

Template VM VMware has been updated:

- the key of the “Event log” item has been changed to `vmware.eventlog[{$URL},skip]` - now skipping old data

Changes in 4.0.7  SNMP interface templates

Update intervals have been changed from 5m to 3m for these LLD item prototypes:

- Interface `{#IFNAME}({#IFALIAS})`: Inbound packets with errors
- Interface `{#IFNAME}({#IFALIAS})`: Outbound packets with errors

in:

- Template Module Interfaces Simple SNMPv1
- Template Module Interfaces Simple SNMPv2
- Template Module Interfaces SNMPv1
- Template Module Interfaces SNMPv2
- Template Module Interfaces Windows SNMPv2

These update intervals have been changed to avoid creation of excess internal events caused by trigger state flapping.

Changes in 4.0.13  Juniper template

The more correct OID of ‘jnxOperatingCPU’ (1.3.6.1.4.1.2636.3.1.13.1.8) is now used instead of ‘jnxOperating5MinLoadAvg’ (1.3.6.1.4.1.2636.3.1.13.1.21) in these LLD item and trigger prototypes:

- `{#SNMPVALUE}`: CPU utilization
- `{#SNMPVALUE}`: High CPU utilization

in:

- Template Net Juniper SNMPv2

Changes in 4.0.14  New Cisco UCS server template

A Cisco UCS server monitoring template - Template Server Cisco UCS SNMPv2 has been added.

It will be available in Configuration → Templates in new installations. If you are upgrading from previous versions, you can find this template in the templates directory of the downloaded latest Zabbix version. Then, while in Configuration → Templates you can import it manually into Zabbix.

HP iLO template

The counter for overall server health check has been fixed in the Template Server HP iLO SNMPv2 template.

HP Comware template

The Template Net HP Comware HH3C SNMPv2 now contains the correct value mapping.

Changes in 4.0.15  Low-level discovery rules have been split from the parent template Template Module HOST-RESOURCES-MIB SNMPv2 into separate linked templates:

- Template Module HOST-RESOURCES-MIB storage SNMPv2
- Template Module HOST-RESOURCES-MIB memory SNMPv2
- Template Module HOST-RESOURCES-MIB CPU SNMPv2

Other changes:

- A CPU utilization item has been added to Template Module HOST-RESOURCES-MIB CPU SNMPv2;
- The filesystem discovery filter has been improved to exclude some unnecessary values in Template Module HOST-RESOURCES-MIB storage SNMPv2 (linked to Template OS Windows SNMPv2, Template Net Arista SNMPv2);
- The network interface discovery filter has been improved to exclude some unnecessary values in Template Module Interfaces Windows SNMPv2 (linked to Template OS Windows SNMPv2);
- Discovery filters in several templates are now defined by template-level user macros (for example `{$VFS.FS.FSNAME.MATCHES}` and `{$VFS.FS.FSNAME.NOT_MATCHES}`) that can be overridden on host or linked-template level for flexibility:
  - Template Module HOST-RESOURCES-MIB storage SNMPv2
  - Template Module HOST-RESOURCES-MIB memory SNMPv2
  - Template Module HOST-RESOURCES-MIB CPU SNMPv2
  - Template Module Interfaces Windows SNMPv2
Changes in 4.0.16  Low-level discovery rules have been split into separate linked templates for the following template:

- Template Module HOST-RESOURCES-MIB SNMPv1

Changes in 4.0.25  VMware template

Template VM VMware has been updated:

- the type of information for the "VMware: Free space on datastore (percentage)" item has been corrected and is now set to Numeric (float).
- The following template macros now have more specific names:
  - {$URL} renamed to {$VMWARE.URL}
  - {$USERNAME} renamed to {$VMWARE.USERNAME}
  - {$PASSWORD} renamed to {$VMWARE.PASSWORD}

9 Upgrade notes for 4.0.0

These notes are for upgrading from Zabbix 3.4.x to Zabbix 4.0.0. All notes are grouped into:

- Critical - the most critical information related to the upgrade process and the changes in Zabbix functionality
- Informational - all remaining information describing the changes in Zabbix functionality

It is possible to upgrade to Zabbix 4.0.0 from versions before Zabbix 3.4.0. See the upgrade procedure section for all relevant information about upgrading from previous Zabbix versions.

Critical  Additional dependencies

- libpthread - the POSIX Threads library is now mandatory when compiling Zabbix server and Zabbix proxy. It is required for process-shared mutexes and read-write locks. If mutexes are available, but cannot be process shared then Zabbix will fall back to using semaphores as before the upgrade.
- zlib - the compression library is now mandatory when compiling Zabbix server and Zabbix proxy.

Compression for server-proxy communication

Communication between Zabbix server and Zabbix proxies is now using compression to reduce network load and increase performance on low bandwidth network links.

Note that the header of Zabbix requests/responses has been changed as part of this development.

Warning:  
If you are using network security devices like IDS/IPS or NGFW in your network and you are using Zabbix proxies, please make sure your application definitions are up to date for the new Zabbix proxy protocol prior to upgrading to 4.0.x as there have been reports on these devices dropping the traffic when encountering the compression in the network stream. Please contact your security vendor for more information on how to obtain updated definitions or possible workarounds if you run into this problem.

Server parameter for passive proxies mandatory

The Server parameter in passive proxy configuration, which previously was ignored, is now mandatory. The passive proxy will reject an address that is not listed in the Server parameter.

Plain text protocol dropped

Support for the plain text protocol has been dropped and a header is now mandatory. A header has been added to Zabbix get requests, Zabbix server/proxy passive check requests and frontend requests to Zabbix server.

As a consequence, Zabbix agents that are older than version 1.4 are no longer supported. Also, messages from self-written senders will be rejected if the header is absent. Whereas previously Zabbix trappers would accept messages without headers as well as messages with headers, now they will only accept messages with protocol header.

Requests from an older Zabbix get version to the new agent will fail. Note that in this case the following error message is displayed:

Check access restrictions in Zabbix agent configuration

Loadable modules

History export via module is no longer supported by Zabbix proxy.

Monitoring → Triggers section removed
Monitoring → Triggers section is now removed. Related global parameters “Show events not older than” and “Max count of events per trigger to show” are removed as well respectively.

Disallowed item key parameter syntax

The following item key parameter syntax is no longer supported:

- Multi-level parameter arrays, e.g. [a, [b, [c, d]], e]
- Zapcat-style parameters, e.g. [a][b]

Note that this syntax was never used by official Zabbix item keys, nor was it ever officially documented as supported. It only existed for backward compatibility with such solutions as Zapcat JMX Zabbix Bridge.

Note that this change does not affect single-level parameters. See aggregate items for information about supported syntax.

MySQL 8.0 support

To be able to add support of MySQL 8.0 in this version, two database changes have been made:

- ‘groups’ table has been renamed to ‘hstgrp’
- ‘function’ field in the ‘functions’ table has been renamed to ‘name’

Trigger functions

During the upgrade, parameter values of the logsource trigger function will be converted to work with added support of regular expressions and global regular expressions. There can be cases when existing parameters contain an extensive amount of regular expression special characters or their length is close to the maximum allowed limit and during conversion will exceed that maximum allowed length limit which is 255 characters. In such cases no changes will be made to those parameters and details about all these cases will be added to the log file. If there are issues with trigger performance because of this, the parameters that were not changed have to be edited manually.

HTTP authentication

When default system authentication was previously set to ‘HTTP authentication’ during the upgrade it will be changed to ‘Internal’ with ‘HTTP Authentication’ enabled by default. For such configuration it is required to clear existing user default password values in the database executing the following query:

```
UPDATE users SET passwd="" WHERE passwd=md5('zabbix')
```

API related changes

HTTP basic-authentication specific code was removed from API, therefore the password field is now mandatory for the API user.login action.

Upgrade with MariaDB 10.2.1 and before

Upgrading Zabbix may fail if database tables were created with MariaDB 10.2.1 and before, because in those versions the default row format is compact. This can be fixed by changing the row format to dynamic (see also ZBX-17690).

API changes

See the list of API changes in Zabbix 4.0.0.

Informational  Deprecated macros in item names

Using positional ($1, $2, ...$9) and user macros in item and item prototype names is now deprecated. As a consequence, positional macros have been removed from item names and item prototype names in the standard templates shipped with Zabbix 4.0.

If you keep using positional macros, you will encounter the following difficulties when using the new graph widget:

- It will not be possible to add any of the items named like CPU $2 time individually to the graph, using its resolved name (like CPU user time)
- It will only be possible to add all items having the name like CPU $2 time to the graph (e.g. CPU user time, CPU system time, CPU idle time, etc.)

If you are using positional macros in item prototype names, it is suggested to update discovery rules manually by replacing the positional macro with the respective low-level discovery macro, for example, replace:
in the old item prototype naming with:

in the new item prototype naming. It will be possible to use items generated this way in the graph widget with no limitations.

Timestamp correction

Zabbix server will no longer adjust value timestamps in cases when Zabbix proxy/active agent/sender time differs from Zabbix server time.

Time triggers processed by history syncers

The processing of time-based trigger functions such as `nodata()`, `date()`, `dayofmonth()`, `dayofweek()`, `time()` and `now()` has been moved from timer processes to history syncers.

While previously all time-based triggers were recalculated at the same time, creating peak loads every 30 seconds, now the time-based trigger processing is evenly spread within those 30 seconds.

With this change, the required number of timer processes may have to be recalculated, especially if previously multiple timers were configured to share the time-based trigger calculation load. Even though the time-based trigger calculations do not affect timer load anymore, maintenance calculations may require more resources and thus multiple timers can be configured to share the maintenance processing load.

Impact of host maintenance on trigger level

When a host enters maintenance, Zabbix server timer processes will now read all open problems to check if it is required to suppress those. This may have a performance impact if there are many open problems. Zabbix server will also read all open problems upon startup, even if there are no maintenance configured at the time.

If maintenance period, hosts, groups or tags are changed by user, the changes will only take effect after configuration cache synchronization.

Auto-registration changes

Auto-registration behavior has been changed in the following way:

- Active agent auto-registration actions will be rerun if host metadata is changed;
- Since metadata is only added during auto-registration, manually created hosts will have metadata missing and auto registration will be re-run;
- If a host is manually changed to be monitored by another Zabbix proxy, then auto-registration will be re-run.

As before, if auto-registration for the same host comes from a new Zabbix proxy, then auto-registration will be re-run.

Problem name generation
Problem and event names are now stored directly in the event and problem tables upon event generation, instead of being generated in runtime as previously. A database patch will populate the new problem name and event name fields without macros expanded. Note that these changes will require more storage space.

Warning:
Database upgrade during the initial server startup may take a long time if there are a lot of old events and {ITEM.VALUE}, {ITEM.LASTVALUE} macros are used in trigger names.

The values for the populated event and problem name fields are:

- For trigger events - trigger name with all the macros resolved
- For internal problem events:
  - Cannot obtain item value - for unsupported items
  - Cannot calculate trigger expression - for unknown triggers
- For the rest of events the name will be empty

Related macro changes
Since problem names are no longer generated in runtime based on the current trigger name, and instead are being generated at the time of event, there are corresponding macro changes:

- In all default messages - {TRIGGER.NAME} has been replaced by {EVENT.NAME};
- In all trigger-based actions - {TRIGGER.NAME} will be replaced by {EVENT.NAME} when upgrading.

See also: known issues
Working with problems
Several changes have been made for working with problems, including changed macros. For more details, see the what’s new entry.

Related API changes
 problem.get and event.get methods have been changed in such a way that input parameter search/filter with object (‘name’: ‘...’) as value is used to find matching results (by field “name”) in the corresponding table (“problem” or “events”).

problem.get and event.get methods have been extended by adding a response parameter called “name”. For both methods, the new parameter contains a value from the newly added “name” field in the database table “problem” or “events”.

Server configuration cache usage
The server configuration cache has been modified to keep all host inventory information in it. If you are using the inventory functionality with hosts, increase the dedicated configuration cache memory for the server accordingly.

Execution of external check script
Upon completion of an external check script, arguments are wrapped to single quotes ' instead of double quotes " . This change allows Zabbix to accept more signs in an external check parameter’s name. For example, the $ sign is no longer ignored.

Zabbix Java gateway availability
From now on Zabbix Java gateway availability status will not change to red each time any of the items become not supported. The JMX availability badge will only become red on network errors - when Java gateway is not available or when there are some communication problems between Zabbix server and Zabbix Java gateway.

Zabbix Java gateway logs modified
If you monitor Java gateway logs, keep in mind that exception stack trace is no longer available in warning and error level logging of Java gateway.

Trigger changes

<p>| Trigger expression's behavior regarding numbers, differing by 0.000001, is now changed. Since logical operators are defined in terms of equality to zero, their result for 0.000001 is affected too: |
|---|---|---|
| Expression (Example) | Before | After |
| 1.000001 &gt; 1 | 1 | 0 |
| 1.000001 &lt;= 1 | 0 | 1 |
| 0 &gt;= 0.000001 | 0 | 1 |
| 0.000001 &lt;&gt; 0 | 1 | 0 |
| 0.000001 = 0 | 0 | 1 |</p>
<table>
<thead>
<tr>
<th>Expression (Example)</th>
<th>Evaluation result</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 or (1/1000000)</td>
<td>1</td>
</tr>
<tr>
<td>not (1/1000000)</td>
<td>0</td>
</tr>
<tr>
<td>1 and 1/1000000</td>
<td>1</td>
</tr>
</tbody>
</table>

Renamed widgets, screen elements and reports

The following elements have been renamed:

<table>
<thead>
<tr>
<th>Previously</th>
<th>In Zabbix 4.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>System status</td>
<td>Problems by severity</td>
</tr>
<tr>
<td>Host status</td>
<td>Problem hosts</td>
</tr>
<tr>
<td>Status of Zabbix</td>
<td>System information</td>
</tr>
</tbody>
</table>

Dashboard API is also affected: some of Dashboard widget property types are now renamed.

Host column always displayed

The host column is now always displayed even if only one host is selected in:

- Monitoring → Latest data
- Monitoring → Web
- Reports → Availability

This results in a wider page than previously with one host data. For more information, see the What’s new section.

JMX monitoring error message

As Zabbix java gateway now supports working with custom MBeans returning non-primitive data types, which override the `toString()` method, the possible error message has been changed the following way:

<table>
<thead>
<tr>
<th>Previously</th>
<th>In Zabbix 4.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>data object type is not primitive: xxx</td>
<td>Data object type cannot be converted to string.</td>
</tr>
</tbody>
</table>

Logging changes

The message printed to the log files about a full history cache has been changed the following way:

<table>
<thead>
<tr>
<th>Previously</th>
<th>In Zabbix 4.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>History buffer is full. Sleeping for 1 second.</td>
<td>History cache is full. Sleeping for 1 second.</td>
</tr>
</tbody>
</table>

See also

- Template changes

10 Upgrade notes for 4.0.1

This minor version does not have any upgrade notes.

11 Upgrade notes for 4.0.2

Frontend changes

- Host group selection window no longer offers to select host groups with templates only in the following locations:
  - Monitoring → Problems filter
  - Monitoring → Dashboard widgets:
    - Problems, Problems by hosts, Problems by severity, Data overview, Trigger overview, Web monitoring
  - Monitoring → Screens:
    - Host issues, Host group issues, Data overview, Trigger overview, Host info, Trigger info
12 Upgrade notes for 4.0.3

Frontend changes
- Frontend no longer enforces HTTP Strict Transport Security (HSTS) policy, introduced in 4.0.0. To protect Zabbix frontend against protocol downgrade attacks, it is recommended to enable HSTS policy on the webserver.

14 Upgrade notes for 4.0.5

This minor version does not have any upgrade notes.

15 Upgrade notes for 4.0.6

Discovered items disallowed as master item
Discovered items no longer can be set as the master item for dependent items.

16 Upgrade notes for 4.0.7

Items
- Trailing whitespace is no longer allowed after the maxdelay parameter in log[], log.count[], logrt[], logrt.count[] items.

17 Upgrade notes for 4.0.8

Frontend
- In this version only, write permissions to the assets directory are required for the web server user. (See also known issues.)
- The styles folder has been moved to the assets directory, which is important if creating a custom theme.
- Media types in the Action log dashboard widget/screen element are now sorted by media type ID instead of media type name.

18 Upgrade notes for 4.0.9

This minor version does not have any upgrade notes.

19 Upgrade notes for 4.0.10

This minor version does not have any upgrade notes.
20 Upgrade notes for 4.0.11

This minor version does not have any upgrade notes.

21 Upgrade notes for 4.0.12

Global notifications

Default audio clips are now in MP3 (it used to be wave files). An embedded media player is not used any more (it was used for Internet Explorer only), so now, in case of custom audio files, you must be sure that your browser can play them (or just use the MP3 format).

Leading and trailing spaces disallowed in host names

Leading and trailing spaces are no longer allowed in host and template names.

22 Upgrade notes for 4.0.13

Item update interval for unreachable hosts

A bug related to item check time on unreachable hosts has been fixed. This bug was introduced in Zabbix version 3.4.9 or 4.0.0. Now the item check period is recalculated based on the UnavailableDelay value, not on the item update period. This can potentially change unreachable poller performance. For example, if item previously had a delay of 1h then now it will be checked based on the UnavailableDelay value, not every 1h as it was (due to bug). Therefore it is recommended to increase UnavailableDelay value to avoid possible unreachable poller overload.

23 Upgrade notes for 4.0.14

Zabbix frontend sets own cookie path

If Zabbix frontend runs behind proxy, cookie path set by Zabbix now needs to be specified in the proxy configuration. See using Zabbix frontend behind proxy for details.

24 Upgrade notes for 4.0.15

This minor version does not have any upgrade notes.

25 Upgrade notes for 4.0.16

Real-time export of events, items, trends

In case of a write error during the export (data cannot be written to the export file or the export file cannot be renamed or a new one cannot be created after renaming it), the data item is now dropped and never written to the export file. It is written only in the Zabbix database. Writing data to the export file is resumed when the writing problem is resolved.

Previously, in case of a write error, Zabbix would retry with a 10 second interval until success. The previous behavior, while ensuring history data equivalence between database and the export files resulted in actually stopping monitoring until the problem with the export file was fixed. Now the priority is given to continued monitoring rather than keeping the export file in sync with database at all cost.

See also: Real-time export of events, items, trends

Sound in browsers

Sounds are now supported in MP3 format only.
26 Upgrade notes for 4.0.17

Timeout value in web scenario steps
The timeout value in a web scenario step can no longer be '0'. Similarly, any user macros used in this field must not resolve to '0'.

27 Upgrade notes for 4.0.18

Building with libxml2
When building with libxml2, pkg-config is now used instead of xml2-config to detect and use libxml2, as xml2-config is to be removed from libxml2 in the future.

DB character set and collation check
A check for the correct character set and collation is now performed on the database, database tables and table fields during the initial frontend installation. If the check fails a warning message is displayed.

A warning message is also displayed in Reports → System information.

28 Upgrade notes for 4.0.19

This minor version does not have any upgrade notes.

29 Upgrade notes for 4.0.20

Item changes
The Timeout configuration parameter is now used for web.page.get, web.page.regexp and web.page.perf items.

Maintenance and Daylight Saving Time
In previous Zabbix versions, maintenance period calculation was unaware of the possible effects caused by Daylight Saving Time change resulting in unpredictable behaviours. In the new version Daylight Saving Time (DST) change is cared for and should not unpredictably affect how long the maintenance will be. Let’s say we have a two-hour maintenance that usually starts at 1am and finishes at 3am. If after one hour of maintenance (at 2am) a DST change happens and current time changes from 2:00 to 3:00, the maintenance will continue for one more hour till 4:00.

Docker appliance support dropped
Zabbix Docker Appliance image has been decommissioned and will not be available for 4.0.20 and newer releases. Please use a separate Docker image for each component instead of the all-in-one solution.

Non-root permissions implemented for Docker images
Zabbix Docker images have been updated to implement non-root container best practices. Due to the change:

• All directories have been restricted for the container user, except directories which are required for the container. For example, /etc/zabbix/ with Zabbix component configuration files.
• Ports 80 and 443 have been changed to 8080 and 8443, because usage of all ports <1024 is restricted for non-privileged users. Zabbix web interface images have been updated to use non-privileged ports 8080, 8443; Zabbix snmptrap images port 1162.
• All Zabbix images are updated to use a non-privileged user. By default, ‘zabbix’ with UID 1997.

A known issue: Nginx based images do not run under root. Will be fixed soon.

30 Upgrade notes for 4.0.21

This minor version has no upgrade notes.
31 Upgrade notes for 4.0.22

Enhanced URL widget security

The URL dashboard widget and the URL screen element now put retrieved URL content into the sandbox. By default, all sandbox restrictions are enabled. It is possible to modify sandbox attribute settings in the defines.inc.php file, however turning sandboxing off is not recommended for security reasons. To learn more about the sandbox attribute, please see the sandbox section of the iframe HTML element description.

32 Upgrade notes for 4.0.23

This minor version does not have any upgrade notes.

33 Upgrade notes for 4.0.24

This minor version does not have any upgrade notes.

34 Upgrade notes for 4.0.25

This minor version does not have any upgrade notes.

35 Upgrade notes for 4.0.26

Dropping values outside history/trend periods

From now on values older than the configured history and trend storage period will be rejected, even if the internal housekeeping is disabled. You may want to adjust history/trend storage periods after the upgrade.

36 Upgrade notes for 4.0.27

Positional macros in web monitoring items

Deprecated positional macros ($1, $2, ...) are no longer used in the item names when creating web monitoring items.

In those cases where positional macros are used in existing web monitoring items, the item names will be updated in the database not to use positional macros as soon as the web scenario is updated.

Web monitoring items

Removed support of {HOST.*} macro in name property of web scenario and web scenario step.

37 Upgrade notes for 4.0.28

Host/template cloning

Long lists of objects to be cloned (items, triggers, graphs, etc) have been removed from host and template full clone forms.
38 Upgrade notes for 4.0.29

This minor version does not have any upgrade notes.

39 Upgrade notes for 4.0.30

This minor version does not have any upgrade notes.

40 Upgrade notes for 4.0.31

This minor version does not have any upgrade notes.

41 Upgrade notes for 4.0.32

This minor version does not have any upgrade notes.

42 Upgrade notes for 4.0.33

This minor version does not have any upgrade notes.

43 Upgrade notes for 4.0.34

Items

The `vmware.eventlog[]` item for VMware monitoring, when used with the 'skip' option, e.g., `vmware.eventlog[<url>,skip]` now behaves differently after being recreated (i.e., previous item removed, new one created with a different internal ID) - now the internal events cache is reset and only new events are read. Previously, the skip option would not be enforced in this scenario.

44 Upgrade notes for 4.0.35

This minor version does not have any upgrade notes.

45 Upgrade notes for 4.0.36

This minor version does not have any upgrade notes.

46 Upgrade notes for 4.0.37

This minor version does not have any upgrade notes.
47 Upgrade notes for 4.0.38

This minor version does not have any upgrade notes.

48 Upgrade notes for 4.0.39

This minor version does not have any upgrade notes.

5. Quickstart

Please use the sidebar to access content in the Quickstart section.

1 Login and configuring user

Overview

In this section you will learn how to log in and set up a system user in Zabbix.

Login

This is the Zabbix “Welcome” screen. Enter the user name Admin with password zabbix to log in as a Zabbix superuser.

When logged in, you will see ‘Connected as Admin’ in the lower right corner of the page. Access to Configuration and Administration menus will be granted.

Protection against brute force attacks

In case of five consecutive failed login attempts, Zabbix interface will pause for 30 seconds in order to prevent brute force and dictionary attacks.

The IP address of a failed login attempt will be displayed after a successful login.

Adding user
To view information about users, go to Administration → Users.

<table>
<thead>
<tr>
<th>Alias</th>
<th>Name</th>
<th>Surname</th>
<th>User Type</th>
<th>User Group</th>
<th>Login Time</th>
<th>Frontend Access</th>
<th>Debug Mode</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin</td>
<td>Zabbix</td>
<td>Administrator</td>
<td>Super Admin</td>
<td>Zabbix administrators</td>
<td>Yes (2015-08-05 17:25:44)</td>
<td>Ok</td>
<td>System default</td>
<td>Disabled</td>
</tr>
<tr>
<td>guest</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

To add a new user, click on Create user.

In the new user form, make sure to add your user to one of the existing user groups, for example ‘Zabbix administrators’.
All mandatory input fields are marked with a red asterisk.

By default, new users have no media (notification delivery methods) defined for them. To create one, go to the ‘Media’ tab and click on Add.
In this pop-up, enter an e-mail address for the user.

You can specify a time period when the medium will be active (see Time period specification page for description of the format), by default a medium is always active. You can also customize trigger severity levels for which the medium will be active, but leave all of them enabled for now.

Click on Add, then click Add in the user properties form. The new user appears in the userlist.

Adding permissions

By default, a new user has no permissions to access hosts. To grant the user rights, click on the group of the user in the Groups column (in this case - 'Zabbix administrators'). In the group properties form, go to the Permissions tab.

This user is to have read-only access to Linux servers group, so click on Select next to the user group selection field.
In this pop-up, mark the checkbox next to ‘Linux servers’, then click Select. Linux servers should be displayed in the selection field. Click the ‘Read’ button to set permission level and then Add to add the group to the list of permissions. In the user group properties form, click Update.

**Attention:**
In Zabbix, access rights to hosts are assigned to user groups, not individual users.

Done! You may try to log in using the credentials of the new user.

**2 New host**

**Overview**
In this section you will learn how to set up a new host.

A host in Zabbix is a networked entity (physical, virtual) that you wish to monitor. The definition of what can be a “host” in Zabbix is quite flexible. It can be a physical server, a network switch, a virtual machine or some application.

**Adding host**
Information about configured hosts in Zabbix is available in Configuration → Hosts. There is already one pre-defined host, called ‘Zabbix server’, but we want to learn adding another.

To add a new host, click on Create host. This will present us with a host configuration form.
All mandatory input fields are marked with a red asterisk.

The bare minimum to enter here is:

**Host name**
- Enter a host name. Alphanumerics, spaces, dots, dashes and underscores are allowed.

**Groups**
- Select one or several existing groups by clicking Select button or enter a non-existing group name to create a new group.

**Note:**
All access permissions are assigned to host groups, not individual hosts. That is why a host must belong to at least one group.

**IP address**
- Enter the IP address of the host. Note that if this is the Zabbix server IP address, it must be specified in the Zabbix agent configuration file ‘Server’ directive.

**Other options** will suit us with their defaults for now.

When done, click Add. Your new host should be visible in the host list.

**Note:**
If the ZBX icon in the Availability column is red, there is some error with communication - move your mouse cursor over it to see the error message. If that icon is gray, no status update has happened so far. Check that Zabbix server is running, and try refreshing the page later as well.

**3 New item**
Overview
In this section you will learn how to set up an item.

Items are the basis of gathering data in Zabbix. Without items, there is no data - because only an item defines a single metric or what data to get off of a host.

Adding item
All items are grouped around hosts. That is why to configure a sample item we go to Configuration → Hosts and find the ‘New host’ we have created.
The Items link in the row of ‘New host’ should display a count of ‘0’. Click on the link, and then click on Create item. This will present us with an item definition form.

All mandatory input fields are marked with a red asterisk.

For our sample item, the essential information to enter is:

**Name**
- Enter CPU Load as the value. This will be the item name displayed in lists and elsewhere.

**Key**
• Manually enter system.cpu.load as the value. This is a technical name of an item that identifies the type of information that will be gathered. The particular key is just one of pre-defined keys that come with Zabbix agent.

**Type of information**

• Select Numeric (float) here. This attribute defines the format of expected data.

**Note:**
You may also want to reduce the amount of days item history will be kept, to 7 or 14. This is good practice to relieve the database from keeping lots of historical values.

**Other options** will suit us with their defaults for now.

When done, click Add. The new item should appear in the itemlist. Click on Details above the list to view what exactly was done.

Seeing data

With an item defined, you might be curious if it is actually gathering data. For that, go to Monitoring → Latest data, select ‘New host’ in the filter and click on Apply.

Then click on the + before - other - and expect your item to be there and displaying data.

With that said, first data may take up to 60 seconds to arrive. That, by default, is how often the server reads configuration changes and picks up new items to execute.

If you see no value in the ‘Change’ column, maybe only one value has been received so far. Wait 30 seconds for another value to arrive.

If you do not see information about the item as in the screenshot, make sure that:

• you entered item ‘Key’ and ‘Type of information’ fields exactly as in the screenshot
• both agent and server are running
• host status is ‘Monitored’ and its availability icon is green
• host is selected in the host dropdown, item is active

**Graphs**

With the item working for a while, it might be time to see something visual. Simple graphs are available for any monitored numeric item without any additional configuration. These graphs are generated on runtime.

To view the graph, go to Monitoring → Latest data and click on the ‘Graph’ link next to the item.
Overview

In this section you will learn how to set up a trigger.

Items only collect data. To automatically evaluate incoming data we need to define triggers. A trigger contains an expression that defines a threshold of what is an acceptable level for the data.

If that level is surpassed by the incoming data, a trigger will “fire” or go into a ‘Problem’ state - letting us know that something has happened that may require attention. If the level is acceptable again, trigger returns to an ‘Ok’ state.

Adding trigger

To configure a trigger for our item, go to Configuration → Hosts, find ‘New host’ and click on Triggers next to it and then on Create trigger. This presents us with a trigger definition form.
All mandatory input fields are marked with a red asterisk.

For our trigger, the essential information to enter here is:

**Name**
- Enter CPU load too high on 'New host' for 3 minutes as the value. This will be the trigger name displayed in lists and elsewhere.

**Expression**
• Enter: \( \{ \text{New host:system.cpu.load.avg(3m)} \}>2 \)

This is the trigger expression. Make sure that the expression is entered right, down to the last symbol. The item key here (system.cpu.load) is used to refer to the item. This particular expression basically says that the problem threshold is exceeded when the CPU load average value for 3 minutes is over 2. You can learn more about the syntax of trigger expressions.

When done, click Add. The new trigger should appear in the trigger list.

Displaying trigger status

With a trigger defined, you might be interested to see its status.

If the CPU load has exceeded the threshold level you defined in the trigger, the problem will be displayed in Monitoring → Problems.

<table>
<thead>
<tr>
<th>Time</th>
<th>Severity</th>
<th>Recovery time</th>
<th>Status</th>
<th>Info</th>
<th>Host</th>
<th>Problem</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>09:48:39</td>
<td>Not classified</td>
<td></td>
<td>PROBLEM</td>
<td>New host</td>
<td>CPU load too high on New host for 3 minutes</td>
<td>1m 23s</td>
<td></td>
</tr>
</tbody>
</table>

The flashing indicates a recent change of trigger status, one that has taken place in the last 30 minutes.

5 Receiving problem notification

Overview

In this section you will learn how to set up alerting in the form of notifications in Zabbix.

With items collecting data and triggers designed to “fire” upon problem situations, it would also be useful to have some alerting mechanism in place that would notify us about important events even when we are not directly looking at Zabbix frontend.

This is what notifications do. E-mail being the most popular delivery method for problem notifications, we will learn how to set up an e-mail notification.

E-mail settings

Initially there are several predefined notification delivery methods in Zabbix. E-mail is one of those.

To configure e-mail settings, go to Administration → Media types and click on Email in the list of pre-defined media types.

This will present us with the e-mail settings definition form.
All mandatory input fields are marked with a red asterisk.

Set the values of SMTP server, SMTP helo and SMTP e-mail to the appropriate for your environment.

**Note:**
‘SMTP email’ will be used as the ‘From’ address for the notifications sent from Zabbix.

Press Update when ready.

Now you have configured ‘Email’ as a working media type. A media type must be linked to users by defining specific delivery addresses (like we did when configuring a new user), otherwise it will not be used.

New action

Delivering notifications is one of the things actions do in Zabbix. Therefore, to set up a notification, go to Configuration → Actions and click on Create action.
All mandatory input fields are marked with a red asterisk.

In this form, enter a name for the action.

In the most simple case, if we do not add any more specific conditions, the action will be taken upon any trigger change from ‘Ok’ to ‘Problem’.

We still should define what the action should do - and that is done in the Operations tab. Click on New in the Operations block, which opens a new operation form.
All mandatory input fields are marked with a red asterisk.

Here, click on Add in the Send to Users block and select the user ("user") we have defined. Select 'Email' as the value of Send only to. When done with this, click on Add in the operation detail block.

{TRIGGER.STATUS} and {TRIGGER.NAME} macros (or variables), visible in the Default subject and Default message fields, will be replaced with the actual trigger status and trigger name values.

That is all for a simple action configuration, so click Add in the action form.

Receiving notification

Now, with delivering notifications configured it would be fun to actually receive one. To help with that, we might on purpose increase the load on our host - so that our trigger "fires" and we receive a problem notification.

Open the console on your host and run:

cat /dev/urandom | md5sum

You may run one or several of these processes.

Now go to Monitoring → Latest data and see how the values of 'CPU Load' have increased. Remember, for our trigger to fire, the
'CPU Load' value has to go over '2' for 3 minutes running. Once it does:

- in Monitoring → Problems you should see the trigger with a flashing 'Problem' status
- you should receive a problem notification in your e-mail

**Attention:**
If notifications do not work:
- verify once again that both the e-mail settings and the action have been configured properly
- make sure the user you created has at least read permissions on the host which generated the event, as noted in the Adding user step. The user, being part of the 'Zabbix administrators' user group must have at least read access to 'Linux servers' host group that our host belongs to.
- Additionally, you can check out the action log by going to Reports → Action log.

### 6 New template

**Overview**

In this section you will learn how to set up a template.

Previously we learned how to set up an item, a trigger and how to get a problem notification for the host.

While all of these steps offer a great deal of flexibility in themselves, it may appear like a lot of steps to take if needed for, say, a thousand hosts. Some automation would be handy.

This is where templates come to help. Templates allow to group useful items, triggers and other entities so that those can be reused again and again by applying to hosts in a single step.

When a template is linked to a host, the host inherits all entities of the template. So, basically a pre-prepared bunch of checks can be applied very quickly.

**Adding template**

To start working with templates, we must first create one. To do that, in Configuration → Templates click on Create template. This will present us with a template configuration form.

![Template Configuration Form](image)

All mandatory input fields are marked with a red asterisk.

The required parameters to enter here are:

**Template name**

- Enter a template name. Alpha-numericals, spaces and underscores are allowed.

**Groups**

- Select one or several groups by clicking Select button. The template must belong to a group.

When done, click Add. Your new template should be visible in the list of templates.
As you may see, the template is there, but it holds nothing in it - no items, triggers or other entities.

**Adding item to template**

To add an item to the template, go to the item list for ’New host’. In Configuration → Hosts click on Items next to ’New host’.

Then:

- mark the checkbox of the ’CPU Load’ item in the list
- click on Copy below the list
- select the template to copy item to

All mandatory input fields are marked with a red asterisk.

- click on Copy

If you now go to Configuration → Templates, ’New template’ should have one new item in it.

We will stop at one item only for now, but similarly you can add any other items, triggers or other entities to the template until it’s a fairly complete set of entities for given purpose (monitoring OS, monitoring single application).

**Linking template to host**

With a template ready, it only remains to add it to a host. For that, go to Configuration → Hosts, click on ’New host’ to open its property form and go to the Templates tab.

There, click on Select next to Link new templates. In the pop-up window click on the name of template we have created (’New template’). As it appears in the Link new templates field, click on Add. The template should appear in the Linked templates list.
Click Update in the form to save the changes. The template is now added to the host, with all entities that it holds.

As you may have guessed, this way it can be applied to any other host as well. Any changes to the items, triggers and other entities at the template level will propagate to the hosts the template is linked to.

Linking pre-defined templates to hosts

As you may have noticed, Zabbix comes with a set of predefined templates for various OS, devices and applications. To get started with monitoring very quickly, you may link the appropriate one of them to a host, but beware that these templates need to be fine-tuned for your environment. Some checks may not be needed, and polling intervals may be way too frequent.

More information about templates is available.

6. Zabbix appliance

Overview As an alternative to setting up manually or reusing an existing server for Zabbix, users may download a Zabbix appliance or a Zabbix appliance installation CD image. Zabbix appliance and installation CD versions are based upon the following OS:

<table>
<thead>
<tr>
<th>Zabbix appliance version</th>
<th>OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0</td>
<td>CentOS 8 (x86_64)</td>
</tr>
</tbody>
</table>

Zabbix appliance installation CD can be used for instant deployment of Zabbix server (MySQL).

System requirements:

- RAM: 1.5 GB
- Disk space: at least 8 GB should be allocated for the virtual machine.

Zabbix installation CD/DVD boot menu:
Zabbix appliance contains a Zabbix server (configured and running on MySQL) and a frontend.

Zabbix virtual appliance is available in the following formats:

- VMWare (.vmx)
- Open virtualization format (.ovf)
- Microsoft Hyper-V 2012 (.vhd)
- Microsoft Hyper-V 2008 (.vhd)
- KVM, Parallels, QEMU, USB stick, VirtualBox, Xen (.raw)
- KVM, QEMU (.qcow2)

To get started, boot the appliance and point a browser at the IP the appliance has received over DHCP.

**Attention:**
DHCP must be enabled on the host.

To get the IP address from inside the virtual machine run:

```
ip addr show
```

To access Zabbix frontend, go to [http://<host_ip>](http://<host_ip>) (for access from the host’s browser bridged mode should be enabled in the VM network settings).

**Note:**
If the appliance fails to start up in Hyper-V, you may want to press Ctrl+Alt+F2 to switch tty sessions.

### 1 Changes to CentOS 8 configuration

The appliance is based on CentOS 8. There are some changes applied to the base CentOS configuration.

#### 1.1 Repositories

Official Zabbix repository has been added to /etc/yum.repos.d:

```
[zabbix]
name=Zabbix Official Repository - $basearch
enabled=1
```
1.2 Firewall configuration

The appliance uses iptables firewall with predefined rules:

- Opened SSH port (22 TCP);
- Opened Zabbix agent (10050 TCP) and Zabbix trapper (10051 TCP) ports;
- Opened HTTP (80 TCP) and HTTPS (443 TCP) ports;
- Opened SNMP trap port (162 UDP);
- Opened outgoing connections to NTP port (53 UDP);
- ICMP packets limited to 5 packets per second;
- All other incoming connections are dropped.

1.3 Using a static IP address

By default the appliance uses DHCP to obtain the IP address. To specify a static IP address:

- Log in as root user;
- Open /etc/sysconfig/network-scripts/ifcfg-eth0 file;
- Replace BOOTPROTO=dhcp with BOOTPROTO=none
- Add the following lines:
  - IPADDR=<IP address of the appliance>
  - PREFIX=<CIDR prefix>
  - GATEWAY=<gateway IP address>
  - DNS1=<DNS server IP address>

- Run `systemctl restart network` command.

Consult the official Red Hat documentation if needed.

1.4 Changing time zone

By default the appliance uses UTC for the system clock. To change the time zone, copy the appropriate file from /usr/share/zoneinfo to /etc/localtime, for example:

```
cp /usr/share/zoneinfo/Europe/Riga /etc/localtime
```

2 Zabbix configuration

Zabbix appliance setup has the following passwords and configuration changes:

2.1 Credentials (login:password)

System:
- root:zabbix

Zabbix frontend:
- Admin:zabbix

Database:
- root:<random>
- zabbix:<random>

**Note:**
Database passwords are randomly generated during the installation process.
Root password is stored inside the /root/.my.cnf file. It is not required to input a password under the “root” account.

To change the database user password, changes have to be made in the following locations:

- MySQL:
  - /etc/zabbix/zabbix_server.conf;
  - /etc/zabbix/web/zabbix.conf.php.

**Note:**
Separate users zabbix_srv and zabbix_web are defined for the server and the frontend respectively.

2.2 File locations

- Configuration files are located in /etc/zabbix.
- Zabbix server, proxy and agent logfiles are located in /var/log/zabbix.
• Zabbix frontend is located in /usr/share/zabbix.
• Home directory for the user zabbix is /var/lib/zabbix.

2.3 Changes to Zabbix configuration

• Frontend timezone is set to Europe/Riga (this can be modified in /etc/php-fpm.d/zabbix.conf);

3 Frontend access  By default, access to the frontend is allowed from anywhere.

The frontend can be accessed at http://<host>/zabbix.
This can be customized in /etc/httpd/conf.d/zabbix.conf. Apache has to be restarted after modifying this file. To do so, log in using SSH as root user and execute:

systemctl restart httpd

4 Firewall  By default, only the ports listed in the configuration changes above are open. To open additional ports, modify "/etc/sysconfig/iptables" file and reload firewall rules:

systemctl reload iptables

5 Upgrading  The Zabbix appliance packages may be upgraded. To do so, run:

dnf update zabbix*

6 System Services  Systemd services are available:

systemctl list-units zabbix*

7 Format-specific notes  7.1 VMware
The images in vmdk format are usable directly in VMware Player, Server and Workstation products. For use in ESX, ESXi and vSphere they must be converted using VMware converter.

7.2 HDD/flash image (raw)

dd if=./zabbix_appliance_4.0.0_x86_64.raw of=/dev/sdc bs=4k conv=fdatasync

Replace /dev/sdc with your Flash/HDD disk device.

7. Configuration

Please use the sidebar to access content in the Configuration section.

1 Configuring a template

Overview

Configuring a template requires that you first create a template by defining its general parameters and then you add entities (items, triggers, graphs etc.) to it.

Creating a template

To create a template, do the following:

• Go to Configuration → Templates
• Click on Create template
• Edit template attributes

The Template tab contains general template attributes.
All mandatory input fields are marked with a red asterisk.

Template attributes:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template name</td>
<td>Unique template name. Alphanumerics, spaces, dots, dashes and underscores are allowed. Note that leading and trailing spaces are disallowed since Zabbix 4.0.12.</td>
</tr>
<tr>
<td>Visible name</td>
<td>If you set this name, it will be the one visible in lists, maps, etc.</td>
</tr>
<tr>
<td>Groups</td>
<td>Host/template groups the template belongs to.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter the templatedescription.</td>
</tr>
</tbody>
</table>

The **Linked templates** tab allows you to link one or more “nested” templates to this template. All entities (items, triggers, graphs etc.) will be inherited from the linked templates.

To link a new template, start typing in the Link new templates field until a list of templates corresponding to the entered letter(s) appear. Scroll down to select. When all templates to be linked are selected, click on Add.

To unlink a template, use one of the two options in the Linked templates block:

- Unlink - unlink the template, but preserve its items, triggers and graphs
- Unlink and clear - unlink the template and remove all its items, triggers and graphs

The **Macros** tab allows you to define template-level user macros. You may also view here macros from linked templates and global macros if you select the Inherited and templatemacrosoption. That is where all defined user macros for the template are displayed with the value they resolve to as well as their origin.

For convenience, links to respective templates and global macro configuration are provided. It is also possible to edit a nested template/global macro on the template level, effectively creating a copy of the macro on the template.

Buttons:

Add the template. The added template should appear in the list.
Update the properties of an existing template.

Create another template based on the properties of the current template, including the entities (items, triggers, etc) inherited from linked templates.

Create another template based on the properties of the current template, including the entities (items, triggers, etc) both inherited from linked templates and directly attached to the current template.

Delete the template; entities of the template (items, triggers, etc) remain with the linked hosts.

Delete the template and all its entities from linked hosts.

Cancel the editing of template properties.

With a template created, it is time to add some entities to it.

**Attention:**
Items have to be added to a template first. Triggers and graphs cannot be added without the corresponding item.

Adding items, triggers, graphs

To add items to the template, do the following:

- Go to Configuration → Hosts (or Templates)
- Click on Items in the row of the required host/template
- Mark the checkboxes of items you want to add to the template
- Click on Copy below the item list
- Select the template (or group of templates) the items should be copied to and click on Copy

All the selected items should be copied to the template.

Adding triggers and graphs is done in similar fashion (from the list of triggers and graphs respectively), again, keeping in mind that they can only be added if the required items are added first.

Adding screens

To add screens to a template in Configuration → Templates, do the following:

- Click on Screens in the row of the template
- Configure a screen following the usual method of configuring screens

**Attention:**
The elements that can be included in a template screen are: simple graph, custom graph, clock, plain text, URL.

**Note:**
For details on accessing host screens that are created from template screens, see the host screen section.

Configuring low-level discovery rules

See the low-level discovery section of the manual.

Adding web scenarios

To add web scenarios to a template in Configuration → Templates, do the following:

- Click on Web in the row of the template
- Configure a web scenario following the usual method of configuring web scenarios
2 Linking/unlinking

Overview
Linking is a process whereby templates are applied to hosts, whereas unlinking removes the association with the template from a host.

Attention:
Templates are linked directly to individual hosts and not to host groups. Simply adding a template to a host group will not link it. Host groups are used only for logical grouping of hosts and templates.

Linking a template
To link a template to the host, do the following:

- Go to Configuration → Hosts
- Click on the required host and switch to the Templates tab
- Click on Add next to Link new templates
- Select one or several templates in the popup window
- Click on Add/Update in the host attributes form

The host will now have all the entities (items, triggers, graphs, etc) of the template.

Attention:
Linking multiple templates to the same host will fail if in those templates there are items with the same item key. And, as triggers and graphs use items, they cannot be linked to a single host from multiple templates either, if using identical item keys.

When entities (items, triggers, graphs etc.) are added from the template:

- previously existing identical entities on the host are updated as entities of the template
- entities from the template are added
- any directly linked entities that, prior to template linkage, existed only on the host remain untouched

In the lists, all entities from the template now are prefixed by the template name, indicating that these belong to the particular template. The template name itself (in gray text) is a link allowing to access the list of those entities on the template level.

If some entity (item, trigger, graph etc.) is not prefixed by the template name, it means that it existed on the host before and was not added by the template.

Entity uniqueness criteria
When adding entities (items, triggers, graphs etc.) from a template it is important to know what of those entities already exist on the host and need to be updated and what entities differ. The uniqueness criteria for deciding upon the sameness/difference are:

- for items - the item key
- for triggers - trigger name and expression
- for custom graphs - graph name and its items
- for applications - application name

Linking templates to several hosts
To update template linkage of many hosts, in Configuration → Hosts select some hosts by marking their checkboxes, then click on Mass update below the list and then in the Templates tab select to link additional templates:
Select Link templates and start typing the template name in the auto-complete field until a dropdown appears offering the matching templates. Just scroll down to select the template to link.

The Replace option will allow to link a new template while unlinking any template that was linked to the hosts before. The Clear when unlinking option will allow to not only unlink any previously linked templates, but also remove all elements inherited from them (items, triggers, etc.).

**Note:**
Zabbix offers a sizable set of predefined templates. You can use these for reference, but beware of using them unchanged in production as they may contain too many items and poll for data too often. If you feel like using them, finetune them to fit your real needs.

**Editing linked entities**

If you try to edit an item or trigger that was linked from the template, you may realize that many key options are disabled for editing. This makes sense as the idea of templates is that things are edited in one-touch manner on the template level. However, you still can, for example, enable/disable an item on the individual host and set the update interval, history length and some other parameters.

If you want to edit the entity fully, you have to edit it on the template level (template level shortcut is displayed in the form name), keeping in mind that these changes will affect all hosts that have this template linked to them.

**Unlinking a template**

To unlink a template from a host, do the following:

- Go to Configuration → Hosts
- Click on the required host and switch to the Templates tab
- Click on Unlink or Unlink and clear next to the template to unlink
- Click on Update in the host attributes form

Choosing the Unlink option will simply remove association with the template, while leaving all its entities (items, triggers, graphs etc.) with the host.

Choosing the Unlink and clear option will remove both the association with the template and all its entities (items, triggers, graphs etc.).

**3 Nesting**

**Overview**

Nesting is a way of one template encompassing one or more other templates.

As it makes sense to separate out entities on individual templates for various services, applications, etc., you may end up with quite a few templates all of which may need to be linked to quite a few hosts. To simplify the picture, it is possible to link some templates together in a single template.

The benefit of nesting is that you have to link only one template ("nest", parent template) to the host and the host will inherit all entities of the linked templates ("nested", child templates) automatically. For example, if we link templates T1 and T2 to template
To link templates, you need to take an existing template or a new one, and then:

- Open the template configuration form
- Look for the Linked templates tab
- Click Select to open the Templates popup window
- In the popup window, choose required templates, then click Select to add the templates to the list
- Click Add or Update in the template configuration form

Thus, all entities of the parent template, as well as all entities of linked templates (such as items, triggers, graphs, etc.) will now appear in the template configuration, except for linked template screens, which will, nevertheless, be inherited by hosts.

To unlink any of the linked templates, in the same form use the Unlink or Unlink and clear buttons and click Update.

Choosing the Unlink option will simply remove the association with the linked template, while not removing all its entities (items, triggers, graphs, etc.).

Choosing the Unlink and clear option will remove both the association with the linked template and all its entities (items, triggers, graphs, etc.).

1 Hosts and host groups

What is a “host”?

Typical Zabbix hosts are the devices you wish to monitor (servers, workstations, switches, etc).

Creating hosts is one of the first monitoring tasks in Zabbix. For example, if you want to monitor some parameters on a server “x”, you must first create a host called, say, “Server X” and then you can look to add monitoring items to it.

Hosts are organized into host groups.

Proceed to creating and configuring a host.

1 Configuring a host

Overview

To configure a host in Zabbix frontend, do the following:

- Go to: Configuration → Hosts
- Click on Create host to the right (or on the host name to edit an existing host)
- Enter parameters of the host in the form

You can also use the Clone and Full clone buttons in the form of an existing host to create a new host. Clicking on Clone will retain all host parameters and template linkage (keeping all entities from those templates). Full clone will additionally retain directly attached entities (applications, items, triggers, graphs, low-level discovery rules and web scenarios).

Note: When a host is cloned, it will retain all template entities as they are originally on the template. Any changes to those entities made on the existing host level (such as changed item interval, modified regular expression or added prototypes to the low-level discovery rule) will not be cloned to the new host; instead they will be as on the template.

Configuration

The Host tab contains general host attributes:
**Parameter** | **Description**
--- | ---
Host name | Enter a unique host name. Alphanumeric, spaces, dots, dashes and underscores are allowed. Note that leading and trailing spaces are disallowed since Zabbix 4.0.12. Note: With Zabbix agent running on the host you are configuring, the agent configuration file parameter Hostname must have the same value as the hostname entered here. The name in the parameter is needed in the processing of active checks.
Visible name | Enter a unique visible name for the host. If you set this name, it will be the one visible in lists, maps, etc instead of the technical host name. This attribute has UTF-8 support.
Groups | Select host groups the host belongs to. A host must belong to at least one host group. A new group can be created and linked to the host group by adding a non-existing group name.
Interfaces | Several host interface types are supported for a host: Agent, SNMP, JMX and IPMI.
To add a new interface, click on Add in the Interfaces block and enter IP/DNS, Connect to and Port info.
Note: Interfaces that are used in any items cannot be removed and link Remove is grayed out for them.
Use bulk requests option for SNMP interfaces allows to enable/disable bulk processing of SNMP requests per interface.
Parameter | Description
--- | ---
IP address | Host IP address (optional).
DNS name | Host DNS name (optional).
Connect to | Clicking the respective button will tell Zabbix server what to use to retrieve data from agents:
- **IP** - Connect to the host IP address (recommended)
- **DNS** - Connect to the host DNS name
Port | TCP/UDP port number. Default values are: 10050 for Zabbix agent, 161 for SNMP agent, 12345 for JMX and 623 for IPMI.
Default | Check the radio button to set the default interface.
Description | Enter the host description.
Monitored by proxy | The host can be monitored either by Zabbix server or one of Zabbix proxies:
- **(no proxy)** - host is monitored by Zabbix server
- **Proxy name** - host is monitored by Zabbix proxy "Proxy name"
Enabled | Mark the checkbox to make the host active, ready to be monitored. If unchecked, the host is not active, thus not monitored.

The **Templates** tab allows you to link templates to the host. All entities (items, triggers, graphs and applications) will be inherited from the template.

To link a new template, start typing in the Link new templates field until a list of matching templates appear. Scroll down to select. When all templates to be linked are selected, click on Add.

To unlink a template, use one of the two options in the Linked templates block:
- **Unlink** - unlink the template, but preserve its items, triggers and graphs
- **Unlink and clear** - unlink the template and remove all its items, triggers and graphs

Listed template names are clickable links leading to the template configuration form.

The **IPMI** tab contains IPMI management attributes.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication algorithm</td>
<td>Select the authentication algorithm.</td>
</tr>
<tr>
<td>Privilege level</td>
<td>Select the privilege level.</td>
</tr>
<tr>
<td>Username</td>
<td>User name for authentication.</td>
</tr>
<tr>
<td>Password</td>
<td>Password for authentication.</td>
</tr>
</tbody>
</table>

The **Macros** tab allows you to define host-level user macros. You may also view here template-level and global macros if you select the Inherited and host macros option. That is where all defined user macros for the host are displayed with the value they resolve to as well as their origin.

For convenience, links to respective templates and global macro configuration are provided. It is also possible to edit a template/global macro on the host level, effectively creating a copy of the macro on the host.

The **Host inventory** tab allows you to manually enter inventory information for the host. You can also select to enable Automatic inventory population, or disable inventory population for this host.

The **Encryption** tab allows you to require encrypted connections with the host.
Parameter Description

Connections to host How Zabbix server or proxy connects to Zabbix agent on a host: no encryption (default), using PSK (pre-shared key) or certificate.

Connections from host Select what type of connections are allowed from the host (i.e., from Zabbix agent and Zabbix sender). Several connection types can be selected at the same time (useful for testing and switching to other connection type). Default is “No encryption”.

Issuer Allowed issuer of certificate. Certificate is first validated with CA (certificate authority). If it is valid, signed by the CA, then the Issuer field can be used to further restrict allowed CA. This field is intended to be used if your Zabbix installation uses certificates from multiple CAs. If this field is empty then any CA is accepted.

Subject Allowed subject of certificate. Certificate is first validated with CA. If it is valid, signed by the CA, then the Subject field can be used to allow only one value of Subject string. If this field is empty then any valid certificate signed by the configured CA is accepted.

PSK identity Pre-shared key identity string.

PSK Pre-shared key (hex-string). Maximum length: 512 hex-digits (256-byte PSK) if Zabbix uses GnuTLS or OpenSSL library, 64 hex-digits (32-byte PSK) if Zabbix uses mbed TLS (PolarSSL) library. Example:

1f87b95725ac58dd977bee14b97461a7c1045b9a1c963065002c5473194952

Creating a host group

To create a host group in Zabbix frontend, do the following:

- Go to: Configuration → Host groups
- Click on Create Group in the upper right corner of the screen
- Enter parameters of the group in the form

All mandatory input fields are marked with a red asterisk.

Parameter Description

Group name Enter a unique host group name.

To create a nested host group, use the ‘/’ forward slash separator, for example Europe/Latvia/Riga/Zabbix servers. You can create this group even if none of the three parent host groups (Europe/Latvia/Riga) exist. In this case creating these parent host groups is up to the user; they will not be created automatically. Leading and trailing slashes, several slashes in a row are not allowed. Escaping of ‘/’ is not supported.

Nested representation of host groups is supported since Zabbix 3.2.0.
**Parameter Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Apply permissions to all subgroups</strong></td>
<td>Checkbox is available to Zabbix Super Admin users only and only when editing an existing host group. Mark this checkbox and click on Update to apply the same level of permissions to all nested host groups. For user groups that may have had differing permissions assigned to nested host groups, the permission level of the parent host group will be enforced on the nested groups. This is a one-time option that is not saved in the database. This option is supported since Zabbix 3.4.0.</td>
</tr>
</tbody>
</table>

**Permissions to nested host groups**

- When creating a child host group to an existing parent host group, user group permissions to the child are inherited from the parent (for example, when creating Riga/Zabbix servers if Riga already exists)
- When creating a parent host group to an existing child host group, no permissions to the parent are set (for example, when creating Riga if Riga/Zabbix servers already exists)

**2 Inventory**

**Overview**

You can keep the inventory of networked devices in Zabbix.

There is a special Inventory menu in the Zabbix frontend. However, you will not see any data there initially and it is not where you enter data. Building inventory data is done manually when configuring a host or automatically by using some automatic population options.

**Building inventory**

**Manual mode**

When configuring a host, in the Host inventory tab you can enter such details as the type of device, serial number, location, responsible person, etc - data that will populate inventory information.

If a URL is included in host inventory information and it starts with ‘http’ or ‘https’, it will result in a clickable link in the Inventory section.

**Automatic mode**

Host inventory can also be populated automatically. For that to work, when configuring a host the inventory mode in the Host inventory tab must be set to Automatic.

Then you can configure host items to populate any host inventory field with their value, indicating the destination field with the respective attribute (called Item will populate host inventory field) in item configuration.

Items that are especially useful for automated inventory data collection:

- system.hw.chassis[full|type|vendor|model|serial] - default is [full], root permissions needed
- system.hw.cpu[all|cpunum,full|maxfreq|vendor|model|curfreq] - default is [all,full]
- system.hw.devices[pci|usb] - default is [pci]
- system.hw.macaddr[interface,short|full] - default is [all,full], interface is regexp
- system.sw.arch
- system.sw.os[name|short|full] - default is [name]
- system.sw.packages[package,manager,short|full] - default is [all,all,full], package is regexp

**Inventory mode selection**

Inventory mode can be selected in the host configuration form.

Inventory mode by default for new hosts is selected based on the Default host inventory mode setting in Administration → General → Other.

For hosts added by network discovery or auto registration actions, it is possible to define a Set host inventory mode operation selecting manual or automatic mode. This operation overrides the Default host inventory mode setting.

**Inventory overview**

The details of all existing inventory data are available in the Inventory menu.
In Inventory → Overview you can get a host count by various fields of the inventory.

In Inventory → Hosts you can see all hosts that have inventory information. Clicking on the host name will reveal the inventory details in a form.

![Host inventory form](image)

The **Overview** tab shows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>Name of the host. Clicking on the name opens a menu with the scripts defined for the host. Host name is displayed with an orange icon, if the host is in maintenance.</td>
</tr>
<tr>
<td>Visible name</td>
<td>Visible name of the host (if defined).</td>
</tr>
<tr>
<td>Host (Agent, SNMP, JMX, IPMI)&lt;br&gt;interfaces</td>
<td>This block provides details of the interfaces configured for the host.</td>
</tr>
<tr>
<td>OS</td>
<td>Operating system inventory field of the host (if defined).</td>
</tr>
<tr>
<td>Hardware</td>
<td>Host hardware inventory field (if defined).</td>
</tr>
<tr>
<td>Software</td>
<td>Host software inventory field (if defined).</td>
</tr>
<tr>
<td>Description</td>
<td>Host description.</td>
</tr>
<tr>
<td>Monitoring</td>
<td>Links to monitoring sections with data for this host: Web, Latest data, Triggers, Problems, Graphs, Screens.</td>
</tr>
<tr>
<td>Configuration</td>
<td>Links to configuration sections for this host: Host, Applications, Items, Triggers, Graphs, Discovery, Web. The amount of configured entities is listed in parenthesis after each link.</td>
</tr>
</tbody>
</table>

The **Details** tab shows all inventory fields that are populated (are not empty).

**Inventory macros**

There are host inventory macros `{INVENTORY.*}` available for use in notifications, for example:

"Server in `{INVENTORY,LOCATION1}` has a problem, responsible person is `{INVENTORY,CONTACT1}`, phone number `{INVENTORY,POC,PRIMARY,PHONE,A1}`."

For more details, see the **supported macro** page.
3 Mass update

Overview

Sometimes you may want to change some attribute for a number of hosts at once. Instead of opening each individual host for editing, you may use the mass update function for that.

Using mass update

To mass-update some hosts, do the following:

- Mark the checkboxes before the hosts you want to update in the host list
- Click on Mass update below the list
- Navigate to the tab with required attributes (Host, Templates, IPMI, Inventory or Encryption)
- Mark the checkboxes of any attribute to update and enter a new value for them

Replace host groups will remove the host from any existing host groups and replace those with the one(s) specified in this field.

Add new or existing host groups allows to specify additional host groups from the existing ones or enter completely new host groups for the hosts.

Remove host groups will remove specific host groups from hosts. In case hosts are already in selected groups, then hosts will be removed from these groups. In case hosts are not in selected groups, nothing will added or removed. In case same host groups are replaced and removed at the same time, hosts are actually left without groups.

These fields are auto-complete - starting to type in them offers a dropdown of matching host groups. If the host group is new, it also appears in the dropdown and it is indicated by (new) after the string. Just scroll down to select.
To update template linkage in the Templates tab, select Link templates and start typing the template name in the auto-complete field until a dropdown appears offering the matching templates. Just scroll down to select the template to link.

The Replace option will allow to link a new template while unlinking any template that was linked to the hosts before. The Clear when unlinking option will allow to not only unlink any previously linked templates, but also remove all elements inherited from them (items, triggers, etc.).

To be able to mass update inventory fields, the Inventory mode should be set to ‘Manual’ or ‘Automatic’.
When done with all required changes, click on Update. The attributes will be updated accordingly for all the selected hosts.

2 Items

Overview

An item is an individual metric. Items are used for collecting data. Once you have configured a host, you must add items to get actual data. One way of quickly adding many items is to attach one of the predefined templates to a host. However, for optimized system performance, you may need to fine-tune the templates to have as many items and as frequent monitoring as necessary.

To specify what sort of data to collect from a host, use the item key. For example, an item with the key name `system.cpu.load` will collect processor load data, while an item with the key name `net.if.in` will collect incoming traffic information.

Additional parameters can be specified in square brackets after the key name. For example, `system.cpu.load[avg5]` will return the processor load average for the last 5 minutes, while `net.if.in[eth0]` will show incoming traffic in the interface “eth0”.

**Note:**

See individual sections of item types for all supported item types and item keys.

Proceed to creating and configuring an item.

1 Creating an item

Overview

To create an item in Zabbix frontend, do the following:

- Go to: Configuration → Hosts
- Click on Items in the row of the host
- Click on Create item in the upper right corner of the screen
- Enter parameters of the item in the form

You can also create an item by opening an existing one, pressing the Clone button and then saving under a different name.

Configuration

The Item tab contains general item attributes.
All mandatory input fields are marked with a red asterisk.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Item name. Note that the use of positional macros ($1, $2, ..., $9 - referring to the first, second... ninth parameter of the item key) is now deprecated. For example: Free disk space on $1. If the item key is &quot;vfs.fs.size[/,free]&quot;, the description will automatically change to &quot;Free disk space on /&quot;</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Type</td>
<td>Item type. See individual item type sections.</td>
</tr>
<tr>
<td>Key</td>
<td>Item key (up to 256 characters). The supported item keys can be found in individual item type sections. The key must be unique within a single host. If key type is ‘Zabbix agent’, ‘Zabbix agent (active)’, ‘Simple check’ or ‘Zabbix aggregate’, the key value must be supported by Zabbix agent or Zabbix server. See also: the correct key format.</td>
</tr>
<tr>
<td>Host interface</td>
<td>Select the host interface. This field is available when editing an item on the host level.</td>
</tr>
<tr>
<td>Type of information</td>
<td>Type of data as stored in the database after performing conversions, if any. Numeric (unsigned) - 64bit unsigned integer Numeric (float) - floating point number Negative values can be stored. Allowed range: -9999999999999.9999 to 9999999999999.9999. Starting with Zabbix 2.2, receiving values in scientific notation is also supported. E.g. 1e+7, 1e-4. Character - short text data Log - long text data with optional log related properties (timestamp, source, severity, logeventid) Text - long text data. See also text data limits.</td>
</tr>
<tr>
<td>Units</td>
<td>If a unit symbol is set, Zabbix will add post processing to the received value and display it with the set unit postfix. By default, if the raw value exceeds 1000, it is divided by 1000 and displayed accordingly. For example, if you set bps and receive a value of 881764, it will be displayed as 881.76 Kbps. The JEDEC memory standard is used for processing B (byte), Bps (bytes per second) units, which are divided by 1024. Thus, if units are set to B or Bps Zabbix will display: 1 as 1B/1Bps 1024 as 1KB/1KBps 1536 as 1.5KB/1.5KBps Special processing is used if the following time-related units are used: unixtime - translated to “yyyy.mm.dd hh:mm:ss”. To translate correctly, the received value must be a Numeric (unsigned) type of information. uptime - translated to “hh:mm:ss” or “N days, hh:mm:ss” For example, if you receive the value as 881764 (seconds), it will be displayed as “10 days, 04:56:04” s - translated to “y yyy mmm ddd hh:mm:ss ms”; parameter is treated as number of seconds. For example, if you receive the value as 881764 (seconds), it will be displayed as “10d 4h 56m” Only 3 upper major units are shown, like “1m 15d 5h” or “2h 4m 46s”. If there are no days to display, only two levels are displayed - “1m 5h” (no minutes, seconds or milliseconds are shown). Will be translated to “&lt; 1 ms” if the value is less than 0.001. Note that if a unit is prefixed with !, then no unit prefixes/processing is applied to item values. See unit conversion.</td>
</tr>
</tbody>
</table>
**Parameter** | **Description**
---|---
**Update interval** | Retrieve a new value for this item every N seconds. Maximum allowed update interval is 86400 seconds (1 day). **Time suffixes** are supported, e.g. 30s, 1m, 2h, 1d. **User macros** and **LLD macros** are supported. A single macro has to fill the whole field. Multiple macros in a field or macros mixed with text are not supported. Note: The update interval can only be set to ‘0’ if custom intervals exist with a non-zero value. If set to ‘0’, and a custom interval (flexible or scheduled) exists with a non-zero value, the item will be polled during the custom interval duration. Note that the first item poll after the item became active or after update interval change might occur earlier than the configured value. An existing passive item can be polled for value immediately by pushing the Check now button.

**Custom intervals** | You can create custom rules for checking the item: **Flexible** - create an exception to the Update interval (interval with different frequency) **Scheduling** - create a custom polling schedule. For detailed information see **Custom intervals**. **Time suffixes** are supported in the Interval field, e.g. 30s, 1m, 2h, 1d. **User macros** and **LLD macros** are supported. A single macro has to fill the whole field. Multiple macros in a field or macros mixed with text are not supported. Scheduling is supported since Zabbix 3.0.0. Note: Not available for Zabbix agent active items.

**History storage period** | Select either: **Do not keep history** - item history is not stored. Useful for master items if only dependent items need to keep history. Note: Before Zabbix 4.0.11, not keeping history had to be specified by entering "0" in the storage period field and it could be overridden by global housekeeper settings (now it cannot). **Storage period** - specify the duration of keeping detailed history in the database (1 hour to 25 years). Older data will be removed by the housekeeper. Stored in seconds. **Time suffixes** are supported, e.g. 2h, 1d. **User macros** are supported. The Storage period value can be overridden globally in Administration → General → **Housekeeper**. If a global overriding setting exists, a green info icon is displayed. If you position your mouse on it, a warning message is displayed, e.g. Overridden by global housekeeper settings (1d). It is recommended to keep the recorded values for the smallest possible time to reduce the size of value history in the database. Instead of keeping a long history of values, you can keep longer data of trends. See also **History and trends**.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trend storage period</td>
<td>Select either: <strong>Do not keep trends</strong> - trends are not stored. Note: Before Zabbix 4.0.11, not keeping trends had to be specified by entering &quot;0&quot; in the storage period field and it could be overridden by global housekeeper settings (now it cannot). <strong>Storage period</strong> - specify the duration of keeping aggregated (hourly min, max, avg, count) history in the database (1 day to 25 years). Older data will be removed by the housekeeper. Stored in seconds. <strong>Time suffixes</strong> are supported, e.g. 24h, 1d. <strong>User macros</strong> are supported. The Storage period value can be overridden globally in Administration → General → <strong>Housekeeper</strong>. If a global overriding setting exists, a green info icon is displayed. If you position your mouse on it, a warning message is displayed, e.g. Overridden by global housekeeper settings (7d). Note: Keeping trends is not available for non-numeric data - character, log and text. See also History and trends.</td>
</tr>
<tr>
<td>Show value</td>
<td>Apply value mapping to this item. Value mapping does not change received values, it is for displaying data only. It works with Numeric(unsigned), Numeric(float) and Character items. For example, &quot;Windows service states&quot;.</td>
</tr>
<tr>
<td>Log time format</td>
<td>Available for items of type <strong>Log</strong> only. Supported placeholders: * y: Year (1970-2038) * M: Month (01-12) * d: Day (01-31) * h: Hour (00-23) * m: Minute (00-59) * s: Second (00-59) If left blank the timestamp will not be parsed. For example, consider the following line from the Zabbix agent log file: &quot;23480:20100328:154718.045 Zabbix agent started. Zabbix 1.8.2 (revision 11211).&quot; It begins with six character positions for PID, followed by date, time, and the rest of the line. Log time format for this line would be &quot;pppppp:yyyyMMdd:hhmmss&quot;. Note that &quot;p&quot; and &quot;:&quot; chars are just placeholders and can be anything but &quot;yyyyMMddhhmmss&quot;.</td>
</tr>
<tr>
<td>New application</td>
<td>Enter the name of a new application for the item.</td>
</tr>
<tr>
<td>Applications</td>
<td>Link item to one or more existing applications.</td>
</tr>
<tr>
<td>Populates host inventory field</td>
<td>You can select a host inventory field that the value of item will populate. This will work if automatic inventory population is enabled for the host. This field is not available if Type of information is set to 'Log'.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter an item description.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Mark the checkbox to enable the item so it will be processed.</td>
</tr>
</tbody>
</table>

**Note:**
Item type specific fields are described on corresponding pages.

**Note:**
When editing an existing template level item on a host level, a number of fields are read-only. You can use the link in the form header and go to the template level and edit them there, keeping in mind that the changes on a template level will change the item for all hosts that the template is linked to.
Item value preprocessing

The **Preprocessing** tab allows to define transformation rules for the received values. One or several transformations are possible before saving values to the database. Transformations are executed in the order in which they are defined. All preprocessing is done by Zabbix server.

See also: **Preprocessing details**

![Preprocessing tab](image)

User macros and user macros with context are supported in item value preprocessing parameters.

**Note:**
An item can become **unsupported** if any of the preprocessing steps fails.

<table>
<thead>
<tr>
<th>Transformation</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Regular expression** | Match the value to the `<pattern>` regular expression and replace value with `<output>`. The regular expression supports extraction of maximum 10 captured groups with the \N sequence. Failure to match the input value will make the item unsupported.  
Parameters:
- **pattern** - regular expression 
- **output** - output formatting template. An \N (where N=1…9) escape sequence is replaced with the Nth matched group. A \0 escape sequence is replaced with the matched text.  
Supported since 3.4.0.  
Please refer to regular expressions section for some existing examples. |
<p>| <strong>Trim</strong>              | Remove specified characters from the beginning and end of the value.        |</p>
<table>
<thead>
<tr>
<th>Transformation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Right trim</td>
<td>Remove specified characters from the end of the value.</td>
</tr>
<tr>
<td>Left trim</td>
<td>Remove specified characters from the beginning of the value.</td>
</tr>
<tr>
<td>XML XPath</td>
<td>Extract value or fragment from XML data using XPath functionality. For this option to work, Zabbix server must be compiled with libxml support. Examples: number(/document/item/value) will extract 10 from &lt;document&gt;&lt;item&gt;&lt;value&gt;10&lt;/value&gt;&lt;/item&gt;&lt;/document&gt; number(/document/item/@attribute) will extract 10 from &lt;document&gt;&lt;item attribute=&quot;10&quot;&gt;&lt;/item&gt;&lt;/document&gt; /document/item will extract &lt;item&gt;&lt;value&gt;10&lt;/value&gt;&lt;/item&gt; from &lt;document&gt;&lt;item&gt;&lt;value&gt;10&lt;/value&gt;&lt;/item&gt;&lt;/document&gt; Note that namespaces are not supported. Supported since 3.4.0.</td>
</tr>
<tr>
<td>JSON Path</td>
<td>Extract value or fragment from JSON data using JSONPath functionality. (Note that only a simple subset of JSONPath functionality is supported before Zabbix 4.0.11.)</td>
</tr>
<tr>
<td>Custom multiplier</td>
<td>Multiply the value by the specified integer or floating-point value. Use this option to convert values received in KB, MBps, etc into B, Bps. Otherwise Zabbix cannot correctly set prefixes (K, M, G etc). Note that if the item type of information is Numeric (unsigned), incoming values with a fractional part will be trimmed (i.e. ‘0.9’ will become ‘0’) before the custom multiplier is applied. Supported: scientific notation, for example, 1e+70 (since version 2.2); user macros and LLD macros (since version 4.0.0); strings that include macros, for example, {#MACRO}e+10, {$MACRO1}e+{$MACRO2} (since version 4.0.28) The macros must resolve to an integer or a floating-point number.</td>
</tr>
<tr>
<td>Simple change</td>
<td>Calculate difference between the current and previous value. Evaluated as value-prev_value, where value - current value; prev_value - previously received value This setting can be useful to measure a constantly growing value. If the current value is smaller than the previous value, Zabbix discards that difference (stores nothing) and waits for another value. Only one change operation per item is allowed.</td>
</tr>
<tr>
<td>Transformation</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Change per second</td>
<td>Calculate the value change (difference between the current and previous value) speed per second. Evaluated as ((\text{value-prev_value})/(\text{time-prev_time}))), where value - current value; prev_value - previously received value; time - current timestamp; prev_time - timestamp of previous value. This setting is extremely useful to get speed per second for a constantly growing value. If the current value is smaller than the previous value, Zabbix discards that difference (stores nothing) and waits for another value. This helps to work correctly with, for instance, a wrapping (overflow) of 32-bit SNMP counters. Note: As this calculation may produce floating point numbers, it is recommended to set the 'Type of information' to Numeric (float), even if the incoming raw values are integers. This is especially relevant for small numbers where the decimal part matters. If the floating point values are large and may exceed the 'float' field length in which case the entire value may be lost, it is actually suggested to use Numeric (unsigned) and thus trim only the decimal part. Only one change operation per item is allowed.</td>
</tr>
<tr>
<td>Boolean to decimal</td>
<td>Convert the value from boolean format to decimal. Textual representation is translated into either 0 or 1. Thus, 'TRUE' is stored as 1 and 'FALSE' is stored as 0. All values are matched in a case-insensitive way. Currently recognized values are, for: TRUE - true, t, yes, y, on, up, running, enabled, available, ok, master FALSE - false, f, no, n, off, down, unused, disabled, unavailable, err, slave Additionally, any non-zero numeric value is considered to be TRUE and zero is considered to be FALSE. Following values are supported since 4.0.0: ok, master, err, slave.</td>
</tr>
<tr>
<td>Octal to decimal</td>
<td>Convert the value from octal format to decimal.</td>
</tr>
<tr>
<td>Hexadecimal to decimal</td>
<td>Convert the value from hexadecimal format to decimal.</td>
</tr>
</tbody>
</table>

**Note:**
If you use a custom multiplier or store value as Change per second for items with the type of information set to Numeric (unsigned) and the resulting calculated value is actually a float number, the calculated value is still accepted as a correct one by trimming the decimal part and storing the value as integer.

**Preprocessing usage examples**

**Filtering VMware event log records**

Using a regular expression preprocessing to filter unnecessary events of the VMWare event log.

1. On a working VMWare Hypervisor host check that the event log item `vmware.eventlog[<url>,<mode>]` is present and working properly. Note that the event log item could already be present on the hypervisor if the Template VM VMWare template has been linked during the host creation.

2. On the VMWare Hypervisor host create a **dependent item** of 'Log' type and set the event log item as its master.

Use group matching and output control. Select "Regular expression" option in the "Preprocessing" tab and fill parameters, for example:

```
pattern: ".*logged in.*", output: \"0\" - filters all logging events in the event log
```
pattern "User (.+)(?=\s\")", output: "\1" - filter only usernames from the event log

Text data limits

Text data limits depend on the database backend. Before storing text values in the database they get truncated to match the database value type limit:

<table>
<thead>
<tr>
<th>Database</th>
<th>Type of information</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Character</td>
</tr>
<tr>
<td>MySQL</td>
<td>255 characters</td>
</tr>
<tr>
<td>PostgreSQL</td>
<td>255 characters</td>
</tr>
<tr>
<td>Oracle</td>
<td>255 characters</td>
</tr>
<tr>
<td>IBM DB2</td>
<td>255 bytes</td>
</tr>
</tbody>
</table>

Unit conversion

By default, specifying a unit for an item results in a multiplier prefix being added - for example, an incoming value '2048' with unit 'B' would be displayed as '2KB'.

Any unit, however, can be prevented from being converted by using a ! prefix, for example !B. To better illustrate how the conversion works with and without the exclamation mark, see the following examples of values and units:

1024 !B → 1024 B
1024 B → 1 KB
61 !s → 61 s
61 s → 1 m 1 s
0 !uptime → 0 uptime
0 uptime → 00:00:00
0 !! → 0
0 ! → 0

Note:

Before Zabbix 4.0, there was hardcoded unit stoplist consisting of ms, rpm, RPM, %. This stoplist has been deprecated, thus the correct way of stoplisting such units is !ms, !rpm, !RPM, !%.

Unsupported items

An item can become unsupported if its value cannot be retrieved for some reason. Such items are still rechecked at a fixed interval, configurable in Administration section.

Unsupported items are reported as having a NOT SUPPORTED state.

Form buttons

Buttons at the bottom of the form allow to perform several operations.

Add an item. This button is only available for new items.

Update the properties of an item.

Create another item based on the properties of the current item.

Execute a check for a new item value immediately. Supported for passive checks only (see more details). Note that when checking for a value immediately, configuration cache is not updated, thus the value will not reflect very recent changes to item configuration.

Delete the item history and trends.

Delete the item.
1 Item key format

Item key format, including key parameters, must follow syntax rules. The following illustrations depict the supported syntax. Allowed elements and characters at each point can be determined by following the arrows - if some block can be reached through the line, it is allowed, if not - it is not allowed.

To construct a valid item key, one starts with specifying the key name, then there's a choice to either have parameters or not - as depicted by the two lines that could be followed.

Key name

The key name itself has a limited range of allowed characters, which just follow each other. Allowed characters are: 0-9a-zA-Z_-.

Which means:

- all numbers;
- all lowercase letters;
- all uppercase letters;
- underscore;
- dash;
- dot.

Key parameters

An item key can have multiple parameters that are comma separated.

Each key parameter can be either a quoted string, an unquoted string or an array.
The parameter can also be left empty, thus using the default value. In that case, the appropriate number of commas must be added if any further parameters are specified. For example, item key `icmping[200,500]` would specify that the interval between individual pings is 200 milliseconds, timeout - 500 milliseconds, and all other parameters are left at their defaults.

Parameter - quoted string

If the key parameter is a quoted string, any Unicode character is allowed.

If the key parameter string contains comma, this parameter has to be quoted.

If the key parameter string contains quotation mark, this parameter has to be quoted and each quotation mark which is a part of the parameter string has to be escaped with a backslash (`\`) character.

**Warning:**

To quote item key parameters, use double quotes only. Single quotes are not supported.

Parameter - unquoted string

If the key parameter is an unquoted string, any Unicode character is allowed except comma and right square bracket (`]`). Unquoted parameter cannot start with left square bracket (`[`).

Parameter - array

If the key parameter is an array, it is again enclosed in square brackets, where individual parameters come in line with the rules and syntax of specifying multiple parameters.
Attention:
Multi-level parameter arrays, e.g. [a, [b, [c, d]], e], are not allowed.

2 Custom intervals

Overview
It is possible to create custom rules regarding the times when an item is checked. The two methods for that are Flexible intervals, which allow to redefine the default update interval, and Scheduling, whereby an item check can be executed at a specific time or sequence of times.

Flexible intervals
Flexible intervals allow to redefine the default update interval for specific time periods. A flexible interval is defined with Interval and Period where:

• Interval – the update interval for the specified time period
• Period – the time period when the flexible interval is active (see the time periods for detailed description of the Period format)

If multiple flexible intervals overlap, the smallest Interval value is used for the overlapping period. Note that if the smallest value of overlapping flexible intervals is ‘0’, no polling will take place. Outside the flexible intervals the default update interval is used.

Note that if the flexible interval equals the length of the period, the item will be checked exactly once. If the flexible interval is greater than the period, the item might be checked once or it might not be checked at all (thus such configuration is not advisable).

If the flexible interval is less than the period, the item will be checked at least once.

If the flexible interval is set to ‘0’, the item is not polled during the flexible interval period and resumes polling according to the default Update interval once the period is over. Examples:

<table>
<thead>
<tr>
<th>Interval</th>
<th>Period</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>1-5, 09:00-18:00</td>
<td>Item will be checked every 10 seconds during working hours.</td>
</tr>
<tr>
<td>0</td>
<td>1-7, 00:00-7:00</td>
<td>Item will not be checked during the night.</td>
</tr>
<tr>
<td>0</td>
<td>7-7, 00:00-24:00</td>
<td>Item will not be checked on Sundays.</td>
</tr>
<tr>
<td>60</td>
<td>1-7, 12:00-12:01</td>
<td>Item will be checked at 12:00 every day. Note that this was used as a workaround for scheduled checks and starting with Zabbix 3.0 it is recommended to use scheduling intervals for such checks.</td>
</tr>
</tbody>
</table>

Scheduling intervals
Scheduling intervals are used to check items at specific times. While flexible intervals are designed to redefine the default item update interval, the scheduling intervals are used to specify an independent checking schedule, which is executed in parallel.

A scheduling interval is defined as: \( md<\text{filter}>wd<\text{filter}>h<\text{filter}>m<\text{filter}>s<\text{filter}> \) where:

• \( md \) - month days
• \( wd \) - week days
• \( h \) - hours
• \( m \) - minutes
• \( s \) - seconds

<filter> is used to specify values for its prefix (days, hours, minutes, seconds) and is defined as: [<from>[<step>]<to>]] where:

• <from> and <to> define the range of matching values (included). If <to> is omitted then the filter matches a <from> – <from> range. If <from> is also omitted then the filter matches all possible values.
• `<step>` defines the skips of the number value through the range. By default `<step>` has the value of 1, which means that all values of the defined range are matched.

While the filter definitions are optional, at least one filter must be used. A filter must either have a range or the `<step>` value defined.

An empty filter matches either ‘0’ if no lower-level filter is defined or all possible values otherwise. For example, if the hour filter is omitted then only ‘0’ hour will match, provided minute and seconds filters are omitted too, otherwise an empty hour filter will match all hour values.

Valid `<from>` and `<to>` values for their respective filter prefix are:

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Description</th>
<th><code>&lt;from&gt;</code></th>
<th><code>&lt;to&gt;</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>md</td>
<td>Month days</td>
<td>1-31</td>
<td>1-31</td>
</tr>
<tr>
<td>wd</td>
<td>Week days</td>
<td>1-7</td>
<td>1-7</td>
</tr>
<tr>
<td>h</td>
<td>Hours</td>
<td>0-23</td>
<td>0-23</td>
</tr>
<tr>
<td>m</td>
<td>Minutes</td>
<td>0-59</td>
<td>0-59</td>
</tr>
<tr>
<td>s</td>
<td>Seconds</td>
<td>0-59</td>
<td>0-59</td>
</tr>
</tbody>
</table>

The `<from>` value must be less or equal to `<to>` value. The `<step>` value must be greater or equal to 1 and less or equal to `<to>` - `<from>`.

Single digit month days, hours, minutes and seconds values can be prefixed with 0. For example md01-31 and h/02 are valid intervals, but md01-031 and wd01-07 are not.

In Zabbix frontend, multiple scheduling intervals are entered in separate rows. In Zabbix API, they are concatenated into a single string with a semicolon ; as a separator.

If a time is matched by several intervals it is executed only once. For example, wd1h9;h9 will be executed only once on Monday at 9am.

Examples:

<table>
<thead>
<tr>
<th>Interval</th>
<th>Will be executed</th>
</tr>
</thead>
<tbody>
<tr>
<td>m0-59</td>
<td>every minute</td>
</tr>
<tr>
<td>h9-17/2</td>
<td>every 2 hours starting with 9:00 (9:00, 11:00 ...)</td>
</tr>
<tr>
<td>m0,30 or m/30</td>
<td>hourly at hh:00 and hh:30</td>
</tr>
<tr>
<td>md/5</td>
<td>every five minutes</td>
</tr>
<tr>
<td>wd1-5h9</td>
<td>every Monday till Friday at 9:00</td>
</tr>
<tr>
<td>wd1-5h9-18</td>
<td>every Monday till Friday at 9:00,10:00,...,18:00</td>
</tr>
<tr>
<td>h9,10 or h9-11</td>
<td>every day at 9:00, 10:00 and 11:00</td>
</tr>
<tr>
<td>md1h9m30</td>
<td>every 1st day of each month at 9:30</td>
</tr>
<tr>
<td>md1wd1h9m30</td>
<td>every 1st day of each month at 9:30 if it is Monday</td>
</tr>
<tr>
<td>h9m/30</td>
<td>every day at 9:00, 9:30</td>
</tr>
<tr>
<td>h9m0-59/30</td>
<td>every day at 9:00, 9:30</td>
</tr>
<tr>
<td>h9,10m/30</td>
<td>every day at 9:00, 9:30, 10:00, 10:30</td>
</tr>
<tr>
<td>h9-10m30</td>
<td>every day at 9:30, 10:30</td>
</tr>
<tr>
<td>h9m10-40/30</td>
<td>every day at 9:10, 9:40</td>
</tr>
<tr>
<td>h9,10m10-40/30</td>
<td>every day at 9:10, 9:40, 10:10, 10:40</td>
</tr>
<tr>
<td>h9-10m10-40/30</td>
<td>every day at 9:10, 9:40, 10:10, 10:40</td>
</tr>
<tr>
<td>h9m10-40/30</td>
<td>every day at 9:10, 9:40, 10:10, 10:40</td>
</tr>
<tr>
<td>h9,10m10-40/30</td>
<td>every day at 9:10, 9:40, 10:10, 10:40</td>
</tr>
<tr>
<td>h9-10m10-40/30</td>
<td>every day at 9:10, 9:40, 10:10, 10:40</td>
</tr>
<tr>
<td>h9m10-40/1</td>
<td>every day at 9:10, 9:11, 9:12, ..., 9:40</td>
</tr>
<tr>
<td>h9,12,15</td>
<td>every day at 9:00, 10:00, 11:00, 12:00, 15:00</td>
</tr>
<tr>
<td>h9-12,15m/0</td>
<td>every day at 9:00, 10:00, 11:00, 12:00, 15:00</td>
</tr>
<tr>
<td>h9-12,15m/0s30</td>
<td>every day at 9:00:30, 10:00:30, 11:00:30, 12:00:30, 15:00:30</td>
</tr>
<tr>
<td>h9-12s30</td>
<td>every day at 9:00:30, 9:01:30, 9:02:30, ..., 12:58:30, 12:59:30</td>
</tr>
<tr>
<td>h9m30/h10 (API-specific syntax)</td>
<td>every day at 9:00, 9:30, 10:00</td>
</tr>
<tr>
<td>h9m30</td>
<td>every day at 9:00, 9:30, 10:00</td>
</tr>
<tr>
<td>h10 (add this as another row in frontend)</td>
<td></td>
</tr>
</tbody>
</table>

2 Item types
Overview

Item types cover various methods of acquiring data from your system. Each item type comes with its own set of supported item keys and required parameters.

The following item types are currently offered by Zabbix:

- Zabbix agent checks
- SNMP agent checks
- IPMI checks
- Simple checks
  - VMware monitoring
- Log file monitoring
- Calculated items
- Zabbix internal checks
- SSH checks
- Telnet checks
- External checks
- Aggregate checks
- Trap items
- JMX monitoring
- ODBC checks
- Dependent items
- HTTP checks

Details for all item types are included in the subpages of this section. Even though item types offer a lot of options for data gathering, there are further options through user parameters or loadable modules.

Some checks are performed by Zabbix server alone (as agent-less monitoring) while others require Zabbix agent or even Zabbix Java gateway (with JMX monitoring).

Attention:
If a particular item type requires a particular interface (like an IPMI check needs an IPMI interface on the host) that interface must exist in the host definition.

Multiple interfaces can be set in the host definition: Zabbix agent, SNMP agent, JMX and IPMI. If an item can use more than one interface, it will search the available host interfaces (in the order: Agent→SNMP→JMX→IPMI) for the first appropriate one to be linked with.

All items that return text (character, log, text types of information) can return whitespace only as well (where applicable) setting the return value to an empty string (supported since 2.0).

1 Zabbix agent

Overview

These checks use the communication with Zabbix agent for data gathering.

There are passive and active agent checks. When configuring an item, you can select the required type:

- Zabbix agent - for passive checks
- Zabbix agent (active) - for active checks

Supported item keys

The table provides details on the item keys that you can use with Zabbix agent items.

See also:

- Items supported by platform
- Item keys specific for Windows agent
- Minimum permission level for Windows agent items

**Mandatory and optional parameters**

Parameters without angle brackets are mandatory. Parameters marked with angle brackets < > are optional.
<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Return value</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>agent.hostname</td>
<td>Agent hostname.</td>
<td>String</td>
<td></td>
<td>Returns the actual value of the agent hostname from a configuration file.</td>
</tr>
<tr>
<td>agent.ping</td>
<td>Agent availability check.</td>
<td>Nothing-unavailable</td>
<td></td>
<td>Use the <strong>nodata()</strong> trigger function to check for host unavailability.</td>
</tr>
<tr>
<td>agent.version</td>
<td>Version of Zabbix agent.</td>
<td>String</td>
<td></td>
<td>Example of returned value: 1.8.2</td>
</tr>
<tr>
<td>kernel.maxfiles</td>
<td>Maximum number of opened files supported by OS.</td>
<td>Integer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>kernel.maxproc</td>
<td>Maximum number of processes supported by OS.</td>
<td>Integer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>log[&lt;regexp&gt;,&lt;encoding&gt;,&lt;maxlines&gt;,&lt;mode&gt;,&lt;output&gt;,&lt;maxdelay&gt;,&lt;options&gt;]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Log file monitoring.**

**Log file** - full path and name of log file

**regexp** - regular expression\(^4\) describing the required pattern

**encoding** - code page identifier

**maxlines** - maximum number of new lines per second the agent will send to Zabbix server or proxy. This parameter overrides the value of 'MaxLinesPer-Second' in `zabbix_agentd.conf`

**mode** - possible values:
- all (default),
- skip - skip processing of older data (affects only newly created items).

**output** - an optional output formatting template. The escape sequence is replaced with the matched part of text (from the first character where match begins until the character where match ends) while an \(N\) (where \(N=1\ldots9\)) escape sequence is replaced with \(N\)th matched group (or an empty string if the \(N\) exceeds the number of captured groups).

**The item must be configured as an active check.**

- If file is missing or permissions do not allow access, item turns unsupported.

- If output is left empty - the whole line containing the matched text is returned. Note that all global regular expression types except 'Result is TRUE' always return the whole matched line and the output parameter is ignored.

**Content extraction using the output parameter takes place on the agent.**

**Examples:**

- `log[/var/log/syslog]`  
- `log[/var/log/syslog,error]`  
- `log[/home/zabbix/logs/logfile,]`

Using **output** parameter for extracting a number from log record:

- `log[/app1/app.log,"task run [0-9.]+ sec, processed ([0-9]+) records, [0-9]+ errors"",\1]`  

will match a log record "2015-11-13 10:08:26 task run 6.08 sec, processed 6080 records,

---

**See also** additional information on log monitoring.
log.count(file,<regexp>,<encoding>,<maxproclines>,<mode>,<maxdelay>,<options>)
### Log File Monitoring

**Key**

<table>
<thead>
<tr>
<th>Count of matched lines in log file monitoring.</th>
<th>Integer</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>file</strong> - full path and name of log file</td>
<td></td>
</tr>
<tr>
<td><strong>regexp</strong> - regular expression⁴ describing the required pattern</td>
<td></td>
</tr>
<tr>
<td><strong>encoding</strong> - code page identifier</td>
<td></td>
</tr>
<tr>
<td><strong>maxproclines</strong> - maximum number of new lines per second the agent will analyze (cannot exceed 10000). Default value is 10⁴*&quot;MaxLines-PerSecond&quot; in zab-bix_agentd.conf.</td>
<td></td>
</tr>
<tr>
<td><strong>mode</strong> - possible values: all (default), skip - skip processing of older data (affects only newly created items).</td>
<td></td>
</tr>
<tr>
<td><strong>maxdelay</strong> - maximum delay in seconds. Type: float. Values: 0 - (default) never ignore log file lines; &gt; 0.0 - ignore older lines in order to get the most recent lines analyzed within &quot;maxdelay&quot; seconds. Read the maxdelay notes before using it!</td>
<td></td>
</tr>
<tr>
<td><strong>options</strong> - additional options: mtime-noreread - non-unique records, reread only if the file size changes (ignore modification time).</td>
<td></td>
</tr>
</tbody>
</table>

The item must be configured as an active check.

Matching lines are counted in the new lines since the last log check by the agent, and thus depend on the item update interval.

If the file is missing or permissions do not allow access, item turns unsupported.

See also additional information on log monitoring.

Supported since Zabbix 3.2.0.

This item is not supported for Windows Event Log.

The options parameter is supported since Zabbix 4.0.19.
Key

logrt[<file_regexp>,<regexp>,<encoding>,<maxlines>,<mode>,<output>,<maxdelay>,<options>]
| Key | Log file monitoring with log rotation support. | **file_regex** - absolute path to file and the file name described by a regular expression. Note that only the file name is a regular expression. **regex** - regular expression describing the required content pattern. **encoding** - code page identifier. **maxlines** - maximum number of new lines per second the agent will send to Zabbix server or proxy. This parameter overrides the value of 'MaxLinesPer-Second' in `zabbix_agentd.conf`. **mode** - possible values: all (default), skip - skip processing of older data (affects only newly created items). **output** - an optional output formatting template. The \0 escape sequence is replaced with the matched part of text (from the first character where match begins until the character where match ends) while an \N (where N=1...9) escape sequence is replaced with the matched text of the Nth group. | The item must be configured as an active check. Log rotation is based on the last modification time of files. Note that logrt is designed to work with one currently active log file, with several other matching inactive files rotated. If, for example, a directory has many active log files, a separate logrt item should be created for each one. Otherwise if one logrt item picks up too many files it may lead to exhausted memory and a crash of monitoring. If output is left empty - the whole line containing the matched text is returned. Note that all global regular expression types except 'Result is TRUE' always return the whole matched line and the output parameter is ignored. Content extraction using the output parameter takes place on the agent. Examples: |
Key

logrt.count[file_regexp,<regexp>,<encoding>,<maxproclines>,<mode>,<maxdelay>,<options>]
<table>
<thead>
<tr>
<th>Key</th>
<th>Count of matched lines in log file monitoring with log rotation support.</th>
<th>file_regex</th>
<th>The item must be configured as an active check.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Integer</td>
<td>Matching lines are counted in the new lines since the last log check by the agent, and thus depend on the item update interval.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>file_regexp - absolute path to file and regular expression describing the file name pattern</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>regular</td>
<td>See also additional information on log monitoring.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>expression</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The options parameter is supported since Zabbix 4.0 (mtime-reread, mtime-noreread options since 4.0.19).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>exp</td>
<td>This item is not supported for Windows Event Log.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Supported since Zabbix 3.2.0.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>encoding</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>code page</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>identifier</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>maxproclines - maximum number of new lines per second the agent will analyze (cannot exceed 10000). Default value is 10^&quot;MaxLines-PerSecond&quot; in zabbix_agentd.conf</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>mode</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>possible</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>values:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>all (default), skip - skip processing of older data (affects only newly created items).</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>maxdelay</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>maximum</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>delay in</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>seconds.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Type: float. Values: 0 - (default) never ignore log file lines; &gt; 0.0 - ignore older lines in order to get the most recent lines analyzed within &quot;maxdelay&quot; seconds. Read the maxdelay notes before using it</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>options</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>type of log file rotation and other options. Possible</td>
<td></td>
</tr>
</tbody>
</table>
Key

net.dns[ip, name, <type>, <timeout>, <count>, <protocol>]

Checks if DNS service is up.

0 - DNS is down (server did not respond or DNS resolution failed)
1 - DNS is up

**ip** - IP address of DNS server (leave empty for the default DNS server, ignored on Windows)

**name** - DNS name to query

**type** - record type to be queried (default is SOA)

**timeout** - timeout for the request in seconds (default is 1 second)

**count** (ignored on Windows) - number of tries for the request (default is 2)

**protocol** - the protocol used to perform DNS queries: udp (default) or tcp

Example:

```java
=>
net.dns[8.8.8.8, example.com, MX, 2, 1]
```

The possible values for **type** are:

- ANY
- A
- NS
- CNAME
- MB
- MG
- MR
- PTR
- MD
- MF
- MX
- SOA
- NULL
- WKS (except for Windows)
- HINFO
- MINFO
- TXT
- SRV

Internationalized domain names are not supported, please use IDNA encoded names instead.

The **protocol** parameter is supported since Zabbix 3.0.

SRV record type is supported since Zabbix agent versions 1.8.6 (Unix) and 2.0.0 (Windows).

Naming before Zabbix 2.0 (still supported):

net.tcp.dns
<table>
<thead>
<tr>
<th>Key</th>
<th>Perform a DNS query.</th>
<th>Character string with the required type of information</th>
<th>ip - IP address of DNS server (leave empty for the default DNS server, ignored on Windows)</th>
<th>Example: =&gt; net.dns.record[8.8.8.8,example.com,MX,2,1]</th>
<th>The possible values for type are: ANY, A, NS, CNAME, MB, MG, MR, PTR, MD, MF, MX, SOA, NULL, WKS (except for Windows), HINFO, MINFO, TXT, SRV</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>DNS name to query</td>
<td></td>
<td>name - DNS name to query</td>
<td></td>
<td></td>
</tr>
<tr>
<td>type</td>
<td>record type to be queried (default is SOA)</td>
<td></td>
<td>type - record type to be queried (default is SOA)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>timeout</td>
<td>timeout for the request in seconds (default is 1 second)</td>
<td></td>
<td>timeout (ignored on Windows) - timeout for the request in seconds (default is 1 second)</td>
<td></td>
<td>Internationlized domain names are not supported, please use IDNA encoded names instead.</td>
</tr>
<tr>
<td>count</td>
<td>number of tries for the request (default is 2)</td>
<td></td>
<td>count (ignored on Windows) - number of tries for the request (default is 2)</td>
<td></td>
<td>The protocol parameter is supported since Zabbix 3.0. SRV record type is supported since Zabbix agent versions 1.8.6 (Unix) and 2.0.0 (Windows).</td>
</tr>
<tr>
<td>protocol</td>
<td>the protocol used to perform DNS queries: udp (default) or tcp</td>
<td></td>
<td>protocol - the protocol used to perform DNS queries: udp (default) or tcp</td>
<td></td>
<td>Naming before Zabbix 2.0 (still supported): net.tcp.dns.query</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Key</th>
<th>Number of out-of-window collisions.</th>
<th>Integer</th>
<th>if - network interface name</th>
</tr>
</thead>
<tbody>
<tr>
<td>net.if.collisions[if]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>net.if.discovery</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key</td>
<td>List of network interfaces. Used for low-level discovery.</td>
<td>JSON object</td>
<td>Supported since Zabbix agent version 2.0. On FreeBSD, OpenBSD and NetBSD supported since Zabbix agent version 2.2. Some Windows versions (for example, Server 2008) might require the latest updates installed to support non-ASCII characters in interface names.</td>
</tr>
<tr>
<td>-----</td>
<td>----------------------------------------------------------</td>
<td>-------------</td>
<td>----------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>net.if.in[if,&lt;mode&gt;]</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Key**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Incoming traffic statistics on network interface.</strong></td>
<td><strong>if</strong> - network interface name (Unix); network interface full description or IPv4 address (Windows)</td>
</tr>
<tr>
<td></td>
<td><strong>mode</strong> - possible values: bytes - number of bytes (default); packets - number of packets; errors - number of errors; dropped - number of dropped packets; overruns (fifo) - the number of FIFO buffer errors; frame - the number of packet framing errors; compressed - the number of compressed packets transmitted or received by the device driver; multicast - the number of multicast frames received by the device driver</td>
</tr>
<tr>
<td></td>
<td>On Windows, the item gets values from 64-bit counters if available. 64-bit interface statistic counters were introduced in Windows Vista and Windows Server 2008. If 64-bit counters are not available, the agent uses 32-bit counters. Multi-byte interface names on Windows are supported since Zabbix agent version 1.8.6.</td>
</tr>
<tr>
<td></td>
<td>You may obtain network interface descriptions on Windows with net.if.discovery or net.if.list items. You may use this key with the Change per second preprocessing step in order to get bytes per second statistics.</td>
</tr>
</tbody>
</table>

Examples:

- `net.if.in[eth0,errors]`  
- `net.if.in[eth0]`  

`net.if.out[if,<mode>]`
<table>
<thead>
<tr>
<th>Key</th>
<th>Outgoing traffic statistics on network interface.</th>
<th>Integer if - network interface name (Unix); network interface full description or IPv4 address (Windows)</th>
<th>On Windows, the item gets values from 64-bit counters if available. 64-bit interface statistic counters were introduced in Windows Vista and Windows Server 2008. If 64-bit counters are not available, the agent uses 32-bit counters. Multi-byte interface names on Windows are supported since Zabbix agent 1.8.6 version. Examples: =&gt; net.if.out[eth0,errors] =&gt; net.if.out[eth0] You may obtain network interface descriptions on Windows with net.if.discovery or net.if.list items. You may use this key with the Change per second preprocessing step in order to get bytes per second statistics.</th>
</tr>
</thead>
<tbody>
<tr>
<td>mode - possible values: bytes - number of bytes (default) packets - number of packets errors - number of errors dropped - number of dropped packets overruns (fifo) - the number of FIFO buffer errors collisions (colls) - the number of collisions detected on the interface carrier - the number of carrier losses detected by the device driver compressed - the number of compressed packets transmitted by the device driver</td>
<td>bytes-number of bytes</td>
<td>packets-number of packets</td>
<td>errors-number of errors</td>
</tr>
<tr>
<td>net.if.total[if,&lt;mode&gt;]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key</td>
<td>Description</td>
<td>Example</td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>-------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Sum of incoming and outgoing traffic statistics on network interface.</strong></td>
<td><strong>Integer</strong></td>
<td><strong>if</strong> - network interface name (Unix); network interface full description or IPv4 address (Windows) <strong>mode</strong> - possible values: <strong>bytes</strong> - number of bytes (default) <strong>packets</strong> - number of packets <strong>errors</strong> - number of errors <strong>dropped</strong> - number of dropped packets <strong>overruns (fifo)</strong> - the number of FIFO buffer errors <strong>compressed</strong> - the number of compressed packets transmitted or received by the device driver</td>
<td>On Windows, the item gets values from 64-bit counters if available. 64-bit interface statistic counters were introduced in Windows Vista and Windows Server 2008. If 64-bit counters are not available, the agent uses 32-bit counters. Examples: <code>=&gt; net.if.total[eth0.errors]</code> <code>=&gt; net.if.total[eth0]</code> You may obtain network interface descriptions on Windows with net.if.discovery or net.if.list items. You may use this key with the Change per second preprocessing step in order to get bytes per second statistics. Note that dropped packets are supported only if both net.if.in and net.if.out work for dropped packets on your platform.</td>
</tr>
</tbody>
</table>

`net.tcp.listen[port]`
### Key

<table>
<thead>
<tr>
<th>net.tcp.listen[port]</th>
<th>Checks if this TCP port is in LISTEN state.</th>
<th>Example:</th>
<th>On Linux supported since Zabbix agent version 1.8.4</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0 - it is not in LISTEN state</td>
<td>=&gt; net.tcp.listen[80]</td>
<td>Since Zabbix 3.0.0, on Linux kernels 2.6.14 and above, information about listening TCP sockets is obtained from the kernel’s NETLINK interface, if possible. Otherwise, the information is retrieved from /proc/net/tcp and /proc/net/tcp6 files.</td>
</tr>
<tr>
<td></td>
<td>1 - it is in LISTEN state</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

net.tcp.port[ip, port]

<table>
<thead>
<tr>
<th>Checks if it is possible to make TCP connection to specified port.</th>
<th>0 - cannot connect</th>
<th>ip - IP or DNS name (default is 127.0.0.1)</th>
<th>Example:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1 - can connect</td>
<td>port - port number</td>
<td>=&gt; net.tcp.port[,80]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>→ can be used to test availability of web server running on port 80.</td>
<td></td>
</tr>
</tbody>
</table>

For simple TCP performance testing use net.tcp.service.perf/tcp,<ip>,<port>;

Note that these checks may result in additional messages in system daemon logfiles (SMTP and SSH sessions being logged usually).

Old naming: check_port[*]
<table>
<thead>
<tr>
<th>Checks if service is running and accepting TCP connections.</th>
<th>0 - service is down</th>
<th>service - either of: ssh, ldap, smtp, ftp, http, pop, nntp, imap, tcp, https, telnet (see details)</th>
<th>Example: =&gt; net.tcp.service[ftp, 45] → can be used to test the availability of FTP server on TCP port 45.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1 - service is running</td>
<td>ip - IP address (default is 127.0.0.1)</td>
<td>Note that these checks may result in additional messages in system daemon logfiles (SMTP and SSH sessions being logged usually).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>port - port number (by default standard service port number is used)</td>
<td>Checking of encrypted protocols (like IMAP on port 993 or POP on port 995) is currently not supported. As a workaround, please use net.tcp.port for checks like these.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Note that the telnet check looks for a login prompt (':' at the end).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>See also known issues of checking HTTPS service.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>https and telnet services are supported since Zabbix 2.0.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Old naming: check_service[*]</td>
</tr>
</tbody>
</table>
net.tcp.service.perf[service,<ip>,<port>]

Checks performance of TCP service.

0 - service is down

seconds - the number of seconds spent while connecting to the service

service - either of: ssh, ldap, smtp, ftp, http, pop, nntp, imap, tcp, https, telnet (see details)

ip - IP address (default is 127.0.0.1)

port - port number (by default standard service port number is used)

Example:
=> net.tcp.service.perf[ssh]
→ can be used to test the speed of initial response from SSH server.

Checking of encrypted protocols (like IMAP on port 993 or POP on port 995) is currently not supported. As a workaround, please use net.tcp.service.perf[tcp,<ip>,<port>] for checks like these.

Checking of LDAP and HTTPS by Windows agent is currently not supported.

Note that the telnet check looks for a login prompt (‘:’ at the end).

See also known issues of checking HTTPS service.

https and telnet services are supported since Zabbix 2.0.

Old naming:
check_service_perf[*]

net.udp.listen[port]

Checks if this UDP port is in LISTEN state.

0 - it is not in LISTEN state

1 - it is in LISTEN state

port - UDP port number

Example:
=> net.udp.listen[68]

On Linux supported since Zabbix agent version 1.8.4

net.udp.service[service,<ip>,<port>]
Checks if service is running and responding to UDP requests.

Key

0 - service is down
1 - service is running

- service - ntp (see details)
- ip - IP address (default is 127.0.0.1)
- port - port number (by default standard service port number is used)

Example:

```
net.udp.service[ntp] 45
```

This item is supported since Zabbix 3.0.0, but ntp service was available for net.tcp.service[] item in prior versions.

---

**net.udp.service.perf[service,<ip>,<port>]**

Checks performance of UDP service.

0 - service is down
0 - service is down

- service - ntp (see details)
- ip - IP address (default is 127.0.0.1)
- port - port number (by default standard service port number is used)

Example:

```
net.udp.service.perf[ntp]
```

This item is supported since Zabbix 3.0.0, but ntp service was available for net.tcp.service[] item in prior versions.

---

**proc.cpu.util[name,<user>,<type>,<cmdline>,<mode>,<zone>]**
<table>
<thead>
<tr>
<th>Key</th>
<th>Float</th>
<th>Examples:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process CPU utilization</td>
<td>name - process name</td>
<td>=&gt; proc.cpu.util[root] → CPU utilization of all processes running under</td>
</tr>
<tr>
<td>percentage.</td>
<td>(default is all processes)</td>
<td>the “root” user</td>
</tr>
<tr>
<td></td>
<td>user - user name</td>
<td>=&gt; proc.cpu.util[zabbix_server,zabbix] → CPU utilization of all zabbix_server processes running under the zabbix user</td>
</tr>
<tr>
<td></td>
<td>type - CPU utilization type:</td>
<td>total (default), user, system</td>
</tr>
<tr>
<td></td>
<td>cmdline - filter by command line (it is a regular expression)</td>
<td>mode - data gathering mode: avg1 (default), avg5, avg15</td>
</tr>
<tr>
<td></td>
<td>zone - target zone:</td>
<td>The returned value is based on single CPU core utilization percentage.</td>
</tr>
<tr>
<td></td>
<td>current (default), all.</td>
<td>For example CPU utilization of a process fully using two cores is 200%.</td>
</tr>
<tr>
<td></td>
<td>This parameter is supported on Solaris only.</td>
<td>The process CPU utilization data is gathered by a collector which supports the maximum of 1024 unique (by name, user and command line) queries. Queries not accessed during the last 24 hours are removed from the collector.</td>
</tr>
</tbody>
</table>

Note that when setting the zone parameter to current (or default) in case the agent has been compiled on a Solaris without zone support, but running on a newer Solaris where zones are supported, then the agent will return NOT-SUPPORTED (the agent
Key

proc.mem[<name>,<user>,<mode>,<cmdline>,<memtype>]
Key

Memory used by process in bytes. Integer - with mode as max, min, sum
Float - with mode as avg

name - process name (default is all processes)
user - user name (default is all users)
mode - possible values: avg, max, min, sum (default)
cmdline - filter by command line (it is a regular expression)
memtype - type of memory used by process

Examples:
=> proc.mem[root] → memory used by all processes running under the "root" user
=> proc.mem[zabbix_server,zabbix] → memory used by all zabbix_server processes running under the zabbix user
=> proc.mem[oracle,max,oracleZABBIX] → memory used by the most memory-hungry process running under oracle having oracleZABBIX in its command line

Note: When several processes use shared memory, the sum of memory used by processes may result in large, unrealistic values.

See notes on selecting processes with name and cmdline parameters (Linux-specific).

When this item is invoked from the command line and contains a command line parameter (e.g. using the agent test mode: zabbix_agentd -t proc.mem[,.,apache2]), one extra process will be
Key

proc.num[<name>,<user>,<state>,<cmdline>,<zone>]

192
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Examples:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>name</strong></td>
<td>process name (default is all processes)</td>
<td>proc.num[,mysql] → number of processes running under the mysql user</td>
</tr>
<tr>
<td><strong>user</strong></td>
<td>user name (default is all users)</td>
<td>proc.num[apache2,www-data] → number of apache2 processes running under the www-data user</td>
</tr>
<tr>
<td><strong>state</strong></td>
<td>possible values: all (default), disk - uninterruptible sleep, run - running, sleep - interruptible sleep, trace - stopped, zomb - zombie</td>
<td>proc.num[,oracle,sleep,oracleZABBIX] → number of processes in sleep state running under oracle having oracleZABBIX in its command line</td>
</tr>
<tr>
<td><strong>cmdline</strong></td>
<td>filter by command line (it is a regular expression)</td>
<td>See notes on selecting processes with name and cmdline parameters (Linux-specific).</td>
</tr>
<tr>
<td><strong>zone</strong></td>
<td>target zone: current (default), all.</td>
<td>On Windows, only the name and user parameters are supported.</td>
</tr>
</tbody>
</table>

This parameter is supported on Solaris only.

Notewhen setting the zone parameter to current (or default) in case the agent has been compiled on a Solaris withoutzone support, but running on a newer Solaris where zones are supported, the agent will return NOT-SUPPORTED (the agent cannot limit resultsto only the current zone). However, all is supported in this case.

Disk and trace values for the state parameter are supported since Zabbix 3.4.0.

When this item is invoked from the command line and contains a command line parameter (e.g. using the agent test mode: zabbix_agentd -t proc.num[,..,apache2]), one extra process will be counted, as the agent will count itself.

Note that when setting the zone parameter to
<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Type</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>sensor[device,sensor,&lt;mode&gt;]</td>
<td>Hardware sensor reading.</td>
<td>Float</td>
<td>Reads ( /proc/sys/dev/sensors ) on Linux 2.4. Example: <code>=&gt; sensor[w83781d-i2c-0-2d,temp1]</code> Prior to Zabbix 1.8.4, the sensor[temp1] format was used. Reads ( /sys/class/hwmon ) on Linux 2.6+. See a more detailed description of sensor item on Linux. Reads the hw.sensors MIB on OpenBSD. Examples: <code>=&gt; sensor[cpu0,temp0]</code> → temperature of one CPU <code>=&gt; sensor[&quot;cpu[0-2]&quot;,temp,avg]</code> → average temperature of the first three CPU's Supported on OpenBSD since Zabbix 1.8.4.</td>
</tr>
<tr>
<td>system.boottime</td>
<td>System boot time.</td>
<td>Integer (Unix timestamp)</td>
<td></td>
</tr>
<tr>
<td>system.cpu.discovery</td>
<td>List of detected CPUs/CPU cores. Used for low-level discovery.</td>
<td>JSON object</td>
<td>Supported on all platforms since 2.4.0.</td>
</tr>
<tr>
<td>system.cpu.intr</td>
<td>Device interrupts.</td>
<td>Integer</td>
<td></td>
</tr>
<tr>
<td>system.cpu.load[&lt;cpu&gt;,&lt;mode&gt;]</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Key | CPU load. | Float | **cpu** - possible values: all (default), percpu (total load divided by online CPU count)  
 hypo - possible values: avg1 (one-minute average, default), avg5, avg15 | Example:  
 => system.cpu.load[,avg5]  
 percpu is supported since Zabbix 2.0.0.  
 Old naming:  
 system.cpu.loadX |
|-----|----------|-------|-------------------------------|----------------------------------|------|
| system.cpu.num[,type] | Number of CPUs. | Integer | **type** - possible values: online (default), max | Example:  
 => system.cpu.num | ------ |
| system.cpu.switches | Count of context switches. | Integer | | Old naming:  
 system[switches] | ------ |
| system.cpu.util[,cpu],[,type],[,mode] | | | | |
Key

<table>
<thead>
<tr>
<th>Feature</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU utilization percentage.</td>
<td>Float</td>
<td><code>cpu</code> - <code>&lt;CPU number&gt;</code> or all (default)</td>
</tr>
<tr>
<td><code>type</code> - possible values:</td>
<td></td>
<td>user (default), idle, nice, system (default for Windows), iowait, interrupt,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>softirq, steal, guest (on Linux kernels 2.6.24 and above), guest_nice (on</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Linux kernels 2.6.33 and above). Parameters user and nice time no longer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>include guest time and guest_nice time since Zabbix 3.0.14, 3.4.5 and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4.0.0. See also platform-specific details for this parameter.</td>
</tr>
<tr>
<td><code>mode</code> - possible values:</td>
<td></td>
<td>avg1 (one-minute average, default), avg5, avg15</td>
</tr>
</tbody>
</table>

On Windows, the value is acquired using the Processor Time performance counter. Note that since Windows 8 its Task Manager shows CPU utilization based on the Processor Utility performance counter, while in previous versions it was the Processor Time counter.

Example:

```
=> system.cpu.util[0,user,avg5]
```

Old naming:

```
system.cpu.idleX, system.cpu.niceX, system.cpu.systemX, system.cpu.userX
```

system.hostname[<type>]
System host name. | String | **type** (Windows only, must not be used on other systems) - possible values: netbios (default) or host

The value is acquired by either GetComputerName() (for netbios) or gethostname() (for host) functions on Windows and by taking nodename from the uname() system API output on other systems.

Examples of returned values:
on Linux:
=> system.hostname
   → linux-w7x1
=> system.hostname
   → www.example.com
on Windows:
=> system.hostname
   → WIN-SERV2008-I6
=> system.hostname[host]
   → Win-Serv2008-I6LonG

The type parameter for this item is supported since Zabbix 1.8.6.

See also a more detailed description.
<table>
<thead>
<tr>
<th>Key</th>
<th>Chassis information.</th>
<th>String info - one of full (default), model, serial, type or vendor</th>
<th>Example: system.hw.chassis[full] Hewlett-Packard HP Pro 3010 Small Form Factor PC CZXXXXXXX Desktop</th>
</tr>
</thead>
</table>

This key depends on the availability of the **SMBIOS** table. Will try to read the DMI table from sysfs, if sysfs access fails then try reading directly from memory.

**Root permissions** are required because the value is acquired by reading from sysfs or memory.

Supported since Zabbix agent version 2.0.
### Key

<table>
<thead>
<tr>
<th>CPU information.</th>
<th>String or integer</th>
<th><strong>cpu</strong> - CPU number or all (default) info - possible values: full (default), curfreq, maxfreq, model or vendor</th>
<th>Example: =&gt; system.hw.cpu[0,vendor] =&gt; AuthenticAMD</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Gathers info from /proc/cpuinfo and /sys/devices/system/cpu/cpu[cpunum]/cpufreq/cpuinfo_max_freq.</td>
<td>If a CPU number and curfreq or maxfreq is specified, a numeric value is returned (Hz).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Supported since Zabbix agent version 2.0.</td>
<td>Supported since Zabbix agent version 2.0.</td>
</tr>
</tbody>
</table>

**system.hw.devices[<type>]**

Listing of PCI or USB devices.

<table>
<thead>
<tr>
<th>type - pci (default) or usb</th>
<th>Example: =&gt; system.hw.devices[pci] 00:00.0 Host bridge: Advanced Micro Devices [AMD] RS780 Host Bridge [...]</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Returns the output of either lspci or lsusb utility (executed without any parameters)</td>
</tr>
<tr>
<td></td>
<td>Supported since Zabbix agent version 2.0.</td>
</tr>
</tbody>
</table>

**system.hw.macaddr[<interface>,<format>]**
Key

| Listing of MAC addresses. | String | interface - all (default) or a regular expression
format - full (default) or short | Lists MAC addresses of the interfaces whose name matches the given interface regular expression (all lists for all interfaces).

Example:
=> system.hw.macaddr("eth0",full)
→ [eth0]
00:11:22:33:44:55

If format is specified as short, interface names and identical MAC addresses are not listed.

Supported since Zabbix agent version 2.0.

---

system.localtime[<type>]

System time. Integer - with type as utc
String - with type as local
type - possible values:
utc - (default) the time since the Epoch (00:00:00 UTC, January 1, 1970), measured in seconds.
local - the time in the 'yyyy-mm-dd, hh:mm:ss.nnnn,+hh:mm' format

Must be used as a passive check only.

Parameters for this item are supported since Zabbix agent version 2.0.

Example:
=> system.localtime[local]
→ create an item using this key and then use it to display host time in the Clock screen element.

---

system.run[command,<mode>]

Use the system.run API call to execute a command on the Zabbix agent.

For more information, refer to the Zabbix documentation on system.run.
Run specified command on the host.

<table>
<thead>
<tr>
<th>command</th>
<th>Text result of the command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - with mode as nowait (regardless of command result)</td>
<td></td>
</tr>
</tbody>
</table>

**command** - command for execution

**mode** - possible values: wait - wait end of execution (default), nowait - do not wait

Up to 512KB of data can be returned, including trailing whitespace that is truncated. To be processed correctly, the output of the command must be text.

Example:

```
=> system.run[ls -l /
]→ detailed file list of root directory.
```

Note: To enable this functionality, the agent configuration file must contain `EnableRemoteCommands=1` option.

The return value of the item is standard output together with standard error produced by command. The exit code is not checked.

Empty result is allowed starting with Zabbix 2.4.0.

See also: Command execution.

```system.stat[resource,<type>]```
### Key

<table>
<thead>
<tr>
<th>System statistics.</th>
<th>Integer or float</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ent</strong> - number of processor units this partition is entitled to receive (float)</td>
<td></td>
</tr>
<tr>
<td><strong>kthr,</strong>&lt;type&gt;** -** information about kernel thread states:</td>
<td></td>
</tr>
<tr>
<td>r - average number of runnable kernel threads (float)</td>
<td></td>
</tr>
<tr>
<td>b - average number of kernel threads placed in the Virtual Memory Manager wait queue (float)</td>
<td></td>
</tr>
<tr>
<td><strong>memory,</strong>&lt;type&gt;** -** information about the usage of virtual and real memory:</td>
<td></td>
</tr>
<tr>
<td>avm - active virtual pages (integer)</td>
<td></td>
</tr>
<tr>
<td>fre - size of the free list (integer)</td>
<td></td>
</tr>
<tr>
<td><strong>page,</strong>&lt;type&gt;** -** information about page faults and paging activity:</td>
<td></td>
</tr>
<tr>
<td>fi - file page-ins per second (float)</td>
<td></td>
</tr>
<tr>
<td>fo - file page-outs per second (float)</td>
<td></td>
</tr>
<tr>
<td>pi - pages paged in from paging space (float)</td>
<td></td>
</tr>
<tr>
<td>po - pages paged out to paging space (float)</td>
<td></td>
</tr>
<tr>
<td>fr - pages freed by page replacement (float)</td>
<td></td>
</tr>
<tr>
<td>sr - pages scanned by page replacement algorithm (float)</td>
<td></td>
</tr>
<tr>
<td><strong>faults,</strong>&lt;type&gt;** -** trap and interrupt rate:</td>
<td></td>
</tr>
<tr>
<td>in - device interrupts (float)</td>
<td></td>
</tr>
<tr>
<td>sy - system calls (float)</td>
<td></td>
</tr>
<tr>
<td>cs - kernel thread context switches (float)</td>
<td></td>
</tr>
<tr>
<td><strong>cpu,</strong>&lt;type&gt;** -** breakdown of percentage usage of processor time:</td>
<td></td>
</tr>
<tr>
<td>us - user time (float)</td>
<td></td>
</tr>
<tr>
<td>sy - system time (float)</td>
<td></td>
</tr>
<tr>
<td>id - idle time (float)</td>
<td></td>
</tr>
<tr>
<td>wa - idletime during which the system had outstanding disk/NFS I/O request(s) (float)</td>
<td></td>
</tr>
<tr>
<td>pc - number of physical processors consumed (float)</td>
<td></td>
</tr>
<tr>
<td>ec - the percentage of entitled capacity consumed (float)</td>
<td></td>
</tr>
<tr>
<td>lbusy - indicates the percentage of logical processor(s) utilization that occurred while executing at the user and system level (float)</td>
<td></td>
</tr>
<tr>
<td>app - indicates the available physical processors in the shared pool (float)</td>
<td></td>
</tr>
<tr>
<td><strong>disk,</strong>&lt;type&gt;** -** disk statistics:</td>
<td></td>
</tr>
<tr>
<td>bps - indicates the amount of data transferred (read or written) to the drive in bytes per second (integer)</td>
<td></td>
</tr>
<tr>
<td>tps - indicates the number of transfers per second that were issued to the physical disk/tape (float)</td>
<td></td>
</tr>
</tbody>
</table>
This item is supported on AIX only, since Zabbix 1.8.1.
The following items are supported only on AIX LPAR of type “Shared”:
- system.stat[cpu,app]
- system.stat[cpu,ec]
(also on “Dedicated” since Zabbix 4.0.1; always returns 100 (percent))
- system.stat[cpu,ibusy]
- system.stat[cpu,pc]
(also on “Dedicated” since Zabbix 4.0.1)
- system.stat[ent]
(also on “Dedicated” since Zabbix 4.0.1)

system.sw.arch

Software architecture information.

Example:
=> system.sw.arch
   → i686

Info is acquired from uname() function.

Supported since Zabbix agent version 2.0.
<table>
<thead>
<tr>
<th>Key</th>
<th>Operating system information.</th>
<th>String info - possible values: full (default), short or name</th>
<th>Example: =&gt; system.sw.os[short]→ Ubuntu 2.6.35-28.50-generic 2.6.35.11</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Info is acquired from (note that not all files and options are present in all distributions): /proc/version (full) /proc/version_signature (short) PRETTY_NAME parameter from /etc/os-release on systems supporting it, or /etc/issue.net (name)</td>
<td>Supported since Zabbix agent version 2.0.</td>
</tr>
</tbody>
</table>

system.sw.packages[<package>,<manager>,<format>]
Key

Listing of installed packages.

| package | all 
| default) or a regular expression | manager | all 
| default) or a package manager | format | full 
| default) or short |

Lists (alphabetically) installed packages whose name matches the given package regular expression (all lists them all).

Example:
```
=> system.sw.packages[mini,dpkg,short]
→ python-minimal, python2.6-minimal, ubuntu-minimal
```

Supported package managers (executed command):
- dpkg (dpkg -- get-selections)
- pkgtool (ls /var/log/packages)
- rpm (rpm -qa)
- pacman (pacman -Q)

If format is specified as full, packages are grouped by package managers (each manager on a separate line beginning with its name in square brackets).

If format is specified as short, packages are not grouped and are listed on a single line.

Supported since Zabbix agent version 2.0.

```
=system.swap.in[<device>,<type>]
```
Key

Swap in (from device into memory) statistics.

| **device** | device used for swapping (default is all) |
| **type** | possible values: count (number of swapins), sectors (sectors swapped in), pages (pages swapped in). |
| **Example:** | => system.swap.in[,pages] |
| **Source:** | /proc/swaps, /proc/partitions, /proc/stat (Linux 2.4) /proc/swaps, /proc/diskstats, /proc/vmstat (Linux 2.6) |

Swap out (from memory onto device) statistics.

| **device** | device used for swapping (default is all) |
| **type** | possible values: count (number of swapouts), sectors (sectors swapped out), pages (pages swapped out). |
| **Example:** | => system.swap.out[,pages] |
| **Source:** | /proc/swaps, /proc/partitions, /proc/stat (Linux 2.4) /proc/swaps, /proc/diskstats, /proc/vmstat (Linux 2.6) |

Swap in (from device into memory) statistics.

| **device** | device used for swapping (default is all) |
| **type** | possible values: count (number of swapins), sectors (sectors swapped in), pages (pages swapped in). |
| **Example:** | => system.swap.in[,pages] |
| **Source:** | /proc/swaps, /proc/partitions, /proc/stat (Linux 2.4) /proc/swaps, /proc/diskstats, /proc/vmstat (Linux 2.6) |

Swap out (from memory onto device) statistics.

<p>| <strong>device</strong> | device used for swapping (default is all) |
| <strong>type</strong> | possible values: count (number of swapouts), sectors (sectors swapped out), pages (pages swapped out). |
| <strong>Example:</strong> | =&gt; system.swap.out[,pages] |
| <strong>Source:</strong> | /proc/swaps, /proc/partitions, /proc/stat (Linux 2.4) /proc/swaps, /proc/diskstats, /proc/vmstat (Linux 2.6) |</p>
<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Swapspace size in bytes or</td>
<td>Integer - for bytes</td>
</tr>
<tr>
<td>in percentage from total.</td>
<td>Float - for percentage</td>
</tr>
<tr>
<td><strong>device</strong> - device used</td>
<td>device used for swapping</td>
</tr>
<tr>
<td>for swapping</td>
<td>(default is all)</td>
</tr>
<tr>
<td><strong>type</strong> - possible values:</td>
<td>free (free swap space, default), pfree (free swap space, in percent),</td>
</tr>
<tr>
<td></td>
<td>pused (used swap space, in percent), total (total swap space), used (used</td>
</tr>
<tr>
<td></td>
<td>swap space)</td>
</tr>
<tr>
<td></td>
<td>See also platform-specific details for this parameter.</td>
</tr>
</tbody>
</table>

Example:

- => system.swap.size[,pfree]  
  \[\rightarrow \text{free swap space percentage}\]

If device is not specified, Zabbix agent will only take into account swap devices (files), physical memory will be ignored. For example, on Solaris systems, `swap -s` command includes a portion of physical memory and swap devices (unlike `swap -l`).

Note that this key might report incorrect swap space size/percentage on virtualized (VMware ESXi, VirtualBox) Windows platforms. In this case, you may use the `perf_counter[\%Total]` key to obtain correct swap space percentage.

Old naming:

- `system.swap.free`, `system.swap.total`
<table>
<thead>
<tr>
<th>Identification of the system.</th>
<th>String Example of returned value (Unix): FreeBSD localhost 4.2-RELEASE FreeBSD 4.2-RELEASE #0: Mon Nov i386</th>
</tr>
</thead>
</table>

On Unix since Zabbix 2.2.0 the value for this item is obtained with `uname()` system call. Previously it was obtained by invoking “uname -a”. The value of this item might differ from the output of “uname -a” and does not include additional information that “uname -a” prints based on other sources.

On Windows since Zabbix 3.0 the value for this item is obtained from `Win32_OperatingSystem` and `Win32_Processor` WMI classes. Previously it was obtained from volatile Windows APIs and undocumented registry keys.
### Key

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
<th>Type</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>system.uptime</td>
<td>System uptime in seconds.</td>
<td>Integer</td>
<td>In configuration, use <code>s</code> or <code>uptime</code> units to get readable values.</td>
</tr>
<tr>
<td>system.users.num</td>
<td>Number of users logged in.</td>
<td>Integer</td>
<td><code>who</code> command is used on the agent side to obtain the value.</td>
</tr>
<tr>
<td>vfs.dev.read[&lt;device&gt;,&lt;type&gt;,&lt;mode&gt;]</td>
<td>Disk read statistics.</td>
<td>Integer</td>
<td>You may use relative device names (for example, sda) as well as an optional <code>/dev/</code> prefix (for example, <code>/dev/sda</code>).</td>
</tr>
</tbody>
</table>

#### `vfs.dev.read[<device>,<type>,<mode>]`

- **device** - disk device (default is all 3).
- **type** - possible values: sectors, operations, bytes, sps, ops, bps.
- **mode** - possible values: avg1 (one-minute average, default), avg5, avg15.

Example:

```
=> vfs.dev.read[,operations]
```

Old naming: `io[*]`
vfs.dev.write[<device>,<type>,<mode>]

Disk write statistics.

- **device** - disk device (default is all 3)
- **type** - possible values: sectors, operations, bytes
- **mode** - possible values: avg1 (one-minute average, default), avg5, avg15.

You may use relative device names (for example, sda) as well as an optional /dev/ prefix (for example, /dev/sda).

LVM logical volumes are supported.

Note: Since 4.0.4, if using an update interval of three hours or more 2, will always return ‘0’

LVM logical volumes are supported.

Old naming:

vfs.dir.count[<dir>,<regex_incl>,<regex_excl>,<types_incl>,<types_excl>,<max_depth>,<min_size>,<max_size>,<min_age>,<max_age>]
<table>
<thead>
<tr>
<th>Key</th>
<th>Directory entry count.</th>
<th>Integer</th>
<th>dir - absolute path to directory</th>
<th>Environment variables, e.g. %APP_HOME%, $HOME and %TEMP% are not supported.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>regex_incl - regular expression</td>
<td>Pseudo-directories &quot;.&quot; and &quot;..&quot; are never counted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>describing the name pattern of the entity (file, directory, symbolic link) to include; include all if empty (default value)</td>
<td>Symbolic links are never followed for directory traversal.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>regex_excl - regular expression</td>
<td>On Windows, directory symlinks are skipped and hard links are counted only once.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>describing the name pattern of the entity (file, directory, symbolic link) to exclude; don't exclude any if empty (default value)</td>
<td>Both regex_incl and regex_excl are being applied to files and directories when calculating entry size, but are ignored when picking subdirectories to traverse (if regex_incl is &quot;(?i)^.+.zip$&quot; and max_depth is not set, then all subdirectories will be traversed, but only files of type zip will be counted).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>types_incl - directory entry types to count, possible values: file - regular file, dir - subdirectory, sym - symbolic link, sock - socket, bdev - block device, cdev - character device, fifo - FIFO, dev - synonymous with &quot;bdev,cdev&quot;, all - all types (default), i.e. &quot;file,dir,sym,sock&quot;. Multiple types must be separated with comma and quoted.</td>
<td>Execution time is limited by the default timeout value in agent configuration (3 sec). Since large directory traversal may take longer than that, no data will be returned and partial count will not be returned.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>types_excl - directory entry types (see &lt;types_incl&gt;) to NOT count. If some entry type is in both &lt;types_incl&gt; and &lt;types_excl&gt;, directory entry will not be counted.</td>
<td>Execution time is limited by the default timeout value in agent configuration (3 sec). Since large directory traversal may take longer than that, no data will be returned and partial count will not be returned.</td>
</tr>
</tbody>
</table>
Key

vfs.dir.size[<regex_incl>,<regex_excl>,<mode>,<max_depth>,<regex_excl_dir>]
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>dir</strong> - absolute path to directory</td>
<td></td>
<td></td>
<td><strong>regex_incl</strong> - regular</td>
<td>expression</td>
<td>describing the name pattern of the entity (file, directory, symbolic link) to include; include all if empty (default value)</td>
<td></td>
<td><strong>regex_excl</strong> - regular</td>
<td>expression</td>
</tr>
<tr>
<td><strong>mode</strong> - possible values: apparent</td>
<td>(default) - gets apparent file sizes rather than disk usage (acts as du -sb dir), disk - gets disk usage (acts as du -a -B1 dir). Unlike du command, vfs.dir.size item takes hidden files in account when calculating directory size (acts as du -ab .[^.]* [^.*] * within dir).</td>
<td></td>
<td><strong>max_depth</strong> - maximum depth of subdirectories to traverse. -1 (default) - unlimited, 0 - no descending into subdirectories.</td>
<td><strong>regex_excl_dir</strong> - regular expression</td>
<td>describing the</td>
<td></td>
<td><strong>max_depth</strong> - maximum depth of subdirectories to traverse. -1 (default) - unlimited, 0 - no descending into subdirectories.</td>
<td><strong>regex_excl_dir</strong> - regular expression</td>
</tr>
</tbody>
</table>

Only directories with at least read permission for zabbix user are calculated.

On Windows any symlink is skipped and hard links are taken into account only once.

With large directories or slow drives this item may time out due to the Timeout setting in agent and server/proxy configuration files. Increase the timeout values as necessary.

Examples:

⇒ vfs.dir.size[/tmp,log]
- calculates size of all files in /tmp which contain 'log'

⇒ vfs.dir.size[/tmp,log,.+\.[old]$]
- calculates size of all files in /tmp which contain 'log', excluding files containing '.old'

The file size limit depends on large file support.

The **regex_excl_dir** parameter is supported since Zabbix 4.0.4.

Supported since Zabbix 3.4.0.
<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Type</th>
<th>Parameters</th>
<th>Example:</th>
</tr>
</thead>
<tbody>
<tr>
<td>vfs.file.cksum[file]</td>
<td>File checksum, calculated by the UNIX cksum algorithm.</td>
<td>Integer</td>
<td>file - full path to file</td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>=&gt; vfs.file.cksum[/etc/passwd]</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Example of returned value: 1938292000</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Old naming: cksum</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>The file size limit depends on large file support.</td>
</tr>
<tr>
<td>vfs.file.contents[file,&lt;encoding&gt;]</td>
<td>Retrieving contents of a file.</td>
<td>Text</td>
<td>file - full path to file encoding - code page identifier</td>
<td>Returns an empty string if the file is empty or contains LF/CR characters only.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Byte order mark (BOM) is excluded from the output since Zabbix 4.0.15.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>=&gt; vfs.file.contents[/etc/passwd]</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>This item is limited to files no larger than 64 Kbytes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Supported since Zabbix agent version 2.0.</td>
</tr>
<tr>
<td>vfs.file.exists[file]</td>
<td>Checks if file exists.</td>
<td>0 - not found</td>
<td>file - full path to file</td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - regular file or a link (symbolic or hard) to regular file exists</td>
<td>=&gt; vfs.file.exists[/tmp/application.pid]</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>The return value depends on what S_ISREG POSIX macro returns.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>The file size limit depends on large file support.</td>
</tr>
<tr>
<td>vfs.file.md5sum[file]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key</td>
<td>MD5 checksum of file.</td>
<td>Character string (MD5 hash of the file)</td>
<td>file - full path to file</td>
<td>Example:</td>
</tr>
<tr>
<td>-----</td>
<td>----------------------</td>
<td>----------------------------------------</td>
<td>------------------------</td>
<td>----------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vfs.file.md5sum[/usr/local/etc/zabbix_agentd.conf]</td>
<td>=&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Example of returned value:</td>
<td>b5052decb577e0fffd622d6ddc017e82</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The file size limit (64 MB)</td>
<td>for this item was removed in version 1.8.6.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The file size limit depends on large file support.</td>
<td></td>
</tr>
<tr>
<td>Key</td>
<td>Description</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>-------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Find string in a file.</td>
<td>The line containing the matched string, or as specified by the optional output parameter</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>file</code> - full path to file</td>
<td>Only the first matching line is returned. An empty string is returned if no line matched the expression.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>regexp</code> - regular expression</td>
<td>Byte order mark (BOM) is excluded from the output since Zabbix 4.0.15.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>encoding</code> - code page identifier</td>
<td>Content extraction using the output parameter takes place on the agent.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>start line</code> - the number of first line to search (first line of file by default).</td>
<td>The start line, end line and output parameters are supported from version 2.2.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>end line</code> - the number of last line to search (last line of file by default).</td>
<td>Examples:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>output</code> - an optional output formatting template. The <code>\0</code> escape sequence is replaced with the matched part of text (from the first character where match begins until the character where match ends) while an \N (where \N = 1...9) escape sequence is replaced with Nth matched group (or an empty string if the N exceeds the number of captured groups).</td>
<td>=&gt;</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

```
vfs.file.regmatch[file,regexp,<encoding>,<start line>,<end line>]
```
<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>vfs.file.size[file]</strong></td>
<td>File size (in bytes).</td>
<td>The file must have read permissions for user zabbix.</td>
</tr>
<tr>
<td><strong>vfs.file.time[file,&lt;mode&gt;]</strong></td>
<td>File time information.</td>
<td>The file size limit depends on large file support.</td>
</tr>
<tr>
<td><strong>vfs.fs.discovery</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key</td>
<td>List of mounted filesystems. Used for low-level discovery.</td>
<td>JSON object</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>------------------------------------------------------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>

**vfs.fs.get**

List of mounted filesystems, their types, disk space and inode statistics. Can be used for low-level discovery.

**vfs.fs.inode[fs,<mode>]**

- Number or percentage of inodes. 
- Integer - for number
- Float - for percentage

- fs - filesystem
- mode - possible values: total (default), free, used, //pfree // (free, percentage), pused (used, percentage)

Example:

```bash
vfs.fs.inode[/,pfree]
```

Old naming:

- vfs.fs.inode.free[*], vfs.fs.inode.pfree[*], vfs.fs.inode.total[*]

**vfs.fs.size[fs,<mode>]**

- Disk space in bytes or in percentage from total.
- Integer - for bytes
- Float - for percentage

- fs - filesystem
- mode - possible values: total (default), free, used, pfree (free, percentage), pused (used, percentage)

Example:

```bash
vfs.fs.size[/tmp,free]
```

In case of a mounted volume, disk space for local file system is returned.

Reserved space of a file system is taken into account and not included when using the free mode.

Old naming:

- vfs.fs.free[*], vfs.fs.total[*], vfs.fs.used[*], vfs.fs.pfree[*], vfs.fs.pused[*]

**vm.memory.size[<mode>]**
<table>
<thead>
<tr>
<th>Key</th>
<th>Memory size in bytes or in percentage from total.</th>
<th>Integer - for bytes</th>
<th>Float - for percentage</th>
<th><strong>mode</strong> - possible values: total (default), active, anon, buffers, cached, exec, file, free, inactive, pinned, shared, slab, wired, used, pused (used, percentage), available, pavailable (available, percentage)</th>
<th>This item accepts three categories of parameters: 1) total - total amount of memory; 2) platform-specific memory types: active, anon, buffers, cached, exec, file, free, inactive, pinned, shared, slab, wired; 3) user-level estimates on how much memory is used and available: used, pused, available, pavailable.</th>
</tr>
</thead>
</table>

```
web.page.get[host, <path>, <port>]
```
<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get content of web page.</td>
<td>Web page source as text (including headers)</td>
</tr>
<tr>
<td><strong>host</strong> - hostname or (since 4.0.10) URL (as scheme://host, where only host is mandatory). Allowed URL schemes: http, https. Missing scheme will be treated as http. If URL is specified path and port must be empty. Specifying user name/password when connecting to servers that require authentication, for example: <a href="http://user:password@www.example.com">http://user:password@www.example.com</a> is only possible with cURL support. Punycode is supported in hostnames (since 4.0.10).</td>
<td>This item turns unsupported if the resource specified in host does not exist or is unavailable.</td>
</tr>
<tr>
<td><strong>port</strong> - port number</td>
<td>(default is 80 for HTTP)</td>
</tr>
</tbody>
</table>

web.page.get[host, <path>, <port>]
<table>
<thead>
<tr>
<th>Key</th>
<th>Float</th>
<th>This item turns unsupported if the resource specified in host does not exist or is unavailable.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loading time of full web page (in seconds).</td>
<td><strong>host</strong> - hostname or (since 4.0.10) URL (as scheme://host, where only host is mandatory). Allowed URL schemes: http, https. Missing scheme will be treated as http. If URL is specified path and port must be empty. Specifying user name/password when connecting to servers that require authentication, for example: <a href="http://user:password@www.example.com">http://user:password@www.example.com</a> is only possible with cURL support. Punycode is supported in hostnames (since 4.0.10). <strong>path</strong> - path to HTML document (default is /) <strong>port</strong> - port number (default is 80 for HTTP)</td>
<td></td>
</tr>
<tr>
<td><strong>port</strong></td>
<td><strong>path</strong></td>
<td><strong>length</strong></td>
</tr>
<tr>
<td>Key</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>host</td>
<td>hostname or domain name, IPv4 or IPv6 address. But for IPv6 address Zabbix agent must be compiled with IPv6 support enabled.</td>
<td></td>
</tr>
<tr>
<td>port</td>
<td>port number (default is 80 for HTTP)</td>
<td></td>
</tr>
<tr>
<td>regexp</td>
<td>regular expression describing the required pattern</td>
<td></td>
</tr>
<tr>
<td>length</td>
<td>maximum number of characters to return</td>
<td></td>
</tr>
<tr>
<td>output</td>
<td>an optional output formatting template. The \0 escape sequence is replaced with the matched part of text (from the first character where match begins until the end of the matched string).</td>
<td></td>
</tr>
<tr>
<td>path</td>
<td>path to HTML document (default is /)</td>
<td></td>
</tr>
<tr>
<td>content extraction</td>
<td>Content extraction using the output parameter is only possible with cURL support.</td>
<td></td>
</tr>
<tr>
<td>Punycode is supported in hostnames (since 4.0.10).</td>
<td>The output parameter is supported from version 2.2.</td>
<td></td>
</tr>
</tbody>
</table>

Example:
```
web.page.regexp[www.example.com, /index.php, 80, OK, 2]
web.page.regexp[https://www.example.com/index.php, 80, OK, 2]
```

This item turns unsupported if the resource specified in host does not exist or is unavailable.
<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>JSON object</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>zabbix.stats[&lt;ip&gt;,&lt;port&gt;]</td>
<td>Return a set of Zabbix server or proxy internal metrics remotely.</td>
<td>JSON object</td>
<td>Note that the stats request will only be accepted from the addresses listed in the 'StatsAllowedIP' server/proxy parameter on the target instance.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Footnotes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
</tbody>
</table>
if a device gets manually removed. Note also that these items, if using an update interval of 3 hours or more, will always return ‘0’.

3 *vfs.dev.read[], vfs.dev.write[]*: If default all is used for the first parameter then the key will return summary statistics, including all block devices like sda, sdb and their partitions (sda1, sda2, sdb3...) and multiple devices (MD raid) based on those block devices/partitions and logical volumes (LVM) based on those block devices/partitions. In such cases returned values should be considered only as relative value (dynamic in time) but not as absolute values.

4 **Perl Compatible Regular Expression (PCRE) since Zabbix 3.4; POSIX-extended regular expression before that. See also:** Regular expressions supported by location.

5 SSL (HTTPS) is supported only if agent is compiled with cURL support. Otherwise the item will turn unsupported.

Encoding settings

To make sure that the acquired data are not corrupted you may specify the correct encoding for processing the check (e.g. ’vfs.file.contents’) in the *encoding* parameter. The list of supported encodings (code page identifiers) may be found in documentation for *libiconv* (GNU Project) or in Microsoft Windows SDK documentation for “Code Page Identifiers”.

If no encoding is specified in the *encoding* parameter the following resolution strategies are applied:

- Standard resolution - UTF-8 is used in Unix/Linux (default in newer distributions); ANSI with a system-specific extension is used in Windows;
- BOM analysis - applicable for items ‘vfs.file.contents’, ‘vfs.file.regexp’, ‘vfs.file.regmatch’ since Zabbix 4.0.15. An attempt is made to determine the correct encoding by using the byte order mark (BOM) at the beginning of the file. If BOM is not present - standard resolution (see above) is applied instead.

Troubleshooting agent items

- If used with the passive agent, Timeout value in server configuration may need to be higher than Timeout in the agent configuration file. Otherwise the item may not get any value because the server request to agent timed out first.

Windows-specific item keys

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Return value</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>eventlog[name,&lt;regexp&gt;,&lt;severity&gt;,&lt;source&gt;,&lt;eventid&gt;,&lt;maxlines&gt;,&lt;mode&gt;]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key</td>
<td>Event log monitoring</td>
<td>Log</td>
<td>name - name of event log</td>
<td>The item must be configured as an active check.</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------------</td>
<td>-----</td>
<td>--------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>regexp - regular expression describing the required pattern</td>
<td>Examples:</td>
<td></td>
<td>=&gt; event-log[Application]</td>
<td></td>
</tr>
<tr>
<td>severity - regular expression describing severity</td>
<td>=&gt; event-log[Security,&quot;Failure Audit&quot;,^(529</td>
<td>680)$]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>This parameter accepts the following values:</td>
<td>=&gt; event-log[System,&quot;Warning</td>
<td>Error&quot;]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;Information&quot;, &quot;Warning&quot;, &quot;Error&quot;, &quot;Critical&quot;, &quot;Verbose&quot; (since Zabbix 2.2.0 running on Windows Vista or newer)</td>
<td>=&gt; event-log[System,^1$]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>source - regular expression describing source identifier (case-insensitive; regular expression is supported since Zabbix 2.2.0)</td>
<td>- here a custom regular expression named TWOSHORT is referenced (defined as a Result is TRUE type, the expression itself being ^1$|^70$).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>eventid - regular expression describing the event identifier(s)</td>
<td>Note that the agent is unable to send in events from the “Forwarded events” log.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>maxlines - maximum number of new lines per second the agent will send to Zabbix server or proxy. This parameter overrides the value of ‘MaxLinesPer-Second’ in zab-bix_agentd.conf</td>
<td>The mode parameter is supported since Zabbix 2.0.0. “Windows Eventing 6.0” is supported since Zabbix 2.2.0.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mode - possible values: all (default), skip - skip processing of older data (affect only newly created items). Item must be configured as an active check.</td>
<td>Note that selecting a non-Log type of information for this item will lead to the loss of local timestamp, as well as log severity and source information.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

See also additional information on log monitoring.
<table>
<thead>
<tr>
<th>Key</th>
<th>Network interface list (includes interface type, status, IPv4 address, description).</th>
<th>Supported since Zabbix agent version 1.8.1. Multi-byte interface names supported since Zabbix agent version 1.8.6. Disabled interfaces are not listed.</th>
</tr>
</thead>
</table>
| perf_counter[counter,<interval>] | Note that enabling/disabling some components may change their ordering in the Windows interface name. Some Windows versions (for example, Server 2008) might require the latest updates installed to support non-ASCII characters in interface names.
### perf_counter_en[counter, <interval>]  

- **Value of any Windows performance counter in English.**
- **counter** - path to the counter
- **interval** - last N seconds for storing the average value.
- The interval must be between 1 and 900 seconds (included) and the default value is 1.
- **Performance Monitor** can be used to obtain list of available counters. Until version 1.6 this parameter will return correct value only for counters that require just one sample (like System\Threads). It will not work as expected for counters that require more than one sample - like CPU utilization. Since 1.6, interval is used, so the check returns an average value for last "interval" seconds every time.

**See also:**
- **Windows performance counters.**

This item is only supported on **Windows Server 2008/Vista** and above.

You can find the list of English strings by viewing the following registry key:
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\009`

Supported since Zabbix agent version 4.0.13.

### proc_info[process, <attribute>, <type>]  

- Value of any Windows performance counter in English.
- **counter** - path to the counter in English
- **interval** - last N seconds for storing the average value.
- The interval must be between 1 and 900 seconds (included) and the default value is 1.

This item is only supported on **Windows Server 2008/Vista** and above.
<table>
<thead>
<tr>
<th>Key</th>
<th>Float</th>
<th>The following attributes are supported:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>process - process name</td>
<td>attribute - requested process attribute</td>
<td>vmsize (default) - size of process virtual memory in Kbytes</td>
<td></td>
</tr>
<tr>
<td>type - representation type</td>
<td>(meaningful when more than one process with the same name exists)</td>
<td>wkset - size of process working set (amount of physical memory used by process) in Kbytes</td>
<td></td>
</tr>
<tr>
<td>io_read_b - number of bytes read by process during I/O operations</td>
<td>io_read_op - number of read operation performed by process</td>
<td>pf - number of page faults</td>
<td></td>
</tr>
<tr>
<td>io_write_b - number of bytes written by process during I/O operations</td>
<td>io_write_op - number of write operation performed by process</td>
<td>ktime - process kernel time in milliseconds</td>
<td></td>
</tr>
<tr>
<td>io_other_b - number of bytes transferred by process during operations other than read and write operations</td>
<td>io_other_op - number of I/O operations performed by process, other than read and write operations</td>
<td>utime - process user time in milliseconds</td>
<td></td>
</tr>
<tr>
<td>gdiobj - number of GDI objects used</td>
<td>userobj - number of USER objects used</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Examples:

- `=]proc_info[iexplore.exe, wkset, sum]` - to get the amount of physical memory taken by all Internet Explorer processes
- `=]proc_info[iexplore.exe, pf, avg]` - to get the average number of page faults for Internet Explorer processes

Note: `io_*`, `gdiobj`, and `userobj` attributes are available only on Windows 2000 and later versions of Windows, not on Windows NT 4.0.
<table>
<thead>
<tr>
<th>key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>service.discovery</td>
<td>List of Windows services. Used for low-level discovery.</td>
</tr>
<tr>
<td>service.info[service,&lt;param&gt;]</td>
<td>Information about a service. Integer - with param as state, startup String - with param as displayname, path, user Text - with param as description Specifically for state: 0 - running, 1 - paused, 2 - start pending, 3 - pause pending, 4 - continue pending, 5 - stop pending, 6 - stopped, 7 - unknown, 255 - no such service Specifically for startup: 0 - automatic, 1 - automatic delayed, 2 - manual, 3 - disabled, 4 - unknown, 5 - automatic trigger start, 6 - automatic delayed trigger start, 7 - manual trigger start</td>
</tr>
<tr>
<td>services[&lt;type&gt;,&lt;state&gt;,&lt;exclude&gt;]</td>
<td>Supported since Zabbix agent version 3.0.</td>
</tr>
</tbody>
</table>

Examples:

- `=> service.info[SNMPTRAP]` - state of the SNMPTrap service
- `=> service.info[SNMP Trap]` - state of the same service, but with display name specified
- `=> service.info[EventLog,startup]` - startup type of the EventLog service

Items `service.info[service,state]` and `service.info[service]` will return the same information.

Note that only with param as state this item returns a value for non-existing services (255).

This item is supported since Zabbix 3.0.0. It should be used instead of the deprecated `service_state[service]` item.
Listing of services.

Text - list of services separated by a newline

- **type** - all (default), automatic, manual or disabled
- **state** - all (default), stopped, started, start_pending, stop_pending, running, continue_pending, pause_pending or paused
- **exclude** - services to exclude from the result. Excluded services should be listed in double quotes, separated by comma, without spaces.

**Examples:**

- `services[started]`
- `services[automatic, stopped]`
- `services[automatic, stopped, 'service1,service2,service3']`

This key is supported since Zabbix 1.8.1.

**wmi.get[<namespace>,<query>]**

Execute WMI query and return the first selected object.

- **namespace** - WMI namespace
- **query** - WMI query returning a single object

**Example:**

```
=> wmi.get[root\cimv2,select status from Win32_DiskDrive where Name like '%PHYSICALDRIVE0%']
```

- returns the status of the first physical disk.

This key is supported since Zabbix 2.2.0.

**vm.vmemory.size[<type>]**
Monitoring Windows services

This tutorial provides step-by-step instructions for setting up the monitoring of Windows services. It is assumed that Zabbix server and agent are configured and operational.

Step 1

Get the service name.

You can get that name by going to MMC Services snap-in and bringing up the properties of the service. In the General tab you should see a field called ‘Service name’. The value that follows is the name you will use when setting up an item for monitoring.

For example, if you wanted to monitor the “workstation” service then your service might be: lanmanworkstation.

Step 2

Configure an item for monitoring the service.

The item service.info[service,<param>] retrieves the information about a particular service. Depending on the information you need, specify the param option which accepts the following values: displayname, state, path, user, startup or description. The default value is state if param is not specified (service.info[service]).

The type of return value depends on chosen param: integer for state and startup; character string for displayname, path and user; text for description.

Example:

• Key: service.info[lanmanworkstation]
• Type of information: Numeric (unsigned)
• Show value: select the Windows service state value mapping

Two value maps are available Windows service state and Windows service startup type to map a numerical value to a text representation in the Frontend.

Discovery of Windows services

Low-level discovery provides a way to automatically create items, triggers, and graphs for different entities on a computer. Zabbix can automatically start monitoring Windows services on your machine, without the need to know the exact name of a service or create items for each service manually. A filter can be used to generate real items, triggers, and graphs only for services of interest.

2 SNMP agent

Overview

You may want to use SNMP monitoring on devices such as printers, network switches, routers or UPS that usually are SNMP-enabled and on which it would be impractical to attempt setting up complete operating systems and Zabbix agents.

To be able to retrieve data provided by SNMP agents on these devices, Zabbix server must be initially configured with SNMP support.

SNMP checks are performed over the UDP protocol only.

Zabbix server and proxy daemons query SNMP devices for multiple values in a single request. This affects all kinds of SNMP items (regular SNMP items, SNMP items with dynamic indexes, and SNMP low-level discovery) and should make SNMP processing much more efficient. See the bulk processing section for technical details on how it works internally. Bulk requests can also be disabled for devices that cannot handle them properly using the "Use bulk requests" setting for each interface.

Zabbix server and proxy daemons log lines similar to the following if they receive an incorrect SNMP response:

SNMP response from host "gateway" does not contain all of the requested variable bindings

While they do not cover all the problematic cases, they are useful for identifying individual SNMP devices for which bulk requests should be disabled.

Zabbix server/proxy will always retry at least one time after an unsuccessful query attempt: either through the SNMP library’s retrying mechanism or through the internal bulk processing mechanism.

Warning: If monitoring SNMPv3 devices, make sure that msgAuthoritativeEngineID (also known as snmpEngineID or “Engine ID”) is never shared by two devices. According to RFC 2571 (section 3.1.1.1) it must be unique for each device.

Configuring SNMP monitoring

To start monitoring a device through SNMP, the following steps have to be performed:

Step 1

Create a host for the device with an SNMP interface.

Enter the IP address/DNS name and port number. You can use one of the provided SNMP templates (Template SNMP Device and others) that will automatically add a set of items. However, the template may not be compatible with the host. Click on Add to save the host.

Step 2

Find out the SNMP string (or OID) of the item you want to monitor.

To get a list of SNMP strings, use the snmpwalk command (part of net-snmp software which you should have installed as part of the Zabbix installation) or equivalent tool:

shell> snmpwalk -v 2c -c public <host IP> .

As ’2c’ here stands for SNMP version, you may also substitute it with ’1’, to indicate SNMP Version 1 on the device.

This should give you a list of SNMP strings and their last value. If it doesn’t then it is possible that the SNMP ‘community’ is different from the standard ‘public’ in which case you will need to find out what it is.

You can then go through the list until you find the string you want to monitor, e.g. if you wanted to monitor the bytes coming in to your switch on port 3 you would use the IF-MIB::ifInOctets.3 string from this line:

IF-MIB::ifInOctets.3 = Counter32: 3409739121

You may now use the snmpget command to find out the numeric OID for ‘IF-MIB::ifInOctets.3’:
shell> snmpget -v 2c -c public -On 10.62.1.22 IF-MIB::ifInOctets.3

Note that the last number in the string is the port number you are looking to monitor. See also: Dynamic indexes.

This should give you something like the following:

.1.3.6.1.2.1.2.2.1.10.3 = Counter32: 3472126941

Again, the last number in the OID is the port number.

Note:
3COM seem to use port numbers in the hundreds, e.g. port 1 = port 101, port 3 = port 103, but Cisco use regular numbers, e.g. port 3 = 3.

Note:
Some of the most used SNMP OIDs are translated automatically to a numeric representation by Zabbix.

In the last example above value type is “Counter32”, which internally corresponds to ASN_COUNTER type. The full list of supported types is ASN_COUNTER, ASN_COUNTER64, ASN_UINT64, ASN_UNSIGNED64, ASN_INTEGER, ASN_INTEGER64, ASN_FLOAT, ASN_DOUBLE, ASN_TIMETICKS, ASN_GAUGE, ASN_IPADDRESS, ASN_OCTET_STR and ASN_OBJECT_ID (since 2.2.8, 2.4.3). These types roughly correspond to “Counter32”, “Counter64”, “UInteger32”, “INTEGER”, “Float”, “Double”, “Timeticks”, “Gauge32”, “IpAddress”, “OCTETSTRING”, “OBJECT IDENTIFIER” in \texttt{snmpget} output, but might also be shown as “STRING”, “Hex-STRING”, “OID” and other, depending on the presence of a display hint.

Step 3
Create an item for monitoring.

So, now go back to Zabbix and click on Items for the SNMP host you created earlier. Depending on whether you used a template or not when creating your host, you will have either a list of SNMP items associated with your host or just an empty list. We will work on the assumption that you are going to create the item yourself using the information you have just gathered using snmpwalk and snmpget, so click on Create item. In the new item form, enter the item ‘Name’. Make sure the ‘Host interface’ field has your switch/router in it and change the ‘Type’ field to “SNMPv* agent”. Enter the community (usually public) and enter the textual or numeric OID that you retrieved earlier into the ‘SNMP OID’ field, for example: .1.3.6.1.2.1.2.1.10.3

Enter the SNMP ‘Port’ as 161 and the ‘Key’ as something meaningful, e.g. SNMP-InOctets-Bps. Set the ‘Type of information’ to Numeric (float) and the preprocessing step as Change per second (important, otherwise you will get cumulative values from the SNMP device instead of the latest change). Choose a custom multiplier if you want one and enter an ‘Update interval’ and ‘History storage period’ if you want them to be different from the default.
All mandatory input fields are marked with a red asterisk.

Now save the item and go to Monitoring → Latest data for your SNMP data!

Take note of specific options available for SNMPv3 items:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Context name</td>
<td>Enter context name to identify item on SNMP subnet. Context name is supported for SNMPv3 items since Zabbix 2.2. User macros are resolved in this field.</td>
</tr>
<tr>
<td>Security name</td>
<td>Enter security name. User macros are resolved in this field.</td>
</tr>
<tr>
<td>Security level</td>
<td>Select security level: &lt;br&gt;<strong>noAuthNoPriv</strong> - no authentication nor privacy protocols are used &lt;br&gt;<strong>AuthNoPriv</strong> - authentication protocol is used, privacy protocol is not &lt;br&gt;<strong>AuthPriv</strong> - both authentication and privacy protocols are used</td>
</tr>
<tr>
<td>Authentication protocol</td>
<td>Select authentication protocol - MD5 or SHA.</td>
</tr>
<tr>
<td>Authentication passphrase</td>
<td>Enter authentication passphrase. User macros are resolved in this field.</td>
</tr>
<tr>
<td>Privacy protocol</td>
<td></td>
</tr>
<tr>
<td>Privacy passphrase</td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td></td>
</tr>
<tr>
<td>Type of information</td>
<td></td>
</tr>
</tbody>
</table>

Parameter Description

- Context name: Enter context name to identify item on SNMP subnet. Context name is supported for SNMPv3 items since Zabbix 2.2. User macros are resolved in this field.
- Security name: Enter security name. User macros are resolved in this field.
- Security level: Select security level:
  - noAuthNoPriv - no authentication nor privacy protocols are used
  - AuthNoPriv - authentication protocol is used, privacy protocol is not
  - AuthPriv - both authentication and privacy protocols are used
- Authentication protocol: Select authentication protocol - MD5 or SHA.
- Authentication passphrase: Enter authentication passphrase. User macros are resolved in this field.
In case of wrong SNMPv3 credentials (security name, authentication protocol/passphrase, privacy protocol) Zabbix receives an ERROR from net-snmp, except for wrong Privacy passphrase in which case Zabbix receives a TIMEOUT error from net-snmp.

**Warning:**
Server/proxy restart is required for changes in Authentication protocol, Authentication passphrase, Privacy protocol or Privacy passphrase to take effect, if the Security name is not changed at the same time. In cases, where Security name is also changed, all parameters will be updated immediately.

---

### Example 1

#### General example:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Community</strong></td>
<td>public</td>
</tr>
<tr>
<td><strong>OID</strong></td>
<td>1.2.3.45.6.7.8.0 (or .1.2.3.45.6.7.8.0)</td>
</tr>
<tr>
<td><strong>Key</strong></td>
<td>&lt;Unique string to be used as reference to triggers&gt; For example, &quot;my_param&quot;.</td>
</tr>
</tbody>
</table>

Note that OID can be given in either numeric or string form. However, in some cases, string OID must be converted to numeric representation. Utility snmpget may be used for this purpose:

```shell
shell> snmpget -On localhost public enterprises.ucdavis.memory.memTotalSwap.0
```

Monitoring of SNMP parameters is possible if --with-net-snmp flag was specified while configuring Zabbix sources.

#### Example 2

Monitoring of uptime:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Community</strong></td>
<td>public</td>
</tr>
<tr>
<td><strong>OID</strong></td>
<td>MIB::sysUpTime.0</td>
</tr>
<tr>
<td><strong>Key</strong></td>
<td>router uptime</td>
</tr>
<tr>
<td><strong>Value type</strong></td>
<td>Float</td>
</tr>
<tr>
<td><strong>Units</strong></td>
<td>uptime</td>
</tr>
<tr>
<td><strong>Multiplier</strong></td>
<td>0.01</td>
</tr>
</tbody>
</table>

---

### Internal workings of bulk processing

Starting from 2.2.3 Zabbix server and proxy query SNMP devices for multiple values in a single request. This affects several types of SNMP items:

- regular SNMP items;
- SNMP items with dynamic indexes;
- SNMP low-level discovery rules.

All SNMP items on a single interface with identical parameters are scheduled to be queried at the same time. The first two types of items are taken by pollers in batches of at most 128 items, whereas low-level discovery rules are processed individually, as before.

On the lower level, there are two kinds of operations performed for querying values: getting multiple specified objects and walking an OID tree.

For "getting", a GetRequest-PDU is used with at most 128 variable bindings. For "walking", a GetNextRequest-PDU is used for SNMPv1 and GetBulkRequest with "max-repetitions" field of at most 128 is used for SNMPv2 and SNMPv3.

Thus, the benefits of bulk processing for each SNMP item type are outlined below:

- regular SNMP items benefit from "getting" improvements;
- SNMP items with dynamic indexes benefit from both "getting" and "walking" improvements: "getting" is used for index verification and "walking" for building the cache;
• SNMP low-level discovery rules benefit from “walking” improvements.

However, there is a technical issue that not all devices are capable of returning 128 values per request. Some always return a proper response, but others either respond with a “tooBig(1)” error or do not respond at all once the potential response is over a certain limit.

In order to find an optimal number of objects to query for a given device, Zabbix uses the following strategy. It starts cautiously with querying 1 value in a request. If that is successful, it queries 2 values in a request. If that is successful again, it queries 3 values in a request and continues similarly by multiplying the number of queried objects by 1.5, resulting in the following sequence of request sizes: 1, 2, 3, 4, 6, 9, 13, 19, 28, 42, 63, 94, 128.

However, once a device refuses to give a proper response (for example, for 42 variables), Zabbix does two things.

First, for the current item batch it halves the number of objects in a single request and queries 21 variables. If the device is alive, then the query should work in the vast majority of cases, because 28 variables were known to work and 21 is significantly less than that. However, if that still fails, then Zabbix falls back to querying values one by one. If it still fails at this point, then the device is definitely not responding and request size is not an issue.

The second thing Zabbix does for subsequent item batches is it starts with the last successful number of variables (28 in our example) and continues incrementing request sizes by 1 until the limit is hit. For example, assuming the largest response size is 32 variables, the subsequent requests will be of sizes 29, 30, 31, 32, and 33. The last request will fail and Zabbix will never issue a request of size 33 again. From that point on, Zabbix will query at most 32 variables for this device.

If large queries fail with this number of variables, it can mean one of two things. The exact criteria that a device uses for limiting response size cannot be known, but we try to approximate that using the number of variables. So the first possibility is that this number of variables is around the device’s actual response size limit in the general case: sometimes response is less than the limit, sometimes it is greater than that. The second possibility is that a UDP packet in either direction simply got lost. For these reasons, if Zabbix gets a failed query, it reduces the maximum number of variables to try to get deeper into the device’s comfortable range, but (starting from 2.2.8) only up to two times.

In the example above, if a query with 32 variables happens to fail, Zabbix will reduce the count to 31. If that happens to fail, too, Zabbix will reduce the count to 30. However, Zabbix will not reduce the count below 30, because it will assume that further failures are due to UDP packets getting lost, rather than the device’s limit.

If, however, a device cannot handle bulk requests properly for other reasons and the heuristic described above does not work, since Zabbix 2.4 there is a “Use bulk requests” setting for each interface that allows to disable bulk requests for that device.

1 Dynamic indexes

Overview

While you may find the required index number (for example, of a network interface) among the SNMP OIDs, sometimes you may not completely rely on the index number always staying the same.

Index numbers may be dynamic - they may change over time and your item may stop working as a consequence.

To avoid this scenario, it is possible to define an OID which takes into account the possibility of an index number changing.

For example, if you need to retrieve the index value to append to ifInOctets that corresponds to the GigabitEthernet0/1 interface on a Cisco device, use the following OID:

```
ifInOctets["index","ifDescr","GigabitEthernet0/1"]
```

The syntax

A special syntax for OID is used:

```
<OID of data>["index","<base OID of index>"","<string to search for>"]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID of data index</td>
<td>Main OID to use for data retrieval on the item. Method of processing. Currently one method is supported: index – search for index and append it to the data OID</td>
</tr>
<tr>
<td>base OID of index</td>
<td>This OID will be looked up to get the index value corresponding to the string.</td>
</tr>
<tr>
<td>string to search for</td>
<td>The string to use for an exact match with a value when doing lookup. Case sensitive.</td>
</tr>
</tbody>
</table>
Example

Getting memory usage of apache process.

If using this OID syntax:

```
HOST-RESOURCES-MIB::hrSWRunPerfMem["index","HOST-RESOURCES-MIB::hrSWRunPath","/usr/sbin/apache2"]
```

the index number will be looked up here:

```
... 
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"
...
```

Now we have the index, 5388. The index will be appended to the data OID in order to receive the value we are interested in:

```
HOST-RESOURCES-MIB::hrSWRunPerfMem.5388 = INTEGER: 31468 KBytes
```

**Index lookup caching**

When a dynamic index item is requested, Zabbix retrieves and caches whole SNMP table under base OID for index, even if a match would be found sooner. This is done in case another item would refer to the same base OID later - Zabbix would look up index in the cache, instead of querying the monitored host again. Note that each poller process uses separate cache.

In all subsequent value retrieval operations only the found index is verified. If it has not changed, value is requested. If it has changed, cache is rebuilt - each poller that encounters a changed index walks the index SNMP table again.

**2 Special OIDs**

Some of the most used SNMP OIDs are translated automatically to a numeric representation by Zabbix. For example, `ifIndex` is translated to `1.3.6.1.2.1.2.2.1.1`. `ifIndex.0` is translated to `1.3.6.1.2.1.2.2.1.1.0`.

The table contains list of the special OIDs.

<table>
<thead>
<tr>
<th>Special OID</th>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ifIndex</td>
<td>1.3.6.1.2.1.2.2.1.1</td>
<td>A unique value for each interface.</td>
</tr>
<tr>
<td>ifDescr</td>
<td>1.3.6.1.2.1.2.2.1.2</td>
<td>A textual string containing information about the interface. This string should include the name of the manufacturer, the product name and the version of the hardware interface.</td>
</tr>
<tr>
<td>ifType</td>
<td>1.3.6.1.2.1.2.2.1.3</td>
<td>The type of interface, distinguished according to the physical/link protocol(s) immediately 'below' the network layer in the protocol stack.</td>
</tr>
<tr>
<td>ifMtu</td>
<td>1.3.6.1.2.1.2.2.1.4</td>
<td>The size of the largest datagram which can be sent / received on the interface, specified in octets.</td>
</tr>
<tr>
<td>ifSpeed</td>
<td>1.3.6.1.2.1.2.2.1.5</td>
<td>An estimate of the interface's current bandwidth in bits per second.</td>
</tr>
<tr>
<td>ifPhysAddress</td>
<td>1.3.6.1.2.1.2.2.1.6</td>
<td>The interface's address at the protocol layer immediately 'below' the network layer in the protocol stack.</td>
</tr>
<tr>
<td>ifAdminStatus</td>
<td>1.3.6.1.2.1.2.2.1.7</td>
<td>The current administrative state of the interface.</td>
</tr>
<tr>
<td>ifOperStatus</td>
<td>1.3.6.1.2.1.2.2.1.8</td>
<td>The current operational state of the interface.</td>
</tr>
<tr>
<td>ifInOctets</td>
<td>1.3.6.1.2.1.2.2.1.10</td>
<td>The total number of octets received on the interface, including framing characters.</td>
</tr>
<tr>
<td>ifInUcastPkts</td>
<td>1.3.6.1.2.1.2.2.1.11</td>
<td>The number of subnetwork-unicast packets delivered to a higher-layer protocol.</td>
</tr>
<tr>
<td>Special OID</td>
<td>Identifier</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ifInNUcastPkts</td>
<td>1.3.6.1.2.1.2.1.12</td>
<td>The number of non-unicast (i.e., subnetwork-broadcast or subnetwork-multicast) packets delivered to a higher-layer protocol.</td>
</tr>
<tr>
<td>ifInDiscards</td>
<td>1.3.6.1.2.1.2.1.13</td>
<td>The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.</td>
</tr>
<tr>
<td>ifInErrors</td>
<td>1.3.6.1.2.1.2.1.14</td>
<td>The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.</td>
</tr>
<tr>
<td>ifInUnknownProtos</td>
<td>1.3.6.1.2.1.2.1.15</td>
<td>The number of packets received via the interface which were discarded because of an unknown or unsupported protocol.</td>
</tr>
<tr>
<td>ifOutOctets</td>
<td>1.3.6.1.2.1.2.2.1.16</td>
<td>The total number of octets transmitted out of the interface, including framing characters.</td>
</tr>
<tr>
<td>ifOutUcastPkts</td>
<td>1.3.6.1.2.1.2.2.1.17</td>
<td>The total number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent.</td>
</tr>
<tr>
<td>ifOutNUcastPkts</td>
<td>1.3.6.1.2.1.2.2.1.18</td>
<td>The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent.</td>
</tr>
<tr>
<td>ifOutDiscards</td>
<td>1.3.6.1.2.1.2.2.1.19</td>
<td>The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.</td>
</tr>
<tr>
<td>ifOutErrors</td>
<td>1.3.6.1.2.1.2.2.1.20</td>
<td>The number of outbound packets that could not be transmitted because of errors.</td>
</tr>
<tr>
<td>ifOutQLen</td>
<td>1.3.6.1.2.1.2.2.1.21</td>
<td>The length of the output packet queue (in packets).</td>
</tr>
</tbody>
</table>

3 MIB files

Introduction

MIB stands for a Management Information Base. MIB files allow you to use textual representation of the OID (Object Identifier).

For example,

ifHCOutOctets

is textual representation of OID

1.3.6.1.2.1.31.1.1.1.10

You can use either, when monitoring SNMP devices with Zabbix, but if you feel more comfortable when using textual representation you have to install MIB files.
Installing MIB files

On Debian-based systems:

# apt install snmp-mibs-downloader
# download-mibs

On RedHat-based systems:

# yum install net-snmp-libs

Enabling MIB files

On RedHat-based systems the mib files should be enabled by default. On Debian-based systems you have to edit file /etc/snmp/snmp.conf and comment out the line that says mibs:

# As the snmp packages come without MIB files due to license reasons, loading # of MIBs is disabled by default. If you added the MIBs you can re-enable # loading them by commenting out the following line.
#mibs:

Testing MIB files

Testing snmp MIBs can be done using snmpwalk utility. If you don’t have it installed, use the following instructions.

On Debian-based systems:

# apt install snmp

On RedHat-based systems:

# yum install net-snmp-utils

After that, the following command must not give error when you query a network device:

$ 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
[...]

Used options:

-v 2c  use SNMP protocol version 2c

Using MIBs in Zabbix

The most important to keep in mind is that Zabbix processes do not get informed of the changes made to MIB files. So after every change you must restart Zabbix server or proxy, e. g.:

# service zabbix-server restart

After that, the changes made to MIB files are in effect.

Using custom MIB files

There are standard MIB files coming with every GNU/Linux distribution. But some device vendors provide their own.

Let’s say, you would like to use CISCO-SMI MIB file. The following instructions will download and install it:

# 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/local/share/snmp/mibs" >> /etc/snmp/snmp.conf
# cp /tmp/CISCO-SMI.my /usr/local/share/snmp/mibs

Now you should be able to use it. Try to translate the name of the object ciscoProducts from the MIB file to OID:

# snmptranslate -IR -On CISCO-SMI::ciscoProducts
.1.3.6.1.4.1.9.1
3 SNMPtraps

Overview

Receiving SNMP traps is the opposite to querying SNMP-enabled devices.

In this case, the information is sent from a SNMP-enabled device and is collected or “trapped” by Zabbix.

Usually, traps are sent upon some condition change and the agent connects to the server on port 162 (as opposed to port 161 on the agent side that is used for queries). Using traps may detect some short problems that occur amidst the query interval and may be missed by the query data.

Receiving SNMP traps in Zabbix is designed to work with `snmptrapd` and one of the built-in mechanisms for passing the traps to Zabbix - either a perl script or `SNMPTT`.

The workflow of receiving a trap:

1. `snmptrapd` receives a trap
2. `snmptrapd` passes the trap to `SNMPTT` or calls Perl trap receiver
3. `SNMPTT` or Perl trap receiver parses, formats and writes the trap to a file
4. Zabbix SNMP trapper reads and parses the trap file
5. For each trap, Zabbix finds all “SNMP trapper” items with host interfaces matching the received trap address. Note that only the selected “IP” or “DNS” in host interface is used during the matching.
6. For each found item, the trap is compared to regexp in "snmptrap[regexp]". The trap is set as the value of all matched items. If no matching item is found and there is an “snmptrap.fallback” item, the trap is set as the value of that.
7. If the trap was not set as the value of any item, Zabbix by default logs the unmatched trap. (This is configured by “Log unmatched SNMP traps” in Administration → General → Other.)

1 Configuring SNMP traps

Configuring the following fields in the frontend is specific for this item type:

- Your host must have an SNMP interface

In Configuration → Hosts, in the Host interface field set an SNMP interface with the correct IP or DNS address. The address from each received trap is compared to the IP and DNS addresses of all SNMP interfaces to find the corresponding hosts.

- Configure the item

In the Key field use one of the SNMP trap keys:

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Return value</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>snmptrap[regexp]</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Key

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>SNMP trap</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catches all SNMP traps that match the <em>regular expression</em> specified in <code>regexp</code>. If <code>regexp</code> is unspecified, catches any trap.</td>
<td>This item can be set only for SNMP interfaces. This item is supported since Zabbix 2.0.0. Note: Starting with Zabbix 2.0.5, user macros and global regular expressions are supported in the parameter of this item key.</td>
<td>SNMPtrap fallback</td>
</tr>
<tr>
<td>snmptrap.fallback</td>
<td>Catches all SNMP traps that were not caught by any of the snmptrap[] items for that interface.</td>
<td>This item can be set only for SNMP interfaces. This item is supported since Zabbix 2.0.0.</td>
</tr>
</tbody>
</table>

**Note:**
Multiline regexp matching is not supported at this time.

Set the **Type of information** to be ‘Log’ for the timestamps to be parsed. Note that other formats such as ‘Numeric’ are also acceptable but might require a custom trap handler.

**Note:**
For SNMP trap monitoring to work, it must first be correctly set up.

---

### 2 Setting up SNMP trap monitoring

#### Configuring Zabbix server/proxy

To read the traps, Zabbix server or proxy must be configured to start the SNMP trapper process and point to the trap file that is being written by SNMPTT or a perl trap receiver. To do that, edit the configuration file (`zabbix_server.conf` or `zabbix_proxy.conf`):

- `StartSNMPTrapper=1`
- `SNMPTrapperFile=[TRAP FILE]

**Warning:**
If systemd parameter `PrivateTmp` is used, this file is unlikely to work in /tmp.

#### Configuring SNMPTT

At first, snmptrapd should be configured to use SNMPTT.

**Note:**
For the best performance, SNMPTT should be configured as a daemon using `snmpthandler-embedded` to pass the traps to it. See instructions for configuring SNMPTT in its homepage: http://snmptt.sourceforge.net/docs/snmptt.shtml

When SNMPTT is configured to receive the traps, configure `snmptt.ini`:

1. enable the use of the Perl module from the NET-SNMP package:
   ```
   net_snmp_perl_enable = 1
   ```

2. log traps to the trap file which will be read by Zabbix:
   ```
   log_enable = 1
   log_file = [TRAP FILE]
   ```

3. set the date-time format:
Warning:
The "net-snmp-perl" package has been removed in RHEL/CentOS 8.0-8.2; re-added in RHEL 8.3. For more information, see the known issues.

Now format the traps for Zabbix to recognize them (edit snmptt.conf):

1. Each FORMAT statement should start with "ZBXTRAP [address]", where [address] will be compared to IP and DNS addresses of SNMP interfaces on Zabbix. E.g.:

   EVENT coldStart .1.3.6.1.6.3.1.1.5.1 "Status Events" Normal
   FORMAT ZBXTRAP $aA Device reinitialized (coldStart)

2. See more about SNMP trap format below.

Attention:
Do not use unknown traps - Zabbix will not be able to recognize them. Unknown traps can be handled by defining a general event in snmptt.conf:

   EVENT general .* "General event" Normal

Configuring Perl trap receiver

Requirements: Perl, Net-SNMP compiled with --enable-embedded-perl (done by default since Net-SNMP 5.4)

Perl trap receiver (look for misc/snmptrap/zabbix_trap_receiver.pl) can be used to pass traps to Zabbix server directly from snmptrapd. To configure it:

- add the perl script to snmptrapd configuration file (snmptrapd.conf), e.g.:

  perl do "[FULL PATH TO PERL RECEIVER SCRIPT]";

- configure the receiver, e.g:

  $SNMPTrapperFile = '[TRAP FILE]';
  $DateTimeFormat = '[DATE TIME FORMAT]';

Note:
If script name is not quoted, snmptrapd will refuse to start up with messages, similar to these:<br><br>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

Warning:
net-snmp agent does not support AES256 with SNMPv3/USM.

SNMP trap format

All customized Perl trap receivers and SNMPTT trap configuration must format the trap in the following way:

[timestamp] [the trap, part 1] ZBXTRAP [address] [the trap, part 2]

where

- [timestamp] - timestamp used for log items
- ZBXTRAP - header that indicates that a new trap starts in this line
- [address] - IP address used to find the host for this trap

Note that "ZBXTRAP" and "[address]" will be cut out from the message during processing. If the trap is formatted otherwise, Zabbix might parse the traps unexpectedly.

Example trap:

11:30:15 2011/07/27 .1.3.6.1.6.3.1.1.5.3 Normal "Status Events" localhost - ZBXTRAP 192.168.1.1 Link down

This will result in the following trap for SNMP interface with IP=192.168.1.1:
3 System requirements

Large file support

Zabbix has "Large file support" for SNMP trapper files. The maximum file size that Zabbix can read is 2^63 (8 EiB). Note that the filesystem may impose a lower limit on the file size.

Log rotation

Zabbix does not provide any log rotation system - that should be handled by the user. The log rotation should first rename the old file and only later delete it so that no traps are lost:

1. Zabbix opens the trap file at the last known location and goes to step 3
2. Zabbix checks if the currently opened file has been rotated by comparing the inode number to the define trap file's inode number. If there is no opened file, Zabbix resets the last location and goes to step 1.
3. Zabbix reads the data from the currently opened file and sets the new location.
4. The new data are parsed. If this was the rotated file, the file is closed and goes back to step 2.
5. If there was no new data, Zabbix sleeps for 1 second and goes back to step 2.

Filesystem

Because of the trap file implementation, Zabbix needs the filesystem to support inodes to differentiate files (the information is acquired by a stat() call).

4 Setup example

This example uses snmptrapd + SMPTT to pass traps to Zabbix server. Setup:

1. **zabbix_server.conf** - configure Zabbix to start SNMP trapper and set the trap file:

   ```
   StartSNMPTrapper=1
   SNMPTrapperFile=/tmp/my_zabbix_traps.tmp
   ```

2. **snmptrapd.conf** - add SMPTT as the trap handler:

   ```
   traphandle default smppt
   ```

3. **snmp.ini** - enable the use of the Perl module from the NET-SNMP package:

   ```
   net_snmp_perl_enable = 1
   ```

   configure output file and time format:

   ```
   log_file = /tmp/my_zabbix_traps.tmp
   date_time_format = %H:%M:%S %Y/%m/%d
   ```

4. **snmp.conf** - define a default trap format:

   ```
   EVENT general .* "General event" Normal
   FORMAT ZBXTRAP $aA $ar
   ```

5. Create an SNMP item TEST:

   ```
   Host's SNMP interface IP: 127.0.0.1
   Key: snmptrap["General"]
   Log time format: hh:mm:ss yyyy/MM/dd
   ```

   This results in:

   1. Command used to send a trap:

   ```
   snmptrap -v 1 -c public 127.0.0.1 .'1.3.6.1.6.3.1.1.5.3' '0.0.0.0' 6 33 '55' .1.3.6.1.6.3.1.1.5.3 s "teststring000"
   ```

   2. The received trap:

   ```
   15:48:18 2011/07/26 .1.3.6.1.6.3.1.1.5.3.0.33 Normal "General event"
   localhost - ZBXTRAP 127.0.0.1 127.0.0.1
   ```
3. Value for item TEST:
15:48:18 2011/07/26 .1.3.6.1.6.3.1.1.5.3.0.33 Normal "General event"
localhost - 127.0.0.1

**Note:**
This simple example uses SNMP TT as traphandle. For better performance on production systems, use embedded Perl to pass traps from snmptrapd to SNMP TT or directly to Zabbix.

See also
- Zabbix blog article on SNMP traps

4 IPMI checks

Overview
You can monitor the health and availability of Intelligent Platform Management Interface (IPMI) devices in Zabbix. To perform IPMI checks Zabbix server must be initially configured with IPMI support.

IPMI is a standardized interface for remote "lights-out" or "out-of-band" management of computer systems. It allows to monitor hardware status directly from the so-called "out-of-band" management cards, independently from the operating system or whether the machine is powered on at all.

Zabbix IPMI monitoring works only for devices having IPMI support (HP iLO, DELL DRAC, IBM RSA, Sun SSP, etc).

Since Zabbix 3.4, a new IPMI manager process has been added to schedule IPMI checks by IPMI pollers. Now a host is always polled by only one IPMI poller at a time, reducing the number of open connections to BMC controllers. With those changes it’s safe to increase the number of IPMI pollers without worrying about BMC controller overloading. The IPMI manager process is automatically started when at least one IPMI poller is started.

See also known issues for IPMI checks.

Configuration

Host configuration
A host must be configured to process IPMI checks. An IPMI interface must be added, with the respective IP and port numbers, and IPMI authentication parameters must be defined.

See the configuration of hosts for more details.

Server configuration
By default, the Zabbix server is not configured to start any IPMI pollers, thus any added IPMI items won’t work. To change this, open the Zabbix server configuration file (`zabbix_server.conf`) as root and look for the following line:

```
# StartIPMIPollers=0
```

Uncomment it and set poller count to, say, 3, so that it reads:

```
StartIPMIPollers=3
```

Save the file and restart zabbix_server afterwards.

Item configuration
When configuring an item on a host level:

- For Host interface select the IPMI IP and port
- Select ‘IPMI agent’ as the Type
- Specify the IPMI sensor (for example ‘FAN MOD 1A RPM’ on Dell Poweredge). By default, sensor ID should be specified. It is also possible to use prefixes before the value:
  - id: - to specify sensor ID;
  - name: - to specify sensor full name. This can be useful in situations when sensors can only be distinguished by specifying the full name.
- Enter an item key that is unique within the host (say, ipmi.fan.rpm)
- Select the respective type of information (‘Numeric (float)’ in this case, for discrete sensors - ‘Numeric (unsigned)’), units (most likely ’rpm’) and any other required item attributes

Timeout and session termination
IPMI message timeouts and retry counts are defined in OpenIPMI library. Due to the current design of OpenIPMI, it is not possible to make these values configurable in Zabbix, neither on interface nor item level.

IPMI session inactivity timeout for LAN is 60 +/-3 seconds. Currently it is not possible to implement periodic sending of Activate Session command with OpenIPMI. If there are no IPMI item checks from Zabbix to a particular BMC for more than the session timeout configured in BMC then the next IPMI check after the timeout expires will time out due to individual message timeouts, retries or receive error. After that a new session is opened and a full rescan of the BMC is initiated. If you want to avoid unnecessary rescans of the BMC it is advised to set the IPMI item polling interval below the IPMI session inactivity timeout configured in BMC.

Notes on IPMI discrete sensors

To find sensors on a host start Zabbix server with `DebugLevel=4` enabled. Wait a few minutes and find sensor discovery records in Zabbix server logfile:

```
$ grep 'Added sensor' zabbix_server.log
8558:20130318:111122.170 Added sensor: host:'192.168.1.12:623' id_type:0 id_sz:17 id:'BB +1.1V P1 Vccp' reading_type:0x1 ('threshold') type:0x2 ('voltage') full_name:'(7.1).BB +1.1V P1 Vccp'
8558:20130318:111122.170 Added sensor: host:'192.168.1.12:623' id_type:0 id_sz:15 id:'CPU Therm Trip' reading_type:0x3 ('discrete_state') type:0x1 ('temperature') full_name:'(7.1).CPU Therm Trip'
8558:20130318:111122.171 Added sensor: host:'192.168.1.12:623' id_type:0 id_sz:17 id:'System Event Log' reading_type:0x6f ('sensor specific') type:0x10 ('event_logging_disabled') full_name:'(7.1).System Event Log'
```


The first parameter to start with is “reading_type”. Use “Table 42-1, Event/Reading Type Code Ranges” from the specifications to decode “reading_type” code. Most of the sensors in our example have “reading_type:0x1” which means “threshold” sensor. “Table 42-3, Sensor Type Codes” shows that “type:0x1” means temperature sensor, “type:0x2” - voltage sensor, “type:0x4” - Fan etc. Threshold sensors sometimes are called “analog” sensors as they measure continuous parameters like temperature, voltage, revolutions per minute.

Another example - a sensor with “reading_type:0x3”). “Table 42-1, Event/Reading Type Code Ranges” says that reading type codes 02h-0Ch mean “Generic Discrete” sensor. Discrete sensors have up to 15 possible states (in other words - up to 15 meaningful bits). For example, for sensor ‘CATERR’ with “type:0x7” the “Table 42-3, Sensor Type Codes” shows that this type means “Processor” and the meaning of individual bits is: 00h (the least significant bit) - IERR, 01h - Thermal Trip etc.

There are few sensors with “reading_type:0x6f” in our example. For these sensors the “Table 42-1, Event/Reading Type Code Ranges” advises to use “Table 42-3, Sensor Type Codes” for decoding meanings of bits. For example, sensor ‘Power Unit Stat’ has type “type:0x9” which means “Power Unit”. Offset 00h means “PowerOff/Power Down”. In other words if the least significant bit is 1, then server is powered off. To test this bit a function `band` with mask 1 can be used. The trigger expression could be like

{www.example.com:Power Unit Stat.band(#1,1))=1

to warn about a server power off.

Notes on discrete sensor names in OpenIPMI-2.0.16, 2.0.17, 2.0.18 and 2.0.19

Names of discrete sensors in OpenIPMI-2.0.16, 2.0.17 and 2.0.18 often have an additional “0” (or some other digit or letter) appended at the end. For example, while `ipmitool` and OpenIPMI-2.0.19 display sensor names as “PhysicalSecurity” or “CATERR”, in OpenIPMI-2.0.16, 2.0.17 and 2.0.18 the names are “PhysicalSecurity0” or “CATERR0”, respectively.

When configuring an IPMI item with Zabbix server using OpenIPMI-2.0.16, 2.0.17 and 2.0.18, use these names ending with “0” in the IPMI sensor field of IPMI agent items. When your Zabbix server is upgraded to a new Linux distribution, which uses OpenIPMI-2.0.19 (or later), items with these IPMI discrete sensors will become “NOT SUPPORTED”. You have to change their IPMI sensor names (remove the ‘0’ in the end) and wait for some time before they turn “Enabled” again.
Notes on threshold and discrete sensor simultaneous availability

Some IPMI agents provide both a threshold sensor and a discrete sensor under the same name. In Zabbix versions prior to 2.2.8 and 2.4.3, the first provided sensor was chosen. Since versions 2.2.8 and 2.4.3, preference is always given to the threshold sensor.

Notes on connection termination

If IPMI checks are not performed (by any reason: all host IPMI items disabled/not supported, host disabled/deleted, host in maintenance etc.) the IPMI connection will be terminated from Zabbix server or proxy in 3 to 4 hours depending on the time when Zabbix server/proxy was started.

5 Simple checks

Overview

Simple checks are normally used for remote agent-less checks of services.

Note that Zabbix agent is not needed for simple checks. Zabbix server/proxy is responsible for the processing of simple checks (making external connections, etc).

Examples of using simple checks:

- net.tcp.service[ftp,,155]
- net.tcp.service[http]
- net.tcp.service.perf[http,,8080]
- net.udp.service.perf[ntp]

Note:

User name and Password fields in simple check item configuration are used for VMware monitoring items; ignored otherwise.

Supported simple checks

List of supported simple checks:

See also:

- VMware monitoring item keys

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Return value</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>icmpping[&lt;target&gt;,&lt;packets&gt;,&lt;interval&gt;,&lt;size&gt;,&lt;timeout&gt;]</td>
<td>Host accessibility by ICMP ping.</td>
<td>0 - ICMP ping fails</td>
<td>target - IP or DNS name packets - number of packets interval - time between successive packets in milliseconds size - packet size in bytes timeout - timeout in milliseconds</td>
<td>Example: icmpping[4] → if at least one packet of the four is returned, the item will return 1. See also: table of default values.</td>
</tr>
<tr>
<td>icmppingloss[&lt;target&gt;,&lt;packets&gt;,&lt;interval&gt;,&lt;size&gt;,&lt;timeout&gt;]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key</td>
<td>Percentage of lost packets.</td>
<td>Float.</td>
<td><strong>target</strong> - host IP or DNS name</td>
<td><strong>packets</strong> - number of packets</td>
</tr>
<tr>
<td>-----</td>
<td>-----------------------------</td>
<td>--------</td>
<td>---------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>icmppingsec[&lt;target&gt;,&lt;packets&gt;,&lt;interval&gt;,&lt;size&gt;,&lt;timeout&gt;,&lt;mode&gt;]</td>
<td>ICMP ping response time (in seconds).</td>
<td>Float.</td>
<td><strong>target</strong> - host IP or DNS name</td>
<td><strong>packets</strong> - number of packets</td>
</tr>
</tbody>
</table>

net.tcp.service[service,<ip>,<port>]
Checks if service is running and accepting TCP connections.

<table>
<thead>
<tr>
<th>Service</th>
<th>Possible Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>ssh</td>
<td></td>
</tr>
<tr>
<td>ldap</td>
<td></td>
</tr>
<tr>
<td>smtp</td>
<td></td>
</tr>
<tr>
<td>ftp</td>
<td></td>
</tr>
<tr>
<td>http</td>
<td></td>
</tr>
<tr>
<td>pop</td>
<td></td>
</tr>
<tr>
<td>nntp</td>
<td></td>
</tr>
<tr>
<td>imap</td>
<td></td>
</tr>
<tr>
<td>tcp</td>
<td></td>
</tr>
<tr>
<td>https</td>
<td></td>
</tr>
<tr>
<td>telnet</td>
<td></td>
</tr>
</tbody>
</table>

ip - IP address or DNS name (by default host IP/DNS is used)

port - port number (by default standard service port number is used).

Example:

```
net.tcp.service[ftp,45] → can be used to test the availability of FTP server on TCP port 45.
```

Note that with tcp service indicating the port is mandatory. These checks may result in additional messages in system daemon logfiles (SMTP and SSH sessions being logged usually).

Checking of encrypted protocols (like IMAP on port 993 or POP on port 995) is currently not supported. As a workaround, please use `net.tcp.service[tcp,<ip>,<port>]` for checks like these.

https and telnet services are supported since Zabbix 2.0.

```
net.tcp.service.perf[service,<ip>,<port>]
```
<table>
<thead>
<tr>
<th>Key</th>
<th>Checks performance of TCP service.</th>
<th>Float. 0.000000 - service is down seconds - the number of seconds spent while connecting to the service</th>
<th>Example: =] net.tcp.service.perf[ssh] → can be used to test the speed of initial response from SSH server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>IP address or DNS name (by default, host IP/DNS is used)</td>
<td></td>
<td>Note that with tcp service indicating the port is mandatory. Checking of encrypted protocols (like IMAP on port 993 or POP on port 995) is currently not supported. As a workaround, please use net.tcp.service.perf[tcp,&lt;ip&gt;,port] for checks like these.</td>
</tr>
<tr>
<td>port</td>
<td>port number (by default standard service port number is used).</td>
<td></td>
<td>https and telnet services are supported since Zabbix 2.0. Called tcp_perf before Zabbix 2.0.</td>
</tr>
<tr>
<td>net.udp.service[service,&lt;ip&gt;,&lt;port&gt;]</td>
<td>Checks if service is running and responding to UDP requests.</td>
<td>0 - service is down 1 - service is running</td>
<td>Example: =] net.udp.service[ntp,45] → can be used to test the availability of NTP service on UDP port 45. This item is supported since Zabbix 3.0, but ntp service was available for net.tcp.service[] item in prior versions.</td>
</tr>
<tr>
<td>net.udp.service.perf[service,&lt;ip&gt;,&lt;port&gt;]</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Key

<table>
<thead>
<tr>
<th>Checks performance of UDP service.</th>
<th>Float.</th>
<th>service - possible values: ntp (see details) ip - IP address or DNS name (by default, host IP/DNS is used) port - port number (by default standard service port number is used).</th>
<th>Example: =&gt; net.udp.service.perf[ntp] (\rightarrow) can be used to test response time from NTP service.</th>
</tr>
</thead>
</table>

**Attention:**

For SourceIP support in LDAP simple checks (e.g. `net.tcp.service[ldap]`), OpenLDAP version 2.6.1 or above is required. SourceIP is supported in LDAP simple checks since Zabbix 4.0.39.

Timeout processing

Zabbix will not process a simple check longer than the Timeout seconds defined in the Zabbix server/proxy configuration file.

ICMP pings

Zabbix uses external utility `fping` for processing of ICMP pings.

The utility is not part of Zabbix distribution and has to be additionally installed. If the utility is missing, has wrong permissions or its location does not match the location set in the Zabbix server/proxy configuration file (`FpingLocation` parameter), ICMP pings (`icmpping`, `icmppingloss`, `icmppingsec`) will not be processed.

See also: [known issues](#)

`fping` must be executable by the user Zabbix daemons run as and setuid root. Run these commands as user **root** in order to set up correct permissions:

```
shell> chown root:zabbix /usr/sbin/fping
shell> chmod 4710 /usr/sbin/fping
```

After performing the two commands above check ownership of the `fping` executable. In some cases the ownership can be reset by executing the `chmod` command.

Also check, if user `zabbix` belongs to group `zabbix` by running:

```
shell> groups zabbix
```

and if it’s not add by issuing:

```
shell> usermod -a -G zabbix zabbix
```

Defaults, limits and description of values for ICMP check parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Unit</th>
<th>Description</th>
<th>Fping’s flag</th>
<th>Defaults set by</th>
<th>Allowed limits by Zabbix</th>
</tr>
</thead>
<tbody>
<tr>
<td>packets</td>
<td>number</td>
<td>number of request packets to a target</td>
<td><code>-C</code></td>
<td><code>Zabbix</code></td>
<td><code>max</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th>Zabbix</th>
<th>max</th>
</tr>
</thead>
<tbody>
<tr>
<td>packets</td>
<td>number</td>
<td>3</td>
<td>1</td>
<td>10000</td>
<td></td>
</tr>
</tbody>
</table>
### Parameter Table

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Unit</th>
<th>Description</th>
<th>Fping’s flag</th>
<th>Defaults set by</th>
<th>Allowed limits by Zabbix</th>
</tr>
</thead>
<tbody>
<tr>
<td>interval</td>
<td>ms</td>
<td>time to wait between successive packets</td>
<td>-p</td>
<td>1000</td>
<td>20 unlimited</td>
</tr>
<tr>
<td>size</td>
<td>bytes</td>
<td>packet size in bytes</td>
<td>-b</td>
<td>56 or 68</td>
<td>24 65507</td>
</tr>
<tr>
<td>timeout</td>
<td>ms</td>
<td>wait after last packet sent</td>
<td>-t</td>
<td>fping v3.x - 500</td>
<td>unlimited</td>
</tr>
<tr>
<td></td>
<td></td>
<td>affected by -C flag</td>
<td></td>
<td>fping v4.x -</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>inherited from -p flag, but not more than 2000</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In addition Zabbix uses fping options -i interval ms (do not mix up with the item parameter interval mentioned in the table above, which corresponds to fping option -p) and -S source IP address (or -I in older fping versions). Those options are auto-detected by running checks with different option combinations. Zabbix tries to detect the minimal value in milliseconds that fping allows to use with -i by trying 3 values: 0, 1 and 10. The value that first succeeds is then used for subsequent ICMP checks. This process is done by each ICMP pinger process individually.

Since Zabbix 4.0.25 auto-detected fping options are invalidated every hour and detected again on the next attempt to perform ICMP check. Set DebugLevel>=4 in order to view details of this process in the server or proxy log file.

**Warning:**
Warning: fping defaults can differ depending on platform and version - if in doubt, check fping documentation.

Zabbix writes IP addresses to be checked by any of three icmpping* keys to a temporary file, which is then passed to fping. If items have different key parameters, only ones with identical key parameters are written to a single file.

All IP addresses written to the single file will be checked by fping in parallel, so Zabbix icmp pinger process will spend fixed amount of time disregarding the number of IP addresses in the file.

1 VMware monitoring item keys

**Item keys**

The table provides details on the simple checks that can be used to monitor VMware environments.

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Return value</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>vmware.cluster.discovery[&lt;url&gt;]</td>
<td>Discovery of VMware clusters.</td>
<td>JSON object</td>
<td>url - VMware service URL</td>
<td></td>
</tr>
<tr>
<td>vmware.cluster.status[&lt;url&gt;, &lt;name&gt;]</td>
<td>VMware cluster status.</td>
<td>Integer: 0 - gray; 1 - green; 2 - yellow; 3 - red</td>
<td>url - VMware service URL name - VMware cluster name</td>
<td></td>
</tr>
<tr>
<td>Key</td>
<td>Description</td>
<td>Type</td>
<td>Details</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Discovery of VMware datastores.</td>
<td></td>
<td>JSON object</td>
<td>url - VMware service URL This item is supported since Zabbix 4.0.10.</td>
<td></td>
</tr>
<tr>
<td>vmware.datastore hv.list[&lt;url&gt;,&lt;datastore&gt;]</td>
<td>List of datastore hypervisors.</td>
<td>JSON object</td>
<td>url - VMware service URL datastore - datastore name This item is supported since Zabbix 4.0.10.</td>
<td></td>
</tr>
<tr>
<td>rmware.datastore.read[&lt;url&gt;,&lt;datastore&gt;,&lt;mode&gt;]</td>
<td>Amount of time for a read operation from the datastore (milliseconds).</td>
<td>Integer ²</td>
<td>url - VMware service URL datastore - datastore name mode - latency (average value, default), maxlatency (maximum value) This item is supported since Zabbix 4.0.10.</td>
<td></td>
</tr>
<tr>
<td>vmware.datastore.size[&lt;url&gt;,&lt;datastore&gt;,&lt;mode&gt;]</td>
<td>VMware datastore space in bytes or in percentage from total.</td>
<td>Integer - for bytes Float - for percentage</td>
<td>url - VMware service URL datastore - datastore name mode - possible values: total (default), free, pfree (free, percentage), uncommitted This item is supported since Zabbix 4.0.10.</td>
<td></td>
</tr>
<tr>
<td>vmware.datastore.write[&lt;url&gt;,&lt;datastore&gt;,&lt;mode&gt;]</td>
<td>Amount of time for a write operation to the datastore (milliseconds).</td>
<td>Integer ²</td>
<td>url - VMware service URL datastore - datastore name mode - latency (average value, default), maxlatency (maximum value) This item is supported since Zabbix 4.0.10.</td>
<td></td>
</tr>
<tr>
<td>vmware.dc.discovery[&lt;url&gt;]</td>
<td>Discovery of VMware datacenters.</td>
<td>JSON object</td>
<td>url - VMware service URL This item is supported since Zabbix 4.0.23.</td>
<td></td>
</tr>
<tr>
<td>vmware.eventlog[&lt;url&gt;,&lt;mode&gt;]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key</td>
<td>Description</td>
<td>Type</td>
<td>URL Options</td>
<td>Notes</td>
</tr>
<tr>
<td>-----</td>
<td>-------------</td>
<td>------</td>
<td>-------------</td>
<td>-------</td>
</tr>
<tr>
<td>vmware.eventlog</td>
<td>VMware event log.</td>
<td>Log</td>
<td>url - VMware service URL mode - all (default), skip - skip processing of older data</td>
<td>There must be only one vmware.eventlog[] item key per URL. See also: example of filtering VMware event log records. The mode parameter is supported since Zabbix 4.0.6.</td>
</tr>
<tr>
<td>vmware.fullname[&lt;url&gt;]</td>
<td>VMware service full name.</td>
<td>String</td>
<td>url - VMware service URL</td>
<td></td>
</tr>
<tr>
<td>vmware hv.cluster.name[&lt;url&gt;,&lt;uuid&gt;]</td>
<td>VMware hypervisor cluster name.</td>
<td>String</td>
<td>url - VMware service URL uuid - VMware hypervisor host name</td>
<td></td>
</tr>
<tr>
<td>vmware hv.cpu.usage[&lt;url&gt;,&lt;uuid&gt;]</td>
<td>VMware hypervisor processor usage (Hz).</td>
<td>Integer</td>
<td>url - VMware service URL uuid - VMware hypervisor host name</td>
<td></td>
</tr>
<tr>
<td>vmware hv.datacenter.name[&lt;url&gt;,&lt;uuid&gt;]</td>
<td>VMware hypervisor datacenter name.</td>
<td>String</td>
<td>url - VMware service URL uuid - VMware hypervisor host name</td>
<td></td>
</tr>
<tr>
<td>vmware hv.datastore.discovery[&lt;url&gt;,&lt;uuid&gt;]</td>
<td>Discovery of VMware hypervisor datastores.</td>
<td>JSON object</td>
<td>url - VMware service URL uuid - VMware hypervisor host name</td>
<td></td>
</tr>
<tr>
<td>vmware hv.datastore.list[&lt;url&gt;,&lt;uuid&gt;]</td>
<td>List of VMware hypervisor datastores.</td>
<td>JSON object</td>
<td>url - VMware service URL uuid - VMware hypervisor host name</td>
<td>This item is supported since Zabbix 4.0.10.</td>
</tr>
<tr>
<td>vmware hv.datastore.read[&lt;url&gt;,&lt;uuid&gt;,&lt;datastore&gt;,&lt;mode&gt;]</td>
<td>Average amount of time for a read operation from the datastore (milliseconds).</td>
<td>Integer</td>
<td>url - VMware service URL uuid - VMware hypervisor host name datastore - datastore name mode - latency (default)</td>
<td></td>
</tr>
</tbody>
</table>
### Key

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
<th>Type</th>
<th>URL</th>
<th>UUID</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vmware.hv.datastore.size</code>&lt;url&gt;,&lt;uuid&gt;,&lt;datastore&gt;,&lt;mode&gt;`</td>
<td>VMware datastore space in bytes or in percentage from total.</td>
<td>Integer</td>
<td><code>url</code> - VMware service URL</td>
<td><code>uuid</code> - VMware hypervisor host name</td>
<td>Available since Zabbix versions 3.0.6, 3.2.2</td>
</tr>
<tr>
<td><code>vmware.hv.datastore.write</code>&lt;url&gt;,&lt;uuid&gt;,&lt;datastore&gt;,&lt;mode&gt;`</td>
<td>Average amount of time for a write operation to the datastore (milliseconds).</td>
<td>Integer²</td>
<td><code>url</code> - VMware service URL</td>
<td><code>uuid</code> - VMware hypervisor host name</td>
<td></td>
</tr>
<tr>
<td><code>vmware.hv.discovery</code>&lt;url&gt;`</td>
<td>Discovery of VMware hypervisors.</td>
<td>JSON object</td>
<td><code>url</code> - VMware service URL</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>vmware.hv.fullname</code>&lt;url&gt;,&lt;uuid&gt;`</td>
<td>VMware hypervisor name.</td>
<td>String</td>
<td><code>url</code> - VMware service URL</td>
<td><code>uuid</code> - VMware hypervisor host name</td>
<td></td>
</tr>
<tr>
<td><code>vmware.hv.hw.cpu.freq</code>&lt;url&gt;,&lt;uuid&gt;`</td>
<td>VMware hypervisor processor frequency (Hz).</td>
<td>Integer</td>
<td><code>url</code> - VMware service URL</td>
<td><code>uuid</code> - VMware hypervisor host name</td>
<td></td>
</tr>
<tr>
<td><code>vmware.hv.hw.cpu.model</code>&lt;url&gt;,&lt;uuid&gt;`</td>
<td>VMware hypervisor processor model.</td>
<td>String</td>
<td><code>url</code> - VMware service URL</td>
<td><code>uuid</code> - VMware hypervisor host name</td>
<td></td>
</tr>
<tr>
<td><code>vmware.hv.hw.cpu.num</code>&lt;url&gt;,&lt;uuid&gt;`</td>
<td>Number of processor cores on VMware hypervisor.</td>
<td>Integer</td>
<td><code>url</code> - VMware service URL</td>
<td><code>uuid</code> - VMware hypervisor host name</td>
<td></td>
</tr>
<tr>
<td><code>vmware.hv.hw.cpu.threads</code>&lt;url&gt;,&lt;uuid&gt;`</td>
<td>Number of processor threads on VMware hypervisor.</td>
<td>Integer</td>
<td><code>url</code> - VMware service URL</td>
<td><code>uuid</code> - VMware hypervisor host name</td>
<td></td>
</tr>
<tr>
<td>Key</td>
<td>Description</td>
<td>Type</td>
<td>Notes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>-------------</td>
<td>------</td>
<td>-------</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| vmware.hv.hw.memory[<url>,<uuid>] | VMware hypervisor total memory size (bytes). | Integer | url - VMware service URL  
| | | | uuid - VMware hypervisor host name |
| vmware.hv.hw.model[<url>,<uuid>] | VMware hypervisor model. | String | url - VMware service URL  
| | | | uuid - VMware hypervisor host name |
| vmware.hv.hw.uuid[<url>,<uuid>] | VMware hypervisor BIOS UUID. | String | url - VMware service URL  
| | | | uuid - VMware hypervisor host name |
| vmware.hv.hw.vendor[<url>,<uuid>] | VMware hypervisor vendor name. | String | url - VMware service URL  
| | | | uuid - VMware hypervisor host name |
| vmware.hv.memory.size.ballooned[<url>,<uuid>] | VMware hypervisor ballooned memory size (bytes). | Integer | url - VMware service URL  
| | | | uuid - VMware hypervisor host name |
| vmware.hv.memory.used[<url>,<uuid>] | VMware hypervisor used memory size (bytes). | Integer | url - VMware service URL  
| | | | uuid - VMware hypervisor host name |
| vmware.hv.network.in[<url>,<uuid>,<mode>] | VMware hypervisor network input statistics (bytes per second). | Integer | url - VMware service URL  
| | | | uuid - VMware hypervisor host name  
| | | | mode - bps (default) |
| vmware.hv.network.out[<url>,<uuid>,<mode>] | VMware hypervisor network output statistics (bytes per second). | Integer | url - VMware service URL  
| | | | uuid - VMware hypervisor host name  
<p>| | | | mode - bps (default) |
| vmware.hv.perfcounter[&lt;url&gt;,&lt;uuid&gt;,&lt;path&gt;,&lt;instance&gt;] | | | |</p>
<table>
<thead>
<tr>
<th>Key</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware hypervisor performance counter value.</td>
<td>Integer</td>
<td>url - VMware service URL uuid - VMware hypervisor host name path - performance counter path instance - performance counter instance. Use empty instance for aggregate values (default)</td>
</tr>
<tr>
<td>vmware.hv.sensor.health.state[&lt;url&gt;,&lt;uuid&gt;]</td>
<td>VMware</td>
<td>VMware hypervisor health state rollup sensor.</td>
</tr>
<tr>
<td>vmware.hv.status[&lt;url&gt;,&lt;uuid&gt;]</td>
<td>VMware</td>
<td>VMware hypervisor status.</td>
</tr>
<tr>
<td>vmware.hv.uptime[&lt;url&gt;,&lt;uuid&gt;]</td>
<td>VMware</td>
<td>VMware hypervisor uptime (seconds).</td>
</tr>
<tr>
<td>vmware.hv.vm.num[&lt;url&gt;,&lt;uuid&gt;]</td>
<td>Integer</td>
<td>Number of virtual machines on VMware hypervisor.</td>
</tr>
<tr>
<td>vmware.version[&lt;url&gt;]</td>
<td>VMware</td>
<td>VMware service version.</td>
</tr>
<tr>
<td>vmware.vm.cluster.name[&lt;url&gt;,&lt;uuid&gt;]</td>
<td>VMware</td>
<td>VMware virtual machine name.</td>
</tr>
<tr>
<td>vmware.vm.cpu.num[&lt;url&gt;,&lt;uuid&gt;]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key</td>
<td>Description</td>
<td>Type</td>
</tr>
<tr>
<td>-----</td>
<td>-------------</td>
<td>------</td>
</tr>
</tbody>
</table>
| vmware.vm.cpu.ready[<url>,<uuid>] | Time (in milliseconds) that the virtual machine was ready, but could not get scheduled to run on the physical CPU. CPU ready time is dependent on the number of virtual machines on the host and their CPU loads (%). | Integer | url - VMware service URL  
uuid - VMware virtual machine host name  
Available since Zabbix version 3.0.0 |
| vmware.vm.cpu.usage[<url>,<uuid>] | VMware virtual machine processor usage (Hz). | Integer | url - VMware service URL  
uuid - VMware virtual machine host name |
| vmware.vm.datacenter.name[<url>,<uuid>] | VMware virtual machine datacenter name. | String | url - VMware service URL  
uuid - VMware virtual machine host name |
| vmware.vm.discovery[<url>] | Discovery of VMware virtual machines. | JSON object | url - VMware service URL |
| vmware.vm hv.name[<url>,<uuid>] | VMware virtual machine hypervisor name. | String | url - VMware service URL  
uuid - VMware virtual machine host name |
| vmware.vm.memory.size[<url>,<uuid>] | VMware virtual machine total memory size (bytes). | Integer | url - VMware service URL  
uuid - VMware virtual machine host name |
| vmware.vm.memory.size.ballooned[<url>,<uuid>] | VMware virtual machine ballooned memory size (bytes). | Integer | url - VMware service URL  
uuid - VMware virtual machine host name |
<p>| vmware.vm.memory.size.compressed[&lt;url&gt;,&lt;uuid&gt;] | | | |</p>
<table>
<thead>
<tr>
<th>Key</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vmware.vm.memory.size.private[&lt;url&gt;,&lt;uuid&gt;]</td>
<td>Integer</td>
<td>VMware virtual machine compressed memory size (bytes).</td>
</tr>
<tr>
<td>vmware.vm.memory.size.shared[&lt;url&gt;,&lt;uuid&gt;]</td>
<td>Integer</td>
<td>VMware virtual machine private memory size (bytes).</td>
</tr>
<tr>
<td>vmware.vm.memory.size.swapped[&lt;url&gt;,&lt;uuid&gt;]</td>
<td>Integer</td>
<td>VMware virtual machine shared memory size (bytes).</td>
</tr>
<tr>
<td>vmware.vm.memory.size.usage.guest[&lt;url&gt;,&lt;uuid&gt;]</td>
<td>Integer</td>
<td>VMware virtual machine guest memory usage (bytes).</td>
</tr>
<tr>
<td>vmware.vm.memory.size.usage.host[&lt;url&gt;,&lt;uuid&gt;]</td>
<td>Integer</td>
<td>VMware virtual machine host memory usage (bytes).</td>
</tr>
<tr>
<td>vmware.vm.net.if.discovery[&lt;url&gt;,&lt;uuid&gt;]</td>
<td>JSON object</td>
<td>Discovery of VMware virtual machine network interfaces.</td>
</tr>
<tr>
<td>vmware.vm.net.if.in[&lt;url&gt;,&lt;uuid&gt;,&lt;instance&gt;,&lt;mode&gt;]</td>
<td>Integer</td>
<td>VMware virtual machine network interface input statistics (bytes/packets per second).</td>
</tr>
<tr>
<td>vmware.vm.net.if.out[&lt;url&gt;,&lt;uuid&gt;,&lt;instance&gt;,&lt;mode&gt;]</td>
<td>Integer</td>
<td>VMware virtual machine network interface output statistics (bytes/packets per second).</td>
</tr>
<tr>
<td>Key</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>VMware virtual machine network interface output statistics</td>
<td>(bytes/packets per second).</td>
<td></td>
</tr>
<tr>
<td>vmware.vm.perfcounter[&lt;url&gt;,&lt;uuid&gt;,&lt;path&gt;,&lt;instance&gt;]</td>
<td>VMware virtual machine performance counter value.</td>
<td></td>
</tr>
<tr>
<td>vmware.vm.powerstate[&lt;url&gt;,&lt;uuid&gt;]</td>
<td>VMware virtual machine power state.</td>
<td></td>
</tr>
<tr>
<td>vmware.vm.storage.committed[&lt;url&gt;,&lt;uuid&gt;]</td>
<td>VMware virtual machine committed storage space (bytes).</td>
<td></td>
</tr>
<tr>
<td>vmware.vm.storage.uncommitted[&lt;url&gt;,&lt;uuid&gt;]</td>
<td>VMware virtual machine uncommitted storage space (bytes).</td>
<td></td>
</tr>
<tr>
<td>vmware.vm.storage.unshared[&lt;url&gt;,&lt;uuid&gt;]</td>
<td>VMware virtual machine unshared storage space (bytes).</td>
<td></td>
</tr>
<tr>
<td>vmware.vm.uptime[&lt;url&gt;,&lt;uuid&gt;]</td>
<td>VMware virtual machine uptime (seconds).</td>
<td></td>
</tr>
<tr>
<td>vmware.vm.vfs.dev.discovery[&lt;url&gt;,&lt;uuid&gt;]</td>
<td>VMware virtual machine network interface instance.</td>
<td></td>
</tr>
</tbody>
</table>

1. Available since Zabbix versions 2.2.9, 2.4.4
2. Integer

url - VMware service URL
uuid - VMware virtual machine host name
instance - network interface instance
mode - bps (default)/pps - bytes/packets per second
path - performance counter path
instance - performance counter instance. Use empty instance for aggregate values (default)
Discovery of VMware virtual machine disk devices.

vmware.vm.vfs.dev.read[<url>,<uuid>,<instance>,<mode>]
VMware virtual machine disk device read statistics (bytes/operations per second).

vmware.vm.vfs.dev.write[<url>,<uuid>,<instance>,<mode>]
VMware virtual machine disk device write statistics (bytes/operations per second).

vmware.vm.vfs.fs.discovery[<url>,<uuid>]
Discovery of VMware virtual machine file systems.

vmware.vm.vfs.fs.size[<url>,<uuid>,<fsname>,<mode>]
VMware virtual machine file system statistics (bytes/percentages).

Footnotes

1 The VMware performance counter path has the group/counter[rollup] format where:
   - group - the performance counter group, for example cpu
   - counter - the performance counter name, for example usagemhz
   - rollup - the performance counter rollup type, for example average
   So the above example would give the following counter path: cpu/usagemhz[average]

The performance counter group descriptions, counter names and rollup types can be found in VMware documentation.

2 The value of these items is obtained from VMware performance counters and the VMwarePerfFrequency parameter is used to refresh their data in Zabbix VMware cache:
   - vmware hv datastore read
More info

See Virtual machine monitoring for detailed information how to configure Zabbix to monitor VMware environments.

6 Log file monitoring

Overview

Zabbix can be used for centralized monitoring and analysis of log files with/without log rotation support.

Notifications can be used to warn users when a log file contains certain strings or string patterns.

To monitor a log file you must have:

- Zabbix agent running on the host
- log monitoring item set up

Attention:
The size limit of a monitored log file depends on large file support.

Configuration

Verify agent parameters

Make sure that in the agent configuration file:

- ‘Hostname’ parameter matches the host name in the frontend
- Servers in the ‘ServerActive’ parameter are specified for the processing of active checks

Item configuration

Configure a log monitoring item.

All mandatory input fields are marked with a red asterisk.

Specifically for log monitoring items you enter:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Select Zabbix agent (active) here.</th>
</tr>
</thead>
</table>
Use one of the following item keys:

- **log[] or logrt[]:**
  These two item keys allow to monitor logs and filter log entries by the content regexp, if present.
  For example: `log[/var/log/syslog, error]`. Make sure that the file has read permissions for the `zabbix` user otherwise the item status will be set to 'unsupported'.

- **log.count[] or logrt.count[]:**
  These two item keys allow to return the number of matching lines only.
  See supported Zabbix agent item key section for details on using these item keys and their parameters.

### Type of information

**Select:**

- For log[] or logrt[] items - Log;
- For log.count[] or logrt.count[] items - Numeric (unsigned).

If optionally using the output parameter, you may select the appropriate type of information other than Log.

Note that choosing a non-Log type of information will lead to the loss of local timestamp.

### Update interval (in sec)

The parameter defines how often Zabbix agent will check for any changes in the log file. Setting it to 1 second will make sure that you get new records as soon as possible.

### Log time format

In this field you may optionally specify the pattern for parsing the log line timestamp.

If left blank the timestamp will not be parsed.

Supported placeholders:

- *y*: Year (0001-9999)
- *M*: Month (01-12)
- *d*: Day (01-31)
- *h*: Hour (00-23)
- *m*: Minute (00-59)
- *s*: Second (00-59)

For example, consider the following line from the Zabbix agent log file:

```
" 23480:20100328:154718.045 Zabbix agent started. Zabbix 1.8.2 (revision 11211)."
```

It begins with six character positions for PID, followed by date, time, and the rest of the line.

Log time format for this line would be

```
"pppppp:yyyyMMdd:hhmmss".
```

Note that "p" and ":" chars are just placeholders and can be anything but "yMdHms".

### Important notes

- The server and agent keep the trace of a monitored log’s size and last modification time (for logrt) in two counters. Additionally:
  - The agent also internally uses inode numbers (on UNIX/GNU/Linux), file indexes (on Microsoft Windows) and MD5 sums of the first 512 log file bytes for improving decisions when logfiles get truncated and rotated.
  - On UNIX/GNU/Linux systems it is assumed that the file systems where log files are stored report inode numbers, which can be used to track files.
  - On Microsoft Windows Zabbix agent determines the file system type the log files reside on and uses:
    - On NTFS file systems 64-bit file indexes.
    - On ReFS file systems (only from Microsoft Windows Server 2012) 128-bit file IDs.
    - On file systems where file indexes change (e.g. FAT32, exFAT) a fall-back algorithm is used to take a sensible approach in uncertain conditions when log file rotation results in multiple log files with the same last modification time.
  - The inode numbers, file indexes and MD5 sums are internally collected by Zabbix agent. They are not transmitted to Zabbix server and are lost when Zabbix agent is stopped.
  - Do not modify the last modification time of log files with 'touch' utility, do not copy a log file with later restoration of the original name (this will change the file inode number). In both cases the file will be counted as different and will
be analyzed from the start, which may result in duplicated alerts.

- If there are several matching log files for logrt[] item and Zabbix agent is following the most recent of them and this most recent log file is deleted, a warning message "there are no files matching "<regexp mask>" in "<directory>" is logged. Zabbix agent ignores log files with modification time less than the most recent modification time seen by the agent for the logrt[] item being checked.

- The agent starts reading the log file from the point it stopped the previous time.
- The number of bytes already analyzed (the size counter) and last modification time (the time counter) are stored in the Zabbix database and are sent to the agent to make sure the agent starts reading the log file from this point in cases when the agent is just started or has received items which were previously disabled or not supported. However, if the agent has received a non-zero size counter from server, but the logrt[] or logrt.count[] item has not found and does not find matching files, the size counter is reset to 0 to analyze from the start if the files appear later.
- Whenever the log file becomes smaller than the log size counter known by the agent, the counter is reset to zero and the agent starts reading the log file from the beginning taking the time counter into account.
- If there are several matching files with the same last modification time in the directory, then the agent tries to correctly analyze all log files with the same modification time and avoid skipping data or analyzing the same data twice, although it cannot be guaranteed in all situations. The agent does not assume any particular log file rotation scheme nor determines one. When presented multiple log files with the same last modification time, the agent will process them in a lexicographically descending order. Thus, for some rotation schemes the log files will be analyzed and reported in their original order. For other rotation schemes the original log file order will not be honored, which can lead to reporting matched log file records in altered order (the problem does not happen if log files have different last modification times).
- Zabbix agent processes new records of a log file once per Update interval seconds.
- Zabbix agent does not send more than maxlines of a log file per second. The limit prevents overloading of network and CPU resources and overrides the default value provided by MaxLinesPerSecond parameter in the agent configuration file.
- To find the required string Zabbix will process 10 times more new lines than set in MaxLinesPerSecond. Thus, for example, if a log[] or logrt[] item has Update interval of 1 second, by default the agent will analyze no more than 200 log file records and will send no more than 20 matching records to Zabbix server in one check. By increasing MaxLinesPerSecond in the agent configuration file or setting maxlines parameter in the item key, the limit can be increased up to 10000 analyzed log file records and 1000 matching records sent to Zabbix server in one check. If the Update interval is set to 2 seconds the limits for one check would be set 2 times higher than with Update interval of 1 second.
- Additionally, log and log.count values are always limited to 50% of the agent send buffer size, even if there are no non-log values in it. So for the maxlines values to be sent in one connection (and not in several connections), the agent BufferSize parameter must be at least maxlines x 2.
- In the absence of log items all agent buffer size is used for non-log values. When log values come in they replace the older non-log values as needed, up to the designated 50%.
- For log file records longer than 256kB, only the first 256kB are matched against the regular expression and the rest of the record is ignored. However, if Zabbix agent is stopped while it is dealing with a long record the agent internal state is lost and the long record may be analyzed again and differently after the agent is started again.
- Special note for "/" path separators: if file_format is "file.log", then there should not be a "file" directory, since it is not possible to unambiguously define whether "." is escaped or is the first symbol of the file name.
- Regular expressions for logrt are supported in filename only, directory regular expression matching is not supported.
- On UNIX platforms a logrt[] item becomes NOTSUPPORTED if a directory where the log files are expected to be found does not exist.
- On Microsoft Windows, if a directory does not exist the item will not become NOTSUPPORTED (for example, if directory is misspelled in item key).
- An absence of log files for logrt[] item does not make it NOTSUPPORTED. Errors of reading log files for logrt[] item are logged as warnings into Zabbix agent log file but do not make the item NOTSUPPORTED.
- Zabbix agent log file can be helpful to find out why a log[] or logrt[] item became NOTSUPPORTED. Zabbix can monitor its agent log file, except when at DebugLevel=4 or DebugLevel=5.

Extracting matching part of regular expression

Sometimes we may want to extract only the interesting value from a target file instead of returning the whole line when a regular expression match is found.

Since Zabbix 2.2.0, log items have the ability to extract desired values from matched lines. This is accomplished by the additional output parameter in log and logrt items.

Using the 'output' parameter allows to indicate the subgroup of the match that we may be interested in.

So, for example

log[/path/to/the/file,"large_result buffer allocation.*Entries: (\[0-9\]+)"\,"\,"\,\]\]

should allow returning the entry count as found in the content of:

Fr 07 Feb 2014 11:07:36.6690 +/ Thread Id 1400 (GLEWF) large result
buffer allocation - /Length: 437136/Entries: 5948/Client Ver: >=10/RPC

263
The reason why Zabbix will return only the number is because 'output' here is defined by \1 referring to the first and only subgroup of interest: ([0-9]+)

And, with the ability to extract and return a number, the value can be used to define triggers.

Using maxdelay parameter

The 'maxdelay' parameter in log items allows ignoring some older lines from log files in order to get the most recent lines analyzed within the 'maxdelay' seconds.

**Warning:**

Specifying 'maxdelay' > 0 may lead to ignoring important log file records and missed alerts. Use it carefully at your own risk only when necessary.

By default items for log monitoring follow all new lines appearing in the log files. However, there are applications which in some situations start writing an enormous number of messages in their log files. For example, if a database or a DNS server is unavailable, such applications flood log files with thousands of nearly identical error messages until normal operation is restored. By default, all those messages will be dutifully analyzed and matching lines sent to server as configured in log and logrt items.

Built-in protection against overload consists of a configurable 'maxlines' parameter (protects server from too many incoming matching log lines) and a 4*‘maxlines’ limit (protects host CPU and I/O from overloading by agent in one check). Still, there are 2 problems with the built-in protection. First, a large number of potentially not-so-informative messages are reported to server and consume space in the database. Second, due to the limited number of lines analyzed per second the agent may lag behind the newest log records for hours. Quite likely, you might prefer to be sooner informed about the current situation in the log files instead of crawling through old records for hours.

The solution to both problems is using the 'maxdelay' parameter. If 'maxdelay' > 0 is specified, during each check the number of processed bytes, the number of remaining bytes and processing time is measured. From these numbers the agent calculates an estimated delay - how many seconds it would take to analyze all remaining records in a log file.

If the delay does not exceed 'maxdelay' then the agent proceeds with analyzing the log file as usual.

If the delay is greater than 'maxdelay' then the agent ignores a chunk of a log file by "jumping" over it to a new estimated position so that the remaining lines could be analyzed within 'maxdelay' seconds.

Note that agent does not even read ignored lines into buffer, but calculates an approximate position to jump to in a file.

The fact of skipping log file lines is logged in the agent log file like this:

```
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
```

The "to byte" number is approximate because after the "jump" the agent adjusts the position in the file to the beginning of a log line which may be further in the file or earlier.

Depending on how the speed of growing compares with the speed of analyzing the log file you may see no "jumps", rare or often "jumps", large or small "jumps", or even a small "jump" in every check. Fluctuations in the system load and network latency also affect the calculation of delay and hence, "jumping" ahead to keep up with the "maxdelay" parameter.

Setting 'maxdelay' < 'update interval' is not recommended (it may result in frequent small "jumps").

Notes on handling 'copytruncate' log file rotation

logrt with the copytruncate option assumes that different log files have different records (at least their timestamps are different), therefore MDS sums of initial blocks (up to the first 512 bytes) will be different. Two files with the same MDS sums of initial blocks means that one of them is the original, another - a copy.

logrt with the copytruncate option makes effort to correctly process log file copies without reporting duplicates. However, things like producing multiple log file copies with the same timestamp, log file rotation more often than logrt[] item update interval, frequent restarting of agent are not recommended. The agent tries to handle all these situations reasonably well, but good results cannot be guaranteed in all circumstances.

Actions if communication fails between agent and server

Each matching line from log[] and logrt[] item and a result of each log.count[] and logrt.count[] item check requires a free slot in the designated 50% area in the agent send buffer. The buffer elements are regularly sent to server (or proxy) and the buffer slots are free again.

While there are free slots in the designated log area in the agent send buffer and communication fails between agent and server (or proxy) the log monitoring results are accumulated in the send buffer. This helps to mitigate short communication failures.
During longer communication failures all log slots get occupied and the following actions are taken:

- `log[]` and `logrt[]` item checks are stopped. When communication is restored and free slots in the buffer are available the checks are resumed from the previous position. No matching lines are lost, they are just reported later.
- `log.count[]` and `logrt.count[]` checks are stopped if `maxdelay = 0` (default). Behavior is similar to `log[]` and `logrt[]` items as described above. Note that this can affect `log.count[]` and `logrt.count[]` results: for example, one check counts 100 matching lines in a log file, but as there are no free slots in the buffer the check is stopped. When communication is restored the agent counts the same 100 matching lines and also 70 new matching lines. The agent now sends count = 170 as if they were found in one check.
- `log.count[]` and `logrt.count[]` checks with `maxdelay > 0`: if there was no “jump” during the check, then behavior is similar to described above. If a “jump” over log file lines took place then the position after “jump” is kept and the counted result is discarded. So, the agent tries to keep up with a growing log file even in case of communication failure.

7 Calculated items

Overview

With calculated items you can create calculations on the basis of other items.

Thus, calculated items are a way of creating virtual data sources. The values will be periodically calculated based on an arithmetical expression. All calculations are done by the Zabbix server - nothing related to calculated items is performed on Zabbix agents or proxies.

The resulting data will be stored in the Zabbix database as for any other item - this means storing both history and trend values for fast graph generation. Calculated items may be used in trigger expressions, referenced by macros or other entities same as any other item type.

To use calculated items, choose the item type Calculated.

Configurable fields

The key is a unique item identifier (per host). You can create any key name using supported symbols.

Calculation definition should be entered in the Formula field. There is virtually no connection between the formula and the key. The key parameters are not used in formula in any way.

The correct syntax of a simple formula is:

```
func(<key>|<hostname:key>,<parameter1>,<parameter2>,...)
```

Where:

<table>
<thead>
<tr>
<th>ARGUMENT</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>func</code></td>
<td>One of the functions supported in trigger expressions: last, min, max, avg, count, etc.</td>
</tr>
<tr>
<td><code>key</code></td>
<td>The key of another item whose data you want to use. It may be defined as key or hostname:key. Note: Putting the whole key in double quotes (“…””) is strongly recommended to avoid incorrect parsing because of spaces or commas within the key. If there are also quoted parameters within the key, those double quotes must be escaped by using the backslash (). See Example 5 below.</td>
</tr>
<tr>
<td><code>parameter(s)</code></td>
<td>Function parameter(s), if required.</td>
</tr>
</tbody>
</table>

**Note:**

All items that are referenced from the calculated item formula must exist and be collecting data (exceptions in functions and unsupported items). Also, if you change the item key of a referenced item, you have to manually update any formulas using that key.

**Attention:**

User macros in the formula will be expanded if used to reference a function parameter or a constant. User macros will NOT be expanded if referencing a function, host name, item key, item key parameter or operator.
A more complex formula may use a combination of functions, operators and brackets. You can use all functions and operators supported in trigger expressions. Note that the syntax is slightly different, however logic and operator precedence are exactly the same.

Unlike trigger expressions, Zabbix processes calculated items according to the item update interval, not upon receiving a new value.

**Note:**
If the calculation result is a float value it will be trimmed to an integer if the calculated item type of information is Numeric (unsigned).

A calculated item may become unsupported in several cases:

1. referenced item(s)
   - is not found
   - is disabled
   - belongs to a disabled host
   - is not supported (see exceptions in functions and unsupported items, Expressions with unsupported items and unknown values and Operators)
2. no data to calculate a function
3. division by zero
4. incorrect syntax used

Support for calculated items was introduced in Zabbix 1.8.1.
Starting from Zabbix 3.2 calculated items in some cases may involve unsupported items as described in functions and unsupported items, Expressions with unsupported items and unknown values and Operators.

**Usage examples**

**Example 1**
Calculating percentage of free disk space on '/'.

Use of function **last**:

```
100*last("vfs.fs.size[/,free"])/last("vfs.fs.size[/,total"])
```

Zabbix will take the latest values for free and total disk spaces and calculate percentage according to the given formula.

**Example 2**
Calculating a 10-minute average of the number of values processed by Zabbix.

Use of function **avg**:

```
avg("Zabbix Server:zabbix[wcach,values]",600)
```

Note that extensive use of calculated items with long time periods may affect performance of Zabbix server.

**Example 3**
Calculating total bandwidth on eth0.

Sum of two functions:

```
last("net.if.in[eth0,bytes"])+last("net.if.out[eth0,bytes"])
```

**Example 4**
Calculating percentage of incoming traffic.

More complex expression:

```
100*last("net.if.in[eth0,bytes"])/(last("net.if.in[eth0,bytes"])+last("net.if.out[eth0,bytes"]))
```

**Example 5**
Using aggregated items correctly within a calculated item.

Take note of how double quotes are escaped within the quoted key:

```
last("grpsum["video","net.if.out[eth0,bytes"]","last"]") / last("grpsum["video","nginx_stat.sh[active]]")
```
8 Internal checks

Overview

Internal checks allow to monitor the internal processes of Zabbix. In other words, you can monitor what goes on with Zabbix server or Zabbix proxy.

Internal checks are calculated:

• on Zabbix server - if the host is monitored by server
• on Zabbix proxy - if the host is monitored by proxy

Internal checks are processed by server or proxy regardless of host maintenance status (since Zabbix 2.4.0).

To use this item, choose the **Zabbix internal** item type.

**Note:**
Internal checks are processed by Zabbix pollers.

Supported checks

• Parameters without angle brackets are constants - for example, 'host' and 'available' in zabbix[host,<type>,available]. Use them in the item key as is.
• Values for items and item parameters that are “not supported on proxy” can only be gathered if the host is monitored by server. And vice versa, values “not supported on server” can only be gathered if the host is monitored by proxy.

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Return value</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>zabbix[boottime]</td>
<td>Startup time of Zabbix server or Zabbix proxy process in seconds.</td>
<td>Integer.</td>
<td></td>
</tr>
<tr>
<td>zabbix[history]</td>
<td>Number of values stored in the HISTORY table.</td>
<td>Integer.</td>
<td>Do not use if MySQL InnoDB, Oracle or PostgreSQL is used!</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(not supported on proxy)</td>
</tr>
<tr>
<td>zabbix[history_log]</td>
<td>Number of values stored in the HISTORY_LOG table.</td>
<td>Integer.</td>
<td>Do not use if MySQL InnoDB, Oracle or PostgreSQL is used!</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>This item is supported starting with Zabbix 1.8.3.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(not supported on proxy)</td>
</tr>
<tr>
<td>Key</td>
<td>Description</td>
<td>Type</td>
<td>Notes</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------</td>
<td>-------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>zabbix[history_text]</code></td>
<td>Number of values stored in the <code>HISTORY_TEXT</code> table.</td>
<td>Integer</td>
<td>Do not use if MySQL InnoDB, Oracle or PostgreSQL is used!</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>This item is supported starting with Zabbix 1.8.3. (not supported on proxy)</td>
</tr>
<tr>
<td><code>zabbix[history_uint]</code></td>
<td>Number of values stored in the <code>HISTORY_UINT</code> table.</td>
<td>Integer</td>
<td>Do not use if MySQL InnoDB, Oracle or PostgreSQL is used!</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>This item is supported starting with Zabbix 1.8.3. (not supported on proxy)</td>
</tr>
<tr>
<td><code>zabbix[host_items]</code></td>
<td>Number of enabled items (supported and not supported) on the host.</td>
<td>Integer</td>
<td>This item is supported starting with Zabbix 3.0.0.</td>
</tr>
<tr>
<td><code>zabbix[host_items_unsupported]</code></td>
<td>Number of enabled unsupported items on the host.</td>
<td>Integer</td>
<td>This item is supported starting with Zabbix 3.0.0.</td>
</tr>
<tr>
<td><code>zabbix[host_maintenance]</code></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key</td>
<td>Value</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>-------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Current maintenance status of a host.</td>
<td>0 - host in normal state, 1 - host in maintenance with data collection, 2 - host in maintenance without data collection.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This item is always processed by Zabbix server regardless of host location (on server or proxy). The proxy will not receive this item with configuration data. The second parameter must be empty and is reserved for future use. This item is supported starting with Zabbix 2.4.0. |

zabbix[host,discovery.interfaces] | Details of all configured interfaces of the host in Zabbix frontend. | JSON object. This item can be used in low-level discovery. This item is supported starting with Zabbix 3.4.0. (not supported on proxy) |

zabbix[host.<type>,available] | | |
Key

| Availability of a particular type of checks on the host. The value of this item corresponds to availability icons in the host list. | 0 - not available, 1 - available, 2 - unknown. | Valid types are: agent, snmp, ipmi, jmx. | The item value is calculated according to configuration parameters regarding host unreachability/unavailability. | This item is supported starting with Zabbix 2.0.0. |

| zabbix[hosts] | Number of monitored hosts. | Integer. | This item is supported starting with Zabbix 2.2.0. |

| zabbix[items] | Number of enabled items (supported and not supported). | Integer. |

| zabbix[items_unsupported] | Number of not supported items. | Integer. |

| zabbix[java_<param>] | | | | |
| Key | Information about Zabbix Java gateway. | If `<param>` is **ping**, "1" is returned. Can be used to check Java gateway availability using `nodata()` trigger function. | Valid values for `<param>` are: ping, version. 
Second parameter must be empty and is reserved for future use. |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>zabbix[preprocessing_queue]</td>
<td>Count of values enqueued in the preprocessing queue.</td>
<td>Integer. This item can be used to monitor the preprocessing queue length.</td>
</tr>
<tr>
<td></td>
<td>zabbix[process,&lt;type&gt;,&lt;mode&gt;,&lt;state&gt;]</td>
<td></td>
<td>This item is supported starting with Zabbix 3.4.0.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Key**

| Time a particular Zabbix process or a group of processes (identified by `<type>` and `<mode>` spent in `<state>` in percentage. It is calculated for the last minute only. If `<mode>` is Zabbix process number that is not running (for example, with 5 pollers running `<mode>` is specified to be 6), such an item will turn into unsupported state. Minimum and maximum refers to the usage percentage for a single process. So if in a group of 3 pollers usage percentages per process were 2, 18 and 66, min would return 2 and max would return 66. Processes report what they are doing in shared memory and the self-monitoring process summarizes that data. | Percentage of time. Float. | Supported types of server processes: alert manager, alerter, configuration syncer, discoverer, escalator, history syncer, housekeeper, http poller, icmp pinger, ipmi manager, ipmi poller, java poller, poller, pre-processing manager, pre-processing worker, proxy poller, self-monitoring, smtp trapper, task manager, timer, trapper, unreachable poller, vmware collector

Supported types of proxy processes: configuration syncer, data sender, discoverer, heartbeat sender, history syncer, housekeeper, http poller, icmp pinger, ipmi manager, ipmi poller, java poller, poller, self-monitoring, smtp trapper, task manager, timer, trapper, unreachable poller,
<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>zabbix[proxy,&lt;name&gt;,&lt;param&gt;]</td>
<td>Information about Zabbix proxy. Integer. &lt;name&gt; - proxy name List of supported parameters (&lt;param&gt;): lastaccess - timestamp of last heart beat message received from proxy Example: =&gt; zabbix[proxy,&quot;Germany&quot;,lastaccess] fuzzytime() function can be used to check availability of proxies. Starting with Zabbix 2.4.0 this item is always processed by Zabbix server regardless of host location (on server or proxy).</td>
</tr>
<tr>
<td>zabbix[proxy_history]</td>
<td>Number of values in the proxy history table waiting to be sent to the server. Integer. This item is supported starting with Zabbix 2.2.0. (not supported on server)</td>
</tr>
<tr>
<td>zabbix[queue,&lt;from&gt;,&lt;to&gt;]</td>
<td>Integer. <em>zabbix[proxy,&lt;name&gt;,&lt;param&gt;] Information about Zabbix proxy. Integer. &lt;name&gt; - proxy name List of supported parameters (&lt;param&gt;): lastaccess - timestamp of last heart beat message received from proxy Example: =&gt; zabbix[proxy,&quot;Germany&quot;,lastaccess] fuzzytime() function can be used to check availability of proxies. Starting with Zabbix 2.4.0 this item is always processed by Zabbix server regardless of host location (on server or proxy).</em>*</td>
</tr>
<tr>
<td></td>
<td>*zabbix[queue,&lt;from&gt;,&lt;to&gt;]</td>
</tr>
<tr>
<td>Key</td>
<td>Type</td>
</tr>
<tr>
<td>--------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Number of monitored items in the queue which are delayed at least by (&lt;from&gt;) seconds but less than by (&lt;to&gt;) seconds.</td>
<td>Integer</td>
</tr>
<tr>
<td>zabbix[rcache,(&lt;cache&gt;,(&lt;mode&gt;)]</td>
<td>Integer (for size); float (for percentage).</td>
</tr>
<tr>
<td>zabbix[requiredperformance]</td>
<td>Float</td>
</tr>
<tr>
<td>(\text{used} - \text{size of used buffer})</td>
<td></td>
</tr>
<tr>
<td>(\text{pused} - \text{percentage of used buffer})</td>
<td></td>
</tr>
</tbody>
</table>
zabbix[stats,<ip>,<port>]

Remote Zabbix server or proxy internal metrics.

JSON object.

- **ip**: IP/DNS/network mask list of servers/proxies to be remotely queried (default is 127.0.0.1)
- **port**: port of server/proxy to be remotely queried (default is 10051)

Note that the stats request will only be accepted from the addresses listed in the ‘StatsAllowedIP’ server/proxy parameter on the target instance.

A selected set of internal metrics is returned by this item. For details, see Remote monitoring of Zabbix stats.

Supported since 4.0.5.

zabbix[stats,<ip>,<port>,queue,<from>,<to>]
Remote Zabbix server or proxy internal queue metrics (see zabbix[queue,<from>,<to>]).

JSON object.

- **ip** - IP/DNS/network mask list of servers/proxies to be remotely queried (default is 127.0.0.1)
- **port** - port of server/proxy to be remotely queried (default is 10051)
- **from** - delayed by at least (default is 6 seconds)
- **to** - delayed by at most (default is infinity)

Note that the stats request will only be accepted from the addresses listed in the `StatsAllowedIP` server/proxy parameter on the target instance.

Supported since 4.0.5.

<p>| <code>zabbix[trends]</code> | Number of values stored in the TRENDS table. | Integer. Do not use if MySQL InnoDB, Oracle or PostgreSQL is used! (not supported on proxy) |</p>
<table>
<thead>
<tr>
<th>Key</th>
<th>Number of values stored in the TRENDS_UINT table.</th>
<th>Integer.</th>
<th>Do not use if MySQL InnoDB, Oracle or PostgreSQL is used! This item is supported starting with Zabbix <strong>1.8.3</strong>. (not supported on proxy)</th>
</tr>
</thead>
<tbody>
<tr>
<td>zabbix[triggers]</td>
<td>Number of enabled triggers in Zabbix database, with all items enabled on enabled hosts.</td>
<td>Integer.</td>
<td>(not supported on proxy)</td>
</tr>
<tr>
<td>zabbix[uptime]</td>
<td>Uptime of Zabbix server or Zabbix proxy process in seconds.</td>
<td>Integer.</td>
<td></td>
</tr>
<tr>
<td>zabbix[vcache,buffer,&lt;mode&gt;]</td>
<td>Availability statistics of Zabbix value cache.</td>
<td>Integer (for size); float (for percentage).</td>
<td>Mode: <strong>total</strong> - total size of buffer <strong>free</strong> - size of free buffer <strong>pfree</strong> - percentage of free buffer <strong>used</strong> - size of used buffer <strong>pused</strong> - percentage of used buffer</td>
</tr>
<tr>
<td>zabbix[vcache,cache,&lt;parameter&gt;]</td>
<td></td>
<td></td>
<td>This item is supported starting with Zabbix <strong>2.2.0</strong>. (not supported on proxy)</td>
</tr>
</tbody>
</table>
Effectiveness statistics of Zabbix value cache.

Integer.

With the **mode** parameter:
- **0** - normal mode,
- **1** - low memory mode

**Parameter:**
- **requests** - total number of requests
- **hits** - number of cache hits (history values taken from the cache)
- **misses** - number of cache misses (history values taken from the database)
- **mode** - value cache operating mode

This item is supported starting with Zabbix **2.2.0** and the **mode** parameter starting with Zabbix **3.0.0**.

(not supported on proxy)

Once the low memory mode has been switched on, the value cache will remain in this state for 24 hours, even if the problem that triggered this mode is resolved sooner.

You may use this key with the Change per second preprocessing step in order to get values per second statistics.
### Key

**zabbix[vmware,buffer,<mode>]**

<table>
<thead>
<tr>
<th>Availability</th>
<th>Mode</th>
<th>Supported from</th>
</tr>
</thead>
<tbody>
<tr>
<td>statistics of Zabbix</td>
<td><strong>total</strong> - total size of buffer</td>
<td>Zabbix 2.2.0.</td>
</tr>
<tr>
<td>vmware</td>
<td><strong>free</strong> - size of free buffer</td>
<td></td>
</tr>
<tr>
<td>cache.</td>
<td><strong>pfree</strong> - percentage of free buffer</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>used</strong> - size of used buffer</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>pused</strong> - percentage of used buffer</td>
<td></td>
</tr>
</tbody>
</table>

This item is supported starting with Zabbix 2.2.0.

---

**zabbix[wcache,<cache>,<mode>]**

<table>
<thead>
<tr>
<th>Statistics and availability of Zabbix write cache.</th>
<th>Mode</th>
<th>Specifying</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>all</strong> (default)</td>
<td>&lt;cache&gt; is</td>
</tr>
<tr>
<td></td>
<td><strong>Cache</strong> values</td>
<td>mandatory.</td>
</tr>
<tr>
<td></td>
<td><strong>Mode</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>total</strong></td>
<td>Counter.</td>
</tr>
<tr>
<td></td>
<td>Number of values</td>
<td>Counter.</td>
</tr>
<tr>
<td></td>
<td>processed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>by Zabbix</td>
<td></td>
</tr>
<tr>
<td></td>
<td>server or Zabbix</td>
<td></td>
</tr>
<tr>
<td></td>
<td>proxy, except</td>
<td></td>
</tr>
<tr>
<td></td>
<td>unsupported items.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>float</strong></td>
<td>Counter.</td>
</tr>
<tr>
<td></td>
<td>Number of</td>
<td>Counter.</td>
</tr>
<tr>
<td></td>
<td>processed</td>
<td>Counter.</td>
</tr>
<tr>
<td></td>
<td>float values.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>uint</strong></td>
<td>Counter.</td>
</tr>
<tr>
<td></td>
<td>Number of</td>
<td>Counter.</td>
</tr>
<tr>
<td></td>
<td>processed</td>
<td>Counter.</td>
</tr>
<tr>
<td></td>
<td>unsigned integer</td>
<td>Counter.</td>
</tr>
<tr>
<td></td>
<td>values.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>str</strong></td>
<td>Counter.</td>
</tr>
<tr>
<td></td>
<td>Number of</td>
<td>Counter.</td>
</tr>
<tr>
<td></td>
<td>processed</td>
<td>Counter.</td>
</tr>
<tr>
<td></td>
<td>character/string</td>
<td>Counter.</td>
</tr>
<tr>
<td></td>
<td>values.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>log</strong></td>
<td>Counter.</td>
</tr>
<tr>
<td></td>
<td>Number of</td>
<td>Counter.</td>
</tr>
<tr>
<td></td>
<td>processed</td>
<td>Counter.</td>
</tr>
<tr>
<td></td>
<td>log values.</td>
<td>Counter.</td>
</tr>
<tr>
<td></td>
<td><strong>text</strong></td>
<td>Counter.</td>
</tr>
<tr>
<td></td>
<td>Number of</td>
<td>Counter.</td>
</tr>
<tr>
<td></td>
<td>processed</td>
<td>Counter.</td>
</tr>
<tr>
<td></td>
<td>text values.</td>
<td>Counter.</td>
</tr>
<tr>
<td>Key</td>
<td>not supported</td>
<td>Number of times item processing resulted in item becoming unsupported or keeping that state.</td>
</tr>
<tr>
<td>-----</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>history</td>
<td>pfree (default)</td>
<td>Percentage of free history buffer.</td>
</tr>
<tr>
<td>free</td>
<td>Size of free history buffer.</td>
<td>Integer.</td>
</tr>
<tr>
<td>total</td>
<td>Total size of history buffer.</td>
<td>Integer.</td>
</tr>
<tr>
<td>used</td>
<td>Size of used history buffer.</td>
<td>Integer.</td>
</tr>
<tr>
<td>pused</td>
<td>Percentage of used history buffer.</td>
<td>Float.</td>
</tr>
<tr>
<td>index</td>
<td>pfree (default)</td>
<td>Percentage of free history index buffer.</td>
</tr>
<tr>
<td>free</td>
<td>Size of free history index buffer.</td>
<td>Integer.</td>
</tr>
<tr>
<td>total</td>
<td>Total size of history index buffer.</td>
<td>Integer.</td>
</tr>
<tr>
<td>used</td>
<td>Size of used history index buffer.</td>
<td>Integer.</td>
</tr>
</tbody>
</table>
### Key

<table>
<thead>
<tr>
<th>Trend</th>
<th>pused Percentage of used history index buffer.</th>
<th>Float.</th>
<th>pused mode is supported starting with Zabbix 4.0.0.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trend</td>
<td>pfree Percentage of free trend cache.</td>
<td>Float.</td>
<td>Trend cache stores aggregate for the current hour for all items that receive data. (not supported on proxy)</td>
</tr>
<tr>
<td>Free</td>
<td>Size of free trend buffer.</td>
<td>Integer.</td>
<td>(not supported on proxy)</td>
</tr>
<tr>
<td>Total</td>
<td>Total size of trend buffer.</td>
<td>Integer.</td>
<td>(not supported on proxy)</td>
</tr>
<tr>
<td>Used</td>
<td>Size of used trend buffer.</td>
<td>Integer.</td>
<td>(not supported on proxy)</td>
</tr>
<tr>
<td>Pused</td>
<td>Percentage of used trend buffer.</td>
<td>Float.</td>
<td>(not supported on proxy)</td>
</tr>
</tbody>
</table>

---

### 9 SSH checks

#### Overview

SSH checks are performed as agent-less monitoring. Zabbix agent is not needed for SSH checks.

To perform SSH checks Zabbix server must be initially configured with SSH2 support (libssh or libssh2). See also: Requirements.

**Attention:**
Starting with RHEL/CentOS 8, only libssh is supported. libssh is supported by Zabbix since 4.0.18.

#### Configuration

**Passphrase authentication**

SSH checks provide two authentication methods - a user/password pair and key-file based.

If you do not intend to use keys, no additional configuration is required, besides linking libssh or libssh2 to Zabbix, if you’re building from source.

**Key file authentication**

To use key based authentication for SSH items, certain changes to the server configuration are required.

Open the Zabbix server configuration file (`zabbix_server.conf`) as root and look for the following line:

```
#### SSHKeyLocation=
```

Uncomment it and set the full path to the folder where the public and private keys will be located:
SSHKeyLocation=/home/zabbix/.ssh

Save the file and restart Zabbix server afterwards.

The path /home/zabbix here is the home directory for the zabbix user account, and .ssh is a directory where by default public and private keys will be generated by an ssh-keygen command inside the home directory.

Usually installation packages of Zabbix server from different OS distributions create the zabbix user account with a home directory elsewhere, for example, /var/lib/zabbix (as for system accounts).

Before generating the keys, you could reallocate the home directory to /home/zabbix, so that it corresponds with the SSHKeyLocation Zabbix server configuration parameter mentioned above.

Note:
The following steps can be skipped if zabbix account has been added manually according to the installation section. In such a case the home directory for the zabbix account is most likely already /home/zabbix.

To change the home directory of the zabbix user account, all working processes which are using it have to be stopped:

```
service zabbix-agent stop
service zabbix-server stop
```

To change the home directory location with an attempt to move it (if it exists) the following command should be executed:

```
usermod -m -d /home/zabbix zabbix
```

It is also possible that a home directory did not exist in the old location (e.g., in the CentOS), so it should be created at the new location. A safe attempt to do that is:

```
test -d /home/zabbix || mkdir /home/zabbix
```

To be sure that all is secure, additional commands could be executed to set permissions to the home directory:

```
chown zabbix:zabbix /home/zabbix
chmod 700 /home/zabbix
```

Previously stopped processes can now be started again:

```
service zabbix-agent start
service zabbix-server start
```

Now, the steps to generate the public and private keys can be performed with the following commands (for better readability, command prompts are commented out):

```
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 o |
 |+ . S |
 |.+ o = |
 |E . * = |
 |o =o ..* . |
 |... oo.o+ |
##### +-----------------+
```

282
Note:
The public and private keys (id_rsa.pub and id_rsa) have been generated by default in the /home/zabbix/.ssh directory, which corresponds to the Zabbix server SSHKeyLocation configuration parameter.

Attention:
Key types other than "rsa" may be supported by the ssh-keygen tool and SSH servers but they may not be supported by libssh2 used by Zabbix.

Shell configuration form

This step should be performed only once for every host that will be monitored by SSH checks.

By using the following commands, the public key file can be installed on a remote host 10.10.10.10, so that the SSH checks can be performed with a root account (for better readability, command prompts are commented out):

```
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.
##### 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:
##### 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.
```

Now it is possible to check the SSH login using the default private key (/home/zabbix/.ssh/id_rsa) for the zabbix user account:

```
sudo -u zabbix ssh root@10.10.10.10
```

If the login is successful, then the configuration part in the shell is finished and the remote SSH session can be closed.

Item configuration

Actual command(s) to be executed must be placed in the Executed script field in the item configuration. Multiple commands can be executed one after another by placing them on a new line. In this case returned values will also be formatted as multilined.

```
* Name: SSH test check (without passphrase)
* Type: SSH agent
* Host interface: 10.10.10.10:10050
* Format: Public key
* User name: root
* Public key file: id_rsa.pub
* Private key file: id_rsa
* Key passphrase:
* Executed script: service mysql-server status
  service mysql-server restart

Type of information: Text
* Update interval: 30s
```

All mandatory input fields are marked with a red asterisk.
The fields that require specific information for SSH items are:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select <strong>SSH agent</strong> here.</td>
<td>&lt;unique short description&gt; is required and should be unique for all SSH items per host.</td>
</tr>
<tr>
<td>Key</td>
<td>Unique (per host) item key in format <code>ssh.run[&lt;unique short description&gt;,&lt;ip&gt;,&lt;port&gt;,&lt;encoding&gt;]</code></td>
<td>Default port is 22, not the port specified in the interface to which this item is assigned.</td>
</tr>
<tr>
<td>Authentication method</td>
<td>One of the &quot;Password&quot; or &quot;Public key&quot;.</td>
<td></td>
</tr>
<tr>
<td>User name</td>
<td>User name to authenticate on remote host. Required.</td>
<td></td>
</tr>
<tr>
<td>Public key file</td>
<td>File name of public key if Authentication method is &quot;Public key&quot;. Required.</td>
<td>Example: <code>id_rsa.pub</code> - default public key file name generated by a command <code>ssh-keygen</code>.</td>
</tr>
<tr>
<td>Private key file</td>
<td>File name of private key if Authentication method is &quot;Public key&quot;. Required.</td>
<td>Example: <code>id_rsa</code> - default private key file name.</td>
</tr>
<tr>
<td>Password or Key passphrase</td>
<td>Password to authenticate or Empty if passphrase was not used.</td>
<td>Leave the Key passphrase field empty if passphrase was not used.</td>
</tr>
<tr>
<td>Executed script</td>
<td>Executed shell command(s) using SSH remote session.</td>
<td>Examples: <code>date +%s</code> <code>service mysql-server status</code> `ps auxww</td>
</tr>
</tbody>
</table>

**Attention:**
libssh2 library may truncate executable scripts to ~32kB.

### 10 Telnet checks

**Overview**
Telnet checks are performed as agent-less monitoring. Zabbix agent is not needed for Telnet checks.

**Configurable fields**
Actual command(s) to be executed must be placed in the **Executed script** field in the item configuration.
Multiple commands can be executed one after another by placing them on a new line. In this case returned value also will be formatted as multi-lined.

Supported characters that the shell prompt can end with:

- `$`
- `#`
- `*`
- `%`

**Note:**
A telnet prompt line which ended with one of these characters will be removed from the returned value, but only for the first command in the commands list, i.e. only at a start of the telnet session.

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>telnet.run[&lt;unique short description&gt;,&lt;ip&gt;,&lt;port&gt;,&lt;encoding&gt;]</code></td>
<td>a command on a remote device using telnet connection</td>
<td></td>
</tr>
</tbody>
</table>
Attention:
If a telnet check returns a value with non-ASCII characters and in non-UTF8 encoding then the <encoding> parameter of the key should be properly specified. See encoding of returned values page for more details.

11 External checks

Overview
External check is a check executed by Zabbix server by running a shell script or a binary. However, when hosts are monitored by a Zabbix proxy, the external checks are executed by the proxy.
External checks do not require any agent running on a host being monitored.
The syntax of the item key is:
`script[<parameter1>,<parameter2>,...]`
Where:

<table>
<thead>
<tr>
<th>ARGUMENT</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>script</td>
<td>Name of a shell script or a binary.</td>
</tr>
<tr>
<td>parameter(s)</td>
<td>Optional command line parameters.</td>
</tr>
</tbody>
</table>

If you don’t want to pass any parameters to the script you may use:

`script[]` or `script`

Zabbix server will look in the directory defined as the location for external scripts (parameter ‘ExternalScripts’ in Zabbix server configuration file) and execute the command. The command will be executed as the user Zabbix server runs as, so any access permissions or environment variables should be handled in a wrapper script, if necessary, and permissions on the command should allow that user to execute it. Only commands in the specified directory are available for execution.

Warning:
Do not overuse external checks! As each script requires starting a fork process by Zabbix server, running many scripts can decrease Zabbix performance a lot.

Usage example
Executing the script `check_oracle.sh` with the first parameters `-h`. The second parameter will be replaced by IP address or DNS name, depending on the selection in the host properties.
`check_oracle.sh["-h","{HOST.CONN}"]`
Assuming host is configured to use IP address, Zabbix will execute:
`check_oracle.sh '-h' '192.168.1.4'`

External check result
The return value of the check is standard output together with standard error (the full output with trimmed trailing whitespace is returned since Zabbix 2.0).

Attention:
A text (character, log or text type of information) item will not become unsupported in case of standard error output.

In case the requested script is not found or Zabbix server has no permissions to execute it, the item will become unsupported and corresponding error message will be set. In case of a timeout, the item will be marked as unsupported as well, an according error message will be displayed and the forked process for the script will be killed.

12 Aggregate checks

Overview
In aggregate checks Zabbix server collects aggregate information from items by doing direct database queries.
Aggregate checks do not require any agent running on the host being monitored.

Syntax
The syntax of the aggregate item key is:

\[ \text{groupfunc["host group","item key",itemfunc,timeperiod]} \]

Supported group functions (groupfunc) are:

<table>
<thead>
<tr>
<th>Group function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>grpavg</td>
<td>Average value</td>
</tr>
<tr>
<td>grpmax</td>
<td>Maximum value</td>
</tr>
<tr>
<td>grpmin</td>
<td>Minimum value</td>
</tr>
<tr>
<td>grpsum</td>
<td>Sum of values</td>
</tr>
</tbody>
</table>

Multiple host groups may be included by inserting a comma-delimited array. Specifying a parent host group will include the parent group and all nested host groups with their items.

All items that are referenced from the aggregate item key must exist and be collecting data. Only enabled items on enabled hosts are included in the calculations.

**Attention:**
The key of the aggregate item must be updated manually, if the item key of a referenced item is changed.

Supported item functions (itemfunc) are:

<table>
<thead>
<tr>
<th>Item function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>avg</td>
<td>Average value</td>
</tr>
<tr>
<td>count</td>
<td>Number of values</td>
</tr>
<tr>
<td>last</td>
<td>Last value</td>
</tr>
<tr>
<td>max</td>
<td>Maximum value</td>
</tr>
<tr>
<td>min</td>
<td>Minimum value</td>
</tr>
<tr>
<td>sum</td>
<td>Sum of values</td>
</tr>
</tbody>
</table>

The `timeperiod` parameter specifies a time period of latest collected values. **Supported unit symbols** can be used in this parameter for convenience, for example ‘5m’ (minutes) instead of ‘300’ (seconds) or ‘1d’ (day) instead of ‘86400’ (seconds).

**Warning:**
An amount of values (prefixed with #) is not supported in the timeperiod.

Timeperiod is ignored by the server if the third parameter (item function) is last and can thus be omitted:

\[ \text{groupfunc["host group","item key",last]} \]

**Note:**
If the aggregate results in a float value it will be trimmed to an integer if the aggregated item type of information is Numeric (unsigned).

An aggregate item may become unsupported if:

- none of the referenced items is found (which may happen if the item key is incorrect, none of the items exist or all included groups are incorrect)
- no data to calculate a function

Usage examples
Examples of keys for aggregate checks:

**Example 1**
Total disk space of host group ‘MySQL Servers’.

\[ \text{grpsum["MySQL Servers","vfs.fs.size[/,total]",last]} \]
Example 2
Average processor load of host group 'MySQL Servers'.
grpavg["MySQL Servers","system.cpu.load[,avg1]",last]

Example 3
5-minute average of the number of queries per second for host group 'MySQL Servers'.
grpavg["MySQL Servers",mysql.qps,avg,5m]

Example 4
Average CPU load on all hosts in multiple host groups.
grpavg["Servers A","Servers B","Servers C"],system.cpu.load,last]

13 Trapper items

Overview
Trapper items accept incoming data instead of querying for it.
It is useful for any data you might want to “push” into Zabbix.

To use a trapper item you must:
• have a trapper item set up in Zabbix
• send in the data into Zabbix

Configuration
Item configuration
To configure a trapper item:
• Go to: Configuration → Hosts
• Click on Items in the row of the host
• Click on Create item
• Enter parameters of the item in the form

All mandatory input fields are marked with a red asterisk.
The fields that require specific information for trapper items are:

<table>
<thead>
<tr>
<th>Type</th>
<th>Select Zabbix trapper here.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key</td>
<td>Enter a key that will be used to recognize the item when sending in data.</td>
</tr>
<tr>
<td>Type of information</td>
<td>Select the type of information that will correspond the format of data that will be sent in.</td>
</tr>
</tbody>
</table>
Allowed hosts

List of comma delimited IP addresses, optionally in CIDR notation, or DNS names.
If specified, incoming connections will be accepted only from the hosts listed here.
If IPv6 support is enabled then ‘127.0.0.1’, ‘::127.0.0.1’, ‘::ffff:127.0.0.1’ are treated equally and ‘::/0’ will allow any IPv4 or IPv6 address.
‘0.0.0.0/0’ can be used to allow any IPv4 address.
Note, that “IPv4-compatible IPv6 addresses” (0000::/96 prefix) are supported but deprecated by RFC4291.
Example: 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}
Spaces and user macros are allowed in this field since Zabbix 2.2.0.
Host macros {HOST.HOST}, {HOST.NAME}, {HOST.IP}, {HOST.DNS}, {HOST.CONN} are allowed in this field since Zabbix 4.0.2.

Note:
You may have to wait up to 60 seconds after saving the item until the server picks up the changes from a configuration cache update, before you can send in values.

Sending in data

In the simplest of cases, we may use zabbix_sender utility to send in some 'test value':

```
zabbix_sender -z <server IP address> -p 10051 -s "New host" -k trap -o "test value"
```

To send in the value we use these keys:
- `-z` - to specify Zabbix server IP address
- `-p` - to specify Zabbix server port number (10051 by default)
- `-s` - to specify the host (make sure to use the 'technical' host name here, instead of the 'visible' name)
- `-k` - to specify the key of the item we just defined
- `-o` - to specify the actual value to send

Attention:
Zabbix trapper process does not expand macros used in the item key in attempt to check corresponding item key existence for targeted host.

Display

This is the result in Monitoring → Latest data:

<table>
<thead>
<tr>
<th>HOST</th>
<th>NAME</th>
<th>LAST CHECK</th>
<th>LAST VALUE</th>
<th>CHANGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>New host</td>
<td>Trapper item</td>
<td>2015-08-11 18:50:53</td>
<td>test value</td>
<td>History</td>
</tr>
</tbody>
</table>

Note that if a single numeric value is sent in, the data graph will show a horizontal line to the left and to the right of the time point of the value.

14 JMX monitoring

Overview

JMX monitoring can be used to monitor JMX counters of a Java application.

JMX monitoring has native support in Zabbix in the form of a Zabbix daemon called “Zabbix Java gateway”, introduced since Zabbix 2.0.
To retrieve the value of a particular JMX counter on a host, Zabbix server queries the Zabbix Java gateway, which in turn uses the JMX management API to query the application of interest remotely.

For more details and setup see the Zabbix Java gateway section.

**Warning:**
Communication between Java gateway and the monitored JMX application should not be firewalled.

Enabling remote JMX monitoring for Java application

A Java application does not need any additional software installed, but it needs to be started with the command-line options specified below to have support for remote JMX monitoring.

As a bare minimum, if you just wish to get started by monitoring a simple Java application on a local host with no security enforced, start it with these options:

```bash
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 /usr/share/doc/openjdk-6-jre-headless/demo/jfc/Notepad/Notepad.jar
```

This makes Java listen for incoming JMX connections on port 12345, from local host only, and tells it not to require authentication or SSL.

If you want to allow connections on another interface, set the -Djava.rmi.server.hostname parameter to the IP of that interface.

If you wish to be more stringent about security, there are many other Java options available to you. For instance, the next example starts the application with a more versatile set of options and opens it to a wider network, not just local host.

```bash
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 /usr/share/doc/openjdk-6-jre-headless/demo/jfc/Notepad/Notepad.jar
```

Most (if not all) of these settings can be specified in /etc/java-6-openjdk/management/management.properties (or wherever that file is on your system).

Note that if you wish to use SSL, you have to modify startup.sh script by adding -Djavax.net.ssl.* options to Java gateway, so that it knows where to find key and trust stores.

See Monitoring and Management Using JMX for a detailed description.

Configuring JMX interfaces and items in Zabbix frontend

With Java gateway running, server knowing where to find it and a Java application started with support for remote JMX monitoring, it is time to configure the interfaces and items in Zabbix GUI.

Configuring JMX interface

You begin by creating a JMX-type interface on the host of interest.
All mandatory input fields are marked with a red asterisk.

Adding JMX agent item

For each JMX counter you are interested in you add **JMX agent** item attached to that interface.

The key in the screenshot below says `jmx["java.lang:type=Memory","HeapMemoryUsage.used"]`. 
All mandatory input fields are marked with a red asterisk.

The fields that require specific information for JMX items are:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Used heap memory</td>
</tr>
<tr>
<td>Type</td>
<td>JMX agent</td>
</tr>
<tr>
<td>* Key</td>
<td><code>jmx[&quot;Java_lang:type=Memory&quot;,&quot;HeapMemoryUsage.used&quot;]</code></td>
</tr>
<tr>
<td>* Host interface</td>
<td>127.0.0.1 : 12245</td>
</tr>
<tr>
<td>* JMX endpoint</td>
<td>service:jmxrmi://jpdmi/[HOST:PORT]:jmxmri</td>
</tr>
<tr>
<td>User name</td>
<td>[JMX_USERNAME]</td>
</tr>
<tr>
<td>Password</td>
<td>[JMX_USERNAME]</td>
</tr>
<tr>
<td>Type of information</td>
<td>Numeric (unsigned)</td>
</tr>
<tr>
<td>Units</td>
<td></td>
</tr>
<tr>
<td>* Update interval</td>
<td>30s</td>
</tr>
</tbody>
</table>

Custom intervals:

<table>
<thead>
<tr>
<th>Type</th>
<th>Interval</th>
<th>Period</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flexible</td>
<td>50s</td>
<td>1.7.00.00-24.00</td>
<td>Remove</td>
</tr>
</tbody>
</table>

* History storage period | 90d
* Trend storage period | 365d

Show value: As is, show value mappings

New application: None

Applications: None

Populates host inventory field: None

Description

Enabled

Set **JMX agent** here.
The `jmx[]` item key contains two parameters:
- **object name** - the object name of an MBean;
- **attribute name** - an MBean attribute name with optional composite data field names separated by dots.

See below for more detail on JMX item keys.
Since Zabbix 3.4, you may discover MBeans and MBean attributes using a `jmx.discovery[]` low-level discovery item.
JMX endpoint
You may specify a custom JMX endpoint. Make sure that JMX endpoint connection parameters match the JMX interface. This can be achieved by using {HOST.*) macros as done in the default JMX endpoint.
This field is supported since 3.4.0. {HOST.*) macros and user macros are supported.

User Name
Specify the user name, if you have configured authentication on your Java application.
User macros are supported.

Password
Specify the password, if you have configured authentication on your Java application.
User macros are supported.

If you wish to monitor a Boolean counter that is either "true" or "false", then you specify type of information as "Numeric (unsigned)" and select "Boolean to decimal" preprocessing step in the Preprocessing tab. Server will store Boolean values as 1 or 0, respectively.

JMX item keys in more detail

Simple attributes
An MBean object name is nothing but a string which you define in your Java application. An attribute name, on the other hand, can be more complex. In case an attribute returns primitive data type (an integer, a string etc.) there is nothing to worry about, the key will look like this:
```
jmx[com.example:Type=Hello,weight]
```
In this example the object name is "com.example:Type=Hello", the attribute name is "weight", and the returned value type should probably be "Numeric (float)".

Attributes returning composite data
It becomes more complicated when your attribute returns composite data. For example: your attribute name is "apple" and it returns a hash representing its parameters, like "weight", "color" etc. Your key may look like this:
```
jmx[com.example:Type=Hello,apple.weight]
```
This is how an attribute name and a hash key are separated, by using a dot symbol. Same way, if an attribute returns nested composite data the parts are separated by a dot:
```
jmx[com.example:Type=Hello,fruits.apple.weight]
```

Problem with dots
So far so good. But what if an attribute name or a hash key contains dot symbol? Here is an example:
```
jmx[com.example:Type=Hello,all.fruits.apple.weight]
```
That’s a problem. How to tell Zabbix that attribute name is “all.fruits”, not just “all”? How to distinguish a dot that is part of the name from the dot that separates an attribute name and hash keys?

Before 2.0.4 Zabbix java gateway was unable to handle such situations and users were left with UNSUPPORTED items. Since 2.0.4 this is possible, all you need to do is to escape the dots that are part of the name with a backslash:
```
jmx[com.example:Type=Hello,all\.fruits.apple.weight]
```
Same way, if your hash key contains a dot you escape it:
```
jmx[com.example:Type=Hello,all\.fruits.apple.total\.weight]
```

Other issues
A backslash character in an attribute name should be escaped:
```
jmx[com.example:type=Hello,c:\\documents]
```
For handling any other special characters in JMX item key, please see the item key format section.

This is actually all there is to it. Happy JMX monitoring!

Non-primitive data types
Since Zabbix 4.0.0 it is possible to work with custom MBeans returning non-primitive data types, which override the toString() method.
Custom endpoint example with JBoss EAP 6.4

Custom endpoints allow working with different transport protocols other than the default RMI.

To illustrate this possibility, let’s try to configure JBoss EAP 6.4 monitoring as an example. First, let’s make some assumptions:

- You have already installed Zabbix Java gateway. If not, then you can do it in accordance with the documentation.
- Zabbix server and Java gateway are installed with the prefix /usr/local/
- JBoss is already installed in /opt/jboss-eap-6.4/ and is running in standalone mode
- We shall assume that all these components work on the same host
- Firewall and SELinux are disabled (or configured accordingly)

Let’s make some simple settings in zabbix_server.conf:

JavaGateway=127.0.0.1
StartJavaPollers=5

And in the zabbix_java/settings.sh configuration file (or zabbix_java_gateway.conf):

START_POLLERS=5

Check that JBoss listens to its standard management port:

$ netstat -natp | grep 9999
 tcp  0 0 127.0.0.1:9999 0.0.0.0:* LISTEN 10148/java

Now let’s create a host with JMX interface 127.0.0.1:9999 in Zabbix.

As we know that this version of JBoss uses the JBoss Remoting protocol instead of RMI, we may mass update the JMX endpoint parameter in our JMX template accordingly:

service:jmx:remoting-jmx://{HOST.CONN}:{HOST.PORT}
Let’s update the configuration cache:

```
$ /usr/local/sbin/zabbix_server -R config_cache_reload
```

Note that you may encounter an error first.

"Unsupported protocol: remoting-jmx" means that Java gateway does not know how to work with the specified protocol. That can be fixed by creating a `~/needed_modules.txt` file with the following content:

```
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
```

and then executing the command:

```
$ for i in $(cat ~/needed_modules.txt); do find /opt/jboss-eap-6.4 -iname "${i}*.jar" -exec cp '{}' /usr/local/sbin/zabbix_java/lib/ \;
```

Thus, Java gateway will have all the necessary modules for working with jmx-remoting. What’s left is to restart the Java gateway, wait a bit and if you did everything right, see that JMX monitoring data begin to arrive in Zabbix:
15 ODBC monitoring

Overview

ODBC monitoring corresponds to the Database monitor item type in the Zabbix frontend.

ODBC is a C programming language middle-ware API for accessing database management systems (DBMS). The ODBC concept was developed by Microsoft and later ported to other platforms.

Zabbix may query any database, which is supported by ODBC. To do that, Zabbix does not directly connect to the databases, but uses the ODBC interface and drivers set up in ODBC. This function allows for more efficient monitoring of different databases for multiple purposes - for example, checking specific database queues, usage statistics and so on. Zabbix supports unixODBC, which is one of the most commonly used open source ODBC API implementations.

Attention:
See also the known issues for ODBC checks.

Installing unixODBC

The suggested way of installing unixODBC is to use the Linux operating system default package repositories. In the most popular Linux distributions unixODBC is included in the package repository by default. If it's not available, it can be obtained at the unixODBC homepage: http://www.unixodbc.org/download.html.

Installing unixODBC on RedHat/Fedora based systems using the yum package manager:

shell> yum -y install unixODBC unixODBC-devel

Installing unixODBC on SUSE based systems using the zypper package manager:

# zypper in unixODBC-devel

Note:
The unixODBC-devel package is needed to compile Zabbix with unixODBC support.

Installing unixODBC drivers

A unixODBC database driver should be installed for the database, which will be monitored. unixODBC has a list of supported databases and drivers: http://www.unixodbc.org/drivers.html. In some Linux distributions database drivers are included in package repositories. Installing MySQL database driver on RedHat/Fedora based systems using the yum package manager:

shell> yum install mysql-connector-odbc

Installing MySQL database driver on SUSE based systems using the zypper package manager:

zypper in MyODBC-unixODBC
Configuring unixODBC

ODBC configuration is done by editing the `odbcinst.ini` and `odbc.ini` files. To verify the configuration file location, type:

```
shell> odbcinst -j
```

**odbcinst.ini** is used to list the installed ODBC database drivers:

```
=mysql
Description = ODBC for MySQL
Driver = /usr/lib/libmyodbc5.so
```

Parameter details:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mysql</td>
<td>Database driver name.</td>
</tr>
<tr>
<td>Description</td>
<td>Database driver description.</td>
</tr>
<tr>
<td>Driver</td>
<td>Database driver library location.</td>
</tr>
</tbody>
</table>

**odbc.ini** is used to define data sources:

```
[test]
Description = MySQL test database
Driver = mysql
Server = 127.0.0.1
User = root
Password =
Port = 3306
Database = zabbix
```

Parameter details:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>test</td>
<td>Data source name (DSN).</td>
</tr>
<tr>
<td>Description</td>
<td>Data source description.</td>
</tr>
<tr>
<td>Driver</td>
<td>Database driver name - as specified in odbcinst.ini</td>
</tr>
<tr>
<td>Server</td>
<td>Database server IP/DNS.</td>
</tr>
<tr>
<td>User</td>
<td>Database user for connection.</td>
</tr>
<tr>
<td>Password</td>
<td>Database user password.</td>
</tr>
<tr>
<td>Port</td>
<td>Database connection port.</td>
</tr>
<tr>
<td>Database</td>
<td>Database name.</td>
</tr>
</tbody>
</table>

To verify if ODBC connection is working successfully, a connection to database should be tested. That can be done with the `isql` utility (included in the unixODBC package):

```
shell> isql test
+---------------------------------------+
| Connected! | | 
|           | | 
| sql-statement | | 
| help [tablename] | | 
| quit | | 
|     | | 
+---------------------------------------+
SQL>
```

Compiling Zabbix with ODBC support

To enable ODBC support, Zabbix should be compiled with the following flag:

```
--with-unixodbc[=ARG] use odbc driver against unixODBC package
```

**Note:**

See more about Zabbix installation from the source code.

Item configuration in Zabbix frontend
Configure a database monitoring item.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>MySQL host count</td>
</tr>
<tr>
<td>Type</td>
<td>Database monitor</td>
</tr>
<tr>
<td>Key</td>
<td><code>db.odbc.select[unique_description,data_source_name]</code></td>
</tr>
<tr>
<td>User name</td>
<td>zabbix</td>
</tr>
<tr>
<td>* SQL query</td>
<td><code>select count(*) from hosts</code></td>
</tr>
<tr>
<td>* Key</td>
<td><code>db.odbc.select[unique_description,data_source_name]</code></td>
</tr>
<tr>
<td>Password</td>
<td></td>
</tr>
<tr>
<td>Type of information</td>
<td>Numeric (unsigned)</td>
</tr>
</tbody>
</table>

All mandatory input fields are marked with a red asterisk.

Specifically for database monitoring items you must enter:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select Database monitor here. Enter <code>db.odbc.select[unique_description,data_source_name]</code>. The unique description will serve to identify the item in triggers etc. The data source name (DSN) must be set as specified in odbc.ini.</td>
</tr>
<tr>
<td>Key</td>
<td>Enter the database user name (optional if user is specified in odbc.ini)</td>
</tr>
<tr>
<td>User name</td>
<td>Enter the database user name (optional if user is specified in odbc.ini)</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the database user password (optional if password is specified in odbc.ini)</td>
</tr>
<tr>
<td>SQL query</td>
<td>Enter the SQL query</td>
</tr>
<tr>
<td>Type of information</td>
<td>It is important to know what type of information will be returned by the query, so that it is selected correctly here. With an incorrect type of information the item will turn unsupported.</td>
</tr>
</tbody>
</table>

Important notes

- Zabbix does not limit the query execution time. It is up to the user to choose queries that can be executed in a reasonable amount of time.
- The Timeout parameter value from Zabbix server is used as the ODBC login timeout (note that depending on ODBC drivers the login timeout setting might be ignored).
- The query must return one value only.
- If a query returns more than one column, only the first column is read.
- If a query returns more than one line, only the first line is read.
- The SQL command must return a result set like any query with `select ...`. The query syntax will depend on the RDBMS which will process them. The syntax of request to a storage procedure must be started with `call` keyword.

Error messages

ODBC error messages are structured into fields to provide detailed information. For example:

```
Cannot execute ODBC query: [SQL_ERROR]:[42601][7][ERROR: syntax error at or near ";"; Error while executing
```

Native error code     Native error message
Note that the error message length is limited to 2048 bytes, so the message can be truncated. If there is more than one ODBC diagnostic record Zabbix tries to concatenate them (separated with |) as far as the length limit allows.

1 Recommended UnixODBC settings for MySQL

Installation

*** Red Hat Enterprise Linux/CentOS***:

# yum install mysql-connector-odbc

***Debian/Ubuntu***:

Please refer to MySQL documentation to download necessary database driver for the corresponding platform.

For some additional information please refer to: installing unixODBC.

Configuration

ODBC configuration is done by editing odbcinst.ini and odbc.ini files. These configuration files can be found in /etc folder. The file odbcinst.ini may be missing and in this case it is necessary to create it manually.

odbcinst.ini

[mysql]
Description = General ODBC for MySQL
Driver = /usr/lib64/libmyodbc5.so
Setup = /usr/lib64/libodbcmyS.so
FileUsage = 1

Please consider the following examples of odbc.ini configuration parameters.

- An example with a connection through an IP:

  [TEST_MYSQL]
  Description = MySQL database 1
  Driver = mysql
  Port = 3306
  Server = 127.0.0.1

- An example with a connection through an IP and with the use of credentials. A Zabbix database is used by default:

  [TEST_MYSQL_FILLED_CRED]
  Description = MySQL database 2
  Driver = mysql
  User = root
  Port = 3306
  Password = zabbix
  Database = zabbix
  Server = 127.0.0.1

- An example with a connection through a socket and with the use of credentials. A Zabbix database is used by default:

  [TEST_MYSQL_FILLED_CRED_SOCK]
  Description = MySQL database 3
  Driver = mysql
  User = root
  Password = zabbix
  Socket = /var/run/mysqld/mysqld.sock
  Database = zabbix

All other possible configuration parameter options can be found in MySQL official documentation web page.

2 Recommended UnixODBC settings for PostgreSQL
Installation

• **Red Hat Enterprise Linux/CentOS**:

  # yum install postgresql-odbc

• **Debian/Ubuntu**:

  Please refer to PostgreSQL documentation to download necessary database driver for the corresponding platform.

  For some additional information please refer to: installing unixODBC.

Configuration

ODBC configuration is done by editing the odbcinst.ini and odbc.ini files. These configuration files can be found in /etc folder. The file odbcinst.ini may be missing and in this case it is necessary to create it manually.

Please consider the following examples:

**odbcinst.ini**

```
[postgresql]
Description = General ODBC for PostgreSQL
Driver = /usr/lib64/libodbcpsql.so
Setup = /usr/lib64/libodbcpsqlS.so
FileUsage = 1
# Since 1.6 if the driver manager was built with thread support you may add another entry to each driver entry.
# This entry alters the default thread serialization level.
Threading = 2
```

**odbc.ini**

```
[Test_PSQL]
Description = PostgreSQL database 1
Driver = postgresql
#ifdefLog = /tmp/sql.log
Username = zbx_test
Password = zabbix
# Name of Server. IP or DNS
Servername = 127.0.0.1
# Database name
Database = zabbix
# Postmaster listening port
Port = 5432
# Database is read only
ReadOnly = No
# PostgreSQL backend protocol
# Note that when using SSL connections this setting is ignored.
# 7.4+: Use the 7.4(V3) protocol. This is only compatible with 7.4 and higher backends.
Protocol = 7.4+
# Includes the OID in SQLColumns
ShowOidColumn = No
# Fakes a unique index on OID
FakeOidIndex = No
# Row Versioning
# Allows applications to detect whether data has been modified by other users
# while you are attempting to update a row.
RowVersioning = No
# Show SystemTables
# The driver will treat system tables as regular tables in SQLTables. This is good for Access so you can see system tables.
ShowSystemTables = No
# If true, the driver automatically uses declare cursor/fetch to handle SELECT statements and keeps 100 rows in cache.
Fetch = Yes
# Bools as Char
# Bools are mapped to SQL_CHAR, otherwise to SQL_BIT.
BoolsAsChar = Yes
# SSL mode
```
SSLmode = Require
# Send to backend on connection
ConnSettings =

3 Recommended UnixODBC settings for Oracle

Installation

Please refer to Oracle documentation for all the necessary instructions.

For some additional information please refer to: Installing unixODBC.

4 Recommended UnixODBC settings for MSSQL

Installation

• **Red Hat Enterprise Linux/CentOS**:
  # yum -y install freetds unixODBC
• **Debian/Ubuntu**:
  Please refer to FreeTDS user guide to download necessary database driver for the corresponding platform.

For some additional information please refer to: installing unixODBC.

Configuration

ODBC configuration is done by editing the odbcinst.ini and odbc.ini files. These configuration files can be found in /etc folder. The file odbcinst.ini may be missing and in this case it is necessary to create it manually.

Please consider the following examples:

**odbcinst.ini**

$ vi /etc/odbcinst.ini
[FreeTDS]
Driver = /usr/lib64/libtdsodbc.so.0

**odbc.ini**

$ vi /etc/odbc.ini
[sql1]
Driver = FreeTDS
Server = <SQL server 1 IP>
PORT = 1433
TDS_Version = 8.0

16 Dependent items

Overview

There are situations when one item gathers multiple metrics at a time or it even makes more sense to collect related metrics simultaneously, for example:

• CPU utilization of individual cores
• Incoming/outgoing/total network traffic

To allow for bulk metric collection and simultaneous use in several related items, Zabbix supports dependent items. Dependent items depend on the master item that collects their data simultaneously, in one query. A new value for the master item automatically populates the values of the dependent items. Dependent items cannot have a different update interval than the master item.

Zabbix preprocessing options can be used to extract the part that is needed for the dependent item from the master item data.

Preprocessing is managed by a preprocessing manager process, which has been added in Zabbix 3.4, along with workers that perform the preprocessing steps. All values (with or without preprocessing) from different data gatherers pass through the preprocessing manager before being added to the history cache. Socket-based IPC communication is used between data gatherers (pollers, trappers, etc) and the preprocessing process.
Only Zabbix server is performing preprocessing steps and is processing dependent items.

Item of any type, even dependent item, can be set as master item. Additional levels of dependent items can be used to extract smaller parts from the value of an existing dependent item.

Limitations

• Only same host (template) dependencies are allowed
• An item prototype can depend on another item prototype or regular item from the same host
• Maximum count of dependent items for one master item is limited to 999 (regardless of the number of dependency levels)
• Maximum 3 dependency levels allowed
• Dependent item on a host with master item from template will not be exported to XML

Item configuration

A dependent item depends on its master item for data. That is why the **master item** must be configured (or exist) first:

• Go to: Configuration → Hosts
• Click on Items in the row of the host
• Click on Create item
• Enter parameters of the item in the form

![Item configuration form](image)

All mandatory input fields are marked with a red asterisk.

Click on Add to save the master item.

Then you can configure a **dependent item**.

![Dependent item configuration form](image)

All mandatory input fields are marked with a red asterisk.

The fields that require specific information for dependent items are:
Type Select Dependent item here.
Key Enter a key that will be used to recognize the item.
Master item Select the master item. Master item value will be used to populate dependent item value.
Type of information Select the type of information that will correspond the format of data that will be stored.

You may use item value preprocessing to extract the required part of the master item value.

Without preprocessing, the dependent item value will be exactly the same as the master item value.

Click on Add to save the dependent item.

A shortcut to creating a dependent item quicker is to use the wizard in the item list:

Display

In the item list dependent items are displayed with their master item name as prefix.

If a master item is deleted, so are all its dependent items.

17 HTTP agent

Overview

This item type allows data polling using the HTTP/HTTPS protocol. Trapping is also possible using Zabbix sender or Zabbix sender protocol.

HTTP item check is executed by Zabbix server. However, when hosts are monitored by a Zabbix proxy, HTTP item checks are executed by the proxy.

HTTP item checks do not require any agent running on a host being monitored.
HTTP agent supports both HTTP and HTTPS. Zabbix will optionally follow redirects (see the Follow redirects option below). Maximum number of redirects is hard-coded to 10 (using cURL option CURLOPT_MAXREDIRS).

See also known issues for when using HTTPS protocol.

**Attention:**
Zabbix server/proxy must be initially configured with cURL (libcurl) support.

Configuration

To configure an HTTP item:

- Go to: Configuration → Hosts
- Click on Items in the row of the host
- Click on Create item
- Enter parameters of the item in the form
All mandatory input fields are marked with a red asterisk.

The fields that require specific information for HTTP items are:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select <strong>HTTP agent</strong> here.</td>
</tr>
<tr>
<td>Key</td>
<td>Enter a unique item key.</td>
</tr>
<tr>
<td>URL</td>
<td>URL to connect to and retrieve data. For example: <a href="https://www.example.com">https://www.example.com</a> <a href="http://www.example.com/download">http://www.example.com/download</a></td>
</tr>
<tr>
<td></td>
<td>Domain names can be specified in Unicode characters. They are automatically punycode-converted to ASCII when executing the HTTP check.</td>
</tr>
<tr>
<td></td>
<td>The Parse button can be used to separate optional query fields (like ?name=Admin&amp;password=mypassword) from the URL, moving the attributes and values into Query fields for automatic URL-encoding.</td>
</tr>
<tr>
<td></td>
<td>Limited to 2048 characters.</td>
</tr>
<tr>
<td></td>
<td>Supported macros: {HOST.IP}, {HOST.CONN}, {HOST.DNS}, {HOST.HOST}, {HOST.NAME}, {ITEM.ID}, {ITEM.KEY}, user macros, low-level discovery macros.</td>
</tr>
<tr>
<td></td>
<td>This sets the CURLOPT_URL cURL option.</td>
</tr>
<tr>
<td>Query fields</td>
<td>Variables for the URL (see above).</td>
</tr>
<tr>
<td>Request type</td>
<td>Select request method type: GET, POST, PUT or HEAD</td>
</tr>
<tr>
<td>Timeout</td>
<td>Zabbix will not spend more than the set amount of time on processing the URL (maximum is 1 minute). Actually this parameter defines the maximum time for making a connection to the URL and maximum time for performing an HTTP request. Therefore, Zabbix will not spend more than 2 x Timeout seconds on one check.</td>
</tr>
<tr>
<td></td>
<td>Time suffixes are supported, e.g. 30s, 1m.</td>
</tr>
<tr>
<td></td>
<td>Supported macros: user macros, low-level discovery macros.</td>
</tr>
<tr>
<td></td>
<td>This sets the CURLOPT_TIMEOUT cURL option.</td>
</tr>
<tr>
<td>Request body type</td>
<td>Select the request body type:</td>
</tr>
<tr>
<td>Raw data</td>
<td>- custom HTTP request body, macros are substituted but no encoding is performed</td>
</tr>
<tr>
<td>JSON data</td>
<td>- HTTP request body in JSON format. Macros can be used as string, number, true and false; macros used as strings must be enclosed in double quotes. Values from macros are resolved and then escaped automatically. If “Content-Type” is not specified in headers then it will default to “Content-Type: application/json”</td>
</tr>
<tr>
<td>XML data</td>
<td>- HTTP request body in XML format. Macros can be used as a text node, attribute or CDATA section. Values from macros are resolved and then escaped automatically in a text node and attribute. If “Content-Type” is not specified in headers then it will default to “Content-Type: application/xml”</td>
</tr>
<tr>
<td>Request body</td>
<td>Enter the request body.</td>
</tr>
<tr>
<td></td>
<td>Supported macros: {HOST.IP}, {HOST.CONN}, {HOST.DNS}, {HOST.HOST}, {HOST.NAME}, {ITEM.ID}, {ITEM.KEY}, user macros, low-level discovery macros.</td>
</tr>
</tbody>
</table>
Headers

Custom HTTP headers that will be sent when performing a request.
Specified as attribute and value pairs.
Supported macros: {HOST.IP}, {HOST.CONN}, {HOST.DNS}, {HOST.HOST}, {HOST.NAME}, {ITEM.ID}, {ITEM.KEY}, user macros, low-level discovery macros.
This sets the CURLOPT_HTTPHEADER cURL option.

Required status codes

List of expected HTTP status codes. If Zabbix gets a code which is not in the list, the item will become unsupported. If empty, no check is performed.
For example: 200,201,210-299
Supported macros in the list: user macros, low-level discovery macros.
This uses the CURLOPT_HTTP_CODE cURL option.

Follow redirects

Mark the checkbox to follow HTTP redirects.
This sets the CURLOPT_FOLLOWLOCATION cURL option.

Retrieve mode

Select the part of response that must be retrieved:
**Body** - body only
**Headers** - headers only
**Body and headers** - body and headers

Convert to JSON

Headers are saved as attribute and value pairs under the “header” key.
If ‘Content-Type: application/json’ is encountered then body is saved as an object, otherwise it is stored as string, for example:

```json
{
    "header": {
        "key1": "value1",
        "key2": "value2"
    },
    "body": "<body>
```
HTTP authentication

Authentication type:
- None - no authentication used.
- Basic authentication - basic authentication is used.
- NTLM authentication - NTLM (Windows NT LAN Manager) authentication is used.

Selecting an authentication method will provide two additional fields for entering a user name and password, where user macros and low-level discovery macros are supported.

This sets the `CURLOPT_HTTPAUTH` cURL option.

SSL verify peer

Mark the checkbox to verify the SSL certificate of the web server. The server certificate will be automatically taken from system-wide certificate authority (CA) location. You can override the location of CA files using Zabbix server or proxy configuration parameter SSLCAlocation.

This sets the `CURLOPT_SSL_VERIFYPEER` cURL option.

SSL verify host

Mark the checkbox to verify that the Common Name field or the Subject Alternate Name field of the web server certificate matches.

This sets the `CURLOPT_SSL_VERIFYHOST` cURL option.

SSL certificate file

Name of the SSL certificate file used for client authentication. The certificate file must be in PEM format. If the certificate file contains also the private key, leave the SSL key file field empty. If the key is encrypted, specify the password in SSL key password field. The directory containing this file is specified by Zabbix server or proxy configuration parameter SSLCertLocation.

Supported macros: {HOST.IP}, {HOST.CONN}, {HOST.DNS}, {HOST.HOST}, {HOST.NAME}, {ITEM.ID}, {ITEM.KEY}, user macros, low-level discovery macros.

This sets the `CURLOPT_SSLCERT` cURL option.

SSL key file

Name of the SSL private key file used for client authentication. The private key file must be in PEM format. The directory containing this file is specified by Zabbix server or proxy configuration parameter SSLKeyLocation.

Supported macros: {HOST.IP}, {HOST.CONN}, {HOST.DNS}, {HOST.HOST}, {HOST.NAME}, {ITEM.ID}, {ITEM.KEY}, user macros, low-level discovery macros.

This sets the `CURLOPT_SSLKEY` cURL option.

SSL key password

SSL private key file password.

Supported macros: user macros, low-level discovery macros.

This sets the `CURLOPT_KEYPASSWD` cURL option.

Enable trapping

With this checkbox marked, the item will also function as trapper item and will accept data sent to this item by Zabbix sender or using Zabbix sender protocol.
Allowed hosts
Visible only if Enable trapping checkbox is marked.
List of comma delimited IP addresses, optionally in CIDR notation, or DNS names.
If specified, incoming connections will be accepted only from the hosts listed here.
If IPv6 support is enabled then ‘127.0.0.1’, '::127.0.0.1’, ‘::ffff:127.0.0.1’ are treated equally and ‘::/0’ will allow any IPv4 or IPv6 address.
‘0.0.0.0/0’ can be used to allow any IPv4 address.
Note, that "IPv4-compatible IPv6 addresses" (0000::/96 prefix) are supported but deprecated by RFC4291.
Example: 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}
Spaces and user macros are allowed in this field.
Host macros {HOST.HOST}, {HOST.NAME}, {HOST.IP}, {HOST.DNS}, {HOST.CONN} are allowed in this field since Zabbix 4.0.2.

Note:
If the HTTP proxy field is left empty, another way for using an HTTP proxy is to set proxy-related environment variables.
For HTTP - set the http_proxy environment variable for the Zabbix server user. For example:
For HTTPS - set the HTTPS_PROXY environment variable. For example:

Attention:
[1] Zabbix supports certificate and private key files in PEM format only. In case you have your certificate and private key data in PKCS #12 format file (usually with extension *.p12 or *.pfx) you may generate the PEM file from it using the following commands:
openssl pkcs12 -in ssl-cert.p12 -clcerts -nokeys -out ssl-cert.pem
openssl pkcs12 -in ssl-cert.p12 -nocerts -nodes -out ssl-cert.key

Examples

Example 1
Send simple GET requests to retrieve data from services such as Elasticsearch:

- Create a GET item with URL: localhost:9200/?pretty
- Notice the response:

```json
{
   "name" : "YQ2VAY-",
   "cluster_name" : "elasticsearch",
   "cluster_uuid" : "kH4C5Qh5QfgeTsjh2F9zg",
   "version" : {
      "number" : "6.1.3",
      "build_hash" : "af51318",
      "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"
}
```
- Now extract the version number using a JSONPath preprocessing step: $.version.number

Example 2
Send simple POST requests to retrieve data from services such as Elasticsearch:
Create a POST item with URL: http://localhost:9200/str/values/_search?scroll=10s
Configure the following POST body to obtain the processor load (1 min average per core)

```json
{
    "query": {
        "bool": {
            "must": [{
                "match": {
                    "itemid": 28275
                }
            }],
            "filter": [{
                "range": {
                    "clock": {
                        "gt": 1517565836,
                        "lte": 1517566137
                    }
                }
            }]
        }
    }
}
```

Received:

```json
{
    "_scroll_id": "DnFlZXJ5VQhlbkZldGNoBQAAAAAAbQF1RM1ZBWS1UU1pxTmdEeGVwQjRBTEAAAAAAJRRZUTJWQVktVFNacU5nRHhlcEI0QUxRAAAAAAAAACYWWVEyVkFZLVRTWnFOZ0R4ZXBCNEFMUQAAAAAAAAAzllRMlZBWS1UU1pxTmdEeGVwQjRBTFEAAAAAAJRRZUTJWQVktVFNacU5nRHhlcEI0QUxR",
    "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
            }
        }]
    }
}
```

Now use a JSONPath preprocessing step to get the item value: `$.hits.hits[0]._source.value`

Example 3

Checking if Zabbix API is alive, using `apiinfo.version`.

* Item configuration:
Note the use of the POST method with JSON data, setting request headers and asking to return headers only:

- Item value preprocessing with regular expression to get HTTP code:

```
Item Preprocessing

<table>
<thead>
<tr>
<th>Preprocessing steps</th>
<th>Name</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regular expression</td>
<td>HTTP/1.1 ([0-9]+)</td>
<td>1</td>
</tr>
</tbody>
</table>
```

Add
• Checking the result in Latest data:

![Latest data](image)

Example 4

Retrieving weather information by connecting to the Openweathermap public service.

• Configure a master item for bulk data collection in a single JSON:
Note the usage of macros in query fields. Refer to the Openweathermap API for how to fill them.

Sample JSON returned in response to HTTP agent:

```json
{
    "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
        }
    }
}
```
The next task is to configure dependent items that extract data from the JSON.

- Configure a sample dependent item for humidity:

Other weather metrics such as 'Temperature' are added in the same manner.

- Sample dependent item value preprocessing with JSONPath:

- Check the result of weather data in Latest data:
Example 5

Connecting to Nginx status page and getting its metrics in bulk.

- Configure Nginx following the official guide.
- Configure a master item for bulk data collection:

Sample Nginx stub status output:

```
Active connections: 1
Active connections:
server accepts handled requests
52 52 52
Reading: 0  Writing: 1  Waiting: 0

The next task is to configure dependent items that extract data.

- Configure a sample dependent item for requests per second:
• Sample dependent item value preprocessing with regular expression:

• Check the complete result from stub module in Latest data:

3 History and trends

Overview

History and trends are the two ways of storing collected data in Zabbix.

Whereas history keeps each collected value, trends keep averaged information on hourly basis and therefore are less resource-hungry.

Keeping history

You can set the storage period for how long the history will be kept:

- in the item properties
- when mass-updating items
- when setting up housekeeper tasks

Any older data will be removed by the housekeeper.

The general strong advice is to keep history for the smallest possible number of days and that way not to overload the database with lots of historical values.

Instead of keeping a long history, you can keep longer data of trends. For example, you could keep history for 14 days and trends for 5 years.

You can get a good idea of how much space is required by history versus trends data by referring to the database sizing page.
While keeping shorter history, you will still be able to review older data in graphs, as graphs will use trend values for displaying older data.

**Attention:**
If history storage period is set to ‘Do not keep history’, the item will update only dependent items and inventory. No trigger functions will be evaluated.

**Note:**
As an alternative way to preserve history consider to use **history export** functionality of loadable modules.

**Keeping trends**

Trends is a built-in historical data reduction mechanism which stores minimum, maximum, average and the total number of values per every hour for numeric data types.

You can set the storage period for how long the trends will be kept:

- in the item properties form
- when mass-updating items
- when setting up Housekeeper tasks

Trends usually can be kept for much longer than history. Any older data will be removed by the housekeeper.

Zabbix server accumulates trend data in runtime in the trend cache, as the data flows in. Server flushes trends into the database (where frontend can find them) in these situations:

- a new hour has started and server receives a new value for the item;
- a new hour is about to end in less than 5 minutes (no new values)
- server stops

To see trends on a graph you need to wait at least to the beginning of the next hour (if item is updated frequently) and at most to the end of the next hour (if item is updated rarely), which is 2 hours maximum.

When server flushes trend cache and there are already trends in the database for this hour (for example, server has been restarted mid-hour), server needs to use update statements instead of simple inserts. Therefore on a bigger installation if restart is needed it is desirable to stop server in the end of one hour and start in the beginning of the next hour to avoid trend data overlap.

History tables do not participate in trend generation in any way.

**Attention:**
If trend storage period is set to ‘Do not keep trends’, Zabbix server does not calculate or store trends at all.

**Note:**
The trends are calculated and stored with the same data type as the original values. As a result the average value calculations of unsigned data type values are rounded and the less the value interval is the less precise the result will be. For example if item has values 0 and 1, the average value will be 0, not 0.5.

Also restarting server might result in the precision loss of unsigned data type average value calculations for the current hour.

### 4 User parameters

**Overview**

Sometimes you may want to run an agent check that does not come predefined with Zabbix. This is where user parameters come to help.

You may write a command that retrieves the data you need and include it in the user parameter in the agent configuration file (‘UserParameter’ configuration parameter).

A user parameter has the following syntax:

```
UserParameter=<key>,<command>
```

As you can see, a user parameter also contains a key. The key will be necessary when configuring an item. Enter a key of your choice that will be easy to reference (it must be unique within a host). Restart the agent.

Then, when configuring an item, enter the key to reference the command from the user parameter you want executed.
User parameters are commands executed by Zabbix agent. Up to 512KB of data can be returned before item preprocessing steps. Note, however, that the text value that can be eventually stored in database is limited to 64KB on MySQL (see info on other databases in the table).

/bin/sh is used as a command line interpreter under UNIX operating systems. User parameters obey the agent check timeout; if timeout is reached the forked user parameter process is terminated.

See also:
- Step-by-step tutorial on making use of user parameters
- Command execution

Examples of simple user parameters

A simple command:

UserParameter=ping,echo 1

The agent will always return ‘1’ for an item with ‘ping’ key.

A more complex example:

UserParameter=mysql.ping,mysqladmin -u root ping | grep -c alive

The agent will return ‘1’, if MySQL server is alive, ‘0’ - otherwise.

Flexible user parameters

Flexible user parameters accept parameters with the key. This way a flexible user parameter can be the basis for creating several items.

Flexible user parameters have the following syntax:

UserParameter=key[\*],command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key</td>
<td>Unique item key. The [*] defines that this key accepts parameters within the brackets. Parameters are given when configuring the item.</td>
</tr>
<tr>
<td>Command</td>
<td>Command to be executed to evaluate value of the key. For flexible user parameters only: You may use positional references $1...$9 in the command to refer to the respective parameter in the item key. Zabbix parses the parameters enclosed in [ ] of the item key and substitutes $1,...,$9 in the command accordingly. $0 will be substituted by the original command (prior to expansion of $0,...,$9) to be run. Positional references are interpreted regardless of whether they are enclosed between double (&quot;) or single (’) quotes. To use positional references unaltered, specify a double dollar sign - for example, awk ‘(print $$2)’. In this case $$2 will actually turn into $2 when executing the command.</td>
</tr>
</tbody>
</table>

Attention:
Positional references with the $ sign are searched for and replaced by Zabbix agent only for flexible user parameters. For simple user parameters, such reference processing is skipped and, therefore, any $ sign quoting is not necessary.

Attention:
Certain symbols are not allowed in user parameters by default. See UnsafeUserParameters documentation for a full list.

Example 1

Something very simple:

UserParameter=ping[\*],echo $1

We may define unlimited number of items for monitoring all having format ping[something].

- ping[0] - will always return ‘0’
Example 2

Let’s add more sense!

\[
\text{UserParameter=mysql.ping\[*\],mysqladmin -u$1 -p$2 ping | grep -c alive}
\]

This parameter can be used for monitoring availability of MySQL database. We can pass user name and password:

mysql.ping[zabbix,our_password]

Example 3

How many lines matching a regular expression in a file?

\[
\text{UserParameter=wc\[*\],grep -c "$2" $1}
\]

This parameter can be used to calculate number of lines in a file.

\[
w[/etc/passwd,root]
w[/etc/services,zabbix]
\]

Command result

The return value of the command is standard output together with standard error.

Attention:

A text (character, log or text type of information) item will not become unsupported in case of standard error output.

User parameters that return text (character, log, text type of information) can return whitespace. In case of invalid result the item will become unsupported.

1 Extending Zabbix agents

This tutorial provides step-by-step instructions on how to extend the functionality of Zabbix agent with the use of a user parameter.

Step 1

Write a script or command line to retrieve required parameter.

For example, we may write the following command in order to get total number of queries executed by a MySQL server:

\[
\text{mysqladmin -uroot status | cut -f4 -d":" | cut -f1 -d"S"}
\]

When executed, the command returns total number of SQL queries.

Step 2

Add the command to zabbix_agentd.conf:

\[
\text{UserParameter=mysql.questions,mysqladmin -uroot status | cut -f4 -d":" | cut -f1 -d"S"}
\]

\text{mysql.questions} is a unique identifier. It can be any valid key identifier, for example, queries.

Test this parameter by using Zabbix agent with “-t” flag (if running under root, however, note that the agent may have different permissions when launched as a daemon):

\[
zabbix_agentd -t mysql.questions
\]

Step 3

Restart Zabbix agent.

Agent will reload configuration file.

Test this parameter by using zabbix_get utility.

Step 4

Add new item with Key=mysql.questions to the monitored host. Type of the item must be either Zabbix Agent or Zabbix Agent (active).

Be aware that type of returned values must be set correctly on Zabbix server. Otherwise Zabbix won’t accept them.
5 Loadable modules

1 Overview

Loadable modules offer a performance-minded option for extending Zabbix functionality.

There already are ways of extending Zabbix functionality by way of:

- **user parameters** (agent metrics)
- **external checks** (agent-less monitoring)
- **system.run[]** Zabbix agent item.

They work very well, but have one major drawback, namely fork(). Zabbix has to fork a new process every time it handles a user metric, which is not good for performance. It is not a big deal normally, however it could be a serious issue when monitoring embedded systems, having a large number of monitored parameters or heavy scripts with complex logic or long startup time.

Support of loadable modules offers ways for extending Zabbix agent, server and proxy without sacrificing performance.

A loadable module is basically a shared library used by Zabbix daemon and loaded on startup. The library should contain certain functions, so that a Zabbix process may detect that the file is indeed a module it can load and work with.

Loadable modules have a number of benefits. Great performance and ability to implement any logic are very important, but perhaps the most important advantage is the ability to develop, use and share Zabbix modules. It contributes to trouble-free maintenance and helps to deliver new functionality easier and independently of the Zabbix core code base.

Module licensing and distribution in binary form is governed by the GPL license (modules are linking with Zabbix in runtime and are using Zabbix headers; currently the whole Zabbix code is licensed under GPL license). Binary compatibility is not guaranteed by Zabbix.

Module API stability is guaranteed during one Zabbix LTS (Long Term Support) release cycle. Stability of Zabbix API is not guaranteed (technically it is possible to call Zabbix internal functions from a module, but there is no guarantee that such modules will work).

2 Module API

In order for a shared library to be treated as a Zabbix module, it should implement and export several functions. There are currently six functions in the Zabbix module API, only one of which is mandatory and the other five are optional.

2.1 Mandatory interface

The only mandatory function is **zbx_module_api_version()**:

```c
int zbx_module_api_version(void);
```

This function should return the API version implemented by this module and in order for the module to be loaded this version must match module API version supported by Zabbix. Version of module API supported by Zabbix is ZBX_MODULE_API_VERSION. So this function should return this constant. Old constant ZBX_MODULE_API_VERSION_ONE used for this purpose is now defined to equal ZBX_MODULE_API_VERSION to preserve source compatibility, but it’s usage is not recommended.

2.2 Optional interface

The optional functions are **zbx_module_init()**, **zbx_module_item_list()**, **zbx_module_item_timeout()**, **zbx_module_history_write_cbs()** and **zbx_module_uninit()**:

```c
int zbx_module_init(void);
```

This function should perform the necessary initialization for the module (if any). If successful, it should return ZBX_MODULE_OK. Otherwise, it should return ZBX_MODULE_FAIL. In the latter case Zabbix will not start.

```c
ZBX_METRIC *zbx_module_item_list(void);
```

This function should return a list of items supported by the module. Each item is defined in a ZBX_METRIC structure, see the section below for details. The list is terminated by a ZBX_METRIC structure with “key” field of NULL.

```c
void zbx_module_item_timeout(int timeout);
```

If module exports **zbx_module_item_list()** then this function is used by Zabbix to specify the timeout settings in Zabbix configuration file that the item checks implemented by the module should obey. Here, the “timeout” parameter is in seconds.

```c
ZBX_HISTORY_WRITE_CBS zbx_module_history_write_cbs(void);
```

This function should return callback functions Zabbix server will use to export history of different data types. Callback functions are provided as fields of ZBX_HISTORY_WRITE_CBS structure, fields can be NULL if module is not interested in the history of certain type.
### 2.3 Defining items

Each item is defined in a ZBX_METRIC structure:

```c
typedef struct {
    char *key;
    unsigned flags;
    int (*function)();
    char *test_param;
} ZBX_METRIC;
```

Here, `key` is the item key (e.g., "dummy.random"), `flags` is either CF_HAVEPARAMS or 0 (depending on whether the item accepts parameters or not), `function` is a C function that implements the item (e.g., "zbx_module_dummy_random"), and `test_param` is the parameter list to be used when Zabbix agent is started with the "-p" flag (e.g., "1,1000", can be NULL). An example definition may look like this:

```c
static ZBX_METRIC keys[] =
{
    { "dummy.random", CF_HAVEPARAMS, zbx_module_dummy_random, "1,1000" },
    { NULL }
}
```

Each function that implements an item should accept two pointer parameters, the first one of type `AGENT_REQUEST` and the second one of type `AGENT_RESULT`:

```c
int zbx_module_dummy_random(AGENT_REQUEST *request, AGENT_RESULT *result)
{
    ...
    SET_UI64_RESULT(result, from + rand() % (to - from + 1));
    return SYSINFO_RET_OK;
}
```

These functions should return SYSINFO_RET_OK, if the item value was successfully obtained. Otherwise, they should return SYSINFO_RET_FAIL. See example “dummy” module below for details on how to obtain information from `AGENT_REQUEST` and how to set information in `AGENT_RESULT`.

### 2.4 Providing history export callbacks

Module can specify functions to export history data by type: Numeric (float), Numeric (unsigned), Character, Text and Log:

```c
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;
```

Each of them should take “history” array of “history_num” elements as arguments. Depending on history data type to be exported, “history” is an array of the following structures, respectively:

```c
int zbx_module_uninit(void);
```

This function should perform the necessary uninitialization (if any) like freeing allocated resources, closing file descriptors, etc.

All functions are called once on Zabbix startup when the module is loaded, with the exception of `zbx_module_uninit()`, which is called once on Zabbix shutdown when the module is unloaded.
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;

Callbacks will be used by Zabbix server history syncer processes in the end of history sync procedure after data is written into Zabbix database and saved in value cache.

2.5 Building modules

Modules are currently meant to be built inside Zabbix source tree, because the module API depends on some data structures that are defined in Zabbix headers.

The most important header for loadable modules is include/module.h, which defines these data structures. Other necessary system headers that help include/module.h to work properly are stdlib.h andstdint.h.

With this information in mind, everything is ready for the module to be built. The module should include stdlib.h,stdint.h and module.h, and the build script should make sure that these files are in the include path. See example “dummy” module below for details.

Another useful header is include/log.h, which defines zabbix_log() function, which can be used for logging and debugging.
purposes.

3 Configuration parameters

Zabbix agent, server and proxy support two parameters to deal with modules:

- **LoadModulePath** - full path to the location of loadable modules
- **LoadModule** – module(s) to load at startup. The modules must be located in a directory specified by LoadModulePath or (since 4.0.9) the path must precede the module name. If the preceding path is absolute (starts with '/') then LoadModulePath is ignored. It is allowed to include multiple LoadModule parameters.

For example, to extend Zabbix agent we could add the following parameters:

```bash
LoadModulePath=/usr/local/lib/zabbix/agent/
LoadModule=mariadb.so
LoadModule=apache.so
LoadModule=kernel.so
LoadModule=/usr/local/lib/zabbix/dummy.so
```

Upon agent startup it will load the mariadb.so, apache.so and kernel.so modules from the /usr/local/lib/zabbix/agent directory while dummy.so will be loaded from /usr/local/lib/zabbix. The agent will fail to start if a module is missing, in case of bad permissions or if a shared library is not a Zabbix module.

4 Frontend configuration

Loadable modules are supported by Zabbix agent, server and proxy. Therefore, item type in Zabbix frontend depends on where the module is loaded. If the module is loaded into the agent, then the item type should be “Zabbix agent” or “Zabbix agent (active)”. If the module is loaded into server or proxy, then the item type should be “Simple check”.

History export through Zabbix modules does not need any frontend configuration. If the module is successfully loaded by server and provides `zbx_module_history_write_cbs()` function which returns at least one non-NULL callback function then history export will be enabled automatically.

5 Dummy module

Zabbix includes a sample module written in C language. The module is located under src/modules/dummy:

```bash
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
```

The module is well documented, it can be used as a template for your own modules.

After ./configure has been run in the root of Zabbix source tree as described above, just run `make` in order to build `dummy.so`.

```c
#include <stdlib.h>
#include <string.h>
#include <time.h>
#include <stdint.h>
```

---

### include <stdlib.h>
### include <string.h>
### include <time.h>
### include <stdint.h>

---

---

322
```c
#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 internal 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}
};

/******************************************************************************
* * 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;
}

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);

    from = strlen(param1);
    to = strlen(param2);

    /* set random value */
    SET_UI64_RESULT(result, (unsigned int)rand() & 0x7fffffff);

    return SYSINFO_RET_OK;
}
/ 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, ... */
    }
}
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;
}

The module exports three new items:

- dummy.ping - always returns ‘1’
- dummy.echo[param1] - returns the first parameter as it is, for example, dummy.echo[ABC] will return ABC
- dummy.random[param1, param2] - returns a random number within the range of param1-param2, for example, dummy.random[1,1000000]

6 Limitations

Support of loadable modules is implemented for the Unix platform only. It means that it does not work for Windows agents.

In some cases a module may need to read module-related configuration parameters from zabbix_agentd.conf. It is not supported currently. If you need your module to use some configuration parameters you should probably implement parsing of a module-specific configuration file.

6 Windows performance counters

Overview

You can effectively monitor Windows performance counters using the perf_counter[] key.

For example:

perf_counter["\Processor(0)\Interrupts/sec"]

or

perf_counter["\Processor(0)\Interrupts/sec", 10]

For more information on using this key or its English-only equivalent perf_counter_en, see Windows-specific item keys.

In order to get a full list of performance counters available for monitoring, you may run:

typeperf -qx

Numeric representation

Windows maintains numeric representations (indexes) for object and performance counter names. Zabbix supports these numeric representations as parameters to the perf_counter, perf_counter_en item keys and in PerfCounter, PerfCounterEn configuration parameters.

However, it’s not recommended to use them unless you can guarantee your numeric indexes map to correct strings on specific hosts. If you need to create portable items that work across different hosts with various localized Windows versions, starting with
Zabbix 4.0.13 you can use the `perf_counter_en` key or `PerfCounterEn` configuration parameter which allow to use English names regardless of system locale.

To find out the numeric equivalents, run `regedit`, then find HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\009. The registry entry contains information like this:

```
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
....
```

Here you can find the corresponding numbers for each string part of the performance counter, like in `\System\% Processor Time`:

```
System → 2
% Processor Time → 6
```

Then you can use these numbers to represent the path in numbers:

```
\2\6
```

Performance counter parameters

You can deploy some PerfCounter parameters for the monitoring of Windows performance counters.

For example, you can add these to the Zabbix agent configuration file:

```
PerfCounter=UserPerfCounter1, "\Memory\Page Reads/sec", 30
or PerfCounter=UserPerfCounter2, "\4\24", 30
```

With such parameters in place, you can then simply use UserPerfCounter1 or UserPerfCounter2 as the keys for creating the respective items.

Remember to restart Zabbix agent after making changes to the configuration file.

### 7 Mass update

Overview

Sometimes you may want to change some attribute for a number of items at once. Instead of opening each individual item for editing, you may use the mass update function for that.

Using mass update

To mass-update some items, do the following:

- Mark the checkboxes of the items to update in the list
- Click on Mass update below the list
- Mark the checkboxes of the attributes to update
- Enter new values for the attributes and click on Update
<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Original</td>
</tr>
<tr>
<td>Host interface</td>
<td>Original</td>
</tr>
<tr>
<td>JMX endpoint</td>
<td>Original</td>
</tr>
<tr>
<td>URL</td>
<td>Original</td>
</tr>
<tr>
<td>Request body type</td>
<td>Original</td>
</tr>
<tr>
<td>Request body</td>
<td>Original</td>
</tr>
<tr>
<td>Headers</td>
<td>Original</td>
</tr>
<tr>
<td>SNMP community</td>
<td>Original</td>
</tr>
<tr>
<td>Connect name</td>
<td>Original</td>
</tr>
<tr>
<td>Security name</td>
<td>Original</td>
</tr>
<tr>
<td>Security level</td>
<td>Original</td>
</tr>
<tr>
<td>Authentication protocol</td>
<td>Original</td>
</tr>
<tr>
<td>Authentication passphrase</td>
<td>Original</td>
</tr>
<tr>
<td>Privacy protocol</td>
<td>Original</td>
</tr>
<tr>
<td>Privacy passphrase</td>
<td>Original</td>
</tr>
<tr>
<td>PXI</td>
<td>Original</td>
</tr>
<tr>
<td>Type of information</td>
<td>Original</td>
</tr>
<tr>
<td>Units</td>
<td>Original</td>
</tr>
<tr>
<td>Authentication method</td>
<td>Original</td>
</tr>
<tr>
<td>User name</td>
<td>Original</td>
</tr>
<tr>
<td>Public key file</td>
<td>Original</td>
</tr>
<tr>
<td>Private key file</td>
<td>Original</td>
</tr>
<tr>
<td>Password</td>
<td>Original</td>
</tr>
<tr>
<td>Preprocessing steps</td>
<td>Original</td>
</tr>
<tr>
<td>Update interval</td>
<td>Original</td>
</tr>
<tr>
<td>History storage period</td>
<td>7d</td>
</tr>
<tr>
<td>Trend storage period</td>
<td>Original</td>
</tr>
<tr>
<td>Status</td>
<td>Original</td>
</tr>
<tr>
<td>Log time format</td>
<td>Original</td>
</tr>
<tr>
<td>Show value</td>
<td>Original</td>
</tr>
<tr>
<td>Enable trapping</td>
<td>Original</td>
</tr>
<tr>
<td>Allowed hosts</td>
<td>Original</td>
</tr>
<tr>
<td>Replace applications</td>
<td>Original</td>
</tr>
<tr>
<td>Add new or existing applications</td>
<td>Original</td>
</tr>
<tr>
<td>Master item</td>
<td>Original</td>
</tr>
<tr>
<td>Description</td>
<td>Original</td>
</tr>
</tbody>
</table>
Replace applications will remove the item from any existing applications and replace those with the one(s) specified in this field.

Add new or existing applications allows to specify additional applications from the existing ones or enter completely new applications for the items.

Both these fields are auto-complete - starting to type in them offers a dropdown of matching applications. If the application is new, it also appears in the dropdown and it is indicated by (new) after the string. Just scroll down to select.

8 Value mapping

Overview
For a more "human" representation of received values, you can use value maps that contain the mapping between numeric values and string representations.

Value mappings can be used in both the Zabbix frontend and notifications sent by email/SMS/jabber etc.

For example, an item which has value '0' or '1' can use value mapping to represent the values in a human-readable form:

- '0' => 'Not Available'
- '1' => 'Available'

Or, a backup related value map could be:

- 'F' → 'Full'
- 'D' → 'Differential'
- 'I' → 'Incremental'

Thus, when configuring items you can use a value map to "humanize" the way an item value will be displayed. To do that, you refer to the name of a previously defined value map in the Show value field.

Note:
Value mapping can be used with items having Numeric (unsigned), Numeric (float) and Character type of information.

Value mappings, starting with Zabbix 3.0, can be exported/imported, either separately, or with the respective template or host. Configuration

To define a value map:

- Go to: Administration → General
- Select Value mapping from the dropdown
- Click on Create value map (or on the name of an existing map)
Parameters of a value map:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name of a set of value mappings.</td>
</tr>
<tr>
<td>Mappings</td>
<td>Individual mappings - pairs of numeric values and their string representations.</td>
</tr>
</tbody>
</table>

All mandatory input fields are marked with a red asterisk.

To add a new individual mapping, click on Add.

How this works

For example, one of the predefined agent items ‘Ping to the server (TCP)’ uses an existing value map called ‘Service state’ to display its values.
In the item configuration form you can see a reference to this value map in the Show value field:

So in Monitoring → Latest data the mapping is put to use to display ‘Up’ (with the raw value in parentheses).

In the Latest data section displayed values are shortened to 20 symbols. If value mapping is used, this shortening is not applied to the mapped value, but only to the raw value separately (displayed in parenthesis).

Note:
A value being displayed in a human-readable form is also easier to understand when receiving notifications.

Without a predefined value map you would only get this:

So in this case you would either have to guess what the ‘1’ stands for or do a search of documentation to find out.

9 Applications

Overview

Applications are used to group items in logical groups.

For example, the MySQL Server application can hold all items related to the MySQL server: availability of MySQL, disk space, processor load, transactions per second, number of slow queries, etc.

Applications are also used for grouping web scenarios.

If you are using applications, then in Monitoring → Latest data you will see items and web scenarios grouped under their respective applications.
Configuration

To work with applications you must first create them and then link items or web scenarios to them.

To create an application, do the following:

- Go to Configuration → Hosts or Templates
- Click on Applications next to the required host or template
- Click on Create application
- Enter the application name and click on Add to save it

You can also create a new application directly in the item properties form.

Items are linked to applications in the item properties form. Select one or more applications the item will belong to.

Web scenarios are linked to applications in the web scenario definition form. Select the application the scenario will belong to.

10 Queue

Overview

The queue displays items that are waiting for a refresh. The queue is just a logical representation of data. There is no IPC queue or any other queue mechanism in Zabbix.

Items monitored by proxies are also included in the queue - they will be counted as queued for the proxy history data update period.

Only items with scheduled refresh times are displayed in the queue. This means that the following item types are excluded from the queue:

- log, logrt and event log active Zabbix agent items
- SNMP trap items
- trapper items
- web monitoring items
- dependent items

Statistics shown by the queue is a good indicator of the performance of Zabbix server.

The queue is retrieved directly from Zabbix server using JSON protocol. The information is available only if Zabbix server is running.

Reading the queue

To read the queue, go to Administration → Queue. Overview should be selected in the dropdown to the right.
The picture here is generally “ok” so we may assume that the server is doing fine.

The queue shows six items waiting for 10 seconds. It would be great to know what items these are.

To do just that, select Details in the dropdown in the upper right corner. Now you can see a list of those delayed items.

With these details provided it may be possible to find out why these items might be delayed.

With one or two delayed items there perhaps is no cause for alarm. They might get updated in a second. However, if you see a bunch of items getting delayed for too long, there might be a more serious problem.

Queue of items to be updated

Is the agent down?

Queue item

A special internal item `zabbix[queue,<from>,<to>]` can be used to monitor the health of the queue in Zabbix. It will return the number of items delayed by the set amount of time. For more information see Internal items.
11 Value cache

Overview

To make the calculation of trigger expressions, calculated/aggregate items and some macros much faster, since Zabbix 2.2 a value cache option is supported by the Zabbix server.

This in-memory cache can be used for accessing historical data, instead of making direct SQL calls to the database. If historical values are not present in the cache, the missing values are requested from the database and the cache updated accordingly.

To enable the value cache functionality, an optional **ValueCacheSize** parameter is supported by the Zabbix server configuration file.

Two internal items are supported for monitoring the value cache: `zabbix[vcache,buffer,<mode>]` and `zabbix[vcache,cache,<parameter>]`. See more details with internal items.

12 Check now

Overview

Checking for a new item value in Zabbix is a cyclic process that is based on configured update intervals. While for many items the update intervals are quite short, there are others (including low-level discovery rules) for which the update intervals are quite long, so in real-life situations there may be a need to check for a new value quicker - to pick up changes in discoverable resources, for example. To accommodate such a necessity, it is possible to reschedule a passive check and retrieve a new value immediately.

This functionality is supported for passive checks only. The following item types are supported:

- Zabbix agent (passive)
- SNMPv1/v2/v3 agent
- IPMI agent
- Simple check
- Zabbix internal
- Zabbix aggregate
- External check
- Database monitor
- JMX agent
- SSH agent
- Telnet
- Calculated
- HTTP agent

**Attention:**
The check must be present in configuration cache in order to get executed; for more information see CacheUpdateFrequency. Before executing the check, the configuration cache is not updated, thus very recent changes to item/discovery rule configuration will not be picked up. Therefore, it is also not possible to check for a new value for an item/rule that has been created just now.

Configuration

To execute a passive check immediately:

- click on Check now in an existing item (or discovery rule) configuration form:

```
| Enabled | Update | Clone | Check now |
```

- click on Check now for selected items/rules in the list of items/discovery rules:
In the latter case several items/rules can be selected and “checked now” at once.

3 Triggers

Overview

Triggers are logical expressions that "evaluate" data gathered by items and represent the current system state.

While items are used to gather system data, it is highly impractical to follow these data all the time waiting for a condition that is alarming or deserves attention. The job of "evaluating" data can be left to trigger expressions.

Trigger expressions allow to define a threshold of what state of data is “acceptable”. Therefore, should the incoming data surpass the acceptable state, a trigger is “fired” - or changes its state to PROBLEM.

A trigger may have the following state:

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OK</td>
<td>This is a normal trigger state.</td>
</tr>
<tr>
<td>Problem</td>
<td>Something has happened. For example, the processor load is too high.</td>
</tr>
<tr>
<td>Unknown</td>
<td>The trigger value cannot be calculated. See Unknown state.</td>
</tr>
</tbody>
</table>

Trigger state (the expression) is recalculated every time Zabbix server receives a new value that is part of the expression.

Triggers are evaluated based on history data only; trend data are never considered.

If time-based functions (nodata(), date(), dayofmonth(), dayofweek(), time(), now()) are used in the expression, the trigger is recalculated also every 30 seconds by a Zabbix history syncer process.

You can build trigger expressions with different degrees of complexity.

Unknown state

It is possible that an unknown operand appears in a trigger expression if:

- an unsupported item is used
- the function evaluation for a supported item results in an error

In this case a trigger generally evaluates to "unknown” (although there are some exceptions). For more details, see Expressions with unknown operands.

It is possible to get notified on unknown triggers.

1 Configuring a trigger

Overview

To configure a trigger, do the following:

- Go to: Configuration → Hosts
- Click on Triggers in the row of the host
• Click on Create trigger to the right (or on the trigger name to edit an existing trigger)
• Enter parameters of the trigger in the form

Configuration

The **Trigger** tab contains all the essential trigger attributes.

![Trigger Form](image)

All mandatory input fields are marked with a red asterisk.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Trigger name.</td>
</tr>
<tr>
<td></td>
<td>The name may contain the supported macros: {HOST.HOST}, {HOST.NAME}, {HOST.CONN}, {HOST.DNS}, {HOST.IP}, {ITEM.VALUE}, {ITEM.LASTVALUE} and {$MACRO}. $1, $2...$9 macros can be used to refer to the first, second...ninth constant of the expression. Note: $1-$9 macros will resolve correctly if referring to constants in relatively simple, straightforward expressions. For example, the name &quot;Processor load above $1 on {HOST.NAME}&quot; will automatically change to &quot;Processor load above 5 on New host&quot; if the expression is {New host:system.cpu.load[percpu,avg1].last()}&gt;5</td>
</tr>
<tr>
<td>Severity</td>
<td>Set the required trigger severity by clicking the buttons.</td>
</tr>
<tr>
<td>Expression</td>
<td>Logical expression used to define the conditions of a problem. A problem is created after all the conditions included in the expression are met, i.e. the expression evaluates to TRUE. The problem will be resolved as soon as the expression evaluates to FALSE, unless additional recovery conditions are specified in Recovery expression.</td>
</tr>
<tr>
<td>OK event generation</td>
<td>OK event generation options:</td>
</tr>
<tr>
<td></td>
<td><strong>Expression</strong> - OK events are generated based on the same expression as problem events;</td>
</tr>
<tr>
<td></td>
<td><strong>Recovery expression</strong> - OK events are generated if the problem expression evaluates to FALSE and the recovery expression evaluates to TRUE;</td>
</tr>
<tr>
<td></td>
<td><strong>None</strong> - in this case the trigger will never return to an OK state on its own.</td>
</tr>
<tr>
<td>Recovery expression</td>
<td>Logical expression (optional) defining additional conditions that have to be met before the problem is resolved, after the original problem expression has already been evaluated as FALSE. Recovery expression is useful for trigger hysteresis. It is <strong>not</strong> possible to resolve a problem by recovery expression alone if the problem expression is still TRUE. This field is only available if ‘Recovery expression’ is selected for OK event generation.</td>
</tr>
<tr>
<td>PROBLEM event generation mode</td>
<td>Mode for generating problem events:</td>
</tr>
<tr>
<td></td>
<td><strong>Single</strong> - a single event is generated when a trigger goes into the ‘Problem’ state for the first time;</td>
</tr>
<tr>
<td></td>
<td><strong>Multiple</strong> - an event is generated upon every ‘Problem’ evaluation of the trigger.</td>
</tr>
<tr>
<td>OK event closes</td>
<td>Select if OK event closes:</td>
</tr>
<tr>
<td></td>
<td><strong>All problems</strong> - all problems of this trigger</td>
</tr>
<tr>
<td></td>
<td><strong>All problems if tag values match</strong> - only those trigger problems with matching event tag values</td>
</tr>
<tr>
<td>Tag for matching</td>
<td>Enter event tag name to use for event correlation. This field is displayed if ‘All problems if tag values match’ is selected for the OK event closes property and is mandatory in this case.</td>
</tr>
</tbody>
</table>

Supports since Zabbix 3.2.0.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Tags               | Set custom tags to mark trigger events.  
Event tags can be used for event correlation, in action conditions and will also be seen in Monitoring → Problems or the Problems widget.  
Tags are a pair of tag name and value. You can use only the name or pair it with a value.  
User macros, user macro context, low-level discovery macros and macro functions with {{{ITEM.VALUE}}}, {{{ITEM.LASTVALUE}}} and low-level discovery macros are supported in event tags.  
Low-level discovery macros can be used inside macro context.  
(TRIGGER.ID) macro is supported in trigger tag values since Zabbix 4.0.14. It may be useful for identifying triggers created from trigger prototypes and, for example, suppressing problems from these triggers during maintenance.  
If the total length of expanded value exceeds 255, it will be cut to 255 characters.  
See all macros supported for event tags.  
Supported since Zabbix 3.2.0.                                                                                                                                |
| Allow manual close | Check to allow manual closing of problem events generated by this trigger. Manual closing is possible when acknowledging problem events.  
Supported since Zabbix 3.2.0.                                                                                                                                                                                      |
| URL                | If not empty, the URL entered here is available as a link in several frontend locations, e.g. when clicking on the problem name in Monitoring → Problems (URL option in the Trigger menu) and Problems dashboard widget.  
Supported macros: {{{ITEM.VALUE}}}, {{{ITEM.LASTVALUE}}}, {{{TRIGGER.ID}}}, several {{{HOST.*}}} macros, user macros.                                                                                      |
| Description        | Text field used to provide more information about this trigger. May contain instructions for fixing specific problem, contact detail of responsible staff, etc.  
Starting with Zabbix 2.2, the description may contain the same set of macros as trigger name.                                                                                           |
| Enabled            | Unchecking this box will disable the trigger if required. Problems of a disabled trigger are no longer displayed in the frontend, but are not deleted.                                                                 |

The Dependencies tab contains all the dependencies of the trigger.

Click on Add to add a new dependency.

**Note:**
You can also configure a trigger by opening an existing one, pressing the Clone button and then saving under a different name.

Testing expressions

It is possible to test the configured trigger expression as to what the expression result would be depending on the received value.

Following expression from an official template is taken as an example:

```
{Template Net Cisco IOS SNMPv2:sensor.temp.value[ciscoEnvMonTemperatureValue.{#SNMPINDEX}].avg(5m)}>$TEMP_WARN
or
{Template Net Cisco IOS SNMPv2:sensor.temp.status[ciscoEnvMonTemperatureState.{#SNMPINDEX}].last(0)}=$TEMP_WARN_STATUS
```

To test the expression, click on Expression constructor under the expression field.
In the Expression constructor, all individual expressions are listed. To open the testing window, click on Test below the expression list.

In the testing window you can enter sample values ("80, 70, 0, 1" in this example) and then see the expression result, by clicking on the Test button.

The result of the individual expressions as well as the whole expression can be seen.

"TRUE" result means the specified expression is correct. In this particular case A, "80" is greater than \( \{ \$ \text{TEMP}_\text{WARN} \} \) specified value, "70" in this example. Respectively, "TRUE" result appears.

"FALSE" result means the specified expression is incorrect. In this particular case B, \( \{ \$ \text{TEMP}_\text{WARN\_STATUS} \} \), "1" in this example, needs to be equal with specified "0" value, that is wrong. Respectively, "FALSE" result appears.

Chosen Expression type is "OR"/"TRUE". If at least one of the specified conditions (A or B in this case) is TRUE, overall result will be TRUE as well. That means, current value exceeds the warning value and a Problem has occurred.

2 Trigger expression

Overview

The expressions used in triggers are very flexible. You can use them to create complex logical tests regarding monitored statistics.

A simple useful expression might look like:
While the syntax is exactly the same, from the functional point of view there are two types of trigger expressions:

- problem expression - defines the conditions of the problem
- recovery expression (optional) - defines additional conditions of the problem resolution

When defining a problem expression alone, this expression will be used both as the problem threshold and the problem recovery threshold. As soon as the problem expression evaluates to TRUE, there is a problem. As soon as the problem expression evaluates to FALSE, the problem is resolved.

When defining both problem expression and the supplemental recovery expression, problem resolution becomes more complex: not only the problem expression has to be FALSE, but also the recovery expression has to be TRUE. This is useful to create hysteresis and avoid trigger flapping.

Functions

Trigger functions allow to reference the collected values, current time and other factors.

A complete list of supported functions is available.

All functions return numeric values only. String comparison is not supported. If you want string comparison, upgrade to Zabbix 5.0.

Function parameters

Most of numeric functions accept the number of seconds as a parameter.

You may use the prefix # to specify that a parameter has a different meaning:

<table>
<thead>
<tr>
<th>FUNCTION CALL</th>
<th>MEANING</th>
</tr>
</thead>
<tbody>
<tr>
<td>sum(600)</td>
<td>Sum of all values in no more than the latest 600 seconds</td>
</tr>
<tr>
<td>sum(#5)</td>
<td>Sum of all values in no more than the last 5 values</td>
</tr>
</tbody>
</table>

The function `last` uses a different meaning for values when prefixed with the hash mark - it makes it choose the n-th previous value, so given the values 3, 7, 2, 6, 5 (from most recent to least recent), `last(#2)` would return 7 and `last(#5)` would return 5.

Several functions support an additional, second `time_shift` parameter. This parameter allows to reference data from a period of time in the past. For example, `avg(1h,1d)` will return the average value for an hour one day ago.

You can use the supported unit symbols in trigger expressions, for example '5m' (minutes) instead of '300' seconds or '1d' (day) instead of '86400' seconds. '1K' will stand for '1024' bytes.

Numbers with a '+' sign are not supported.

Operators

The following operators are supported for triggers (in descending priority of execution):

<table>
<thead>
<tr>
<th>PRIORITY OPERATOR</th>
<th>DEFINITION</th>
<th>Notes for unknown values</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>-</td>
<td>Unary minus</td>
</tr>
<tr>
<td>2</td>
<td>not</td>
<td>Logical NOT</td>
</tr>
<tr>
<td>3</td>
<td>*</td>
<td>Multiplication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(yes, Unknown, not 0 - to not lose Unknown in arithmetic operations)</td>
</tr>
<tr>
<td></td>
<td>/</td>
<td>Division</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unknown / 0 → error</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unknown / 1.2 → Unknown</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0.0 / Unknown → Unknown</td>
</tr>
<tr>
<td>4</td>
<td>+</td>
<td>Arithmetical plus</td>
</tr>
<tr>
<td></td>
<td>-</td>
<td>Arithmetical minus</td>
</tr>
</tbody>
</table>
Notes for unknown values

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;</td>
<td>Less than</td>
<td>5 &lt; Unknown $\rightarrow$ Unknown</td>
</tr>
<tr>
<td>&lt;=</td>
<td>Less than or equal to</td>
<td>Unknown &lt;= Unknown $\rightarrow$ Unknown</td>
</tr>
<tr>
<td>&gt;</td>
<td>More than</td>
<td>1.2 &gt; Unknown $\rightarrow$ Unknown</td>
</tr>
<tr>
<td>&gt;=</td>
<td>More than or equal to</td>
<td>Unknown &gt;= Unknown $\rightarrow$ Unknown</td>
</tr>
<tr>
<td>=</td>
<td>Equal</td>
<td>6 = Unknown $\rightarrow$ Unknown</td>
</tr>
</tbody>
</table>

Less than.
The operator is defined as:

$$A < B \iff (A < B - 0.000001)$$

Less than or equal to. The operator is defined as:

$$A \leq B \iff (A \leq B + 0.000001)$$

More than.
The operator is defined as:

$$A > B \iff (A > B + 0.000001)$$

More than or equal to. The operator is defined as:

$$A \geq B \iff (A \geq B - 0.000001)$$

Is equal.
The operator is defined as:

$$A = B \iff (A = B - 0.000001) \text{ and } (A \leq B + 0.000001)$$
Notes for unknown values

not, and and or operators are case-sensitive and must be in lowercase. They also must be surrounded by spaces or parentheses. All operators, except unary - and not, have left-to-right associativity. Unary - and not are non-associative (meaning -(-1) and not (not 1) should be used instead of --1 and not not 1).

Evaluation result:

- <, <=, >, >=, =, <> operators shall yield ‘1’ in the trigger expression if the specified relation is true and ‘0’ if it is false. If at least one operand is Unknown the result is Unknown;
- and for known operands shall yield ‘1’ if both of its operands compare unequal to ‘0’; otherwise, it yields ‘0’; for unknown operands and yields ‘0’ only if one operand compares equal to ‘0’; otherwise, it yields ‘Unknown’;
- or for known operands shall yield ‘1’ if either of its operands compare unequal to ‘0’; otherwise, it yields ‘0’; for unknown operands or yields ‘1’ only if one operand compares unequal to ‘0’; otherwise, it yields ‘Unknown’;
- The result of the logical negation operator not for a known operand is ‘0’ if the value of its operand compares unequal to ‘0’; ‘1’ if the value of its operand compares equal to ‘0’. For unknown operand not yields ‘Unknown’.

Value caching

Values required for trigger evaluation are cached by Zabbix server. Because of this trigger evaluation causes a higher database load for some time after the server restarts. The value cache is not cleared when item history values are removed (either manually or by housekeeper), so the server will use the cached values until they are older than the time periods defined in trigger functions or server is restarted.

Examples of triggers

Example 1
Processor load is too high on www.example.com

{www.example.com:system.cpu.load[all,avg1].last()}>5

‘www.example.com:system.cpu.load[all,avg1]’ gives a short name of the monitored parameter. It specifies that the server is ‘www.example.com’ and the key being monitored is ‘system.cpu.load[all,avg1]’. By using the function ‘last()’, we are referring to the most recent value. Finally, ‘>5’ means that the trigger is in the PROBLEM state whenever the most recent processor load measurement from www.example.com is greater than 5.

Example 2
www.example.com is overloaded

{www.example.com:system.cpu.load[all,avg1].last()}>5 or {www.example.com:system.cpu.load[all,avg1].min(10m)}>2

The expression is true when either the current processor load is more than 5 or the processor load was more than 2 during last 10 minutes.

Example 3
/etc/passwd has been changed
Use of function diff:
{www.example.com:vfs.file.cksum[/etc/passwd].diff()}=1
The expression is true when the previous value of checksum of /etc/passwd differs from the most recent one.
Similar expressions could be useful to monitor changes in important files, such as /etc/passwd, /etc/inetd.conf, /kernel, etc.
Example 4
Someone is downloading a large file from the Internet
Use of function min:
{www.example.com:net.if.in[eth0,bytes].min(5m)}>100K
The expression is true when number of received bytes on eth0 is more than 100 KB within last 5 minutes.
Example 5
Both nodes of clustered SMTP server are down
Note use of two different hosts in one expression:
{smtp1.example.com:net.tcp.service[smtp].last()}=0 and {smtp2.example.com:net.tcp.service[smtp].last()}=0
The expression is true when both SMTP servers are down on both smtp1.example.com and smtp2.example.com.
Example 6
Zabbix agent needs to be upgraded
Use of function str():
{example.example.com:agent.version.str("beta8")}=1
The expression is true if Zabbix agent has version beta8 (presumably 1.0beta8).
Example 7
Server is unreachable
{example.example.com:icmp.ping.count(30m,0)}>5
The expression is true if host "example.example.com" is unreachable more than 5 times in the last 30 minutes.
Example 8
No heartbeats within last 3 minutes
Use of function nodata():
{example.example.com:tick.nodata(3m)}=1
To make use of this trigger, 'tick' must be defined as a Zabbix trapper item. The host should periodically send data for this item using zabbix_sender. If no data is received within 180 seconds, the trigger value becomes PROBLEM.
Note that 'nodata' can be used for any item type.
Example 9
CPU activity at night time
Use of function time():
{zabbix:system.cpu.load[all,avg1].min(5m)}>2 and {zabbix:system.cpu.load[all,avg1].time()}>000000 and {zabbix:system.cpu.load[all,avg1].time()}<060000
The trigger may change its state to true only at night time (00:00 - 06:00).
Example 10
CPU activity at any time with exception
Use of function time() and not operator:
{zabbix:system.cpu.load[all,avg1].min(5m)}>2 and not ({zabbix:system.cpu.load[all,avg1].dayofweek(0)}=7 and {zabbix:system.cpu.load[all,avg1].time(0)}>230000) and not ({zabbix:system.cpu.load[all,avg1].dayofweek(0)}=1 and {zabbix:system.cpu.load[all,avg1].time(0)}<010000)
The trigger may change its state to true at any time, except for 2 hours on a week change (Sunday, 23:00 - Monday, 01:00).

Example 11
Check if client local time is in sync with Zabbix server time
Use of function fuzzytime():
{MySQL_DB:system.localtime.fuzzytime(10)}=0
The trigger will change to the problem state in case when local time on server MySQL_DB and Zabbix server differs by more than 10 seconds. Note that 'system.localtime' must be configured as a passive check.

Example 12
Comparing average load today with average load of the same time yesterday (using a second time_shift parameter).
{server:system.cpu.load.avg(1h)}/{server:system.cpu.load.avg(1h,1d)}>2
This expression will fire if the average load of the last hour tops the average load of the same hour yesterday more than two times.

Example 13
Using the value of another item to get a trigger threshold:
{Template PfSense:hrStorageFree[#SNMPVALUE].last()}<>{Template PfSense:hrStorageSize[#SNMPVALUE].last()}*0.1
The trigger will fire if the free storage drops below 10 percent.

Example 14
Using evaluation result to get the number of triggers over a threshold:
({server1:system.cpu.load[all,avg1].last()}>5) + ({server2:system.cpu.load[all,avg1].last()}>5) + ({server3:system.cpu.load[all,avg1].last()}>5)>=2
The trigger will fire if at least two of the triggers in the expression are over 5.

Hysteresis
Sometimes an interval is needed between problem and recovery states, rather than a simple threshold. For example, if we want to define a trigger that reports a problem when server room temperature goes above 20°C and we want it to stay in the problem state until the temperature drops below 15°C, a simple trigger threshold at 20°C will not be enough.

Instead, we need to define a trigger expression for the problem event first (temperature above 20°C). Then we need to define an additional recovery condition (temperature below 15°C). This is done by defining an additional Recovery expression parameter when defining a trigger.

In this case, problem recovery will take place in two steps:
- First, the problem expression (temperature above 20°C) will have to evaluate to FALSE
- Second, the recovery expression (temperature below 15°C) will have to evaluate to TRUE

The recovery expression will be evaluated only when the problem event is resolved first.

Warning:
The recovery expression being TRUE alone does not resolve a problem if the problem expression is still TRUE!

Example 1
Temperature in server room is too high.
Problem expression:
{server:temp.last()}>20
Recovery expression:
{server:temp.last()}<=15
Example 2
Free disk space is too low.
Problem expression: it is less than 10GB for last 5 minutes
{server:vfs.fs.size[/,free].max(5m)}<10G
Recovery expression: it is more than 40GB for last 10 minutes
{server:vfs.fs.size[/,free].min(10m)}>40G
Expressions with unknown operands

Generally an unknown operand (such as an unsupported item) in the expression will immediately render the trigger value to Unknown. However, in some cases unknown operands (unsupported items, function errors) are admitted into expression evaluation:

- The nodata() function is evaluated regardless of whether the referenced item is supported or not.
- Logical expressions with OR and AND can be evaluated to known values in two cases regardless of unknown operands:
  - **Case 1**: "1 or unsupported_item1.some_function() or unsupported_item2.some_function() or ...") can be evaluated to known result ('1' or "Problem"),
  - **Case 2**: "0 and unsupported_item1.some_function() and unsupported_item2.some_function() and ...") can be evaluated to known result ('0' or "OK").
Zabbix tries to evaluate such logical expressions by taking unsupported items as unknown operands. In the two cases above a known value will be produced ("Problem" or "OK", respectively); in **all other** cases the trigger will evaluate to Unknown.

- If the function evaluation for a supported item results in error, the function value becomes Unknown and it takes part as unknown operand in further expression evaluation.

Note that unknown operands may “disappear” only in logical expressions as described above. In arithmetic expressions unknown operands always lead to the result Unknown (except division by 0).

**Attention:**
An expression that results in Unknown does not change the trigger state ("Problem/OK"). So, if it was "Problem" (see Case 1), it stays in the same problem state even if the known part is resolved ("1’ becomes ‘0’), because the expression is now evaluated to Unknown and that does not change the trigger state.

If a trigger expression with several unsupported items evaluates to Unknown the error message in the frontend refers to the last unsupported item evaluated.

3 Trigger dependencies

Overview

Sometimes the availability of one host depends on another. A server that is behind some router will become unreachable if the router goes down. With triggers configured for both, you might get notifications about two hosts down - while only the router was the guilty party.

This is where some dependency between hosts might be useful. With dependency set notifications of the dependents could be withheld and only the notification for the root problem sent.

While Zabbix does not support dependencies between hosts directly, they may be defined with another, more flexible method - trigger dependencies. A trigger may have one or more triggers it depends on.

So in our simple example we open the server trigger configuration form and set that it depends on the respective trigger of the router. With such dependency the server trigger will not change state as long as the trigger it depends on is in ‘PROBLEM’ state - and thus no dependent actions will be taken and no notifications sent.

If both the server and the router are down and dependency is there, Zabbix will not execute actions for the dependent trigger.

Actions on dependent triggers will not be executed if the trigger they depend on:

- changes its state from ‘PROBLEM’ to ‘UNKNOWN’
- is closed manually, by correlation or with the help of time- based functions
- is resolved by a value of an item not involved in dependent trigger

Note that “secondary” (dependent) trigger in the above-mentioned cases will not be immediately updated.

Also:

- Trigger dependency may be added from any host trigger to any other host trigger, as long as it wouldn’t result in a circular dependency.
- Trigger dependency may be added from a template to a template. If a trigger from template A depends on a trigger from template B, template A may only be linked to a host (or another template) together with template B, but template B may be linked to a host (or another template) alone.
- Trigger dependency may be added from template trigger to a host trigger. In this case, linking such a template to a host will create a host trigger that depends on the same trigger template trigger was depending on. This allows to, for example, have a template where some triggers depend on router (host) triggers. All hosts linked to this template will depend on that specific router.
• Trigger dependency from a host trigger to a template trigger may not be added.
• Trigger dependency may be added from a trigger prototype to another trigger prototype (within the same low-level discovery rule) or a real trigger. A trigger prototype may not depend on a trigger prototype from a different LLD rule or on a trigger created from trigger prototype. Host trigger prototype cannot depend on a trigger from a template.

Configuration

To define a dependency, open the Dependencies tab in a trigger configuration form. Click on Add in the ‘Dependencies’ block and select one or more triggers that our trigger will depend on.

Click Update. Now the trigger has an indication of its dependency in the list.

Example of several dependencies

For example, a Host is behind a Router2 and the Router2 is behind a Router1.

Zabbix - Router1 - Router2 - Host

If Router1 is down, then obviously Host and Router2 are also unreachable yet we don’t want to receive three notifications about Host, Router1 and Router2 all being down.

So in this case we define two dependencies:

'Host is down' trigger depends on 'Router2 is down' trigger
'Router2 is down' trigger depends on 'Router1 is down' trigger

Before changing the status of the ‘Host is down’ trigger, Zabbix will check for corresponding trigger dependencies. If found, and one of those triggers is in ‘Problem’ state, then the trigger status will not be changed and thus actions will not be executed and notifications will not be sent.

Zabbix performs this check recursively. If Router1 or Router2 is unreachable, the Host trigger won’t be updated.

4 Trigger severity

Trigger severity represents the level of importance of a trigger.

Zabbix supports the following default trigger severities.

<table>
<thead>
<tr>
<th>Severity</th>
<th>Color</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not classified</td>
<td>Gray</td>
<td>Can be used where the severity level of an event is unknown, has not been determined, is not part of the regular monitoring scope, etc., for example, during initial configuration, as a placeholder for future assessment, or as part of an integration process.</td>
</tr>
<tr>
<td>Information</td>
<td>Light blue</td>
<td>Can be used for informational events that do not require immediate attention, but can still provide valuable insights.</td>
</tr>
<tr>
<td>Warning</td>
<td>Yellow</td>
<td>Can be used to indicate a potential issue that might require investigation or action, but that is not critical.</td>
</tr>
<tr>
<td>Average</td>
<td>Orange</td>
<td>Can be used to indicate a significant issue that should be addressed relatively soon to prevent further problems.</td>
</tr>
</tbody>
</table>
### Severity Color Description

<table>
<thead>
<tr>
<th>Severity</th>
<th>Color</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Light red</td>
<td>Can be used to indicate critical issues that need immediate attention to avoid significant disruptions.</td>
</tr>
<tr>
<td>Disaster</td>
<td>Red</td>
<td>Can be used to indicate a severe incident that requires immediate action to prevent, for example, system outages or data loss.</td>
</tr>
</tbody>
</table>

**Note:**
Trigger severity names and colors can be customized.

Trigger severities are used for:

- visual representation of triggers - different colors for different severities;
- audio in global alarms - different audio for different severities;
- user media - different media (notification channel) for different severities (for example, SMS for triggers of High and Disaster severity, and Email for triggers of other severities);
- limiting actions by conditions against trigger severities.

### 5 Customizing trigger severities

Trigger severity names and colors for severity related GUI elements can be configured in Administration → General → Trigger severities. Colors are shared among all GUI themes.

Translating customized severity names

**Attention:**
If Zabbix frontend translations are used, custom severity names will override translated names by default.

Default trigger severity names are available for translation in all locales. If a severity name is changed, custom name is used in all locales and additional manual translation is needed.

Custom severity name translation procedure:

- set required custom severity name, for example ‘important’
- edit `<frontend_dir>/locale/<required_locale>/LC_MESSAGES/frontend.po`
- add 2 lines:
  ```
  msgid "Important"
  msgstr "<translation string>"
  ```
  and save file.

Here `msgid` should match the new custom severity name and `msgstr` should be the translation for it in the specific language.

This procedure should be performed after each severity name change.

### 6 Mass update

**Overview**

With mass update you may change some attribute for a number of triggers at once, saving you the need to open each individual trigger for editing.

**Using mass update**

To mass-update some triggers, do the following:

- Mark the checkboxes of the triggers to update in the list
- Click on Mass update below the list
- Mark the checkboxes of the attributes to update
- Specify new values for the attributes and click on Update
Replace dependencies and Replace tags will replace existing trigger dependencies/tags (if any) with the ones specified in mass update.

7 Predictive trigger functions

Overview

Sometimes there are signs of the upcoming problem. These signs can be spotted so that actions may be taken in advance to prevent or at least minimize the impact of the problem.

Zabbix has tools to predict the future behavior of the monitored system based on historic data. These tools are realized through predictive trigger functions.

1 Functions

Two things one needs to know is how to define a problem state and how much time is needed to take action. Then there are two ways to set up a trigger signaling about a potential unwanted situation. First: trigger must fire when the system after "time to act" is expected to be in problem state. Second: trigger must fire when the system is going to reach the problem state in less than "time to act". Corresponding trigger functions to use are forecast and timeleft. Note that underlying statistical analysis is basically identical for both functions. You may set up a trigger whichever way you prefer with similar results.

2 Parameters

Both functions use almost the same set of parameters. Use the list of supported functions for reference.

2.1 Time interval

First of all you should specify the historic period Zabbix should analyze to come up with prediction. You do it in a familiar way by means of sec or #num parameter and optional time_shift like you do it with avg, count, delta, max, min and sum functions.

2.2 Forecasting horizon

(forecast only)

Parameter time specifies how far in the future Zabbix should extrapolate dependencies it finds in historic data. No matter if you use time_shift or not, time is always counted starting from the current moment.

2.3 Threshold to reach

(timeleft only)

Parameter threshold specifies a value the analyzed item has to reach, no difference if from above or from below. Once we have determined \( f(t) \) (see below) we should solve equation \( f(t) = \text{threshold} \) and return the root which is closer to now and to the right from now or 999999999999.9999 if there is no such root.
2.4 Fit functions

Default fit is the linear function. But if your monitored system is more complicated you have more options to choose from.

<table>
<thead>
<tr>
<th>fit</th>
<th>x = f(t)</th>
</tr>
</thead>
<tbody>
<tr>
<td>linear</td>
<td>x = a + b*t</td>
</tr>
<tr>
<td>polynomialN</td>
<td>x = a_0 + a_1<em>t + a_2</em>t^2 + ... + a_n*t^n</td>
</tr>
<tr>
<td>exponential</td>
<td>x = a<em>exp(b</em>t)</td>
</tr>
<tr>
<td>logarithmic</td>
<td>x = a + b*log(t)</td>
</tr>
<tr>
<td>power</td>
<td>x = a*t^b</td>
</tr>
</tbody>
</table>

2.5 Modes

(only)

Every time a trigger function is evaluated it gets data from the specified history period and fits a specified function to the data. So, if the data is slightly different the fitted function will be slightly different. If we simply calculate the value of the fitted function at a specified time in the future you will know nothing about how the analyzed item is expected to behave between now and that moment in the future. For some fit options (like polynomial) a simple value from the future may be misleading.

<table>
<thead>
<tr>
<th>mode</th>
<th>forecast result</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>f(now + time)</td>
</tr>
<tr>
<td>max</td>
<td>max_{now &lt;= t &lt;= now + time} f(t)</td>
</tr>
<tr>
<td>min</td>
<td>min_{now &lt;= t &lt;= now + time} f(t)</td>
</tr>
<tr>
<td>delta</td>
<td>max - min</td>
</tr>
<tr>
<td>avg</td>
<td>average_{now &lt;= t &lt;= now + time} f(t) according to definition</td>
</tr>
</tbody>
</table>

3 Details

To avoid calculations with huge numbers we consider the timestamp of the first value in specified period plus 1 ns as a new zero-time (current epoch time is of order 10^9, epoch squared is 10^18, double precision is about 10^-16). 1 ns is added to provide all positive time values for logarithmic and power fits which involve calculating log(t). Time shift does not affect linear, polynomial, exponential (apart from easier and more precise calculations) but changes the shape of logarithmic and power functions.

4 Potential errors

Functions return -1 in such situations:

- specified evaluation period contains no data;
- result of mathematical operation is not defined;
- numerical complications (unfortunately, for some sets of input data range and precision of double-precision floating-point format become insufficient).

5 Examples and dealing with errors

To get a warning when you are about to run out of free disk space on your host you may use a trigger expression like this:

1Secure indicates that the cookie should only be transmitted over a secure HTTPS connection from the client. When set to ‘true’, the cookie will only be set if a secure connection exists.
2For example fitting exponential or power functions involves calculating log() of item values. If data contains zeros or negative numbers you will get an error since log() is defined for positive values only.
3For linear, exponential, logarithmic and power fits all necessary calculations can be written explicitly. For polynomial only value can be calculated without any additional steps. Calculating avg involves computing polynomial antiderivative (analytically). Computing max, min and delta involves computing polynomial derivative (analytically) and finding its roots (numerically). Solving f(t) = 0 involves finding polynomial roots (numerically).
However, error code -1 may come into play and put your trigger in a problem state. Generally it's good because you get a warning that your predictions don't work correctly and you should look at them more thoroughly to find out why. But sometimes it's bad because -1 can simply mean that there was no data about the host free disk space obtained in the last hour. If you are getting too many false positive alerts consider using more complicated trigger expression:

{host:vfs.fs.size[/,free].timeleft(1h,,0)}<1h and {host:vfs.fs.size[/,free].timeleft(1h,,0)}<>-1

Situation is a bit more difficult with forecast. First of all, -1 may or may not put the trigger in a problem state depending on whether you have expression like {host:item.forecast(...)}<... or like {host:item.forecast(...)}>...

Furthermore, -1 may be a valid forecast if it's normal for the item value to be negative. But probability of this situation in the real world situation is negligible (see how operator = works). So add ... or {host:item.forecast(...)}=-1 or ... and {host:item.forecast(...)}<>-1 if you want or don't want to treat -1 as a problem respectively.

4 Events

Overview

There are several types of events generated in Zabbix:

- trigger events - whenever a trigger changes its status (OK→PROBLEM→OK)
- discovery events - when hosts or services are detected
- auto registration events - when active agents are auto-registered by server
- internal events - when an item/low-level discovery rule becomes unsupported or a trigger goes into an unknown state

Note:
Internal events are supported starting with Zabbix 2.2 version.

Events are time-stamped and can be the basis of actions such as sending notification e-mail etc.

To view details of events in the frontend, go to Monitoring → Problems. There you can click on the event date and time to view details of an event.

More information is available on:

- trigger events
- other event sources

1 Trigger event generation

Overview

Change of trigger status is the most frequent and most important source of events. Each time the trigger changes its state, an event is generated. The event contains details of the trigger state’s change - when it happened and what the new state is.

Two types of events are created by triggers - Problem and OK.

Problem events

A problem event is created:

- when a trigger expression evaluates to TRUE if the trigger is in OK state;
- each time a trigger expression evaluates to TRUE if multiple problem event generation is enabled for the trigger.

OK events

An OK event closes the related problem event(s) and may be created by 3 components:

- triggers - based on ‘OK event generation’ and ‘OK event closes’ settings;
- event correlation
- task manager - when an event is manually closed

Triggers

Triggers have an ‘OK event generation’ setting that controls how OK events are generated:

But in this case -1 can cause your trigger to recover from the problem state. To be fully protected use: {host:vfs.fs.size[/,free].timeleft(1h,,0)}<1h and ((TRIGGER.VALUE)=0 and {host:vfs.fs.size[/,free].timeleft(1h,,0)}<>-1 or (TRIGGER.VALUE)=1)
• Expression - an OK event is generated for a trigger in problem state when its expression evaluates to FALSE. This is the simplest setting, enabled by default.

• Recovery expression - an OK event is generated for a trigger in problem state when its expression evaluates to FALSE and the recovery expression evaluates to TRUE. This can be used if trigger recovery criteria is different from problem criteria.

• None - an OK event is never generated. This can be used in conjunction with multiple problem event generation to simply send a notification when something happens.

Additionally triggers have an ‘OK event closes’ setting that controls which problem events are closed:

• All problems - an OK event will close all open problems created by the trigger
• All problems if tag values match - an OK event will close open problems created by the trigger and having at least one matching tag value. The tag is defined by ‘Tag for matching’ trigger setting. If there are no problem events to close then OK event is not generated. This is often called trigger level event correlation.

Event correlation

Event correlation (also called global event correlation) is a way to set up custom event closing (resulting in OK event generation) rules.

The rules define how the new problem events are paired with existing problem events and allow to close the new event or the matched events by generating corresponding OK events.

However, event correlation must be configured very carefully, as it can negatively affect event processing performance or, if misconfigured, close more events than intended (in the worst case even all problem events could be closed). A few configuration tips:

1. always reduce the correlation scope by setting a unique tag for the control event (the event that is paired with old events) and use the ‘new event tag’ correlation condition
2. don’t forget to add a condition based on the old event when using ‘close old event’ operation, or all existing problems could be closed
3. avoid using common tag names used by different correlation configurations

Task manager

If the ‘Allow manual close’ setting is enabled for trigger, then it’s possible to manually close problem events generated by the trigger. This is done in the frontend when updating a problem. The event is not closed directly – instead a ‘close event’ task is created, which is handled by the task manager shortly. The task manager will generate a corresponding OK event and the problem event will be closed.

2 Other event sources

Discovery events

Zabbix periodically scans the IP ranges defined in network discovery rules. Frequency of the check is configurable for each rule individually. Once a host or a service is discovered, a discovery event (or several events) are generated.

Zabbix generates the following events:

<table>
<thead>
<tr>
<th>Event</th>
<th>When generated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Up</td>
<td>Every time Zabbix detects active service.</td>
</tr>
<tr>
<td>Service Down</td>
<td>Every time Zabbix cannot detect service.</td>
</tr>
<tr>
<td>Host Up</td>
<td>If at least one of the services is UP for the IP.</td>
</tr>
<tr>
<td>Host Down</td>
<td>If all services are not responding.</td>
</tr>
<tr>
<td>Service Discovered</td>
<td>If the service is back after downtime or discovered for the first time.</td>
</tr>
<tr>
<td>Service Lost</td>
<td>If the service is lost after being up.</td>
</tr>
<tr>
<td>Host Discovered</td>
<td>If host is back after downtime or discovered for the first time.</td>
</tr>
<tr>
<td>Host Lost</td>
<td>If host is lost after being up.</td>
</tr>
</tbody>
</table>

Active agent auto-discovery events

Active agent auto-registration creates events in Zabbix.

If configured, active agent auto-registration event is created when a previously unknown active agent asks for checks or if the host metadata has changed. The server adds a new auto-registered host, using the received IP address and port of the agent.

For more information, see the active agent auto-registration page.

Internal events
Internal events happen when:

- an item changes state from 'normal' to 'unsupported'
- an item changes state from 'unsupported' to 'normal'
- a low-level discovery rule changes state from 'normal' to 'unsupported'
- a low-level discovery rule changes state from 'unsupported' to 'normal'
- a trigger changes state from 'normal' to 'unknown'
- a trigger changes state from 'unknown' to 'normal'

Internal events are supported since Zabbix 2.2. The aim of introducing internal events is to allow users to be notified when any internal event takes place, for example, an item becomes unsupported and stops gathering data.

Internal events are only created when internal actions for these events are enabled. To stop generation of internal events (for example, for items becoming unsupported), disable all actions for internal events in Configuration → Actions → Internal actions.

**Note:**

If internal actions are disabled, while an object is in the 'unsupported' state, recovery event for this object will still be created.

If internal actions are enabled, while an object is in the 'unsupported' state, recovery event for this object will be created, even though 'problem event' has not been created for the object.

### 3 Manual closing of problems

#### Overview

While generally problem events are resolved automatically when trigger status goes from 'Problem' to 'OK', there may be cases when it is difficult to determine if a problem has been resolved by means of a trigger expression. In such cases, the problem needs to be resolved manually.

For example, syslog may report that some kernel parameters need to be tuned for optimal performance. In this case the issue is reported to Linux administrators, they fix it and then close the problem manually.

Problems can be closed manually only for triggers with the Allow manual close option enabled.

When a problem is “manually closed”, Zabbix generates a new internal task for Zabbix server. Then the task manager process executes this task and generates an OK event, therefore closing problem event.

A manually closed problem does not mean that the underlying trigger will never go into a ‘Problem’ state again. When new data arrive for any item included in the trigger expression, the whole expression is re-evaluated and may result in a problem again, and also, the trigger is re-evaluated when time-based functions are used in the expression. Complete time-based function list can be found on [Triggers page](#).

#### Configuration

Two steps are required to close a problem manually.

**Trigger configuration**

In trigger configuration, enable the Allow manual close option.

Problem update screen

If a problem arises for a trigger with the Manual close flag, you can go to the problem update screen of that problem and close the problem manually.

To close the problem, check the Close problem option in the form and click on Update.
All mandatory input fields are marked with a red asterisk.

The request is processed by Zabbix server. Normally it will take a few seconds to close the problem. During that process CLOSING is displayed in Monitoring → Problems as the status of the problem.

Verification

It can be verified that a problem has been closed manually:

- in event details, available through Monitoring → Problems;
- by using the {EVENT.UPDATE.HISTORY} macro in notification messages that will provide this information.

5 Event correlation

Overview

Event correlation allows to correlate problem events to their resolution in a manner that is very precise and flexible.

Event correlation can be defined:

- on trigger level - one trigger may be used to relate separate problems to their solution
- globally - problems can be correlated to their solution from a different trigger/polling method using global correlation rules

1 Trigger-based event correlation

Overview

Trigger-based event correlation allows to correlate separate problems reported by one trigger.
While generally an OK event can close all problem events created by one trigger, there are cases when a more detailed approach is needed. For example, when monitoring log files you may want to discover certain problems in a log file and close them individually rather than all together.

This is the case with triggers that have Multiple Problem Event Generation enabled. Such triggers are normally used for log monitoring, trap processing, etc.

It is possible in Zabbix to relate problem events based on the event tags. Tags are used to extract values and create identification for problem events. Taking advantage of that, problems can also be closed individually based on matching tag.

In other words, the same trigger can create separate events identified by the event tag. Therefore problem events can be identified one-by-one and closed separately based on the identification by the event tag.

How it works

In log monitoring you may encounter lines similar to these:

Line1: Application 1 stopped
Line2: Application 2 stopped
Line3: Application 1 was restarted
Line4: Application 2 was restarted

The idea of event correlation is to be able to match the problem event from Line1 to the resolution from Line3 and the problem event from Line2 to the resolution from Line4, and close these problems one by one:

Line1: Application 1 stopped
Line3: Application 1 was restarted #problem from Line 1 closed

Line2: Application 2 stopped
Line4: Application 2 was restarted #problem from Line 2 closed

To do this you need to tag these related events as, for example, “Application 1” and “Application 2”. That can be done by applying a regular expression to the log line to extract the tag value. Then, when events are created, they are tagged “Application 1” and “Application 2” respectively and problem can be matched to the resolution.

Configuration

To configure event correlation on trigger level:

- go to the trigger configuration form
All mandatory input fields are marked with a red asterisk.

- select ‘Problem event generation mode’ as Multiple
- select that ‘OK event closes’ All problems if tag values match
- enter the name of the tag for event matching
- configure the tags to extract tag values from log lines

If configured successfully you will be able to see problem events tagged by application and matched to their resolution in Monitoring – Problems.

**Warning:**
Because misconfiguration is possible, when similar event tags may be created for unrelated problems, please review the cases outlined below!

- With two applications writing error and recovery messages to the same log file a user may decide to use two Application tags in the same trigger with different tag values by using separate regular expressions in the tag values to extract the names of, say, application A and application B from the (ITEM.VALUE) macro (e.g. when the message formats differ). However, this may not work as planned if there is no match to the regular expressions. Non-matching regexps will yield empty tag values and a single empty tag value in both problem and OK events is enough to correlate them. So a recovery message from application A may accidentally close an error message from application B.

- Actual tags and tag values only become visible when a trigger fires. If the regular expression used is invalid, it is silently replaced with an *UNKNOWN* string. If the initial problem event with an *UNKNOWN* tag value is missed, there may appear subsequent OK events with the same *UNKNOWN* tag value that may close problem events which they shouldn’t have closed.

- If a user uses the (ITEM.VALUE) macro without macro functions as the tag value, the 255-character limitation applies. When log messages are long and the first 255 characters are non-specific, this may also result in similar event tags for unrelated problems.

**Event tags**

**Overview**

There is an option to define custom event tags in Zabbix. Event tags are defined on the trigger level. After the tags are defined, corresponding new events get marked with tag data.

Having custom event tags allows for more flexibility. Most importantly, events can be **correlated** based on event tags. In other uses, actions can be defined based on event tags.

Event tags are realized as a pair of the tag name and value. You can use only the name or pair it with a value:

MySQL, Service:MySQL, Services, Services:Customer, Applications, Application:Java, Priority:High

An entity (trigger, template, host or event) may have several tags with the same name, but different values - these tags will not be considered ‘duplicates’. Similarly, a tag with no value and the same tag with a value can be used simultaneously.

**Use cases**

Some use cases for this functionality are as follows:

1. Identify problems in a log file and close them separately
   - Define tags in the log trigger that will identify events using value extraction by the %%(ITEM.VALUE)
   - In trigger configuration, have multiple problem event generation mode;
   - In trigger configuration, use [[:manual/config/event_correlation|event correlation]]: select the option
   - See problem events created with a tag and closed individually.

- Use it to filter notifications
  - Define tags on the trigger level to mark events by different tags;
  - Use tag filtering in action conditions to receive notifications only on the events that match tag data;

- See event tag information in the frontend
  - Define tags on the trigger level to mark events by different tags;
  - See this information in //Monitoring// – //Problems//.
- Use information extracted from item value as tag value
  * Use an %{{ITEM.VALUE<N>}.regsub()}%% macro in the tag value;
  * See tag values in //Monitoring// → //Problems// as extracted data from item value.
- Identify problems better in notifications
  * Define tags on the trigger level;
  * Use an {EVENT.TAGS} macro in the problem notification;
  * Easier identify which application/service the notification belongs to.
- Simplify configuration tasks by using tags on the template level
  * Define tags on the template trigger level;
  * See these tags on all triggers created from template triggers.
- Create triggers with tags from low-level discovery (LLD)
  * Define tags on trigger prototypes;
  * Use LLD macros in the tag name or value;
  * See these tags on all triggers created from trigger prototypes.

Configuration

Event tags are defined in trigger configuration. Event tags can be defined for triggers, template triggers and trigger prototypes.

Macro support

The following macros may be used in event tags:

- {ITEM.VALUE}, {ITEM.LASTVALUE}, {HOST.HOST}, {HOST.NAME}, {HOST.CONN}, {HOST.DNS}, {HOST.IP}, {HOST.PORT} and {HOST.ID} macros can be used to populate the tag name or tag value.
- {INVENTORY.*} macros can be used to reference host inventory values from one or several hosts in a trigger expression (supported since 4.0.0).
- User macros and user macro context is supported for the tag name/value. User macro context may include low-level discovery macros.
- Low-level discovery macros can be used for the tag name/value in trigger prototypes.

{EVENT.TAGS} and {EVENT.RECOVERY.TAGS} macros can be used in trigger-based notifications and they will resolve to a comma separated list of event tags or recovery event tags.

Substring extraction

Substring extraction is supported for populating the tag name or tag value, using a macro function - applying a regular expression to the value obtained by the {ITEM.VALUE}, {ITEM.LASTVALUE} macro or a low-level discovery macro. For example:

```plaintext
{{ITEM.VALUE}.regsub(pattern, output)}
{{ITEM.VALUE}.iregsub(pattern, output)}
{{#LLDMACRO}.regsub(pattern, output)}
{{#LLDMACRO}.iregsub(pattern, output)}
```

Tag name and value will be cut to 255 characters if their length exceeds 255 characters after macro resolution.

See also: Using macro functions in low-level discovery macros for event tagging.

Viewing event tags

Event tags, if defined, can be seen with new events in:
• Monitoring → Problems
• Monitoring → Problems → Event details
• Monitoring → Dashboard → Problems widget (in popup window that opens when rolling the mouse over problem name)

Only the first three tag entries are displayed. If there are more than three tag entries, it is indicated by three dots. If you roll your mouse over these three dots, all tag entries are displayed in a pop-up window.

Note that the order in which tags are displayed is affected by tag filtering and the Tag display priority option in the filter of Monitoring → Problems or the Problems dashboard widget.

2 Global event correlation

Overview

Global event correlation allows to reach out over all metrics monitored by Zabbix and create correlations.

It is possible to correlate events created by completely different triggers and apply the same operations to them all. By creating intelligent correlation rules it is actually possible to save yourself from thousands of repetitive notifications and focus on root causes of a problem!

Global event correlation is a powerful mechanism, which allows you to untie yourself from one trigger based problem and resolution logic. So far, a single problem event was created by one trigger and we were dependent on that same trigger for the problem resolution. We could not resolve a problem created by one trigger with another trigger. But with event correlation based on event tagging, we can.

For example, a log trigger may report application problems, while a polling trigger may report the application to be up and running. Taking advantage of event tags you can tag the log trigger as Status: Down while tag the polling trigger as Status: Up. Then, in a global correlation rule you can relate these triggers and assign an appropriate operation to this correlation such as closing the old events.

In another use, global correlation can identify similar triggers and apply the same operation to them. What if we could get only one problem report per network port problem? No need to report them all. That is also possible with global event correlation.

Global event correlation is configured in correlation rules. A correlation rule defines how the new problem events are paired with existing problem events and what to do in case of a match (close the new event, close matched old events by generating corresponding OK events). If a problem is closed by global correlation, it is reported in the Info column of Monitoring → Problems.

Configuring global correlation rules is available to Zabbix Super Admin level users only.

**Attention:**

Event correlation must be configured very carefully, as it can negatively affect event processing performance. If misconfigured, close more events than was intended (in the worst case even all problem events could be closed).

To configure global correlation safely, observe the following important tips:

• Reduce the correlation scope. Always set a unique tag for the new event that is paired with old events and use the New event tag correlation condition;
• Add a condition based on the old event when using the Close old event operation (or else all existing problems could be closed);
• Avoid using common tag names that may end up being used by different correlation configurations;
• Keep the number of correlation rules limited to the ones you really need.

See also: known issues.

Configuration

To configure event correlation rules globally:

• Go to Configuration → Event correlation
• Click on Create correlation to the right (or on the correlation name to edit an existing rule)
• Enter parameters of the correlation rule in the form
All mandatory input fields are marked with a red asterisk.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique correlation rule name.</td>
</tr>
<tr>
<td>Type of calculation</td>
<td>The following options of calculating conditions are available:</td>
</tr>
<tr>
<td></td>
<td>- <strong>And</strong> - all conditions must be met</td>
</tr>
<tr>
<td></td>
<td>- <strong>Or</strong> - enough if one condition is met</td>
</tr>
<tr>
<td></td>
<td>- <strong>And/Or</strong> - AND with different condition types and OR with the same</td>
</tr>
<tr>
<td></td>
<td>condition type</td>
</tr>
<tr>
<td></td>
<td>- <strong>Custom expression</strong> - a user-defined calculation formula for</td>
</tr>
<tr>
<td></td>
<td>evaluating action conditions. It must include all conditions</td>
</tr>
<tr>
<td></td>
<td>(represented as uppercase letters A, B, C, ...) and may include spaces,</td>
</tr>
<tr>
<td></td>
<td>tabs, brackets ( ), <strong>and</strong> (case sensitive), <strong>or</strong> (case sensitive),</td>
</tr>
<tr>
<td></td>
<td><strong>not</strong> (case sensitive).</td>
</tr>
<tr>
<td>Conditions</td>
<td>List of conditions, as selected from the New condition field.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| New condition      | Select conditions for correlating events and click on Add. Note that if no old event condition is specified, all old events may be matched and closed. Similarly if no new event condition is specified, all new events may be matched and closed. The following conditions are available:  
  **Old event tag** - specify the old event tag for matching.  
  **New event tag** - specify the new event tag for matching.  
  **New event host group** - specify the new event host group for matching.  
  **Event tag pair** - specify new event tag and old event tag for matching. In this case there will be a match if the values of the tags in both events match. Tag names need not match. This option is useful for matching runtime values, which may not be known at the time of configuration (see also Example 1).  
  **Old event tag value** - specify the old event tag name and value for matching, using the following operators:  
    - equals - has the old event tag value  
    - does not equal - does not have the old event tag value  
    - contains - has the string in the old event tag value  
    - does not contain - does not have the string in the old event tag value  
  **New event tag value** - specify the new event tag name and value for matching, using the following operators:  
    - equals - has the new event tag value  
    - does not equal - does not have the new event tag value  
    - contains - has the string in the new event tag value  
    - does not contain - does not have the string in the new event tag value |
| Description        | Correlation rule description.                                                                                                                                                                           |
| Enabled            | If you mark this checkbox, the correlation rule will be enabled.                                                                                                                                       |

- Select the operation of the correlation rule in the form

![Correlation Operations](image)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operations</td>
<td>List of operations, selected from the New operation field.</td>
</tr>
</tbody>
</table>
| New operation  | Select operation to perform when event is correlated and click on Add. The following operations are available:  
  **Close old events** - close old events when a new event happens. Always add a condition based on the old event when using the Close old events operation or all existing problems could be closed.  
  **Close new event** - close the new event when it happens                                                                                      |

**Warning:**
Because misconfiguration is possible, when similar event tags may be created for unrelated problems, please review the cases outlined below!
• Actual tags and tag values only become visible when a trigger fires. If the regular expression used is invalid, it is silently replaced with an *UNKNOWN* string. If the initial problem event with an *UNKNOWN* tag value is missed, there may appear subsequent OK events with the same *UNKNOWN* tag value that may close problem events which they shouldn’t have closed.

• If a user uses the \{ITEM.VALUE\} macro without macro functions as the tag value, the 255-character limitation applies. When log messages are long and the first 255 characters are non-specific, this may also result in similar event tags for unrelated problems.

Examples

Example 1

Stop repetitive problem events from the same network port.

![Correlation Operations](image)

This global correlation rule will correlate problems if Host and Port tag values exist on the trigger and they are the same in the original event and the new one.

![Correlation Operations](image)

This operation will close new problem events on the same network port, keeping only the original problem open.

6 Visualization

1 Graphs

Overview
With lots of data flowing into Zabbix, it becomes much easier for the users if they can look at a visual representation of what is going on rather than only numbers.

This is where graphs come in. Graphs allow to grasp the data flow at a glance, correlate problems, discover when something started or make a presentation of when something might turn into a problem.

Zabbix provides users with:

- built-in simple graphs of one item data
- the possibility to create more complex customized graphs
- access to a comparison of several items quickly in ad-hoc graphs
- modern customisable vector graphs

## 1 Simple graphs

### Overview

Simple graphs are provided for the visualization of data gathered by items. No configuration effort is required on the user part to view simple graphs. They are freely made available by Zabbix. Just go to Monitoring → Latest data and click on the Graph link for the respective item and a graph will be displayed.

![Simple graph example](image)

**Note:**
Simple graphs are provided for all numeric items. For textual items, a link to History is available in Monitoring → Latest data.

### Time period selector

Take note of the time period selector above the graph. It allows to select often required periods with one mouse click.

Note that such options as Today, This week, This month, This year display the whole period, including the hours/days in the future. Today so far, in contrast, only displays the hours passed.

Once a period is selected, it can be moved back and forth in time by clicking on the arrow buttons. The Zoom out button allows to zoom out the period two times or by 50% in each direction. Zoom out is also possible by double-clicking in the graphs. The whole time period selector can be collapsed by clicking on the tab label containing the selected period string.

The From/To fields display the selected period in either:

- absolute time syntax in format Y-m-d H:i:s
• relative time syntax, e.g.: now-1d

A date in **relative** format can contain one or several mathematical operations (- or +), e.g. now-1d or now-1d-2h+5m. For relative time the following abbreviations are supported:

- now
- s (seconds)
- m (minutes)
- h (hours)
- d (days)
- w (weeks)
- M (months)
- y (years)

**Precision** is supported in the time filter (e. g., an expression like now-1d/M). Details of precision:

<table>
<thead>
<tr>
<th>Precision</th>
<th>From</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>minutes</td>
<td>Y-m-d H:m:00</td>
<td>Y-m-d H:m:59</td>
</tr>
<tr>
<td>hours</td>
<td>Y-m-d H:00:00</td>
<td>Y-m-d H:59:59</td>
</tr>
<tr>
<td>days</td>
<td>Y-m-d 00:00:00</td>
<td>Y-m-d 23:59:59</td>
</tr>
<tr>
<td>weeks</td>
<td>Monday of the week 00:00:00</td>
<td>Sunday of the week 23:59:59</td>
</tr>
<tr>
<td>months</td>
<td>First day of the month 00:00:00</td>
<td>Last day of the month 23:59:59</td>
</tr>
<tr>
<td>years</td>
<td>1st of January of the year 00:00:00</td>
<td>31st of December of the year 23:59:59</td>
</tr>
</tbody>
</table>

For example:

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Selected period</th>
</tr>
</thead>
<tbody>
<tr>
<td>now/d</td>
<td>now/d</td>
<td>00:00 - 23:59 today</td>
</tr>
<tr>
<td>now/d</td>
<td>now/d+1d</td>
<td>00:00 today - 23:59 tomorrow</td>
</tr>
<tr>
<td>now/w</td>
<td>now/w</td>
<td>Monday 00:00:00 - Sunday 23:59:59 this week</td>
</tr>
<tr>
<td>now-1y/w</td>
<td>now-1y/w</td>
<td>The week of Monday 00:00:00 - Sunday 23:59:59 one year ago</td>
</tr>
</tbody>
</table>

**Date picker**

It is possible to pick a specific start/end date by clicking on the calendar icon next to the From/To fields. In this case, the date picker popup will open.

Within the date picker, it is possible to navigate between the blocks of year/month/date using Tab and Shift+Tab. Keyboard arrows or arrow buttons allow to select the desired value. Pressing Enter (or clicking on the desired value) activates the choice.

Another way of controlling the displayed time is to highlight an area in the graph with the left mouse button. The graph will zoom into the highlighted area once you release the left mouse button.

In case no time value is specified or field is left blank, time value will be set to "00:00:00". This doesn’t apply to today’s date selection: in that case time will be set to current value.

**Recent data vs longer periods**

For very recent data a **single** line is drawn connecting each received value. The single line is drawn as long as there is at least one horizontal pixel available for one value.
For data that show a longer period **three lines** are drawn - a dark green one shows the average, while a light pink and a light green line shows the maximum and minimum values at that point in time. The space between the highs and the lows is filled with yellow background.

Working time (working days) is displayed in graphs as a white background, while non-working time is displayed in gray (with the Original blue default frontend theme).

![Graph showing network traffic](image)

Working time is always displayed in simple graphs, whereas displaying it in **custom graphs** is a user preference.

Working time is not displayed if the graph shows more than 3 months.

**Trigger lines**

Simple triggers are displayed as lines with black dashes over trigger severity color -- take note of the blue line on the graph and the trigger information displayed in the legend. Up to 3 trigger lines can be displayed on the graph; if there are more triggers then the triggers with lower severity are prioritized. Triggers are always displayed in simple graphs, whereas displaying them in **custom graphs** is a user preference.

![Graph showing trigger](image)

Generating from history/trends

Graphs can be drawn based on either item **history** or **trends**.

For the users who have frontend **debug mode** activated, a gray, vertical caption is displayed at the bottom right of a graph indicating where the data come from.

Several factors influence whether history of trends is used:
• longevity of item history. For example, item history can be kept for 14 days. In that case, any data older than the fourteen days will be coming from trends.

• data congestion in the graph. If the amount of seconds to display in a horizontal graph pixel exceeds 3600/16, trend data are displayed (even if item history is still available for the same period).

• if trends are disabled, item history is used for graph building - if available for that period. This is supported starting with Zabbix 2.2.1 (before, disabled trends would mean an empty graph for the period even if item history was available).

Absence of data
For items with a regular update interval, nothing is displayed in the graph if item data are not collected.
However, for trapper items and items with a scheduled update interval (and regular update interval set to 0), a straight line is drawn leading up to the first collected value and from the last collected value to the end of graph; the line is on the level of the first/last value respectively.

Switching to raw values
A dropdown on the upper right allows to switch from the simple graph to the Values/500 latest values listings. This can be useful for viewing the numeric values making up the graph.

The values represented here are raw, i.e. no units or postprocessing of values is used. Value mapping, however, is applied.

Known issues
See known issues for graphs.

2 Custom graphs

Overview
Custom graphs, as the name suggests, offer customisation capabilities.
While simple graphs are good for viewing data of a single item, they do not offer configuration capabilities.
Thus, if you want to change graph style or the way lines are displayed or compare several items, for example incoming and outgoing traffic in a single graph, you need a custom graph.

Custom graphs are configured manually.
They can be created for a host or several hosts or for a single template.

Configuring custom graphs
To create a custom graph, do the following:
• Go to Configuration → Hosts (or Templates)
• Click on Graphs in the row next to the desired host or template
• In the Graphs screen click on Create graph
• Edit graph attributes
All mandatory input fields are marked with a red asterisk.

Graph attributes:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique graph name. Starting with Zabbix 2.2, item values can be referenced in the name by using simple macros with the standard {$host: key . func (param)$} syntax. Only \textbf{avg}, \textbf{last, max} and \textbf{min} as functions with seconds as parameter are supported within this macro. (HOST.HOST&lt;1-9&gt;) macros are supported for the use within this macro, referencing the first, second, third, etc. host in the graph, for example {${HOST . HOST1} : key . func (param)$}.</td>
</tr>
<tr>
<td>Width</td>
<td>Graph width in pixels (for preview and pie/exploded graphs only).</td>
</tr>
<tr>
<td>Height</td>
<td>Graph height in pixels.</td>
</tr>
<tr>
<td>Graph type</td>
<td>Graph type: \textbf{Normal} - normal graph, values displayed as lines \textbf{Stacked} - stacked graph, filled areas displayed \textbf{Pie} - pie graph \textbf{Exploded} - “exploded” pie graph, portions displayed as “cut out” of the pie</td>
</tr>
<tr>
<td>Show legend</td>
<td>Checking this box will set to display the graph legend.</td>
</tr>
<tr>
<td>Show working time</td>
<td>If selected, non-working hours will be shown with gray background. Not available for pie and exploded pie graphs.</td>
</tr>
<tr>
<td>Show triggers</td>
<td>If selected, simple triggers will be displayed as lines with black dashes over trigger severity color. Not available for pie and exploded pie graphs.</td>
</tr>
<tr>
<td>Percentile line (left)</td>
<td>Display percentile for left Y axis. If, for example, 95% percentile is set, then the percentile line will be at the level where 95 per cent of the values fall under. Displayed as a bright green line. Only available for normal graphs.</td>
</tr>
<tr>
<td>Percentile line (right)</td>
<td>Display percentile for right Y axis. If, for example, 95% percentile is set, then the percentile line will be at the level where 95 per cent of the values fall under. Displayed as a bright red line. Only available for normal graphs.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Y axis MIN value</td>
<td>Minimum value of Y axis:</td>
</tr>
<tr>
<td></td>
<td><strong>Calculated</strong> - Y axis minimum value will be automatically calculated</td>
</tr>
<tr>
<td></td>
<td><strong>Fixed</strong> - fixed minimum value for Y axis. Not available for pie and exploded pie graphs.</td>
</tr>
<tr>
<td></td>
<td><strong>Item</strong> - last value of the selected item will be the minimum value</td>
</tr>
<tr>
<td>Y axis MAX value</td>
<td>Maximum value of Y axis:</td>
</tr>
<tr>
<td></td>
<td><strong>Calculated</strong> - Y axis maximum value will be automatically calculated</td>
</tr>
<tr>
<td></td>
<td><strong>Fixed</strong> - fixed maximum value for Y axis. Not available for pie and exploded pie graphs.</td>
</tr>
<tr>
<td></td>
<td><strong>Item</strong> - last value of the selected item will be the maximum value</td>
</tr>
<tr>
<td>3D view</td>
<td>Enable 3D style. For pie and exploded pie graphs only.</td>
</tr>
<tr>
<td>Items</td>
<td>Items, data of which are to be displayed in this graph. Click on Add to select items. You can also select various displaying options (function, draw style, left/right axis display, color).</td>
</tr>
<tr>
<td>Sort order</td>
<td>Draw order. 0 will be processed first. Can be used to draw lines or regions behind (or in front of) another. You can drag and drop items by the arrow in the beginning of (0→100) line to set the sort order or which item is displayed in front of the other.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the selected item is displayed as a link. Clicking on the link opens the list of other available items.</td>
</tr>
<tr>
<td>Type</td>
<td>Type (only available for pie and exploded pie graphs):</td>
</tr>
<tr>
<td></td>
<td><strong>Simple</strong> - value of the item is represented proportionally on the pie</td>
</tr>
<tr>
<td></td>
<td><strong>Graph sum</strong> - value of the item represents the whole pie</td>
</tr>
<tr>
<td></td>
<td>Note that colouring of the “graph sum” item will only be visible to the extent that it is not taken up by “proportional” items.</td>
</tr>
<tr>
<td>Function</td>
<td>Select what values will be displayed when more than one value exists per vertical graph pixel for an item:</td>
</tr>
<tr>
<td></td>
<td><strong>all</strong> - display all possible values (minimum, maximum, average) in the graph. Note that for shorter periods this setting has no effect; only for longer periods, when data congestion in a vertical graph pixel increases, ‘all’ starts displaying minimum, maximum and average values. This function is only available for Normal graph type. See also: Generating graphs from history/trends.</td>
</tr>
<tr>
<td></td>
<td><strong>avg</strong> - display the average values</td>
</tr>
<tr>
<td></td>
<td><strong>last</strong> - display the latest values. This function is only available if either Pie/Exploded pie is selected as graph type.</td>
</tr>
<tr>
<td></td>
<td><strong>max</strong> - display the maximum values</td>
</tr>
<tr>
<td></td>
<td><strong>min</strong> - display the minimum values</td>
</tr>
<tr>
<td>Draw style</td>
<td>Select the draw style (only available for normal graphs; for stacked graphs filled region is always used) to apply to the item data - Line, Bold line, Filled region, Dot, Dashed line, Gradient line.</td>
</tr>
<tr>
<td>Y axis side</td>
<td>Select the Y axis side to show the item data - Left, Right.</td>
</tr>
<tr>
<td>Color</td>
<td>Select the color to apply to the item data.</td>
</tr>
</tbody>
</table>

Graph preview

In the Preview tab, a preview of the graph is displayed so you can immediately see what you are creating.
Note that the preview will not show any data for template items.

In this example, pay attention to the dashed bold line displaying the trigger level and the trigger information displayed in the legend.

**Note:**
No more than 3 trigger lines can be displayed. If there are more triggers then the triggers with lower severity are prioritized for display.

If graph height is set as less than 120 pixels, no trigger will be displayed in the legend.

### 3 Ad-hoc graphs

**Overview**

While a *simple graph* is great for accessing data of one item and *custom graphs* offer customisation options, none of the two allow to quickly create a comparison graph for multiple items with little effort and no maintenance.

To address this issue, since Zabbix 2.4 it is possible to create ad-hoc graphs for several items in a very quick way.

**Configuration**

To create an ad-hoc graph, do the following:

- Go to Monitoring → Latest data
- Use filter to display items that you want
- Mark checkboxes of the items you want to graph
• Click on Display stacked graph or Display graph buttons

Your graph is created instantly:

Note that to avoid displaying too many lines in the graph, only the average value for each item is displayed (min/max value lines are not displayed). Triggers and trigger information is not displayed in the graph.

In the created graph window you have the time period selector available and the possibility to switch from the “normal” line graph to a stacked one (and back).
2 Network maps

Overview

If you have a network to look after, you may want to have an overview of your infrastructure somewhere. For that purpose you can create maps in Zabbix - of networks and of anything you like.

All users can create network maps. The maps can be public (available to all users) or private (available to selected users).

Proceed to configuring a network map.

1 Configuring a network map

Overview

Configuring a map in Zabbix requires that you first create a map by defining its general parameters and then you start filling the actual map with elements and their links.

You can populate the map with elements that are a host, a host group, a trigger, an image or another map.

Icons are used to represent map elements. You can define the information that will be displayed with the icons and set that recent problems are displayed in a special way. You can link the icons and define information to be displayed on the links.

You can add custom URLs to be accessible by clicking on the icons. Thus you may link a host icon to host properties or a map icon to another map.

Maps are managed in Monitoring → Maps, where they can be configured, managed and viewed. In the monitoring view you can click on the icons and take advantage of the links to some scripts and URLs.

Network maps are based on vector graphics (SVG) since Zabbix 3.4.

Public and private maps

All users in Zabbix (including non-admin users) can create network maps. Maps have an owner - the user who created them. Maps can be made public or private.

• Public maps are visible to all users, although to see it the user must have read access to at least one map element. Public maps can be edited in case a user/ user group has read-write permissions for this map and at least read permissions to all elements of the corresponding map including triggers in the links.

• Private maps are visible only to their owner and the users/user groups the map is shared with by the owner. Regular (non-Super admin) users can only share with the groups and users they are member of. Admin level users can see private maps regardless of being the owner or belonging to the shared user list. Private maps can be edited by the owner of the map and in case a user/ user group has read-write permissions for this map and at least read permissions to all elements of the corresponding map including triggers in the links.
Map elements that the user does not have read permission to are displayed with a grayed out icon and all textual information on the element is hidden. However, trigger label is visible even if the user has no permission to the trigger.

To add an element to the map the user must also have at least read permission to the element.

Creating a map

To create a map, do the following:

- Go to Monitoring → Maps
- Go to the view with all maps
- Click on Create map

You can also use the Clone and Full clone buttons in the configuration form of an existing map to create a new map. Clicking on Clone will retain general layout attributes of the original map, but no elements. Full clone will retain both the general layout attributes and all elements of the original map.

The Map tab contains general map attributes:

![Map tab interface](image)

All mandatory input fields are marked with a red asterisk.

General map attributes:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owner</td>
<td>Name of map owner.</td>
</tr>
<tr>
<td>Name</td>
<td>Unique map name.</td>
</tr>
<tr>
<td>Width</td>
<td>Map width in pixels.</td>
</tr>
<tr>
<td>Height</td>
<td>Map height in pixels.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Background image</td>
<td>Use background image:</td>
</tr>
<tr>
<td><strong>No image</strong></td>
<td>- no background image (white background)</td>
</tr>
<tr>
<td><strong>Image</strong></td>
<td>- selected image to be used as a background image. No scaling is performed. You may use a geographical map or any other image to enhance your map.</td>
</tr>
<tr>
<td>Automatic icon mapping</td>
<td>You can set to use an automatic icon mapping, configured in Administration → General → Icon mapping. Icon mapping allows to map certain icons against certain host inventory fields.</td>
</tr>
<tr>
<td>Icon highlighting</td>
<td>If you check this box, map elements will receive highlighting. Elements with an active trigger will receive a round background, in the same color as the highest severity trigger. Moreover, a thick green line will be displayed around the circle, if all problems are acknowledged. Elements with &quot;disabled&quot; or &quot;in maintenance&quot; status will get a square background, gray and orange respectively. See also: Viewing maps</td>
</tr>
<tr>
<td>Mark elements on trigger status change</td>
<td>A recent change of trigger status (recent problem or resolution) will be highlighted with markers (inward-pointing red triangles) on the three sides of the element icon that are free of the label. Markers are displayed for 30 minutes.</td>
</tr>
<tr>
<td>Display problems</td>
<td>Select how problems are displayed with a map element:</td>
</tr>
<tr>
<td><strong>Expand single problem</strong></td>
<td>- name of the most critical problem is displayed</td>
</tr>
<tr>
<td><strong>Number of problems</strong></td>
<td>- the total number of problems is displayed</td>
</tr>
<tr>
<td><strong>Number of problems and expand most critical one</strong></td>
<td>- name of the most critical problem and the total number of problems is displayed. 'Most critical' is determined based on problem severity and, if equal, problem event ID (higher ID or later problem displayed first). (Note that trigger ID instead of problem event ID was evaluated before 4.0.7.) For trigger map element it is based on problem severity and, if equal, trigger position in the trigger list. In case of multiple problems of the same trigger, the most recent one will be displayed.</td>
</tr>
<tr>
<td>Advanced labels</td>
<td>If you check this box you will be able to define separate label types for separate element types.</td>
</tr>
<tr>
<td>Map element label type</td>
<td>Label type used for map elements:</td>
</tr>
<tr>
<td><strong>Label</strong></td>
<td>- map element label</td>
</tr>
<tr>
<td><strong>IP address</strong></td>
<td>- IP address</td>
</tr>
<tr>
<td><strong>Element name</strong></td>
<td>- element name (for example, host name)</td>
</tr>
<tr>
<td><strong>Status only</strong></td>
<td>- status only (OK or PROBLEM)</td>
</tr>
<tr>
<td><strong>Nothing</strong></td>
<td>- no labels are displayed</td>
</tr>
<tr>
<td>Map element label location</td>
<td>Label location in relation to the map element:</td>
</tr>
<tr>
<td><strong>Bottom</strong></td>
<td>- beneath the map element</td>
</tr>
<tr>
<td><strong>Left</strong></td>
<td>- to the left</td>
</tr>
<tr>
<td><strong>Right</strong></td>
<td>- to the right</td>
</tr>
<tr>
<td><strong>Top</strong></td>
<td>- above the map element</td>
</tr>
<tr>
<td>Problem display</td>
<td>Display problem count as:</td>
</tr>
<tr>
<td><strong>All</strong></td>
<td>- full problem count will be displayed</td>
</tr>
<tr>
<td><strong>Separated</strong></td>
<td>- unacknowledged problem count will be displayed separated as a number of the total problem count</td>
</tr>
<tr>
<td><strong>Unacknowledged only</strong></td>
<td>- only the unacknowledged problem count will be displayed</td>
</tr>
<tr>
<td>Minimum trigger severity</td>
<td>Problems below the selected minimum severity level will not be displayed in the map. For example, with Warning selected, changes with Information and Not classified level triggers will not be reflected in the map. This parameter is supported starting with Zabbix 2.2.</td>
</tr>
<tr>
<td>Show suppressed problems</td>
<td>Mark the checkbox to display problems which would otherwise be suppressed (not shown) because of host maintenance.</td>
</tr>
</tbody>
</table>
Parameter Description

URLs
- URLs for each element type can be defined (with a label). These will be displayed as links when a user clicks on the element in the map viewing mode.
- Macros that can be used in map URLs: (MAP.ID), (HOSTGROUP.ID), (HOST.ID), (TRIGGER.ID)

Sharing

The **Sharing** tab contains the map type as well as sharing options (user groups, users) for private maps:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select map type:</td>
</tr>
<tr>
<td></td>
<td><strong>Private</strong> - map is visible only to selected user groups and users</td>
</tr>
<tr>
<td></td>
<td><strong>Public</strong> - map is visible to all</td>
</tr>
<tr>
<td>List of user group shares</td>
<td>Select user groups that the map is accessible to.</td>
</tr>
<tr>
<td></td>
<td>You may allow read-only or read-write access.</td>
</tr>
<tr>
<td>List of user shares</td>
<td>Select users that the map is accessible to.</td>
</tr>
<tr>
<td></td>
<td>You may allow read-only or read-write access.</td>
</tr>
</tbody>
</table>

When you click on Add to save this map, you have created an empty map with a name, dimensions and certain preferences. Now you need to add some elements. For that, click on Constructor in the map list to open the editable area.

Adding elements

To add an element, click on Add next to **Map element**. The new element will appear at the top left corner of the map. Drag and drop it wherever you like.

Note that with the Grid option “On”, elements will always align to the grid (you can pick various grid sizes from the dropdown, also hide/show the grid). If you want to put elements anywhere without alignment, turn the option to “Off”. (Random elements can later again be aligned to the grid with the Align map elements button.)

Now that you have some elements in place, you may want to start differentiating them by giving names etc. By clicking on the element, a form is displayed and you can set the element type, give a name, choose a different icon etc.
Map element attributes:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Type      | Type of the element:  
  - **Host** - icon representing status of all triggers of the selected host  
  - **Map** - icon representing status of all elements of a map  
  - **Trigger** - icon representing status of one or more triggers  
  - **Host group** - icon representing status of all triggers of all hosts belonging to the selected group  
  - **Image** - an icon, not linked to any resource |
| Label     | Icon label, any string.  
  - **Macros** and multiline strings can be used in labels. |
| Label location | Label location in relation to the icon:  
  - **Default** - map's default label location  
  - **Bottom** - beneath the icon  
  - **Left** - to the left  
  - **Right** - to the right  
  - **Top** - above the icon |
<p>| Host      | Enter the host, if the element type is 'Host'. This field is auto-complete so starting to type the name of a host will offer a dropdown of matching hosts. Scroll down to select. Click on 'x' to remove the selected. |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Map</td>
<td>Select the map, if the element type is ‘Map’.</td>
</tr>
<tr>
<td>Triggers</td>
<td>If the element type is ‘Trigger’, select one or more triggers in the New triggers field below and click on Add. The order of selected triggers can be changed, but only within the same severity of triggers. Multiple trigger selection also affects (HOST.*) macro resolution both in the construction and view modes.</td>
</tr>
<tr>
<td></td>
<td>// 1 In construction mode/ the first displayed (HOST.*) macros will be resolved depending on the first trigger in the list (based on trigger severity).</td>
</tr>
<tr>
<td></td>
<td>// 2 View mode// depends on the Display problems parameter in General map attributes.</td>
</tr>
<tr>
<td></td>
<td>* If Expand single problem mode is chosen the first displayed (HOST.*) macros will be resolved depending on the latest detected problem trigger (not mattering the severity) or the first trigger in the list (in case no problem detected);</td>
</tr>
<tr>
<td></td>
<td>* If Number of problems and expand most critical one mode is chosen the first displayed (HOST.*) macros will be resolved depending on the trigger severity.</td>
</tr>
<tr>
<td>Host group</td>
<td>Enter the host group, if the element type is ‘Host group’. This field is auto-complete so starting to type the name of a group will offer a dropdown of matching groups. Scroll down to select. Click on ‘x’ to remove the selected.</td>
</tr>
<tr>
<td>Application</td>
<td>You can select an application, allowing to only display problems of triggers that belong to the given application. This field is available for host and host group element types, and supported since Zabbix 2.4.0.</td>
</tr>
<tr>
<td>Automatic icon selection</td>
<td>In this case an icon mapping will be used to determine which icon to display.</td>
</tr>
<tr>
<td>Icons</td>
<td>You can choose to display different icons for the element in these cases: default, problem, maintenance, disabled.</td>
</tr>
<tr>
<td>Coordinate X</td>
<td>X coordinate of the map element.</td>
</tr>
<tr>
<td>Coordinate Y</td>
<td>Y coordinate of the map element.</td>
</tr>
<tr>
<td>URLs</td>
<td>Element-specific URLs can be set for the element. These will be displayed as links when a user clicks on the element in the map viewing mode. If the element has its own URLs and there are map level URLs for its type defined, they will be combined in the same menu.</td>
</tr>
</tbody>
</table>

**Attention:**

Added elements are not automatically saved. If you navigate away from the page, all changes may be lost. Therefore it is a good idea to click on the **Update** button in the top right corner. Once clicked, the changes are saved regardless of what you choose in the following popup.

Selected grid options are also saved with each map.

Selecting elements

To select elements, select one and then hold down Ctrl to select the others.

You can also select multiple elements by dragging a rectangle in the editable area and selecting all elements in it (option available since Zabbix 2.0).

Once you select more than one element, the element property form shifts to the mass-update mode so you can change attributes of selected elements in one go. To do so, mark the attribute using the checkbox and enter a new value for it. You may use macros here (such as, say, {HOST.NAME} for the element label).
Linking elements

Once you have put some elements on the map, it is time to start linking them. To link two elements you must first select them. With the elements selected, click on Add next to Link.

With a link created, the single element form now contains an additional Links section. Click on Edit to edit link attributes.
Link attributes:
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>Label that will be rendered on top of the link. The {host:key.func(param)} macro is supported in this field, but only with avg, last, min and max trigger functions, with seconds as parameter.</td>
</tr>
<tr>
<td>Connect to</td>
<td>The element that the link connects to.</td>
</tr>
<tr>
<td>Type (OK)</td>
<td>Default link style:</td>
</tr>
<tr>
<td></td>
<td><strong>Line</strong> - single line</td>
</tr>
<tr>
<td></td>
<td><strong>Bold line</strong> - bold line</td>
</tr>
<tr>
<td></td>
<td><strong>Dot</strong> - dots</td>
</tr>
<tr>
<td></td>
<td><strong>Dashed line</strong> - dashed line</td>
</tr>
<tr>
<td>Color (OK)</td>
<td>Default link color.</td>
</tr>
<tr>
<td>Link indicators</td>
<td>List of triggers linked to the link. In case a trigger has status PROBLEM, its style is applied to the link.</td>
</tr>
</tbody>
</table>

Moving and copy-pasting elements

Several selected elements can be **moved** to another place in the map by clicking on one of the selected elements, holding down the mouse button and moving the cursor to the desired location.

One or more elements can be **copied** by selecting the elements, then clicking on a selected element with the right mouse button and selecting Copy from the menu.

To paste the elements, click on a map area with the right mouse button and select Paste from the menu. The Paste without external links option will paste the elements retaining only the links that are between the selected elements.

Copy-pasting works within the same browser window. Keyboard shortcuts are not supported.

Adding shapes

In addition to map elements, it is also possible to add some shapes. Shapes are not map elements; they are just a visual representation. For example, a rectangle shape can be used as a background to group some hosts. Rectangle and ellipse shapes can be added.

To add a shape, click on Add next to Shape. The new shape will appear at the top left corner of the map. Drag and drop it wherever you like.

A new shape is added with default colors. By clicking on the shape, a form is displayed and you can customize the way a shape looks, add text, etc.
To select shapes, select one and then hold down Ctrl to select the others. With several shapes selected, common properties can be mass updated, similarly as with elements.

Text can be added in the shapes. To display text only the shape can be made invisible by removing the shape border (select 'None' in the Border field). For example, take note of how the `{MAP.NAME}` macro, visible in the screenshot above, is actually a rectangle shape with text, which can be seen when clicking on the macro:

{MAP.NAME} resolves to the configured map name, when viewing the map.

If hyperlinks are used in the text, they become clickable when viewing the map.

Line wrapping for text is always "on" within shapes. However, within an ellipse the lines are wrapped as though the ellipse were
Adding lines

In addition to shapes, it is also possible to add some lines. Lines can be used to link elements or shapes in a map.

To add a line, click on Add next to Shape. A new shape will appear at the top left corner of the map. Select it and click on Line in the editing form to change the shape into a line. Then adjust line properties, such as line type, width, color, etc.

Ordering shapes and lines

To bring one shape in front of the other (or vice versa) click on the shape with the right mouse button bringing up the map shape menu.
2 Host group elements

Overview

This section explains how to add a “Host group” type element when configuring a network map.

Configuration
All mandatory input fields are marked with a red asterisk.

This table consists of parameters typical for Host group element type:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select Type of the element:</td>
</tr>
<tr>
<td></td>
<td><strong>Host group</strong> - icon representing status of all triggers of all hosts belonging to the selected group</td>
</tr>
<tr>
<td>Show</td>
<td>Show options:</td>
</tr>
<tr>
<td></td>
<td><strong>Host group</strong> - selecting this option will result as one single icon displaying corresponding information about the certain host group</td>
</tr>
<tr>
<td></td>
<td><strong>Host group elements</strong> - selecting this option will result as multiple icons displaying corresponding information about each single element (host) of the certain host group</td>
</tr>
<tr>
<td>Area type</td>
<td>This setting is available if “Host group elements” parameter is selected:</td>
</tr>
<tr>
<td></td>
<td><strong>Fit to map</strong> - all host group elements are equally placed within the map</td>
</tr>
<tr>
<td></td>
<td><strong>Custom size</strong> - manual setting of the map area for all the host group elements to be displayed</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Area size</td>
<td>This setting is available if “Host group elements” parameter and “Area type” parameter are selected:</td>
</tr>
<tr>
<td></td>
<td><strong>Width</strong> - numeric value to be entered to specify map area width</td>
</tr>
<tr>
<td></td>
<td><strong>Height</strong> - numeric value to be entered to specify map area height</td>
</tr>
<tr>
<td>Placing algorithm</td>
<td>Grid - only available option of displaying all the host group elements</td>
</tr>
<tr>
<td>Label</td>
<td>Icon label, any string.</td>
</tr>
<tr>
<td></td>
<td><strong>Macros</strong> and multiline strings can be used in labels.</td>
</tr>
<tr>
<td></td>
<td>If the type of the map element is “Host group” specifying a certain Macro has impact on the map view displaying corresponding information about each single host. For example, if {HOST.IP} macro is used, edit map view will only display the macro {HOST.IP} itself while map view will include and display each host’s unique IP address</td>
</tr>
</tbody>
</table>

**Viewing host group elements**

This option is available if “Host group elements” show option is chosen. When selecting “Host group elements” as the show option, you will at first see only one icon for the host group. However, when you save the map and then go to the map view, you will see that the map includes all the elements (hosts) of the certain host group:

Notice how the {HOST.NAME} macro is used. In map editing the macro name in unresolved, while in map view all the unique names of the hosts are displayed.

**3 Link indicators**

**Overview**

You can assign some triggers to a link between elements in a network map. When these triggers go into a problem state, the link can reflect that.
When you configure a link, you set the default link type and color. When you assign triggers to a link, you can assign different link types and colors with these triggers.

Should any of these triggers go into a problem state, their link style and color will be displayed on the link. So maybe your default link was a green line. Now, with the trigger in problem state, your link may become bold red (if you have defined it so).

Configuration

To assign triggers as link indicators, do the following:

- select a map element
- click on Edit in the Links section for the appropriate link
- click on Add in the Link indicators block and select one or more triggers
All mandatory input fields are marked with a red asterisk.

Added triggers can be seen in the Link indicators list.

You can set the link type and color for each trigger directly from the list. When done, click on Apply, close the form and click on Update to save the map changes.

Display

In Monitoring → Maps the respective color will be displayed on the link if the trigger goes into a problem state.

**Note:**

If multiple triggers go into a problem state, the problem with the highest severity will determine the link style and color. If multiple triggers with the same severity are assigned to the same map link, the one with the lowest ID takes precedence.

Note also that:

1. Minimum trigger severity and Show suppressed problem settings from map configuration affect which problems are taken into account.
2. In case with triggers with multiple problems (multiple problem generation), each problem may have severity that differs from trigger severity (changed manually), may have different tags (due to macros) and may be suppressed.

### 3 Screens

**Overview**

On Zabbix screens you can group information from various sources for a quick overview on a single screen. Building the screens is quite easy and intuitive.

Essentially a screen is a table. You choose how many cells per table and what elements to display in the cells. The following elements can be displayed:

- simple graphs
- simple graph prototypes
- user-defined custom graphs
- custom graph prototypes
- maps
- other screens
Global screens are managed in Monitoring → Screens, where they can be configured, managed and viewed. They can also be added to the favorites section of Monitoring → Dashboard.

Host-level screens are configured on template level and then generated for hosts once the template is linked to the hosts.

To configure a screen you must first create it by defining its general properties and then add individual elements in the cells.

All users in Zabbix (including non-admin users) can create screens. Screens have an owner - the user who created them.

Screens can be made public or private. Public screens are visible to all users.

Private screens are visible only to their owner. Private screens can be shared by the owner to other users and user groups. Regular (non-Super admin) users can only share with the groups and users they are member of. Private screens will be visible to their owner and the users the screen is shared with as long as they have read permissions to all screen elements. Admin level users, as long as they have read permissions to all screen elements, can see and edit private screens regardless of being the owner or belonging to the shared user list.

**Warning:**
For both public and private screens a user must have at least read permissions to all screen elements in order to see the screen. To add an element to a screen a user must also have at least read permission to it.

Creating a screen

To create a screen, do the following:

- Go to Monitoring → Screens
- Go to the view with all screens
- Click on Create Screen

The **Screen** tab contains general screen attributes:

All mandatory input fields are marked with a red asterisk.

Give your screen a unique name and set the number of columns (vertical cells) and rows (horizontal cells).

The **Sharing** tab contains the screen type as well as sharing options (user groups, users) for private screens:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owner</td>
<td>Select the screen owner.</td>
</tr>
<tr>
<td>Type</td>
<td>Select screen type:</td>
</tr>
<tr>
<td></td>
<td><strong>Private</strong> - screen is visible only to selected user groups and users</td>
</tr>
<tr>
<td></td>
<td><strong>Public</strong> - screen is visible to all</td>
</tr>
<tr>
<td>List of user group shares</td>
<td>Select user groups that the screen is accessible to.</td>
</tr>
<tr>
<td></td>
<td>You may allow read-only or read-write access.</td>
</tr>
<tr>
<td>List of user shares</td>
<td>Select users that the screen is accessible to.</td>
</tr>
<tr>
<td></td>
<td>You may allow read-only or read-write access.</td>
</tr>
</tbody>
</table>

Click on Add to save the screen.

Adding elements

To add elements to the screen, click on Constructor next to the screen name in the list.

On a new screen you probably only see links named Change. Clicking those links opens a form whereby you set what to display in each cell.

On an existing screen you click on the existing elements to open the form whereby you set what to display.
All mandatory input fields are marked with a red asterisk.

Screen element attributes:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource</td>
<td>Information displayed in the cell:</td>
</tr>
<tr>
<td></td>
<td><strong>Action log</strong> - history of recent actions</td>
</tr>
<tr>
<td></td>
<td><strong>Clock</strong> - digital or analog clock displaying current server or local time</td>
</tr>
<tr>
<td></td>
<td><strong>Data overview</strong> - latest data for a group of hosts</td>
</tr>
<tr>
<td></td>
<td><strong>Graph</strong> - single custom graph</td>
</tr>
<tr>
<td></td>
<td><strong>Graph prototype</strong> - custom graph from low-level discovery rule</td>
</tr>
<tr>
<td></td>
<td><strong>History of events</strong> - latest events</td>
</tr>
<tr>
<td></td>
<td><strong>Host group issues</strong> - status of triggers filtered by the host group</td>
</tr>
<tr>
<td></td>
<td>(includes triggers without events, since Zabbix 2.2)</td>
</tr>
<tr>
<td></td>
<td><strong>Host info</strong> - high level host related information</td>
</tr>
<tr>
<td></td>
<td><strong>Host issues</strong> - status of triggers filtered by the host</td>
</tr>
<tr>
<td></td>
<td>(includes triggers without events, since Zabbix 2.2)</td>
</tr>
<tr>
<td></td>
<td><strong>Map</strong> - single map</td>
</tr>
<tr>
<td></td>
<td><strong>Plain text</strong> - plain text data</td>
</tr>
<tr>
<td></td>
<td><strong>Screen</strong> - screen (one screen may contain other screens inside)</td>
</tr>
<tr>
<td></td>
<td><strong>Simple graph</strong> - single simple graph</td>
</tr>
<tr>
<td></td>
<td><strong>Simple graph prototype</strong> - simple graph based on item generated by low-level discovery</td>
</tr>
<tr>
<td></td>
<td><strong>System information</strong> - high-level information about Zabbix server</td>
</tr>
<tr>
<td></td>
<td><strong>Problems by severity</strong> - displays problems by severity (similar to the Dashboard)</td>
</tr>
<tr>
<td></td>
<td><strong>Trigger info</strong> - high level trigger related information</td>
</tr>
<tr>
<td></td>
<td><strong>Trigger overview</strong> - status of triggers for a host group</td>
</tr>
<tr>
<td></td>
<td><strong>URL</strong> - include content from the specified resource</td>
</tr>
</tbody>
</table>

See also more information on configuring each resource.

Horizontal align
Possible values:
- Center
- Left
- Right

Vertical align
Possible values:
- Middle
- Top
- Bottom

Column span
Extend cell to a number of columns, same way as HTML column spanning works.

Row span
Extend cell to a number of rows, same way as HTML row spanning works.

Take note of the `+' and `-` controls on each side of the table.
Clicking on `+' above the table will add a column. Clicking on `-` beneath the table will remove a column.
Clicking on `+' on the left side of the table will add a row. Clicking on `-` on the right side of the table will remove a row.

**Attention:**
If graph height is set as less than 120 pixels, no trigger will be displayed in the legend.

Dynamic elements

For some of the elements there is an extra option called Dynamic item. Checking this box at first does not to seem to change anything.

However, once you go to Monitoring → Screens, you may realize that now you have extra dropdowns there for selecting the host. Thus you have a screen where some elements display the same information while others display information depending on the currently selected host.

The benefit of this is that you do not need to create extra screens just because you want to see the same graphs containing data from various hosts.
Dynamic item option is available for several screen elements:

- Graphs (custom graphs)
- Graph prototypes
- Simple graphs
- Simple graph prototypes
- Plain text
- URL

**Note:**
Clicking on a dynamic graph opens it in full view; although with custom graphs and graph prototypes that is currently supported with the default host only (i.e. with host 'not selected' in the dropdown). When selecting another host in the dropdown, the dynamic graph is created using item data of that host and the resulting graph is not clickable.

**Note:**
Dynamic URL elements will not be displayed in Monitoring → Screens, unless a host is selected. Without a selected host the “No host selected” message will be visible only.

### 1 Screen elements

#### Overview

This section lists available screen elements and provides details for screen element configuration.

#### 1 Action log

In the action log element you can display details of action operations (notifications, remote commands). It replicates information from Reports → Audit.

To configure, select Action log as resource:

All mandatory input fields are marked with a red asterisk.

You may set the following specific options:

<table>
<thead>
<tr>
<th>Show lines</th>
<th>Set how many action log lines will be displayed in the screen cell.</th>
</tr>
</thead>
</table>
| Sort entries by | Sort entries by:  
  - **Time** (descending or ascending)  
  - **Type** (descending or ascending)  
  - **Status** (descending or ascending)  
  - **Recipient** (descending or ascending). |

#### 2 Clock

In the clock element you may display local, server or specified host time.

To configure, select Clock as resource:

You may set the following specific options:

<table>
<thead>
<tr>
<th>Time type</th>
<th>Select local, server or specified host time.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item</td>
<td>Select the item for displaying time. To display host time, use the <code>system.localtime[local]</code> item. This item must exist on the host. This field is available only when Host time is selected.</td>
</tr>
<tr>
<td>Width</td>
<td>Select clock width.</td>
</tr>
<tr>
<td>Height</td>
<td>Select clock height.</td>
</tr>
</tbody>
</table>

#### 3 Data overview

In the data overview element you can display the latest data for a group of hosts. It replicates information from Monitoring → Overview (when Data is selected as Type there).

To configure, select Data overview as resource:
You may set the following specific options:

<table>
<thead>
<tr>
<th>Group</th>
<th>Select host group.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Enter application name.</td>
</tr>
<tr>
<td>Hosts location</td>
<td>Select host location - left or top.</td>
</tr>
</tbody>
</table>

4 Graph

In the graph element you can display a single custom graph.

To configure, select Graph as resource:

You may set the following specific options:

<table>
<thead>
<tr>
<th>Graph</th>
<th>Select the graph to display.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Width</td>
<td>Select graph width.</td>
</tr>
<tr>
<td></td>
<td>Note that a line graph may actually take up more space due to legend text.</td>
</tr>
<tr>
<td>Height</td>
<td>Select graph height.</td>
</tr>
<tr>
<td></td>
<td>Note that a line graph may actually take up more space due to legend text.</td>
</tr>
<tr>
<td>Dynamic item</td>
<td>Set graph to display different data depending on the selected host.</td>
</tr>
</tbody>
</table>

5 Graph prototype

In the graph prototype element you can display a custom graph from a low-level discovery rule.

To configure, select Graph prototype as resource:

You may set the following specific options:

<table>
<thead>
<tr>
<th>Graph prototype</th>
<th>Select the graph prototype to display.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max columns</td>
<td>In how many columns generated graphs should be displayed in the screen cell.</td>
</tr>
<tr>
<td></td>
<td>Useful when there are many LLD-generated graphs.</td>
</tr>
<tr>
<td>Width</td>
<td>Select graph width.</td>
</tr>
<tr>
<td></td>
<td>Note that a line graph may actually take up more space due to legend text.</td>
</tr>
<tr>
<td>Height</td>
<td>Select graph height.</td>
</tr>
<tr>
<td></td>
<td>Note that a line graph may actually take up more space due to legend text.</td>
</tr>
<tr>
<td>Dynamic item</td>
<td>Set graph to display different data depending on the selected host.</td>
</tr>
</tbody>
</table>

6 History of events

In the history of events element you can display latest events.

To configure, select History of events as resource:

You may set the following specific option:

| Show lines | Set how many event lines will be displayed in the screen cell. |

7 Host group issues

In the host group issue element you can display problem details filtered by the selected host group.

The problem severity color displayed is originally from the underlying trigger, but can be adjusted in the problem update screen.

To configure, select Host group issues as resource:

You may set the following specific options:
### 8 Host info

In the host information element you can display high-level information about host availability.

To configure, select Host info as resource:

You may set the following specific options:

<table>
<thead>
<tr>
<th>Group</th>
<th>Select host group(s).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Style</td>
<td>Select vertical or horizontal display.</td>
</tr>
</tbody>
</table>

### 9 Host issues

In the host issue element you can display problem details filtered by the selected host.

The problem severity color displayed is originally from the underlying trigger, but can be adjusted in the problem update screen.

To configure, select Host issues as resource:

You may set the following specific options:

<table>
<thead>
<tr>
<th>Host</th>
<th>Select the host.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show lines</td>
<td>Set how many problem lines will be displayed in the screen cell.</td>
</tr>
<tr>
<td>Sort triggers by</td>
<td>Select from the dropdown to sort problems by last change, severity (both descending) or host (ascending).</td>
</tr>
</tbody>
</table>

### 10 Map

In the map element you can display a configured network map.

To configure, select Map as resource:

You may set the following specific options:

| Map       | Select the map to display. |

### 11 Plain text

In the plain text element you can display latest item data in plain text.

To configure, select Plain text as resource:

You may set the following specific options:

<table>
<thead>
<tr>
<th>Item</th>
<th>Select the item.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show lines</td>
<td>Set how many latest data lines will be displayed in the screen cell.</td>
</tr>
<tr>
<td>Show text as HTML</td>
<td>Set to display text as HTML.</td>
</tr>
<tr>
<td>Dynamic item</td>
<td>Set to display different data depending on the selected host.</td>
</tr>
</tbody>
</table>

### 12 Screen

In the screen element you can display another Zabbix screen. One screen may contain other screens inside.

To configure, select Screen as resource:

You may set the following specific options:
13 Simple graph

In the simple graph element you can display a single simple graph.

To configure, select Simple graph as resource:

You may set the following specific options:

<table>
<thead>
<tr>
<th>Item</th>
<th>Select the item for the simple graph.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Width</td>
<td>Select graph width. Note that a line graph may actually take up more space due to legend text.</td>
</tr>
<tr>
<td>Height</td>
<td>Select graph height. Note that a line graph may actually take up more space due to legend text.</td>
</tr>
<tr>
<td>Dynamic item</td>
<td>Set graph to display different data depending on the selected host.</td>
</tr>
</tbody>
</table>

14 Simple graph prototype

In the simple graph prototype element you can display a simple graph based on an item generated by low-level discovery.

To configure, select Simple graph prototype as resource:

You may set the following specific options:

| Item prototype | Select the item prototype for the simple graph. |
| Max columns | In how many columns generated graphs should be displayed in the screen cell. Useful when there are many LLD-generated graphs. |
| Width | Select graph width. Note that a line graph may actually take up more space due to legend text. |
| Height | Select graph height. Note that a line graph may actually take up more space due to legend text. |
| Dynamic item | Set graph to display different data depending on the selected host. |

15 System information

In the system information element you can display high-level Zabbix and Zabbix server information.

To configure, select System information as resource:

16 Problems by severity

In this element you can display problems by severity similarly as in the Dashboard widget.
To configure, select Problems by severity as resource:

<table>
<thead>
<tr>
<th>Resource</th>
<th>Problems by severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vertical align</td>
<td>Top Middle Bottom</td>
</tr>
<tr>
<td>* Column span</td>
<td>1</td>
</tr>
<tr>
<td>* Row span</td>
<td>1</td>
</tr>
<tr>
<td>Add</td>
<td>Cancel</td>
</tr>
</tbody>
</table>

17 Trigger info

In the trigger info element you can display high-level information about trigger states.

To configure, select Trigger info as resource:

You may set the following specific options:

- **Group**: Select the host group(s).
- **Style**: Select vertical or horizontal display.

18 Trigger overview

In the trigger overview element you can display the trigger states for a group of hosts. It replicates information from Monitoring → Overview (when Triggers is selected as Type there).

To configure, select Trigger overview as resource:

You may set the following specific options:

- **Group**: Select the host group(s).
- **Application**: Enter the application name.
- **Hosts location**: Select host location - left or top.

19 URL

The URL element displays the content retrieved from the specified URL.

To configure, select URL as resource:

You may set the following specific options:

- **URL**: Enter the URL to display. Relative paths are allowed since Zabbix 4.0.20.
- **Width**: Select window width.
- **Height**: Select window width.
- **Dynamic item**: Set to display different URL content depending on the selected host.

**Attention:**

Browsers might not load an HTTP page included in a screen (using URL element), if Zabbix frontend is accessed over HTTPS.
4 Slide shows

Overview

In a slide show you can configure that a number of screens are displayed one after another at set intervals. Sometimes you might want to switch between some configured screens. While that can be done manually, doing that more than once or twice may become very tedious. This is where the slide show function comes to rescue.

All users in Zabbix (including non-admin users) can create slide shows. Slide shows have an owner - the user who created them. Slide shows can be made public or private. Public slide shows are visible to all users, however, they must have at least read permissions to all slide show elements (screens) to see it. To add a screen to the slide show the user must also have at least read permission to it.

Private slide shows are visible only to their owner. Private slide shows can be shared by the owner to other users and user groups. Regular (non-Super admin) users can only share with the groups and users they are member of. Private slide shows will be visible to their owner and the users the slide show is shared with as long as they have read permissions to all included screens. Admin level users, as long as they have read permissions to all included screens, can see and edit private slide shows regardless of being the owner or belonging to the shared user list.

Configuration

To create a slide show, do the following:

• Go to Monitoring → Screens
• Select Slide shows in the dropdown
• Go to the view with all slide shows
• Click on Create slide show

The Slide tab contains general slide show attributes:

All mandatory input fields are marked with a red asterisk.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owner</td>
<td>Select the slide show owner. Specifying owner is mandatory. Unique name of the slide show.</td>
</tr>
<tr>
<td>Name</td>
<td>How long one screen is displayed by default, before rotating to the next. Time suffixes are supported, e.g. 30s, 5m, 2h, 1d.</td>
</tr>
<tr>
<td>Default delay</td>
<td>List of screens to be rotated. Click on Add to select screens. The Up/Down arrow before the screen allows to drag a screen up and down in the sort order of display.</td>
</tr>
<tr>
<td>Slides</td>
<td>If you want to display only, say, a single graph in the slide show, create a screen containing just that one graph.</td>
</tr>
<tr>
<td>Screen</td>
<td>Screen name.</td>
</tr>
<tr>
<td>Delay</td>
<td>A custom value for how long the screen will be displayed, in seconds. If set to 0, the Default delay value will be used.</td>
</tr>
<tr>
<td>Action</td>
<td>Click on Remove to remove a screen from the slide show.</td>
</tr>
</tbody>
</table>

The slide show in this example consists of two screens which will be displayed in the following order:

Zabbix server → Displayed for 30 seconds → Zabbix server2 → Displayed for 15 seconds → Zabbix server → Displayed for 30 seconds → Zabbix server2 → ...

The Sharing tab contains the slide show type as well as sharing options (user groups, users) for private slide shows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select slide show type:</td>
</tr>
<tr>
<td></td>
<td><strong>Private</strong> - slide show is visible only to selected user groups and users</td>
</tr>
<tr>
<td></td>
<td><strong>Public</strong> - slide show is visible to all</td>
</tr>
<tr>
<td>List of user group shares</td>
<td>Select user groups that the slide show is accessible to. You may allow read-only or read-write access.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>List of user shares</td>
<td>Select users that the slide show is accessible to. You may allow read-only or read-write access.</td>
</tr>
</tbody>
</table>

Click on Add to save the slide show.

Display

Slide shows that are ready can be viewed in Monitoring → Screens, then choosing Slide shows from the dropdown and clicking on the slide show name.

With the Menu option next to the dropdown, you can accelerate or slow down the display by choosing a slide delay multiplier:

![Refresh Interval Multiplier](image)

**Attention:**
If a delay ends up as being less than 5 seconds (either by having entered a delay less than 5 seconds or by using the slide delay multiplier), a 5-second minimum delay will be used.

## 5 Host screens

Overview

Host screens look similar to global screens, however, host screens display data about the host only. Host screens are configured on the template level and then are generated for a host, once the template is linked to the host.

Host screens cannot be configured or directly accessed in the Monitoring → Screens section, which is reserved for global screens. The ways to access host screens are listed below in this section.
Accessing host screens

Access to host screens is provided:

- From the **host menu** that is available in many frontend locations:
  - click on the host name and then select Host screens from the drop-down menu

- When searching for a host name in **global search**:
  - click on the Screens link provided in search results

- When clicking on a host name in Inventory → **Hosts**:
  - click on the Screens link provided
7 Templates

Overview

A template is a set of entities that can be conveniently applied to multiple hosts.

The entities may be:

- items
- triggers
- graphs
- applications
- screens (since Zabbix 2.0)
- low-level discovery rules (since Zabbix 2.0)
- web scenarios (since Zabbix 2.2)

As many hosts in real life are identical or fairly similar so it naturally follows that the set of entities (items, triggers, graphs,...) you have created for one host, may be useful for many. Of course, you could copy them to each new host, but that would be a lot of manual work. Instead, with templates you can copy them to one template and then apply the template to as many hosts as needed.

When a template is linked to a host, all entities (items, triggers, graphs,...) of the template are added to the host. Templates are assigned to each individual host directly (and not to a host group).

Templates are often used to group entities for particular services or applications (like Apache, MySQL, PostgreSQL, Postfix...) and then applied to hosts running those services.

Another benefit of using templates is when something has to be changed for all the hosts. Changing something on the template level once will propagate the change to all the linked hosts.

Thus, the use of templates is an excellent way of reducing one’s workload and streamlining the Zabbix configuration.

Proceed to creating and configuring a template.

8 Templates out of the box

Overview

Zabbix strives to provide a growing list of useful out-of-the-box templates. Out-of-the-box templates come preconfigured and thus are a useful way for speeding up the deployment of monitoring jobs.

1 Standardized templates for network devices

Overview

In order to provide monitoring for network devices such as switches and routers, we have created two so-called models: for the network device itself (its chassis basically) and for network interface.

Since Zabbix 3.4 templates for many families of network devices are provided. All templates cover (where possible to get these items from the device):

- Chassis fault monitoring (power supplies, fans and temperature, overall status)
- Chassis performance monitoring (CPU and memory items)
- Chassis inventory collection (serial numbers, model name, firmware version)
- Network interface monitoring with IF-MIB and EtherLike-MIB (interface status, interface traffic load, duplex status for Ethernet)

These templates are available:

- In new installations - in Configuration → Templates;
- If you are upgrading from previous versions, you can find these templates in the templates directory of the downloaded latest Zabbix version. While in Configuration → Templates you can import them manually from this directory.

If you are importing the new out-of-the-box templates, you may want to also update the @Network interfaces for discovery global regular expression to:
Result is FALSE: ^Software Loopback Interface
Result is FALSE: ^(In)?[1L]oop[0-9._]*$
Result is FALSE: ^NULL[0-9._]*$
Result is FALSE: ^[sS]ystem$
Result is FALSE: ^Nu[0-9._]*$

to filter out loopbacks and null interfaces on most systems.

Devices

List of device families for which templates are available:

<table>
<thead>
<tr>
<th>Template name</th>
<th>Device family</th>
<th>Known models</th>
<th>OS used</th>
<th>Tags</th>
</tr>
</thead>
<tbody>
<tr>
<td>Net Alcatel Alcatel</td>
<td>ALCATEL SR 7750</td>
<td>TIMETRA- SYSTEM-MIB, TIMETRA- CHASSIS-MIB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Timetra TIMOS SNMPv2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Template Net Brocade Brocade FC</td>
<td>Brocade 300 SAN Switch</td>
<td>SW- Performance, Fault MIB, ENTITY-MIB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Template Net Brocade_Brocade Foundry ICX</td>
<td>Brocade ICX6610, Brocade ICX7250-48, Brocade ICX7450-48F</td>
<td>FOUNDRY- Certified SN- AGENT-MIB, FOUNDRY- STACKING-MIB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Template Net Brocade_Brocade Foundry Foundry Nonstackable SNMPv2</td>
<td>Brocade MLXe, Foundry FLS648, Foundry FWSX424</td>
<td>FOUNDRY- Performance, Fault SN- AGENT-MIB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Template Net Cisco Cisco IOS</td>
<td>Cisco C2950</td>
<td>IOS CISCO- PROCESS-MIB, CISCO- MEMORY-POOL-MIB, CISCO- ENVMON-MIB Certified</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Template Net Cisco Cisco IOS releases</td>
<td>-</td>
<td>IOS CISCO- PROCESS-MIB, CISCO- MEMORY-POOL-MIB, CISCO- ENVMON-MIB Certified</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Template Net Cisco releases later than 12.0_3_T and prior to 12.2_3.5_SNMPv2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Template Net Cisco releases prior to 12.0_3_T SNMPv2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

398
<table>
<thead>
<tr>
<th>Template name</th>
<th>Vendor</th>
<th>Device family</th>
<th>Known models</th>
<th>OS</th>
<th>MIBs used</th>
<th>Tags</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template Net</td>
<td>D-Link</td>
<td>DES-7xxx</td>
<td>D-Link DES 7206</td>
<td>-</td>
<td>ENTITY-MIB, MY-SYSTEM-MIB, MY-PROCESS-MIB, MY-MEMORY-MIB</td>
<td>Performance Fault Interfaces</td>
</tr>
<tr>
<td>Template Net</td>
<td>Dell</td>
<td>Dell Force S-Series</td>
<td>S4810</td>
<td>-</td>
<td>F10-S-SERIES-CHASSIS-MIB</td>
<td>Certified</td>
</tr>
<tr>
<td>Template Net</td>
<td>Extreme</td>
<td>EXOS</td>
<td>X670V-48x</td>
<td>-</td>
<td>EXO-EXTREME-MIB, EXTREME-SYSTEM-MIB, EXTREME-SOFTWARE-MONITOR-MIB</td>
<td>Certified</td>
</tr>
<tr>
<td>Template Net</td>
<td>Huawei</td>
<td>VRP</td>
<td>S2352P-EI</td>
<td>-</td>
<td>ENTITY-MIB, HUAWEI-ENTITY-EXTENT-MIB, ICS-CHASSIS-MIB</td>
<td>Certified</td>
</tr>
<tr>
<td>Template Net</td>
<td>Intel/QLogic</td>
<td>Infiniband devices</td>
<td>12300</td>
<td>-</td>
<td>JunIPER-MIB</td>
<td>Fault Inventory</td>
</tr>
<tr>
<td>Template Net</td>
<td>Juniper</td>
<td>MX,SRX,EX models</td>
<td>Juniper MX240, Juniper EX4200-24F</td>
<td>-</td>
<td>JunIPER-MIB</td>
<td>Certified</td>
</tr>
<tr>
<td>Template Net</td>
<td>Mellanox</td>
<td>Infiniband devices</td>
<td>SX1036</td>
<td>-</td>
<td>MLNXHOST-OS-MIB, ENTITY-MIB, ENTITY-SENSOR-MIB, MELLANOX-MIB</td>
<td>Certified</td>
</tr>
<tr>
<td>Template name</td>
<td>Vendor</td>
<td>Device family</td>
<td>Known models</td>
<td>OS used</td>
<td>Tags</td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>--------</td>
<td>---------------</td>
<td>--------------</td>
<td>---------</td>
<td>------</td>
<td></td>
</tr>
<tr>
<td>Net QTech SNMPv2</td>
<td>QTech</td>
<td>Qtech devices</td>
<td>Qtech QSW-2800-28T</td>
<td>SNMPv2</td>
<td>QTECH-PerformanceInventory MIB, ENTITY-MIB</td>
<td></td>
</tr>
<tr>
<td>Net Ubiquiti SNMPv2</td>
<td>Ubiquiti</td>
<td>AirOS wireless devices</td>
<td>NanoBridge, NanoStation, Unifi</td>
<td>SNMPv1</td>
<td>NanOS-RPC, NanOS-FORWARDING, NanOS-INTERFACES, NanOS-RESOURCES-MIB, IEEE802dot11-MIB</td>
<td></td>
</tr>
<tr>
<td>Net HP Comware SNMPv2</td>
<td>HP Comware</td>
<td>HP (H3C) Switch</td>
<td>HP A5500-24G-4SFP</td>
<td>SNMPv2</td>
<td>HH3C-CERTIFIED-ENTITY-EXT-MIB, ENTITY-MIB</td>
<td></td>
</tr>
<tr>
<td>Net HP Enterprise Switch SNMPv2</td>
<td>HP Enterprise Switch</td>
<td>HP ProCurve J9400B Switch</td>
<td>HP J9728A 2920-48G Switch</td>
<td>SNMPv2</td>
<td>STATISTICS-CERTIFIED-MIB, NETSWITCH-MIB, HP-ICF-CHASSIS-ENTITY-MIB, SEMI-MIB</td>
<td></td>
</tr>
<tr>
<td>Net TP-LINK SNMPv2</td>
<td>TP-LINK</td>
<td>TP-LINK T2600G-28TS v2.0</td>
<td>TP-LINK SYMONITOR-MIB, TP-LINK SYINFO-MIB</td>
<td>SNMPv2</td>
<td>TPLINK-PerformanceInventory MIB, FASTPATH-FAULT-INVENTORY SWITCHING-MIB, FASTPATH-BOXSERVICES-PRIVATE-MIB</td>
<td></td>
</tr>
<tr>
<td>Net Netgear Fastpath SNMPv2</td>
<td>Netgear Fastpath</td>
<td>M5300-28G</td>
<td>FASTPATH-Fault Inventory</td>
<td>SNMPv2</td>
<td>FASTPATH-FAULT-INVENTORY MIB, FASTPATH-BOXSERVICES-PRIVATE-MIB</td>
<td></td>
</tr>
</tbody>
</table>

Template design

Templates were designed with the following in mind:

- User macros are used as much as possible so triggers can be tuned by the user
- Low-level discovery is used as much as possible to minimize the number of unsupported items
- Templates are provided for SNMPv2. SNMPv1 is used if it is known that the majority of devices don’t support SNMPv2.
- All templates depend on Template ICMP Ping so all devices are also checked by ICMP
- Items don’t use any MIBs - SNMP OIDs are used in items and low-level discoveries. So it’s not necessary to load any MIBs into Zabbix for templates to work.
- Loopback network interfaces are filtered when discovering as well as interfaces with ifAdminStatus = down(2)
• 64bit counters are used from IF-MIB::ifXTable where possible. If it is not supported, default 32bit counters are used instead.
• All discovered network interfaces have a trigger that controls its operational status(link).
  - If you do not want to monitor this condition for a specific interface create a user macro with context with the value 0. For example:

![Image of Host Macros](image)

where Gi0/0 is {#IFNAME}. That way the trigger is not used any more for this specific interface.

* You can also change the default behavior for all triggers not to fire and activate this trigger only to limited number of interfaces like uplinks

Tags

• Performance – device family MIBs provide a way to monitor CPU and memory items;
• Fault - device family MIBs provide a way to monitor at least one temperature sensor;
• Inventory – device family MIBs provide a way to collect at least the device serial number and model name;
• Certified – all three main categories above are covered.

9 Notifications upon events

Overview

Assuming that we have configured some items and triggers and now are getting some events happening as a result of triggers changing state, it is time to consider some actions.

To begin with, we would not want to stare at the triggers or events list all the time. It would be much better to receive notification if something significant (such as a problem) has happened. Also, when problems occur, we would like to see that all the people concerned are informed.

That is why sending notifications is one of the primary actions offered by Zabbix. Who and when should be notified upon a certain event can be defined.

To be able to send and receive notifications from Zabbix you have to:

• define some media
• configure an action that sends a message to one of the defined media

Actions consist of conditions and operations. Basically, when conditions are met, operations are carried out. The two principal operations are sending a message (notification) and executing a remote command.
For discovery and auto-registration created events, some additional operations are available. Those include adding or removing a host, linking a template etc.

1 Media types

Overview

Media are the delivery channels used for sending notifications and alerts in Zabbix.

You can configure several media types:

• E-mail
• SMS
• Jabber
• Ez Texting
• Custom alertscripts

1 E-mail

Overview

To configure e-mail as the delivery channel for messages, you need to configure e-mail as the media type and assign specific addresses to users.

Configuration

To configure e-mail as the media type:

• Go to Administration → Media types
• Click on Create media type (or click on E-mail in the list of pre-defined media types).

The Media type tab contains general media type attributes:
All mandatory input fields are marked with a red asterisk.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the media type.</td>
</tr>
<tr>
<td>Type</td>
<td>Select Email as the type.</td>
</tr>
<tr>
<td>SMTP server</td>
<td>Set an SMTP server to handle outgoing messages.</td>
</tr>
<tr>
<td>SMTP server port</td>
<td>Set the SMTP server port to handle outgoing messages.  This option is supported starting with Zabbix 3.0.</td>
</tr>
<tr>
<td>SMTP helo</td>
<td>Set a correct SMTP helo value, normally a domain name.</td>
</tr>
</tbody>
</table>

Parameter Description

- **Name**: Email
- **Type**: Email
- **SMTP server**: mail.company.com
- **SMTP server port**: 25
- **SMTP helo**: company.com
- **SMTP email**: Zabbix info <zabbix@company.com>
- Connection security: None, STARTTLS, SSL/TLS
- **SSL verify peer**: False
- **SSL verify host**: False
- **Authentication**: None, Username and password
- **Username**: 
- **Password**: 
- **Enabled**: True
**Parameter** | **Description**
---|---
SMTP email | The address entered here will be used as the From address for the messages sent. Adding a sender display name (like "Zabbix-HQ" in Zabbix-HQ <zabbix@company.com> in the screenshot above) with the actual e-mail address is supported since Zabbix 2.2 version. There are some restrictions on display names in Zabbix emails in comparison to what is allowed by RFC 5322, as illustrated by examples: Valid examples: zabbix@company.com (only email address, no need to use angle brackets) Zabbix HQ <zabbix@company.com> (display name and email address in angle brackets) ΣΩ-monitoring <zabbix@company.com> (UTF-8 characters in display name) Invalid examples: Zabbix HQ zabbix@company.com (display name present but no angle brackets around email address) “Zabbix\@<H(comment)Q>“ <zabbix@company.com> (although valid by RFC 5322, quoted pairs and comments are not supported in Zabbix emails)

**Connection security** | Select the level of connection security:  
**None** - do not use the CURLOPT_USE_SSL option  
**STARTTLS** - use the CURLOPT_USE_SSL option with CURLUSESSL_ALL value  
**SSL/TLS** - use of CURLOPT_USE_SSL is optional  
This option is supported starting with Zabbix 3.0.

**SSL verify peer** | Mark the checkbox to verify the SSL certificate of the SMTP server. The value of “SSLCALocation” server configuration directive should be put into CURLOPT_CAPATH for certificate validation. This sets cURL option CURLOPT_SSL_VERIFYPEER.  
This option is supported starting with Zabbix 3.0.

**SSL verify host** | Mark the checkbox to verify that the Common Name field or the Subject Alternate Name field of the SMTP server certificate matches. This sets cURL option CURLOPT_SSL_VERIFYHOST.  
This option is supported starting with Zabbix 3.0.

**Authentication** | Select the level of authentication:  
**None** - no cURL options are set  
(since 3.4.2) **Username and password** - implies “AUTH=**” leaving the choice of authentication mechanism to cURL  
(untill 3.4.2) **Normal password** - CURLOPT_LOGIN_OPTIONS is set to “AUTH=PLAIN”  
This option is supported starting with Zabbix 3.0.

**Username** | User name to use in authentication.  
This sets the value of CURLOPT_USERNAME.  
This option is supported starting with Zabbix 3.0.

**Password** | Password to use in authentication.  
This sets the value of CURLOPT_PASSWORD.  
This option is supported starting with Zabbix 3.0.

**Enabled** | Mark the checkbox to enable the media type.

---

**Attention:**
To enable SMTP authentication options, Zabbix server must be both compiled with the --with-libcurl compilation option (with cURL 7.20.0 or higher) and use the libcurl-full packages during runtime.

**Options**
The **Options** tab in the e-mail media type configuration contains alert processing settings. The same set of options are configurable for other media types, too.
All media types are processed in parallel. The maximum number of concurrent sessions is configurable per media type, but the total number of alerter processes on server can only be limited by the StartAlerters parameter. Alerts generated by one trigger are processed sequentially.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concurrent sessions</td>
<td>Select the number of parallel alerter sessions for the media type:</td>
</tr>
<tr>
<td></td>
<td><strong>One</strong> - one session</td>
</tr>
<tr>
<td></td>
<td><strong>Unlimited</strong> - unlimited number of sessions</td>
</tr>
<tr>
<td></td>
<td><strong>Custom</strong> - select a custom number of sessions</td>
</tr>
<tr>
<td></td>
<td>Unlimited/high values mean more parallel sessions and increased capacity for sending notifications. Unlimited/high values should be used in large environments where lots of notifications may need to be sent simultaneously.</td>
</tr>
<tr>
<td></td>
<td>If more notifications need to be sent than there are concurrent sessions, the remaining notifications will be queued; they will not be lost.</td>
</tr>
<tr>
<td>Attempts</td>
<td>Number of attempts for trying to send a notification. Up to 10 attempts can be specified; default value is ‘3’. If ‘1’ is specified Zabbix will send the notification only once and will not retry if the sending fails.</td>
</tr>
<tr>
<td>Attempt interval</td>
<td>Frequency of trying to resend a notification in case the sending failed, in seconds (0-60). If ‘0’ is specified Zabbix will retry immediately.</td>
</tr>
<tr>
<td></td>
<td>Time suffixes are supported, e.g. 5s, 1m.</td>
</tr>
</tbody>
</table>

User media

To assign a specific address to the user:

- Go to Administration → Users
- Open the user properties form
- In Media tab, click on Add
User media attributes:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select Email as the type. Specify e-mail addresses to send the messages to. To add more than one address click on Add below the address field. If multiple e-mail addresses are specified, one e-mail will be sent to all the specified recipients. You may add the recipient display name (like &quot;Recipient name&quot; in Recipient name <a href="mailto:address1@company.com">address1@company.com</a> in the screenshot above) with the actual e-mail address. See examples and restrictions on display name and email address in media type attribute SMTP email description.</td>
</tr>
<tr>
<td>Send to</td>
<td>When active You can limit the time when messages are sent, for example, the working days only (1-5, 09:00-18:00). See the Time period specification page for description of the format. User macros are supported.</td>
</tr>
<tr>
<td>When active</td>
<td>Use if severity Mark the checkboxes of trigger severities that you want to receive notifications for. Note that the default severity ('Not classified') must be checked if you want to receive notifications for non-trigger events. After saving, the selected trigger severities will be displayed in the corresponding severity colors while unselected ones will be grayed out.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the user media. Enabled - is in use. Disabled - is not being used.</td>
</tr>
</tbody>
</table>

2 SMS

Overview

Zabbix supports the sending of SMS messages using a serial GSM modem connected to Zabbix server’s serial port.

Make sure that:
• The speed of the serial device (normally /dev/ttyS0 under Linux) matches that of the GSM modem. Zabbix does not set the speed of the serial link. It uses default settings.
• The ‘zabbix’ user has read/write access to the serial device. Run the command ls -l /dev/ttyS0 to see current permissions of the serial device.
• The GSM modem has PIN entered and it preserves it after power reset. Alternatively you may disable PIN on the SIM card.

Zabbix has been tested with these GSM modems:
• Siemens MC35
• Teltonika ModemCOM/G10

To configure SMS as the delivery channel for messages, you also need to configure SMS as the media type and enter the respective phone numbers for the users.

Configuration
To configure SMS as the media type:
• Go to Administration → Media types
• Click on Create media type (or click on SMS in the list of pre-defined media types).

The **Media type** tab contains general media type attributes:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Name of the media type.</td>
</tr>
<tr>
<td>Type</td>
<td>Select SMS as the type.</td>
</tr>
<tr>
<td>GSM modem</td>
<td>Set the serial device name of the GSM modem.</td>
</tr>
</tbody>
</table>

The **Options** tab contains alert **processing settings** that are common for all media types. Note that parallel processing of sending SMS notifications is not possible.

User media
To assign a phone number to the user:
• Go to Administration → Users
• Open the user properties form
• In Media tab, click on Add

User media attributes:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select SMS as the type.</td>
</tr>
<tr>
<td>Send to</td>
<td>Specify the phone number to send messages to. You can limit the time when messages are sent, for example, the working days only (1-5, 09:00-18:00). See the Time period specification page for description of the format.</td>
</tr>
<tr>
<td>When active</td>
<td>You can limit the time when messages are sent, for example, the working days only (1-5, 09:00-18:00). See the Time period specification page for description of the format.</td>
</tr>
<tr>
<td>Use if severity</td>
<td>Mark the checkboxes of trigger severities that you want to receive notifications for. Note that the default severity ('Not classified') must be checked if you want to receive notifications for non-trigger events. After saving, the selected trigger severities will be displayed in the corresponding severity colors while unselected ones will be grayed out.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the user media.</td>
</tr>
<tr>
<td></td>
<td><strong>Enabled</strong> - is in use.</td>
</tr>
<tr>
<td></td>
<td><strong>Disabled</strong> - is not being used.</td>
</tr>
</tbody>
</table>

3 Jabber

Overview
Zabbix supports sending Jabber messages.
When sending notifications, Zabbix tries to look up the Jabber SRV record first, and if that fails, it uses an address record for that domain. Among Jabber SRV records, the one with the highest priority and maximum weight is chosen. If it fails, other records are not tried.

To configure Jabber as the delivery channel for messages, you need to configure Jabber as the media type and enter the respective addresses for the users.

Configuration
To configure Jabber as the media type:

• Go to Administration → Media types
• Click on Create media type (or click on Jabber in the list of pre-defined media types).

The **Media type** tab contains general media type attributes:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Name of the media type.</td>
</tr>
<tr>
<td>Type</td>
<td>Select Jabber as the type.</td>
</tr>
<tr>
<td>Jabber identifier</td>
<td>Enter Jabber identifier.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter Jabber password.</td>
</tr>
</tbody>
</table>

The **Options** tab contains alert processing settings that are common for all media types.

User media
To assign a Jabber address to the user:

• Go to Administration → Users
• Open the user properties form
• In Media tab, click on Add

User media attributes:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select Jabber as the type.</td>
</tr>
<tr>
<td>Send to</td>
<td>Specify the address to send messages to.</td>
</tr>
<tr>
<td>When active</td>
<td>You can limit the time when messages are sent, for example, the working days only (1-5,09:00-18:00). See the Time period specification page for description of the format.</td>
</tr>
<tr>
<td>Use if severity</td>
<td>Mark the checkboxes of trigger severities that you want to receive notifications for. Note that the default severity (‘Not classified’) <strong>must be</strong> checked if you want to receive notifications for non-trigger events. After saving, the selected trigger severities will be displayed in the corresponding severity colors while unselected ones will be grayed out.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the user media.</td>
</tr>
<tr>
<td></td>
<td><strong>Enabled</strong> - is in use.</td>
</tr>
<tr>
<td></td>
<td><strong>Disabled</strong> - is not being used.</td>
</tr>
</tbody>
</table>

**4 Ez Texting**

Overview
You can use Zabbix technological partner Ez Texting for message sending.

To configure Ez Texting as the delivery channel for messages, you need to configure Ez Texting as the media type and assign recipient identification to the users.

Configuration
To configure Ez Texting as the media type:

• Go to Administration → Media types
• Click on Create media type
The **Media type** tab contains general media type attributes:

All mandatory input fields are marked with a red asterisk.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Name of the media type.</td>
</tr>
<tr>
<td>Type</td>
<td>Select Ez Texting as the type.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the Ez Texting username.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the Ez Texting password.</td>
</tr>
<tr>
<td>Message text limit</td>
<td>Select the message text limit.</td>
</tr>
<tr>
<td></td>
<td><strong>USA (160 characters)</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Canada (136 characters)</strong></td>
</tr>
</tbody>
</table>

The **Options** tab contains alert processing settings that are common for all media types.

**User media**

To assign Ez Texting recipient identification to the user:

- Go to Administration → Users
- Open the user properties form
- In Media tab, click on Add

**User media attributes:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select the Ez Texting media type.</td>
</tr>
<tr>
<td>Send to</td>
<td>Specify the recipient to send the messages to.</td>
</tr>
<tr>
<td>When active</td>
<td>You can limit the time when messages are sent, for example, the working days only (1-5,09:00-18:00). See the Time period specification page for description of the format.</td>
</tr>
</tbody>
</table>
**Parameter Description**

**Use if severity**
Mark the checkboxes of trigger severities that you want to receive notifications for.
Note that the default severity ('Not classified') **must be** checked if you want to receive notifications for non-trigger events.
After saving, the selected trigger severities will be displayed in the corresponding severity colors while unselected ones will be grayed out.

**Status**
Status of the user media.
- **Enabled** - is in use.
- **Disabled** - is not being used.

---

### 5 Custom alertscripts

**Overview**

If you are not satisfied with existing media types for sending alerts there is an alternative way to do that. You can create a script that will handle the notification your way.

Alert scripts are executed on Zabbix server. These scripts must be located in the directory specified in the server configuration file `AlertScriptsPath` parameter.

Here is an example alert script:

```bash
#!/bin/bash
to=$1
subject=$2
body=$3
cat <<EOF | mail -s "$subject" "$to"
$body
EOF
```

**Attention:**
Starting from version 3.4 Zabbix checks for the exit code of the executed commands and scripts. Any exit code which is different from **0** is considered as a **command execution** error. In such case Zabbix will try to repeat failed execution.

Environment variables are not preserved or created for the script, so they should be handled explicitly.

**Configuration**

To configure custom alertscripts as the media type:

- Go to Administration → Media types
- Click on Create media type

The **Media type** tab contains general media type attributes:
All mandatory input fields are marked with a red asterisk.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter name of the media type.</td>
</tr>
<tr>
<td>Type</td>
<td>Select Script as the type.</td>
</tr>
<tr>
<td>Script name</td>
<td>Enter the name of the script file (e.g., notification.sh) that is located in the directory specified in the server configuration file AlertScriptsPath parameter.</td>
</tr>
<tr>
<td>Script parameters</td>
<td>Add command-line parameters to the script. ( {\text{ALERT SENDTO}}, {\text{ALERT SUBJECT}} ) and ( {\text{ALERT MESSAGE}} ) macros are supported in script parameters. Customizing script parameters is supported since Zabbix 3.0.</td>
</tr>
</tbody>
</table>

The **Options** tab contains alert processing settings that are common for all media types.

**Attention:**

As parallel processing of media types is implemented since Zabbix 3.4.0, it is important to note that with more than one script media type configured, these scripts may be processed in parallel by alerter processes. The total number of alerter processes is limited by the **StartAlerters** parameter.

User media

To assign custom alertscripts to the user:

- Go to Administration → Users
- Open the user properties form
- In Media tab, click on Add

**User media attributes:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select the custom alertscripts media type.</td>
</tr>
<tr>
<td>Send to</td>
<td>Specify the recipient to receive the alerts.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>When active</td>
<td>You can limit the time when alert scripts are executed, for example, the working days only (1-5, 09:00-18:00).</td>
</tr>
<tr>
<td></td>
<td>See the Time period specification page for description of the format.</td>
</tr>
<tr>
<td>Use if severity</td>
<td>Mark the checkboxes of trigger severities that you want to activate the alert script for.</td>
</tr>
<tr>
<td></td>
<td>Note that the default severity ('Not classified') must be checked if you want to receive notifications for non-trigger events. After saving, the selected trigger severities will be displayed in the corresponding severity colors while unselected ones will be grayed out.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the user media.</td>
</tr>
<tr>
<td></td>
<td><strong>Enabled</strong> - is in use.</td>
</tr>
<tr>
<td></td>
<td><strong>Disabled</strong> - is not being used.</td>
</tr>
</tbody>
</table>

### 2 Actions

**Overview**

If you want some operations taking place as a result of events (for example, notifications sent), you need to configure actions.

**Actions can be defined in response to events of all supported types:**

- Trigger events - when trigger status changes from OK to PROBLEM and back
- Discovery events - when network discovery takes place
- Auto registration events - when new active agents auto-register (or host metadata changes for registered ones)
- Internal events - when items become unsupported or triggers go into an unknown state

**Configuring an action**

To configure an action, do the following:

- Go to Configuration → Actions
- From the Event source dropdown select the required source
- Click on Create action
- Name the action
- Choose conditions upon which operations are carried out
- Choose the **operations** to carry out
- Choose the **recovery operations** to carry out

**General action attributes:**
Parameters| Description
---|---
**Name** | Unique action name.
**Type of calculation** | Select the evaluation option for action conditions (with more than one condition):
- **And** - all conditions must be met
- **Or** - enough if one condition is met
- **And/Or** - combination of the two: AND with different condition types and OR with the same condition type
- **Custom expression** - a user-defined calculation formula for evaluating action conditions.

**Conditions** | List of action conditions.
If no conditions are configured, the action will run for every event that corresponds to the event source selected for the action.

**New condition** | Select a new action condition and click on Add.

**Enabled** | Mark the checkbox to enable the action. Otherwise it will be disabled.

### 1 Conditions

**Overview**

It is possible to define that an action is executed only if the event matches a defined set of conditions. Conditions are set when configuring the action.

Condition matching is case-sensitive.

The following conditions can be set for trigger-based actions:
<table>
<thead>
<tr>
<th>Condition type</th>
<th>Supported operators</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>equals</td>
<td>Specify an application or an application to exclude.</td>
</tr>
<tr>
<td></td>
<td>contains</td>
<td>equals - event belongs to a trigger of the item that is linked to the specified application.</td>
</tr>
<tr>
<td></td>
<td>does not contain</td>
<td>contains - event belongs to a trigger of the item that is linked to an application containing the string.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>does not contain - event belongs to a trigger of the item that is linked to an application not containing the string.</td>
</tr>
<tr>
<td>Host group</td>
<td>equals</td>
<td>Specify host groups or host groups to exclude.</td>
</tr>
<tr>
<td></td>
<td>does not equal</td>
<td>equals - event belongs to this host group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>does not equal - event does not belong to this host group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Specifying a parent host group implicitly selects all nested host groups. To specify the parent group only, all nested groups have to be additionally set with the does not equal operator.</td>
</tr>
<tr>
<td>Template</td>
<td>equals</td>
<td>Specify templates or templates to exclude.</td>
</tr>
<tr>
<td></td>
<td>does not equal</td>
<td>equals - event belongs to a trigger inherited from this template.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>does not equal - event does not belong to a trigger inherited from this template.</td>
</tr>
<tr>
<td>Host</td>
<td>equals</td>
<td>Specify hosts or hosts to exclude.</td>
</tr>
<tr>
<td></td>
<td>does not equal</td>
<td>equals - event belongs to this host.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>does not equal - event does not belong to this host.</td>
</tr>
<tr>
<td>Tag</td>
<td>equals</td>
<td>Specify event tag or event tag to exclude.</td>
</tr>
<tr>
<td></td>
<td>does not equal</td>
<td>equals - event has this tag</td>
</tr>
<tr>
<td></td>
<td>contains</td>
<td>does not equal - event does not have this tag</td>
</tr>
<tr>
<td></td>
<td>does not contain</td>
<td>contains - event has a tag containing this string</td>
</tr>
<tr>
<td></td>
<td></td>
<td>does not contain - event does not have a tag containing this string</td>
</tr>
<tr>
<td>Condition type</td>
<td>Supported operators</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Tag value</td>
<td>equals</td>
<td>Specify event tag and value combination or tag and value combination to exclude.</td>
</tr>
<tr>
<td></td>
<td>does not equal</td>
<td><strong>equals</strong> - event has this tag and value</td>
</tr>
<tr>
<td></td>
<td>contains</td>
<td><strong>does not equal</strong> - event does not have this tag and value</td>
</tr>
<tr>
<td></td>
<td>does not contain</td>
<td><strong>contains</strong> - event has a tag and value containing these strings</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>does not contain</strong> - event does not have a tag and value containing these strings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: Entered value will be compared to trigger name with all macros expanded.</td>
</tr>
<tr>
<td>Trigger</td>
<td>equals</td>
<td>Specify triggers or triggers to exclude.</td>
</tr>
<tr>
<td></td>
<td>does not equal</td>
<td><strong>equals</strong> - event is generated by this trigger.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>does not equal</strong> - event is generated by any other trigger, except this one.</td>
</tr>
<tr>
<td>Trigger name</td>
<td>contains</td>
<td>Specify a string in the trigger name or a string to exclude.</td>
</tr>
<tr>
<td></td>
<td>does not contain</td>
<td><strong>contains</strong> - event is generated by a trigger, containing this string in the name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>does not contain</strong> - this string cannot be found in the trigger name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: Entered value will be compared to trigger name with all macros expanded.</td>
</tr>
<tr>
<td>Trigger severity</td>
<td>equals</td>
<td>Specify trigger severity.</td>
</tr>
<tr>
<td></td>
<td>does not equal</td>
<td><strong>equals</strong> - equal to trigger severity.</td>
</tr>
<tr>
<td></td>
<td>is greater than or equals</td>
<td><strong>does not equal</strong> - not equal to trigger severity</td>
</tr>
<tr>
<td></td>
<td>is less than or equals</td>
<td><strong>is greater than or equals</strong> - more or equal to trigger severity</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>is less than or equals</strong> - less or equal to trigger severity</td>
</tr>
<tr>
<td>Time period</td>
<td>in</td>
<td>Specify a time period or a time period to exclude.</td>
</tr>
<tr>
<td></td>
<td>not in</td>
<td><strong>in</strong> - event time is within the time period.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>not in</strong> - event time is not within the time period.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See the <a href="#">time period specification</a> page for description of the format.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>User macros</strong> are supported, since Zabbix 3.4.0.</td>
</tr>
<tr>
<td>Condition type</td>
<td>Supported operators</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Problem is suppressed</td>
<td>no</td>
<td>Specify if the problem is suppressed (not shown) because of host maintenance.</td>
</tr>
<tr>
<td></td>
<td>yes</td>
<td>no - problem is not suppressed. yes - problem is suppressed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The following conditions can be set for discovery-based events:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Condition type</td>
<td>Supported operators</td>
<td>Description</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host IP</td>
<td>equals</td>
<td>Specify an IP address range or a range to exclude for a discovered host.</td>
</tr>
<tr>
<td></td>
<td>does not equal</td>
<td>equals - host IP is in the range.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>does not equal - host IP is not in the range.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>It may have the following formats:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Single IP: 192.168.1.33</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range of IP addresses: 192.168.1-10.1-254</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IP mask: 192.168.4.0/24</td>
</tr>
<tr>
<td></td>
<td></td>
<td>List: 192.168.1.1-254, 192.168.2.1-100, 192.168.2.200, 192.168.4.0/24</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Support for spaces in the list format is provided since Zabbix 3.0.0.</td>
</tr>
<tr>
<td>Service type</td>
<td>equals</td>
<td>Specify a service type of a discovered service or a service type to exclude.</td>
</tr>
<tr>
<td></td>
<td>does not equal</td>
<td>equals - matches the discovered service.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>does not equal - does not match the discovered service.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Available service types: SSH, LDAP, SMTP, FTP, HTTP, HTTPS (available since Zabbix 2.2 version), POP, NNTP, IMAP, TCP, Zabbix agent, SNMPv1 agent, SNMPv2 agent, SNMPv3 agent, ICMP ping, telnet (available since Zabbix 2.2 version).</td>
</tr>
<tr>
<td>Service port</td>
<td>equals</td>
<td>Specify a TCP port range of a discovered service or a range to exclude.</td>
</tr>
<tr>
<td></td>
<td>does not equal</td>
<td>equals - service port is in the range.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>does not equal - service port is not in the range.</td>
</tr>
<tr>
<td>Condition type</td>
<td>Supported operators</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Discovery rule</td>
<td>equals, does not equal</td>
<td>Specify a discovery rule or a discovery rule to exclude.</td>
</tr>
<tr>
<td></td>
<td><strong>equals</strong> - using this discovery rule.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>does not equal</strong> - using any other discovery rule, except this one.</td>
<td></td>
</tr>
<tr>
<td>Discovery check</td>
<td>equals, does not equal</td>
<td>Specify a discovery check or a discovery check to exclude.</td>
</tr>
<tr>
<td></td>
<td><strong>equals</strong> - using this discovery check.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>does not equal</strong> - using any other discovery check, except this one.</td>
<td></td>
</tr>
<tr>
<td>Discovery object</td>
<td>equals</td>
<td>Specify the discovered object.</td>
</tr>
<tr>
<td></td>
<td><strong>equals</strong> - equal to discovered object (a device or a service).</td>
<td></td>
</tr>
<tr>
<td>Discovery status</td>
<td>equals</td>
<td><strong>Up</strong> - matches ‘Host Up’ and ‘Service Up’ events</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Down</strong> - matches ‘Host Down’ and ‘Service Down’ events</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Discovered</strong> - matches ‘Host Discovered’ and ‘Service Discovered’ events</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Lost</strong> - matches ‘Host Lost’ and ‘Service Lost’ events</td>
</tr>
<tr>
<td>Uptime/Downtime</td>
<td>is greater than or equals, is less than or equals</td>
<td>Uptime for ‘Host Up’ and ‘Service Up’ events.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Downtime for ‘Host Down’ and ‘Service Down’ events.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>is greater than or equals</strong> - is more or equal to. Parameter is given in seconds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>is less than or equals</strong> - is less or equal to. Parameter is given in seconds.</td>
</tr>
<tr>
<td>Condition type</td>
<td>Supported operators</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Received value</td>
<td>equals, does not equal, is greater than or equals, is less than or equals, contains, does not contain</td>
<td>Specify the value received from an agent (Zabbix, SNMP) check in a discovery rule. String comparison. If several Zabbix agent or SNMP checks are configured for a rule, received values for each of them are checked (each check generates a new event which is matched against all conditions). <strong>equals</strong> - equal to the value. <strong>does not equal</strong> - not equal to the value. <strong>is greater than or equals</strong> - more or equal to the value. <strong>is less than or equals</strong> - less or equal to the value. <strong>contains</strong> - contains the substring. Parameter is given as a string. <strong>does not contain</strong> - does not contain the substring. Parameter is given as a string.</td>
</tr>
<tr>
<td>Proxy</td>
<td>equals, does not equal</td>
<td>Specify a proxy or a proxy to exclude. <strong>equals</strong> - using this proxy. <strong>does not equal</strong> - using any other proxy except this one.</td>
</tr>
</tbody>
</table>

**Note:**
Service checks in a discovery rule, which result in discovery events, do not take place simultaneously. Therefore, if multiple values are configured for Service type, Service port or Received value conditions in the action, they will be compared to one discovery event at a time, but not to several events simultaneously. As a result, actions with multiple values for the same check types may not be executed correctly.

The following conditions can be set for actions based on active agent auto-registration:

<table>
<thead>
<tr>
<th>Condition type</th>
<th>Supported operators</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host metadata</td>
<td>contains, does not contain</td>
<td>Specify host metadata or host metadata to exclude. <strong>contains</strong> - host metadata contains the string. <strong>does not contain</strong> - host metadata does not contain the string. Host metadata can be specified in an agent configuration file.</td>
</tr>
<tr>
<td>Host name</td>
<td>contains, does not contain</td>
<td>Specify a host name or a host name to exclude. <strong>contains</strong> - host name contains the string. <strong>does not contain</strong> - host name does not contain the string.</td>
</tr>
<tr>
<td>Condition type</td>
<td>Supported operators</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Proxy</td>
<td>equals</td>
<td>Specify a proxy or a proxy to exclude.</td>
</tr>
<tr>
<td></td>
<td>does not equal</td>
<td><strong>equals</strong> - using this proxy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>does not equal</strong> - using any other proxy except this one.</td>
</tr>
</tbody>
</table>

The following conditions can be set for actions based on internal events:

<table>
<thead>
<tr>
<th>Condition type</th>
<th>Supported operators</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>equals</td>
<td>Specify an application or an application to exclude.</td>
</tr>
<tr>
<td></td>
<td>contains</td>
<td><strong>equals</strong> - event belongs to an item that is linked to the specified application.</td>
</tr>
<tr>
<td></td>
<td>does not contain</td>
<td><strong>contains</strong> - event belongs to an item that is linked to an application containing the string.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>does not contain</strong> - event belongs to an item that is linked to an application not containing the string.</td>
</tr>
<tr>
<td>Event type</td>
<td>equals</td>
<td><strong>Item in “not supported” state</strong> - matches events where an item goes from a ‘normal’ to ‘not supported’ state.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Low-level discovery rule in “not supported” state</strong> - matches events where a low-level discovery rule goes from a ‘normal’ to ‘not supported’ state.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Trigger in “unknown” state</strong> - matches events where a trigger goes from a ‘normal’ to ‘unknown’ state.</td>
</tr>
<tr>
<td>Host group</td>
<td>equals</td>
<td>Specify host groups or host groups to exclude.</td>
</tr>
<tr>
<td></td>
<td>does not equal</td>
<td><strong>equals</strong> - event belongs to this host group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>does not equal</strong> - event does not belong to this host group.</td>
</tr>
<tr>
<td>Template</td>
<td>equals</td>
<td>Specify templates or templates to exclude.</td>
</tr>
<tr>
<td></td>
<td>does not equal</td>
<td><strong>equals</strong> - event belongs to an item/trigger/low-level discovery rule inherited from this template.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>does not equal</strong> - event does not belong to an item/trigger/low-level discovery rule inherited from this template.</td>
</tr>
<tr>
<td>Condition type</td>
<td>Supported operators</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>----------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Host</td>
<td>equals</td>
<td>Specify hosts or hosts to exclude.</td>
</tr>
<tr>
<td></td>
<td>does not equal</td>
<td><strong>equals</strong> - event belongs to this host.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>does not equal</strong> - event does not belong to this host.</td>
</tr>
</tbody>
</table>

Type of calculation

The following options of calculating conditions are available:

- **And** - all conditions must be met

Note that using “And” calculation is disallowed between several triggers when they are selected as a Trigger= condition. Actions can only be executed based on the event of one trigger.

- **Or** - enough if one condition is met

- **And/Or** - combination of the two: AND with different condition types and OR with the same condition type, for example:

<table>
<thead>
<tr>
<th>Host group equals Oracle servers</th>
<th>Host group equals MySQL servers</th>
<th>Trigger name contains ‘Database is down’</th>
<th>Trigger name contains ‘Database is unavailable’</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>is evaluated as</td>
<td></td>
</tr>
<tr>
<td>(Host group equals Oracle servers</td>
<td>Host group equals MySQL servers)</td>
<td><strong>and</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Trigger name contains ‘Database is down’</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>or Trigger name contains ‘Database is unavailable’)</td>
<td></td>
</tr>
</tbody>
</table>

- **Custom expression** - a user-defined calculation formula for evaluating action conditions. It must include all conditions (represented as uppercase letters A, B, C, ...) and may include spaces, tabs, brackets ( ), **and** (case sensitive), **or** (case sensitive).

While the previous example with And/Or would be represented as (A or B) and (C or D), in a custom expression you may as well have multiple other ways of calculation:

(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 etc.

Actions disabled due to deleted objects

If a certain object (host, template, trigger, etc) used in an action condition/operation is deleted, the condition/operation is removed and the action is disabled to avoid incorrect execution of the action. The action can be re-enabled by the user.

This behavior takes place when deleting:

- host groups ("host group" condition, "remote command" operation on a specific host group);
- hosts ("host" condition, "remote command" operation on a specific host);
- templates ("template" condition, "link to template" and "unlink from template" operations);
- triggers ("trigger" condition);
- discovery rules (when using "discovery rule" and "discovery check" conditions).

Note: If a remote command has many target hosts, and we delete one of them, only this host will be removed from the target list, the operation itself will remain. But, if it’s the only host, the operation will be removed, too. The same goes for "link to template" and "unlink from template" operations.

Actions are not disabled when deleting a user or user group used in a "send message" operation.

2 Operations

Overview

You can define the following operations for all events:

- send a message
- execute a remote command (including IPMI)
Attention:
Zabbix server does not create alerts if access to the host is explicitly “denied” for the user defined as action operation recipient or if the user has no rights defined to the host at all.

For discovery and auto-registration events, there are additional operations available:

- add host
- remove host
- enable host
- disable host
- add to host group
- remove from host group
- link to template
- unlink from template
- set host inventory mode

Configuring an operation

To configure an operation, go to the Operations tab in action configuration and click on New in the Operations block. Edit the operation step and click on Add to add to the list of Operations.

Operation attributes:
All mandatory input fields are marked with a red asterisk.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default operation step duration</td>
<td>Duration of one operation step by default (60 seconds to 1 week). For example, an hour-long step duration means that if an operation is carried out, an hour will pass before the next step. <strong>Time suffixes</strong> are supported, e.g. 60s, 1m, 2h, 1d, since Zabbix 3.4.0. <strong>User macros</strong> are supported, since Zabbix 3.4.0.</td>
</tr>
<tr>
<td>Default subject</td>
<td></td>
</tr>
<tr>
<td>Default message</td>
<td>Default message for notifications. The message may contain <strong>macros</strong>. It is limited to a certain amount of characters depending on the type of database (see <strong>Sending message</strong> for more information).</td>
</tr>
</tbody>
</table>
Parameter | Description
---|---
Pause operations for suppressed problems | Mark this checkbox to delay the start of operations for the duration of a maintenance period. When operations are started, after the maintenance, all operations are performed including those for the events during the maintenance. Note that this setting affects only problem escalations; recovery and update operations will not be affected.
If you unmark this checkbox, operations will be executed without delay even during a maintenance period.
This option is supported since Zabbix 3.2.0.

Operations | Action operations are displayed, with these details:
Steps - escalation step(s) to which the operation is assigned
Details - type of operation and its recipient/target.
Since Zabbix 2.2, the operation list also displays the media type (e-mail, SMS, Jabber, etc) used in sending a message as well as the name and surname (in parentheses after the alias) of a notification recipient.
Start in - how long after an event the operation is performed
Duration (sec) - step duration is displayed. Default is displayed if the step uses default duration, and a time is displayed if custom duration is used.
Action - links for editing and removing an operation are displayed.
To configure a new operation, click on New.

Operation details | This block is used to configure the details of an operation.
Steps | Select the step(s) to assign the operation to in an escalation schedule:
From - execute starting with this step
To - execute until this step (0=Infinity, execution will not be limited)
Step duration | Custom duration for these steps (0=use default step duration).
Time suffixes are supported, e.g. 60s, 1m, 2h, 1d, since Zabbix 3.4.0.
User macros are supported, since Zabbix 3.4.0.
Several operations can be assigned to the same step. If these operations have different step duration defined, the shortest one is taken into account and applied to the step.

Operation type | Two operation types are available for all events:
Send message - send message to user
Remote command - execute a remote command
More operations are available for discovery and auto-registration based events (see above).
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send to user groups</td>
<td>Click on Add to select user groups to send the message to. The user group must have at least “read” permissions to the host in order to be notified.</td>
</tr>
<tr>
<td>Send to users</td>
<td>Click on Add to select users to send the message to. The user must have at least “read” permissions to the host in order to be notified.</td>
</tr>
<tr>
<td>Send only to</td>
<td>Send message to all defined media types or a selected one only.</td>
</tr>
<tr>
<td>Default message</td>
<td>If selected, the default message will be used (see above).</td>
</tr>
<tr>
<td>Subject</td>
<td>Subject of the custom message. The subject may contain macros. It is limited to 255 characters.</td>
</tr>
<tr>
<td>Message</td>
<td>The custom message. The message may contain macros. It is limited to certain amount of characters depending on the type of database (see Sending message for more information).</td>
</tr>
</tbody>
</table>

**Operation type:**

- **Remote command**

**Target list**

Select targets to execute the command on:

- **Current host** - command is executed on the host of the trigger that caused the problem event. This option will not work if there are multiple hosts in the trigger.

- **Host** - select host(s) to execute the command on.

- **Host group** - select host group(s) to execute the command on. Specifying a parent host group implicitly selects all nested host groups. Thus the remote command will also be executed on hosts from nested groups.

A command on a host is executed only once, even if the host matches more than once (e.g. from several host groups; individually and from a host group).

The target list is meaningless if a custom script is executed on Zabbix server. Selecting more targets in this case only results in the script being executed on the server more times.

Note that for global scripts, the target selection also depends on the Host group setting in global script configuration.

**Type**

Select the command type:

- **IPMI** - execute an IPMI command
- **Custom script** - execute a custom set of commands
- **SSH** - execute an SSH command
- **Telnet** - execute a Telnet command
- **Global script** - execute one of the global scripts defined in Administration→Scripts.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execute on</td>
<td>Execute a custom script on:</td>
</tr>
<tr>
<td></td>
<td><strong>Zabbix agent</strong> - the script will be executed by Zabbix agent on the host</td>
</tr>
<tr>
<td></td>
<td><strong>Zabbix server (proxy)</strong> - the script will be executed by Zabbix server or proxy - depending on whether the host is monitored by server or proxy</td>
</tr>
<tr>
<td></td>
<td><strong>Zabbix server</strong> - the script will be executed by Zabbix server only</td>
</tr>
<tr>
<td></td>
<td>To execute scripts on the agent, it must be <strong>configured</strong> (EnableRemoteCommands parameter enabled) to allow remote commands from the server.</td>
</tr>
<tr>
<td></td>
<td>To execute scripts on proxy, it must be <strong>configured</strong> (EnableRemoteCommands parameter enabled) to allow remote commands from the server.</td>
</tr>
<tr>
<td></td>
<td>This field is available if ‘Custom script’ is selected as Type.</td>
</tr>
<tr>
<td>Commands</td>
<td>Enter the command(s).</td>
</tr>
<tr>
<td></td>
<td>Supported macros will be resolved based on the trigger expression that caused the event. For example, host macros will resolve to the hosts of the trigger expression (and not of the target list).</td>
</tr>
<tr>
<td>Conditions</td>
<td>Condition for performing the operation:</td>
</tr>
<tr>
<td></td>
<td><strong>Not ack</strong> - only when the event is unacknowledged</td>
</tr>
<tr>
<td></td>
<td><strong>Ack</strong> - only when the event is acknowledged.</td>
</tr>
</tbody>
</table>

1 Sending message

Overview

Sending a message is one of the best ways of notifying people about a problem. That is why it is one of the primary actions offered by Zabbix.

Configuration

To be able to send and receive notifications from Zabbix you have to:

- **define the media** to send a message to

  **Warning:**
  
  The default trigger severity ('Not classified') **must be** checked in user media **configuration** if you want to receive notifications for non-trigger events such as discovery, active agent auto-registration or internal events.

- **configure an action operation** that sends a message to one of the defined media

  **Attention:**
  
  Zabbix sends notifications only to those users that have at least ‘read’ permissions to the host that generated the event. At least one host of a trigger expression must be accessible.

You can configure custom scenarios for sending messages using **escalations**.

To successfully receive and read e-mails from Zabbix, e-mail servers/clients must support standard ‘SMTP/MIME e-mail’ format since Zabbix sends UTF-8 data (If the subject contains ASCII characters only, it is not UTF-8 encoded.). The subject and the body of the message are base64-encoded to follow ‘SMTP/MIME e-mail’ format standard.

Message limit after all macros expansion is the same as message limit for **Remote commands**.
Tracking messages

You can view the status of messages sent in Monitoring → Problems.

In the Actions column you can see summarized information about actions taken. In there green numbers represent messages sent, red ones - failed messages. In progress indicates that an action is initiated. Failed informs that no action has executed successfully.

If you click on the event time to view event details, you will also see the Message actions block containing details of messages sent (or not sent) due to the event.

In Reports → Action log you will see details of all actions taken for those events that have an action configured.

2 Remote commands

Overview

With remote commands you can define that a certain pre-defined command is automatically executed on the monitored host upon some condition.

Thus remote commands are a powerful mechanism for smart pro-active monitoring.

In the most obvious uses of the feature you can try to:

- Automatically restart some application (web server, middleware, CRM) if it does not respond
- Use IPMI ‘reboot’ command to reboot some remote server if it does not answer requests
- Automatically free disk space (removing older files, cleaning /tmp) if running out of disk space
- Migrate a VM from one physical box to another depending on the CPU load
- Add new nodes to a cloud environment upon insufficient CPU (disk, memory, whatever) resources

Configuring an action for remote commands is similar to that for sending a message, the only difference being that Zabbix will execute a command instead of sending a message.

Remote commands can be executed by Zabbix server, proxy or agent. Remote commands on Zabbix agent can be executed directly by Zabbix server or through Zabbix proxy. Both on Zabbix agent and Zabbix proxy remote commands are disabled by default. They can be enabled by setting the EnableRemoteCommands parameter to ‘1’.

Remote command limit after all macros expansion depends on the type of database and character set (non-ASCII characters require more than one byte to be stored):

<table>
<thead>
<tr>
<th>Database</th>
<th>Limit in characters</th>
<th>Limit in bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>MySQL</td>
<td>65535</td>
<td>65535</td>
</tr>
<tr>
<td>Oracle Database</td>
<td>2048</td>
<td>4000</td>
</tr>
<tr>
<td>PostgreSQL</td>
<td>65535</td>
<td>not limited</td>
</tr>
<tr>
<td>IBM DB2</td>
<td>2048</td>
<td>2048</td>
</tr>
<tr>
<td>SQLite (only Zabbix proxy)</td>
<td>65535</td>
<td>not limited</td>
</tr>
</tbody>
</table>

Remote commands executed by Zabbix server are run as described in Command execution including exit code checking.

Remote commands are executed even if the target host is in maintenance.

Configuration

Those remote commands that are executed on Zabbix agent (custom scripts) must be first enabled in the respective zabbix_agentd.conf.

Make sure that the EnableRemoteCommands parameter is set to 1 and uncommented. Restart agent daemon if changing this parameter.

Attention:
Remote commands do not work with active Zabbix agents.

Then, when configuring a new action in Configuration → Actions:
• Define the appropriate conditions. In this example, set that the action is activated upon any disaster problems with one of Apache applications:

All mandatory input fields are marked with a red asterisk.

• In the Operations tab, select the Remote command operation type
• Select the remote command type (IPMI, Custom script, SSH, Telnet, Global script)
• If Custom script type is selected, choose the way how custom script will be executed (by Zabbix agent, Zabbix server (proxy) or Zabbix server only)
• Enter the remote command

For example:

```bash
sudo /etc/init.d/apache restart
```

In this case, Zabbix will try to restart an Apache process. With this command, make sure that the command is executed on Zabbix agent (click the Zabbix agent button against Execute on).

**Attention:**

Note the use of `sudo` - Zabbix user does not have permissions to restart system services by default. See below for hints on how to configure `sudo`.

**Note:**

Zabbix agent should run on the remote host and accept incoming connections. Zabbix agent executes commands in background.

Remote commands on Zabbix agent are executed without timeout by the system.run[.nowait] key and are not checked for execution results. On Zabbix server and Zabbix proxy, remote commands are executed with timeout as set in the TrapperTimeout parameter of zabbix_server.conf or zabbix_proxy.conf file and are checked for execution results.

**Access permissions**

Make sure that the 'zabbix' user has execute permissions for configured commands. One may be interested in using `sudo` to give access to privileged commands. To configure access, execute as root:

```
# visudo
```

Example lines that could be used in sudoers file:

```bash
# allows 'zabbix' user to run all commands without password.
zabbix ALL=NOPASSWD: ALL

# allows 'zabbix' user to restart apache without password.
zabbix ALL=NOPASSWD: /etc/init.d/apache restart
```
Remote commands with multiple interfaces

If the target system has multiple interfaces of the selected type (Zabbix agent or IPMI), remote commands will be executed on the default interface.

It is possible to execute remote commands via SSH and Telnet using another interface than the Zabbix agent one. The available interface to use is selected in the following order:

- Zabbix agent default interface
- SNMP default interface
- JMX default interface
- IPMI default interface

IPMI remote commands

For IPMI remote commands the following syntax should be used:

\[ <command> \ [<value>] \]

where

- \(<command>\) - one of IPMI commands without spaces
- \(<value>\) - 'on', 'off' or any unsigned integer. \(<value>\) is an optional parameter.

Examples

**Example 1**

Restart of Windows on certain condition.

In order to automatically restart Windows upon a problem detected by Zabbix, define the following actions:

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation type</td>
<td>'Remote command'</td>
</tr>
<tr>
<td>Type</td>
<td>'Custom script'</td>
</tr>
<tr>
<td>Command</td>
<td><code>c:\windows\system32\shutdown.exe -r -f</code></td>
</tr>
</tbody>
</table>

**Example 2**

Restart the host by using IPMI control.

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation type</td>
<td>'Remote command'</td>
</tr>
<tr>
<td>Type</td>
<td>'IPMI'</td>
</tr>
<tr>
<td>Command</td>
<td>reset</td>
</tr>
</tbody>
</table>

**Example 3**

Power off the host by using IPMI control.

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation type</td>
<td>'Remote command'</td>
</tr>
<tr>
<td>Type</td>
<td>'IPMI'</td>
</tr>
<tr>
<td>Command</td>
<td>power off</td>
</tr>
</tbody>
</table>

3 Additional operations

Overview

In this section you may find some details of **additional operations** for discovery/auto-registration events.
Adding host

Hosts are added during the discovery process, as soon as a host is discovered, rather than at the end of the discovery process.

**Note:**
As network discovery can take some time due to many unavailable hosts/services having patience and using reasonable IP ranges is advisable.

When adding a host, its name is decided by the standard `gethostbyname` function. If the host can be resolved, resolved name is used. If not, the IP address is used. Besides, if IPv6 address must be used for a host name, then all `:` (colons) are replaced by `__` (underscores), since colons are not allowed in host names.

**Attention:**
If performing discovery by a proxy, currently hostname lookup still takes place on Zabbix server.

**Attention:**
If a host already exists in Zabbix configuration with the same name as a newly discovered one, versions of Zabbix prior to 1.8 would add another host with the same name. Zabbix 1.8.1 and later adds _N to the hostname, where N is increasing number, starting with 2.

4 Using macros in messages

Overview

In message subjects and message text you can use macros for more efficient problem reporting.

A full list of macros supported by Zabbix is available.

Examples

Examples here illustrate how you can use macros in messages.

Example 1

Message subject:
Problem: {TRIGGER.NAME}

When you receive the message, the message subject will be replaced by something like:

Problem: Processor load is too high on Zabbix server

Example 2

Message:
Processor load is: {zabbix.zabbix.com:system.cpu.load[,avg1].last()}

When you receive the message, the message will be replaced by something like:

Processor load is: 1.45

Example 3

Message:
Latest value: {{HOST.HOST}:{ITEM.KEY}.last()}
MAX for 15 minutes: {{HOST.HOST}:{ITEM.KEY}.max(900)}
MIN for 15 minutes: {{HOST.HOST}:{ITEM.KEY}.min(900)}

When you receive the message, the message will be replaced by something like:

Latest value: 1.45
MAX for 15 minutes: 2.33
MIN for 15 minutes: 1.01

Example 4

Message:
http://<server_ip_or_name>/zabbix/tr_events.php?triggerid={TRIGGER.ID}&eventid={EVENT.ID}
When you receive the message, it will contain a link to the Event details page, which provides information about the event, its trigger, and a list of latest events generated by the same trigger.

Example 5

Informing about values from several hosts in a trigger expression.

Message:

Problem name: {TRIGGER.NAME}
Trigger expression: {TRIGGER.EXPRESSION}

1. Item value on {HOST.NAME1}: {ITEM.VALUE1} ({ITEM.NAME1})
2. Item value on {HOST.NAME2}: {ITEM.VALUE2} ({ITEM.NAME2})

When you receive the message, the message will be replaced by something like:

Problem name: Processor load is too high on a local host
Trigger expression: {Myhost:system.cpu.load[percpu,avg1].last()}>5 or {Myotherhost:system.cpu.load[percpu,avg1].last()}>5

1. Item value on Myhost: 0.83 (Processor load (1 min average per core))
2. Item value on Myotherhost: 5.125 (Processor load (1 min average per core))

Example 6

Receiving details of both the problem event and recovery event in a recovery message:

Message:

Problem:

Event ID: {EVENT.ID}
Event value: {EVENT.VALUE}
Event status: {EVENT.STATUS}
Event time: {EVENT.TIME}
Event date: {EVENT.DATE}
Event age: {EVENT.AGE}
Event acknowledgment: {EVENT.ACK.STATUS}
Event update history: {EVENT.UPDATE.HISTORY}

Recovery:

Event ID: {EVENT.RECOVERY.ID}
Event value: {EVENT.RECOVERY.VALUE}
Event status: {EVENT.RECOVERY.STATUS}
Event time: {EVENT.RECOVERY.TIME}
Event date: {EVENT.RECOVERY.DATE}

When you receive the message, the macros will be replaced by something like:

Problem:

Event ID: 21874
Event value: 1
Event status: PROBLEM
Event time: 13:04:30
Event date: 2018.01.02
Event age: 5m
Event acknowledgment: Yes
Event update history: 2018.01.02 13:05:51 "John Smith (Admin)"
Actions: acknowledged.

Recovery:

Event ID: 21896
Event value: 0
Event status: OK
Event time: 13:10:07
Event date: 2018.01.02
3 Recovery operations

Overview

Recovery operations allow you to be notified when problems are resolved.

Both messages and remote commands are supported in recovery operations. Recovery operations do not support escalating - all operations are assigned to a single step.

Use cases

Some use cases for recovery operations are as follows:

1. Notify on a recovery all users that were notified on the problem:
   • Select Notify all involved as operation type.
2. Have multiple operations upon recovery: send a notification and execute a remote command:
   • Add operation types for sending a message and executing a command.
3. Open a ticket in external helpdesk/ticketing system and close it when the problem is resolved:
   • Create an external script that communicates with the helpdesk system
   • Create an action having operation that executes this script and thus opens a ticket.
   • Have a recovery operation that executes this script with other parameters and closes the ticket.
   • Use the {EVENT.ID} macro to reference the original problem.

Configuring a recovery operation

To configure a recovery operation:

• Go to the Recovery operations tab in action configuration
• Click on New in the Operations block
• Edit the operation details and click on Add

Several operations can be added.

Recovery operation attributes:
All mandatory input fields are marked with a red asterisk.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default subject</td>
<td>Default message subject for recovery notifications. The subject may contain macros.</td>
</tr>
<tr>
<td>Default message</td>
<td>Default message for recovery notifications. The message may contain macros.</td>
</tr>
<tr>
<td>Operations</td>
<td>Recovery operation details are displayed. To configure a new recovery operation, click on New.</td>
</tr>
<tr>
<td>Operation details</td>
<td>This block is used to configure the details of a recovery operation.</td>
</tr>
</tbody>
</table>
Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Operation type | Three operation types are available for recovery events:  
  **Send message** - send recovery message to specified user  
  **Remote command** - execute a remote command  
  **Notify all involved** - send recovery message to all users who were notified on the problem event  
  Note that if the same recipient with unchanged default subject/message is defined in several operation types, duplicate notifications are not sent. |

**Operation type:**  
**send message**  
Send to user groups  
Click on Add to select user groups to send the recovery message to.  
The user group must have at least “read” permissions to the host in order to be notified.  
Send to users  
Click on Add to select users to send the recovery message to.  
The user must have at least “read” permissions to the host in order to be notified.  
Send only to  
Send recovery message to all defined media types or a selected one only.  
Default message  
If selected, the default message will be used (see above).  
Subject  
Subject of the custom message. The subject may contain macros.  
Message  
The custom message. The message may contain macros.  

**Operation type:**  
**remote command**  
Click on **Remote command** to execute a remote command.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target list</td>
<td>Select targets to execute the command on:</td>
</tr>
<tr>
<td>Current host</td>
<td>- command is executed on the host of the trigger that caused the problem event. This option will not work if there are multiple hosts in the trigger.</td>
</tr>
<tr>
<td>Host</td>
<td>- select host(s) to execute the command on.</td>
</tr>
<tr>
<td>Host group</td>
<td>- select host group(s) to execute the command on. Specifying a parent host group implicitly selects all nested host groups. Thus the remote command will also be executed on hosts from nested groups.</td>
</tr>
<tr>
<td></td>
<td>A command on a host is executed only once, even if the host matches more than once (e.g. from several host groups; individually and from a host group).</td>
</tr>
<tr>
<td></td>
<td>The target list is meaningless if the command is executed on Zabbix server. Selecting more targets in this case only results in the command being executed on the server more times.</td>
</tr>
<tr>
<td></td>
<td>Note that for global scripts, the target selection also depends on the Host group setting in global script configuration.</td>
</tr>
<tr>
<td>Type</td>
<td>Select the command type:</td>
</tr>
<tr>
<td>IPMI</td>
<td>- execute an IPMI command</td>
</tr>
<tr>
<td>Custom script</td>
<td>- execute a custom set of commands</td>
</tr>
<tr>
<td>SSH</td>
<td>- execute an SSH command</td>
</tr>
<tr>
<td>Telnet</td>
<td>- execute a Telnet command</td>
</tr>
<tr>
<td>Global script</td>
<td>- execute one of the global scripts defined in Administration→Scripts.</td>
</tr>
<tr>
<td>Execute on</td>
<td>Execute a custom script on:</td>
</tr>
<tr>
<td>Zabbix agent</td>
<td>- the script will be executed by Zabbix agent on the host</td>
</tr>
<tr>
<td>Zabbix server (proxy)</td>
<td>- the script will be executed by Zabbix server or proxy - depending on whether the host is monitored by server or proxy</td>
</tr>
<tr>
<td>Zabbix server</td>
<td>- the script will be executed by Zabbix server only</td>
</tr>
<tr>
<td></td>
<td>To execute scripts on the agent, it must be configured to allow remote commands from the server.</td>
</tr>
<tr>
<td></td>
<td>This field is available if ‘Custom script’ is selected as Type.</td>
</tr>
<tr>
<td>Commands</td>
<td>Enter the command(s). Supported macros will be resolved based on the trigger expression that caused the event. For example, host macros will resolve to the hosts of the trigger expression (and not of the target list).</td>
</tr>
<tr>
<td>Operation type:</td>
<td>no-tify all involved if selected, the default message will be used (see above).</td>
</tr>
<tr>
<td>Subject</td>
<td>Subject of the custom message. The subject may contain macros.</td>
</tr>
</tbody>
</table>
### 4 Update operations

**Overview**

Update operations allow you to be notified when problems are updated by other users, i.e.:

- commented upon
- acknowledged
- severity changed
- closed (manually)

Update operations are available in actions with the event source as Triggers.

Both messages and remote commands are supported in update operations. Update operations do not support escalating - all operations are assigned to a single step.

**Configuring an update operation**

To configure an update operation:

- Go to the Update operations tab in action configuration
- Click on New in the Operations block
- Edit the operation details and click on Add

Several operations can be added.

**Update operation attributes:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message</td>
<td>The custom message. The message may contain macros.</td>
</tr>
</tbody>
</table>
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default subject</td>
<td>Default message subject for update notifications. The subject may contain macros.</td>
</tr>
<tr>
<td>Default message</td>
<td>Default message for update notifications. The message may contain macros.</td>
</tr>
<tr>
<td>Operations</td>
<td>Update operation details are displayed. To configure a new update operation, click on New.</td>
</tr>
<tr>
<td>Operation details</td>
<td>This block is used to configure the details of an update operation.</td>
</tr>
</tbody>
</table>
Three operation types are available for update operations:

- **Send message** - send update message to specified user when event is updated, for example, acknowledged
- **Remote command** - execute a remote command when event is updated, for example, acknowledged
- **Notify all involved** - send notification message to all users who received notification about the problem appearing and/or have updated the problem event.

If the same recipient with unchanged default subject/message is defined in several operation types, duplicate notifications are not sent.

The person who updates a problem does not receive notification about their own update.

---

**Parameter** | **Description**
---|---
**Operation type** | Three operation types are available for update operations:
- **Send message** - send update message to specified user when event is updated, for example, acknowledged
- **Remote command** - execute a remote command when event is updated, for example, acknowledged
- **Notify all involved** - send notification message to all users who received notification about the problem appearing and/or have updated the problem event.

If the same recipient with unchanged default subject/message is defined in several operation types, duplicate notifications are not sent.

The person who updates a problem does not receive notification about their own update.

**Operation type:**
**send message**
Send to user groups
Click on Add to select user groups to send the update message to.
The user group must have at least "read" permissions to the host in order to be notified.

**Send to users**
Click on Add to select users to send the update message to.
The user must have at least "read" permissions to the host in order to be notified.

**Send only to**
Send update message to all defined media types or a selected one only.

**Default message**
If selected, the default message will be used (see above).

**Subject**
Subject of the custom message. The subject may contain macros.

**Message**
The custom message. The message may contain macros.

**Operation type:**
**remote command**
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target list</td>
<td>Select targets to execute the command on: <strong>Current host</strong> - command is executed on the host of the trigger that caused the problem event. This option will not work if there are multiple hosts in the trigger. <strong>Host</strong> - select host(s) to execute the command on. <strong>Host group</strong> - select host group(s) to execute the command on. Specifying a parent host group implicitly selects all nested host groups. Thus the remote command will also be executed on hosts from nested groups. A command on a host is executed only once, even if the host matches more than once (e.g. from several host groups; individually and from a host group). The target list is meaningless if the command is executed on Zabbix server. Selecting more targets in this case only results in the command being executed on the server more times. Note that for global scripts, the target selection also depends on the Host group setting in global script configuration.</td>
</tr>
<tr>
<td>Type</td>
<td>Select the command type: <strong>IPMI</strong> - execute an IPMI command <strong>Custom script</strong> - execute a custom set of commands <strong>SSH</strong> - execute an SSH command <strong>Telnet</strong> - execute a Telnet command <strong>Global script</strong> - execute one of the global scripts defined in Administration→Scripts.</td>
</tr>
<tr>
<td>Execute on</td>
<td>Execute a custom script on: <strong>Zabbix agent</strong> - the script will be executed by Zabbix agent on the host <strong>Zabbix server (proxy)</strong> - the script will be executed by Zabbix server or proxy - depending on whether the host is monitored by server or proxy <strong>Zabbix server</strong> - the script will be executed by Zabbix server only To execute scripts on the agent, it must be configured to allow remote commands from the server. This field is available if 'Custom script' is selected as Type.</td>
</tr>
<tr>
<td>Commands</td>
<td>Enter the command(s). Supported macros will be resolved based on the trigger expression that caused the event. For example, host macros will resolve to the hosts of the trigger expression (and not of the target list).</td>
</tr>
<tr>
<td>Operation type:</td>
<td>notify all involved</td>
</tr>
</tbody>
</table>
5 Escalations

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.

Miscellaneous aspects of escalation behavior

Let’s consider what happens in different circumstances if an action contains several escalation steps.

<table>
<thead>
<tr>
<th>Situation</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>The host in question goes into maintenance after the initial problem notification is sent</td>
<td>Depending on the Pause operations for suppressed problems setting in action configuration, all remaining escalation steps are executed either with a delay caused by the maintenance period or without delay. A maintenance period does not cancel operations.</td>
</tr>
<tr>
<td>The time period defined in the Time period action condition ends after the initial notification is sent</td>
<td>All remaining escalation steps are executed. The Time period condition cannot stop operations; it has effect with regard to when actions are started/not started, not operations.</td>
</tr>
<tr>
<td>A problem starts during maintenance and continues (is not resolved) after maintenance ends</td>
<td>Depending on the Pause operations for suppressed problems setting in action configuration, all escalation steps are executed either from the moment maintenance ends or immediately.</td>
</tr>
<tr>
<td>A problem starts during a no-data maintenance and continues (is not resolved) after maintenance ends</td>
<td>It must wait for the trigger to fire, before all escalation steps are executed.</td>
</tr>
</tbody>
</table>
Different escalations follow in close succession and overlap

The execution of each new escalation supersedes the previous escalation, but for at least one escalation step that is always executed on the previous escalation. This behavior is relevant in actions upon events that are created with EVERY problem evaluation of the trigger. The message in progress is sent and then one more message on the escalation is sent. The follow-up message will have the cancellation text at the beginning of the message body (NOTE: Escalation canceled) naming the reason (for example, NOTE: Escalation canceled: action `<Action name>` disabled). This way the recipient is informed that the escalation is canceled and no more steps will be executed. This message is sent to all who received the notifications before. The reason of cancellation is also logged to the server log file (starting from Debug Level 3=Warning).

Note that the Escalation canceled message is also sent if operations are finished, but recovery operations are configured and are not executed yet (starting with Zabbix 4.0.6).

During an escalation in progress (like a message being sent) the action is disabled.

Based on trigger event: the trigger is disabled.
Based on internal event about triggers: the trigger is disabled.
Based on internal event about items/low-level discovery rules: the item is disabled.
The host or item is disabled.
The host is disabled.

During an escalation in progress (like a message being sent) the action is deleted.

No more messages are sent. The information is logged to the server log file (starting from Debug Level 3=Warning), for example: escalation canceled: action id:334 deleted.

Escalation examples

Example 1

Sending a repeated notification once every 30 minutes (5 times in total) to a ‘MySQL Administrators’ group. To configure:

- In Operations tab, set the Default operation step duration to ‘30m’ (30 minutes)
- Set the escalation steps to be From ‘1’ To ‘5’
- Select the ‘MySQL Administrators’ group as recipients of the message

Notifications will be sent at 0:00, 0:30, 1:00, 1:30, 2:00 hours after the problem starts (unless, of course, the problem is resolved sooner).

If the problem is resolved and a recovery message is configured, it will be sent to those who received at least one problem message within this escalation scenario.
Note:
If the trigger that generated an active escalation is disabled, Zabbix sends an informative message about it to all those that have already received notifications.

Example 2
Sending a delayed notification about a long-standing problem. To configure:

- In Operations tab, set the Default operation step duration to '10h' (10 hours)
- Set the escalation steps to be From '2' To '2'

A notification will only be sent at Step 2 of the escalation scenario, or 10 hours after the problem starts.

You can customize the message text to something like 'The problem is more than 10 hours old'.

Example 3
Escalating the problem to the Boss.

In the first example above we configured periodical sending of messages to MySQL administrators. In this case, the administrators will get four messages before the problem will be escalated to the Database manager. Note that the manager will get a message only in case the problem is not acknowledged yet, supposedly no one is working on it.
Note the use of \{ESC.HISTORY\} macro in the message. The macro will contain information about all previously executed steps on this escalation, such as notifications sent and commands executed.

Example 4

A more complex scenario. After multiple messages to MySQL administrators and escalation to the manager, Zabbix will try to restart the MySQL database. It will happen if the problem exists for 2:30 hours and it hasn’t been acknowledged.

If the problem still exists, after another 30 minutes Zabbix will send a message to all guest users.

If this does not help, after another hour Zabbix will reboot server with the MySQL database (second remote command) using IPMI commands.
Example 5

An escalation with several operations assigned to one step and custom intervals used. The default operation step duration is 30 minutes.

Notifications will be sent as follows:

- to MySQL administrators at 0:00, 0:30, 1:00, 1:30 after the problem starts
- to Database manager at 2:00 and 2:10 (and not at 3:00; seeing that steps 5 and 6 overlap with the next operation, the shorter custom step duration of 10 minutes in the next operation overrides the longer step duration of 1 hour tried to set here)
- to Zabbix administrators at 2:00, 2:10, 2:20 after the problem starts (the custom step duration of 10 minutes working)
- to guest users at 4:00 hours after the problem start (the default step duration of 30 minutes returning between steps 8 and 11)
3 Receiving notification on unsupported items

Overview
Receiving notifications on unsupported items is supported since Zabbix 2.2.

It is part of the concept of internal events in Zabbix, allowing users to be notified on these occasions. Internal events reflect a change of state:

• when items go from 'normal' to 'unsupported' (and back)
• when triggers go from 'normal' to 'unknown' (and back)
• when low-level discovery rules go from 'normal' to 'unsupported' (and back)

This section presents a how-to for receiving notification when an item turns unsupported.

Configuration

Overall, the process of setting up the notification should feel familiar to those who have set up alerts in Zabbix before.

Step 1

Configure some media, such as e-mail, SMS or Jabber, to use for the notifications. Refer to the corresponding sections of the manual to perform this task.

Attention:
For notifying on internal events the default severity ('Not classified') is used, so leave it checked when configuring user media if you want to receive notifications for internal events.

Step 2

Go to Configuration→Actions and select Internal as the event source. Click on Create action on the upper right to open an action configuration form.

Step 3

In the Action tab enter a name for the action. Then select Event type in the New condition block and select Item in "not supported" state as the value.
Don’t forget to click on Add to actually list the condition in the Conditions block.

Step 4

In the Operations tab, enter the subject/content of the problem message.

Click on New in the Operations block and select some recipients of the message (user groups/users) and the media types (or ‘All’) to use for delivery.

Click on Add in the Operation details block to actually list the operation in the Operations block.

If you wish to receive more than one notification, set the operation step duration (interval between messages sent) and add another
Step 5

The **Recovery operations** tab allows to configure a recovery notification when an item goes back to the normal state.

Enter the subject/content of the recovery message.

Click on New in the Operations block and select some recipients of the message (user groups/users) and the media types (or ‘All’) to use for delivery.

Click on Add in the Operation details block to actually list the operation in the Operations block.

Step 6

When finished, click on the **Add** button underneath the form.

And that’s it, you’re done! Now you can look forward to receiving your first notification from Zabbix if some item turns unsupported.

10 Macros

**Overview**

Zabbix supports a number of macros which may be used in various situations. Macros are variables, identified by a specific syntax: `{MACRO}`

Macros resolve to a specific value depending on the context.

Effective use of macros allows to save time and make Zabbix configuration more transparent.
In one of typical uses, a macro may be used in a template. Thus a trigger on a template may be named “Processor load is too high on \{HOST.NAME\}”. When the template is applied to the host, such as Zabbix server, the name will resolve to “Processor load is too high on Zabbix server” when the trigger is displayed in the Monitoring section.

Macros may be used in item key parameters. A macro may be used for only a part of the parameter, for example \item.key[server_{HOST.HOST}_local]. Double-quoting the parameter is not necessary as Zabbix will take care of any ambiguous special symbols, if present in the resolved macro.

See also:
- full list of supported macros
- macro functions
- how to configure user macros

1 Macro functions

Overview

Macro functions offer the ability to customize macro values.

Sometimes a macro may resolve to a value that is not necessarily easy to work with. It may be long or contain a specific substring of interest that you would like to extract. This is where macro functions can be useful.

The syntax of a macro function is:

\{<macro>.<func>(<params>)\}

where:

- `<macro>` - the macro to customize (for example \{ITEM.VALUE\} or \#LLDMACRO\})
- `<func>` - the function to apply
- `<params>` - a comma-delimited list of function parameters. Parameters must be quoted if they start with " " (space), " or contain ),,,.

For example:

\{{ITEM.VALUE}.regsub(pattern, output)}
\{{#LLDMACRO}.regsub(pattern, output)}

Supported macro functions

<table>
<thead>
<tr>
<th>FUNCTION</th>
<th>Description</th>
<th>Parameter Supported for</th>
</tr>
</thead>
<tbody>
<tr>
<td>regsub</td>
<td>Substring extraction by a regular expression match (case sensitive).</td>
<td>{ITEM.VALUE} {ITEM.LASTVALUE} Low-level discovery macros (except in low-level discovery rule filter)</td>
</tr>
<tr>
<td></td>
<td>\textbf{pattern} - the regular expression to match \textbf{output} - the output options. \1 - \9 placeholders are supported to capture groups. \0 returns the matched text.</td>
<td></td>
</tr>
</tbody>
</table>
**FUNCTION**

`iregsub (<pattern>, <output>)`

- **Substring extraction by a regular expression match** (case insensitive).
- **pattern** - the regular expression to match
- **output** - the output options. \1 - \9 placeholders are supported to capture groups.
- \0 returns the matched text.

If a function is used in a supported location, but applied to a macro not supporting macro functions, then the macro evaluates to 'UNKNOWN'.

If pattern is not a correct regular expression then the macro evaluates to 'UNKNOWN' (excluding low-level discovery macros where the function will be ignored in that case and macro will remain unexpanded).

If a macro function is applied to the macro in locations not supporting macro functions then the function is ignored.

**Examples**

The ways in which macro functions can be used to customize macro values is illustrated in the following examples containing log lines as received value:

<table>
<thead>
<tr>
<th>Received value</th>
<th>Macro</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>123Log line</td>
<td>{{ITEM.VALUE}.regsub('^[0-9]+', 'Problem')}</td>
<td>Problem</td>
</tr>
<tr>
<td>123 Log line</td>
<td>{{ITEM.VALUE}.regsub('{\1}', 'Problem')}</td>
<td>Problem</td>
</tr>
<tr>
<td>123 Log line</td>
<td>{{ITEM.VALUE}.regsub('^[0-9]+', 'Problem ID: \1')}</td>
<td>Problem ID: 123</td>
</tr>
<tr>
<td>Log line</td>
<td>{{ITEM.VALUE}.regsub('.*', 'Problem ID: \1')}</td>
<td>&quot;Problem ID: \1&quot;</td>
</tr>
<tr>
<td>MySQL crashed errno 123</td>
<td>{{ITEM.VALUE}.regsub('.*', 'Problem ID: \1')}</td>
<td>&quot;Problem ID: \1&quot;</td>
</tr>
<tr>
<td>123 Log line</td>
<td>{{ITEM.VALUE}.regsub('^[1-9]+', 'Problem ID: \1')}</td>
<td>Problem ID: \1</td>
</tr>
<tr>
<td>customername_1</td>
<td>{{#IFALIAS}.regsub(&quot;(.*)_[[0-9]+&quot;, \1)}</td>
<td>customername</td>
</tr>
<tr>
<td>customername_1</td>
<td>{{#IFALIAS}.regsub(&quot;(.*([0-9]+)+&quot;, \2)}</td>
<td>1</td>
</tr>
<tr>
<td>customername_1</td>
<td>{{#IFALIAS}.regsub(&quot;.*([0-9]+)+&quot;, \1)\2}</td>
<td>(invalid regular expression)</td>
</tr>
</tbody>
</table>

448
2 User macros

Overview

User macros are supported in Zabbix for greater flexibility, in addition to the macros supported out-of-the-box.

User macros can be defined on global, template and host level. These macros have a special syntax:

`{$MACRO}`

Zabbix expands macros according to the following precedence:

1. host level macros (checked first)
2. macros defined for first level templates of the host (i.e., templates linked directly to the host), sorted by template ID
3. macros defined for second level templates of the host, sorted by template ID
4. macros defined for third level templates of the host, sorted by template ID, etc.
5. global macros (checked last)

In other words, if a macro does not exist for a host, Zabbix will try to find it in the host templates of increasing depth. If still not found, a global macro will be used, if exists.

**Warning:**
If a macro with the same name exists on multiple templates of the same level, the macro from the template with the lowest ID will be used. Thus having macros with the same name in multiple templates is a configuration risk.

If Zabbix is unable to find a macro, the macro will not be expanded.

**Attention:**
Macros (including user macros) are left unresolved in the Configuration section (for example, in the trigger list) by design to make complex configuration more transparent.

User macros can be used in:

- item name
- item key parameter
- item update intervals and flexible intervals
- trigger name and description
- trigger expression parameters and constants (see examples)
- many other locations - see the full list

Common use cases of global and host macros

---

<table>
<thead>
<tr>
<th>Received value</th>
<th>Macro</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>customername_1</td>
<td>{$MACRO:&quot;{{#IFALIAS}.regsub(&quot;(.*)_([0-9]+)&quot;, \1)&quot;}&quot;}</td>
<td>{$MACRO:&quot;customername&quot;}</td>
</tr>
<tr>
<td>customername_1</td>
<td>{$MACRO:&quot;{{#IFALIAS}.regsub(&quot;(.*)_([0-9]+)&quot;, \1)&quot;}&quot;}</td>
<td>{$MACRO:&quot;1&quot;}</td>
</tr>
<tr>
<td>customername_1</td>
<td>{$MACRO:&quot;{{#IFALIAS}.regsub(&quot;(.*)_([0-9]+)&quot;, \1)&quot;}&quot;}</td>
<td>{$MACRO:&quot;{{#IFALIAS}.regsub(&quot;(.*)_([0-9]+)&quot;, \1)&quot;}&quot;} (invalid regular expression)</td>
</tr>
</tbody>
</table>

Seeing full item values

Long values of resolved `{ITEM.VALUE}` and `{ITEM.LASTVALUE}` macros for text/log items are truncated to 20 characters in some frontend locations. To see the full values of these macros you may use macro functions, e.g.:

```
{{ITEM.VALUE}.regsub("(.*)", \1)}
{{ITEM.LASTVALUE}.regsub("(.*)", \1)}
```

See also: `{ITEM.VALUE}` and `{ITEM.LASTVALUE}` macro details.
• use a global macro in several locations; then change the macro value and apply configuration changes to all locations with one click
• take advantage of templates with host-specific attributes: passwords, port numbers, file names, regular expressions, etc.

Configuration
To define user macros, go to the corresponding locations in the frontend:
• for global macros, visit Administration → General → Macros
• for host and template level macros, open host or template properties and look for the Macros tab

Note:
If a user macro is used in items or triggers in a template, it is suggested to add that macro to the template even if it is defined on a global level. That way, exporting the template to XML and importing it in another system will still allow it to work as expected.

The following characters are allowed in the macro names: A-Z, 0-9, _, .

Examples
Example 1
Use of host-level macro in the “Status of SSH daemon” item key:
net.tcp.service[ssh,,{$SSH_PORT}]
This item can be assigned to multiple hosts, providing that the value of {$SSH_PORT} is defined on those hosts.

Example 2
Use of host-level macro in the “CPU load is too high” trigger:
{ca_001:system.cpu.load[,avg1].last()}>{MAX_CPULOAD}
Such a trigger would be created on the template, not edited in individual hosts.

Note:
If you want to use amount of values as the function parameter (for example, max(#3)), include hash mark in the macro definition like this: SOME_PERIOD=>#3

Example 3
Use of two macros in the “CPU load is too high” trigger:
{ca_001:system.cpu.load[,avg1].min({$CPULOAD_PERIOD})}>{MAX_CPULOAD}
Note that a macro can be used as a parameter of trigger function, in this example function min().

Attention:
In trigger expressions user macros will resolve if referencing a parameter or constant. They will NOT resolve if referencing the host, item key, function, operator or another trigger expression.

Example 4
Synchronize the agent unavailability condition with the item update interval:
• define {$INTERVAL} macro and use it in the item update interval;
• use {$INTERVAL} as parameter of the agent unavailability trigger:
{ca_001:agent.ping.nodata({$INTERVAL})}=1

Example 5
Centralize configuration of working hours:
• create a global {$WORKING_HOURS} macro equal to 1–5, 09:00–18:00;
• use it in Administration → General → Working time;
• use it in User → Media → When active;
• use it to set up more frequent item polling during working hours:
• use it in the Time period action condition;
• adjust the working time in Administration → General → Macros, if needed.

User macro context
An optional context can be used in user macros, allowing to override the default value with context-specific one.

User macros with context have a similar syntax:

```
{$MACRO:context}
```

Macro context is a simple text value. The common use case for macro contexts would be using a low-level discovery macro value as a user macro context. For example, a trigger prototype could be defined for mounted file system discovery to use a different low space limit depending on the mount points or file system types.

Only low-level discovery macros are supported in macro contexts. Any other macros are ignored and treated as plain text.

Technically, macro context is specified using rules similar to item key parameters, except macro context is not parsed as several parameters if there is a `, character:

• Macro context must be quoted with " if the context contains a } character or starts with a " character. Quotes inside quoted context must be escaped with the `\` character. The `\` character itself is not escaped, which means it's impossible to have a quoted context ending with the `\` character - the macro `{\$MACRO: "a:\b\c\"}` is invalid.
• The leading spaces in context are ignored, the trailing spaces are not. For example `{\$MACRO: A}` is the same as `{\$MACRO: A};`, but not `{\$MACRO: A }`.
• All spaces before leading quotes and after trailing quotes are ignored, but all spaces inside quotes are not. Macros `{\$MACRO: "A"}`, `{\$MACRO: "A"}`, `{\$MACRO: " A "}` and `{\$MACRO: " A "}` are not.

The following macros are all equivalent, because they have the same context: `{\$MACRO: A}`, `{\$MACRO: A}` and `{\$MACRO: "A"}`. This is in contrast with item keys, where key[a], key[ a] and key["a"] are the same semantically, but different for uniqueness purposes.

When context macros are processed, Zabbix looks up the macro with its context. If a macro with this context is not defined by host or linked templates, and it is not a defined as a global macro with context, then the macro without context is searched for.

See usage example of macro context in a disk space trigger prototype and take limitation clause into consideration.

3 Low-level discovery macros

Overview
There is a type of macro used within the low-level discovery (LLD) function:

```
{#MACRO}
```

It is a macro that is used in an LLD rule and returns real values of file system names, network interfaces and SNMP OIDs.

These macros can be used for creating item, trigger and graph prototypes. Then, when discovering real file systems, network interfaces etc., these macros are substituted with real values and are the basis for creating real items, triggers and graphs.

These macros are also used in creating host and host group prototypes in virtual machine discovery.

Some low-level discovery macros come "pre-packaged" with the LLD function in Zabbix - `{#FSNAME}`, `{#FSTYPE}`, `{#IFNAME}`, `{#SNMPINDEX}`, `{#SNMPVALUE}`. However, adhering to these names is not compulsory when creating a custom low-level discovery rule. Then you may use any other LLD macro name and refer to that name.

Supported locations
LLD macros can be used:

• in the low-level discovery rule filter
• for item prototypes in
  - names
- key parameters
- units
- update intervals
- history storage periods
- trend storage periods
- application prototypes
- SNMP OIDs
- IPMI sensor fields
- calculated item formulas
- SSH and Telnet scripts
- database monitoring SQL queries
- jMX item endpoint fields
- descriptions
- since Zabbix 4.0 also in:
  - item value preprocessing steps
  - HTTP agent URL field
  - HTTP agent HTTP query fields field
  - HTTP agent request body field
  - HTTP agent required status codes field
  - HTTP agent headers field key and value
  - HTTP agent HTTP authentication username field
  - HTTP agent HTTP authentication password field
  - HTTP agent HTTP proxy field
  - HTTP agent HTTP SSL certificate file field
  - HTTP agent HTTP SSL key file field
  - HTTP agent HTTP SSL key password field
  - HTTP agent HTTP timeout field

- for trigger prototypes in
  - names
  - expression (only in constants and function parameters)
  - URLs
  - descriptions
  - event tag names and values
- for graph prototypes in
  - names
- for host prototypes in
  - names
  - visible names
  - host group prototype names
  - (see the full list)

In all those places LLD macros can be used inside user macro context.

Using macro functions

Macro functions are supported with low-level discovery macros (except in low-level discovery rule filter), allowing to extract a certain part of the macro value using a regular expression.

For example, you may want to extract the customer name and interface number from the following LLD macro for the purposes of event tagging:

```
{#IFALIAS}=customername_1
```

To do so, the `regsub` macro function can be used with the macro in the event tag value field of a trigger prototype:

```
<Tags>
  <Customer>{{#IFALIAS}.regsub("(.*)_(\[0-9\]+)", \1)}</Customer>
  <Interface>{{#IFALIAS}.regsub("(.*)_(\[0-9\]+)", \2)}</Interface>
</Tags>
```

Note, that commas are not allowed in unquoted item key parameters, so the parameter containing a macro function has to be quoted. The backslash (\) character should be used to escape double quotes inside the parameter. Example:

```
net.if.in["{{#IFALIAS}.regsub("(.*)_([0-9]+)\", \1)"}, bytes]
```
For more information on macro function syntax, see: Macro functions

Macro functions are supported in low-level discovery macros since Zabbix 4.0.

Footnotes

1 In the fields marked with 1 a single macro has to fill the whole field. Multiple macros in a field or macros mixed with text are not supported.

11 Users and user groups

Overview

All users in Zabbix access the Zabbix application through the web-based frontend. Each user is assigned a unique login name and a password.

All user passwords are encrypted and stored in the Zabbix database. Users cannot use their user id and password to log directly into the UNIX server unless they have also been set up accordingly to UNIX. Communication between the web server and the user browser can be protected using SSL.

With a flexible user permission schema you can restrict and differentiate access to:

- administrative Zabbix frontend functions
- monitored hosts in hostgroup

1 Configuring a user

Overview

The initial Zabbix installation has two predefined users:

- Admin - a Zabbix superuser with full permissions;
- guest - a special Zabbix user. As a guest, you may access monitoring pages in Zabbix without being logged in. Note that by default, ‘guest’ has no permissions on Zabbix objects. (Starting with Zabbix 4.0.15, the ‘guest’ user is disabled by default. To re-enable it, add it to the Guests user group.)

To configure a new user:

- Go to Administration → Users
- Click on Create user (or on the user name to edit an existing user)
- Edit user attributes in the form

General attributes

The User tab contains general user attributes:
All mandatory input fields are marked with a red asterisk.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Alias</strong></td>
<td>Unique username, used as the login name.</td>
</tr>
<tr>
<td>Name</td>
<td>User first name (optional). If not empty, visible in acknowledgment information and notification recipient information.</td>
</tr>
<tr>
<td>Surname</td>
<td>User last name (optional). If not empty, visible in acknowledgment information and notification recipient information.</td>
</tr>
<tr>
<td><strong>Groups</strong></td>
<td>Select user groups the user belongs to. Starting with Zabbix 3.4.3 this field is auto-complete so starting to type the name of a user group will offer a dropdown of matching groups. Scroll down to select. Alternatively, click on Select to add groups. Click on 'x' to remove the selected. Adherence to user groups determines what host groups and hosts the user will have access to.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Two fields for entering the user password. With an existing password, contains a Password button, clicking on which opens the password fields.</td>
</tr>
<tr>
<td><strong>Password (once again)</strong></td>
<td>Two fields for entering the user password. With an existing password, contains a Password button, clicking on which opens the password fields.</td>
</tr>
<tr>
<td>Language</td>
<td>Language of the Zabbix frontend. The php gettext extension is required for the translations to work.</td>
</tr>
<tr>
<td>Theme</td>
<td>Defines how the frontend looks like: <strong>System default</strong> - use default system settings <strong>Blue</strong> - standard blue theme <strong>Dark</strong> - alternative dark theme <strong>High-contrast light</strong> - light theme with high contrast <strong>High-contrast dark</strong> - dark theme with high contrast</td>
</tr>
<tr>
<td>Auto-login</td>
<td>Mark this checkbox to make Zabbix remember the user and log the user in automatically for 30 days. Browser cookies are used for this.</td>
</tr>
</tbody>
</table>
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-logout</td>
<td>With this checkbox marked the user will be logged out automatically, after the set amount of seconds (minimum 90 seconds, maximum 1 day). Time suffixes are supported, e.g. 90s, 5m, 2h, 1d. Note that this option will not work: * If the “Show warning if Zabbix server is down” global configuration option is enabled and Zabbix frontend is kept open; * When Monitoring menu pages perform background information refreshes; * If logging in with the Remember me for 30 days option checked.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Set the refresh rate used for graphs, screens, plain text data, etc. Can be set to 0 to disable.</td>
</tr>
<tr>
<td>Rows per page</td>
<td>You can determine how many rows per page will be displayed in lists.</td>
</tr>
<tr>
<td>URL (after login)</td>
<td>You can make Zabbix transfer the user to a specific URL after successful login, for example, to Problems page.</td>
</tr>
</tbody>
</table>

### User media

The Media tab contains a listing of all media defined for the user. Media are used for sending notifications. Click on Add to assign media to the user.

See the Media types section for details on configuring media types.

### Permissions

The Permissions tab contains information on:

- the user type (Zabbix User, Zabbix Admin, Zabbix Super Admin). Users cannot change their own type.
- host groups the user has access to. ‘Zabbix User’ and ‘Zabbix Admin’ users do not have access to any host groups and hosts by default. To get access they need to be included in user groups that have access to respective host groups and hosts.

See the User permissions page for details.

## 2 Permissions

### Overview

You can differentiate user permissions in Zabbix by defining the respective user type and then by including the unprivileged users in user groups that have access to host group data.

### User type

The user type defines the level of access to administrative menus and the default access to host group data.

<table>
<thead>
<tr>
<th>User type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zabbix User</td>
<td>The user has access to the Monitoring menu. The user has no access to any resources by default. Any permissions to host groups must be explicitly assigned.</td>
</tr>
<tr>
<td>Zabbix Admin</td>
<td>The user has access to the Monitoring and Configuration menus. The user has no access to any host groups by default. Any permissions to host groups must be explicitly given.</td>
</tr>
<tr>
<td>Zabbix Super Admin</td>
<td>The user has access to everything: Monitoring, Configuration and Administration menus. The user has a read-write access to all host groups. Permissions cannot be revoked by denying access to specific host groups.</td>
</tr>
</tbody>
</table>

### Permissions to host groups

Access to any host data in Zabbix are granted to user groups on host group level only.

That means that an individual user cannot be directly granted access to a host (or host group). It can only be granted access to a host by being part of a user group that is granted access to the host group that contains the host.
3 User groups

Overview

User groups allow to group users both for organizational purposes and for assigning permissions to data. Permissions to monitoring data of host groups are assigned to user groups, not individual users.

It may often make sense to separate what information is available for one group of users and what - for another. This can be accomplished by grouping users and then assigning varied permissions to host groups.

A user can belong to any number of groups.

Configuration

To configure a user group:

- Go to Administration → User groups
- Click on Create user group (or on the group name to edit an existing group)
- Edit group attributes in the form

The User group tab contains general group attributes:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group name</td>
<td>Unique group name.</td>
</tr>
<tr>
<td>Users</td>
<td>How the users of the group are authenticated.</td>
</tr>
<tr>
<td>Frontend access</td>
<td>System default - use default authentication method (set globally)</td>
</tr>
<tr>
<td></td>
<td>Internal - use Zabbix internal authentication (even if LDAP authentication is used globally).</td>
</tr>
<tr>
<td></td>
<td>LDAP - use LDAP authentication (even if internal authentication is used globally).</td>
</tr>
<tr>
<td></td>
<td>Ignored if HTTP authentication is the global default.</td>
</tr>
<tr>
<td></td>
<td>Disabled - access to Zabbix frontend is forbidden for this group</td>
</tr>
</tbody>
</table>

All mandatory input fields are marked with a red asterisk.

The Permissions tab allows you to specify user group access to host group (and thereby host) data:
Current permissions to host groups are displayed in the Permissions block.

If current permissions of the host group are inherited by all nested host groups, this is indicated after the host group name ("including subgroups"). Note that a Zabbix Super admin user can enforce nested host groups to have the same level of permissions as the parent host group; this can be done in the host group configuration form.

You may change the level of access to a host group:

- **Read-write** - read-write access to a host group;
- **Read** - read-only access to a host group;
- **Deny** - access to a host group denied;
- **None** - no permissions are set.

Use the selection field below to select host groups and the level of access to them. This field is auto-complete so starting to type the name of a host group will offer a dropdown of matching host groups. If you wish to see all host groups, click on Select. If you wish to include nested host groups, mark the Include subgroups checkbox. Click on to add the selected host groups to the list of host group permissions.

**Attention:**
Adding a parent host group with the Include subgroups checkbox marked will override (and remove from the list) previously configured permissions of all related nested host groups. Adding a host group with None as the level of access selected will remove the host group from the list if the host group is already in the list.

The **Tag filter** tab allows you to set tag based permissions for user groups to see problems filtered by tag name and its value:

To select a host group to apply a tag filter for, click Select to get the complete list of existing host groups or start to type the name of a host group to get a dropdown of matching groups. If you want to apply tag filters to nested host groups, mark the Include subgroups checkbox.

Tag filter allows to separate the access to host group from the possibility to see problems.

For example, if a database administrator needs to see only "MySQL" database problems, it is required to create a user group for database administrators first, than specify "Service" tag name and "MySQL" value.

If "Service" tag name is specified and value field is left blank, corresponding user group will see all problems for selected host...
group with tag name “Service”. If both tag name and value fields are left blank but host group selected, corresponding user group will see all problems for selected host group. Make sure a tag name and tag value are correctly specified otherwise a corresponding user group will not see any problems.

Let’s review an example when a user is a member of several user groups selected. Filtering in this case will use OR condition for tags.

<table>
<thead>
<tr>
<th>User group A</th>
<th>User group B</th>
<th>Visible result for a user (member) of both groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tag filter</td>
<td>Tag name</td>
<td>Tag value</td>
</tr>
<tr>
<td>Host group</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Templates/Databases</td>
<td>Service</td>
<td>MySQL</td>
</tr>
<tr>
<td>Templates/Databases</td>
<td>blank</td>
<td>blank</td>
</tr>
<tr>
<td>not selected</td>
<td>blank</td>
<td>blank</td>
</tr>
</tbody>
</table>

**Attention:**
Adding a filter (for example, all tags in a certain host group “Templates/Databases”) results in not being able to see the problems of other host groups.

Host access from several user groups

A user may belong to any number of user groups. These groups may have different access permissions to hosts. Therefore, it is important to know what hosts an unprivileged user will be able to access as a result. For example, let us consider how access to host X (in Hostgroup 1) will be affected in various situations for a user who is in user groups A and B.

- If Group A has only Read access to Hostgroup 1, but Group B Read-write access to Hostgroup 1, the user will get **Read-write** access to ‘X’.

**Attention:**
“Read-write” permissions have precedence over “Read” permissions starting with Zabbix 2.2.

- In the same scenario as above, if ‘X’ is simultaneously also in Hostgroup 2 that is denied to Group A or B, access to ‘X’ will be **unavailable**, despite a Read-write access to Hostgroup 1.
- If Group A has no permissions defined and Group B has a Read-write access to Hostgroup 1, the user will get **Read-write** access to ‘X’.
- If Group A has Deny access to Hostgroup 1 and Group B has a Read-write access to Hostgroup 1, the user will get access to ‘X’ **denied**.

Other details

- An Admin level user with Read-write access to a host will not be able to link/unlink templates, if he has no access to the Templates group. With Read access to Templates group he will be able to link/unlink templates to the host, however, will not see any templates in the template list and will not be able to operate with templates in other places.
- An Admin level user with Read access to a host will not see the host in the configuration section host list; however, the host triggers will be accessible in IT service configuration.
- Any non-Zabbix Super Admin user (including ‘guest’) can see network maps as long as the map is empty or has only images. When hosts, host groups or triggers are added to the map, permissions are respected. The same applies to screens and slideshows as well. The users, regardless of permissions, will see any objects that are not directly or indirectly linked to hosts.
- Zabbix server will not send notifications to users defined as action operation recipients if access to the concerned host is explicitly “denied”.

458
8. Service monitoring

Overview  Service monitoring functionality is intended for those who want to get a high-level (business) view of monitored infrastructure. In many cases, we are not interested in low-level details, like the lack of disk space, high processor load, etc. What we are interested in is the availability of service provided by our IT department. We can also be interested in identifying weak places of IT infrastructure, SLA of various IT services, the structure of existing IT infrastructure, and other information of a higher level.

Zabbix service monitoring provides answers to all mentioned questions.

Services is a hierarchy representation of monitored data.

A very simple service structure may look like:

```
Service
 |
 |-Workstations
 | |
 | |-Workstation1
 | | |
 | | |-Workstation2
 | |
 |-Servers
```

Each node of the structure has attribute status. The status is calculated and propagated to upper levels according to the selected algorithm. At the lowest level of services are triggers. The status of individual nodes is affected by the status of their triggers.

**Note:**
Note that triggers with a Not classified or Information severity do not impact SLA calculation.

Configuration  To configure services, go to: Configuration → Services.

On this screen you can build a hierarchy of your monitored infrastructure. The highest-level parent service is ‘root’. You can build your hierarchy downward by adding lower-level parent services and then individual nodes to them.

Click on Add child to add services. To edit an existing service, click on its name. A form is displayed where you can edit the service attributes.

Configuring a service
The **Service** tab contains general service attributes:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Service name.</td>
</tr>
<tr>
<td>Parent service</td>
<td>Parent service the service belongs to.</td>
</tr>
<tr>
<td>Status calculation algorithm</td>
<td>Method of calculating service status:</td>
</tr>
<tr>
<td></td>
<td><strong>Do not calculate</strong> - do not calculate service status</td>
</tr>
<tr>
<td></td>
<td><strong>Problem, if at least one child has a problem</strong> - problem status, if at least one child service has a problem</td>
</tr>
<tr>
<td></td>
<td><strong>Problem, if all children have problems</strong> - problem status, if all child services are having problems</td>
</tr>
<tr>
<td>Calculate SLA, acceptable SLA (in %)</td>
<td>Enable SLA calculation and display. SLA percentage that is acceptable for this service. Used for reporting.</td>
</tr>
<tr>
<td>Trigger</td>
<td>Linkage to trigger:</td>
</tr>
<tr>
<td></td>
<td><strong>None</strong> - no linkage</td>
</tr>
<tr>
<td></td>
<td><strong>trigger name</strong> - linked to the trigger, thus depends on the trigger status</td>
</tr>
<tr>
<td></td>
<td>Services of the lowest level must be linked to triggers. (Otherwise their state will not be represented accurately.)</td>
</tr>
<tr>
<td></td>
<td>When triggers are linked, their state prior to linking is not counted.</td>
</tr>
<tr>
<td>Sort order (0-&gt;999)</td>
<td>Sort order for display, lowest comes first.</td>
</tr>
</tbody>
</table>

All mandatory input fields are marked with a red asterisk.

The **Dependencies** tab contains services the service depends on. Click on Add to add a service from those that are configured.
Hard and soft dependency

Availability of a service may depend on several other services, not just one. The first option is to add all those directly as child services.

However, if some service is already added somewhere else in the services tree, it cannot be simply moved out of there to a child service here. How to create a dependency on it? The answer is “soft” linking. Add the service and mark the Soft check box. That way the service can remain in its original location in the tree, yet be depended upon from several other services. Services that are “soft-linked” are displayed in gray in the tree. Additionally, if a service has only “soft” dependencies, it can be deleted directly, without deleting child services first.

The Time tab contains the service time specification.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service times</td>
<td>By default, all services are expected to operate 24x7x365. If exceptions needed, add new service times.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| New service time      | Service times:  
**Uptime** - service uptime  
**Downtime** - service state within this period does not affect SLA.  
**One-time downtime** - a single downtime. Service state within this period does not affect SLA.  
Add the respective hours.  
Note: Service times affect only the service they are configured for. Thus, a parent service will not take into account the service time configured on a child service (unless a corresponding service time is configured on the parent service as well).  
Service times are taken into account when calculating service status and SLA by the frontend. However, information on service availability is being inserted into database continuously, regardless of service times. |

**Display**  
To monitor services, go to Monitoring → Services.

### 9. Web monitoring

**Overview**  
With Zabbix you can check several availability aspects of web sites.

---

**Attention:**  
To perform web monitoring Zabbix server must be initially configured with cURL (libcurl) support.

To activate web monitoring you need to define web scenarios. A web scenario consists of one or several HTTP requests or “steps”. The steps are periodically executed by Zabbix server in a pre-defined order. If a host is monitored by proxy, the steps are executed by the proxy.

Since Zabbix 2.2 web scenarios are attached to hosts/templates in the same way as items, triggers, etc. That means that web scenarios can also be created on a template level and then applied to multiple hosts in one move.

The following information is collected in any web scenario:

- average download speed per second for all steps of whole scenario  
- number of the step that failed  
- last error message

The following information is collected in any web scenario step:

- download speed per second  
- response time  
- response code

For more details, see web monitoring items.

Data collected from executing web scenarios is kept in the database. The data is automatically used for graphs, triggers and notifications.

Zabbix can also check if a retrieved HTML page contains a pre-defined string. It can execute a simulated login and follow a path of simulated mouse clicks on the page.

Zabbix web monitoring supports both HTTP and HTTPS. When running a web scenario, Zabbix will optionally follow redirects (see option Follow redirects below). Maximum number of redirects is hard-coded to 10 (using cURL option `CURLOPT_MAXREDIRS`). All cookies are preserved during the execution of a single scenario.

See also known issues for web monitoring using HTTPS protocol.

**Configuring a web scenario**  
To configure a web scenario:

- Go to: Configuration → Hosts (or Templates)  
- Click on Web in the row of the host/template  
- Click on Create web scenario to the right (or on the scenario name to edit an existing scenario)
• Enter parameters of the scenario in the form

The **Scenario** tab allows you to configure the general parameters of a web scenario.

### Scenario parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique scenario name.</td>
</tr>
<tr>
<td>Application</td>
<td>Select an application the scenario will belong to. Web scenario items will be grouped under the selected application in Monitoring → Latest data.</td>
</tr>
<tr>
<td>New application</td>
<td>Enter the name of a new application for the scenario.</td>
</tr>
<tr>
<td>Update interval</td>
<td>How often the scenario will be executed. Time suffixes are supported, e.g. 30s, 1m, 2h, 1d, since Zabbix 3.4.0. User macros are supported, since Zabbix 3.4.0. Note that if a user macro is used and its value is changed (e.g. 5m → 30s), the next check will be executed according to the previous value (farther in the future with the example values).</td>
</tr>
</tbody>
</table>
**Parameter** | **Description**
---|---
Attempts | The number of attempts for executing web scenario steps. In case of network problems (timeout, no connectivity, etc) Zabbix can repeat executing a step several times. The figure set will equally affect each step of the scenario. Up to 10 attempts can be specified, default value is 1.
  Note: Zabbix will not repeat a step because of a wrong response code or the mismatch of a required string.
  This parameter is supported starting with Zabbix 2.2.
Agent | Select a client agent.
  Zabbix will pretend to be the selected browser. This is useful when a website returns different content for different browsers.
  User macros can be used in this field, starting with Zabbix 2.2.
HTTP proxy | You can specify an HTTP proxy to use, using the format
[protocol://][username[:password]@]proxy.example.com[:port].
  This sets the CURLOPT_PROXY cURL option.
  The optional protocol:// prefix may be used to specify alternative proxy protocols (the protocol prefix support was added in cURL 7.21.7). With no protocol specified, the proxy will be treated as an HTTP proxy.
  By default, 1080 port will be used.
  If specified, the proxy will overwrite proxy related environment variables like http_proxy, HTTPS_PROXY. If not specified, the proxy will not overwrite proxy-related environment variables. The entered value is passed on “as is”, no sanity checking takes place.
  You may also enter a SOCKS proxy address. If you specify the wrong protocol, the connection will fail and the item will become unsupported.
  Note that only simple authentication is supported with HTTP proxy.
  User macros can be used in this field.
  This parameter is supported starting with Zabbix 2.2.
Variables | Variables that may be used in scenario steps (URL, post variables).
  They have the following format:
  `{macro1}=value1`  
  `{macro2}=value2`  
  `{macro3}=regex:<regular expression>`
  For example:
  `{username}=Alexei`  
  `{password}=kj3h5kJ34bd`  
  `{hostid}=regex:hostidis([0-9]+)`
  The macros can then be referenced in the steps as `username`, `password` and `hostid`. Zabbix will automatically replace them with actual values.
  Note that variables with regex: need one step to get the value of the regular expression so the extracted value can only be applied to the step after.
  If the value part starts with regex: then the part after it is treated as a regular expression that searches the web page and, if found, stores the match in the variable. At least one subgroup must be present so that the matched value can be extracted.
  Regular expression match in variables is supported since Zabbix 2.2.
  User macros and `{HOST.*}` macros are supported, since Zabbix 2.2.
  Variables are automatically URL-encoded when used in query fields or form data for post variables, but must be URL-encoded manually when used in raw post or directly in URL.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Headers   | Custom HTTP headers that will be sent when performing a request. Headers should be listed using the same syntax as they would appear in the HTTP protocol, optionally using some additional features supported by the `CURLOPT_HTTPHEADER` cURL option. For example:  
  - `Accept-Charset=utf-8`  
  - `Accept-Language=en-US`  
  - `Content-Type=application/xml; charset=utf-8`  
  - `User macros and {HOST.*} macros are supported`.  
  - Specifying custom headers is supported starting with Zabbix 2.4. The scenario is active if this box is checked, otherwise - disabled. |
| Enabled   | |

Note that when editing an existing scenario, two extra buttons are available in the form:

- **Clone**: Create another scenario based on the properties of the existing one.
- **Clear history and trends**: Delete history and trend data for the scenario. This will make the server perform the scenario immediately after deleting the data.

**Note:**

If HTTP proxy field is left empty, another way for using an HTTP proxy is to set proxy related environment variables. For HTTP checks - set the `http_proxy` environment variable for the Zabbix server user. For example, `http_proxy=http://proxy_ip:proxy_port`. For HTTPS checks - set the `HTTPS_PROXY` environment variable. For example, `HTTPS_PROXY=http://proxy_ip:proxy_port`. More details are available by running a shell command: `# man curl`.

The **Steps** tab allows you to configure the web scenario steps. To add a web scenario step, click on Add in the Steps block.
### Configuring steps

Step parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique step name.</td>
</tr>
</tbody>
</table>
| URL              | URL to connect to and retrieve data. For example:  
https://www.example.com  
http://www.example.com/download  
Domain names can be specified in Unicode characters since Zabbix 3.4. They are automatically punycode-converted to ASCII when executing the web scenario step.  
The Parse button can be used to separate optional query fields (like ?name=Admin&password=mypassword) from the URL, moving the attributes and values into Query fields for automatic URL-encoding.  
Variables can be used in the URL, using the {macro} syntax.  
Variables can be URL-encoded manually using a {{macro}.urlencode()} syntax.  
User macros and {HOST.*} macros are supported, since Zabbix 2.2. Limited to 2048 characters starting with Zabbix 2.4. |
<p>| URL              | <a href="http://www.google.com">http://www.google.com</a> |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Query fields</td>
<td>HTTP GET variables for the URL. Values are URL-encoded automatically. Values from scenario variables, user macros or <code>{HOST.*}</code> macros are resolved and then URL-encoded automatically. Using a <code>{macro}.urlencode()</code> syntax will double URL-encode them. User macros and <code>{HOST.*}</code> macros are supported since Zabbix 2.2.</td>
</tr>
<tr>
<td>Post</td>
<td>HTTP POST variables.</td>
</tr>
<tr>
<td></td>
<td>In Form data mode, specified as attribute and value pairs. Values are URL-encoded automatically. Values from scenario variables, user macros or <code>{HOST.*}</code> macros are resolved and then URL-encoded automatically. In Raw data mode, attributes/values are displayed on a single line and concatenated with a &amp; symbol. Raw values can be URL-encoded/decoded manually using a <code>{macro}.urlencode()</code> syntax. For example: id=2345&amp;userid={user} If {user} is defined as a variable of the web scenario, it will be replaced by its value when the step is executed. If you want to URL-encode the variable, substitute {user} with <code>{user}.urlencode()</code>. User macros and <code>{HOST.*}</code> macros are supported, since Zabbix 2.2.</td>
</tr>
</tbody>
</table>
| Variables             | Step-level variables that may be used for GET and POST functions. Step-level variables override scenario-level variables or variables from the previous step. However, the value of a step-level variable only affects the step after (and not the current step). They have the following format:  
{macro} = value  
{macro} = regex:<regular expression>  
For more information see variable description on the scenario level. Having step-level variables is supported since Zabbix 2.2. Variables are automatically URL-encoded when used in query fields or form data for post variables, but must be URL-encoded manually when used in raw post or directly in URL. |
| Headers               | Custom HTTP headers that will be sent when performing a request. Specified as attribute and value pairs. Headers on the step level will overwrite the headers specified for the scenario. For example, setting a 'User-Agent' attribute with no value will remove the User-Agent value set on scenario level. User macros and `{HOST.*}` macros are supported. This sets the CURLOPT_HTTPHEADER cURL option. Specifying custom headers is supported starting with Zabbix 2.4. |
| Follow redirects      | Mark the checkbox to follow HTTP redirects. This sets the CURLOPT_FOLLOWLOCATION cURL option. This option is supported starting with Zabbix 2.4. |
| Retrieve only headers | Mark the checkbox to retrieve only headers from the HTTP response. This sets the CURLOPT_NOBODY cURL option. This option is supported starting with Zabbix 2.4. |
| Timeout               | Zabbix will not spend more than the set amount of time on processing the URL (from one second to maximum of 1 hour). Actually this parameter defines the maximum time for making connection to the URL and maximum time for performing an HTTP request. Therefore, Zabbix will not spend more than 2 x Timeout seconds on the step. Time suffixes are supported, e.g. 30s, 1m, 1h. User macros are supported. |
**Parameter** | **Description**
---|---
Required string | Required regular expression pattern. Unless retrieved content (HTML) matches the required pattern the step will fail. If empty, no check on required string is performed. For example:
Homepage of Zabbix
Welcome.*admin
Note: Referencing regular expressions created in the Zabbix frontend is not supported in this field.
User macros and \{HOST.*\} macros are supported, since Zabbix 2.2.

Required status codes | List of expected HTTP status codes. If Zabbix gets a code which is not in the list, the step will fail. If empty, no check on status codes is performed. For example: 200,201,210-299 User macros are supported since Zabbix 2.2.

---

**Note:**
Any changes in web scenario steps will only be saved when the whole scenario is saved.

See also a [real-life example](#) of how web monitoring steps can be configured.

**Configuring authentication** The Authentication tab allows you to configure scenario authentication options.

![Authentication tab](image)

**Authentication parameters:**

| Parameter | Description |
---|---|
Authentication | Authentication options. **None** - no authentication used. **Basic authentication** - basic authentication is used. **NTLM authentication** - NTLM (Windows NT LAN Manager) authentication is used. Selecting an authentication method will provide two additional fields for entering a user name and password. User macros can be used in user and password fields, starting with Zabbix 2.2. |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL verify peer</td>
<td>Mark the checkbox to verify the SSL certificate of the web server. The server certificate will be automatically taken from system-wide certificate authority (CA) location. You can override the location of CA files using Zabbix server or proxy configuration parameter <strong>SSLCALocation</strong>. This sets the CURLOPT_SSL_VERIFYPEER cURL option. This option is supported starting with Zabbix 2.4.</td>
</tr>
<tr>
<td>SSL verify host</td>
<td>Mark the checkbox to verify that the Common Name field or the Subject Alternate Name field of the web server certificate matches. This sets the CURLOPT_SSL_VERIFYHOST cURL option. This option is supported starting with Zabbix 2.4.</td>
</tr>
<tr>
<td>SSL certificate file</td>
<td>Name of the SSL certificate file used for client authentication. The certificate file must be in PEM(^1) format. If the certificate file contains also the private key, leave the SSL key field field empty. If the key is encrypted, specify the password in SSL key password field. The directory containing this file is specified by Zabbix server or proxy configuration parameter <strong>SSLCertLocation</strong>. HOST.* macros and user macros can be used in this field. This sets the CURLOPT_SSLCERT cURL option. This option is supported starting with Zabbix 2.4.</td>
</tr>
<tr>
<td>SSL key file</td>
<td>Name of the SSL private key file used for client authentication. The private key file must be in PEM(^1) format. The directory containing this file is specified by Zabbix server or proxy configuration parameter <strong>SSLKeyLocation</strong>. HOST.* macros and user macros can be used in this field. This sets the CURLOPT_SSLKEY cURL option. This option is supported starting with Zabbix 2.4.</td>
</tr>
<tr>
<td>SSL key password</td>
<td>SSL private key file password. User macros can be used in this field. This sets the CURLOPT_KEYPASSWD cURL option. This option is supported starting with Zabbix 2.4.</td>
</tr>
</tbody>
</table>

**Attention:**

[1] Zabbix supports certificate and private key files in PEM format only. In case you have your certificate and private key data in PKCS #12 format file (usually with extension *.p12 or *.pfx) you may generate the PEM file from it using the following commands:

```
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:**

Zabbix server picks up changes in certificates without a restart.

**Note:**

If you have client certificate and private key in a single file just specify it in a "SSL certificate file" field and leave “SSL key file” field empty. The certificate and key must still be in PEM format. Combining certificate and key is easy:

```
cat client.crt client.key > client.pem
```

**Display** To view detailed data of defined web scenarios, go to Monitoring → Web or Latest data. Click on the scenario name to see more detailed statistics.
An overview of web monitoring scenarios can be viewed in Monitoring → Dashboard.

**Extended monitoring** Sometimes it is necessary to log received HTML page content. This is especially useful if some web scenario step fails. Debug level 5 (trace) serves that purpose. This level can be set in server and proxy configuration files or using a runtime control option (`-R log_level_increase="http poller,N"`, where N is the process number). The following examples demonstrate how extended monitoring can be started provided debug level 4 is already set:

- **Increase log level of all http pollers:**
  ```shell```
  shell> zabbix_server -R log_level_increase="http poller"
  ```

- **Increase log level of second http poller:**
  ```shell```
  shell> zabbix_server -R log_level_increase="http poller,2"
  ```

If extended web monitoring is not required it can be stopped using the `-R log_level_decrease` option.

**1 Web monitoring items**

**Overview**

Some new items are automatically added for monitoring when web scenarios are created.

**Scenario items**
As soon as a scenario is created, Zabbix automatically adds the following items for monitoring, linking them to the selected application.

<table>
<thead>
<tr>
<th>Item Description</th>
<th>Item Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Download speed for scenario</td>
<td>{host:web.test.in[Scenario,,bps].last()}</td>
</tr>
<tr>
<td>Item will collect information about the download speed (bytes per second) of the</td>
<td></td>
</tr>
<tr>
<td>whole scenario, i.e. average for all steps.</td>
<td></td>
</tr>
<tr>
<td>Item key: web.test.in[Scenario,,bps]</td>
<td></td>
</tr>
<tr>
<td>Type: Numeric(float)</td>
<td></td>
</tr>
<tr>
<td>Failed step of scenario</td>
<td>{host:web.test.fail[Scenario].last()}</td>
</tr>
<tr>
<td>This item will display the number of the step that failed on the scenario.</td>
<td></td>
</tr>
<tr>
<td>If all steps are executed successfully, 0 is returned.</td>
<td></td>
</tr>
<tr>
<td>Item key: web.test.fail[Scenario]</td>
<td></td>
</tr>
<tr>
<td>Type: Numeric(unsigned)</td>
<td></td>
</tr>
<tr>
<td>Last error message of scenario</td>
<td>{host:web.test.error[Scenario].last()}</td>
</tr>
<tr>
<td>This item returns the last error message text of the scenario.</td>
<td></td>
</tr>
<tr>
<td>A new value is stored only if the scenario has a failed step.</td>
<td></td>
</tr>
<tr>
<td>If all steps are ok, no new value is collected.</td>
<td></td>
</tr>
<tr>
<td>Item key: web.test.error[Scenario]</td>
<td></td>
</tr>
<tr>
<td>Type: Character</td>
<td></td>
</tr>
</tbody>
</table>

The actual scenario name will be used instead of “Scenario”.

**Note:**

Web monitoring items are added with a 30 day history and a 90 day trend retention period.

**Note:**

If scenario name starts with a doublequote or contains comma or square bracket, it will be properly quoted in item keys. In other cases no additional quoting will be performed.

These items can be used to create triggers and define notification conditions.

**Example 1**

To create a “Web scenario failed” trigger, you can define a trigger expression:

```
{host:web.test.fail[Scenario].last()}<>0
```

Make sure to replace ‘Scenario’ with the real name of your scenario.

**Example 2**

To create a “Web scenario failed” trigger with a useful problem description in the trigger name, you can define a trigger with name:

```
Web scenario "Scenario" failed: {ITEM.VALUE}
```

and trigger expression:

```
{host:web.test.error[Scenario].strlen()}>0 and {host:web.test.fail[Scenario].last()}>0
```

Make sure to replace ‘Scenario’ with the real name of your scenario.

**Example 3**

To create a “Web application is slow” trigger, you can define a trigger expression:

```
{host:web.test.in[Scenario,,bps].last()}<10000
```

Make sure to replace ‘Scenario’ with the real name of your scenario.

**Scenario step items**

As soon as a step is created, Zabbix automatically adds the following items for monitoring, linking them to the selected application.

<table>
<thead>
<tr>
<th>Item Description</th>
<th>Item Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Download speed for step &lt;Step&gt; of scenario &lt;Scenario&gt;</td>
<td>{host:web.test.in[Scenario,Step,bps].last()}</td>
</tr>
<tr>
<td>This item will collect information about the download speed (bytes per second) of</td>
<td></td>
</tr>
<tr>
<td>the step.</td>
<td></td>
</tr>
<tr>
<td>Item key: web.test.in[Scenario,Step,bps]</td>
<td></td>
</tr>
<tr>
<td>Type: Numeric(float)</td>
<td></td>
</tr>
<tr>
<td>Item Description</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Response time for step <Step> of scenario <Scenario> | This item will collect information about the response time of the step in seconds. Response time is counted from the beginning of the request until all information has been transferred.  
Item key: `web.test.time[Scenario,Step,resp]`  
Type: Numeric(float) |
| Response code for step <Step> of scenario <Scenario> | This item will collect response codes of the step.  
Item key: `web.test.rspcode[Scenario,Step]`  
Type: Numeric(unsigned) |

Actual scenario and step names will be used instead of "Scenario" and "Step" respectively.

**Note:**
Web monitoring items are added with a 30 day history and a 90 day trend retention period.

**Note:**
If scenario name starts with a doublequote or contains comma or square bracket, it will be properly quoted in item keys. In other cases no additional quoting will be performed.

These items can be used to create triggers and define notification conditions. For example, to create a “Zabbix GUI login is too slow” trigger, you can define a trigger expression:

```
{zabbix:web.test.time[ZABBIX GUI,Login,resp].last()}>3
```

### 2 Real life scenario

**Overview**

This section presents a step-by-step real-life example of how web monitoring can be used.

Let’s use Zabbix web monitoring to monitor the web interface of Zabbix. We want to know if it is available, provides the right content and how quickly it works. To do that we also must log in with our user name and password.

**Scenario**

**Step 1**

Add a new web scenario.

We will add a scenario to monitor the web interface of Zabbix. The scenario will execute a number of steps.

Go to Configuration → Hosts, pick a host and click on Web in the row of that host. Then click on Create web scenario.
All mandatory input fields are marked with a red asterisk.

In the new scenario form we will name the scenario as Zabbix frontend and create a new Zabbix frontend application for it.

Note that we will also create two variables: {user} and {password}.

Step 2
Define steps for the scenario.

Click on Add button in the Steps tab to add individual steps.

Web scenario step 1
We start by checking that the first page responds correctly, returns with HTTP response code 200 and contains text "Zabbix SIA".
When done configuring the step, click on Add.

Web scenario step 2

We continue by logging into the Zabbix frontend, and we do so by reusing the macros (variables) we defined on the scenario level - \{user\} and \{password\}.
Attention:
Note that Zabbix frontend uses JavaScript redirect when logging in, thus first we must log in, and only in further steps we may check for logged-in features. Additionally, the login step must use full URL to index.php file.

Take note also of how we are getting the content of the {sid} variable (session ID) using a variable syntax with regular expression: regex:name="csrf-token" content="([0-9a-z]{16})". This variable will be required in step 4.

Web scenario step 3
Being logged in, we should now verify the fact. To do so, we check for a string that is only visible when logged in - for example, Administration.
Web scenario step 4

Now that we have verified that frontend is accessible and we can log in and retrieve logged-in content, we should also log out - otherwise Zabbix database will become polluted with lots and lots of open session records.
Web scenario step 5

We can also check that we have logged out by looking for the **Username** string.
Complete configuration of steps

A complete configuration of web scenario steps should look like this:

Step 3

Save the finished web monitoring scenario.

The scenario will appear in Monitoring → Web:
10. Virtual machine monitoring

Overview  Support of monitoring VMware environments is available in Zabbix starting with version 2.2.0.

Zabbix can use low-level discovery rules to automatically discover VMware hypervisors and virtual machines and create hosts to monitor them, based on pre-defined host prototypes.

The default dataset in Zabbix offers several ready-to-use templates for monitoring VMware vCenter or ESX hypervisor.

The minimum required VMware vCenter or vSphere version is 4.1.
Details  The virtual machine monitoring is done in two steps. First, virtual machine data is gathered by vmware collector Zabbix processes. Those processes obtain necessary information from VMware web services over the SOAP protocol, pre-process it and store into Zabbix server shared memory. Then, this data is retrieved by pollers using Zabbix simple check VMware keys.

Starting with Zabbix version 2.4.4 the collected data is divided into 2 types: VMware configuration data and VMware performance counter data. Both types are collected independently by vmware collectors. Because of this it is recommended to enable more collectors than the monitored VMware services. Otherwise retrieval of VMware performance counter statistics might be delayed by the retrieval of VMware configuration data (which takes a while for large installations).

Currently only datastore, network interface and disk device statistics and custom performance counter items are based on the VMware performance counter information.

Configuration  For virtual machine monitoring to work, Zabbix should be compiled with the --with-libxml2 and --with-libcurl compilation options.

The following configuration file options can be used to tune the Virtual machine monitoring:

- **StartVMwareCollectors** - the number of pre-forked vmware collector instances. This value depends on the number of VMware services you are going to monitor. For the most cases this should be: servicenum < StartVMwareCollectors < (servicenum * 2)
  where servicenum is the number of VMware services. E.g. if you have 1 VMware service to monitor set StartVMwareCollectors to 2, if you have 3 VMware services, set it to 5. Note that in most cases this value should not be less than 2 and should not be 2 times greater than the number of VMware services that you monitor. Also keep in mind that this value also depends on your VMware environment size and VMwareFrequency and VMwarePerfFrequency configuration parameters (see below).

- **VMwareCacheSize**
- **VMwareFrequency**
- **VMwarePerfFrequency**
- **VMwareTimeout**

For more details, see the configuration file pages for Zabbix server and proxy.

Attention: To support datastore capacity metrics Zabbix requires VMware configuration vpxd.stats.maxQueryMetrics parameter to be at least 64. See also the VMware knowledge base article.

Discovery  Zabbix can use a low-level discovery rule to automatically discover VMware hypervisors and virtual machines.
All mandatory input fields are marked with a red asterisk.

Discovery rule key in the above screenshot is `vmware.hv.discovery[{$URL}]`.

**Host prototypes** Host prototypes can be created with the low-level discovery rule. When virtual machines are discovered, these prototypes become real hosts. Prototypes, before becoming discovered, cannot have their own items and triggers, other than those from the linked templates. Discovered hosts will belong to an existing host and will take the IP of the existing host for the host configuration.
In a host prototype configuration, LLD macros are used for the host name, visible name and host group prototype fields. Linkage to existing host groups, template linkage and encryption are other options that can be set.

If Create enabled is checked, the host will be added in an enabled state. If unchecked, the host will be added, but in disabled state.

Discovered hosts are prefixed with the name of the discovery rule that created them, in the host list. Discovered hosts can be manually deleted. Discovered hosts will also be automatically deleted, based on the Keep lost resources period (in days) value of the discovery rule. Most of the configuration options are read-only, except for enabling/disabling the host and host inventory. Discovered hosts cannot have host prototypes of their own.

**Ready-to-use templates** The default dataset in Zabbix offers several ready-to-use templates for monitoring VMware vCenter or directly ESX hypervisor.

These templates contain pre-configured LLD rules as well as a number of built-in checks for monitoring virtual installations.

Note that “Template VM VMware” template should be used for VMware vCenter and ESX hypervisor monitoring. The “Template VM VMware Hypervisor” and “Template VM VMware Guest” templates are used by discovery and normally should not be manually linked to a host.
Note:
If your server has been upgraded from a pre-2.2 version and has no such templates, you can import them manually, downloading from the community page with official templates. However, these templates have dependencies from the VMware VirtualMachinePowerState and VMware status value maps, so it is necessary to create these value maps first (using an SQL script, manually or importing from an XML) before importing the templates.

Host configuration To use VMware simple checks the host must have the following user macros defined:

- $VMWARE.URL - VMware service (vCenter or ESX hypervisor) SDK URL (https://servername/sdk)
- $VMWARE.USERNAME - VMware service user name
- $VMWARE.PASSWORD - VMware service ($VMWARE.USERNAME) user password

Example The following example demonstrates how to quickly setup VMware monitoring on Zabbix:
- compile zabbix server with required options (--with-libxml2 and --with-libcurl)
- set the StartVMwareCollectors option in Zabbix server configuration file to 1 or more
- create a new host
- set the host macros required for VMware authentication:

```
<table>
<thead>
<tr>
<th>MACRO</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>$VMWARE.PASSWORD</td>
<td>&lt;password&gt;</td>
</tr>
<tr>
<td>$VMWARE.URL</td>
<td>&lt;url&gt;</td>
</tr>
<tr>
<td>$VMWARE.USERNAME</td>
<td>&lt;username&gt;</td>
</tr>
</tbody>
</table>
```

- link the host to the VMware service template:
Extended logging  The data gathered by VMware collector can be logged for detailed debugging using debug level 5. This level can be set in server and proxy configuration files or using a runtime control option (-R log_level_increase="vmware collector,N", where N is a process number). The following examples demonstrate how extended logging can be started provided debug level 4 is already set:

Increase log level of all vmware collectors:
shell> zabbix_server -R log_level_increase="vmware collector"

Increase log level of second vmware collector:
shell> zabbix_server -R log_level_increase="vmware collector,2"

If extended logging of VMware collector data is not required it can be stopped using the -R log_level_decrease option.

Troubleshooting

• In case of unavailable metrics, please make sure if they are not made unavailable or turned off by default in recent VMware vSphere versions or if some limits are not placed on performance-metric database queries. See ZBX-12094 for additional details.

• To fix the 'config.vpxd.stats.maxQueryMetrics' is invalid or exceeds the maximum number of characters permitted** error, check value of the maxQuerySize parameter in VMware’s web.xml, then go to the advanced vCenter Server settings and add a config.vpxd.stats.maxQueryMetrics parameter with the same value. See this VMware knowledge base article for details.

1 Virtual machine discovery key fields

The following table lists fields returned by virtual machine related discovery keys.

<table>
<thead>
<tr>
<th>Item key</th>
<th>Field</th>
<th>Retrieved content</th>
</tr>
</thead>
<tbody>
<tr>
<td>vmware.cluster.discovery</td>
<td>{#CLUSTER.ID}</td>
<td>Cluster identifier.</td>
</tr>
<tr>
<td></td>
<td>{#CLUSTER.NAME}</td>
<td>Cluster name.</td>
</tr>
</tbody>
</table>
vmware.datastore.discovery
Performs datastore discovery.

vmware.dc.discovery
Performs datacenter discovery (since Zabbix 4.0.23).

vmware.hv.discovery
Performs hypervisor discovery.
Item key

{#PARENT.TYPE} of container in which the hypervisor is stored. The values could be Datacenter, Folder, ClusterComputeResource, VMware, where ‘VMware’ stands for unknown container type. Supported since Zabbix 4.0.3.

vmware.hv.datastore.discovery
Performs hypervisor datastore discovery. Note that multiple hypervisors can use the same datastore.

vmware.vm.discovery
Performs virtual machine discovery.

vmware.vm.net.if.discovery
Performs virtual machine network interface discovery.

vmware.vm.vfs.dev.discovery
### 11. Maintenance

**Overview**  You can define maintenance periods for host groups, hosts and specific triggers/services in Zabbix.

There are two maintenance types - with data collection and with no data collection.

During a maintenance "with data collection" triggers are processed as usual and events are created when required. However, problem escalations are paused for hosts/triggers in maintenance, if the Pause operations for suppressed problems option is checked in action configuration. In this case, escalation steps that may include sending notifications or remote commands will be ignored for as long as the maintenance period lasts. Note that problem recovery and update operations are not suppressed during maintenance, only escalations.

For example, if escalation steps are scheduled at 0, 30 and 60 minutes after a problem start, and there is a half-hour long maintenance lasting from 10 minutes to 40 minutes after a real problem arises, steps two and three will be executed a half-hour later, or at 60 minutes and 90 minutes (providing the problem still exists). Similarly, if a problem arises during the maintenance, the escalation will start after the maintenance.

To receive problem notifications during the maintenance normally (without delay), you have to uncheck the Pause operations for suppressed problems option in action configuration.

**Note:**  If at least one host (used in the trigger expression) is not in maintenance mode, Zabbix will send a problem notification.

Zabbix server must be running during maintenance. Timer processes are responsible for switching host status to/from maintenance at 0 seconds of every minute. Note that when a host enters maintenance, Zabbix server timer processes will read all open problems to check if it is required to suppress those. This may have a performance impact if there are many open problems. Zabbix server will also read all open problems upon startup, even if there are no maintenances configured at the time.

A proxy will always collect data regardless of the maintenance type (including "no data" maintenance). The data is later ignored by the server if ‘no data collection’ is set.

When "no data" maintenance ends, triggers using nodata() function will not fire before the next check during the period they are checking.

If a log item is added while a host is in maintenance and the maintenance ends, only new logfile entries since the end of the maintenance will be gathered.

If a timestamped value is sent for a host that is in a "no data" maintenance type (e.g. using Zabbix sender) then this value will be dropped however it is possible to send a timestamped value in for an expired maintenance period and it will be accepted.

**Attention:**  To ensure predictable behavior of recurring maintenance periods (daily, weekly, monthly), it is required to use a common time zone for all parts of Zabbix.

If maintenance period, hosts, groups or tags are changed by user, the changes will only take effect after configuration cache synchronization.

**Configuration**  To configure a maintenance period:

- Go to: Configuration → Maintenance
- Click on Create maintenance period (or on the name of an existing maintenance period)
The Maintenance tab contains general maintenance period attributes:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the maintenance period.</td>
</tr>
</tbody>
</table>
| Maintenance type| Two types of maintenance can be set: **With data collection** - data will be collected by the server during maintenance, triggers will be processed  
**No data collection** - data will not be collected by the server during maintenance |
| Active since    | The date and time when executing maintenance periods becomes active.  
*Note: Setting this time alone does not activate a maintenance period; for that go to the Periods tab.* |
| Active till     | The date and time when executing maintenance periods stops being active. |
| Description     | Description of maintenance period. |

All mandatory input fields are marked with a red asterisk.

The Periods tab allows you to define the exact days and hours when the maintenance takes place. Clicking on New opens a flexible Maintenance period form where you can define the times - for daily, weekly, monthly or one-time maintenance.
Notes:

- Daily and weekly periods have an Every day/Every week parameter, which defaults to ‘1’. Setting it to ‘2’ would make the maintenance take place every two days or every two weeks and so on. In this case the starting day or week is the day/week that the Active since time falls on. For example:
  - with Active since set to January 1st at 12:00 and a one-hour maintenance set for every two days at 11pm will result in the first maintenance period starting on January 1st at 11pm, while the second maintenance period will start on January 3rd at 11pm;
  - with the same Active since time and a one-hour maintenance set for every two days at 1am, the first maintenance period will start on January 3rd at 1am, while the second maintenance period will start on January 5th at 1am.
- Since Zabbix 4.0.20, Daylight Saving Time (DST) changes do not affect how long the maintenance will be. Let’s say we have a two-hour maintenance that usually starts at 1am and finishes at 3am:
  - If after one hour of maintenance (at 2am) a DST change happens and current time changes from 2:00 to 3:00, the maintenance will continue for one more hour till 4:00;
  - If after two hours of maintenance (at 3am) a DST change happens and current time changes from 3:00 to 2:00, the maintenance will stop because two hours have passed.

The **Hosts and groups** tab allows you to select the host groups, hosts and problem tags for maintenance.
Parameter Description

Host groups
Select host groups that the maintenance will be activated for. The maintenance will be activated for all hosts from the specified host group(s). This field is auto-complete, so starting to type in it will display a dropdown of all available host groups. Specifying a parent host group implicitly selects all nested host groups. Thus the maintenance will also be activated on hosts from nested groups.

Hosts
Select hosts that the maintenance will be activated for. This field is auto-complete, so starting to type in it will display a dropdown of all available hosts.

Tags
If maintenance tags are specified, maintenance for the selected hosts will still be activated, but problems will only be suppressed (i.e. no actions will be taken) if their tags are a match. In case of multiple tags, they are calculated as follows:
- **And/Or** - all tags must correspond; however tags with the same tag name are calculated by the Or condition
- **Or** - enough if one tag corresponds

There are two ways of matching the tag value:
- **Contains** - case-sensitive substring match (tag value contains the entered string)
- **Equals** - case-sensitive string match (tag value equals the entered string)

**Display** Displaying hosts in maintenance

An orange wrench icon next to the host name indicates that this host is in maintenance in:
- Monitoring → Dashboard
- Monitoring → Problems
- Inventory → Hosts → Host inventory details
- Configuration → Hosts (See ‘Status’ column. Note that before 4.0.9, an orange In maintenance string was displayed as status instead of the icon.)
Maintenance details are displayed when the mouse pointer is positioned over the icon.

Additionally, hosts in maintenance get an orange background in Monitoring → Maps.

Displaying suppressed problems

Normally problems for hosts in maintenance are suppressed, i.e. not displayed in the frontend. However, it is also possible to configure that suppressed problems are shown, by selecting the Show suppressed problems option in these locations:

- Monitoring → Dashboard (in Problem hosts, Problems, Problems by severity, Trigger overview widget configuration)
- Monitoring → Problems (in the filter)
- Monitoring → Overview (in the filter; with 'Triggers' as Type)
- Monitoring → Maps (in map configuration)
- Global notifications (in user profile configuration)

When suppressed problems are displayed, the following icon is displayed: 🚫. Rolling a mouse over the icon displays more details:

12. Regular expressions

Overview  Perl Compatible Regular Expressions (PCRE) are supported in Zabbix.

There are two ways of using regular expressions in Zabbix:

- manually entering a regular expression
- using a global regular expression created in Zabbix

Regular expressions  You may manually enter a regular expression in supported places. Note that the expression may not start with @ because that symbol is used in Zabbix for referencing global regular expressions.

Warning:  It's possible to run out of stack when using regular expressions. See the pcrestack man page for more information.

Note that in multiline matching, the ^ and $ anchors match at the beginning/end of each line respectively, instead of the beginning/end of the entire string.

Global regular expressions  There is an advanced editor for creating and testing complex regular expressions in Zabbix frontend.

Once a regular expression has been created this way, it can be used in several places in the frontend by referring to its name, prefixed with @, for example, @mycustomregexp.

To create a global regular expression:

- Go to: Administration → General
- Select Regular expressions from the dropdown
- Click on New regular expression
The **Expressions** tab allows to set the regular expression name and add subexpressions.

![Expressions tab](image)

All mandatory input fields are marked with a red asterisk.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Set the regular expression name. Any Unicode characters are allowed.</td>
</tr>
<tr>
<td>Expressions</td>
<td>Click on Add in the Expressions block to add a new subexpression.</td>
</tr>
<tr>
<td>Expression type</td>
<td>Select expression type:</td>
</tr>
<tr>
<td></td>
<td><strong>Character string included</strong> - match the substring</td>
</tr>
<tr>
<td></td>
<td><strong>Any character string included</strong> - match any substring from a delimited list. The delimited list includes a comma (,), a dot (.) or a forward slash (/).</td>
</tr>
<tr>
<td></td>
<td><strong>Character string not included</strong> - match any string except the substring</td>
</tr>
<tr>
<td></td>
<td><strong>Result is TRUE</strong> - match the regular expression</td>
</tr>
<tr>
<td></td>
<td><strong>Result is FALSE</strong> - do not match the regular expression</td>
</tr>
<tr>
<td>Delimiter</td>
<td>A comma (,), a dot (.) or a forward slash (/) to separate text strings in a regular expression. This parameter is active only when &quot;Any character string included&quot; expression type is selected.</td>
</tr>
<tr>
<td>Case sensitive</td>
<td>A checkbox to specify whether a regular expression is sensitive to capitalization of letters.</td>
</tr>
</tbody>
</table>

Since Zabbix 2.4.0, a forward slash (/) in the expression is treated literally, rather than a delimiter. This way it is possible to save expressions containing a slash, whereas previously it would produce an error.

**Attention:**
A custom regular expression name in Zabbix may contain commas, spaces, etc. In those cases where that may lead to misinterpretation when referencing (for example, a comma in the parameter of an item key) the whole reference may be put in quotes like this: "@My custom regexp for purpose1, purpose2". Regular expression names must not be quoted in other locations (for example, in LLD rule properties).

**Example**  Use of the following regular expression in LLD to discover databases not taking into consideration a database with a specific name:

```
^TESTDATABASE$```

492
Chosen Expression type: "Result is FALSE". Doesn't match name, containing string "TESTDATABASE".

**Example with an inline regex modifier**  Use of the following regular expression including an inline modifier (?!i) to match the characters "error":

```
(?!i)error
```

Chosen Expression type: "Result is TRUE". Characters "error" are matched.

**Another example with an inline regex modifier**  Use of the following regular expression including multiple inline modifiers to match the characters after a specific line:

```
(?<=match (?!i)everything(?i) after this line)\n(?sx).## we add s modifier to allow . match newline characters
```

Chosen Expression type: "Result is TRUE". (?!i)everything(?-i) after this line

Combined result

TRUE
Chosen Expression type: "Result is TRUE". Characters after a specific line are matched.

**Attention:**

`g` modifier can’t be specified in line. The list of available modifiers can be found in pcresyntax man page. For more information about PCRE syntax please refer to PCRE HTML documentation.

**More complex example**  
A custom regular expression may consist of multiple subexpressions, and it can be tested in the Test tab by providing a test string.

<table>
<thead>
<tr>
<th>Expressions</th>
<th>Test</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test string</td>
<td>lo</td>
</tr>
<tr>
<td>Expression type</td>
<td>Expression</td>
</tr>
<tr>
<td>Result is FALSE</td>
<td>&quot;Software Loopback Interface&quot;</td>
</tr>
<tr>
<td>Result is FALSE</td>
<td>&quot;(In)?[Ll]oop[Bb]ack[0-9._]*&quot;</td>
</tr>
<tr>
<td>Result is FALSE</td>
<td>&quot;NULL[0-9.]*&quot;</td>
</tr>
<tr>
<td>Result is FALSE</td>
<td>&quot;Nu[0-9.]*&quot;</td>
</tr>
<tr>
<td>Combined result</td>
<td></td>
</tr>
</tbody>
</table>

Results show the status of each subexpression and total custom expression status.

Total custom expression status is defined as Combined result. If several sub expressions are defined Zabbix uses AND logical operator to calculate Combined result. It means that if at least one Result is False Combined result has also False status.

**Explanation of global regular expressions**

<table>
<thead>
<tr>
<th>Global regexp</th>
<th>Expression</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File systems for discovery</td>
<td>^/(btrfs</td>
<td>ext2</td>
</tr>
<tr>
<td>Network interfaces for discovery</td>
<td>^Software Loopback Interface &quot;lo$</td>
<td>Matches strings with &quot;Software Loopback Interface&quot;</td>
</tr>
<tr>
<td></td>
<td>^((In)?[Ll]oop([Bb]\ack[0-9._.]*)+$</td>
<td>Matches strings that optionally start with &quot;In&quot;, then have &quot;L&quot; or &quot;l&quot;, then &quot;oop&quot;, then &quot;b&quot; or &quot;b&quot;, then &quot;ack&quot;, which can be optionally followed by any number of digits, dots or underscores</td>
</tr>
<tr>
<td></td>
<td>^&quot;NULL[0-9.]*&quot;</td>
<td>Matches strings staring with &quot;NULL&quot; optionally followed by any number of digits or dots</td>
</tr>
<tr>
<td></td>
<td>^&quot;[Ll]o[0-9.]*&quot;</td>
<td>Matches strings starting with &quot;Lo&quot; or &quot;lo&quot; and optionally followed by any number of digits or dots</td>
</tr>
<tr>
<td></td>
<td>^&quot;[Ss]\ystem&quot;</td>
<td>Matches &quot;System&quot; or &quot;system&quot;</td>
</tr>
<tr>
<td></td>
<td>^&quot;Nu[0-9.]*&quot;</td>
<td>Matches strings staring with &quot;Nu&quot; optionally followed by any number of digits or dots</td>
</tr>
<tr>
<td>Global regexp</td>
<td>Expression</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Storage devices for SNMP discovery</td>
<td><code>(Physical memory|Virtual memory|Memory buffers|Cached memory|Swap space)</code></td>
<td>Matches “Physical memory” or “Virtual memory” or “Memory buffers” or “Cached memory” or “Swap space”</td>
</tr>
<tr>
<td>Windows service names for discovery</td>
<td><code>(MMCSS|gupdate|SysmonLog)</code></td>
<td>Matches “MMCSS” or “gupdate” or “SysmonLog” or strings like “clr_optimization_v2.0.50727_32” and “clr_optimization_v4.0.30319_32” where instead of dots you can put any character except newline.</td>
</tr>
<tr>
<td>Windows service startup states for discovery</td>
<td><code>(automatic|automatic delayed)</code></td>
<td>Matches “automatic” or “automatic delayed”.</td>
</tr>
</tbody>
</table>

### Regular expression support by location

<table>
<thead>
<tr>
<th>Location</th>
<th>Regular expression</th>
<th>Global regular expression</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent items</td>
<td>eventlog[]</td>
<td>Yes</td>
<td>regexp, severity, source, eventid parameters</td>
</tr>
<tr>
<td></td>
<td>log[]</td>
<td></td>
<td>regexp parameter</td>
</tr>
<tr>
<td></td>
<td>log.count[]</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>logrt[]</td>
<td>Yes/No</td>
<td>regexp parameter supports both, file_regexp parameter supports non-global expressions only</td>
</tr>
<tr>
<td></td>
<td>logrt.count[]</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>proc.cpu.util[]</td>
<td>No</td>
<td>cmdline parameter</td>
</tr>
<tr>
<td></td>
<td>proc.mem[]</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>proc.num[]</td>
<td></td>
<td>device and sensor parameters on Linux 2.4 interface</td>
</tr>
<tr>
<td></td>
<td>sensor[]</td>
<td></td>
<td>package parameter</td>
</tr>
<tr>
<td></td>
<td>system.hw.macaddr[]</td>
<td></td>
<td>regex_incl, regex_excl parameters, since 4.0.4 also regex_excl_dir parameter</td>
</tr>
<tr>
<td></td>
<td>system.sw.packages[]</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>vfs.dir.count[]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location</td>
<td>Regular expression</td>
<td>Global regular expression</td>
<td>Comments</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------</td>
<td>------------------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>vfs.dir.size[]</td>
<td></td>
<td></td>
<td>regex_incl, regex_excl</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>parameters, since 4.0.4 also</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>regex_excl_dir parameter</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>regexp parameter</td>
</tr>
<tr>
<td>vfs.file.regexp[]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vfs.file.regmatch[]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>web.page.regexp[]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SNMP traps</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>snmptrap[]</td>
<td>Yes</td>
<td></td>
<td>regexp parameter</td>
</tr>
<tr>
<td><strong>Item value</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>preprocessing</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Trigger</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>functions</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>count[]</td>
<td>Yes</td>
<td></td>
<td>pattern parameter</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>parameter if operator is regex or iregexp</td>
</tr>
<tr>
<td>logeventid()</td>
<td></td>
<td></td>
<td>pattern parameter</td>
</tr>
<tr>
<td>logsoure()</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iregexp()</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Low-level</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>discovery</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>monitoring</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Filter field</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No</td>
<td>Variables with a regex: prefix</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Required string field</td>
</tr>
<tr>
<td><strong>Macro</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>functions</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>regsub()</td>
<td>No</td>
<td></td>
<td>pattern parameter</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iregsub()</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Icon</strong></td>
<td></td>
<td>Yes</td>
<td>Expression field</td>
</tr>
<tr>
<td><strong>mapping</strong></td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

13. Problem acknowledgment

**Overview**  Problem events in Zabbix can be acknowledged by users.

If a user gets notified about a problem event, they can go to Zabbix frontend, navigate from the problem list to the problem update screen and acknowledge the problem. When acknowledging, they can enter their comment for it, saying that they are working on it or whatever else they may feel like saying about it.

This way, if another system user spots the same problem, they immediately see if it has been acknowledged and the comments so far.

This way the workflow of resolving problems with more than one system user can take place in a more coordinated way.

Acknowledgment status is also used when defining action operations. You can define, for example, that a notification is sent to a higher level manager only if an event is not acknowledged for some time.
To acknowledge events and comment on them, a user must have at least read permissions to the corresponding triggers. To change problem severity or close problem, a user must have read-write permissions to the corresponding triggers.

There are several ways to access the problem update screen, which allows to acknowledge a problem.

- You may select problems in Monitoring → Problems and then click on Mass update below the list.
- You can click in the Ack column showing the acknowledgment status of problems in:
  - Monitoring → Dashboard (Problems and Problems by severity widgets)
  - Monitoring → Problems
  - Monitoring → Problems → Event details
  - Monitoring → Screens (Host group issues, Host issues, Problems by severity elements)

The Ack column contains either a 'Yes' or a 'No' link, indicating an acknowledged or an unacknowledged problem respectively. Clicking on the links will take you to the problem update screen.

- You can click on an unresolved problem cell in:
  - Monitoring → Dashboard (Trigger overview widget)
  - Monitoring → Overview
  - Monitoring → Screens (Trigger overview element)

The popup menu contains an Acknowledge option that will take you to the problem update screen.

**Updating problems** The problem update screen allows to:

- comment on the problem
- view comments and actions so far
- change problem severity
- acknowledge problem
- manually close problem

All mandatory input fields are marked with a red asterisk.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message</td>
<td>Enter text to comment on the problem (maximum 256 characters). Previous activities and comments on the problem are listed, along with the time and user details. For the meaning of icons used to denote user actions see the event detail page.</td>
</tr>
<tr>
<td>History</td>
<td>Define the scope of such actions as changing severity, acknowledging or manually closing problems: <strong>Only selected problem</strong> - will affect this event only <strong>Selected and all other problems of related triggers</strong> - in case of acknowledgment/closing problem, will affect this event and all other problems that are not acknowledged/closed so far. If the scope contains problems already acknowledged or closed, these problems will not be acknowledged/closed repeatedly. On the other hand, the number of message and severity change operations are not limited.</td>
</tr>
<tr>
<td>Change severity</td>
<td>Mark the checkbox and click on the severity button to update problem severity. Since Zabbix 4.0.12, the checkbox for changing severity is available if read-write permissions exist for at least one of the selected problems. Only those problems that are read-writable will be updated when clicking on Update. If read-write permissions exist for none of the selected triggers, the checkbox is disabled. Before Zabbix 4.0.12, changing severity in this way was possible if read-write permissions existed for each selected problem. If at least one problem was not read-writable, the checkbox was disabled.</td>
</tr>
<tr>
<td>Acknowledge</td>
<td>Mark the checkbox to acknowledge the problem. This option is disabled if all selected problems are already acknowledged. If at least one is unacknowledged, the option is available and in this case it will be possible to acknowledge only the unacknowledged problem(s). It is not possible to add another acknowledgment for an already acknowledged problem (it is possible to add another comment though).</td>
</tr>
<tr>
<td>Close problem</td>
<td>Mark the checkbox to manually close the problem. Since Zabbix 4.0.12, the checkbox for closing a problem is available if the Allow manual close option is checked in trigger configuration for at least one of the selected problems. Only those problems will be closed that are allowed to be closed when clicking on Update. If no problem is manually closeable, the checkbox is disabled. Already closed problems will not be closed repeatedly. Before Zabbix 4.0.12, closing a problem in this way was possible if the Allow manual close option was checked in trigger configuration for each selected problem. If at least one problem was not manually closeable, the checkbox was disabled.</td>
</tr>
</tbody>
</table>

**Display** Based on acknowledgment information it is possible to configure how the problem count is displayed in the dashboard or maps. To do that, you have to make selections in the Problem display option, available in both map configuration and the Problems by severity dashboard widget. It is possible to display all problem count, unacknowledged problem count as separated from the total or unacknowledged problem count only.

Based on problem update information (acknowledgment, etc.) it is possible to configure update operations - send message or execute remote commands.

**14. Configuration export/import**
Overview  Zabbix export/import functionality makes it possible to exchange various configuration entities between one Zabbix system and another.

Typical use cases for this functionality:

- share templates or network maps - Zabbix users may share their configuration parameters
- share web scenarios on share.zabbix.com - export a template with the web scenarios and upload to share.zabbix.com. Then others can download the template and import the XML into Zabbix.
- integrate with third-party tools - the universal XML format makes integration and data import/export possible with third party tools and applications

What can be exported/imported

Objects that can be exported/imported are:

- host groups (through Zabbix API only)
- templates
- hosts
- network maps
- images
- screens
- value maps

Export format

Data can be exported using the Zabbix web frontend or Zabbix API. Supported export formats are:

- XML - in the frontend
- XML or JSON - in Zabbix API

Details about export

- All supported elements are exported in one file.
- Host and template entities (items, triggers, graphs, discovery rules) that are inherited from linked templates are not exported. Any changes made to those entities on a host level (such as changed item interval, modified regular expression or added prototypes to the low-level discovery rule) will be lost when exporting; when importing, all entities from linked templates are re-created as on the original linked template.
- Entities created by low-level discovery and any entities depending on them are not exported. For example, a trigger created for an LLD-rule generated item will not be exported.

Details about import

- Import stops at the first error.
- When updating existing images during image import, "imagetype" field is ignored, i.e. it is impossible to change image type via import.
- When importing hosts/templates using the "Delete missing" option, host/template macros not present in the imported XML file will be deleted too.
- Empty tags for items, triggers, graphs, host/template applications, discoveryRules, itemPrototypes, triggerPrototypes, graphPrototypes are meaningless i.e. it's the same as if it was missing. Other tags, for example, item applications, are meaningful i.e. empty tag means no applications for item, missing tag means don't update applications.
- Import supports both XML and JSON, the import file must have a correct file extension: .xml for XML and .json for JSON.
- See compatibility information about supported XML versions.
1 Host groups

In the frontend host groups can be exported only with host or template export. When a host or template is exported all groups it belongs to are exported with it automatically.

API allows to export host groups independently from hosts or templates.

```xml
<groups>
  <group>
    <name>Zabbix servers</name>
  </group>
</groups>
```

### groups/group

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>string</td>
<td>Group name.</td>
<td></td>
</tr>
</tbody>
</table>

2 Templates

Overview

Templates are exported with many related objects and object relations.

Template export contains:

- linked host groups
- template data
- linkage to other templates
- linkage to host groups
- directly linked applications
- directly linked items
- directly linked triggers
- directly linked graphs
- directly linked screens
- directly linked discovery rules with all prototypes
- directly linked web scenarios
- value maps

Exporting

To export templates, do the following:

- Go to: Configuration → Templates
- Mark the checkboxes of the templates to export
- Click on Export below the list
Selected templates are exported to a local XML file with default name `zabbix_export_templates.xml`.

**Importing**

To import templates, do the following:

- Go to: Configuration → Templates
- Click on Import to the right
- Select the import file
- Mark the required options in import rules
- Click on Import
Note that before Zabbix 4.0.16, when a template is imported and updated, it can only be linked to additional templates and never be unlinked from any.

A success or failure message of the import will be displayed in the frontend.

Import rules:

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update existing</td>
<td>Existing elements will be updated with data taken from the import file. Otherwise they will not be updated.</td>
</tr>
<tr>
<td>Create new</td>
<td>The import will add new elements using data from the import file. Otherwise it will not add them.</td>
</tr>
<tr>
<td>Delete missing</td>
<td>The import will remove existing elements not present in the import file. Otherwise it will not remove them.</td>
</tr>
</tbody>
</table>

If Delete missing is marked for template linkage (only available since 4.0.16), existing template linkage not present in the import file will be removed from the template along with all entities inherited from the potentially unlinked templates (items, triggers, etc).

Export format

```xml
<?xml version="1.0" encoding="UTF-8"?>
<zabbix_export>
  <version>4.0</version>
</zabbix_export>
```
0 - MySQL server is down
1 - MySQL server is up

It requires user parameter mysql.ping, which is defined in userparameter_mysql.conf.
MySQL begin operations per second

It requires user parameter mysql.status[*], which is defined in userparameter_mysql.conf.
<step>
  <type>10</type>
  <params/>
</step>
</preprocessing>
<jmx_endpoint/>
<timeout>3s</timeout>
?url/>
<query_fields/>
<posts/>
<brace>status_codes</brace>200</brace>
<brace>follow_redirects</brace>1</brace>
<brace>post_type</brace>0</brace>
<brace>http_proxy/>
<brace>headers/>
<brace>retrieve_mode</brace>0</brace>
<brace>request_method</brace>1</brace>
<brace>output_format</brace>0</brace>
<brace>allow_traps</brace>0</brace>
<brace>ssl_cert_file/>
<brace>ssl_key_file/>
<brace>ssl_key_password/>
<brace>verify_peer</brace>0</brace>
<brace>verify_host</brace>0</brace>
<brace>master_item/>
</item>
<item>
  <name>MySQL queries per second</name>
  <type>0</type>
  <snmp_community/>
  <snmp_oid/>
  <key>mysql.status[Questions]</key>
  <delay>1m</delay>
  <history>1w</history>
  <trends>365d</trends>
  <status>0</status>
  <value_type>0</value_type>
  <allowed_hosts/>
  <units>qps</units>
  <snmpv3_contextname/>
  <snmpv3_securityname/>
  <snmpv3_securitylevel>0</snmpv3_securitylevel>
  <snmpv3_authprotocol>0</snmpv3_authprotocol>
  <snmpv3_authtype>0</snmpv3_authtype>
  <snmpv3_privprotocol>0</snmpv3_privprotocol>
  <snmpv3_privtype>0</snmpv3_privtype>
  <params/>
  <ipmi_sensor/>
  <authtype>0</authtype>
  <username/>
  <password/>
  <publickey/>
  <privatekey/>
  <port/>
  <description>It requires user parameter mysql.status[*], which is defined in userparameter_mysql.conf.</description>
  <inventory_link>0</inventory_link>
</application>
</applications>
<valuemap/>
<logtimefmt/>
<preprocessing>
  <step>
    <type>10</type>
    <params/>
  </step>
</preprocessing>
<jmx_endpoint/>
<timeout>3s</timeout>
<url/>
<query_fields/>
<posts/>
<status_codes>200</status_codes>
<follow_redirections>1</follow_redirections>
<post_type>0</post_type>
<html_proxy/>
<headers/>
<retrieve_mode>0</retrieve_mode>
<request_method>1</request_method>
<output_format>0</output_format>
<allow_traps>0</allow_traps>
<ssl_cert_file/>
<ssl_key_file/>
<ssl_key_password/>
<verify_peer>0</verify_peer>
<verify_host>0</verify_host>
<master_item/>
</item>
</items>
<discovery_rules/>
<httptests/>
<macros/>
<templates/>
<screens>
  <screen>
    <name>MySQL performance</name>
    <hsize>2</hsize>
    <vsize>1</vsize>
    <screen_items>
      <screen_item>
        <resourcetype>0</resourcetype>
        <width>500</width>
        <height>200</height>
        <x>0</x>
        <y>0</y>
        <colspan>1</colspan>
        <rowspan>1</rowspan>
        <elements>0</elements>
        <valign>1</valign>
        <halign>0</halign>
        <style>0</style>
        <url/>
        <dynamic>0</dynamic>
        <sort_triggers>0</sort_triggers>
        <resource>
          <name>MySQL operations</name>
          <host>Template DB MySQL</host>
        </resource>
      </screen_item>
    </screen_items>
  </screen>
</screens>
<screens>
  <template>
    <triggers>
      <trigger>
        <expression>{Template DB MySQL:mysql.ping.last(0)}=0</expression>
        <recovery_mode>0</recovery_mode>
        <name>MySQL is down</name>
        <correlation_mode>0</correlation_mode>
        <correlation_tag/>
        <status>0</status>
        <priority>2</priority>
        <description/>
        <type>0</type>
        <manual_close>0</manual_close>
        <dependencies/>
        <tags/>
      </trigger>
    </triggers>
  </template>
</screens>

<graphs>
  <graph>
    <name>MySQL operations</name>
    <width>900</width>
    <height>200</height>
    <yaxismin>0.0000</yaxismin>
    <yaxismax>100.0000</yaxismax>
    <show_work_period>1</show_work_period>
    <show_triggers>1</show_triggers>
    <type>0</type>
    <show_legend>1</show_legend>
    <show_3d>0</show_3d>
    <percent_left>0.0000</percent_left>
    <percent_right>0.0000</percent_right>
    <ymin_type_1>0</ymin_type_1>
    <ymax_type_1>0</ymax_type_1>
    <ymin_item_1>0</ymin_item_1>
    <ymax_item_1>0</ymax_item_1>
    <graph_items>
      <graph_item>
        <sortorder>0</sortorder>
        <drawtype>0</drawtype>
        <color>C8C800</color>
        <yaxisside>0</yaxisside>
        <calc_fnc>2</calc_fnc>
        <type>0</type>
        <item>
          <host>Template DB MySQL</host>
          <key>mysql.status[Com_begin]</key>
        </item>
      </graph_item>
    </graph_items>
  </graph>
</graphs>

<value_maps>
  <value_map>
    <name>Service state</name>
    <mapping>
      <value>0</value>
      <newvalue>Down</newvalue>
    </mapping>
  </value_map>
</value_maps>
Element tags

Element tag values are explained in the table below.

Template tags

<table>
<thead>
<tr>
<th>Element</th>
<th>Element property</th>
<th>Type</th>
<th>Range</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>templates</td>
<td>template</td>
<td>string</td>
<td></td>
<td>Root element for templates.</td>
</tr>
<tr>
<td></td>
<td>template name</td>
<td>string</td>
<td></td>
<td>Individual template.</td>
</tr>
<tr>
<td></td>
<td>template description</td>
<td>text</td>
<td></td>
<td>Unique template name.</td>
</tr>
<tr>
<td>groups</td>
<td>group name</td>
<td>string</td>
<td></td>
<td>Visible template name.</td>
</tr>
<tr>
<td></td>
<td>group name</td>
<td>string</td>
<td></td>
<td>Template description.</td>
</tr>
<tr>
<td>applications</td>
<td>application name</td>
<td></td>
<td></td>
<td>Root element for host groups.</td>
</tr>
<tr>
<td></td>
<td>application name</td>
<td></td>
<td></td>
<td>Individual host group.</td>
</tr>
<tr>
<td></td>
<td>name</td>
<td>string</td>
<td></td>
<td>Unique group name.</td>
</tr>
<tr>
<td>macros</td>
<td>macro name</td>
<td>string</td>
<td></td>
<td>Root element for template applications.</td>
</tr>
<tr>
<td></td>
<td>macro name</td>
<td>string</td>
<td></td>
<td>Individual template application.</td>
</tr>
<tr>
<td></td>
<td>name</td>
<td>string</td>
<td></td>
<td>Application name.</td>
</tr>
<tr>
<td></td>
<td>value</td>
<td>string</td>
<td></td>
<td>User macro name.</td>
</tr>
<tr>
<td>templates</td>
<td>template name</td>
<td>string</td>
<td></td>
<td>User macro value.</td>
</tr>
<tr>
<td></td>
<td>template name</td>
<td>string</td>
<td></td>
<td>Root element for linked templates.</td>
</tr>
<tr>
<td></td>
<td>template name</td>
<td>string</td>
<td></td>
<td>Individual template.</td>
</tr>
</tbody>
</table>

Template item tags

<table>
<thead>
<tr>
<th>Element</th>
<th>Element property</th>
<th>Type</th>
<th>Range</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>items</td>
<td>item</td>
<td>name</td>
<td>string</td>
<td>Root element for items.</td>
</tr>
<tr>
<td></td>
<td>item</td>
<td>name</td>
<td></td>
<td>Individual item.</td>
</tr>
<tr>
<td></td>
<td>name</td>
<td>string</td>
<td></td>
<td>Item name.</td>
</tr>
<tr>
<td>Element</td>
<td>Element property</td>
<td>Type</td>
<td>Range</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------</td>
<td>--------</td>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>type</td>
<td></td>
<td>integer</td>
<td>0-Zabbix agent</td>
<td>Item type.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - SNMPv1 agent</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 - Zabbix trapper</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 - simple check</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4 - SNMPv2 agent</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5 - internal</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6 - SNMPv3 agent</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7 - Zabbix agent (active)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>8 - aggregate</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>9 - HTTP test (web monitoring scenario step)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>10 - external</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>11 - database monitor</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>12 - IPMI agent</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>13 - SSH agent</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>14 - Telnet agent</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>15 - calculated</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>16 - JMX agent</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>17 - SNMP trap</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>18 - Dependent item</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>19 - HTTP agent item</td>
<td></td>
</tr>
</tbody>
</table>

<p>| snmp_community | string | SNMP community name if 'type' is 1,4. |
| snmp_oid      | string | SNMP object ID. |
| key           | string | Item key. |
| delay         | string | Update interval of the item. Seconds, time unit with suffix, custom intervals, user macros or LLD macro. |
| history       | string | A time unit of how long the history data should be stored. Time unit with suffix, user macro or LLD macro. |
| trends        | string | A time unit of how long the trends data should be stored. Time unit with suffix, user macro or LLD macro. |
| status        | integer | 0 - enabled, 1 - disabled | Item status. |</p>
<table>
<thead>
<tr>
<th>Element</th>
<th>Element property</th>
<th>Type</th>
<th>Range</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>value_type</td>
<td></td>
<td>integer</td>
<td>0 - float</td>
<td>Received value type.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - character</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 - log</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 - unsigned integer</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4 - text</td>
<td></td>
</tr>
<tr>
<td>allowed_hosts</td>
<td></td>
<td>string</td>
<td>List of IP addresses (comma delimited) of hosts allowed sending data for the item if 'type' is 2 or 19.</td>
<td></td>
</tr>
<tr>
<td>units</td>
<td></td>
<td>string</td>
<td>Units of returned values (bps, B).</td>
<td></td>
</tr>
<tr>
<td>snmpv3_contextname</td>
<td></td>
<td>string</td>
<td>SNMPv3 context name.</td>
<td></td>
</tr>
<tr>
<td>snmpv3_securityname</td>
<td></td>
<td>string</td>
<td>SNMPv3 security name.</td>
<td></td>
</tr>
<tr>
<td>snmpv3_securitylevel</td>
<td></td>
<td>integer</td>
<td>0 - noAuthNoPriv</td>
<td>SNMPv3 security level.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - authNoPriv</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 - authPriv</td>
<td></td>
</tr>
<tr>
<td>snmpv3_authprotocol</td>
<td></td>
<td>integer</td>
<td>0 - MD5</td>
<td>SNMPv3 authentication protocol.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - SHA</td>
<td></td>
</tr>
<tr>
<td>snmpv3_authpassphrase</td>
<td></td>
<td>string</td>
<td>SNMPv3 authentication passphrase.</td>
<td></td>
</tr>
<tr>
<td>snmpv3_privprotocol</td>
<td></td>
<td>integer</td>
<td>0 - DES</td>
<td>SNMPv3 privacy protocol.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - AES</td>
<td></td>
</tr>
<tr>
<td>snmpv3_privpassphrase</td>
<td></td>
<td>string</td>
<td>SNMPv3 privacy passphrase.</td>
<td></td>
</tr>
<tr>
<td>params</td>
<td></td>
<td>text</td>
<td>Name of the &quot;Executed script&quot; if 'type' is 13,14 &quot;SQL query&quot; field if 'type' is 11 &quot;Formula&quot; field if 'type' is 15.</td>
<td></td>
</tr>
<tr>
<td>ipmi_sensor</td>
<td></td>
<td>string</td>
<td>IPMI sensor ID if 'type' is 12.</td>
<td></td>
</tr>
<tr>
<td>authtype</td>
<td></td>
<td>integer</td>
<td>Authentication type for SSH agent items: 0 - password 1 - key</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Authentication type for HTTP agent items: 0 - none 1 - basic 2 - NTLM</td>
<td></td>
</tr>
<tr>
<td>username</td>
<td></td>
<td>string</td>
<td>User name if 'type' is 11,13,14,19.</td>
<td></td>
</tr>
<tr>
<td>password</td>
<td></td>
<td>string</td>
<td>Password if 'type' is 11,13,14,19.</td>
<td></td>
</tr>
<tr>
<td>publickey</td>
<td></td>
<td>string</td>
<td>Name of the public key file if 'type' is 13.</td>
<td></td>
</tr>
<tr>
<td>privatekey</td>
<td></td>
<td>string</td>
<td>Name of the private key file if 'type' is 13.</td>
<td></td>
</tr>
<tr>
<td>port</td>
<td></td>
<td>string</td>
<td>Custom port for the item.</td>
<td></td>
</tr>
<tr>
<td>description</td>
<td></td>
<td>text</td>
<td>Item description.</td>
<td></td>
</tr>
<tr>
<td>Element</td>
<td>Element property</td>
<td>Type</td>
<td>Range</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------</td>
<td>----------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>inventory_link</td>
<td>integer</td>
<td>0 - no link number - number of field in the 'host_inventory' table</td>
<td>Use item value to populate this inventory field.</td>
<td></td>
</tr>
<tr>
<td>logtimefmt</td>
<td>string</td>
<td></td>
<td></td>
<td>Format of the time in log entries. Used only by log items.</td>
</tr>
<tr>
<td>jmx_endpoint</td>
<td>string</td>
<td></td>
<td></td>
<td>JMX endpoint if 'type' is 16.</td>
</tr>
<tr>
<td>url</td>
<td>string</td>
<td>0 - Do not allow trapping. 1 - Allow trapping.</td>
<td>Property allows to send data to item if 'type' is 19.</td>
<td></td>
</tr>
<tr>
<td>allow_traps</td>
<td>integer</td>
<td>0 - Do not allow redirects. 1 - Follow redirects.</td>
<td>Follow HTTP redirects if 'type' is 19.</td>
<td></td>
</tr>
<tr>
<td>follow_redirects</td>
<td>integer</td>
<td>0 - Do not follow redirects. 1 - Follow redirects.</td>
<td>Object with HTTP(S) request headers if 'type' is 19.</td>
<td></td>
</tr>
<tr>
<td>headers</td>
<td>object</td>
<td></td>
<td></td>
<td>HTTP(S) proxy connection string if 'type' is 19.</td>
</tr>
<tr>
<td>http_proxy</td>
<td>string</td>
<td></td>
<td></td>
<td>HTTP(S) proxy connection string if 'type' is 19.</td>
</tr>
<tr>
<td>output_format</td>
<td>integer</td>
<td>0 - Store as is. 1 - Convert to JSON.</td>
<td>How to process response if 'type' is 19.</td>
<td></td>
</tr>
<tr>
<td>post_type</td>
<td>integer</td>
<td>0 - Raw data. 2 - JSON data. 3 - XML data.</td>
<td>Type of request body if 'type' is 19.</td>
<td></td>
</tr>
<tr>
<td>posts</td>
<td>text</td>
<td></td>
<td></td>
<td>Request body if 'type' is 19.</td>
</tr>
<tr>
<td>query_fields</td>
<td>array</td>
<td></td>
<td></td>
<td>Array of objects for request query fields if 'type' is 19.</td>
</tr>
<tr>
<td>request_method</td>
<td>integer</td>
<td>0 - GET 1 - POST 2 - PUT 3 - HEAD</td>
<td>Request method if 'type' is 19.</td>
<td></td>
</tr>
<tr>
<td>retrieve_mode</td>
<td>integer</td>
<td>0 - Body. 1 - Headers. 2 - Both body and headers will be stored.</td>
<td>What part of response should be stored if 'type' is 19.</td>
<td></td>
</tr>
<tr>
<td>ssl_cert_file</td>
<td>string</td>
<td></td>
<td></td>
<td>Public SSL Key file path if 'type' is 19.</td>
</tr>
<tr>
<td>ssl_key_file</td>
<td>string</td>
<td></td>
<td></td>
<td>Private SSL Key file path if 'type' is 19.</td>
</tr>
<tr>
<td>ssl_key_password</td>
<td>string</td>
<td></td>
<td></td>
<td>Password for SSL Key file if 'type' is 19.</td>
</tr>
<tr>
<td>status_codes</td>
<td>string</td>
<td></td>
<td></td>
<td>Ranges of required HTTP status codes separated by commas if 'type' is 19.</td>
</tr>
<tr>
<td>timeout</td>
<td>string</td>
<td></td>
<td></td>
<td>Item data polling request timeout if 'type' is 19.</td>
</tr>
<tr>
<td>Element</td>
<td>Element property</td>
<td>Type</td>
<td>Range</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------</td>
<td>--------</td>
<td>----------------</td>
<td>---------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>verify_host</td>
<td></td>
<td>integer</td>
<td>0 - Do not validate. 1 - Validate.</td>
<td>Validate host name in URL is in Common Name field or a Subject Alternate Name field of host certificate if 'type' is 19. Validate is host certificate authentic if 'type' is 19.</td>
</tr>
<tr>
<td>verify_peer</td>
<td></td>
<td>integer</td>
<td>0 - Do not validate. 1 - Validate.</td>
<td>Validate is host certificate authentic if 'type' is 19.</td>
</tr>
<tr>
<td>value map</td>
<td>name</td>
<td>string</td>
<td></td>
<td>Value map.</td>
</tr>
<tr>
<td>applications</td>
<td>name</td>
<td>string</td>
<td></td>
<td>Name of the value map to use for the item.</td>
</tr>
<tr>
<td>application</td>
<td>name</td>
<td>string</td>
<td></td>
<td>Root element for applications.</td>
</tr>
<tr>
<td>preprocessing</td>
<td>name</td>
<td>string</td>
<td></td>
<td>Individual application.</td>
</tr>
<tr>
<td>step</td>
<td>name</td>
<td>string</td>
<td></td>
<td>Individual item value preprocessing.</td>
</tr>
<tr>
<td>type</td>
<td></td>
<td>integer</td>
<td>1 - custom multiplier 2 - right trim 3 - left trim 4 - trim from both sides 5 - regular expression matching 6 - boolean to decimal 7 - octal to decimal 8 - hexadecimal to decimal 9 - simple change; calculated as (received value-previous value) 10 - change per second; calculated as (received value-previous value)/(time now-time of last check) 11 - XML Path 12 - JSONPath</td>
<td>Type of the item value preprocessing step.</td>
</tr>
<tr>
<td>params</td>
<td></td>
<td>string</td>
<td></td>
<td>Parameters of the item value preprocessing step.</td>
</tr>
<tr>
<td>master_item</td>
<td>key</td>
<td>string</td>
<td></td>
<td>Individual item master item data.</td>
</tr>
<tr>
<td>key</td>
<td></td>
<td>string</td>
<td></td>
<td>Dependent item master item key value.</td>
</tr>
</tbody>
</table>
## Template low-level discovery rule tags

<table>
<thead>
<tr>
<th>Element</th>
<th>Element property</th>
<th>Type</th>
<th>Range</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>discovery_rule</td>
<td></td>
<td></td>
<td></td>
<td>Individual low-level discovery rule.</td>
</tr>
</tbody>
</table>

*For most of the element tag values, see element tag values for a regular item. Only the tags that are specific to low-level discovery rules, are described below.*

**lifetime**
- **Type:** string
- **Range:**
- **Description:** Time period after which items that are no longer discovered will be deleted. Seconds, time unit with suffix or user macro.

**filter**
- **evaltype**
  - **Type:** integer
  - **Range:** 0 - And/or logic, 1 - And logic, 2 - Or logic, 3 - custom formula
  - **Description:** Logic to use for checking low-level discovery rule filter conditions.
- **formula**
  - **Type:** string
  - **Description:** Custom calculation formula for filter conditions.
- **conditions**
  - **Description:** Root element for filter conditions.

**condition**
- **macro**
  - **Type:** string
  - **Description:** Individual filter condition.
- **value**
  - **Type:** string
  - **Description:** Filter value: regular expression or global regular expression.
- **operator**
  - **Type:** integer
- **formulaid**
  - **Type:** character
  - **Description:** Filter condition ID. Used in the custom calculation formula.

**item_prototypes**
- **Description:** Root element for item_prototypes.

**item_prototype**
- **Description:** Individual item_prototype.

**application_prototypes**
- **Description:** Root element for application prototypes.

**application_prototype**
- **Description:** Individual application prototype.

**master_item**
- **name**
  - **Type:** string
  - **Description:** Application prototype name.
- **key**
  - **Type:** string
  - **Description:** Individual item prototype master item/item prototype data.
- **value**
  - **Description:** Dependent item prototype master item/item prototype key value.

## Template trigger tags

<table>
<thead>
<tr>
<th>Element</th>
<th>Element property</th>
<th>Type</th>
<th>Range</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>triggers</td>
<td></td>
<td></td>
<td></td>
<td>Root element for triggers.</td>
</tr>
<tr>
<td>Element</td>
<td>Element property</td>
<td>Type</td>
<td>Range</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------</td>
<td>---------</td>
<td>-----------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>trigger</td>
<td>expression</td>
<td>string</td>
<td></td>
<td>Trigger expression.</td>
</tr>
<tr>
<td></td>
<td>recovery_mode</td>
<td>integer</td>
<td>0 -</td>
<td>Basis for generating OK events.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>expression</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 -</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>recovery</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>expression</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 -</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>recovery_expression</td>
<td>string</td>
<td></td>
<td>Trigger recovery expression.</td>
</tr>
<tr>
<td></td>
<td>name</td>
<td>string</td>
<td></td>
<td>Trigger name.</td>
</tr>
<tr>
<td></td>
<td>correlation_mode</td>
<td>integer</td>
<td>0 -</td>
<td>Correlation mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>no event</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>correlation</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>by tag</td>
<td></td>
</tr>
<tr>
<td></td>
<td>correlation_tag</td>
<td>string</td>
<td></td>
<td>The tag name to be used for event correlation.</td>
</tr>
<tr>
<td></td>
<td>url</td>
<td>string</td>
<td>0 -</td>
<td>Trigger URL.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td></td>
<td>status</td>
<td>integer</td>
<td>0 -</td>
<td>Trigger status.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>disabled</td>
<td></td>
</tr>
<tr>
<td></td>
<td>priority</td>
<td>integer</td>
<td>0 -</td>
<td>Trigger severity.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>not</td>
<td>classified</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 -</td>
<td>information</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2 - warning</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3 - average</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4 - high</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5 - disaster</td>
</tr>
<tr>
<td></td>
<td>description</td>
<td>text</td>
<td></td>
<td>Trigger description.</td>
</tr>
<tr>
<td></td>
<td>type</td>
<td>integer</td>
<td>0 -</td>
<td>Event generation type.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>single</td>
<td>problem event</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 -</td>
<td>multiple problem events</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>not</td>
<td>allowed</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 -</td>
<td>allowed</td>
</tr>
<tr>
<td>dependencies</td>
<td></td>
<td></td>
<td></td>
<td>Root element for dependencies.</td>
</tr>
<tr>
<td>dependency</td>
<td>name</td>
<td>string</td>
<td></td>
<td>Individual dependency.</td>
</tr>
<tr>
<td></td>
<td>expression</td>
<td>string</td>
<td></td>
<td>Dependency trigger name.</td>
</tr>
<tr>
<td></td>
<td>recovery_expression</td>
<td>string</td>
<td></td>
<td>Dependency trigger expression.</td>
</tr>
<tr>
<td>tags</td>
<td>tag</td>
<td>string</td>
<td></td>
<td>Root element for event tags.</td>
</tr>
<tr>
<td></td>
<td>value</td>
<td>string</td>
<td></td>
<td>Individual event tag.</td>
</tr>
</tbody>
</table>

Template graph tags

<table>
<thead>
<tr>
<th>Element</th>
<th>Element property</th>
<th>Type</th>
<th>Range</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>graphs</td>
<td>graph</td>
<td></td>
<td></td>
<td>Root element for graphs.</td>
</tr>
<tr>
<td></td>
<td>name</td>
<td>string</td>
<td></td>
<td>Individual graph.</td>
</tr>
<tr>
<td></td>
<td>width</td>
<td>integer</td>
<td></td>
<td>Graph name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Graph width, in pixels. Used for preview and for pie/exploded graphs.</td>
</tr>
<tr>
<td>Element</td>
<td>Element property</td>
<td>Type</td>
<td>Range</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------</td>
<td>--------</td>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>height</td>
<td></td>
<td>integer</td>
<td></td>
<td>Graph height, in pixels. Used for preview and for pie/exploded graphs.</td>
</tr>
<tr>
<td>yaxismin</td>
<td></td>
<td>double</td>
<td></td>
<td>Value of Y axis minimum if 'ymin_type_1' is 1.</td>
</tr>
<tr>
<td>yaxismax</td>
<td></td>
<td>double</td>
<td></td>
<td>Value of Y axis maximum if 'ymax_type_1' is 1.</td>
</tr>
<tr>
<td>show_work_period</td>
<td></td>
<td>integer</td>
<td>0 - no</td>
<td>Highlight non-working hours if 'type' is 0, 1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - yes</td>
<td></td>
</tr>
<tr>
<td>show_triggers</td>
<td></td>
<td>integer</td>
<td>0 - no</td>
<td>Display simple trigger values as a line if 'type' is 0, 1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - yes</td>
<td></td>
</tr>
<tr>
<td>type</td>
<td></td>
<td>integer</td>
<td>0 - normal</td>
<td>Graph type.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - stacked</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 - pie</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 - exploded</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4 - 3D pie</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5 - 3D exploded</td>
<td></td>
</tr>
<tr>
<td>show_legend</td>
<td></td>
<td>integer</td>
<td>0 - no</td>
<td>Display graph legend.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - yes</td>
<td></td>
</tr>
<tr>
<td>show_3d</td>
<td></td>
<td>integer</td>
<td>0 - 2D</td>
<td>Enable 3D style if 'type' is 2, 3.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - 3D</td>
<td></td>
</tr>
<tr>
<td>percent_left</td>
<td></td>
<td>double</td>
<td></td>
<td>Show the percentile line for left axis if 'type' is 0.</td>
</tr>
<tr>
<td>percent_right</td>
<td></td>
<td>double</td>
<td></td>
<td>Show the percentile line for right axis if 'type' is 0.</td>
</tr>
<tr>
<td>ymin_type_1</td>
<td></td>
<td>integer</td>
<td>0 - calculated</td>
<td>Minimum value of Y axis if 'type' is 0, 1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - fixed</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 - last value of the selected item</td>
<td></td>
</tr>
<tr>
<td>ymax_type_1</td>
<td></td>
<td>integer</td>
<td>0 - calculated</td>
<td>Maximum value of Y axis if 'type' is 0, 1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - fixed</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 - last value of the selected item</td>
<td></td>
</tr>
<tr>
<td>ymin_item_1</td>
<td></td>
<td>string</td>
<td>null or item details</td>
<td>Item details if 'ymin_type_1' is 2.</td>
</tr>
<tr>
<td>ymax_item_1</td>
<td></td>
<td>string</td>
<td>null or item details</td>
<td>Item details if 'ymax_type_1' is 2.</td>
</tr>
<tr>
<td>graph_items</td>
<td></td>
<td></td>
<td></td>
<td>Root element for graph items.</td>
</tr>
<tr>
<td>graph_item</td>
<td></td>
<td></td>
<td></td>
<td>Individual graph item.</td>
</tr>
<tr>
<td>sortorder</td>
<td></td>
<td>integer</td>
<td></td>
<td>Draw order. The smaller value is drawn first. Can be used to draw lines or regions behind (or in front of) another.</td>
</tr>
<tr>
<td>drawtype</td>
<td></td>
<td>integer</td>
<td>0 - single line</td>
<td>Draw style if graph 'type' is 0.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - filled region</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 - bold line</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 - dotted line</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4 - dashed line</td>
<td></td>
</tr>
<tr>
<td>Element</td>
<td>Element property</td>
<td>Type</td>
<td>Range</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------</td>
<td>---------</td>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>color</td>
<td></td>
<td>string</td>
<td></td>
<td>Element color (6 symbols, hex).</td>
</tr>
<tr>
<td>yaxisside</td>
<td></td>
<td>integer</td>
<td>0 - left axis, 1 - right axis</td>
<td>Y axis position (left or right) the element belongs to if graph ‘type’ is 0,1.</td>
</tr>
<tr>
<td>calc_fnc</td>
<td></td>
<td>integer</td>
<td>1 - minimum, 2 - average, 4 - maximum, 7 - all (minimum, average and maximum, if graph ‘type’ is 0), 9 - last (if graph ‘type’ is not 0,1)</td>
<td>Data to draw if more than one value exists for an item.</td>
</tr>
<tr>
<td>type</td>
<td></td>
<td>integer</td>
<td>1 - value of the item is represented proportionally on the pie, 2 - value of the item represents the whole pie (graph sum)</td>
<td>Draw type for pie/exploded graphs.</td>
</tr>
<tr>
<td></td>
<td>item</td>
<td></td>
<td></td>
<td>Individual item.</td>
</tr>
<tr>
<td></td>
<td>host</td>
<td>string</td>
<td></td>
<td>Item host.</td>
</tr>
<tr>
<td></td>
<td>key</td>
<td>string</td>
<td></td>
<td>Item key.</td>
</tr>
</tbody>
</table>

**Template web scenario tags**

<table>
<thead>
<tr>
<th>Element</th>
<th>Element property</th>
<th>Type</th>
<th>Range</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>httptests</td>
<td></td>
<td></td>
<td></td>
<td>Root element for web scenarios.</td>
</tr>
<tr>
<td>httptest</td>
<td></td>
<td></td>
<td></td>
<td>Individual web scenario.</td>
</tr>
<tr>
<td></td>
<td>name</td>
<td>string</td>
<td></td>
<td>Web scenario name.</td>
</tr>
<tr>
<td></td>
<td>delay</td>
<td>string</td>
<td></td>
<td>Frequency of executing the web scenario. Seconds, time unit with suffix or user macro.</td>
</tr>
<tr>
<td>attempts</td>
<td>integer</td>
<td></td>
<td>1-10</td>
<td>The number of attempts for executing web scenario steps.</td>
</tr>
<tr>
<td>agent</td>
<td>string</td>
<td></td>
<td></td>
<td>Client agent. Zabbix will pretend to be the selected browser. This is useful when a website returns different content for different browsers.</td>
</tr>
<tr>
<td>http_proxy</td>
<td>string</td>
<td></td>
<td></td>
<td>Specify an HTTP proxy to use, using the format: http://[username[:password]@]proxy.example.com[:port]</td>
</tr>
<tr>
<td>variables</td>
<td>text</td>
<td></td>
<td></td>
<td>List of scenario-level variables (macros) that may be used in scenario steps.</td>
</tr>
<tr>
<td>Element</td>
<td>Element property</td>
<td>Type</td>
<td>Range</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------</td>
<td>----------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>headers</td>
<td></td>
<td>text</td>
<td></td>
<td>HTTP headers that will be sent when performing a request.</td>
</tr>
<tr>
<td>status</td>
<td></td>
<td>integer</td>
<td>0 - enabled</td>
<td>Web scenario status.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - disabled</td>
<td></td>
</tr>
<tr>
<td></td>
<td>authentication</td>
<td>integer</td>
<td>0 - none</td>
<td>Authentication method.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - basic</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 - NTLM</td>
<td></td>
</tr>
<tr>
<td>http_user</td>
<td></td>
<td>string</td>
<td></td>
<td>Authentication user name.</td>
</tr>
<tr>
<td>http_password</td>
<td></td>
<td>string</td>
<td></td>
<td>Authentication password for specified user name.</td>
</tr>
<tr>
<td>verify_peer</td>
<td></td>
<td>integer</td>
<td>0 - no</td>
<td>Verify the SSL certificate of the web server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - yes</td>
<td></td>
</tr>
<tr>
<td>verify_host</td>
<td></td>
<td>integer</td>
<td>0 - no</td>
<td>Verify that the Common Name field or the Subject Alternative Name field of the</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - yes</td>
<td>web server certificate matches.</td>
</tr>
<tr>
<td></td>
<td>ssl_cert_file</td>
<td>string</td>
<td></td>
<td>Name of the SSL certificate file used for client authentication.</td>
</tr>
<tr>
<td></td>
<td>ssl_key_file</td>
<td>string</td>
<td></td>
<td>Name of the SSL private key file used for client authentication.</td>
</tr>
<tr>
<td></td>
<td>ssl_key_password</td>
<td>string</td>
<td></td>
<td>SSL private key file password.</td>
</tr>
<tr>
<td>steps</td>
<td></td>
<td></td>
<td></td>
<td>Root element for web scenario steps.</td>
</tr>
<tr>
<td>step</td>
<td></td>
<td></td>
<td></td>
<td>Individual web scenario step.</td>
</tr>
<tr>
<td>name</td>
<td></td>
<td>string</td>
<td></td>
<td>Web scenario step name.</td>
</tr>
<tr>
<td>url</td>
<td></td>
<td>string</td>
<td></td>
<td>URL for monitoring.</td>
</tr>
<tr>
<td>posts</td>
<td></td>
<td>text</td>
<td></td>
<td>List of ‘Post’ variables.</td>
</tr>
<tr>
<td>variables</td>
<td></td>
<td>text</td>
<td></td>
<td>List of step-level variables (macros) that should be applied after this step.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>If the variable value has a ‘regex:’ prefix, then its value is extracted from the data returned by this step according to the regular expression pattern following the ‘regex:’ prefix</td>
</tr>
<tr>
<td>headers</td>
<td></td>
<td>text</td>
<td></td>
<td>HTTP headers that will be sent when performing a request.</td>
</tr>
<tr>
<td>follow_redirects</td>
<td></td>
<td>integer</td>
<td>0 - no</td>
<td>Follow HTTP redirects.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - yes</td>
<td></td>
</tr>
<tr>
<td>retrieve_mode</td>
<td></td>
<td>integer</td>
<td>0 - content</td>
<td>HTTP response retrieve mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - headers only</td>
<td></td>
</tr>
<tr>
<td>timeout</td>
<td></td>
<td>string</td>
<td></td>
<td>Timeout of step execution. Seconds, time unit with suffix or user macro.</td>
</tr>
<tr>
<td>required</td>
<td></td>
<td>string</td>
<td></td>
<td>Required string. Ignored if empty.</td>
</tr>
<tr>
<td>status_codes</td>
<td></td>
<td>string</td>
<td></td>
<td>A comma delimited list of accepted status codes. Ignored if empty. For example: 200-201,210-299</td>
</tr>
</tbody>
</table>
3 Hosts

Overview

Hosts are exported with many related objects and object relations.

Host export contains:

- linked host groups
- host data
- template linkage
- host group linkage
- host interfaces
- directly linked applications
- directly linked items
- directly linked triggers
- directly linked graphs
- directly linked discovery rules with all prototypes
- directly linked web scenarios
- host macros
- host inventory data
- value maps

Exporting

To export hosts, do the following:

- Go to: Configuration → Hosts
- Mark the checkboxes of the hosts to export
- Click on Export below the list

Selected hosts are exported to a local XML file with default name zbx_export_hosts.xml.

Importing

To import hosts, do the following:

- Go to: Configuration → Hosts
- Click on Import to the right
- Select the import file
- Mark the required options in import rules
- Click on Import
Note that before Zabbix 4.0.16, when a host is imported and updated, it can only be linked to additional templates and never be unlinked from any.

A success or failure message of the import will be displayed in the frontend.

Import rules:

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update existing</td>
<td>Existing elements will be updated with data taken from the import file. Otherwise they will not be updated.</td>
</tr>
<tr>
<td>Create new</td>
<td>The import will add new elements using data from the import file. Otherwise it will not add them.</td>
</tr>
<tr>
<td>Delete missing</td>
<td>The import will remove existing elements not present in the import file. Otherwise it will not remove them. If Delete missing is marked for template linkage (only available since 4.0.16), existing template linkage not present in the import file will be removed from the host along with all entities inherited from the potentially unlinked templates (items, triggers, etc).</td>
</tr>
</tbody>
</table>

Export format

```xml
<?xml version="1.0" encoding="UTF-8"?>
<zabbix_export>
  <version>4.0</version>
</zabbix_export>
```
<groups>
  <group>
    <name>Zabbix servers</name>
  </group>
</groups>

<hosts>
  <host>
    <name>Export host</name>
    <description/>
    <proxy/>
    <status>0</status>
    <ipmi_authtype>-1</ipmi_authtype>
    <ipmi_privilege>2</ipmi_privilege>
    <ipmi_username/>
    <ipmi_password/>
    <tls_connect>1</tls_connect>
    <tls_accept>1</tls_accept>
    <tls_issuer/>
    <tls_subject/>
    <tls_psk_identity/>
    <tls_psk/>
    <templates/>
    <groups>
      <group>
        <name>Zabbix servers</name>
      </group>
    </groups>
  </host>
</hosts>

<interfaces>
  <interface>
    <default>1</default>
    <type>1</type>
    <useip>1</useip>
    <ip>127.0.0.1</ip>
    <dns/>
    <port>10050</port>
    <bulk>1</bulk>
    <interface_ref>if1</interface_ref>
  </interface>
</interfaces>

<applications>
  <application>
    <name>Application</name>
  </application>
</applications>

<items>
  <item>
    <name>Item</name>
    <type>0</type>
    <snmp_community/>
    <snmp_oid/>
    <key>item.key</key>
    <delay>30s</delay>
    <history>90d</history>
    <trends>365d</trends>
    <status>0</status>
    <value_type>3</value_type>
    <allowed_hosts/>
    <units/>
    <snmpv3_contextname/>
    <snmpv3_securityname/>
<snmpv3_securitylevel>0</snmpv3_securitylevel>
<snmpv3_authprotocol>0</snmpv3_authprotocol>
<snmpv3_authpassphrase/>
<snmpv3_privprotocol>0</snmpv3_privprotocol>
<snmpv3_privpassphrase/>
<params/>
<ipmi_sensor/>
<authtype>0</authtype>
$username/>
$password/>
$publickey/>
$privatekey/>
$port/>
<description/>
$inventory_link>0</inventory_link>
$applications>
 <application>
   <name>Application</name>
 </application>
 </applications>
<valuemap>
 <name>Host status</name>
 </valuemap>
$logtimefmt/>
<preprocessing/>
$interface_ref_if1</interface_ref/>
$jmx_endpoint/>
$master_item/>
$timeout>3s</timeout>
$url/>
$query_fields/>
<posts/>
$status_codes>200</status_codes>
$follow_redirects>1</follow_redirects>
$post_type>0</post_type>
$http_proxy/>
$headers/>
$retrieve_mode>0</retrieve_mode>
$request_method>1</request_method>
$output_format>0</output_format>
$allow_traps>0</allow_traps>
$ssl_cert_file/>
$ssl_key_file/>
$ssl_key_password/>
$verify_peer>0</verify_peer>
$verify_host>0</verify_host>
</item>
</items>
<discovery_rules/>
<httptests/>
<macros/>
<inventory/>
</host>
</hosts>
<triggers>
 <trigger>
   <expression>{Export host:item.key.last()}>0</expression>
   <recovery_mode>0</recovery_mode>
   <recovery_expression/>
   $correlation_mode>0</correlation_mode>
   $correlation_tag/>
   $name>Item value not 0</name>
</trigger>
<url/>
<status>0</status>
<priority>2</priority>
<description/>
<type>0</type>
<manual_close>0</manual_close>
<dependencies/>
<tags/>
</trigger>
</triggers>
<graphs>
  <graph>
    <name>Example graph</name>
    <width>900</width>
    <height>200</height>
    <yaxismin>0.0000</yaxismin>
    <yaxismax>100.0000</yaxismax>
    <show_work_period>1</show_work_period>
    <show_triggers>1</show_triggers>
    <type>0</type>
    <show_legend>1</show_legend>
    <show_3d>0</show_3d>
    <percent_left>0.0000</percent_left>
    <percent_right>0.0000</percent_right>
    <ymin_type_1>0</ymin_type_1>
    <ymax_type_1>0</ymax_type_1>
    <ymin_item_1>0</ymin_item_1>
    <ymax_item_1>0</ymax_item_1>
    <graph_items>
      <graph_item>
        <sortorder>0</sortorder>
        <drawtype>0</drawtype>
        <color>1A7C11</color>
        <yaxisside>0</yaxisside>
        <calc_fnc>2</calc_fnc>
        <type>0</type>
        <item>
          <host>Export host</host>
          <key>item.key</key>
        </item>
      </graph_item>
    </graph_items>
  </graph>
</graphs>

<value_maps>
  <value_map>
    <name>Host status</name>
    <mappings>
      <mapping>
        <value>0</value>
        <newvalue>Up</newvalue>
      </mapping>
      <mapping>
        <value>2</value>
        <newvalue>Unreachable</newvalue>
      </mapping>
    </mappings>
  </value_map>
</value_maps>
</zabbix_export>
Element tag values are explained in the table below.

### Host tags

<table>
<thead>
<tr>
<th>Element</th>
<th>Element property</th>
<th>Type</th>
<th>Range</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>groups</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>group</td>
<td>name</td>
<td>string</td>
<td></td>
<td>Unique group name. Individual group.</td>
</tr>
<tr>
<td>hosts</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>host</td>
<td>name</td>
<td>string</td>
<td></td>
<td>Unique host name.</td>
</tr>
<tr>
<td></td>
<td>description</td>
<td>text</td>
<td></td>
<td>Visible host name.</td>
</tr>
<tr>
<td></td>
<td>status</td>
<td>integer</td>
<td>0 - monitored</td>
<td>Host status.</td>
</tr>
<tr>
<td>ipmi_auth_type</td>
<td>integer</td>
<td>-1 - default</td>
<td>0 - none 1 - MD2 2 - MD5 4 - straight 5 - OEM 6 - RMCP+</td>
<td>IPMI session authentication type.</td>
</tr>
<tr>
<td>ipmi_privilege</td>
<td>integer</td>
<td>1 - callback</td>
<td>2 - user 3 - operator 4 - admin 5 - OEM</td>
<td>IPMI session privilege level.</td>
</tr>
<tr>
<td>ipmi_username</td>
<td>string</td>
<td></td>
<td></td>
<td>Username for IPMI checks.</td>
</tr>
<tr>
<td>ipmi_password</td>
<td>string</td>
<td></td>
<td></td>
<td>Password for IPMI checks.</td>
</tr>
<tr>
<td>tls_connect</td>
<td>integer</td>
<td>1 - unencrypted</td>
<td>2 - TLS with PSK 4 - TLS with certificate</td>
<td>Type of outgoing connection.</td>
</tr>
<tr>
<td>tls_accept</td>
<td>integer</td>
<td>1 - unencrypted</td>
<td>2 - TLS with PSK 3 - unencrypted and TLS with PSK 4 - TLS with certificate 5 - unencrypted and TLS with certificate 6 - TLS with PSK or certificate 7 - unencrypted and TLS with PSK or certificate</td>
<td>Type of incoming connection.</td>
</tr>
<tr>
<td>tls_issuer</td>
<td>string</td>
<td></td>
<td></td>
<td>Allowed agent/proxy certificate issuer.</td>
</tr>
<tr>
<td>tls_subject</td>
<td>string</td>
<td></td>
<td></td>
<td>Allowed agent/proxy certificate subject.</td>
</tr>
<tr>
<td>Element</td>
<td>Element property</td>
<td>Type</td>
<td>Range</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------------</td>
<td>---------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>proxy</td>
<td>name</td>
<td>string</td>
<td></td>
<td>Name of the proxy (if any) that monitors the host.</td>
</tr>
<tr>
<td>templates</td>
<td>name</td>
<td>string</td>
<td></td>
<td>Root element for linked templates.</td>
</tr>
<tr>
<td>interfaces</td>
<td>name</td>
<td>string</td>
<td></td>
<td>Root element for host interfaces.</td>
</tr>
<tr>
<td>interface</td>
<td>default</td>
<td>integer</td>
<td>0 - secondary</td>
<td>Only one primary interface of one type can be on a host.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - primary</td>
<td>(default)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Interface status.</td>
</tr>
<tr>
<td></td>
<td>type</td>
<td>integer</td>
<td>0 - unknown</td>
<td>Interface type.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - Zabbix</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 - SNMP</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 - IPMI</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4 - JMX</td>
<td></td>
</tr>
<tr>
<td></td>
<td>useip</td>
<td>integer</td>
<td>0 - use DNS</td>
<td>Interface to use for connecting to the host.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>name</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - use IP</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ip</td>
<td>string</td>
<td></td>
<td>IP address, can be either IPv4 or IPv6.</td>
</tr>
<tr>
<td></td>
<td>dns</td>
<td>string</td>
<td></td>
<td>DNS name.</td>
</tr>
<tr>
<td></td>
<td>port</td>
<td>string</td>
<td></td>
<td>Port number.</td>
</tr>
<tr>
<td></td>
<td>bulk</td>
<td>integer</td>
<td>0 - disable</td>
<td>Use bulk requests for SNMP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface_ref</td>
<td>string</td>
<td></td>
<td>Interface reference name to be used in items.</td>
</tr>
<tr>
<td>applications</td>
<td></td>
<td></td>
<td></td>
<td>Root element for applications.</td>
</tr>
<tr>
<td>application</td>
<td>name</td>
<td>string</td>
<td></td>
<td>Individual application.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Application name.</td>
<td></td>
</tr>
<tr>
<td>macros</td>
<td>name</td>
<td>string</td>
<td></td>
<td>Root element for macros.</td>
</tr>
<tr>
<td>macro</td>
<td></td>
<td></td>
<td>Individual macro.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>value</td>
<td>string</td>
<td></td>
<td>User macro name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>User macro value.</td>
<td></td>
</tr>
</tbody>
</table>

**Host item tags**

<table>
<thead>
<tr>
<th>Element</th>
<th>Element property</th>
<th>Type</th>
<th>Range</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>items</td>
<td></td>
<td></td>
<td></td>
<td>Root element for items.</td>
</tr>
<tr>
<td>item</td>
<td></td>
<td></td>
<td></td>
<td>Individual item.</td>
</tr>
<tr>
<td></td>
<td>name</td>
<td>string</td>
<td></td>
<td>Item name.</td>
</tr>
<tr>
<td>Element</td>
<td>Element property</td>
<td>Type</td>
<td>Range</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------</td>
<td>---------</td>
<td>-------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>type</td>
<td></td>
<td>integer</td>
<td>0-Zabbix agent 1 - SNMPv1 agent 2 - Zabbix trapper 3 - simple check 4 - SNMPv2 agent 5 - internal 6 - SNMPv3 agent 7 - Zabbix agent (active) 8 - aggregate 9 - HTTP test (web monitoring scenario step) 10 - external 11 - database monitor 12 - IPMI agent 13 - SSH agent 14 - Telnet agent 15 - calculated 16 - JMX agent 17 - SNMP trap 18 - Dependent item 19 - HTTP agent item</td>
<td>Item type.</td>
</tr>
</tbody>
</table>

<p>| snmp_community | string | SNMP community name if 'type' is 1,4. |
| snmp_oid       | string | SNMP object ID. |
| key            | string | Item key. |
| delay          | string | Update interval of the item. Seconds, time unit with suffix, custom intervals or user macros. Note that delay will be always '0' for trapper items. |
| history        | string | A time unit of how long the history data should be stored. Time unit with suffix or user macro. |</p>
<table>
<thead>
<tr>
<th>Element</th>
<th>Element property</th>
<th>Type</th>
<th>Range</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>trends</td>
<td></td>
<td>string</td>
<td></td>
<td>A time unit of how long the trends data should be stored. Time unit with suffix or user macro.</td>
</tr>
<tr>
<td>status</td>
<td></td>
<td>integer</td>
<td>0 - enabled</td>
<td>Item status.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - disabled</td>
<td></td>
</tr>
<tr>
<td>value_type</td>
<td></td>
<td>integer</td>
<td>0 - float</td>
<td>Received value type.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - character</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 - log</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 - unsigned</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4 - text</td>
<td></td>
</tr>
<tr>
<td>allowed_hosts</td>
<td></td>
<td>string</td>
<td></td>
<td>List of IP addresses (comma delimited) of hosts allowed sending data for the item if ‘type’ is 2 or 19.</td>
</tr>
<tr>
<td>units</td>
<td></td>
<td>string</td>
<td></td>
<td>Units of returned values (bps, B).</td>
</tr>
<tr>
<td>snmpv3_contextname</td>
<td></td>
<td>string</td>
<td></td>
<td>SNMPv3 context name.</td>
</tr>
<tr>
<td>snmpv3_securityname</td>
<td></td>
<td>string</td>
<td></td>
<td>SNMPv3 security name.</td>
</tr>
<tr>
<td>snmpv3_securitylevel</td>
<td></td>
<td>integer</td>
<td>0 - noAuthNoPriv</td>
<td>SNMPv3 security level.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - authNoPriv</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 - authPriv</td>
<td></td>
</tr>
<tr>
<td>snmpv3_authprotocol</td>
<td></td>
<td>integer</td>
<td>0 - MD5</td>
<td>SNMPv3 authentication protocol.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - SHA</td>
<td></td>
</tr>
<tr>
<td>snmpv3_authpassphrase</td>
<td></td>
<td>string</td>
<td></td>
<td>SNMPv3 authentication passphrase.</td>
</tr>
<tr>
<td>snmpv3_privprotocol</td>
<td></td>
<td>integer</td>
<td>0 - DES</td>
<td>SNMPv3 privacy protocol.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - AES</td>
<td></td>
</tr>
<tr>
<td>snmpv3_privpassphrase</td>
<td></td>
<td>string</td>
<td></td>
<td>SNMPv3 privacy passphrase.</td>
</tr>
<tr>
<td>params</td>
<td></td>
<td>text</td>
<td></td>
<td>Name of the “Executed script” if ‘type’ is 13,14 “SQL query” field if ‘type’ is 11 “Formula” field if ‘type’ is 15.</td>
</tr>
<tr>
<td>ipmi_sensor</td>
<td></td>
<td>string</td>
<td></td>
<td>IPMI sensor ID if ‘type’ is 12.</td>
</tr>
<tr>
<td>authtype</td>
<td></td>
<td>integer</td>
<td></td>
<td>Authentication type for SSH agent items: 0 - password 1 - key Authentication type for HTTP agent items: 0 - none 1 - basic 2 - NTLM</td>
</tr>
<tr>
<td>username</td>
<td></td>
<td>string</td>
<td></td>
<td>User name if ‘type’ is 11,13,14,19.</td>
</tr>
<tr>
<td>password</td>
<td></td>
<td>string</td>
<td></td>
<td>Password if ‘type’ is 11,13,14,19.</td>
</tr>
<tr>
<td>publickey</td>
<td></td>
<td>string</td>
<td></td>
<td>Name of the public key file if ‘type’ is 13.</td>
</tr>
<tr>
<td>privatekey</td>
<td></td>
<td>string</td>
<td></td>
<td>Name of the private key file if ‘type’ is 13.</td>
</tr>
<tr>
<td>Element</td>
<td>Element property</td>
<td>Type</td>
<td>Range</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------</td>
<td>---------</td>
<td>------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>port</td>
<td></td>
<td>string</td>
<td></td>
<td>Custom port for the item.</td>
</tr>
<tr>
<td>description</td>
<td></td>
<td>text</td>
<td></td>
<td>Item description.</td>
</tr>
<tr>
<td>inventory_link</td>
<td></td>
<td>integer</td>
<td>0 - no link number -</td>
<td>Use item value to populate this inventory field.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>number of field in the</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>‘host_inventory’ table</td>
<td></td>
</tr>
<tr>
<td>logtimefmt</td>
<td></td>
<td>string</td>
<td></td>
<td>Format of the time in log entries. Used only by log items.</td>
</tr>
<tr>
<td>interface_ref</td>
<td></td>
<td>string</td>
<td></td>
<td>Reference to host interface.</td>
</tr>
<tr>
<td>jmx_endpoint</td>
<td></td>
<td>string</td>
<td></td>
<td>JMX endpoint if ‘type’ is 16.</td>
</tr>
<tr>
<td>url</td>
<td></td>
<td>string</td>
<td></td>
<td>URL string if ‘type’ is 19.</td>
</tr>
<tr>
<td>allow_traps</td>
<td></td>
<td>integer</td>
<td>0 - Do not allow</td>
<td>Property to allow to send data to item if ‘type’ is 19.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>trapping.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - Allow trapping.</td>
<td></td>
</tr>
<tr>
<td>follow_redirects</td>
<td></td>
<td>integer</td>
<td>0 - Do not follow</td>
<td>Follow HTTP redirects if ‘type’ is 19.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>redirects.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - Follow redirects.</td>
<td></td>
</tr>
<tr>
<td>headers</td>
<td></td>
<td>object</td>
<td></td>
<td>Object with HTTP(S) request headers if ‘type’ is 19.</td>
</tr>
<tr>
<td>http_proxy</td>
<td></td>
<td>string</td>
<td></td>
<td>HTTP(S) proxy connection string if ‘type’ is 19.</td>
</tr>
<tr>
<td>output_format</td>
<td></td>
<td>integer</td>
<td>0 - Store as is.</td>
<td>How to process response if ‘type’ is 19.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - Convert to JSON.</td>
<td></td>
</tr>
<tr>
<td>post_type</td>
<td></td>
<td>integer</td>
<td>0 - Raw data.</td>
<td>Type of request body if ‘type’ is 19.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 - JSON data.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 - XML data.</td>
<td></td>
</tr>
<tr>
<td>posts</td>
<td></td>
<td>text</td>
<td></td>
<td>Request body if ‘type’ is 19.</td>
</tr>
<tr>
<td>query_fields</td>
<td></td>
<td>array</td>
<td></td>
<td>Array of objects for request query fields if ‘type’ is 19.</td>
</tr>
<tr>
<td>request_method</td>
<td></td>
<td>integer</td>
<td>0 - GET</td>
<td>Request method if ‘type’ is 19.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - POST</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 - PUT</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 - HEAD</td>
<td></td>
</tr>
<tr>
<td>retrieve_mode</td>
<td></td>
<td>integer</td>
<td>0 - Body.</td>
<td>What part of response should be stored if ‘type’ is 19.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - Headers.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 - Both body and</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>headers will be stored.</td>
<td></td>
</tr>
<tr>
<td>ssl_cert_file</td>
<td></td>
<td>string</td>
<td></td>
<td>Public SSL Key file path if ‘type’ is 19.</td>
</tr>
<tr>
<td>ssl_key_file</td>
<td></td>
<td>string</td>
<td></td>
<td>Private SSL Key file path if ‘type’ is 19.</td>
</tr>
<tr>
<td>ssl_key_password</td>
<td></td>
<td>string</td>
<td></td>
<td>Password for SSL Key file if ‘type’ is 19.</td>
</tr>
<tr>
<td>status_codes</td>
<td></td>
<td>string</td>
<td></td>
<td>Ranges of required HTTP status codes separated by commas if ‘type’ is 19.</td>
</tr>
<tr>
<td>timeout</td>
<td></td>
<td>string</td>
<td></td>
<td>Item data polling request timeout if ‘type’ is 19.</td>
</tr>
<tr>
<td>Element</td>
<td>Element property</td>
<td>Type</td>
<td>Range</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------</td>
<td>--------</td>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>verify_host</td>
<td></td>
<td>integer</td>
<td>0 - Do not validate.</td>
<td>Validate host name in URL is in Common Name field or a Subject Alternate Name field of host certificate if 'type' is 19.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - Validate.</td>
<td>Validate is host certificate authentic if 'type' is 19.</td>
</tr>
<tr>
<td>verify_peer</td>
<td></td>
<td>integer</td>
<td>0 - Do not validate.</td>
<td>Validate is host certificate authentic if 'type' is 19.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - Validate.</td>
<td>Validate is host certificate authentic if 'type' is 19.</td>
</tr>
<tr>
<td>value map</td>
<td>name</td>
<td>string</td>
<td></td>
<td>Value map.</td>
</tr>
<tr>
<td>applications</td>
<td>name</td>
<td>string</td>
<td></td>
<td>Name of the value map to use for the item.</td>
</tr>
<tr>
<td>application</td>
<td>name</td>
<td>string</td>
<td></td>
<td>Root element for applications.</td>
</tr>
<tr>
<td>preproccessing</td>
<td>name</td>
<td>string</td>
<td></td>
<td>Individual application.</td>
</tr>
<tr>
<td>step</td>
<td>name</td>
<td>string</td>
<td></td>
<td>Application name.</td>
</tr>
<tr>
<td></td>
<td>type</td>
<td>integer</td>
<td>1 - custom multiplier</td>
<td>Individual item value preprocessing.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 - right trim</td>
<td>Type of the item value preprocessing step.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 - left trim</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4 - trim from both sides</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5 - regular expression</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>matching</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6 - boolean to decimal</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7 - octal to decimal</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>8 - hexadecimal to decimal</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>9 - simple change;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>calculated as (received</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>value-previous value)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>10 - change per second;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>calculated as (received</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>value-previous value)/(</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>time now-time of last</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>check)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>11 - XML Path</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>12 - JSONPath</td>
<td></td>
</tr>
<tr>
<td>params</td>
<td>params</td>
<td>string</td>
<td>Parameters of the item</td>
<td>Individual item master item value preprocessing step.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>value preprocessing step.</td>
<td></td>
</tr>
<tr>
<td>master_item</td>
<td>key</td>
<td>string</td>
<td>Individual item master item data</td>
<td></td>
</tr>
<tr>
<td></td>
<td>key</td>
<td></td>
<td>Dependent item master</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>item key value.</td>
<td></td>
</tr>
</tbody>
</table>
### Host low-level discovery rule tags

<table>
<thead>
<tr>
<th>Element</th>
<th>Element property</th>
<th>Type</th>
<th>Range</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>discovery_rule</td>
<td></td>
<td></td>
<td></td>
<td>Individual low-level discovery rule.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>For most of the element tag values, see element tag values for a regular item.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Only the tags that are specific to low-level discovery rules, are described below.</td>
</tr>
<tr>
<td>lifetime</td>
<td></td>
<td>string</td>
<td></td>
<td>Time period after which items that are no longer discovered will be deleted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Seconds, time unit with suffix or user macro.</td>
<td></td>
</tr>
<tr>
<td>filter</td>
<td>evaltype</td>
<td>integer</td>
<td>0 - And/or logic 1 - And logic 2 - Or logic 3 - custom formula</td>
<td>Logic to use for checking low-level discovery rule filter conditions.</td>
</tr>
<tr>
<td></td>
<td>formula</td>
<td>string</td>
<td></td>
<td>Custom calculation formula for filter conditions.</td>
</tr>
<tr>
<td></td>
<td>conditions</td>
<td></td>
<td></td>
<td>Root element for filter conditions.</td>
</tr>
<tr>
<td>condition</td>
<td>macro</td>
<td>string</td>
<td></td>
<td>Individual filter condition.</td>
</tr>
<tr>
<td></td>
<td>value</td>
<td>string</td>
<td></td>
<td>Low-level discovery macro name.</td>
</tr>
<tr>
<td></td>
<td>operator</td>
<td>integer</td>
<td></td>
<td>Filter value: regular expression or global regular expression.</td>
</tr>
<tr>
<td></td>
<td>formulaid</td>
<td>character</td>
<td></td>
<td>Filter condition ID. Used in the custom calculation formula.</td>
</tr>
<tr>
<td>item_prototypes</td>
<td></td>
<td></td>
<td></td>
<td>Root element for item_prototypes.</td>
</tr>
<tr>
<td>item_prototype</td>
<td></td>
<td></td>
<td></td>
<td>Individual item_prototype.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>For most of the element tag values, see element tag values for a regular item.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Only the tags that are specific to item_prototypes, are described below.</td>
</tr>
<tr>
<td>application_prototypes</td>
<td></td>
<td></td>
<td></td>
<td>Root element for application prototypes.</td>
</tr>
<tr>
<td>application_prototype</td>
<td></td>
<td></td>
<td></td>
<td>Individual application prototype.</td>
</tr>
<tr>
<td></td>
<td>name</td>
<td></td>
<td></td>
<td>Application prototype name.</td>
</tr>
<tr>
<td>master_item</td>
<td>key</td>
<td>string</td>
<td></td>
<td>Dependent item prototype master item/item prototype key value.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Host trigger tags

<table>
<thead>
<tr>
<th>Element</th>
<th>Element property</th>
<th>Type</th>
<th>Range</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>triggers</td>
<td></td>
<td></td>
<td></td>
<td>Root element for triggers.</td>
</tr>
<tr>
<td>Element</td>
<td>Element property</td>
<td>Type</td>
<td>Range</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------</td>
<td>----------</td>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>trigger</td>
<td>expression</td>
<td>string</td>
<td>0 - expression</td>
<td>Trigger expression.</td>
</tr>
<tr>
<td></td>
<td>recovery_mode</td>
<td>integer</td>
<td>1 - recovery expression</td>
<td>Basis for generating OK events.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 - none</td>
<td></td>
</tr>
<tr>
<td></td>
<td>recovery_expression</td>
<td>string</td>
<td></td>
<td>Trigger recovery expression.</td>
</tr>
<tr>
<td></td>
<td>name</td>
<td>string</td>
<td></td>
<td>Trigger name.</td>
</tr>
<tr>
<td></td>
<td>correlation_mode</td>
<td>integer</td>
<td>0 - no event correlation</td>
<td>Correlation mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - event correlation</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>by tag</td>
<td></td>
</tr>
<tr>
<td></td>
<td>correlation_tag</td>
<td>string</td>
<td></td>
<td>The tag name to be used for event correlation.</td>
</tr>
<tr>
<td></td>
<td>url</td>
<td>string</td>
<td>0 - enabled</td>
<td>Trigger URL.</td>
</tr>
<tr>
<td></td>
<td>status</td>
<td>integer</td>
<td>1 - disabled</td>
<td>Trigger status.</td>
</tr>
<tr>
<td></td>
<td>priority</td>
<td>integer</td>
<td>0 - not classified</td>
<td>Trigger severity.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - information</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 - warning</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 - average</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4 - high</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5 - disaster</td>
<td></td>
</tr>
<tr>
<td></td>
<td>description</td>
<td>text</td>
<td></td>
<td>Trigger description.</td>
</tr>
<tr>
<td></td>
<td>type</td>
<td>integer</td>
<td>0 - single problem event</td>
<td>Event generation type.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - multiple problem events</td>
<td></td>
</tr>
<tr>
<td></td>
<td>manual_close</td>
<td>integer</td>
<td>0 - not allowed</td>
<td>Manual closing of problem events.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - allowed</td>
<td></td>
</tr>
<tr>
<td>dependencies</td>
<td>dependency</td>
<td>string</td>
<td></td>
<td>Root element for dependencies.</td>
</tr>
<tr>
<td></td>
<td>name</td>
<td>string</td>
<td></td>
<td>Individual dependency.</td>
</tr>
<tr>
<td></td>
<td>expression</td>
<td>string</td>
<td></td>
<td>Dependency trigger name.</td>
</tr>
<tr>
<td></td>
<td>recovery_expression</td>
<td>string</td>
<td></td>
<td>Dependency trigger expression.</td>
</tr>
<tr>
<td></td>
<td>recovery_expression</td>
<td>string</td>
<td></td>
<td>Dependency trigger recovery expression.</td>
</tr>
<tr>
<td>tags</td>
<td>tag</td>
<td>string</td>
<td></td>
<td>Root element for event tags.</td>
</tr>
<tr>
<td></td>
<td>value</td>
<td>string</td>
<td></td>
<td>Individual event tag.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Tag name.</td>
</tr>
</tbody>
</table>

Host graph tags

<table>
<thead>
<tr>
<th>Element</th>
<th>Element property</th>
<th>Type</th>
<th>Range</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>graphs</td>
<td>graph</td>
<td>string</td>
<td></td>
<td>Root element for graphs.</td>
</tr>
<tr>
<td></td>
<td>name</td>
<td>string</td>
<td></td>
<td>Individual graph.</td>
</tr>
<tr>
<td></td>
<td>width</td>
<td>integer</td>
<td></td>
<td>Graph name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Graph width, in pixels. Used for preview and for pie/exploded graphs.</td>
</tr>
<tr>
<td>Element</td>
<td>Element property</td>
<td>Type</td>
<td>Range</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------</td>
<td>--------</td>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>height</td>
<td>integer</td>
<td></td>
<td>Graph height, in pixels. Used for preview and for pie/exploded graphs.</td>
</tr>
<tr>
<td></td>
<td>yaxismin</td>
<td>double</td>
<td></td>
<td>Value of Y axis minimum if 'ymin_type_1' is 1.</td>
</tr>
<tr>
<td></td>
<td>yaxismax</td>
<td>double</td>
<td></td>
<td>Value of Y axis maximum if 'ymax_type_1' is 1.</td>
</tr>
<tr>
<td></td>
<td>show_work_period</td>
<td>integer</td>
<td>0 - no, 1 - yes</td>
<td>Highlight non-working hours if 'type' is 0, 1.</td>
</tr>
<tr>
<td></td>
<td>show_triggers</td>
<td>integer</td>
<td>0 - no, 1 - yes</td>
<td>Display simple trigger values as a line if 'type' is 0, 1.</td>
</tr>
<tr>
<td></td>
<td>type</td>
<td>integer</td>
<td>0 - normal, 1 - stacked, 2 - pie, 3 - exploded, 4 - 3D pie, 5 - 3D exploded</td>
<td>Graph type.</td>
</tr>
<tr>
<td></td>
<td>show_legend</td>
<td>integer</td>
<td>0 - no, 1 - yes</td>
<td>Display graph legend.</td>
</tr>
<tr>
<td></td>
<td>show_3d</td>
<td>integer</td>
<td>0 - 2D, 1 - 3D</td>
<td>Enable 3D style if 'type' is 2, 3.</td>
</tr>
<tr>
<td></td>
<td>percent_left</td>
<td>double</td>
<td></td>
<td>Show the percentile line for left axis if 'type' is 0.</td>
</tr>
<tr>
<td></td>
<td>percent_right</td>
<td>double</td>
<td></td>
<td>Show the percentile line for right axis if 'type' is 0.</td>
</tr>
<tr>
<td></td>
<td>ymin_type_1</td>
<td>integer</td>
<td>0 - calculated, 1 - fixed, 2 - last value of the selected item</td>
<td>Minimum value of Y axis if 'type' is 0, 1.</td>
</tr>
<tr>
<td></td>
<td>ymax_type_1</td>
<td>integer</td>
<td>0 - calculated, 1 - fixed, 2 - last value of the selected item</td>
<td>Maximum value of Y axis if 'type' is 0, 1.</td>
</tr>
<tr>
<td></td>
<td>ymin_item_1</td>
<td>string</td>
<td>null or item details</td>
<td>Item details if 'ymin_type_1' is 2.</td>
</tr>
<tr>
<td></td>
<td>ymax_item_1</td>
<td>string</td>
<td>null or item details</td>
<td>Item details if 'ymax_type_1' is 2.</td>
</tr>
<tr>
<td></td>
<td>graph_items</td>
<td></td>
<td></td>
<td>Root element for graph items.</td>
</tr>
<tr>
<td></td>
<td>graph_item</td>
<td></td>
<td></td>
<td>Individual graph item. Draw order. The smaller value is drawn first. Can be used to draw lines or regions behind (or in front of) another.</td>
</tr>
<tr>
<td></td>
<td>sortorder</td>
<td>integer</td>
<td></td>
<td>Draw style if graph 'type' is 0.</td>
</tr>
<tr>
<td></td>
<td>drawtype</td>
<td>integer</td>
<td>0 - single line, 1 - filled region, 2 - bold line, 3 - dotted line, 4 - dashed line</td>
<td>Draw style if graph 'type' is 0.</td>
</tr>
<tr>
<td>Element</td>
<td>Element property</td>
<td>Type</td>
<td>Range</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>------------------</td>
<td>--------</td>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>color</td>
<td></td>
<td>string</td>
<td></td>
<td>Element color (6 symbols, hex).</td>
</tr>
<tr>
<td>yaxisside</td>
<td></td>
<td>integer</td>
<td>0 - left axis, 1 - right axis</td>
<td>Y axis position (left or right) the element belongs to if graph 'type' is 0,1.</td>
</tr>
<tr>
<td>calc_fnc</td>
<td></td>
<td>integer</td>
<td>1 - minimum, 2 - average, 4 - maximum, 7 - all (minimum, average and maximum, if graph 'type' is 0), 9 - last (if graph 'type' is not 0,1)</td>
<td>Data to draw if more than one value exists for an item.</td>
</tr>
<tr>
<td>type</td>
<td></td>
<td>integer</td>
<td>1 - value of the item is represented proportionally on the pie, 2 - value of the item represents the whole pie (graph sum)</td>
<td>Draw type for pie/exploded graphs.</td>
</tr>
</tbody>
</table>

**Item**

- **host**: string
- **key**: string

**Host web scenario tags**

<table>
<thead>
<tr>
<th>Element</th>
<th>Element property</th>
<th>Type</th>
<th>Range</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>httptests</td>
<td></td>
<td></td>
<td></td>
<td>Root element for web scenarios.</td>
</tr>
<tr>
<td>httptest</td>
<td></td>
<td></td>
<td></td>
<td>Individual web scenario.</td>
</tr>
<tr>
<td>name</td>
<td></td>
<td>string</td>
<td></td>
<td>Web scenario name.</td>
</tr>
<tr>
<td>delay</td>
<td></td>
<td>string</td>
<td></td>
<td>Frequency of executing the web scenario. Seconds, time unit with suffix or user macro.</td>
</tr>
<tr>
<td>attempts</td>
<td></td>
<td>integer</td>
<td>1-10</td>
<td>The number of attempts for executing web scenario steps.</td>
</tr>
<tr>
<td>agent</td>
<td></td>
<td>string</td>
<td></td>
<td>Client agent. Zabbix will pretend to be the selected browser. This is useful when a website returns different content for different browsers.</td>
</tr>
<tr>
<td>http_proxy</td>
<td></td>
<td>string</td>
<td></td>
<td>Specify an HTTP proxy to use, using the format: http://[username[:password]@]proxy.example.com[:port]</td>
</tr>
<tr>
<td>variables</td>
<td></td>
<td>text</td>
<td></td>
<td>List of scenario-level variables (macros) that may be used in scenario steps.</td>
</tr>
<tr>
<td>Element</td>
<td>Element Property</td>
<td>Type</td>
<td>Range</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------</td>
<td>-----------</td>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>headers</td>
<td></td>
<td>text</td>
<td></td>
<td>HTTP headers that will be sent when performing a request.</td>
</tr>
<tr>
<td>status</td>
<td></td>
<td>integer</td>
<td>0 - enabled</td>
<td>Web scenario status.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - disabled</td>
<td></td>
</tr>
<tr>
<td>authentication</td>
<td></td>
<td>integer</td>
<td>0 - none</td>
<td>Authentication method.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - basic</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 - NTLM</td>
<td></td>
</tr>
<tr>
<td>http_user</td>
<td></td>
<td>string</td>
<td></td>
<td>Authentication user name.</td>
</tr>
<tr>
<td>http_password</td>
<td></td>
<td>string</td>
<td></td>
<td>Authentication password for specified user name.</td>
</tr>
<tr>
<td>verify_peer</td>
<td></td>
<td>integer</td>
<td>0 - no</td>
<td>Verify the SSL certificate of the web server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - yes</td>
<td></td>
</tr>
<tr>
<td>verify_host</td>
<td></td>
<td>integer</td>
<td>0 - no</td>
<td>Verify that the Common Name field of the web server certificate matches.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - yes</td>
<td>Alternate Name field of the web server certificate matches.</td>
</tr>
<tr>
<td>ssl_cert_file</td>
<td></td>
<td>string</td>
<td></td>
<td>Name of the SSL certificate file used for client authentication.</td>
</tr>
<tr>
<td>ssl_key_file</td>
<td></td>
<td>string</td>
<td></td>
<td>Name of the SSL private key file used for client authentication.</td>
</tr>
<tr>
<td>ssl_key_password</td>
<td></td>
<td>string</td>
<td></td>
<td>SSL private key file password.</td>
</tr>
<tr>
<td>steps</td>
<td></td>
<td></td>
<td></td>
<td>Root element for web scenario steps.</td>
</tr>
<tr>
<td>step</td>
<td></td>
<td></td>
<td></td>
<td>Individual web scenario step.</td>
</tr>
<tr>
<td>name</td>
<td></td>
<td>string</td>
<td></td>
<td>Web scenario step name.</td>
</tr>
<tr>
<td>url</td>
<td></td>
<td>string</td>
<td></td>
<td>URL for monitoring.</td>
</tr>
<tr>
<td>posts</td>
<td></td>
<td>text</td>
<td></td>
<td>List of 'Post' variables.</td>
</tr>
<tr>
<td>variables</td>
<td></td>
<td>text</td>
<td></td>
<td>List of step-level variables (macros) that should be applied after this step.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>If the variable value has a 'regex:' prefix, then its value is extracted from the data returned by this step according to the regular expression pattern following the 'regex:' prefix.</td>
</tr>
<tr>
<td>headers</td>
<td></td>
<td>text</td>
<td></td>
<td>HTTP headers that will be sent when performing a request.</td>
</tr>
<tr>
<td>follow_redirects</td>
<td></td>
<td>integer</td>
<td>0 - no</td>
<td>Follow HTTP redirects.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - yes</td>
<td></td>
</tr>
<tr>
<td>retrieve_mode</td>
<td></td>
<td>integer</td>
<td>0 - content</td>
<td>HTTP response retrieve mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - headers only</td>
<td></td>
</tr>
<tr>
<td>timeout</td>
<td></td>
<td>string</td>
<td></td>
<td>Timeout of step execution.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Seconds, time unit with suffix or user macro.</td>
<td></td>
</tr>
<tr>
<td>required</td>
<td></td>
<td>string</td>
<td></td>
<td>Required string. Ignored if empty.</td>
</tr>
<tr>
<td>status_codes</td>
<td></td>
<td>string</td>
<td></td>
<td>A comma delimited list of accepted status codes. Ignored if empty. For example: 200-201,210-299</td>
</tr>
</tbody>
</table>
4 Network maps

Overview

Network map export contains:

- all related images
- map structure - all map settings, all contained elements with their settings, map links and map link status indicators

Not exported are host groups, hosts, triggers, other maps or any other elements that may be related to the exported map. Thus, if at least one of the elements the map refers to is missing, importing it will fail.

Network map export/import is supported since Zabbix 1.8.2.

Exporting

To export network maps, do the following:

- Go to: Monitoring → Maps
- Mark the checkboxes of the network maps to export
- Click on Export below the list

Selected maps are exported to a local XML file with default name zabbix_export_maps.xml.

Importing

To import network maps, do the following:

- Go to: Monitoring → Maps
- Click on Import to the right
- Select the import file
- Mark the required options in import rules
- Click on Import
All mandatory input fields are marked with a red asterisk.

A success or failure message of the import will be displayed in the frontend.

Import rules:

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update existing</td>
<td>Existing maps will be updated with data taken from the import file. Otherwise they will not be updated.</td>
</tr>
<tr>
<td>Create new</td>
<td>The import will add new maps using data from the import file. Otherwise it will not add them.</td>
</tr>
</tbody>
</table>

If you uncheck both map options and check the respective options for images, images only will be imported. Image importing is only available to Zabbix Super Admin users.

**Warning:**
If replacing an existing image, it will affect all maps that are using this image.

Export format

Exporting a small network map with three elements, their images and some links between them. Note that images are truncated to save space.
<xml version="1.0" encoding="UTF-8"?>
<zabbix_export>
  <version>4.0</version>
  <date>2016-10-05T08:16:20Z</date>
  <images>
    <image>
      <name>Server_(64)</name>
      <imagetype>1</imagetype>
      <encodedImage>iVBOR...SuQmCC</encodedImage>
    </image>
    <image>
      <name>Workstation_(64)</name>
      <imagetype>1</imagetype>
      <encodedImage>iVBOR...SuQmCC</encodedImage>
    </image>
    <image>
      <name>Zabbix_server_3D_(96)</name>
      <imagetype>1</imagetype>
      <encodedImage>iVBOR...ggg==</encodedImage>
    </image>
  </images>
  <maps>
    <map>
      <name>Network</name>
      <width>590</width>
      <height>400</height>
      <label_type>0</label_type>
      <label_location>0</label_location>
      <highlight>1</highlight>
      <expandproblem>0</expandproblem>
      <markelements>1</markelements>
      <show_unack>0</show_unack>
      <severity_min>0</severity_min>
      <show_suppressed>0</show_suppressed>
      <grid_size>40</grid_size>
      <grid_show>1</grid_show>
      <grid_align>1</grid_align>
      <label_format>0</label_format>
      <label_type_host>2</label_type_host>
      <label_type_hostgroup>2</label_type_hostgroup>
      <label_type_trigger>2</label_type_trigger>
      <label_type_map>2</label_type_map>
      <label_type_image>2</label_type_image>
      <label_string_host/>
      <label_string_hostgroup/>
      <label_string_trigger/>
      <label_string_map/>
      <label_string_image/>
      <expand_macros>0</expand_macros>
      <background/>
      <iconmap/>
      <urls/>
      <selements>
        <selement>
          <elementtype>0</elementtype>
          <label>Host 1</label>
          <label_location>-1</label_location>
          <x>476</x>
          <y>28</y>
          <elementsubtype>0</elementsubtype>
          <areatype>0</areatype>
          <width>200</width>
        </selement>
      </selements>
    </map>
  </maps>
</zabbix_export>
Element tags
Element tag values are explained in the table below.

<table>
<thead>
<tr>
<th>Element</th>
<th>Element property</th>
<th>Type</th>
<th>Range</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>images</td>
<td></td>
<td></td>
<td></td>
<td>Root element for images.</td>
</tr>
<tr>
<td>image</td>
<td>name</td>
<td>string</td>
<td></td>
<td>Unique image name.</td>
</tr>
<tr>
<td></td>
<td>imagetype</td>
<td>integer</td>
<td>1 - image</td>
<td>Image type.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 - background</td>
<td></td>
</tr>
<tr>
<td>maps</td>
<td>encodedImage</td>
<td>Base64 encoded image</td>
<td></td>
<td>Root element for maps.</td>
</tr>
<tr>
<td>map</td>
<td>name</td>
<td>string</td>
<td></td>
<td>Unique map name.</td>
</tr>
<tr>
<td></td>
<td>width</td>
<td>integer</td>
<td></td>
<td>Map width, in pixels.</td>
</tr>
<tr>
<td></td>
<td>height</td>
<td>integer</td>
<td></td>
<td>Map height, in pixels.</td>
</tr>
<tr>
<td>Element</td>
<td>Element property</td>
<td>Type</td>
<td>Range</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------</td>
<td>-----------</td>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>label_type</td>
<td>integer</td>
<td>0 - label</td>
<td>1 - host IP address 2 - element name 3 - status only 4 - nothing</td>
<td>Map element label type.</td>
</tr>
<tr>
<td>label_location</td>
<td>integer</td>
<td>0 - bottom</td>
<td>1 - left 2 - right 3 - top</td>
<td>Map element label location by default.</td>
</tr>
<tr>
<td>highlight</td>
<td>integer</td>
<td>0 - no</td>
<td>1 - yes</td>
<td>Enable icon highlighting for active triggers and host statuses.</td>
</tr>
<tr>
<td>expand_problem</td>
<td>integer</td>
<td>0 - no</td>
<td>1 - yes</td>
<td>Display problem trigger for elements with a single problem.</td>
</tr>
<tr>
<td>markelements</td>
<td>integer</td>
<td>0 - no</td>
<td>1 - yes</td>
<td>Highlight map elements that have recently changed their status.</td>
</tr>
<tr>
<td>show_unack</td>
<td>integer</td>
<td>0 - count of all problems 1 - count of unacknowledged problems 2 - count of acknowledged and unacknowledged problems separately</td>
<td>Problem display.</td>
<td></td>
</tr>
<tr>
<td>severity_min</td>
<td>integer</td>
<td>0 - not classified 1 - information 2 - warning 3 - average 4 - high 5 - disaster</td>
<td>Minimum trigger severity to show on the map by default.</td>
<td></td>
</tr>
<tr>
<td>show_suppressed</td>
<td>integer</td>
<td>0 - no</td>
<td>1 - yes</td>
<td>Display problems which would otherwise be suppressed (not shown) because of host maintenance.</td>
</tr>
<tr>
<td>grid_size</td>
<td>integer</td>
<td>20, 40, 50, 75 or 100</td>
<td>Display a grid in map configuration.</td>
<td></td>
</tr>
<tr>
<td>grid_show</td>
<td>integer</td>
<td>0 - yes</td>
<td>1 - no</td>
<td>Automatically align icons in map configuration.</td>
</tr>
<tr>
<td>grid_align</td>
<td>integer</td>
<td>0 - yes</td>
<td>1 - no</td>
<td>Use advanced label configuration.</td>
</tr>
<tr>
<td>Element</td>
<td>Element Property</td>
<td>Type</td>
<td>Range</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------</td>
<td>----------</td>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>label_type_host</td>
<td>integer</td>
<td>integer</td>
<td>0 - label</td>
<td>Display as host label, if “label_format=1”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - host IP address</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 - element name</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 - status only</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4 - nothing</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5 - custom label</td>
<td></td>
</tr>
<tr>
<td>label_type_hostgroup</td>
<td>integer</td>
<td>integer</td>
<td>0 - label</td>
<td>Display as host group label, if “label_format=1”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 - element name</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 - status only</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4 - nothing</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5 - custom label</td>
<td></td>
</tr>
<tr>
<td>label_type_trigger</td>
<td>integer</td>
<td>integer</td>
<td>0 - label</td>
<td>Display as trigger label, if “label_format=1”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 - element name</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 - status only</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4 - nothing</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5 - custom label</td>
<td></td>
</tr>
<tr>
<td>label_type_map</td>
<td>integer</td>
<td>integer</td>
<td>0 - label</td>
<td>Display as map label, if “label_format=1”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 - element name</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 - status only</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4 - nothing</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5 - custom label</td>
<td></td>
</tr>
<tr>
<td>label_type_image</td>
<td>integer</td>
<td>integer</td>
<td>0 - label</td>
<td>Display as image label, if “label_format=1”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 - element name</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4 - nothing</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5 - custom label</td>
<td></td>
</tr>
<tr>
<td>label_string_host</td>
<td>string</td>
<td>string</td>
<td>Custom label for host</td>
<td>Custom label for host elements, if “label_type_host=5”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>elements, if</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>“label_type_host=5”</td>
<td></td>
</tr>
<tr>
<td>label_string_hostgroup</td>
<td>string</td>
<td>string</td>
<td>Custom label for host</td>
<td>Custom label for host group elements, if “label_type_hostgroup=5”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>group elements, if</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>“label_type_hostgroup=5”</td>
<td></td>
</tr>
<tr>
<td>label_string_trigger</td>
<td>string</td>
<td>string</td>
<td>Custom label for trigger</td>
<td>Custom label for trigger elements, if “label_type_trigger=5”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>elements, if</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>“label_type_trigger=5”</td>
<td></td>
</tr>
<tr>
<td>label_string_map</td>
<td>string</td>
<td>string</td>
<td>Custom label for map</td>
<td>Custom label for map elements, if “label_type_map=5”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>elements, if</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>“label_type_map=5”</td>
<td></td>
</tr>
<tr>
<td>label_string_image</td>
<td>string</td>
<td>string</td>
<td>Custom label for image</td>
<td>Custom label for image elements, if “label_type_image=5”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>elements, if</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>“label_type_image=5”</td>
<td></td>
</tr>
<tr>
<td>expand_macros</td>
<td>integer</td>
<td>integer</td>
<td>0 - no</td>
<td>Expand macros in labels in map configuration.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - yes</td>
<td></td>
</tr>
<tr>
<td>background</td>
<td>id</td>
<td>id</td>
<td>ID of the background image</td>
<td>ID of the background image (if any), if “imagetype=2”</td>
</tr>
<tr>
<td>iconmap</td>
<td>id</td>
<td>id</td>
<td>ID of the icon mapping</td>
<td>ID of the icon mapping (if any).</td>
</tr>
<tr>
<td>Element</td>
<td>Element property</td>
<td>Type</td>
<td>Range</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>------------------</td>
<td>----------</td>
<td>------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>urls</td>
<td>url</td>
<td>string</td>
<td></td>
<td>Individual URL.</td>
</tr>
<tr>
<td></td>
<td>name</td>
<td>string</td>
<td></td>
<td>Link name.</td>
</tr>
<tr>
<td></td>
<td>url</td>
<td>string</td>
<td></td>
<td>Link URL.</td>
</tr>
<tr>
<td></td>
<td>elementtype</td>
<td>integer</td>
<td>0 - host 1 - map 2 - trigger 3 - host group 4 - image</td>
<td>Map item type the link belongs to.</td>
</tr>
<tr>
<td>selements</td>
<td>selement</td>
<td>elementtype</td>
<td>integer</td>
<td>0 - host 1 - map 2 - trigger 3 - host group 4 - image</td>
</tr>
<tr>
<td></td>
<td>label</td>
<td>string</td>
<td></td>
<td>Icon label.</td>
</tr>
<tr>
<td></td>
<td>label_location</td>
<td>integer</td>
<td>-1 - use map default 0 - bottom 1 - left 2 - right 3 - top</td>
<td>Location on the X axis. Location on the Y axis.</td>
</tr>
<tr>
<td></td>
<td>x</td>
<td>integer</td>
<td></td>
<td>Location on the X axis. Location on the Y axis.</td>
</tr>
<tr>
<td></td>
<td>y</td>
<td>integer</td>
<td></td>
<td>Location on the X axis. Location on the Y axis.</td>
</tr>
<tr>
<td></td>
<td>elementssubtype</td>
<td>integer</td>
<td>0 - single host group 1 - all host groups</td>
<td>Element subtype, if &quot;elementtype=3&quot;</td>
</tr>
<tr>
<td></td>
<td>areatype</td>
<td>integer</td>
<td>0 - same as whole map 1 - custom size</td>
<td>Area size, if &quot;elementssubtype=1&quot;</td>
</tr>
<tr>
<td></td>
<td>width</td>
<td>integer</td>
<td></td>
<td>Width of area, if &quot;areatype=1&quot;</td>
</tr>
<tr>
<td></td>
<td>height</td>
<td>integer</td>
<td></td>
<td>Height of area, if &quot;areatype=1&quot;</td>
</tr>
<tr>
<td></td>
<td>viewtype</td>
<td>integer</td>
<td>0 - place evenly in the area</td>
<td>Area placement algorithm, if &quot;elementssubtype=1&quot;</td>
</tr>
<tr>
<td></td>
<td>use_iconmap</td>
<td>integer</td>
<td>0 - no 1 - yes</td>
<td>Use icon mapping for this element. Relevant only if icon mapping is activated on map level.</td>
</tr>
<tr>
<td></td>
<td>selementid</td>
<td>id</td>
<td></td>
<td>Unique element record ID.</td>
</tr>
<tr>
<td></td>
<td>application</td>
<td>string</td>
<td></td>
<td>Application name filter. If an application name is given, only problems of triggers that belong to the given application will be displayed on the map.</td>
</tr>
<tr>
<td>elements</td>
<td>element</td>
<td>host</td>
<td></td>
<td>Individual Zabbix entity that is represented on the map (map, hostgroup, host, etc).</td>
</tr>
<tr>
<td></td>
<td>icon_off</td>
<td>image</td>
<td></td>
<td>Image to use when element is in 'OK' status.</td>
</tr>
<tr>
<td></td>
<td>icon_on</td>
<td>image</td>
<td></td>
<td>Image to use when element is in 'Problem' status.</td>
</tr>
<tr>
<td>Element</td>
<td>Element property</td>
<td>Type</td>
<td>Range</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------</td>
<td>---------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>icon_disabled</td>
<td></td>
<td></td>
<td></td>
<td>Image to use when element is disabled.</td>
</tr>
<tr>
<td>icon_maintenance</td>
<td></td>
<td></td>
<td></td>
<td>Image to use when element is in maintenance.</td>
</tr>
<tr>
<td>name</td>
<td></td>
<td>string</td>
<td></td>
<td>Unique image name.</td>
</tr>
<tr>
<td>links</td>
<td>link</td>
<td></td>
<td></td>
<td>Individual link between map elements.</td>
</tr>
<tr>
<td>drawtype</td>
<td></td>
<td>integer</td>
<td>0 - line</td>
<td>Link style.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 - bold line</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 - dotted line</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4 - dashed line</td>
<td></td>
</tr>
<tr>
<td>color</td>
<td></td>
<td>string</td>
<td></td>
<td>Link color (6 symbols, hex).</td>
</tr>
<tr>
<td>label</td>
<td></td>
<td>string</td>
<td></td>
<td>Link label.</td>
</tr>
<tr>
<td>selementid1</td>
<td></td>
<td>id</td>
<td></td>
<td>ID of one element to connect.</td>
</tr>
<tr>
<td>selementid2</td>
<td></td>
<td>id</td>
<td></td>
<td>ID of the other element to connect.</td>
</tr>
<tr>
<td>linktriggers</td>
<td>linktrigger</td>
<td></td>
<td></td>
<td>Individual link status indicator.</td>
</tr>
<tr>
<td>drawtype</td>
<td></td>
<td>integer</td>
<td>0 - line</td>
<td>Link style when trigger is in the ‘Problem’ state.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 - bold line</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 - dotted line</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4 - dashed line</td>
<td></td>
</tr>
<tr>
<td>color</td>
<td></td>
<td>string</td>
<td></td>
<td>Link color (6 symbols, hex) when trigger is in the ‘Problem’ state.</td>
</tr>
<tr>
<td>trigger</td>
<td></td>
<td></td>
<td></td>
<td>Trigger used for indicating link status.</td>
</tr>
<tr>
<td>description</td>
<td></td>
<td>string</td>
<td></td>
<td>Trigger name.</td>
</tr>
<tr>
<td>expression</td>
<td></td>
<td>string</td>
<td></td>
<td>Trigger expression.</td>
</tr>
<tr>
<td>recovery_expression</td>
<td></td>
<td>string</td>
<td></td>
<td>Trigger recovery expression.</td>
</tr>
</tbody>
</table>

### 5 Screens

**Overview**

Screen **export** contains the screen structure - all screen settings and all screen elements along with their configuration.

Anything included in the screen itself (like a host, host group or any other data) is not exported. Thus, if at least one of the elements the screen refers to is missing, importing it will fail.

**Exporting**

To export screens, do the following:

- Go to: Monitoring → Screens
- Mark the checkboxes of the screens to export
- Click on Export below the list
Selected screens are exported to a local XML file with default name `zabbix_export_screens.xml`.

**Importing**

To import screens, do the following:

- Go to: Monitoring → Screens
- Click on Import to the right
- Select the import file
- Mark the required options in import rules
- Click on Import
All mandatory input fields are marked with a red asterisk.

A success or failure message of the import will be displayed in the frontend.

**Import rules:**

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update existing</td>
<td>Existing screens will be updated with data taken from the import file. Otherwise they will not be updated.</td>
</tr>
<tr>
<td>Create new</td>
<td>The import will add new screens using data from the import file. Otherwise it will not add them.</td>
</tr>
</tbody>
</table>

**Export format**

Exporting a small screen with two graphs taking up the first row of the screen.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<zabbix_export>
    <version>4.0</version>
    <date>2016-10-07T08:02:40Z</date>
    <screens>
        <screen>
            <name>Zabbix server</name>
            <hsize>2</hsize>
        </screen>
    </screens>
</zabbix_export>
```
Element tags

Element tag values are explained in the table below.

<table>
<thead>
<tr>
<th>Element</th>
<th>Element property</th>
<th>Type</th>
<th>Range</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>screens</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>screen</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>name</td>
<td>string</td>
<td></td>
<td>Unique screen name.</td>
</tr>
<tr>
<td></td>
<td>hsize</td>
<td>integer</td>
<td></td>
<td>Horizontal size, number of columns.</td>
</tr>
<tr>
<td></td>
<td>vsize</td>
<td>integer</td>
<td></td>
<td>Vertical size, number of rows.</td>
</tr>
<tr>
<td>Element</td>
<td>Element property</td>
<td>Type</td>
<td>Range</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------</td>
<td>--------</td>
<td>-------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>screen_items</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>screen_item</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>resourcetype</td>
<td>integer</td>
<td>0 - graph</td>
<td>1 - simple graph</td>
<td>Resource type.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 - map</td>
<td>3 - plain text</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 - host info</td>
<td>5 - trigger info</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>6 - server info</td>
<td>7 - clock</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>8 - screen</td>
<td>9 - trigger overview</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>10 - data overview</td>
<td>11 - URL</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>12 - history of actions</td>
<td>13 - history of events</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>14 - host group issues</td>
<td>15 - problems by severity</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>16 - host issues</td>
<td>19 - simple graph prototype</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>20 - graph prototype</td>
<td></td>
<td></td>
</tr>
<tr>
<td>width</td>
<td>integer</td>
<td></td>
<td></td>
<td>Width of the screen item (in pixels) if ‘resourcetype’ is 0, 1, 7, 11, 19 or 20.</td>
</tr>
<tr>
<td>height</td>
<td>integer</td>
<td></td>
<td></td>
<td>Height of the screen item (in pixels) if ‘resourcetype’ is 0, 1, 7, 11, 19 or 20.</td>
</tr>
<tr>
<td>x</td>
<td>integer</td>
<td></td>
<td></td>
<td>X-coordinates of the screen item on the screen, from left to right.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>‘0’ means start from first column.</td>
</tr>
<tr>
<td>y</td>
<td>integer</td>
<td></td>
<td></td>
<td>Y-coordinates of the screen item on the screen, from top to bottom.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>‘0’ means start from first row.</td>
</tr>
<tr>
<td>colspan</td>
<td>integer</td>
<td></td>
<td></td>
<td>Number of columns the screen item will span across.</td>
</tr>
<tr>
<td>rowspan</td>
<td>integer</td>
<td></td>
<td></td>
<td>Number of rows the screen item will span across.</td>
</tr>
<tr>
<td>elements</td>
<td>integer</td>
<td></td>
<td></td>
<td>Number of lines to display on the screen item if ‘resourcetype’ is 3, 12, 13, 14 or 16.</td>
</tr>
<tr>
<td>Element</td>
<td>Element property</td>
<td>Type</td>
<td>Range</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------</td>
<td>---------</td>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>valign</td>
<td></td>
<td>integer</td>
<td>0 - middle (default) 1 - top 2 - bottom</td>
<td>Vertical alignment.</td>
</tr>
<tr>
<td>halign</td>
<td></td>
<td>integer</td>
<td>0 - center (default) 1 - left 2 - right</td>
<td>Horizontal alignment.</td>
</tr>
<tr>
<td>style</td>
<td></td>
<td>integer</td>
<td>0 - plain text 1 - HTML</td>
<td>Option of displaying screen item if 'resourcetype' is 3.</td>
</tr>
<tr>
<td>style</td>
<td></td>
<td>integer</td>
<td>0 - local time 1 - server time 2 - host time</td>
<td>Option of displaying screen item if 'resourcetype' is 7.</td>
</tr>
<tr>
<td>style</td>
<td></td>
<td>integer</td>
<td>0 - horizontal 1 - vertical</td>
<td>Option of displaying screen item if 'resourcetype' is 4,5.</td>
</tr>
<tr>
<td>style</td>
<td></td>
<td>integer</td>
<td>0 - left side 1 - top</td>
<td>Option of displaying screen item if 'resourcetype' is 9,10.</td>
</tr>
<tr>
<td>url</td>
<td></td>
<td>string</td>
<td></td>
<td>Link URL if 'resourcetype' is 11.</td>
</tr>
<tr>
<td>dynamic</td>
<td></td>
<td>integer</td>
<td>0 - no 1 - yes</td>
<td>Make screen item dynamic if 'resourcetype' is 0, 1, 3, 19 or 20.</td>
</tr>
<tr>
<td>sort_triggers</td>
<td></td>
<td>integer</td>
<td>0 - last change (descending) 1 - severity (descending) 2 - host (ascending)</td>
<td>Option to sort triggers by if 'resourcetype' is 14,16.</td>
</tr>
<tr>
<td>sort_triggers</td>
<td></td>
<td>integer</td>
<td>3 - time (ascending) 4 - time (descending) 5 - type (ascending) 6 - type (descending) 7 - status (ascending) 8 - status (descending) 9 - retries left (ascending) 10 - retries left (descending) 11 - recipient (ascending) 12 - recipient (descending)</td>
<td>Option to sort triggers by if 'resourcetype' is 12.</td>
</tr>
<tr>
<td>max_columns</td>
<td></td>
<td>integer</td>
<td></td>
<td>In how many columns generated graphs should be displayed in the screen cell if 'resourcetype' is 19 or 20. Useful when there are many LLD-generated graphs.</td>
</tr>
</tbody>
</table>
15. Discovery

Please use the sidebar to access content in the Discovery section.

1 Network discovery

Overview

Zabbix offers automatic network discovery functionality that is effective and very flexible.

With network discovery properly set up you can:

- speed up Zabbix deployment
- simplify administration
- use Zabbix in rapidly changing environments without excessive administration

Zabbix network discovery is based on the following information:

- IP ranges
- Availability of external services (FTP, SSH, WEB, POP3, IMAP, TCP, etc)
- Information received from Zabbix agent (only unencrypted mode is supported)
- Information received from SNMP agent

It does NOT provide:

- Discovery of network topology

Network discovery basically consists of two phases: discovery and actions.

Discovery

Zabbix periodically scans the IP ranges defined in network discovery rules. The frequency of the check is configurable for each rule individually.

Note that one discovery rule will always be processed by a single discoverer process. The IP range will not be split between multiple discoverer processes.

Each rule has a set of service checks defined to be performed for the IP range.

**Note:** Discovery checks are processed independently from the other checks. If any checks do not find a service (or fail), other checks will still be processed.

Every check of a service and a host (IP) performed by the network discovery module generates a discovery event.

<table>
<thead>
<tr>
<th>Event</th>
<th>Check of service result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Discovered</td>
<td>The service is ‘up’ after it was ‘down’ or when discovered for the first time.</td>
</tr>
<tr>
<td>Service Up</td>
<td>The service is ‘up’, after it was already ‘up’.</td>
</tr>
<tr>
<td>Service Lost</td>
<td>The service is ‘down’ after it was ‘up’.</td>
</tr>
<tr>
<td>Service Down</td>
<td>The service is ‘down’, after it was already ‘down’.</td>
</tr>
<tr>
<td>Host Discovered</td>
<td>At least one service of a host is ‘up’ after all services of that host were ‘down’ or a service is discovered which belongs to a not registered host.</td>
</tr>
<tr>
<td>Host Up</td>
<td>At least one service of a host is ‘up’, after at least one service was already ‘up’.</td>
</tr>
<tr>
<td>Host Lost</td>
<td>All services of a host are ‘down’ after at least one was ‘up’.</td>
</tr>
<tr>
<td>Host Down</td>
<td>All services of a host are ‘down’, after they were already ‘down’.</td>
</tr>
</tbody>
</table>
Actions

Discovery events can be the basis of relevant actions, such as:

- Sending notifications
- Adding/removing hosts
- Enabling/disabling hosts
- Adding hosts to a group
- Removing hosts from a group
- Linking hosts to/unlinking from a template
- Executing remote scripts

These actions can be configured with respect to the device type, IP, status, uptime/downtime, etc. For full details on configuring actions for network-discovery based events, see action operation and conditions pages.

Note:

Linking a discovered host to templates will fail collectively if any of the linkable templates has a unique entity (e.g. item key) that is the same as a unique entity (e.g. item key) already existing on the host or on another of the linkable templates.

Host creation

A host is added if the Add host operation is selected. A host is also added, even if the Add host operation is missing, if you select operations resulting in actions on a host. Such operations are:

- enable host
- disable host
- add host to a host group
- link template to a host

When adding hosts, a host name is the result of reverse DNS lookup or IP address if reverse lookup fails. Lookup is performed from the Zabbix server or Zabbix proxy, depending on which is doing the discovery. If lookup fails on the proxy, it is not retried on the server. If the host with such a name already exists, the next host would get _2 appended to the name, then _3 and so on.

Created hosts are added to the Discovered hosts group (by default, configurable in Administration → General → Other). If you wish hosts to be added to another group, add a Remove from host groups operation (specifying “Discovered hosts”) and also add an Add to host groups operation (specifying another host group), because a host must belong to a host group.

If a host already exists with the discovered IP address, a new host is not created. However, if the discovery action contains operations (link template, add to host group, etc), they are performed on the existing host.

Host removal

Hosts discovered by a network discovery rule are removed automatically from Monitoring → Discovery if a discovered entity is not in the rule’s IP range any more. Hosts are removed immediately.

Interface creation when adding hosts

When hosts are added as a result of network discovery, they get interfaces created according to these rules:

- the services detected - for example, if an SNMP check succeeded, an SNMP interface will be created
- if a host responded both to Zabbix agent and SNMP requests, both types of interfaces will be created
- if uniqueness criteria are Zabbix agent or SNMP-returned data, the first interface found for a host will be created as the default one. Other IP addresses will be added as additional interfaces. Note that this will work if all interfaces are discovered by the same discovery rule. If a different discovery rule discovers a different interface of the same host, an additional host will be added.
- if a host responded to agent checks only, it will be created with an agent interface only. If it would start responding to SNMP later, additional SNMP interfaces would be added.
- if 3 separate hosts were initially created, having been discovered by the "IP" uniqueness criteria, and then the discovery rule is modified so that hosts A, B and C have identical uniqueness criteria result, B and C are created as additional interfaces for A, the first host. The individual hosts B and C remain. In Monitoring → Discovery the added interfaces will be displayed in the "Discovered device" column, in black font and indented, but the "Monitored host" column will only display A, the first created host. “Uptime/Downtime” is not measured for IPs that are considered to be additional interfaces.

1 Configuring a network discovery rule

Overview

To configure a network discovery rule used by Zabbix to discover hosts and services:

- Go to Configuration → Discovery
• Click on Create rule (or on the rule name to edit an existing one)
• Edit the discovery rule attributes

**Rule attributes**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name of the rule. For example, “Local network”.</td>
</tr>
</tbody>
</table>
| Discovery by proxy | What performs discovery:  
  **no proxy** - Zabbix server is doing discovery  
  **<proxy name>** - this proxy performs discovery |

**Parameter Description**

- **Name**: Local network
- **Discovery by proxy**: No proxy
- **IP range**: 192.168.0.1-254
- **Update interval**: 1h
- **Checks**: HTTP, HTTPS, ICMP ping, Zabbix agent "system.uname", SNMPv2 agent "1.3.6.1.2.1.1.1.0"
- **Device uniqueness criteria**: IP address
- **Enabled**: Enabled
Parameter | Description
--- | ---
IP range | The range of IP addresses for discovery. It may have the following formats:
  - Single IP: 192.168.1.33
  - Range of IP addresses: 192.168.1-10.1-255. The range is limited by the total number of covered addresses (less than 64K).
  - IP mask: 192.168.4.0/24
 supported IP masks:
  - /16 - /30 for IPv4 addresses
  - /12 - /128 for IPv6 addresses
  - List: 192.168.1.1-255, 192.168.2.1-100, 192.168.2.200, 192.168.4.0/24
 Since Zabbix 3.0.0 this field supports spaces, tabulation and multiple lines.

Update interval | This parameter defines how often Zabbix will execute the rule.
The interval is measured after the execution of previous discovery instance ends so there is no overlap.

  - Time suffixes are supported, e.g. 30s, 1m, 2h, 1d, since Zabbix 3.4.0.

  - User macros are supported, since Zabbix 3.4.0.

  - Note that if a user macro is used and its value is changed (e.g. 1w → 1h), the next check will be executed according to the previous value (far in the future with the example values).

Checks | Zabbix will use this list of checks for discovery.

  - Supported checks: SSH, LDAP, SMTP, FTP, HTTP, HTTPS, POP, NNTP, IMAP, TCP, Telnet, Zabbix agent, SNMPv1 agent, SNMPv2 agent, SNMPv3 agent, ICMP ping.

  - A protocol-based discovery uses the net.tcp.service[] functionality to test each host, except for SNMP which queries an SNMP OID. Zabbix agent is tested by querying an item in unencrypted mode. Please see agent items for more details.

  - The ‘Ports’ parameter may be one of following:
    - Single port: 22
    - Range of ports: 22-45
    - List: 22-45,55,60-70

Device uniqueness criteria | Uniqueness criteria may be:

  - **IP address** - no processing of multiple single-IP devices. If a device with the same IP already exists it will be considered already discovered and a new host will not be added.

  - **Type of discovery check** - either SNMP or Zabbix agent check.

Enabled | With the check-box marked the rule is active and will be executed by Zabbix server.

  - If unmarked, the rule is not active. It won’t be executed.

### Changing proxy setting

Since Zabbix 2.2.0 the hosts discovered by different proxies are always treated as different hosts. While this allows to perform discovery on matching IP ranges used by different subnets, changing proxy for an already monitored subnet is complicated because the proxy changes must be also applied to all discovered hosts. For example the steps to replace proxy in a discovery rule:

1. disable discovery rule
2. sync proxy configuration
3. replace the proxy in the discovery rule
4. replace the proxy for all hosts discovered by this rule
5. enable discovery rule

### A real life scenario

In this example we would like to set up network discovery for the local network having an IP range of 192.168.1.1-192.168.1.254.

In our scenario we want to:

- discover those hosts that have Zabbix agent running
- run discovery every 10 minutes
- add a host to monitoring if the host uptime is more than 1 hour
• remove hosts if the host downtime is more than 24 hours
• add Linux hosts to the “Linux servers” group
• add Windows hosts to the “Windows servers” group
• use Template OS Linux for Linux hosts
• use Template OS Windows for Windows hosts

Step 1

Defining a network discovery rule for our IP range.

Zabbix will try to discover hosts in the IP range of 192.168.1.1-192.168.1.254 by connecting to Zabbix agents and getting the value from `system.uname` key. The value received from the agent can be used to apply different actions for different operating systems. For example, link Windows servers to Template OS Windows, Linux servers to Template OS Linux.

The rule will be executed every 10 minutes (600 seconds).

When this rule is added, Zabbix will automatically start the discovery and generating discovery-based events for further processing.

Step 2

Defining an action for adding the discovered Linux servers to the respective group/template.
The action will be activated if:

- the “Zabbix agent” service is “up”
- the value of system.uname (the Zabbix agent key we used in rule definition) contains “Linux”
- Uptime is 1 hour (3600 seconds) or more

The action will execute the following operations:

- add the discovered host to the “Linux servers” group (and also add host if it wasn’t added previously)
- link host to the “Template OS Linux” template. Zabbix will automatically start monitoring the host using items and triggers
Step 3
Defining an action for adding the discovered Windows servers to the respective group/template.

Step 4
Defining an action for removing lost servers.
A server will be removed if “Zabbix agent” service is ‘down’ for more than 24 hours (86400 seconds).

2 Active agent auto-registration

Overview

It is possible to allow active Zabbix agent auto-registration, after which the server can start monitoring them. This way new hosts can be added for monitoring without configuring them manually on the server.

Auto registration can happen when a previously unknown active agent asks for checks.

The feature might be very handy for automatic monitoring of new Cloud nodes. As soon as you have a new node in the Cloud Zabbix will automatically start the collection of performance and availability data of the host.
Active agent auto-registration also supports the monitoring of added hosts with passive checks. When the active agent asks for checks, providing it has the 'ListenIP' or 'ListenPort' configuration parameters defined in the configuration file, these are sent along to the server. (If multiple IP addresses are specified, the first one is sent to the server.)

Server, when adding the new auto-registered host, uses the received IP address and port to configure the agent. If no IP address value is received, the one used for the incoming connection is used. If no port value is received, 10050 is used.

Auto-registration is rerun:
- if host metadata information changes
  - due to HostMetadata changed and agent restarted
  - due to value returned by HostMetadataItem changed
- for manually created hosts with metadata missing
- if a host is manually changed to be monitored by another Zabbix proxy
- if auto-registration for the same host comes from a new Zabbix proxy

Configuration

Specify server

Make sure you have the Zabbix server identified in the agent configuration file - zabbix_agentd.conf

ServerActive=10.0.0.1

Unless you specifically define a Hostname in zabbix_agentd.conf, the system hostname of agent location will be used by server for naming the host. The system hostname in Linux can be obtained by running the 'hostname' command.

Restart the agent after making any changes to the configuration file.

Action for active agent auto-registration

When server receives an auto-registration request from an agent it calls an action. An action of event source “Auto registration” must be configured for agent auto-registration.

Note:
Setting up network discovery is not required to have active agents auto-register.

In the Zabbix frontend, go to Configuration → Actions, select Auto registration as the event source and click on Create action:
- In the Action tab, give your action a name
- Optionally specify conditions. If you are going to use the "Host metadata" condition, see the next section.
- In the Operations tab, add relevant operations, such as - 'Add host', 'Add to host group' (for example, Discovered hosts), 'Link to templates', etc.

Note:
If the hosts that will be auto-registering are likely to be supported for active monitoring only (such as hosts that are firewalled from your Zabbix server) then you might want to create a specific template like Template_Linux-active to link to.

Created hosts are added to the Discovered hosts group (by default, configurable in Administration → General → Other). If you wish hosts to be added to another group, add a Remove from host group operation (specifying “Discovered hosts”) and also add an Add to host group operation (specifying another host group), because a host must belong to a host group.

Using host metadata

When agent is sending an auto-registration request to the server it sends its hostname. In some cases (for example, Amazon cloud nodes) a hostname is not enough for Zabbix server to differentiate discovered hosts. Host metadata can be optionally used to send other information from an agent to the server.

Host metadata is configured in the agent configuration file - zabbix_agentd.conf. There are 2 ways of specifying host metadata in the configuration file:

HostMetadata
HostMetadataItem

See the description of the options in the link above.

Attention:
An auto-registration attempt happens every time an active agent sends a request to refresh active checks to the server. The delay between requests is specified in the RefreshActiveChecks parameter of the agent. The first request is sent immediately after the agent is restarted.
Example 1

Using host metadata to distinguish between Linux and Windows hosts.

Say you would like the hosts to be auto-registered by the Zabbix server. You have active Zabbix agents (see “Configuration” section above) on your network. There are Windows hosts and Linux hosts on your network and you have “Template OS Linux” and “Template OS Windows” templates available in your Zabbix frontend. So at host registration you would like the appropriate Linux/Windows template to be applied to the host being registered. By default only the hostname is sent to the server at auto-registration, which might not be enough. In order to make sure the proper template is applied to the host you should use host metadata.

Frontend configuration

The first thing to do is to configure the frontend. Create 2 actions. The first action:

• Name: Linux host autoregistration
• Conditions: Host metadata contains Linux
• Operations: Link to templates: Template OS Linux

Note:
You can skip an “Add host” operation in this case. Linking to a template requires adding a host first so the server will do that automatically.

The second action:

• Name: Windows host autoregistration
• Conditions: Host metadata contains Windows
• Operations: Link to templates: Template OS Windows

Agent configuration

Now you need to configure the agents. Add the next line to the agent configuration files:

HostMetadataItem=system.uname

This way you make sure host metadata will contain “Linux” or “Windows” depending on the host an agent is running on. An example of host metadata in this case:

Linux: Linux server3 3.2.0-4-686-pae #1 SMP Debian 3.2.41-2 i686 GNU/Linux

Do not forget to restart the agent after making any changes to the configuration file.

Example 2

Step 1

Using host metadata to allow some basic protection against unwanted hosts registering.

Frontend configuration

Create an action in the frontend, using some hard-to-guess secret code to disallow unwanted hosts:

• Name: Auto registration action Linux
• Conditions:
  * Type of calculation: AND
  * Condition (A): Host metadata contains //Linux//
  * Condition (B): Host metadata contains //21df83bf21bf0be663090bb8d4128558ab9b95fba66a6dbf834f8b91ae5e08ae//
• Operations:
  * Send message to users: Admin via all media
  * Add to host groups: Linux servers
  * Link to templates: Template OS Linux

Please note that this method alone does not provide strong protection because data is transmitted in plain text. Configuration cache reload is required for changes to have an immediate effect.

Agent configuration

Add the next line to the agent configuration file:

HostMetadata=Linux 21df83bf21bf0be663090bb8d4128558ab9b95fba66a6dbf834f8b91ae5e08ae
where "Linux" is a platform, and the rest of the string is the hard-to-guess secret text.

Do not forget to restart the agent after making any changes to the configuration file.

Step 2

It is possible to add additional monitoring for an already registered host.

Frontend configuration

Update the action in the frontend:

- **Name**: Autoregistration action Linux
- **Conditions**:
  - *Type of calculation*: AND
  - *Condition (A)*: Host metadata contains Linux
  - *Condition (B)*: Host metadata contains 21df83bf21bf0be663090bb8d4128558ab9b95fba66a6dbf834f8b91ae5e08ae
- **Operations**:
  - *Send message to users*: Admin via all media
  - *Add to host groups*: Linux servers
  - *Link to templates*: Template OS Linux
  - *Link to templates*: Template DB MySQL

Agent configuration

Update the next line in the agent configuration file:

HostMetadata=MySQL on Linux 21df83bf21bf0be663090bb8d4128558ab9b95fba66a6dbf834f8b91ae5e08ae

Do not forget to restart the agent after making any changes to the configuration file.

### 3 Low-level discovery

**Overview**

Low-level discovery provides a way to automatically create items, triggers, and graphs for different entities on a computer. For instance, Zabbix can automatically start monitoring file systems or network interfaces on your machine, without the need to create items for each file system or network interface manually. Additionally, it is possible to configure Zabbix to remove unneeded entities automatically based on actual results of periodically performed discovery.

A user can define their own types of discovery, provided they follow a particular JSON protocol.

The general architecture of the discovery process is as follows.

First, a user creates a discovery rule in "Configuration" → "Templates" → "Discovery" column. A discovery rule consists of (1) an item that discovers the necessary entities (for instance, file systems or network interfaces) and (2) prototypes of items, triggers, and graphs that should be created based on the value of that item.

An item that discovers the necessary entities is like a regular item seen elsewhere: the server asks a Zabbix agent (or whatever the type of the item is set to) for a value of that item, the agent responds with a textual value. The difference is that the value the agent responds with should contain a list of discovered entities in a specific JSON format. While the details of this format are only important for implementers of custom discovery checks, it is necessary to know that the returned value contains a list of macro → value pairs. For instance, item "net.if.discovery" might return two pairs: "{#IFNAME}" → "lo" and "{#IFNAME}" → "eth0".

These macros are used in names, keys, and other prototype fields where they are then substituted with the received values for creating real items, triggers, graphs, or even hosts for each discovered entity. See the full list of options for using LLD macros.

When the server receives a value for a discovery item, it looks at the macro → value pairs and for each pair generates real items, triggers, and graphs, based on their prototypes. In the example with "net.if.discovery" above, the server would generate one set of items, triggers, and graphs for the loopback interface "lo", and another set for interface "eth0".

See also: Discovered entities

Configuring low-level discovery

We will illustrate low-level discovery based on an example of file system discovery.

To configure the discovery, do the following:

- **Go to**: Configuration → Templates or Hosts
- **Click on Discovery in the row of an appropriate template/host**
• Click on Create discovery rule in the upper right corner of the screen
• Fill in the discovery rule form with the required details

Discovery rule

The **Discovery rule** tab contains general discovery rule attributes:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of discovery rule.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of check to perform discovery; should be Zabbix agent or</td>
</tr>
<tr>
<td></td>
<td>Zabbix agent (active) for file system discovery.</td>
</tr>
<tr>
<td>Host interface</td>
<td>192.168.3.31:10050</td>
</tr>
<tr>
<td>Key</td>
<td>vfs.fs.discovery</td>
</tr>
<tr>
<td>Update interval</td>
<td>1h</td>
</tr>
<tr>
<td>Keep lost resources period</td>
<td>30d</td>
</tr>
<tr>
<td>Description</td>
<td>Discovery of file systems of different types as defined in global</td>
</tr>
<tr>
<td></td>
<td>regular expression &quot;File systems for discovery&quot;.</td>
</tr>
</tbody>
</table>

All mandatory input fields are marked with a red asterisk.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key</td>
<td>Enter the discovery item key. For example, you may use the built-in &quot;vfs.fs.discovery&quot; item key to return a JSON with the list of file systems present on the computer and their types. Note that another option for filesystem discovery is using discovery results by the &quot;vfs.fs.get&quot; agent key, supported since Zabbix 4.0.17 (see example).</td>
</tr>
<tr>
<td>Update interval</td>
<td>This field specifies how often Zabbix performs discovery. In the beginning, when you are just setting up file system discovery, you might wish to set it to a small interval, but once you know it works you can set it to 30 minutes or more, because file systems usually do not change very often. Time suffixes are supported, e.g. 30s, 1m, 2h, 1d, since Zabbix 3.4.0. User macros are supported, since Zabbix 3.4.0. Note: The update interval can only be set to ‘0’ if custom intervals exist with a non-zero value. If set to ‘0’, and a custom interval (flexible or scheduled) exists with a non-zero value, the item will be polled during the custom interval duration. Note that for an existing discovery rule the discovery can be performed immediately by pushing the Check now button.</td>
</tr>
<tr>
<td>Custom intervals</td>
<td>You can create custom rules for checking the item: Flexible - create an exception to the Update interval (interval with different frequency) Scheduling - create a custom polling schedule. For detailed information see Custom intervals. Scheduling is supported since Zabbix 3.0.0.</td>
</tr>
<tr>
<td>Keep lost resources period</td>
<td>This field allows you to specify the duration for how long the discovered entity will be retained (won’t be deleted) once its discovery status becomes “Not discovered anymore” (between 1 hour to 25 years; or “0”). Time suffixes are supported, e.g. 2h, 1d, since Zabbix 3.4.0. User macros are supported, since Zabbix 3.4.0. Note: If set to “0”, entities will be deleted immediately. Using “0” is not recommended, since just wrongly editing the filter may end up in the entity being deleted with all the historical data.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description.</td>
</tr>
<tr>
<td>Enabled</td>
<td>If checked, the rule will be processed.</td>
</tr>
</tbody>
</table>

**Discovery rule filter**

The Filters tab contains discovery rule filter definitions:
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type of calculation</strong></td>
<td>The following options for calculating filters are available:</td>
</tr>
<tr>
<td></td>
<td><em>And</em> - all filters must be passed;</td>
</tr>
<tr>
<td></td>
<td><em>Or</em> - enough if one filter is passed;</td>
</tr>
<tr>
<td></td>
<td><em>And/Or</em> - uses And with different macro names and Or with the same macro name;</td>
</tr>
<tr>
<td></td>
<td><em>Custom expression</em> - offers the possibility to define a custom calculation of filters. The formula must include all filters in the list.</td>
</tr>
<tr>
<td></td>
<td>Limited to 255 symbols.</td>
</tr>
</tbody>
</table>

**Filters**

A filter can be used to generate real items, triggers, and graphs only for certain file systems. It expects a **Perl Compatible Regular Expression** (PCRE). For instance, if you are only interested in C:, D:, and E: file systems, you could put `{#FSNAME}` into “Macro” and `"^C|^D|^E"` regular expression into “Regular expression” text fields. Filtering is also possible by file system types using `{#FSTYPE}` macro (e.g. “^ext|^reiserfs”) and by drive types (supported only by Windows agent) using `{#FSDRIVETYPE}` macro (e.g., “fixed”).

You can enter a regular expression or reference a global **regular expression** in “Regular expression” field.

In order to test a regular expression you can use “grep -E”, for example:

```plaintext
for f in ext2 nfs reiserfs smbfs; do echo $f \| grep -E '^ext'|^reiserfs' \| \| echo "SKIP: $f"; done
```

Filter drop-down offers two values to specify whether a macro matches a regular expression or does not match.

---

**Attention:**

Zabbix database in MySQL must be created as case-sensitive if file system names that differ only by case are to be discovered correctly.

**Attention:**

The mistake or typo in regex used in LLD rule may cause deleting thousands of configuration elements, historical values and events for many hosts. For example, incorrect “File systems for discovery” regular expression may cause deleting thousands of items, triggers, historical values and events.

**Note:**

Discovery rule history is not preserved.

**Form buttons**

Buttons at the bottom of the form allow to perform several operations.

- **Add**
  
  Add a discovery rule. This button is only available for new discovery rules.

- **Update**
  
  Update the properties of a discovery rule. This button is only available for existing discovery rules.

- **Clone**
  
  Create another discovery rule based on the properties of the current discovery rule.
Perform discovery based on the discovery rule immediately. The discovery rule must already exist. See more details. Note that when performing discovery immediately, configuration cache is not updated, thus the result will not reflect very recent changes to discovery rule configuration.

Delete the discovery rule.

Cancel the editing of discovery rule properties.

Item prototypes

Once a rule is created, go to the items for that rule and press “Create item prototype” to create an item prototype.

Note how the {#FSNAME} macro is used where a file system name is required. The use of a low-level discovery macro is mandatory in the item key to make sure that the discovery is processed correctly. When the discovery rule is processed, this macro will be substituted with the discovered file system.
**Name**: Free disk space on {#FSNAME} (percentage)

**Type**: Zabbix agent

**Key**: vs.fs.size(#FSNAME),pfree

**Type of information**: Numeric (float)

**Units**: %

**Update interval**: 1m

**Custom intervals**:

<table>
<thead>
<tr>
<th>Type</th>
<th>Interval</th>
<th>Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flexible</td>
<td>50s</td>
<td>1-7,00:00</td>
</tr>
<tr>
<td>Scheduling</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**History storage period**: 1w

**Trend storage period**: 365d

**Show value**: As is

**New application**

**Applications**

- None
- CPU
- Filesystems
- General
- Memory
- Network interfaces
- OS
- Performance
- Processes
- Security
- Others

**New application prototype**: Application_{#FSNAME}

**Application prototypes**

- None

**Description**

**Create enabled**: ✔️

[Add] [Cancel]
Low-level discovery macros and user macros are supported in item prototype configuration and item value preprocessing parameters. Note that when used in update intervals, a single macro has to fill the whole field. Multiple macros in one field or macros mixed with text are not supported.

**Note:**
Context-specific escaping of low-level discovery macros is performed for safe use in regular expression and XPath preprocessing parameters.

Attributes that are specific for item prototypes:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New application prototype</td>
<td>You may define a new application prototype. In application prototypes you can use low-level discovery macros that, after discovery, will be substituted with real values to create applications that are specific for the discovered entity. See also application discovery notes for more specific information.</td>
</tr>
<tr>
<td>Application prototypes</td>
<td>Select from the existing application prototypes. If checked the item will be added in an enabled state. If unchecked, the item will be added to a discovered entity, but in a disabled state.</td>
</tr>
</tbody>
</table>

We can create several item prototypes for each file system metric we are interested in:

<table>
<thead>
<tr>
<th>NAME</th>
<th>KEY</th>
<th>INTERVAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free disk space on {#FSNAME}</td>
<td>vfs.fs.size[#FSNAME].free</td>
<td>1m</td>
</tr>
<tr>
<td>Free disk space on {#FSNAME} (percentage)</td>
<td>vfs.fs.size[#FSNAME].pfree</td>
<td>1m</td>
</tr>
<tr>
<td>Free inodes on {#FSNAME} (percentage)</td>
<td>vfs.fs.inode[#FSNAME].pfree</td>
<td>1m</td>
</tr>
<tr>
<td>Total disk space on {#FSNAME}</td>
<td>vfs.fs.size[#FSNAME].total</td>
<td>1h</td>
</tr>
<tr>
<td>Used disk space on {#FSNAME}</td>
<td>vfs.fs.size[#FSNAME].used</td>
<td>1m</td>
</tr>
</tbody>
</table>

Trigger prototypes

We create trigger prototypes in a similar way as item prototypes:
### Attributes that are specific for trigger prototypes:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create enabled</td>
<td>If checked the trigger will be added in an enabled state. If unchecked, the trigger will be added to a discovered entity, but in a disabled state.</td>
</tr>
</tbody>
</table>

When real triggers are created from the prototypes, there may be a need to be flexible as to what constant (‘20’ in our example) is used for comparison in the expression. See how [user macros with context](#) can be useful to accomplish such flexibility.

You can define [dependencies](#) between trigger prototypes as well (supported since Zabbix 3.0). To do that, go to the Dependencies tab. A trigger prototype may depend on another trigger prototype from the same low-level discovery (LLD) rule or on a regular
trigger. A trigger prototype may not depend on a trigger prototype from a different LLD rule or on a trigger created from trigger prototype. Host trigger prototype cannot depend on a trigger from a template.

Graph prototypes

We can create graph prototypes, too:

Finally, we have created a discovery rule that looks like shown below. It has five item prototypes, two trigger prototypes, and one graph prototype.
Note: For configuring host prototypes, see the section about host prototype configuration in virtual machine monitoring.

**Discovered entities**

The screenshots below illustrate how discovered items, triggers, and graphs look like in the host’s configuration. Discovered entities are prefixed with an orange link to a discovery rule they come from.

---

Note that discovered entities will not be created in case there are already existing entities with the same uniqueness criteria, for example, an item with the same key or graph with the same name. An error message is displayed in this case in the frontend that the low-level discovery rule could not create certain entities. The discovery rule itself, however, will not turn unsupported because some entity could not be created and had to be skipped. The discovery rule will go on creating/updating other entities.

Items (similarly, triggers and graphs) created by a low-level discovery rule will be deleted automatically if a discovered entity (file system, interface, etc) stops being discovered (or does not pass the filter anymore). In this case the items, triggers and graphs will be deleted after the days defined in the Keep lost resources period field pass.

When discovered entities become ‘Not discovered anymore’, a lifetime indicator is displayed in the item list. Move your mouse pointer over it and a message will be displayed indicating how many days are left until the item is deleted.

If entities were marked for deletion, but were not deleted at the expected time (disabled discovery rule or item host), they will be deleted the next time the discovery rule is processed.

Entities containing other entities, which are marked for deletion, will not update if changed on the discovery rule level. For example, LLD-based triggers will not update if they contain items that are marked for deletion.
Other types of discovery

More detail and how-tos on other types of out-of-the-box discovery is available in the following sections:

- discovery of network interfaces;
- discovery of CPUs and CPU cores;
- discovery of SNMP OIDs;
- discovery of JMX objects;
- discovery using ODBC SQL queries;
- discovery of Windows services;
- discovery of host interfaces in Zabbix.

For more detail on the JSON format for discovery items and an example of how to implement your own file system discoverer as a Perl script, see creating custom LLD rules.

Data limits for return values

There is no limit for low-level discovery rule JSON data if it is received directly by Zabbix server, because return values are processed without being stored in a database. There’s also no limit for custom low-level discovery rules, however, if it is intended to acquire custom LLD data using a user parameter, then user parameter return value limit applies (512 KB).

If data has to go through Zabbix proxy it has to store this data in database so database limits apply, for example, 2048 bytes on a Zabbix proxy run with IBM DB2 database.

Multiple LLD rules for same item

Since Zabbix agent version 3.2 it is possible to define several low-level discovery rules with the same discovery item.

To do that you need to define the Alias agent parameter, allowing to use altered discovery item keys in different discovery rules, for example vfs.fs.discovery[foo], vfs.fs.discovery[bar], etc.

Creating custom LLD rules

It is also possible to create a completely custom LLD rule, discovering any type of entities - for example, databases on a database server.

To do so, a custom item should be created that returns JSON, specifying found objects and optionally - some properties of them. The amount of macros per entity is not limited - while the built-in discovery rules return either one or two macros (for example, two for filesystem discovery), it is possible to return more.
The required JSON format is best illustrated with an example. Suppose we are running an old Zabbix 1.8 agent (one that does not support "vfs.fs.discovery"), but we still need to discover file systems. Here is a simple Perl script for Linux that discovers mounted file systems and outputs JSON, which includes both file system name and type. One way to use it would be as a UserParameter with key "vfs.fs.discovery_perl":

```perl
#!/usr/bin/perl

$first = 1;

print "{";
print "\t"."data":\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"};

    print \t,\n}

print \n	],\n}

print "}";
```

**Attention:**
Allowed symbols for LLD macro names are 0-9, A-Z, _, .
Lowercase letters are not supported in the names.

An example of its output (reformatted for clarity) is shown below. JSON for custom discovery checks has to follow the same format.

```json
{
    "data": [
        {
            "{#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"
        }
    ]
}
```

Then, in the discovery rule's "Filter" field, we could specify "{#FSTYPE}" as a macro and "rootfs|ext3" as a regular expression.

**Note:**
You don't have to use macro names FSNAME/FSTYPE with custom LLD rules, you are free to use whatever names you like.

Note that, if using a user parameter, the return value is limited to 512 KB. For more details, see data limits for LLD return values.

Using LLD macros in user macro contexts

User macros with context can be used to accomplish more flexible thresholds in trigger expressions. Different thresholds may be defined on user macro level and then used in trigger constants depending on the discovered context. Discovered context appears
when the low-level discovery macros used in the macros are resolved to real values.

To illustrate we can use data from the example above and assume that the following file systems will be discovered: /, /home, /tmp, /usr, /var.

We may define a free-disk-space trigger prototype for a host, where the threshold is expressed by a user macro with context:

\[ \{\text{host:vfs.fs.size[#{FSNAME},pfree].last()}\} < \{\text{LOW_SPACE_LIMIT:"#{FSNAME}"}\} \]

Then add user macros:

- \{\text{LOW_SPACE_LIMIT} 10\}
- \{\text{LOW_SPACE_LIMIT:/home} 20\}
- \{\text{LOW_SPACE_LIMIT:/tmp} 50\}

Now, once the file systems are discovered, events will be generated if /, /usr and /var file systems have less than 10% of free disk space, the /home file system - less than 20% of free disk space or the /tmp file system - less than 50% of free disk space.

1 Discovery of mounted filesystems

Overview

It is possible to discover mounted filesystems and their properties (mountpoint name, mountpoint type, filesystem size and inode statistics).

To do that, you may use a combination of:

- the vfs.fs.get agent item (supported since Zabbix 4.0.17) as the master item
- a low-level discovery rule and dependent item prototypes

Configuration

Master item

Create a Zabbix agent item using the following key:

vfs.fs.get

<table>
<thead>
<tr>
<th>Item</th>
<th>Preprocessing</th>
</tr>
</thead>
<tbody>
<tr>
<td>* Name</td>
<td>vfs.fs.get item</td>
</tr>
<tr>
<td>Type</td>
<td>Zabbix agent</td>
</tr>
<tr>
<td>* Key</td>
<td>vfs.fs.get</td>
</tr>
<tr>
<td>* Host interface</td>
<td>192.168.3.205 : 10050</td>
</tr>
</tbody>
</table>

Set the type of information to "Text" for possibly big JSON data.

The data returned by this item will contain something like the following for a mounted filesystem:

```json
{
    "fsname": "/",
    "fstype": "rootfs",
    "bytes": {
        "total": 1000,
        "free": 500,
        "used": 500,
        "pfree": 50.00,
        "pused": 50.00
    }
}
```
Low-level discovery rule

Create a low-level discovery rule using the in-built discovery key:

text

This discovery rule will return discovery macros such as {#FSNAME}, {#FSTYPE} that can be used in creating item prototypes. Dependent item prototype

Create an item prototype with "Dependent item" type in this LLD rule. As master item for this prototype select the vfs.fs.get item we created.

Note the use of macros in the item prototype name and key:

- Name: Free disk space on {#FSNAME}, type: {#FSTYPE}
- Key: Free[{#FSNAME}]

As type of information, use:

- Numeric (unsigned) for metrics like ‘free’, ‘total’, ‘used’
- Numeric (float) for metrics like ‘pfree’, ‘pused’ (percentage)

In the item prototype "Preprocessing" tab select JSONPath and use the following JSONPath expression as parameter:

$.?[@.fsname=='{#FSNAME}']].bytes.free.first()
When discovery starts, one item per each mountpoint will be created. This item will return the number of free bytes for the given mountpoint.

### 1 Discovery of network interfaces

In a similar way as file systems are discovered, it is possible to also discover network interfaces.

**Item key**

The item key to use in the discovery rule is `net.if.discovery`

This item is supported since Zabbix agent 2.0.

**Supported macros**

You may use the `{#IFNAME}` macro in the discovery rule filter and prototypes of items, triggers and graphs.

Examples of item prototypes that you might wish to create based on "net.if.discovery":

- "net.if.in[{#IFNAME},bytes]."
- "net.if.out[{#IFNAME},bytes]."

### 2 Discovery of CPUs and CPU cores

In a similar way as file systems are discovered, it is possible to also discover CPUs and CPU cores.

**Item key**

The item key to use in the discovery rule is `system.cpu.discovery`

This item is supported since Zabbix agent 2.4.

**Supported macros**

This discovery key returns two macros - `{#CPU.NUMBER}` and `{#CPU.STATUS}` identifying the CPU order number and status respectively. Note that a clear distinction cannot be made between actual, physical processors, cores and hyperthreads. `{#CPU.STATUS}` on Linux, UNIX and BSD systems returns the status of the processor, which can be either "online" or "offline". On Windows systems, this same macro may represent a third value - "unknown" - which indicates that a processor has been detected, but no information has been collected for it yet.

CPU discovery relies on the agent’s collector process to remain consistent with the data provided by the collector and save resources on obtaining the data. This has the effect of this item key not working with the test (-t) command-line flag of the agent binary, which will return a NOT_SUPPORTED status and an accompanying message indicating that the collector process has not been started.

Item prototypes that can be created based on CPU discovery include, for example:

- `system.cpu.util[{#CPU.NUMBER}, <type>, <mode>]`
- `system.hw.cpu[{#CPU.NUMBER}, <info>].`

For detailed item key description, see Zabbix agent item keys.

### 3 Discovery of SNMP OIDs

**Overview**

In this section we will perform an SNMP discovery on a switch.

**Item key**
Unlike with file system and network interface discovery, the item does not necessarily have to have an "snmp.discovery" key - item type of SNMP agent is sufficient.

Discovery of SNMP OIDs is supported since Zabbix server/proxy 2.0.

To configure the discovery rule, do the following:

- Go to: Configuration → Templates
- Click on Discovery in the row of an appropriate template
- Click on Create discovery rule in the upper right corner of the screen
- Fill in the discovery rule form with the required details as in the screenshot below

All mandatory input fields are marked with a red asterisk.
The OIDs to discover are defined in SNMP OID field in the following format: discovery[{#MACRO1}, oid1, {#MACRO2}, oid2, ...]

where {#MACRO1}, {#MACRO2} ... are valid Ild macro names and oid1, oid2... are OIDs capable of generating meaningful values for these macros. A built-in macro {#SNMPINDEX} containing index of the discovered OID is applied to discovered entities. The discovered entities are grouped by {#SNMPINDEX} macro value.

To understand what we mean, let us perform few snmpwalks on our switch:

$ 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

And set SNMP OID to: discovery[{#IFDESCR}, ifDescr, {#IFPHYSADDRESS}, ifPhysAddress]

Now this rule will discover entities with {#IFDESCR} macros set to WAN, LAN1 and LAN2, {#IFPHYSADDRESS} macros set to 8:0:27:90:7a:75, 8:0:27:90:7a:76, and 8:0:27:2b:af:9e, {#SNMPINDEX} macros set to the discovered OIDs indexes 1, 2 and 3:

```javascript
{
  "data": [
    {
      "{#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"
    }
  ]
}
```

If an entity does not have the specified OID, then the corresponding macro will be omitted for this entity. For example if we have the following data:

ifDescr.1 "Interface #1"
ifDescr.2 "Interface #2"
ifDescr.4 "Interface #4"

ifAlias.1 "eth0"
ifAlias.2 "eth1"
ifAlias.3 "eth2"
ifAlias.5 "eth4"

Then in this case SNMP discovery discovery[{#IFDESCR}, ifDescr, {#IFALIAS}, ifAlias] will return the following structure:

```javascript
{
  "data": [
    {
      "{#SNMPINDEX}": 1,
      "{#IFDESCR}": "Interface #1",
      "{#IFALIAS}": "eth0"
    },
    {
      
```
The following screenshot illustrates how we can use these macros in item prototypes:
Again, creating as many item prototypes as needed:
The following screenshot illustrates how we can use these macros in trigger prototypes:
The following screenshot illustrates how we can use these macros in graph prototypes:

A summary of our discovery rule:
Discovered entities

When server runs, it will create real items, triggers and graphs based on the values the SNMP discovery rule returns. In the host configuration they are prefixed with an orange link to a discovery rule they come from.
4 Discovery of JMX objects

Overview

It is possible to discover all JMX MBeans or MBean attributes or to specify a pattern for the discovery of these objects.

It is mandatory to understand the difference between Mbean and Mbean attributes for discovery rule configuration. An MBean is an object which can represent a device, an application, or any resource that needs to be managed. For example, there is an MBean which represents a web-server. Its attributes are connection count, thread count, request timeout, http file cache, memory usage, etc. Expressing this thought in human comprehensive language we can define a coffee machine as an MBean which has the following attributes to be monitored: water amount per cup, average consumption of water for a certain period of time, number of coffee beans required per cup, coffee beans and water refill time, etc.

Item key

In discovery rule configuration, select JMX agent in the Type field.

The item key to use is

\[ \text{jmx.discovery[<discovery mode>,<object name>]} \]

where

- discovery mode - one of the following: attributes (retrieve JMX MBean attributes, default) or beans (retrieve JMX MBeans)
- object name - object name pattern identifying the MBean names to be retrieved (empty by default, retrieving all registered beans).

You may consult ObjectName documentation for the options of specifying object name pattern.

If no parameters are passed, all MBean attributes from JMX are requested.

Attention:

Not specifying parameters for JMX discovery or trying to receive all attributes for a wide range like \*:type=*,name=*
may lead to potential performance problems.

This item key is supported since Zabbix Java gateway 3.4.

Item key examples:

- jmx.discovery\#Retrieve all JMX MBean attributes\n- jmx.discovery[beans]\#Retrieve all JMX MBeans\n- jmx.discovery[attributes,"*:type=GarbageCollector,name=*"]\#Retrieve all garbage collector attributes\n- jmx.discovery[beans,\"*:type=GarbageCollector,name=\"]\#Retrieve all garbage collectors

This item returns a JSON object. For example, in the discovery of MBean attributes (reformatted for clarity):

```json
{
  "data": [
    {
      "{#JMXVALUE}": "0",
      "{#JMXTYPE}": "java.lang.Long",
      "{#JMXOBJ}": "java.lang:type=GarbageCollector,name=PS Scavenge",
    }
  ]
}
```
In the discovery of MBeans (reformatted for clarity):
{
  "data": [
    {
      "#JMXDOMAIN": "java.lang",
      "#JMXTYPE": "GarbageCollector",
      "#JMXXOBJ": "java.lang:type=GarbageCollector,name=PS Scavenge",
      "#JMXNAME": "PS Scavenge"
    }
  ]
}

Supported macros

The following macros are supported for use in the discovery rule filter and prototypes of items, triggers and graphs:

<table>
<thead>
<tr>
<th>Macro</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#JMXVALUE</td>
<td>Attribute value.</td>
</tr>
<tr>
<td>#JMXTYPE</td>
<td>Attribute type.</td>
</tr>
<tr>
<td>#JMXXOBJ</td>
<td>Object name.</td>
</tr>
<tr>
<td>#JMXDESC</td>
<td>Object name including attribute name.</td>
</tr>
<tr>
<td>#JMXXATTR</td>
<td>Attribute name.</td>
</tr>
<tr>
<td>#JMXDOMAIN</td>
<td>MBean domain. (Zabbix reserved name)</td>
</tr>
<tr>
<td>#JMXXOBJ</td>
<td>Object name. (Zabbix reserved name)</td>
</tr>
</tbody>
</table>
Macro Description

{#JMX<key property>} MBean properties (like {#JMXTYPE}, {#JMXNAME}). Some important notes to pay attention to when defining MBean attribute name that is created from MBean property name by the following algorithm:

* attribute name case is changed to uppercase;
* attribute name case is ignored (no LLD macro is generated) in case it consists of not supported characters. Supported characters can be described by the following regular expression: “A-Z0-9_.”;
* if an attribute name is called “obj” or “domain” it will be replaced with the values of Zabbix properties {#JMXOBJ} and {#JMXDOMAIN} (supported since Zabbix 3.4.3).

Please consider this jmx.discovery (with “beans” mode) example. MBean has the following properties defined:

```java
name=test
    =Type
attributes []={1,2,3}
Name=NameOfTheTest
domAin=some
```

As a result of JMX discovery, the following LLD macros will be generated:

- {#JMXDOMAIN} - Zabbix internal, describing the domain of MBean
- {#JMXOBJ} - Zabbix internal, describing MBean object
- {#JMXNAME} - created from “name” property

Ignored properties are:

- **type**: its name contains unsupported characters (non-ASCII)
- attributes[]: its name contains unsupported characters (square brackets are not supported)
- Name: it's already defined (name=test)
- domAin: it's a Zabbix reserved name

Let's review two more practical examples of a LLD rule creation with the use of Mbean. To understand the difference between a LLD rule collecting Mbeans and a LLD rule collecting Mbean attributes better please take a look at following table:

<table>
<thead>
<tr>
<th>MBean1</th>
<th>MBean2</th>
<th>MBean3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute1</td>
<td>Attribute1</td>
<td>Attribute1</td>
</tr>
<tr>
<td>Attribute2</td>
<td>Attribute2</td>
<td>Attribute2</td>
</tr>
<tr>
<td>Attribute3</td>
<td>Attribute3</td>
<td>Attribute3</td>
</tr>
</tbody>
</table>

**LLD rule collecting Mbeans**

This rule will return 3 objects: the top row of the column: MBean1, MBean2, MBean3.

For more information about objects please refer to supported macros table, Discovery of MBeans section.

**Discovery rule configuration collecting Mbeans (without the attributes) looks like the following:**

```
jmx.discovery[beans,"*:type=GarbageCollector,name=*"]
```
All the garbage collectors without attributes will be discovered. As Garbage collectors have the same attribute set, we can use desired attributes in item prototypes the following way:

Keys used:

- jmx[#{JMXOBJ},CollectionCount]
- jmx[#{JMXOBJ},CollectionTime]
- jmx[#{JMXOBJ},Valid]

LLD discovery rule will result in something close to this (items are discovered for two Garbage collectors):

LLD rule collecting Mbean attributes

This rule will return 9 objects with the following fields: MBean1Attribute1, MBean2Attribute1, Mbean3Attribute1, MBean1Attribute2, MBean2Attribute2, Mbean3Attribute2, MBean1Attribute3, MBean2Attribute3, Mbean3Attribute3.

For more information about objects please refer to supported macros table, Discovery of MBean attributes section.

Discovery rule configuration collecting Mbean attributes looks like the following:

Key used:

- jmx.discovery[attributes,"*:type=GarbageCollector,name=*"]

All the garbage collectors with a single item attribute will be discovered.
In this particular case an item will be created from prototype for every MBean attribute. The main drawback of this configuration is that trigger creation from trigger prototypes is impossible as there is only one item prototype for all attributes. So this setup can be used for data collection, but is not recommended for automatic monitoring.

5 Discovery using ODBC SQL queries

Overview

This type of low-level discovery is done using SQL queries, whose results get automatically transformed into a JSON object suitable for low-level discovery.

Item key

SQL queries are performed using a “Database monitor” item type. Therefore, most of the instructions on ODBC monitoring page apply in order to get a working “Database monitor” discovery rule, the only difference being that a `db.odbc.discovery[<description>,dsn]` key should be used instead of `db.odbc.select[<description>,dsn]`.

Discovery using SQL queries is supported since Zabbix server/proxy 3.0.

As a practical example to illustrate how the SQL query is transformed into JSON, let us consider low-level discovery of Zabbix proxies by performing an ODBC query on Zabbix database. This is useful for automatic creation of “zabbix[proxy,<name>,lastaccess]” internal items to monitor which proxies are alive.

Let us start with discovery rule configuration:
All mandatory input fields are marked with a red asterisk.

Here, the following direct query on Zabbix database is used to select all Zabbix proxies, together with the number of hosts they are monitoring. The number of hosts can be used, for instance, to filter out empty proxies:

```sql
mysql> SELECT h1.host, COUNT(h2.host) AS count FROM hosts h1 LEFT JOIN hosts h2 ON h1.hostid = h2.proxy_hostid WHERE h1.status IN (5, 6) GROUP BY h1.host;
```

<table>
<thead>
<tr>
<th>host</th>
<th>count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Japan 1</td>
<td>5</td>
</tr>
<tr>
<td>Japan 2</td>
<td>12</td>
</tr>
<tr>
<td>Latvia</td>
<td>3</td>
</tr>
</tbody>
</table>

By the internal workings of "db.odbc.discovery[proxies,{$DSN}]" item, the result of this query gets automatically transformed into the following JSON:

```json
...
```
It can be seen that column names become macro names and selected rows become the values of these macros.

**Note:**
If it is not obvious how a column name would be transformed into a macro name, it is suggested to use column aliases like "COUNT(h2.host) AS count" in the example above.

In case a column name cannot be converted into a valid macro name, the discovery rule becomes not supported, with the error message detailing the offending column number. If additional help is desired, the obtained column names are provided under DebugLevel=4 in Zabbix server log file:

```
$ grep db.odbc.discovery /tmp/zabbix_server.log
```

Now that we understand how a SQL query is transformed into a JSON object, we can use `{#HOST}` macro in item prototypes:
Once discovery is performed, an item will be created for each proxy:

6 Discovery of Windows services

Overview

In a similar way as file systems are discovered, it is possible to also discover Windows services.

Item key

The item to use in the discovery rule is

\texttt{service.discovery}

This item is supported since Zabbix Windows agent 3.0.

Supported macros

The following macros are supported for use in the discovery rule \texttt{filter} and prototypes of items, triggers and graphs:

<table>
<thead>
<tr>
<th>Macro</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>{#SERVICE.NAME}</td>
<td>Service name.</td>
</tr>
</tbody>
</table>
Macro | Description
--- | ---
{#SERVICE.DISPLAYNAME} | Displayed service name.
{#SERVICE.DESCRIPTION} | Service description.
{#SERVICE.STATE} | Numerical value of the service state:
0 - Running
1 - Paused
2 - Start pending
3 - Pause pending
4 - Continue pending
5 - Stop pending
6 - Stopped
7 - Unknown
{#SERVICE.STATENAME} | Name of the service state (Running, Paused, Start pending, Pause pending, Continue pending, Stop pending, Stopped or Unknown).
{#SERVICE.PATH} | Service path.
{#SERVICE.USER} | Service user.
{#SERVICE.STARTUP} | Numerical value of the service startup type:
0 - Automatic
1 - Automatic delayed
2 - Manual
3 - Disabled
4 - Unknown
{#SERVICE.STARTUPNAME} | Name of the service startup type (Automatic, Automatic delayed, Manual, Disabled, Unknown).
{#SERVICE.STARTUPTRIGGER} | Numerical value to indicate if the service startup type has:
0 - no startup triggers
1 - has startup triggers
This macro is supported since Zabbix 3.4.4. It is useful to discover such service startup types as Automatic (trigger start), Automatic delayed (trigger start) and Manual (trigger start).

Based on Windows service discovery you may create an item prototype like

```
service.info[{{SERVICE.NAME},<param>}
```

where param accepts the following values: state, displayname, path, user, startup or description.

For example, to acquire the display name of a service you may use a “service.info[{{SERVICE.NAME},displayname}” item. If param value is not specified (“service.info[{{SERVICE.NAME}]”), the default state parameter is used.

7 Discovery of host interfaces in Zabbix

Overview

It is possible to discover all interfaces configured in Zabbix frontend for a host.

Item key

The item to use in the discovery rule is the

```
zabbix[host,discovery,interfaces]
```

internal item. This item is supported since Zabbix server 3.4.

This item returns a JSON with the description of interfaces, including:

- IP address/DNS hostname (depending on the “Connect to” host setting)
- Port number
- Interface type (Zabbix agent, SNMP, JMX, IPMI)
- If it is the default interface or not
- If the bulk request feature is enabled - for SNMP interfaces only.

For example:

```
{"data":[{"#IF.CONN}":"192.168.3.1","{#IF.IP}":"192.168.3.1","{#IF.DNS}"":"","{#IF.PORT}":"10050"},{#IF.TYPE}]
```
With multiple interfaces their records in JSON are ordered by:

- Interface type,
- Default - the default interface is put before non-default interfaces,
- Interface ID (in ascending order).

Supported macros

The following macros are supported for use in the discovery rule filter and prototypes of items, triggers and graphs:

<table>
<thead>
<tr>
<th>Macro</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>{#IF.CONN}</td>
<td>Interface IP address or DNS host name.</td>
</tr>
<tr>
<td>{#IF.IP}</td>
<td>Interface IP address.</td>
</tr>
<tr>
<td>{#IF.DNS}</td>
<td>Interface DNS host name.</td>
</tr>
<tr>
<td>{#IF.PORT}</td>
<td>Interface port number.</td>
</tr>
<tr>
<td>{#IF.TYPE}</td>
<td>Interface type (&quot;AGENT&quot;, &quot;SNMP&quot;, &quot;JMX&quot;, or &quot;IPMI&quot;).</td>
</tr>
<tr>
<td>{#IF.DEFAULT}</td>
<td>Default status for the interface:</td>
</tr>
<tr>
<td></td>
<td>0 - not default interface</td>
</tr>
<tr>
<td></td>
<td>1 - default interface</td>
</tr>
<tr>
<td>{#IF.SNMP.BULK}</td>
<td>SNMP bulk processing status for the interface:</td>
</tr>
<tr>
<td></td>
<td>0 - disabled</td>
</tr>
<tr>
<td></td>
<td>1 - enabled</td>
</tr>
</tbody>
</table>
| This macro is returned only if interface type is “SNMP”.

Notes on low-level discovery

Application discovery

Application prototypes support LLD macros.

One application prototype can be used by several item prototypes of the same discovery rule.

If created application prototype is not used by any item prototype it gets removed from 'Application prototypes' list automatically.

Like other discovered entities applications follow the lifetime defined in discovery rule ('keep lost resources period' setting) - they are removed after not being discovered for the specified number of days.

If an application is not discovered anymore, the application itself may not be removed because of the 'lost resources period' setting, however:

- items that are still discovered are automatically removed from it;
- items that are no longer discovered are not removed from it (note that they would be removed before Zabbix 4.0.18).

Application prototypes defined by one discovery rule can't discover the same application. In this situation only the first prototype discovery will succeed, the rest will report appropriate LLD error. Only application prototypes defined in different discovery rules can result in discovering the same application.

16. Distributed monitoring

Overview

Zabbix provides an effective and reliable way of monitoring a distributed IT infrastructure using Zabbix proxies.

Proxies can be used to collect data locally on behalf of a centralized Zabbix server and then report the data to the server.

<table>
<thead>
<tr>
<th>Proxy Feature</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lightweight</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GUI</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Works independently</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Easy maintenance</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Automatic DB creation¹</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Local administration</td>
<td></td>
<td>No</td>
</tr>
</tbody>
</table>
### 1 Proxies

**Overview**

A Zabbix proxy can collect performance and availability data on behalf of the Zabbix server. This way, a proxy can take on itself some of the load of collecting data and offload the Zabbix server.

Also, using a proxy is the easiest way of implementing centralized and distributed monitoring, when all agents and proxies report to one Zabbix server and all data is collected centrally.

A Zabbix proxy can be used to:

- Monitor remote locations
- Monitor locations having unreliable communications
- Offload the Zabbix server when monitoring thousands of devices
- Simplify the maintenance of distributed monitoring

The proxy requires only one TCP connection to the Zabbix server. This way it is easier to get around a firewall as you only need to configure one firewall rule.

**Attention:**
Zabbix proxy must use a separate database. Pointing it to the Zabbix server database will break the configuration.

All data collected by the proxy is stored locally before transmitting it over to the server. This way no data is lost due to any temporary communication problems with the server. The ProxyLocalBuffer and ProxyOfflineBuffer parameters in the proxy configuration file control for how long the data are kept locally.

**Attention:**
It may happen that a proxy, which receives the latest configuration changes directly from Zabbix server database, has a more up-to-date configuration than Zabbix server whose configuration may not be updated as fast due to the value of CacheUpdateFrequency. As a result, proxy may start gathering data and send them to Zabbix server that ignores these data.
Zabbix proxy is a data collector. It does not calculate triggers, process events or send alerts. For an overview of what proxy functionality is, review the following table:

<table>
<thead>
<tr>
<th>Function</th>
<th>Supported by proxy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Items</strong></td>
<td></td>
</tr>
<tr>
<td>Zabbix agent checks</td>
<td>Yes</td>
</tr>
<tr>
<td>Zabbix agent checks (active)</td>
<td>Yes [1]</td>
</tr>
<tr>
<td>Simple checks</td>
<td>Yes</td>
</tr>
<tr>
<td>Trapper items</td>
<td>Yes</td>
</tr>
<tr>
<td>SNMP checks</td>
<td>Yes</td>
</tr>
<tr>
<td>SNMP traps</td>
<td>Yes</td>
</tr>
<tr>
<td>IPMI checks</td>
<td>Yes</td>
</tr>
<tr>
<td>JMX checks</td>
<td>Yes</td>
</tr>
<tr>
<td>Log file monitoring</td>
<td>Yes</td>
</tr>
<tr>
<td>Internal checks</td>
<td>Yes</td>
</tr>
<tr>
<td>SSH checks</td>
<td>Yes</td>
</tr>
<tr>
<td>Telnet checks</td>
<td>Yes</td>
</tr>
<tr>
<td>External checks</td>
<td>Yes</td>
</tr>
<tr>
<td>Dependent items</td>
<td>Yes [2]</td>
</tr>
<tr>
<td>Built-in web monitoring</td>
<td>Yes</td>
</tr>
<tr>
<td>Network discovery</td>
<td>Yes</td>
</tr>
<tr>
<td>Low-level discovery</td>
<td>Yes</td>
</tr>
<tr>
<td>Remote commands</td>
<td>Yes</td>
</tr>
<tr>
<td>Calculating triggers</td>
<td>No</td>
</tr>
<tr>
<td>Processing events</td>
<td>No</td>
</tr>
<tr>
<td>Event correlation</td>
<td>No</td>
</tr>
<tr>
<td>Sending alerts</td>
<td>No</td>
</tr>
<tr>
<td>Item value preprocessing</td>
<td>No</td>
</tr>
</tbody>
</table>

**Note:**

[1] To make sure that an agent asks the proxy (and not the server) for active checks, the proxy must be listed in the **ServerActive** parameter in the agent configuration file.

[2] Item value preprocessing by Zabbix server is required to extract the required value from the master item data.

Configuration

Once you have installed and configured a proxy, it is time to configure it in the Zabbix frontend.

Adding proxies

To configure a proxy in Zabbix frontend:

- Go to: Administration → Proxies
- Click on Create proxy

![Proxy Configuration Form](image)
### Parameter Description

- **Proxy name**: Enter the proxy name. It must be the same name as in the Hostname parameter in the proxy configuration file.

- **Proxy mode**:
  - **Active**: The proxy will connect to the Zabbix server and request configuration data.
  - **Passive**: Zabbix server connects to the proxy.

  Note that without encrypted communications (sensitive) proxy configuration data may become available to parties having access to the Zabbix server trapper port when using an active proxy. This is possible because anyone may pretend to be an active proxy and request configuration data if authentication does not take place or proxy addresses are not limited in the Proxy address field.

- **Proxy address**: If specified then active proxy requests are only accepted from this list of comma-delimited IP addresses, optionally in CIDR notation, or DNS names of active Zabbix proxy. This field is only available if an active proxy is selected in the Proxy mode field. Macros are not supported. This option is supported since Zabbix 4.0.0.

- **Interface**:

  - **IP address**: IP address of the passive proxy (optional).
  - **DNS name**: DNS name of the passive proxy (optional).

  Connect to

  - **IP**: Connect to the proxy IP address (recommended)
  - **DNS**: Connect to the proxy DNS name

  Port

  - TCP/UDP port number of the passive proxy (10051 by default).

- **Description**: Enter the proxy description.

---

### The Encryption tab allows you to require encrypted connections with the proxy.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connections to proxy</td>
<td>How the server connects to the passive proxy: no encryption (default), using PSK (pre-shared key) or certificate.</td>
</tr>
<tr>
<td>Connections from proxy</td>
<td>Select what type of connections are allowed from the active proxy. Several connection types can be selected at the same time (useful for testing and switching to other connection type). Default is “No encryption”.</td>
</tr>
<tr>
<td>Issuer</td>
<td>Allowed issuer of certificate. Certificate is first validated with CA (certificate authority). If it is valid, signed by the CA, then the Issuer field can be used to further restrict allowed CA. This field is optional, intended to use if your Zabbix installation uses certificates from multiple CAs.</td>
</tr>
<tr>
<td>Subject</td>
<td>Allowed subject of certificate. Certificate is first validated with CA. If it is valid, signed by the CA, then the Subject field can be used to allow only one value of Subject string. If this field is empty then any valid certificate signed by the configured CA is accepted.</td>
</tr>
<tr>
<td>PSK identity</td>
<td>Pre-shared key identity string. Do not put sensitive information in the PSK identity, it is transmitted unencrypted over the network to inform a receiver which PSK to use.</td>
</tr>
</tbody>
</table>
### Encryption

#### Overview
Zabbix supports encrypted communications between Zabbix components using Transport Layer Security (TLS) protocol v.1.2 and 1.3 (depending on the crypto library). Certificate-based and pre-shared key-based encryption is supported.

Encryption can be configured between Zabbix server, Zabbix proxy, Zabbix agent, zabbix_sender and zabbix_get utilities.

Encryption is optional and configurable for individual components:

- Some proxies and agents can be configured to use certificate-based encryption with the server, while others can use pre-shared key-based encryption, and yet others continue with unencrypted communications (as before)
- Server (proxy) can use different encryption configurations for different hosts

Zabbix daemon programs use one listening port for encrypted and unencrypted incoming connections. Adding an encryption does not require opening new ports on firewalls.

#### Limitations

- Private keys are stored in plain text in files readable by Zabbix components during startup
- Pre-shared keys are entered in Zabbix frontend and stored in Zabbix database in plain text
- Built-in encryption does not protect communications:
  - Between the web server running Zabbix frontend and user web browser
  - Between Zabbix frontend and Zabbix server
  - Between Zabbix server (proxy) and Zabbix database
- Currently each encrypted connection opens with a full TLS handshake, no session caching and tickets are used
- Adding encryption increases the time for item checks and actions, depending on network latency:
  - For example, if packet delay is 100ms then opening a TCP connection and sending unencrypted request takes around 200ms. With encryption about 1000 ms are added for establishing the TLS connection;
  - Timeouts may need to be increased, otherwise some items and actions running remote scripts on agents may not complete
- Encryption is not supported by [[/manual/discovery/network_discovery|network discovery]]. Zabbix agent checks will be unencrypted and if Zabbix agent is configured to reject unencrypted connections such checks will not succeed.

#### Compiling Zabbix with encryption support
To support encryption Zabbix must be compiled and linked with one of four crypto libraries:

- GnuTLS - from version 3.1.18
- OpenSSL - versions 1.0.1, 1.0.2, 1.1.0 (OpenSSL 1.1.1 is supported since Zabbix 4.0.1).
- LibreSSL (supported since Zabbix 4.0.6) - tested with versions 2.7.4, 2.8.2:
  - LibreSSL 2.6.x is not supported
  - LibreSSL is supported as a compatible replacement of OpenSSL; the new tls_*() LibreSSL-specific API functions are not used. Zabbix components compiled with LibreSSL will not be able to use PSK, only certificates can be used.
- mbed TLS (formerly PolarSSL) - version 1.3.9 and later 1.3.x:
- mbed TLS 2.x is not currently supported; it is not a drop-in replacement for the 1.3 branch, Zabbix will not compile with mbed TLS 2.x.

The library is selected by specifying the respective option to “configure” script:

- `--with-gnutls [=DIR]`
- `--with-openssl [=DIR]` (also used for LibreSSL)
- `--with-mbedtls [=DIR]`

For example, to configure the sources for server and agent with OpenSSL you may use something like:

```
./configure --enable-server --enable-agent --with-mysql --enable-ipv6 --with-net-snmp --with-libcurl --with-libxml2 --with-openssl
```

Different Zabbix components may be compiled with different crypto libraries (e.g. a server with OpenSSL, an agent with GnuTLS).

**Attention:**
If you plan to use pre-shared keys (PSK) consider using GnuTLS or mbed TLS libraries in Zabbix components using PSKs. GnuTLS and mbed TLS libraries support PSK ciphersuites with **Perfect Forward Secrecy**. OpenSSL library (versions 1.0.1, 1.0.2c) does support PSKs but available PSK ciphersuites do not provide Perfect Forward Secrecy.

**Connection encryption management**
Connections in Zabbix can use:

- no encryption (default)
- RSA certificate-based encryption
- PSK-based encryption

There are two important parameters used to specify encryption between Zabbix components:

- `TLSConnect` - specifies what encryption to use for outgoing connections (unencrypted, PSK or certificate)
- `TLSAccept` - specifies what types of connections are allowed for incoming connections (unencrypted, PSK or certificate). One or more values can be specified.

`TLSConnect` is used in the configuration files for Zabbix proxy (in active mode, specifies only connections to server) and Zabbix agent (for active checks). In Zabbix frontend the `TLSConnect` equivalent is the Connections to host field in Configuration → Hosts → `<some host>` → Encryption tab and the Connections to proxy field in Administration → Proxies → `<some proxy>` → Encryption tab. If the configured encryption type for connection fails, no other encryption types will be tried.

`TLSAccept` is used in the configuration files for Zabbix proxy (in passive mode, specifies only connections from server) and Zabbix agent (for passive checks). In Zabbix frontend the `TLSAccept` equivalent is the Connections from host field in Configuration → Hosts → `<some host>` → Encryption tab and the Connections from proxy field in Administration → Proxies → `<some proxy>` → Encryption tab.

Normally you configure only one type of encryption for incoming encryptions. But you may want to switch the encryption type, e.g. from unencrypted to certificate-based with minimum downtime and rollback possibility. To achieve this:

- Set `TLSAccept=unencrypted, cert` in the agent configuration file and restart Zabbix agent.
- Test connection with `zabbix_get` to the agent using certificate. If it works, you can reconfigure encryption for that agent in Zabbix frontend in the Configuration → Hosts → `<some host>` → Encryption tab by setting Connections to host to "Certificate".
- When server configuration cache gets updated (and proxy configuration is updated if the host is monitored by proxy) then connections to that agent will be encrypted.
- If everything works as expected you can set `TLSAccept=cert` in the agent configuration file and restart Zabbix agent. Now the agent will be accepting only encrypted certificate-based connections. Unencrypted and PSK-based connections will be rejected.

In a similar way it works on server and proxy. If in Zabbix frontend in host configuration Connections from host is set to "Certificate" then only certificate-based encrypted connections will be accepted from the agent (active checks) and `zabbix_sender` (trapper items).

Most likely you will configure incoming and outgoing connections to use the same encryption type or no encryption at all. But technically it is possible to configure it asymmetrically, e.g. certificate-based encryption for incoming and PSK-based for outgoing connections.

Encryption configuration for each host is displayed in the Zabbix frontend, in Configuration → Hosts in the Agent encryption column. For example:

<table>
<thead>
<tr>
<th>Example</th>
<th>Connections to host</th>
<th>Allowed connections from host</th>
<th>Rejected connections from host</th>
</tr>
</thead>
<tbody>
<tr>
<td>NONE</td>
<td>Unencrypted</td>
<td>Unencrypted</td>
<td>Encrypted, certificate and PSK-based encrypted</td>
</tr>
</tbody>
</table>
### Example Connections to host

<table>
<thead>
<tr>
<th>Connections to host</th>
<th>Allowed connections from host</th>
<th>Rejected connections from host</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypted,</td>
<td>Encrypted, certificate-based</td>
<td>Unencrypted and PSK-based encrypted</td>
</tr>
<tr>
<td>certificate-based</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encrypted, PSK-based</td>
<td>Encrypted, PSK-based</td>
<td>Unencrypted and certificate-based encrypted</td>
</tr>
<tr>
<td>Encrypted, PSK-based</td>
<td>Unencrypted and PSK-based encrypted</td>
<td>Certificate-based encrypted</td>
</tr>
<tr>
<td>Encrypted,</td>
<td>Unencrypted, PSK or certificate-based</td>
<td></td>
</tr>
<tr>
<td>certificate-based</td>
<td>encrypted</td>
<td></td>
</tr>
</tbody>
</table>

**Attention:**
Connections are unencrypted by default. Encryption must be configured for each host and proxy individually.

**zabbix_get and zabbix_sender with encryption**
See zabbix_get and zabbix_sender manpages for using them with encryption.

**Ciphersuites**
Ciphersuites by default are configured internally during Zabbix startup and, before Zabbix 4.0.19, are not user-configurable.

Since Zabbix 4.0.19 also user-configured ciphersuites are supported for GnuTLS and OpenSSL. Users may configure ciphersuites according to their security policies. Using this feature is optional (built-in default ciphersuites still work).

For crypto libraries compiled with default settings Zabbix built-in rules typically result in the following ciphersuites (in order from higher to lower priority):

<table>
<thead>
<tr>
<th>Library</th>
<th>Certificate ciphersuites</th>
<th>PSK ciphersuites</th>
</tr>
</thead>
<tbody>
<tr>
<td>mbed TLS (PolarSSL) 1.3.9</td>
<td>TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256</td>
<td>TLS-ECDHE-PSK-WITH-AES-128-CBC-SHA256</td>
</tr>
<tr>
<td>GnuTLS 3.1.18</td>
<td>TLS_ECDHE_RSA_AES_128_GCM_SHA256</td>
<td>TLS_ECDHE_PSK_AES_128_CBC_SHA256</td>
</tr>
<tr>
<td>OpenSSL 1.0.2c</td>
<td>ECDHE-RSA-AES128-GCM-SHA256</td>
<td>PSK-AES128-CBC-SHA</td>
</tr>
<tr>
<td>OpenSSL 1.1.0</td>
<td>ECDHE-RSA-AES128-GCM-SHA256</td>
<td>ECDHE-PSK-AES128-CBC-SHA256</td>
</tr>
</tbody>
</table>

**Cipher suites using certificates:**

<table>
<thead>
<tr>
<th>TLS client</th>
<th>TLS server</th>
<th>GnuTLS</th>
<th>OpenSSL 1.0.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>GnuTLS</td>
<td>TLS_ECDHE_RSA_AES_128_CBC_SHA256</td>
<td>TLS_ECDHE_RSA_AES_128_CBC_SHA256</td>
<td>TLS_ECDHE_RSA_AES_128_CBC_SHA256</td>
</tr>
<tr>
<td>OpenSSL 1.0.2</td>
<td>ECDHE-RSA-AES128-GCM-SHA256</td>
<td>ECDHE-PSK-AES128-CBC-SHA256</td>
<td>TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256</td>
</tr>
<tr>
<td>Ciphersuites using PSK:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>TLS server</strong></td>
<td><strong>TLS client</strong></td>
<td><strong>GnuTLS</strong></td>
<td><strong>OpenSSL 1.0.2</strong></td>
</tr>
<tr>
<td>TLS-PSK-WITH-AES-128-CBC-SHA</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**User-configured ciphersuites**  The built-in ciphersuite selection criteria can be overridden with user-configured ciphersuites (since Zabbix 4.0.19).

### Attention:
User-configured ciphersuites is a feature intended for advanced users who understand TLS ciphersuites, their security and consequences of mistakes, and who are comfortable with TLS troubleshooting.

The built-in ciphersuite selection criteria can be overridden using the following parameters:

<table>
<thead>
<tr>
<th>Override scope</th>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ciphersuite selection for certificates</td>
<td>TLSCipherCert13</td>
<td>Valid OpenSSL 1.1.1 cipher strings for TLS 1.3 protocol (their values are passed to the OpenSSL function SSL_CTX_set_ciphersuites()). Only OpenSSL 1.1.1 or newer.</td>
<td>Certificate-based ciphersuite selection criteria for TLS 1.3</td>
</tr>
<tr>
<td></td>
<td>TLSCipherCert</td>
<td>Valid OpenSSL cipher strings for TLS 1.2 or valid GnuTLS priority strings. Their values are passed to the SSL_CTX_set_cipher_list() or gnutls_priority_init() functions, respectively.</td>
<td>Certificate-based ciphersuite selection criteria for TLS 1.2/1.3 (GnuTLS), TLS 1.2 (OpenSSL)</td>
</tr>
<tr>
<td>Override scope</td>
<td>Parameter</td>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------</td>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Ciphersuite selection for PSK</td>
<td>TLSCipherPSK13</td>
<td>Valid OpenSSL 1.1.1 cipher strings for TLS 1.3 protocol (their values are passed to the OpenSSL function <code>SSL_CTX_set_ciphersuites()</code>).</td>
<td>PSK-based ciphersuite selection criteria for TLS 1.3. Only OpenSSL 1.1.1 or newer.</td>
</tr>
<tr>
<td></td>
<td>TLSCipherPSK</td>
<td>Valid OpenSSL cipher strings for TLS 1.2 or valid GnuTLS priority strings. Their values are passed to the <code>SSL_CTX_set_cipher_list()</code> or <code>gnutls_priority_init()</code> functions, respectively.</td>
<td>PSK-based ciphersuite selection criteria for TLS 1.2/1.3 (GnuTLS), TLS 1.2 (OpenSSL).</td>
</tr>
<tr>
<td>Combined ciphersuite list for certificate and PSK</td>
<td>TLSCipherAll13</td>
<td>Valid OpenSSL 1.1.1 cipher strings for TLS 1.3 protocol (their values are passed to the OpenSSL function <code>SSL_CTX_set_ciphersuites()</code>).</td>
<td>Ciphersuite selection criteria for TLS 1.3. Only OpenSSL 1.1.1 or newer.</td>
</tr>
<tr>
<td></td>
<td>TLSCipherAll</td>
<td>Valid OpenSSL cipher strings for TLS 1.2 or valid GnuTLS priority strings. Their values are passed to the <code>SSL_CTX_set_cipher_list()</code> or <code>gnutls_priority_init()</code> functions, respectively.</td>
<td>Ciphersuite selection criteria for TLS 1.2/1.3 (GnuTLS), TLS 1.2 (OpenSSL).</td>
</tr>
</tbody>
</table>

To override the ciphersuite selection in **zabbix_get** and **zabbix_sender** utilities - use the command-line parameters:

- `--tls-cipher13`
- `--tls-cipher`

The new parameters are optional. If a parameter is not specified, the internal default value is used. If a parameter is defined it cannot be empty.

If the setting of a TLSCipher* value in the crypto library fails then the server, proxy or agent will not start and an error is logged.

It is important to understand when each parameter is applicable.

Outgoing connections

The simplest case is outgoing connections:
• For outgoing connections with certificate - use TLSCipherCert13 or TLSCipherCert
• For outgoing connections with PSK - use TLSCipherPSK13 and TLSCipherPSK
• In case of zabbix_get and zabbix_sender utilities the command-line parameters --tls-cipher13 and --tls-cipher can be used (encryption is unambiguously specified with a --tls-connect parameter)

Incoming connections

It is a bit more complicated with incoming connections because rules are specific for components and configuration.

For Zabbix **agent**:

<table>
<thead>
<tr>
<th>Agent connection setup</th>
<th>Cipher configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLSConnect=cert</td>
<td>TLSCipherCert, TLSCipherCert13</td>
</tr>
<tr>
<td>TLSConnect=psk</td>
<td>TLSCipherPSK, TLSCipherPSK13</td>
</tr>
<tr>
<td>TLSAccept=cert</td>
<td>TLSCipherCert, TLSCipherCert13</td>
</tr>
<tr>
<td>TLSAccept=psk</td>
<td>TLSCipherPSK, TLSCipherPSK13</td>
</tr>
<tr>
<td>TLSAccept=cert,psk</td>
<td>TLSCipherAll, TLSCipherAll13</td>
</tr>
</tbody>
</table>

For Zabbix **server** and **proxy**:

<table>
<thead>
<tr>
<th>Connection setup</th>
<th>Cipher configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outgoing connections using PSK</td>
<td>TLSCipherPSK, TLSCipherPSK13</td>
</tr>
<tr>
<td>Incoming connections using certificates</td>
<td>TLSCipherAll, TLSCipherAll13</td>
</tr>
<tr>
<td>Incoming connections using PSK if server has no certificate</td>
<td>TLSCipherPSK, TLSCipherPSK13</td>
</tr>
<tr>
<td>Incoming connections using PSK if server has certificate</td>
<td>TLSCipherAll, TLSCipherAll13</td>
</tr>
</tbody>
</table>

Some pattern can be seen in the two tables above:

- TLSCipherAll and TLSCipherAll13 can be specified only if a combined list of certificate- and PSK-based ciphersuites is used. There are two cases when it takes place: server (proxy) with a configured certificate (PSK ciphersuites are always configured on server, proxy if crypto library supports PSK), agent configured to accept both certificate- and PSK-based incoming connections
- in other cases TLSCipherCert* and/or TLSCipherPSK* are sufficient

The following tables show the TLSCipher* built-in default values. They could be a good starting point for your own custom values.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>GnuTLS 3.6.12</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>OpenSSL 1.1.1d 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLSCipherCert13</td>
<td>ECDH+aRSA+AES128:RSA+aRSA+AES128</td>
</tr>
<tr>
<td>TLSCipherCert</td>
<td>TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td>TLSCipherPSK13</td>
<td>kECDHEPSK+AES128:kPSK+AES128</td>
</tr>
<tr>
<td>TLSCipherPSK</td>
<td>kECDHEPSK+AES128:kPSK+AES128</td>
</tr>
<tr>
<td>TLSCipherAll13</td>
<td>ECDH+aRSA+AES128:RSA+aRSA+AES128:kECDHEPSK+AES128:kPSK+AES128</td>
</tr>
</tbody>
</table>

1 Default values are different for older OpenSSL versions (1.0.1, 1.0.2, 1.1.0), for LibreSSL and if OpenSSL is compiled without PSK support.

** Examples of user-configured ciphersuites **

See below the following examples of user-configured ciphersuites:
Testing cipher strings and allowing only PFS ciphersuites

Switching from AES128 to AES256

To see which ciphersuites have been selected you need to set `DebugLevel=4` in the configuration file, or use the `-vv` option for `zabbix_sender`.

Some experimenting with TLSCipher* parameters might be necessary before you get the desired ciphersuites. It is inconvenient to restart Zabbix server, proxy or agent multiple times just to tweak TLSCipher* parameters. More convenient options are using `zabbix_sender` or the `openssl` command. Let’s show both.

1. Using `zabbix_sender`.

Let’s make a test configuration file, for example `/home/zabbix/test.conf`, with the syntax of a `zabbix_agentd.conf` file:

```
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
```

You need valid CA and agent certificates and PSK for this example. Adjust certificate and PSK file paths and names for your environment.

If you are not using certificates, but only PSK, you can make a simpler test file:

```
Hostname=nonexisting
ServerActive=nonexisting

TLSConnect=psk
TLSPSKIdentity=nonexisting
TLSPSKFile=/home/zabbix/agentd.psk
```

The selected ciphersuites can be seen by running `zabbix_sender` (example compiled with OpenSSL 1.1.d):

```
$ zabbix_sender -vv -c /home/zabbix/test.conf -k nonexisting_item -o 1 2>&1 | grep ciphersuites
```

Here you see the ciphersuites selected by default. These default values are chosen to ensure interoperability with Zabbix agents running on systems with older OpenSSL versions (from 1.0.1).

With newer systems you can choose to tighten security by allowing only a few ciphersuites, e.g. only ciphersuites with PFS (Perfect Forward Secrecy). Let’s try to allow only ciphersuites with PFS using TLSCipher* parameters.

Add two lines to the `test.conf` configuration file:

```
TLSCipherCert=EECDH+aRSA+AES128
TLSCipherPSK=kECDHEPSK+AES128
```

and test again:

```
$ zabbix_sender -vv -c /home/zabbix/test.conf -k nonexisting_item -o 1 2>&1 | grep ciphersuites
```

The "certificate ciphersuites" and "PSK ciphersuites" lists have changed - they are shorter than before, only containing TLS 1.3 ciphersuites and TLS 1.2 ECDHE-* ciphersuites as expected.

### Attention:

The result will not be interoperable with systems using OpenSSL 1.0.1 and 1.0.2, if PSK is used. Certificate-based encryption should work.
2. TLSCipherAll and TLSCipherAll13 cannot be tested with zabbix_sender; they do not affect "certificate and PSK ciphersuites" value shown in the example above. To tweak TLSCipherAll and TLSCipherAll13 you need to experiment with the agent, proxy or server.

So, to allow only PFS ciphersuites you may need to add up to three parameters

```
TLSCipherCert=EECDH+aRSA+AES128
TLSCipherPSK=kECDHEPSK+AES128
TLSCipherAll=EECDH+aRSA+AES128:kECDHEPSK+AES128
```

to zabbix_agentd.conf, zabbix_proxy.conf and zabbix_server_conf if each of them has a configured certificate and agent has also PSK.

If your Zabbix environment uses only PSK-based encryption and no certificates, then only one:

```
TLSCipherPSK=kECDHEPSK+AES128
```

Now that you understand how it works you can test the ciphersuite selection even outside of Zabbix, with the openssl command.

Let's test all three TLSCipher* parameter values:

```
$ openssl ciphers EECDH+aRSA+AES128 | sed 's/:/ /g'
```

You may prefer openssl ciphers with option -V for a more verbose output:

```
$ 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=ECDHE Au=RSA Enc=AESGCM(128) Mac=AEAD
0xC0,0x27 - ECDHE-RSA-AES128-SHA256 TLSv1.2 Kx=ECDHE Au=RSA Enc=AES(128) Mac=SHA256
0xC0,0x13 - ECDHE-RSA-AES128-SHA TLSv1 Kx=ECDHE 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-TLSv1 Kx=ECDHEPSK Au=PSK Enc=AES(128) Mac=SHA1
```

Similarly, you can test the priority strings for GnuTLS:

```
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, GROUP-FFDHE3072, GROUP-FFDHE4096, GROUP-FFDHE521, GROUP-FFDHE6144, GROUP-FFDHE8192
PK-signatures: SIGN-RSA-SHA256, SIGN-RSA-PSS-SHA256, SIGN-RSA-PSS-RSAE-SHA256, SIGN-ECDSA-SHA256, ...

Switching from AES128 to AES256

Zabbix uses AES128 as the built-in default for data. Let's assume you are using certificates and want to switch to AES256, on OpenSSL 1.1.1.

This can be achieved by adding the respective parameters in zabbix_server.conf:

```
TLSCAFilename=/home/zabbix/ca.crt
TLSCertFilename=/home/zabbix/server.crt
TLSSKeyFilename=/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
```

601
Attention:
Although only certificate-related ciphersuites will be used, TLSCipherPSK* parameters are defined as well to avoid their default values which include less secure ciphers for wider interoperability. PSK ciphersuites cannot be completely disabled on server/proxy.

And in zabbix_agentd.conf:

    TLSConnect=cert
    TLAcept=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 Using certificates

Overview
Zabbix can use RSA certificates in PEM format, signed by a public or in-house certificate authority (CA). Certificate verification is done against a pre-configured CA certificate. Optionally certificate revocation lists (CRL) can be used. Each Zabbix component can have only one certificate configured.

For more information how to set up and operate internal CA, how to generate certificate requests and sign them, how to revoke certificates you can find numerous online how-tos, for example, OpenSSLPKI Tutorial v1.1.

Carefully consider and test your certificate extensions - see Limitations on using X.509 v3 certificate extensions.

Certificate configuration parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Mandatory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLSCAFile</td>
<td>*</td>
<td>Full pathname of a file containing the top-level CA(s) certificates for peer certificate verification. In case of certificate chain with several members they must be ordered: lower level CA certificates first followed by certificates of higher level CA(s). Certificates from multiple CA(s) can be included in a single file.</td>
</tr>
<tr>
<td>TLSCertFile</td>
<td>*</td>
<td>Full pathname of a file containing certificate (certificate chain). In case of certificate chain with several members they must be ordered: server, proxy, or agent certificate first, followed by lower level CA certificates then certificates of higher level CA(s).</td>
</tr>
<tr>
<td>TLSKeyFile</td>
<td>*</td>
<td>Full pathname of a file containing private key. Set access rights to this file - it must be readable only by Zabbix user.</td>
</tr>
<tr>
<td>TLSServerCertIssuer</td>
<td></td>
<td>Allowed server certificate issuer.</td>
</tr>
<tr>
<td>TLSServerCertSubject</td>
<td></td>
<td>Allowed server certificate subject.</td>
</tr>
</tbody>
</table>

Configuring certificate on Zabbix server

1. In order to verify peer certificates, Zabbix server must have access to file with their top-level self-signed root CA certificates. For example, if we expect certificates from two independent root CAs, we can put their certificates into file /home/zabbix/zabbix_ca_file like this:
```plaintext
2. Put Zabbix server certificate chain into file, for example, /home/zabbix/zabbix_server.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+MRMwEQYKCIZImiZPyLGQB....
9wEzdN8uTrqoyU78gi12mjpLj08LegRKjb5hFTVm0
-----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-----
MIID3DCCAsKgAwIBAgIBATANBgkqhkiG9w0BAQUFADB/MRMwEQYKCIZImiZPyLGQB....
vdGNYoSfvu4lQQR5v5FvJxJ5Q3B6894GY1zY=
-----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=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

603
```
X509v3 Basic Constraints:
CA:FALSE

-----BEGIN CERTIFICATE-----
MIIECDCCAvCgAwIBAgIBATANBgkqhkiG9w0BAQUFADCBgTETMBEGCgmSJomT8ixk...h02u1GIy46GI+xfR3LsPWk1kTaaLal/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+MRMwEQYKCIz4imtZPyLQGB...
dyGeWvL7u5sd6fff0iRny0QzbHKmQt/wUt+cVivWXdMIFJMOHw==
-----END CERTIFICATE-----

Here the first is Zabbix server certificate, followed by intermediate CA certificate.

3. Put Zabbix server private key into file, for example, /home/zabbix/zabbix_server.key:

     -----BEGIN PRIVATE KEY-----
MIIwAIBAfIwAAIGkqhkkiGv0BAQUFADB+MRMwEQYKCIz4imtZPyLQGB...
JLkhbybBYef47MLfW4a7KzTBY=
-----END PRIVATE KEY-----

4. Edit TLS parameters in Zabbix server configuration file like this:

     TLSCAFile=/home/zabbix/zabbix_ca_file
     TLSCertFile=/home/zabbix/zabbix_server.crt
     TLSKeyFile=/home/zabbix/zabbix_server.key

Configuring certificate-based encryption for Zabbix proxy:

1. Prepare files with top-level CA certificates, proxy certificate (chain) and private key as described in Configuring certificate on Zabbix server. Edit parameters TLSCAFile, TLSCertFile, TLSKeyFile in proxy configuration accordingly.

2. For active proxy edit TLSConnect parameter:

     TLSConnect=cert

For passive proxy edit TLSAccept parameter:

     TLSAccept=cert

3. Now you have a minimal certificate-based proxy configuration. You may prefer to improve proxy security by setting TSServerCertIssuer and TSServerCertSubject parameters (see Restricting allowed certificate Issuer and Subject).

4. In final proxy configuration file TLS parameters may look like:

     TLSCAFile=/home/zabbix/zabbix_ca_file
     TSServerCertIssuer=CN=Signing CA,OU=Development group,O=Zabbix SIA,DC=zabbix,DC=com
     TSServerCertSubject=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

5. Configure encryption for this proxy in Zabbix frontend:
   
   • Go to: Administration → Proxies
   • Select proxy and click on Encryption tab

   In examples below Issuer and Subject fields are filled in - see Restricting allowed certificate Issuer and Subject why and how to use these fields.

   For active proxy

   ![Active Proxy Encryption Configuration](image)

   For passive proxy

   ![Passive Proxy Encryption Configuration](image)

Configuring certificate-based encryption for Zabbix agent

1. Prepare files with top-level CA certificates, agent certificate (chain) and private key as described in Configuring certificate on Zabbix server. Edit parameters TLSCAFile, TLSCertFile, TLSKeyFile in agent configuration accordingly.

2. For active checks edit TLSConnect parameter:

   TLSConnect=cert

For passive checks edit TLSAccept parameter:

   TLSAccept=cert
3. Now you have a minimal certificate-based agent configuration. You may prefer to improve agent security by setting `TLSServerCertIssuer` and `TLSServerCertSubject` parameters. (see Restricting allowed certificate Issuer and Subject).

4. In final agent configuration file TLS parameters may look like:

   ```conf
   TLSConnect=cert
   TLSAccept=cert
   TLSCAFile=/home/zabbix/zabbix_ca_file
   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
   ```

   (Example assumes that host is monitored via proxy, hence proxy certificate Subject.)

5. Configure encryption for this agent in Zabbix frontend:

   - Go to: Configuration → Hosts
   - Select host and click on Encryption tab

In example below Issuer and Subject fields are filled in - see Restricting allowed certificate Issuer and Subject why and how to use these fields.

![Encryption settings](image)

Restricting allowed certificate Issuer and Subject

When two Zabbix components (e.g. server and agent) establish a TLS connection they both check each others certificates. If a peer certificate is signed by a trusted CA (with pre-configured top-level certificate in `TLSCAFile`), is valid, has not expired and passes some other checks then communication can proceed. Certificate issuer and subject are not checked in this simplest case.

Here is a risk - anybody with a valid certificate can impersonate anybody else (e.g. a host certificate can be used to impersonate server). This may be acceptable in small environments where certificates are signed by a dedicated in-house CA and risk of impersonating is low.

If your top-level CA is used for issuing other certificates which should not be accepted by Zabbix or you want to reduce risk of impersonating you can restrict allowed certificates by specifying their Issuer and Subject strings.

For example, you can write in Zabbix proxy configuration file:

   ```conf
   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
   ```

   With these settings, an active proxy will not talk to Zabbix server with different Issuer or Subject string in certificate, a passive proxy will not accept requests from such server.

A few notes about Issuer or Subject string matching:

1. Issuer and Subject strings are checked independently. Both are optional.
2. UTF-8 characters are allowed.
3. Unspecified string means any string is accepted.
4. Strings are compared "as-is", they must be exactly the same to match.
5. Wildcards and regexp's are not supported in matching.
6. Only some requirements from RFC 4514 Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names are implemented:
   2. escape characters space ( ‘ ‘ U+0020) or number sign (‘#’ U+0023) at the beginning of string.
   3. escape character space ( ‘ ‘ U+0020) at the end of string.
7. Match fails if a null character (U+0000) is encountered (RFC 4514 allows it).

Order of fields in Issuer and Subject strings and formatting are important! Zabbix follows RFC 4514 recommendation and uses “reverse” order of fields.

The reverse order can be illustrated by example:
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

Note that it starts with low level (CN), proceeds to mid-level (OU, O) and ends with top-level (DC) fields.

OpenSSL by default shows certificate Issuer and Subject fields in “normal” order, depending on additional options used:

```
$ 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
```

Here Issuer and Subject strings start with top-level (DC) and end with low-level (CN) field, spaces and field separators depend on options used. None of these values will match in Zabbix Issuer and Subject fields!

**Attention:**

To get proper Issuer and Subject strings usable in Zabbix invoke OpenSSL with special options

```
-nameopt esc_2253,esc_ctrl,utf8,dump_nostr,dump_unknown,dump_der,sep_comma_plus,dn_rev,sname:
```

```
$ 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
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
```

Now string fields are in reverse order, fields are comma-separated, can be used in Zabbix configuration files and frontend.

Limitations on using X.509 v3 certificate extensions

- **Subject Alternative Name (subjectAltName) extension.** Alternative subject names from subjectAltName extension (like IP address, e-mail address) are not supported by Zabbix.
  Only value of “Subject” field can be checked in Zabbix (see Restricting allowed certificate Issuer and Subject).
  If certificate uses the subjectAltName extension then result depends on particular combination of crypto toolkits Zabbix components are compiled with (it may or may not work, Zabbix may refuse to accept such certificates from peers).
- **Extended Key Usage** extension.
  If used then generally both clientAuth (TLS WWW client authentication) and serverAuth (TLS WWW server authentication) are necessary.
  For example, in passive checks Zabbix agent acts in a TLS server role, so serverAuth must be set in agent certificate. For active checks agent certificate needs clientAuth to be set.
  GnuTLS issues a warning in case of key usage violation but allows communication to proceed.
- **Name Constraints** extension.
  Not all crypto toolkits support it. This extension may prevent Zabbix from loading CA certificates where this section is marked as critical (depends on particular crypto toolkit).

Certificate Revocation Lists (CRL)
If a certificate is compromised CA can revoke it by including in CRL. CRLs can be configured in server, proxy and agent configuration file using parameter TLS_CRLFile. For example:

```
TLSCRLFile=/home/zabbix/zabbix_crl_file
```

where `zabbix_crl_file` may contain CRLs from several CAs and look like:

```
-----BEGIN X509 CRL-----
MIIB/DCB5QIBATANBgkqhkiG9w0BAQUFADCBgTETMBEGCgmSJomT8iXkARkVA2Nv...
-----END X509 CRL-----
```

```
-----BEGIN X509 CRL-----
MIIB+TCB4gIBATANBgkqhkiG9w0BAQUFADB/MRMwEQYKCIImiZPyLQQBGRYDY29t...
-----END X509 CRL-----
```

CRL file is loaded only on Zabbix start. CRL update requires restart.

**Attention:**

If Zabbix component is compiled with OpenSSL and CRLs are used then each top and intermediate level CA in certificate chains must have a corresponding CRL (it can be empty) in TLS_CRLFile.

Limitations on using CRL extensions

- **Authority Key Identifier** extension.

  CRLs for CAs with identical names may not work in case of mbedTLS (PolarSSL), even with "Authority Key Identifier" extension.

**2 Using pre-shared keys**

**Overview**

Each pre-shared key (PSK) in Zabbix actually is a pair of:

- non-secret PSK identity string,
- secret PSK string value.

PSK identity string is a non-empty UTF-8 string. For example, "PSK ID 001 Zabbix agentd". It is a unique name by which this specific PSK is referred to by Zabbix components. Do not put sensitive information in PSK identity string - it is transmitted over the network unencrypted.

PSK value is a hard to guess string of hexadecimal digits, for example, "e560cb0d918d26d31b4f642181f5f70ad89a390931102e5391d08327ba434e9".

**Size limits**

There are size limits for PSK identity and value in Zabbix, in some cases a crypto library can have lower limit:

<table>
<thead>
<tr>
<th>Component</th>
<th>PSK identity max size</th>
<th>PSK value min size</th>
<th>PSK value max size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zabbix</td>
<td>128 UTF-8 characters</td>
<td>128-bit (16-byte PSK, entered as 32 hexadecimal digits)</td>
<td>2048-bit (256-byte PSK, entered as 512 hexadecimal digits)</td>
</tr>
<tr>
<td>GnuTLS</td>
<td>128 bytes (may include UTF-8 characters)</td>
<td>-</td>
<td>2048-bit (256-byte PSK, entered as 512 hexadecimal digits)</td>
</tr>
<tr>
<td>mbed TLS (PolarSSL)</td>
<td>128 UTF-8 characters</td>
<td>-</td>
<td>256-bit (default limit) (32-byte PSK, entered as 64 hexadecimal digits)</td>
</tr>
<tr>
<td>OpenSSL 1.0.x, 1.1.0</td>
<td>127 bytes (may include UTF-8 characters)</td>
<td>-</td>
<td>2048-bit (256-byte PSK, entered as 512 hexadecimal digits)</td>
</tr>
<tr>
<td>OpenSSL 1.1.1</td>
<td>127 bytes (may include UTF-8 characters)</td>
<td>-</td>
<td>512-bit (64-byte PSK, entered as 128 hexadecimal digits)</td>
</tr>
</tbody>
</table>
### Attention:
Zabbix frontend allows configuring up to 128-character long PSK identity string and 2048-bit long PSK regardless of crypto libraries used.
If some Zabbix components support lower limits, it is the user’s responsibility to configure PSK identity and value with allowed length for these components.
Exceeding length limits results in communication failures between Zabbix components.

Before Zabbix server connects to agent using PSK, the server looks up the PSK identity and PSK value configured for that agent in database (actually in configuration cache). Upon receiving a connection the agent uses PSK identity and PSK value from its configuration file. If both parties have the same PSK identity string and PSK value the connection may succeed.

### Attention:
Each PSK identity must be paired with only one value. It is the user’s responsibility to ensure that there are no two PSKs with the same identity string but different values. Failing to do so may lead to unpredictable errors or disruptions of communication between Zabbix components using PSKs with this PSK identity string.

---

### Generating PSK
For example, a 256-bit (32 bytes) PSK can be generated using the following commands:

- with OpenSSL:
  
  ```
  $ openssl rand -hex 32
  af8ced32dfe8714e54b694e2d29e1a14ba6fa13f216cb35c19d0fe
  b1084b0429
  ```

- with GnuTLS:
  
  ```
  $ pskttool -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
  ```

Note that "psktool" above generates a database file with a PSK identity and its associated PSK. Zabbix expects just a PSK in the PSK file, so the identity string and colon (':') should be removed from the file.

### Configuring PSK for server-agent communication (example)

On the agent host, write the PSK value into a file, for example, `/home/zabbix/zabbix_agentd.psk`. The file must contain PSK in the first text string, for example:

```
1f87b596725ac58dd977beef14b97461a7c1045b9a1c963065002c5473194952
```  

Set access rights to PSK file - it must be readable only by Zabbix user.

Edit TLS parameters in agent configuration file `zabbix_agentd.conf`, for example, set:

```
TLSConnect=psk
TLSAccept=psk
TLSPSKFile=/home/zabbix/zabbix_agentd.psk
TLSPSKIdentity=PSK 001
```

The agent will connect to server (active checks) and accept from server and `zabbix_get` only connections using PSK. PSK identity will be "PSK 001".

Restart the agent. Now you can test the connection using `zabbix_get`, for example:

```
$ zabbix_get -s 127.0.0.1 -k "system.cpu.load[all,avg1]" --tls-connect=psk
   --tls-psk-identity="PSK 001" --tls-psk-file=/home/zabbix/zabbix_agentd.psk
```

(To minimize downtime see how to change connection type in **Connection encryption management**).

Configure PSK encryption for this agent in Zabbix frontend:
• Go to: Configuration → Hosts
• Select host and click on Encryption tab

Example:

![Configuration Interface](image)

All mandatory input fields are marked with a red asterisk.

When configuration cache is synchronized with database the new connections will use PSK. Check server and agent logfiles for error messages.

Configuring PSK for server - active proxy communication (example)

On the proxy, write the PSK value into a file, for example, /home/zabbix/zabbix_proxy.psk. The file must contain PSK in the first text string, for example:

```
e560cb0d918d26d31b4f642181f5f570ad89a390931102e5391d08327ba434e9
```

Set access rights to PSK file - it must be readable only by Zabbix user.

Edit TLS parameters in proxy configuration file zabbix_proxy.conf, for example, set:

```
TLSConnect=psk
TLPSKFile=/home/zabbix/zabbix_proxy.psk
TLPSKIdentity=PSK 002
```

The proxy will connect to server using PSK. PSK identity will be “PSK 002”.

(To minimize downtime see how to change connection type in Connection encryption management).

Configure PSK for this proxy in Zabbix frontend. Go to Administration → Proxies, select the proxy, go to "Encryption" tab. In "Connections from proxy" mark PSK. Paste into "PSK identity" field "PSK 002" and "e560cb0d918d26d31b4f642181f5f570ad89a390931102e5391d08327ba434e9" into "PSK" field. Click "Update".

Restart proxy. It will start using PSK-based encrypted connections to server. Check server and proxy logfiles for error messages.

For a passive proxy the procedure is very similar. The only difference - set TLSAccept=psk in proxy configuration file and set “Connections to proxy” in Zabbix frontend to PSK.

### 3 Troubleshooting

General recommendations

- Start with understanding which component acts as a TLS client and which one acts as a TLS server in problem case. Zabbix server, proxies and agents, depending on interaction between them, all can work as TLS servers and clients. For example, Zabbix server connecting to agent for a passive check, acts as a TLS client. The agent is in role of TLS server. Zabbix agent, requesting a list of active checks from proxy, acts as a TLS client. The proxy is in role of TLS server. zabbix_get and zabbix_sender utilities always act as TLS clients.
• Zabbix uses mutual authentication. Each side verifies its peer and may refuse connection. For example, Zabbix server connecting to agent can close connection immediately if agent’s certificate is invalid. And vice versa - Zabbix agent accepting a connection from server can close connection if server is not trusted by agent.
• Examine logfiles in both sides - in TLS client and TLS server. The side which refuses connection may log a precise reason why it was refused. Other side often reports rather general error (e.g. “Connection closed by peer”, “connection was non-properly terminated”).
• Sometimes misconfigured encryption results in confusing error messages in no way pointing to real cause. In subsections below we try to provide a (far from exhaustive) collection of messages and possible causes which could help in troubleshooting.

Please note that different crypto toolkits (OpenSSL, GnuTLS, mbed TLS (PolarSSL)) often produce different error messages in same problem situations. Sometimes error messages depend even on particular combination of crypto toolkits on both sides.

1 Connection type or permission problems

Server is configured to connect with PSK to agent but agent accepts only unencrypted connections
In server or proxy log (with mbed TLS (PolarSSL) 1.3.11)
Get value from agent failed: ssl_handshake(): SSL - The connection indicated an EOF
In server or proxy log (with GnuTLS 3.3.16)
Get value from agent failed: zbx_tls_connect(): gnutls_handshake() failed:
-110 The TLS connection was non-properly terminated.
In server or proxy log (with 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
One side connects with certificate but other side accepts only PSK or vice versa
In any log (with mbed TLS (PolarSSL)):
failed to accept an incoming connection: from 127.0.0.1: ssl_handshake():
SSL - The server has no ciphersuites in common with the client
In any log (with GnuTLS):
failed to accept an incoming connection: from 127.0.0.1: zbx_tls_accept(): gnutls_handshake() failed:
-21 Could not negotiate a supported cipher suite.
In any log (with OpenSSL 1.0.2c):
failed to accept an incoming connection: from 127.0.0.1: TLS handshake returned error code 1:
file .\ssl\v3_srvr.c line 1411: error:1408A0C1:SSL routines:ssl3_get_client_hello:no shared cipher:
TLS write fatal alert "handshake failure"

Attempting to use Zabbix sender compiled with TLS support to send data to Zabbix server/proxy compiled without TLS
In connecting-side log:

Linux:
...In zbx_tls_init_child()
...OpenSSL library (version OpenSSL 1.1.1 11 Sep 2018) initialized
...
...In zbx_tls_connect(): psk_identity:"PSK test sender"
...End of zbx_tls_connect():FAIL error:'connection closed by peer'
...send value error: TCP successful, cannot establish TLS to [[localhost]:10051]: connection closed by peer

Windows:
...OpenSSL library (version OpenSSL 1.1.1a 20 Nov 2018) initialized
...
...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() I/O error: [0x00000000] The operation completed successfully.'
...send value error: TCP successful, cannot establish TLS to [[192.168.1.2]:10051]: SSL_connect() I/O error
In accepting-side log:
...failed to accept an incoming connection: from 127.0.0.1: support for TLS was not compiled in
One side connects with PSK but other side uses LibreSSL or has been compiled without encryption support
LibreSSL does not support PSK.
In connecting-side log:
...TCP successful, cannot establish TLS to [[192.168.1.2]:10050]: SSL_connect() I/O error: [0] Success
In accepting-side log:
...failed to accept an incoming connection: from 192.168.1.2: support for PSK was not compiled in
In Zabbix frontend:
Get value from agent failed: TCP successful, cannot establish TLS to [[192.168.1.2]:10050]: SSL_connect()
One side connects with PSK but other side uses OpenSSL with PSK support disabled
In connecting-side log:
...TCP successful, cannot establish TLS to [[192.168.1.2]:10050]: SSL_connect() set result code to SSL_ERROR_SSL
In accepting-side log:
...failed to accept an incoming connection: from 192.168.1.2: TLS handshake set result code to 1: file ssl

2 Certificate problems

OpenSSL used with CRLs and for some CA in the certificate chain its CRL is not included in TLSCRLFile
In TLS server log in case of mbed TLS (PolarSSL) and OpenSSL peers:
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 failed:
    TLS write fatal alert "unknown CA"
In TLS server log in case of GnuTLS peer:
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:
CRL expired or expires during server operation
OpenSSL, in server log:
• before expiration:
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"
• after expiration:
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"
The point here is that with valid CRL a revoked certificate is reported as "certificate revoked". When CRL expires the error message changes to "certificate expired" which is quite misleading.
GnuTLS, in server log:
• before and after expiration the same:
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.
mbed TLS (PolarSSL), in server log:
• before expiration:
cannot connect to proxy "proxy-openssl-1.0.1e": TCP successful, cannot establish TLS to [[127.0.0.1]:20004]
  invalid peer certificate: revoked
• after expiration:
cannot connect to proxy "proxy-openssl-1.0.1e": TCP successful, cannot establish TLS to [[127.0.0.1]:20004]
  invalid peer certificate: revoked, CRL expired

Self-signed certificate, unknown CA

OpenSSL, in log:
error:'self signed certificate: SSL_connect() set result code to SSL_ERROR_SSL: file ..ssl/statem/statem_clnt.c line 1924: error:1416F086:SSL routines:tls_process_server_certificate:certificate verify failed:
  TLS write fatal alert "unknown CA"

This was observed when server certificate by mistake had the same Issuer and Subject string, although it was signed by CA. Issuer and Subject are equal in top-level CA certificate, but they cannot be equal in server certificate. (The same applies to proxy and agent certificates.)

3 PSK problems

PSK contains an odd number of hex-digits
Proxy or agent does not start, message in the proxy or agent log:
invalid PSK in file "./home/zabbix/zabbix_proxy.psk"
PSK identity string longer than 128 bytes is passed to GnuTLS
In TLS client side log:
gnutls_handshake() failed: -110 The TLS connection was non-properly terminated.
In TLS server side log.
gnutls_handshake() failed: -90 The SRP username supplied is illegal.
PSK longer than 32 bytes is passed to mbed TLS (PolarSSL)
In any Zabbix log:
ssl_set_psk(): SSL - Bad input parameters to function
Too long PSK value used with OpenSSL 1.1.1
In connecting-side log:
...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\extensions_clnt.c line 801: error:14212044:SSL routines:tls_construct_ctos_early_data:internal error: TLS write fatal alert "internal error"
In accepting-side log:
...Message from 123.123.123.123 is missing header. Message ignored.

This problem typically arises when upgrading OpenSSL from 1.0.x or 1.1.0 to 1.1.1 and if the PSK value is longer than 512-bit (64-byte PSK, entered as 128 hexadecimal digits).

See also: Value size limits

18. Web interface
Overview  For an easy access to Zabbix from anywhere and from any platform, the web-based interface is provided.

Note: Trying to access two Zabbix frontend installations on the same host, on different ports, simultaneously will fail. Logging into the second one will terminate the session on the first one - unless the default frontend session name is adjusted for the second frontend in frontend definitions (see ZBX_SESSION_NAME).

1 Frontend sections

1 Monitoring

Overview
The Monitoring menu is all about displaying data. Whatever information Zabbix is configured to gather, visualize and act upon, it will be displayed in the various sections of the Monitoring menu.

1 Dashboard

Overview
The Monitoring → Dashboard section is designed to display summaries of all the important information.

A dashboard consists of widgets and each widget is designed to display information of a certain kind and source, which can be a summary, a map, a graph, the clock, etc.

Access to hosts in the widgets depends on host permissions.

Widgets are added and edited in the dashboard editing mode. Widgets are viewed in the dashboard viewing mode.

While in a single dashboard you can group widgets from various sources for a quick overview, it is also possible to create several dashboards containing different sets of overviews and switch between them.

The time period that is displayed in graph widgets is controlled by the time period selector located above the widgets. The time period selector label, located to the right, displays the currently selected time period. Clicking the tab label allows to expand and collapse the time period selector.

Note that when the dashboard is displayed in kiosk mode (accessible from the fullscreen mode) and widgets only are displayed, it is possible to zoom out the graph period by double clicking in the graph.
Viewing dashboards

To access all configured dashboards, click on the All dashboards link just below the section title.

To view a single dashboard, click on its name in the list of all dashboards.

To delete one or several dashboards, mark the checkboxes of the respective dashboards and click on Delete below the list.

Creating a dashboard

When viewing all dashboards, you can click on the Create dashboard button to create a new dashboard:

Initially the dashboard is empty. You can add widgets to the dashboard by:

- clicking on the Add widget button
- clicking on the Add a new widget link in the widget placeholder

Click on the Save changes button to save the dashboard. If you click on Cancel, the dashboard will not be created.

Adding widgets

To add widget to a dashboard:

- Click on the Add widget button/link in dashboard editing mode
- Select the Type of widget
- Enter widget parameters
- Click on Add
The following widgets can be added to a dashboard:

- Action log
- Clock
- Data overview
- Discovery status
- Favorite graphs
- Favorite maps
- Favorite screens
- Graph
- Graph (classic)
- Problem hosts
- Map
- Map navigation tree
- Plain text
- Problems
- System information
- Problems by severity
- Trigger overview
- URL
- Web monitoring

In dashboard editing mode widgets can be moved around the dashboard by clicking on the widget title bar and dragging it to a new location. Also, you can click on the following buttons within the widget to:

- edit a widget;
- remove a widget

Click on Save changes for the dashboard to make any changes to the widgets permanent.

Dynamic widgets

When configuring some of the widgets:

- Graphs (simple and custom)
- Plain text
- URL

there is an extra option called Dynamic item. You can check this box to make the widget dynamic - i.e. capable of displaying different content based on the selected host.

Now, when saving the dashboard, you will notice that two new dropdowns have appeared atop the dashboard for selecting the host group/host:

Thus you have a widget, which can display content that is based on the data from the host that is selected in the dropdown. The benefit of this is that you do not need to create extra widgets just because, for example, you want to see the same graphs containing data from various hosts.

Viewing and editing a dashboard

When viewing a single dashboard, the following options are available:
Switch to the dashboard editing mode.

Open the action menu.

Sharing
Edit sharing preferences for the dashboard. Dashboards can be made public or private. Public dashboards are visible to all users. Private dashboards are visible only to their owner. Private dashboards can be shared by the owner to other users and user groups. For details on configuring sharing, see the map configuration section.

Create new
Create a new dashboard. First you are prompted to enter general properties of the new dashboard - owner and name. Then, the new dashboard opens in editing mode and you can add widgets.

Clone
Create a new dashboard by copying properties of the existing one. First you are prompted to enter general properties of the new dashboard - owner and name. Then, the new dashboard opens in editing mode with all the widgets of the original dashboard.

Delete
Delete the dashboard.

Display dashboard in fullscreen mode. Since Zabbix 4.0.1, the fullscreen mode can also be accessed with the following URL parameters:
/zabbix.php?action=dashboard.view&fullscreen=1
To exit:
/zabbix.php?action=dashboard.view&fullscreen=0

Display dashboard in kiosk mode. In this mode only widgets are displayed. The kiosk mode button appears when the fullscreen mode is activated. To exit kiosk mode, move the mouse cursor until the exit button appears and click on it. Note that you will be taken back to normal mode (not fullscreen mode).
Since Zabbix 4.0.1, the kiosk mode can also be accessed with the following URL parameters:
/zabbix.php?action=dashboard.view&kiosk=1
To exit to normal mode:
/zabbix.php?action=dashboard.view&fullscreen=0

Editing mode is opened:

• when a new dashboard is being created
• when you click the Edit dashboard button for an existing dashboard
In the dashboard editing mode the following options are available:

- **Edit general dashboard properties - name and owner.**
- **Add a new widget.**
- **Save dashboard changes.**
- **Cancel dashboard changes.**

Permissions to dashboards

Permissions to dashboards for regular and Zabbix Admin users are limited in the following way:

- They can see and clone a dashboard if they have at least READ rights to it;
- They can edit and delete dashboard only if they have READ/WRITE rights to it;
- They cannot change the dashboard owner.

Host menu

Clicking on a host in the Problems widget brings up the host menu. It includes links to custom scripts, inventory, latest data, problems, graphs and screens for the host.

![Host menu](image)

The host menu is accessible by clicking on a host in several other frontend sections:
Problem event popup

The problem event popup includes the list of problem events for this trigger and, if defined, the trigger description and a clickable URL.

To bring up the problem event popup:

- roll a mouse over the problem name in the Problem-Severity column of the Problems widget. The popup disappears once you remove the mouse from the problem name.
- click on the problem name in the Problem-Severity column of the Problems widget. The popup disappears only if you click on the problem name again.

1 Dashboard widgets

Overview

This section lists available dashboard widgets and provides details for widget configuration.

The following parameters are common for every single widget:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a widget name.</td>
</tr>
<tr>
<td>Refresh interval</td>
<td>Configure default refresh interval. Default refresh intervals for widgets range from No refresh to 15 minutes depending on the type of widget. For example: No refresh for URL widget, 1 minute for action log widget, 15 minutes for clock widget.</td>
</tr>
</tbody>
</table>

Refresh intervals for a widget can be set to a default value for all the corresponding users and also each user can set his own refresh interval value:

- To set a default value for all the corresponding users switch to editing mode (click the Edit dashboard button, find the right widget, click the Edit button opening the editing form of a widget) and choose the required refresh interval from the dropdown list.
- Setting a unique refresh interval for each user separately is possible in view mode by clicking the *** button for a certain widget.

Unique refresh interval set by a user has a priority over widget’s setting and once it's set it's always preserved when widget’s setting is modified.

Action log

In the action log widget you can display details of action operations (notifications, remote commands). It replicates information from Reports → Action log.

To configure, select Action log as type:
You may set the following specific options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sort entries by</td>
<td>Sort entries by:</td>
</tr>
<tr>
<td></td>
<td>Time (descending or ascending)</td>
</tr>
<tr>
<td></td>
<td>Type (descending or ascending)</td>
</tr>
<tr>
<td></td>
<td>Status (descending or ascending)</td>
</tr>
<tr>
<td></td>
<td>Recipient (descending or ascending)</td>
</tr>
<tr>
<td>Show lines</td>
<td>Set how many action log lines will be displayed in the widget.</td>
</tr>
</tbody>
</table>

**Clock**

In the clock widget you may display local, server or specified host time.

To configure, select Clock as type:

You may set the following specific options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time type</td>
<td>Select local, server or specified host time.</td>
</tr>
<tr>
<td>Item</td>
<td>Select the item for displaying time. To display host time, use the <code>system localtime[local] item</code>. This item must exist on the host. This field is available only when Host time is selected.</td>
</tr>
</tbody>
</table>

**Data overview**

In the data overview widget you can display the latest data for a group of hosts. It replicates information from Monitoring → Overview (when Data is selected as Type there).

To configure, select Data overview as type:
You may set the following specific options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host groups</td>
<td>Select host groups. This field is auto-complete so starting to type the name of a group will offer a dropdown of matching groups. Scroll down to select. Click on 'x' to remove the selected.</td>
</tr>
<tr>
<td>Application</td>
<td>Enter application name.</td>
</tr>
<tr>
<td>Show suppressed</td>
<td>Mark the checkbox to display problems which would otherwise be suppressed (not shown) because of host maintenance.</td>
</tr>
<tr>
<td>Hosts location</td>
<td>Select host location - left or top.</td>
</tr>
</tbody>
</table>

Discovery status
This widget displays a status summary of the active network discovery rules.

Favorite graphs
This widget contains shortcuts to the most needed graphs, sorted alphabetically.

The list of shortcuts is populated when you view a graph and then click on its Add to favorites button.

Favorite maps
This widget contains shortcuts to the most needed maps, sorted alphabetically.

The list of shortcuts is populated when you view a map and then click on its Add to favorites button.

Favorite screens
This widget contains shortcuts to the most needed screens and slide shows, sorted alphabetically.

The list of shortcuts is populated when you view a screen/slider show and then click on its Add to favorites button.

Graph
The graph widget provides a modern and versatile way of visualizing data collected by Zabbix using a vector image drawing technique. This graph widget is supported since Zabbix 4.0. The graph widget supported before can still be used and is now renamed to Graph (classic).

To configure, select Graph as type:
The **Data set** tab allows to add data sets and define their visual representation:

### Data set
Select hosts and items to display on the graph. Alternatively you may enter host and item patterns. Wildcard patterns may be used (for example, `*` will return results that match zero or more characters). Up to 50 items may be displayed in the graph.

Multiple entities (hosts, host patterns, items, item patterns) are separated with a comma. Therefore hosts or items with a comma in the name are not supported.

Host pattern and item pattern fields are mandatory.

Note that item names containing deprecated positional macros ($1-$9) are not resolved in this field. Therefore it will not be possible to add any of the items named like CPU $2 time individually to the graph using its resolved name (like CPU user time); while using its unresolved name CPU $2 time will add all corresponding items to the graph (e.g. CPU user time, CPU system time, CPU idle time, etc.).

### Base color
Adjust base color, either from the color picker or manually. Base color is used to calculate different colors for each item of the data set. Base color input field is mandatory.

### Draw
Choose the draw type of the metric. Possible draw types are Line (set by default), Points and Staircase.

Note that, since 4.0.4, if there’s only one data point in line/staircase graph it is drawn as point regardless of draw type. The point size is calculated from line width, but it cannot be smaller than 3 pixels, even if line width is less.

### Width
Set the line width. This option is available when Line or Staircase draw type is selected.

### Point size
Set the point size. This option is available when Points draw type is selected.

### Transparency
Set the transparency level.

### Fill
Set the fill level. This option is available when Line or Staircase draw type is selected.

### Missing data
Select the option for displaying missing data:  
- **None** - the gap is left empty  
- **Connected** - two border values are connected  
- **Treat as 0** - the missing data is displayed as 0 values  
Not applicable for Points draw type.
Y-axis Select the side of the graph where Y-axis will be displayed.
Time shift Set the time shift. Negative values allowed.

Existing data sets are displayed in a list. You may:

- click on this button to add a new data set
- click on the color icon to expand/collapse data set details
- click on the move icon and drag a data set to a new place in the list

The **Displaying options** tab allows to define history data selection:

<table>
<thead>
<tr>
<th>Data set</th>
<th>Displaying options</th>
<th>Time period</th>
<th>Axes</th>
<th>Legend</th>
<th>Problems</th>
<th>Overrides</th>
</tr>
</thead>
<tbody>
<tr>
<td>History data selection</td>
<td>Auto</td>
<td>History</td>
<td>Trends</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

History data selection Set the source of the history data. Possible options are Auto (set by default, as implemented in classic graphs), History and Trends.

The **Time period** tab allows to set a custom time period:

Set custom time period Mark this checkbox to set custom time period for the graph (unmarked by default).
From Set the start time of the custom time period for the graph.
To Set the end time of the custom time period for the graph.

The **Axes** tab allows to customize how axes are displayed:

<table>
<thead>
<tr>
<th>Data set</th>
<th>Displaying options</th>
<th>Time period</th>
<th>Axes</th>
<th>Legend</th>
<th>Problems</th>
<th>Overrides</th>
</tr>
</thead>
<tbody>
<tr>
<td>Left Y</td>
<td>Show</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Min calculated
Max calculated
Units Auto

Right Y Show
| | | | |

Min calculated
Max calculated
Units Auto

X-Axis Show
| | | |

Min 10
Max 100
Units Auto

Left Y Mark this checkbox to make left Y axis visible. The Checkbox may be disabled in case it's not chosen either in Data set or in Overrides tab.
Right Y Mark this checkbox to make right Y axis visible. The Checkbox may be disabled in case it's not chosen either in Data set or in Overrides tab.
X-Axis Unmark this checkbox to hide X axis (marked by default).
Min Set the minimum value of the corresponding axis. Visible range minimum value of Y axis is specified.
Max Set the maximum value of the corresponding axis. Visible range maximum value of Y axis is specified.

Units Choose the unit for the graph axis values from the dropdown. If Auto option is chosen axis values are displayed using units of the first item of corresponding axis. Static option allows you to assign corresponding axis’ custom name. If Static option is chosen and value input field left blank the corresponding axis name will only consist of a numeric value.

The **Legend** tab allows to customize the graph legend:

<table>
<thead>
<tr>
<th>Data set</th>
<th>Displaying options</th>
<th>Time period</th>
<th>Axes</th>
<th>Legend</th>
<th>Problems</th>
<th>Overrides</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show legend</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of rows</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Show legend Unmark this checkbox to hide the legend on the graph (marked by default).

Number of rows Set the number of rows to be displayed on the graph.

The **Problems** tab allows to customize the problem display:

<table>
<thead>
<tr>
<th>Data set</th>
<th>Displaying options</th>
<th>Time period</th>
<th>Axes</th>
<th>Legend</th>
<th>Problems</th>
<th>Overrides</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show problems</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Selected items only</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Problem hosts Zabbix

Severity Not classified Information Warning Average High Disaster

Problem problem pattern

Tags And/Or Or

Add

Show problems Mark this checkbox to enable problem displaying on the graph (unmarked, i.e. disabled by default).  
Selected items only Mark this checkbox to include problems for the selected items only to be displayed on the graph.  
Problem hosts Select the problem hosts to be displayed on the graph. Wildcard patterns may be used (for example, * will return results that match zero or more characters).  
Multiple hosts are separated with a comma. Therefore hosts with a comma in the visible name are not supported.  
Severity Mark the problem severities to be displayed on the graph.  
Problem Specify the problem’s name to be displayed on the graph.  
Tags Specify tag name and value to limit the number of problems displayed on the graph. To add more tag names and values, click on Add.  
There are two calculation types for several conditions:  
**And/Or** - all conditions must be met, conditions having same tag name will be grouped by Or condition  
**Or** - enough if one condition is met  
There are two ways of matching the tag value:  
**Contains** - case-sensitive substring match (tag value contains the entered string)  
**Equals** - case-sensitive string match (tag value equals the entered string)
The **Overrides** tab allows to add custom overrides for data set properties:

![Edit widget](image)

Overrides are useful when several items are selected for a data set using the * wildcard and you want to change how the items are displayed by default (e.g. default base color or any other property).

Existing overrides (if any) are displayed in a list. To add a new override:

- Click on the **Add new override** button
- Select hosts and items for the override. Alternatively you may enter host and item patterns. Wildcard patterns may be used (for example, * will return results that match zero or more characters). Multiple entities (hosts, host patterns, items, item patterns) are separated with a comma. Therefore hosts or items with a comma in the name are not supported. Host pattern and item pattern fields are mandatory.
- Click on **Add new override** to select override parameters. At least one override parameter should be selected. For parameter descriptions, see the Data set tab above.

**Graph (classic)**

In the classic graph widget you can display a single custom graph or simple graph.

To configure, select Graph as type:
You may set the following specific options:

<table>
<thead>
<tr>
<th>Source</th>
<th>Select graph type:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Graph</td>
<td>custom graph</td>
</tr>
<tr>
<td>Simple graph</td>
<td>simple graph</td>
</tr>
</tbody>
</table>

**Graph**
Select the custom graph to display.
This option is available if ‘Graph’ is selected as Source.

**Item**
Select the item to display in a simple graph.
This option is available if ‘Simple graph’ is selected as Source.

**Dynamic item**
Set graph to display different data depending on the selected host.

**Map**
In the map widget you can display either:

- a single configured network map
- one of the configured network maps in the map navigation tree (when clicking on the map name in the tree).

To configure, select Map as type:

You may set the following specific options:

<table>
<thead>
<tr>
<th>Source type</th>
<th>Select to display:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Map</td>
<td>network map</td>
</tr>
</tbody>
</table>
| Map navigation tree | one of the maps in the selected map navigation tree

**Map**
Select the map to display.
This option is available if ‘Map’ is selected as Source type.

**Filter**
Select the map navigation tree to display the maps of.
This option is available if ‘Map navigation tree’ is selected as Source type.
See also: known issue with IE11

Map navigation tree

This widget allows to build a hierarchy of existing maps while also displaying problem statistics with each included map and map group.

It becomes even more powerful if you link the Map widget to the navigation tree. In this case, clicking on a map name in the navigation tree displays the map in full in the Map widget.

Statistics with the top level map in the hierarchy display a sum of problems of all submaps and its own problems.

To configure the navigation tree widget, select Map navigation tree as type:

You may set the following specific options:

- **Show unavailable maps**: Mark this checkbox to display maps that the user does not have read permission to. Unavailable maps in the navigation tree will be displayed with a grayed out icon. Note that if this checkbox is marked, available submaps are displayed even if the parent level map is unavailable. If unmarked, available submaps to an unavailable parent map will not be displayed at all.

- Problem count is calculated based on available maps and available map elements.

Plain text

In the plain text widget you can display latest item data in plain text.

To configure, select Plain text as type:
You may set the following specific options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Items</td>
<td>Select the items.</td>
</tr>
<tr>
<td>Items location</td>
<td>Choose the location of selected items to be displayed in the widget.</td>
</tr>
<tr>
<td>Show lines</td>
<td>Set how many latest data lines will be displayed in the widget.</td>
</tr>
<tr>
<td>Show text as HTML</td>
<td>Set to display text as HTML.</td>
</tr>
<tr>
<td>Dynamic item</td>
<td>Set to display different data depending on the selected host.</td>
</tr>
</tbody>
</table>

Problem hosts

In the host information widget you can display high-level information about host availability.

To configure, select Problem hosts as type:
You may set the following specific options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host groups</td>
<td>Enter host groups to display in the widget. This field is auto-complete so starting to type the name of a group will offer a dropdown of matching groups. Specifying a parent host group implicitly selects all nested host groups. Host data from these host groups will be displayed in the widget. If no host groups are entered, all host groups will be displayed.</td>
</tr>
<tr>
<td>Exclude host groups</td>
<td>Enter host groups to hide from the widget. This field is auto-complete so starting to type the name of a group will offer a dropdown of matching groups. Specifying a parent host group implicitly selects all nested host groups. Host data from these host groups will not be displayed in the widget. For example, hosts 001, 002, 003 may be in Group A and hosts 002, 003 in Group B as well. If we select to show Group A and exclude Group B at the same time, only data from host 001 will be displayed in the Dashboard.</td>
</tr>
<tr>
<td>Hosts</td>
<td>Enter hosts to display in the widget. This field is auto-complete so starting to type the name of a host will offer a dropdown of matching hosts. If no hosts are entered, all hosts will be displayed.</td>
</tr>
<tr>
<td>Problem</td>
<td>You can limit the number of problem hosts displayed by the problem name. If you enter a string here, only those hosts with problems whose name contains the entered string will be displayed. Macros are not expanded.</td>
</tr>
<tr>
<td>Severity</td>
<td>Mark the problem severities to be displayed in the widget.</td>
</tr>
<tr>
<td>Show suppressed problems</td>
<td>Mark the checkbox to display problems which would otherwise be suppressed (not shown) because of host maintenance.</td>
</tr>
<tr>
<td>Hide groups without problems</td>
<td>Mark the Hide groups without problems option to hide data from host groups without problems in the widget.</td>
</tr>
<tr>
<td>Problem display</td>
<td>Display problem count as: All - full problem count will be displayed. Separated - unacknowledged problem count will be displayed separated as a number of the total problem count. Unacknowledged only - only the unacknowledged problem count will be displayed.</td>
</tr>
</tbody>
</table>
Problems

In this widget you can display current problems. The information in this widget is similar to Monitoring → Problems.

To configure, select Problems as type:

You can limit how many problems are displayed in the widget in various ways - by problem status, problem name, severity, host group, host, event tag, acknowledgment status, etc.
### Host groups
Enter host groups to display problems of in the widget. This field is auto-complete so starting to type the name of a group will offer a dropdown of matching groups. Specifying a parent host group implicitly selects all nested host groups. Problems from these host groups will be displayed in the widget. If no host groups are entered, problems from all host groups will be displayed.

### Exclude host groups
Enter host groups to hide problems of from the widget. This field is auto-complete so starting to type the name of a group will offer a dropdown of matching groups. Specifying a parent host group implicitly selects all nested host groups. Problems from these host groups will not be displayed in the widget. For example, hosts 001, 002, 003 may be in Group A and hosts 002, 003 in Group B as well. If we select to show Group A and exclude Group B at the same time, only problems from host 001 will be displayed in the widget.

### Hosts
Enter hosts to display problems of in the widget. This field is auto-complete so starting to type the name of a host will offer a dropdown of matching hosts. If no hosts are entered, problems of all hosts will be displayed.

### Problem
You can limit the number of problems displayed by their name. If you enter a string here, only those problems whose name contains the entered string will be displayed. Macros are not expanded.

### Severity
Mark the problem severities to be displayed in the widget.

### Tags
Specify event tag name and value to limit the number of problems displayed. To add more event tag names and values, click on Add.

There are two calculation types for several conditions:
- **And/Or** - all conditions must be met, conditions having same tag name will be grouped by Or condition
- **Or** - enough if one condition is met

There are two ways of matching the tag value:
- **Contains** - case-sensitive substring match (tag value contains the entered string)
- **Equals** - case-sensitive string match (tag value equals the entered string)

When filtered, the tags specified here will be displayed first with the problem, unless overridden by the Tag display priority (see below) list.

### Show tags
Select the number of displayed tags:
- **None** - no Tags column in Monitoring → Problems
- **1** - Tags column contains one tag
- **2** - Tags column contains two tags
- **3** - Tags column contains three tags

To see all tags for the problem roll your mouse over the three dots icon.

### Tag name
Select tag name display mode:
- **Full** - tag names and values are displayed in full
- **Shortened** - tag names are shortened to 3 symbols; tag values are displayed in full
- **None** - only tag values are displayed; no names

### Tag display priority
Enter tag display priority for a problem, as a comma-separated list of tags (for example: Services, Applications, Application). Tag names only should be used, no values. The tags of this list will always be displayed first, overriding the natural ordering by alphabet.

### Show suppressed problems
Mark the checkbox to display problems which would otherwise be suppressed (not shown) because of host maintenance.

### Show unacknowledged only
Mark the checkbox to display unacknowledged problems only.

### Show latest values
Mark the checkbox to display latest value(s) of the items in the underlying trigger expression of the problem.

This option is supported since 4.0.3.

### Sort entries by
Sort entries by:
- **Time** (descending or ascending)
- **Severity** (descending or ascending)
- **Problem name** (descending or ascending)
- **Host** (descending or ascending)

### Show timeline
Mark the checkbox to display a visual timeline.

### Show lines
Specify the number of problem lines to display.

---

**Problems by severity**

In this widget you can display problems by severity. You can limit what hosts and triggers are displayed in the widget and define how the problem count is displayed.
To configure, select Problems by severity as type:

### Add widget

<table>
<thead>
<tr>
<th>Field</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>Problems by severity</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>Problems by severity</td>
</tr>
<tr>
<td><strong>Refresh interval</strong></td>
<td>Default (1 minute)</td>
</tr>
<tr>
<td><strong>Host groups</strong></td>
<td>Discovered hosts [x]</td>
</tr>
<tr>
<td></td>
<td>type here to search</td>
</tr>
<tr>
<td><strong>Exclude host groups</strong></td>
<td>type here to search</td>
</tr>
<tr>
<td><strong>Hosts</strong></td>
<td>type here to search</td>
</tr>
<tr>
<td><strong>Problem</strong></td>
<td></td>
</tr>
</tbody>
</table>

#### Specific Options:

- **Host groups**: Enter host groups to display in the widget. This field is auto-complete so starting to type the name of a group will offer a dropdown of matching groups. Specifying a parent host group implicitly selects all nested host groups. Host data from these host groups will be displayed in the widget. If no host groups are entered, all host groups will be displayed.

- **Exclude host groups**: Enter host groups to hide from the widget. This field is auto-complete so starting to type the name of a group will offer a dropdown of matching groups. Specifying a parent host group implicitly selects all nested host groups. Host data from these host groups will not be displayed in the widget. For example, hosts 001, 002, 003 may be in Group A and hosts 002, 003 in Group B as well. If we select to show Group A and exclude Group B at the same time, only data from host 001 will be displayed in the Dashboard.

- **Hosts**: Enter hosts to display in the widget. This field is auto-complete so starting to type the name of a host will offer a dropdown of matching hosts. If no hosts are entered, all hosts will be displayed.

- **Problem**: You can limit the number of problem hosts displayed by the problem name. If you enter a string here, only those hosts with problems whose name contains the entered string will be displayed. Macros are not expanded.

- **Severity**: Mark the problem severities to be displayed in the widget.

- **Show suppressed problems**: Mark the checkbox to display problems which would otherwise be suppressed (not shown) because of host maintenance.

- **Hide groups without problems**: Mark the Hide groups without problems option to hide data from host groups without problems in the widget.

---

632
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show latest values</td>
<td>Mark the checkbox to display latest value(s) of the items in the underlying trigger expression of the problem.</td>
</tr>
<tr>
<td></td>
<td>This option is supported since 4.0.3.</td>
</tr>
<tr>
<td>Problem display</td>
<td>Display problem count as:</td>
</tr>
<tr>
<td></td>
<td><strong>All</strong> - full problem count will be displayed</td>
</tr>
<tr>
<td></td>
<td><strong>Separated</strong> - unacknowledged problem count will be displayed separated as a number of the total problem count</td>
</tr>
<tr>
<td></td>
<td><strong>Unacknowledged only</strong> - only the unacknowledged problem count will be displayed.</td>
</tr>
<tr>
<td>Show timeline</td>
<td>Mark the checkbox to display a visual timeline.</td>
</tr>
</tbody>
</table>

**System information**

In the System information widget you can display high-level Zabbix and Zabbix server information.

To configure, select System information as type:

![Add widget](Image)

**Trigger overview**

In the trigger overview widget you can display the trigger states for a group of hosts. It replicates information from Monitoring → Overview (when Triggers is selected as Type there).

To configure, select Trigger overview as type:

![Add widget](Image)

You may set the following specific options:
### Filter Triggers by Trigger State

Filter triggers by trigger state:
- **Recent problems** - (default) show triggers that recently have been or still are in a PROBLEM state (resolved and unresolved);
- **Problems** - show triggers that are in a PROBLEM state (unresolved);
- **Any** - show all triggers.

### Host Groups
Select the host group(s). This field is auto-complete so starting to type the name of a group will offer a dropdown of matching groups.

### Application
Enter the application name.

### Show Suppressed Problems
Mark the checkbox to display problems which would otherwise be suppressed (not shown) because of host maintenance.

### Hosts Location
Select host location - left or top.

### URL
This widget displays the content retrieved from the specified URL.

To configure, select URL as type:

![Add widget]

**URL**
- Enter the URL to display.
- Relative paths are allowed since Zabbix 4.0.20.
- {HOST.*} macros are supported.

**Dynamic item**
- Set to display different URL content depending on the selected host.
- This can work if {HOST.*} macros are used in the URL.

**Attention:**
Browsers might not load an HTTP page included in the widget, if Zabbix frontend is accessed over HTTPS.

### Web Monitoring
This widget displays a status summary of the active web monitoring scenarios.

**Note:**
In cases when a user does not have permission to access certain widget elements, that element’s name will appear as Inaccessible during the widget’s configuration. This results in Inaccessible Item, Inaccessible Host, Inaccessible Group, Inaccessible Map and Inaccessible Graph appearing instead of the “real” name of the element.

### 2 Problems

Overview
In Monitoring → Problems you can see what problems you currently have. Problems are those triggers that are in the “Problem” state.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Problem start time is displayed.</td>
</tr>
<tr>
<td>Severity</td>
<td>Problem severity is displayed. Problem severity is originally based on the severity of the underlying problem trigger, however, after the event has happened it can be updated using the Update problem screen. Color of the problem severity is used as cell background during problem time.</td>
</tr>
<tr>
<td>Recovery time</td>
<td>Problem resolution time is displayed.</td>
</tr>
<tr>
<td>Status</td>
<td>Problem status is displayed: <strong>Problem</strong> - unresolved problem <strong>Resolved</strong> - recently resolved problem. You can hide recently resolved problems using the filter. New and recently resolved problems blink for 2 minutes. Resolved problems are displayed for 5 minutes in total. Both of these values are configurable in Administration → General → Trigger displaying options.</td>
</tr>
<tr>
<td>Info</td>
<td>A green information icon is displayed if a problem is closed by global correlation or manually when updating the problem. Rolling a mouse over the icon will display more details:</td>
</tr>
<tr>
<td>Host</td>
<td>Problem host is displayed.</td>
</tr>
<tr>
<td>Problem</td>
<td>Problem name is displayed. Problem name is based on the name of the underlying problem trigger. Clicking on the problem name brings up the event menu.</td>
</tr>
<tr>
<td>Latest values</td>
<td>Latest value(s) of the items in the underlying trigger expression of the problem are displayed. This column is only displayed if the Show latest values option is selected in the filter. Supported since 4.0.3.</td>
</tr>
<tr>
<td>Duration</td>
<td>Problem duration is displayed. See also: negative problem duration</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Ack    | The acknowledgment status of the problem is displayed:  
Yes - green text indicating that the problem is acknowledged. A problem is considered to be acknowledged if all events for it are acknowledged.  
No - a red link indicating unacknowledged events.  
If you click on the link you will be taken to the problem update screen where various actions can be taken on the problem, including commenting and acknowledging the problem. |
| Actions| History of activities about the problem is displayed using symbolic icons:  
1 - comments have been made. The number of comments is also displayed.  
2 - problem severity has been increased (e.g. Information → Warning)  
3 - problem severity has been decreased (e.g. Warning → Information)  
4 - problem severity has been changed, but returned to the original level (e.g. Warning → Information → Warning)  
5 - actions have been taken. The number of actions is also displayed.  
6 - actions have been taken, at least one is in progress. The number of actions is also displayed.  
7 - actions have been taken, at least one has failed. The number of actions is also displayed.  
When rolling the mouse over the icons, popups with details about the activity are displayed. See viewing details for the explanation on icons used in the popup for actions taken. |
| Tags   | Event tags are displayed (if any). |

Negative problem duration

It is actually possible in some common situations to have negative problem duration i.e. when the problem resolution time is earlier than problem creation time, e.g.:

- If some host is monitored by proxy and a network error happens, leading to no data received from the proxy for a while, the item.nodata() trigger will be fired by the server. When the connection is restored, the server will receive item data from the proxy having a time from the past. Then, the item.nodata() problem will be resolved and it will have a negative problem duration;
- When item data that resolve the problem event are sent by Zabbix sender and contain a timestamp earlier than the problem creation time, a negative problem duration will also be displayed.

**Note:**
Since Zabbix 4.0.4, negative problem duration is not affecting SLA calculation or Availability report of a particular trigger in any way; it neither reduces nor expands problem time. See also: known issues for 4.0.0-4.0.3.

Mass editing options

Buttons below the list offer some mass-editing options:

- Mass update - update the selected problems by navigating to the problem update screen

To use this option, mark the checkboxes before the respective problems, then click on the Mass update button.

**Buttons**

Buttons to the right offer the following options:

- Export content from all pages as a CSV file.  
Note that before Zabbix 4.0.15 only the currently selected page is exported.
Display page in full screen mode.

Display page in kiosk mode. In this mode only page content is displayed. The kiosk mode button appears when the full screen mode is activated.

To exit kiosk mode, move the mouse cursor until the exit button appears and click on it. Note that you will be taken back to normal mode (not full screen mode).

Using filter

You can use the filter to display only the problems you are interested in. The filter is located above the table.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Show**        | Filter by problem status: **Recent problems** - unresolved and recently resolved problems are displayed (default)  
 |                  | **Problems** - unresolved problems are displayed                                                  |
 |                  | **History** - history of all events is displayed                                                   |
| **Host groups** | Filter by one or more host groups. Specifying a parent host group implicitly selects all nested host groups. |
| **Hosts**       | Filter by one or more hosts.                                                                     |
| **Application** | Filter by application name.                                                                      |
| **Triggers**    | Filter by one or more triggers.                                                                   |
| **Problem**     | Filter by problem name.                                                                           |
| **Minimum severity** | Filter by minimum trigger (problem) severity.                                                    |
| **Age less than** | Filter by how old the problem is.                                                                 |
| **Host inventory** | Filter by inventory type and value.                                                               |
| **Tags**        | Filter by event tag name and value. Several conditions can be set. There are two calculation types for conditions:  
 |                  | **And/Or** - all conditions must be met, conditions having same tag name will be grouped by Or condition  
 |                  | **Or** - enough if one condition is met                                                                 |
|                  | There are two ways of matching the tag value:                                                     |
|                  | **Contains** - case-sensitive substring match (tag value contains the entered string)            |
|                  | **Equals** - case-sensitive string match (tag value equals the entered string)                   |
|                  | When filtered, the tags specified here will be displayed first with the problem, unless overridden by the Tag display priority (see below) list. |

637
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Show tags</strong></td>
<td>Select the number of displayed tags:</td>
</tr>
<tr>
<td></td>
<td><strong>None</strong> - no Tags column in Monitoring → Problems</td>
</tr>
<tr>
<td></td>
<td><strong>1</strong> - Tags column contains one tag</td>
</tr>
<tr>
<td></td>
<td><strong>2</strong> - Tags column contains two tags</td>
</tr>
<tr>
<td></td>
<td><strong>3</strong> - Tags column contains three tags</td>
</tr>
<tr>
<td></td>
<td>To see all tags for the problem roll your mouse over the three dots icon.</td>
</tr>
<tr>
<td><strong>Tag name</strong></td>
<td>Select tag name display mode:</td>
</tr>
<tr>
<td></td>
<td><strong>Full</strong> - tag names and values are displayed in full</td>
</tr>
<tr>
<td></td>
<td><strong>Shortened</strong> - tag names are shortened to 3 symbols; tag values are displayed in full</td>
</tr>
<tr>
<td></td>
<td><strong>None</strong> - only tag values are displayed; no names</td>
</tr>
<tr>
<td><strong>Tag display priority</strong></td>
<td>Enter tag display priority for a problem, as a comma-separated list of tags (for example: Services, Applications, Application). Tag names only should be used, no values. The tags of this list will always be displayed first, overriding the natural ordering by alphabet.</td>
</tr>
<tr>
<td><strong>Show suppressed problems</strong></td>
<td>Mark the checkbox to display problems which would otherwise be suppressed (not shown) because of host maintenance.</td>
</tr>
<tr>
<td><strong>Compact view</strong></td>
<td>Mark the checkbox to enable compact view.</td>
</tr>
<tr>
<td><strong>Show details</strong></td>
<td>Mark the checkbox to display underlying trigger expressions of the problems. Disabled if Compact view checkbox is marked.</td>
</tr>
<tr>
<td><strong>Show latest values</strong></td>
<td>Mark the checkbox to display latest value(s) of the items in the underlying trigger expression of the problem. Supported since 4.0.3.</td>
</tr>
<tr>
<td><strong>Show unacknowledged only</strong></td>
<td>Mark the checkbox to display unacknowledged problems only.</td>
</tr>
<tr>
<td><strong>Show timeline</strong></td>
<td>Mark the checkbox to display the visual timeline and grouping. Disabled if Compact view checkbox is marked.</td>
</tr>
<tr>
<td><strong>Highlight whole row</strong></td>
<td>Mark the checkbox to highlight the full line for unresolved problems. The problem severity color is used for the highlighting. Enabled only if the Compact view checkbox is marked in the standard blue and dark themes. Highlight whole row is not available in the high-contrast themes.</td>
</tr>
</tbody>
</table>

**Event menu**

Clicking on the problem name brings up the event menu:

![Event menu](image)

The event menu allows to filter the problems of the trigger, access the trigger description (if available) and the trigger configuration. Access to simple graph/item history of the underlying item(s) is also available.
Attention:
Resolved values of \{ITEM.VALUE\} and \{ITEM.LASTVALUE\} macros in trigger descriptions are truncated to 20 characters. To see the entire values you may use \textit{macro functions} with these macros, e.g. \texttt{\{ITEM.VALUE\}.regsub("(.*)", \1)}, \texttt{\{ITEM.LASTVALUE\}.regsub("(.*)", \1)} as a workaround.

Viewing details
The times for problem start and recovery in Monitoring → Problems are links. Clicking on them opens more details of the event.

Event details

Note how the problem severity differs for the trigger and the problem event - for the problem event it has been updated using the Update problem \texttt{screen}.

In the action list, the following icons are used to denote the activity type:

- \(\rightarrow\) - problem event generated
- \(\leftarrow\) - message has been sent
- \(\downarrow\) - problem event acknowledged
- \(\uparrow\) - comment has been added
- \(\Rightarrow\) - problem severity has been increased (e.g. Information → Warning)
- \(\Rightarrow\) - problem severity has been decreased (e.g. Warning → Information)
- \(\Rightarrow\) - problem severity has been changed, but returned to the original level (e.g. Warning → Information → Warning)
- \(\Rightarrow\) - remote command has been executed
- \(\checkmark\) - problem event has recovered
- \(\checkmark\) - problem has been closed manually

3 Overview

Overview
The Monitoring → Overview section offers an overview of trigger states or a comparison of data for various hosts at once.
The following display options are available:

- select all hosts or specific host groups in the Group dropdown
- choose what type of information to display (triggers or data) in the Type dropdown
- select horizontal or vertical display of information in the Hosts location dropdown

**Overview of triggers**

In the next screenshot Triggers are selected in the Type dropdown. As a result, trigger states of two local hosts are displayed as coloured blocks (the color of problem triggers depends on the problem severity color, which can be adjusted in the problem update screen):

Note that recent trigger changes (within the last 2 minutes) will be displayed as blinking blocks.

Blue up and down arrows indicate triggers that have dependencies. On mouseover, dependency details are revealed.

A checkbox icon indicates acknowledged problems. All problems or resolved problems of the trigger must be acknowledged for this icon to be displayed. (Before 4.0.14 it was enough for the last problem to be acknowledged.)

Clicking on a trigger block provides context-dependent links to problem events of the trigger, the problem acknowledgment screen, trigger configuration, trigger URL or a simple graph/latest values list.

**Buttons**

Buttons to the right offer the following options:

- Display page in fullscreen mode.

- Display page in kiosk mode. In this mode only page content displayed.
  The kiosk mode button appears when the fullscreen mode is activated.

  To exit kiosk mode, move the mouse cursor until the exit button appears and click on it. Note that you will be taken back to normal mode (not fullscreen mode).
Using filter

You can use the filter to display only the problems you are interested in. The filter is located above the table.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show</td>
<td>Filter by problem status:</td>
</tr>
<tr>
<td></td>
<td><strong>Recent problems</strong> - unresolved and recently resolved problems are displayed (default)</td>
</tr>
<tr>
<td></td>
<td><strong>Problems</strong> - unresolved problems are displayed</td>
</tr>
<tr>
<td></td>
<td><strong>Any</strong> - history of all events is displayed</td>
</tr>
<tr>
<td>Acknowledge status</td>
<td>Filter by acknowledgment status:</td>
</tr>
<tr>
<td></td>
<td><strong>Any</strong> - acknowledged and unacknowledged problems are displayed (default)</td>
</tr>
<tr>
<td></td>
<td><strong>With unacknowledged events</strong> - problems with unacknowledged events are displayed</td>
</tr>
<tr>
<td></td>
<td><strong>With last event unacknowledged</strong> - problems with last event unacknowledged are displayed</td>
</tr>
<tr>
<td>Minimum severity</td>
<td>Filter by minimum problem severity.</td>
</tr>
<tr>
<td>Age (less than)</td>
<td>Mark the checkbox to filter by problem age.</td>
</tr>
<tr>
<td>Name</td>
<td>Filter by problem name.</td>
</tr>
<tr>
<td>Application</td>
<td>Filter by application.</td>
</tr>
<tr>
<td>Host inventory</td>
<td>Filter by inventory type and value.</td>
</tr>
<tr>
<td>Show suppressed problems</td>
<td>Mark the checkbox to display problems which would otherwise be suppressed (not shown) because of host maintenance.</td>
</tr>
</tbody>
</table>

**Overview of data**

In the next screenshot Data is selected in the Type dropdown. As a result, performance item data of two local hosts are displayed.

The color of problem items is based on the problem severity color, which can be adjusted in the problem update screen.
Only values that fall within the last 24 hours are displayed by default. This limit has been introduced with the aim of improving initial loading times for large pages of latest data. It is also possible to change this limitation by changing the value of `ZBX_HISTORY_PERIOD` constant in `include/defines.inc.php`.

Clicking on a piece of data offers links to some predefined graphs or latest values.

**4 Web**

**Overview**

In the Monitoring → Web section current information about web scenarios is displayed.

Note: The name of a disabled host is displayed in red (in both the host dropdown and the list). Data of disabled hosts is accessible starting with Zabbix 2.2.0.

Only values that fall within the last 24 hours are displayed by default. This limit has been introduced with the aim of improving initial loading times for large pages of web monitoring. It is also possible to change this limitation by changing the value of `ZBX_HISTORY_PERIOD` constant in `include/defines.inc.php`.

The scenario name is link to more detailed statistics about it:
Buttons

Buttons to the right offer the following options:

- Display page in fullscreen mode.
- Display page in kiosk mode. In this mode only page content displayed.
  The kiosk mode button appears when the fullscreen mode is activated.
  To exit kiosk mode, move the mouse cursor until the exit button appears and click on it. Note that you will be taken back to normal mode (not fullscreen mode).

5 Latest data

Overview

The section in Monitoring → Latest data can be used to view latest values gathered by items as well as to access various graphs for the items.

When you open this page for the first time, nothing is displayed.
To access data, you need to make selections in the filter such as host group, host, application or item name.

In the list displayed, click on before a host and the relevant application to reveal latest values of that host and application.

You can expand all hosts and all applications, thus revealing all items by clicking on in the header row.

Note: The name of a disabled host is displayed in red. Data of disabled hosts, including graphs and item value lists, is accessible in Latest data since Zabbix 2.2.0.

Items are displayed with their name, last check time, last value, change amount and a link to a simple graph/history of item values.

By default only values that fall within the last 24 hours are displayed. This limit has been introduced with the aim of improving initial loading times for large pages of latest data. It is also possible to change this limitation by changing the value of ZBX_HISTORY_PERIOD constant in include/defines.inc.php.

Attention:
For items with update frequency of 1 day or more the change amount will never be displayed (with the default setting). Also in this case the last value will not be displayed at all if it was received more than 24 hours ago.
Buttons

Buttons to the right offer the following options:

- **Display page in fullscreen mode.**
- **Display page in kiosk mode.** In this mode only page content displayed. The kiosk mode button appears when the fullscreen mode is activated.
- **To exit kiosk mode,** move the mouse cursor until the exit button appears and click on it. Note that you will be taken back to normal mode (not fullscreen mode).

Using filter

You can use the filter to display only the items you are interested in. The Filter link is located above the table to the right. You can use it to filter items by host group, host, application, a string in the item name; you can also select to display items that have no data gathered.

Specifying a parent host group implicitly selects all nested host groups.

Show details allows to extend displayable information on the items. Such details as refresh interval, history and trends settings, item type and item errors (fine/unsupported) are displayed. A link to item configuration is also available.

By default, items without data are shown but details are not displayed.

**Ad-hoc graphs for comparing items**

You may use the checkbox in the second column to select several items and then compare their data in a simple or stacked ad-hoc graph. To do that, select items of interest, then click on the required graph button below the table.

**Links to value history/simple graph**

The last column in the latest value list offers:

- **a History link** (for all textual items) - leading to listings (Values/500 latest values) displaying the history of previous item values.

- **a Graph link** (for all numeric items) - leading to a simple graph. However, once the graph is displayed, a dropdown on the upper right offers a possibility to switch to Values/500 latest values as well.
The values displayed in this list are “raw”, that is, no postprocessing is applied.

**Note:**
The total amount of values displayed is defined by the value of Limit for search and filter results parameter, set in Administration → General.

### 6 Graphs

#### Overview

In the Monitoring → Graphs section any custom graph that has been configured can be displayed.
To display a graph, select the host group, host and then the graph from the dropdowns to the right.

Note: In the host dropdown, a disabled host is highlighted in red. Graphs for disabled hosts are accessible starting with Zabbix 2.2.0.

Time period selector

Take note of the time period selector above the graph. It allows to select often required periods with one mouse click.

See also: Time period selector

Buttons

Buttons to the right offer the following options:

- Add graph to the favorites widget in the Dashboard.
- The graph is in the favorites widget in the Dashboard. Click to remove graph from the favorites widget.
- Display page in fullscreen mode.
- Display page in kiosk mode. In this mode only page content displayed.
  The kiosk mode button appears when the full screen mode is activated.
  To exit kiosk mode, move the mouse cursor until the exit button appears and click on it. Note that you will be taken back to normal mode (not fullscreen mode).

7 Screens

Overview

In the Monitoring → Screens section you can configure, manage and view Zabbix global screens and slideshows.

When you open this section, you will either see the last screen/slideshow you accessed or a listing of all entities you have access to. Screen/Slide show listing can be filtered by name.

Since Zabbix 3.0 all screens/slideshows can be either public or private. The public ones are available to all users, while private ones are accessible only to their owner and the users the entity is shared with.

Use the dropdown in the title bar to switch between screens and slide shows.

Screen listing

Displayed data:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the screen. Click on the name to view the screen.</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Dimensions</td>
<td>The number of columns and rows of the screen.</td>
</tr>
<tr>
<td>Actions</td>
<td>Two actions are available:</td>
</tr>
<tr>
<td></td>
<td><strong>Properties</strong> - edit general screen properties (name and dimensions)</td>
</tr>
<tr>
<td></td>
<td><strong>Constructor</strong> - access the grid of screen elements for editing</td>
</tr>
</tbody>
</table>

To create a new screen, click on the Create screen button in the top right-hand corner. To import a screen from an XML file, click on the Import button in the top right-hand corner. The user who imports the screen will be set as its owner.

**Mass editing options**

Buttons below the list offer some mass-editing options:

- Export - export the screens to an XML file
- Delete - delete the screens

To use these options, mark the checkboxes before the respective screens, then click on the required button.

**Viewing screens**

To view a screen, click on its name in the list of all screens.

**Time period selector**

Take note of the time period selector above the screen. It allows to select often required periods with one mouse click, affecting the data displayed in graphs etc.

See also: **Time period selector**

**Buttons**

Buttons to the right offer the following options:

Go to the screen constructor to edit the screen.
Add screen to the favorites widget in the Dashboard.

The screen is in the favorites widget in the Dashboard. Click to remove screen from the favorites widget.

Display page in fullscreen mode.

Display page in kiosk mode. In this mode only page content displayed.
The kiosk mode button appears when the fullscreen mode is activated.

To exit kiosk mode, move the mouse cursor until the exit button appears and click on it. Note that you will be taken back to normal mode (not fullscreen mode).

Slide show listing

Use the dropdown in the title bar to switch from screens to slide shows.

Displayed data:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the slide show. Click on the name to view the slide show.</td>
</tr>
<tr>
<td>Delay</td>
<td>The default duration of showing one slide is displayed.</td>
</tr>
<tr>
<td>Number of slides</td>
<td>The number of slides in the slide show is displayed.</td>
</tr>
<tr>
<td>Actions</td>
<td>One action is available: Properties - edit slide show properties</td>
</tr>
</tbody>
</table>

To create a new slide show, click on the Create slide show button in the top right-hand corner.

Mass editing options

A button below the list offers one mass-editing option:
  - Delete - delete the slide shows

To use this option, mark the checkboxes before the respective slide shows and click on Delete.

Viewing slide shows

To view a slide show, click on its name in the list of all slide shows.

Buttons

Buttons to the right offer the following options:

Edit slide show

Go to the slide show properties.
Add slide show to the favorites widget in the Dashboard.

The slide show is in the favorites widget in the Dashboard. Click to remove slide show from the favorites widget.

Slow down or speed up a slide show.

Display page in fullscreen mode.

Display page in kiosk mode. In this mode only page content displayed. The kiosk mode button appears when the fullscreen mode is activated.

To exit kiosk mode, move the mouse cursor until the exit button appears and click on it. Note that you will be taken back to normal mode (not fullscreen mode).

Referencing a screen

Screens can be referenced by both elementid and screenname GET parameters. For example,


will open the screen with that name (Zabbix server).

If both elementid (screen ID) and screenname (screen name) are specified, screenname has higher priority.

8 Maps

Overview

In the Monitoring → Maps section you can configure, manage and view network maps.

When you open this section, you will either see the last map you accessed or a listing of all maps you have access to. Map listing can be filtered by name.

Since Zabbix 3.0 all maps can be either public or private. Public maps are available to all users, while private maps are accessible only to their owner and the users the map is shared with.

Map listing

<table>
<thead>
<tr>
<th>Name</th>
<th>Width</th>
<th>Height</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local network</td>
<td>600</td>
<td>600</td>
<td>Properties Constructor</td>
</tr>
<tr>
<td>Local network_2</td>
<td>600</td>
<td>450</td>
<td>Properties Constructor</td>
</tr>
<tr>
<td>Offices</td>
<td>750</td>
<td>600</td>
<td>Properties Constructor</td>
</tr>
</tbody>
</table>

Displayed data:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the map. Click on the name to view the map.</td>
</tr>
<tr>
<td>Width</td>
<td>Map width is displayed.</td>
</tr>
</tbody>
</table>
To **configure** a new map, click on the Create map button in the top right-hand corner. To import a map from an XML file, click on the Import button in the top right-hand corner. The user who imports the map will be set as its owner.

Two buttons below the list offer some mass-editing options:

- Export - export the maps to an XML file
- Delete - delete the maps

To use these options, mark the checkboxes before the respective maps, then click on the required button.

** Viewing maps **

To view a map, click on its name in the list of all maps.

You can use the dropdown in the map title bar to select the lowest severity level of the problem triggers to display. The severity marked as default is the level set in map configuration. If the map contains a submap, navigating to the submap will retain the higher-level map severity (except if it is Not classified, in this case it will not be passed to the submap).

** Icon highlighting **

If a map element is in problem status, it is highlighted with a round circle. The fill color of the circle corresponds to the severity color of the problem. Only problems on or above the selected severity level will be displayed with the element. If all problems are acknowledged, a thick green border around the circle is displayed.

Additionally:

- a host in **maintenance** is highlighted with an orange, filled square. Note that maintenance highlighting has priority over the problem severity highlighting.
- a disabled (not-monitored) host is highlighted with a gray, filled square.

Highlighting is displayed if the Icon highlighting check-box is marked in map **configuration**.

** Recent change markers **
Inward pointing red triangles around an element indicate a recent trigger status change – one that’s happened within the last 30 minutes. These triangles are shown if the Mark elements on trigger status change check-box is marked in map configuration.

Links
Clicking on a map element opens a menu with some available links.

Buttons
Buttons to the right offer the following options:

- Go to map constructor to edit the map content.
- Add map to the favorites widget in the Dashboard.
- The map is in the favorites widget in the Dashboard. Click to remove map from the favorites widget.
- Display page in fullscreen mode.
- Display page in kiosk mode. In this mode only page content displayed. The kiosk mode button appears when the fullscreen mode is activated.
- To exit kiosk mode, move the mouse cursor until the exit button appears and click on it. Note that you will be taken back to normal mode (not fullscreen mode).

Readable summary in maps
A hidden “aria-label” property is available allowing map information to be read with a screen reader. Both general map description and individual element description is available, in the following format:

- for map description: <Map name>, <*> of <*> items in problem state>, <*> problems in total>.
- for describing one element with one problem: <Element type>, Status <Element status>, <Element name>, <Problem description>.
- for describing one element with multiple problems: <Element type>, Status <Element status>, <Element name>, <*> problems>.
- for describing one element without problems: <Element type>, Status <Element status>, <Element name>.

For example, this description is available:

'Local network, 1 of 6 elements in problem state, 1 problem in total. Host, Status problem, My host, Free disk space is ... servers. Host, Status ok, Server 1. Host, Status ok, Server 2. Host, Status ok, Server 3. Host, Status ok, Server 4. ' for the following map:
Referencing a network map

Network maps can be referenced by both sysmapid and mapname GET parameters. For example, 
http://zabbix/zabbix/zabbix.php?action=map.view&mapname=Local%20network
will open the map with that name (Local network).

If both sysmapid (map ID) and mapname (map name) are specified, mapname has higher priority.

9 Discovery

Overview

In the Monitoring → Discovery section results of network discovery are shown. Discovered devices are sorted by the discovery rule.

With nothing selected in the filter, all enabled discovery rules are displayed. To select a specific discovery rule for display, start typing its name in the filter. All matching enabled discovery rules will be listed for selection. More than one discovery rule can be selected.

Note that in Zabbix 4.0.0-4.0.6 there is a dropdown instead of the filter for discovery rule selecting.
If a device is already monitored, the host name will be listed in the Monitored host column, and the duration of the device being discovered or lost after previous discovery is shown in the Uptime/Downtime column.

After that follow the columns showing the state of individual services for each discovered device (red cells show services that are down). Service uptime or downtime is included within the cell.

**Attention:**
Only those services that have been found on at least one device will have a column showing their state.

**Buttons**

Buttons to the right offer the following options:

- Display page in fullscreen mode.
- Display page in kiosk mode. In this mode only page content displayed.
  The kiosk mode button appears when the fullscreen mode is activated.

To exit kiosk mode, move the mouse cursor until the exit button appears and click on it. Note that you will be taken back to normal mode (not fullscreen mode).

**10 Services**

**Overview**

In the Monitoring → Services section the status of IT infrastructure or business services is displayed.

<table>
<thead>
<tr>
<th>Service</th>
<th>Status</th>
<th>Reason</th>
<th>Problem time</th>
<th>SLA / Acceptable SLA</th>
</tr>
</thead>
<tbody>
<tr>
<td>root</td>
<td>OK</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&gt; Servers</td>
<td>OK</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&gt; Business system</td>
<td>OK</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&gt; Network service</td>
<td>OK</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch1 - Operational status was changed on Switch1 interface DEFAULT_VLAN</td>
<td>OK</td>
<td></td>
<td>100.0000</td>
<td>99.9000</td>
</tr>
<tr>
<td>&gt; Public cloud service</td>
<td>Warning</td>
<td>Free disk space is less than 20% on volume /</td>
<td>100.0000</td>
<td>0.0000</td>
</tr>
<tr>
<td>Cloud1 - Free disk space is less than 20% on volume /</td>
<td>Warning</td>
<td>Free disk space is less than 20% on volume /</td>
<td>Only the last 20% of the indicator is displayed.</td>
<td></td>
</tr>
</tbody>
</table>

A list of the existing services is displayed along with data of their status and SLA. From the dropdown in the upper right corner you can select a desired period for display.

**Displayed data:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
<td>Service name.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of service: OK - no problems (trigger color and severity) - indicates a problem and its severity</td>
</tr>
<tr>
<td>Reason</td>
<td>Indicates the reason of problem (if any).</td>
</tr>
<tr>
<td>Problem time</td>
<td>Displays SLA bar. Green/red ratio indicates the proportion of availability/problems. The bar displays the last 20% of SLA (from 80% to 100%). The bar contains a link to a graph of availability data.</td>
</tr>
</tbody>
</table>
Parameter | Description
--- | ---
SLA/Acceptable SLA | Displays current SLA/expected SLA value. If current value is below the acceptable level, it is displayed in red.

You can also click on the service name to access the Service availability report.

Here you can assess service availability data over a longer period of time on daily/weekly/monthly/yearly basis.

Buttons

Buttons to the right offer the following options:

- Display page in fullscreen mode.
- Display page in kiosk mode. In this mode only page content displayed. The kiosk mode button appears when the fullscreen mode is activated.
- To exit kiosk mode, move the mouse cursor until the exit button appears and click on it. Note that you will be taken back to normal mode (not fullscreen mode).

2 Inventory

Overview

The Inventory menu features sections providing an overview of host inventory data by a chosen parameter as well as the ability to view host inventory details.

1 Overview

Overview

The Inventory → Overview section provides ways of having an overview of host inventory data.

For an overview to be displayed, choose a host group (or all groups) and the inventory field by which to display data. The number of hosts corresponding to each entry of the chosen field will be displayed.

The completeness of an overview depends on how much inventory information is maintained with the hosts.

Numbers in the Host count column are links; they lead to these hosts being filtered out in the Host Inventories table.
2 Hosts

Overview

In the Inventory → Hosts section inventory data of hosts are displayed.

Select a group from the dropdown in the upper right corner to display the inventory data of hosts in that group. You can also filter the hosts by any inventory field to display only the hosts you are interested in.

To display all host inventories, select "all" in the group dropdown, clear the comparison field in the filter and press "Filter".

While only some key inventory fields are displayed in the table, you can also view all available inventory information for that host. To do that, click on the host name in the first column.

Inventory details

The Overview tab contains some general information about the host along with links to predefined scripts, latest monitoring data and host configuration options:
The **Details** tab contains all available inventory details for the host:

<table>
<thead>
<tr>
<th>Overview</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>Zabbix server</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>linux-qwt</td>
</tr>
<tr>
<td><strong>OS</strong></td>
<td>Linux version 3.11.10-21-default #1 SMP Mon Jul 21 15:28:46 U</td>
</tr>
<tr>
<td><strong>OS (Full details)</strong></td>
<td>Linux version 3.11.10-21-default (geeko@buildhost) (gcc version 4.8.1 20130909 (gcc 4.8-branch revision 202388) (SUSE Linux)) #1 SMP Mon Jul 21 15:28:46 UTC 2014 (9a9585d)</td>
</tr>
<tr>
<td><strong>MAC address</strong></td>
<td>[enp0s3] 08:00:27:52:c4:53, [enp0s3] 08:00:27:52:c4:53</td>
</tr>
<tr>
<td><strong>Location</strong></td>
<td>Head Office</td>
</tr>
<tr>
<td><strong>Site city</strong></td>
<td>Riga</td>
</tr>
</tbody>
</table>

The completeness of inventory data depends on how much inventory information is maintained with the host. If no information is maintained, the Details tab is disabled.

### 3 Reports

**Overview**

The Reports menu features several sections that contain a variety of predefined and user-customizable reports focused on displaying an overview of such parameters as system information, triggers and gathered data.

### 1 System information

**Overview**

In Reports → System information a summary of key system data is displayed.

<table>
<thead>
<tr>
<th>System information</th>
<th>Value</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zabbix server is running</td>
<td>Yes</td>
<td>localhost:10001</td>
</tr>
<tr>
<td>Number of hosts (enabled/disabled/templates)</td>
<td>92</td>
<td>12 / 0 / 80</td>
</tr>
<tr>
<td>Number of items (enabled/disabled/not supported)</td>
<td>349</td>
<td>330 / 0 / 19</td>
</tr>
<tr>
<td>Number of triggers (enabled/disabled [problem/ok])</td>
<td>211</td>
<td>209 / 3 [18 / 192]</td>
</tr>
<tr>
<td>Number of users (online)</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Required server performance, new values per second</td>
<td>7.32</td>
<td></td>
</tr>
</tbody>
</table>

This report is also displayed as a widget in the Dashboard.

Displayed data
Parameter | Value |
--- | ---
Zabbix server is running | Status of Zabbix server: **Yes** - server is running  
**No** - server is not running  
*Note: To display the rest of the information the web frontend needs the server to be running and there must be at least one trapper process started on the server (StartTrappers parameter in `zabbix_server.conf` file > 0).*

Location and port of Zabbix server.

Number of hosts | Total number of hosts configured is displayed.  
Templates are counted as a type of host too.

Number of monitored hosts/not monitored hosts/templates.

Number of items | Total number of items is displayed.

Number of monitored/disabled/unsupported items.

Items on disabled hosts are counted as disabled.

Number of triggers | Total number of triggers is displayed.

Number of enabled/disabled triggers.  
[Triggers in problem/ok state.]

Triggers assigned to disabled hosts or depending on disabled items are counted as disabled.

Number of users | Total number of users configured is displayed.

Number of users online.

Required server performance, new values per second | The expected number of new values processed by Zabbix server per second is displayed.

Required server performance is an estimate and can be useful as a guideline. For precise numbers of values processed, use the `zabbix[wcache,values,all]` internal item.

Enabled items from monitored hosts are included in the calculation. Log items are counted as one value per item update interval. Regular interval values are counted; flexible and scheduling interval values are not. The calculation is not adjusted during a “nodata” maintenance period. Trapper items are not counted.

Starting with Zabbix 4.0.18, System information will also display an error message if the database used does not have the required character set or collation (UTF-8).

2 Availability report

Overview

In Reports → Availability report you can see what proportion of time each trigger has been in problem/ok state. The percentage of time for each state is displayed.

Thus it is easy to determine the availability situation of various elements on your system.
From the dropdown in the upper right corner you can choose the selection mode - whether to display triggers by hosts or by triggers belonging to a template.

The name of the trigger is a link to the latest events of that trigger.

Using filter
Filter can help narrow down the number of hosts and/or triggers displayed. The filter is located below the Availability report bar. It can be opened and collapsed by clicking on the Filter tab on the left.

Filtering by trigger template
In the by trigger template mode results can be filtered by one or several parameters listed below.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template group</td>
<td>Select all hosts with triggers from templates belonging to that group. Any host group that includes at least one template can be selected.</td>
</tr>
<tr>
<td>Template</td>
<td>Select hosts with triggers from chosen template and all nested templates. Only triggers inherited from the selected template will be displayed. If a nested template has additional own triggers, those triggers will not be displayed.</td>
</tr>
<tr>
<td>Template trigger</td>
<td>Select hosts with chosen trigger. Other triggers of the selected hosts will not be displayed.</td>
</tr>
<tr>
<td>Host group</td>
<td>Select hosts belonging to the group.</td>
</tr>
</tbody>
</table>
Filtering by host

In the by host mode results can be filtered by host or by host group. Specifying a parent host group implicitly selects all nested host groups.

Time period selector

The time period selector allows to select often required periods with one mouse click. The time period selector can be opened by clicking on the time period tab next to the filter.

Clicking on Show in the Graph column displays a bar graph where availability information is displayed in bar format each bar representing a past week of the current year.

The green part of a bar stands for OK time and red for problem time.

3 Triggers top 100

Overview

In Reports → Triggers top 100 you can see the triggers that have changed their state most often within the period of evaluation, sorted by the number of status changes.

Both host and trigger column entries are links that offer some useful options:
• for host - links to user-defined scripts, latest data, inventory, graphs and screens for the host
• for trigger - links to latest events, the trigger configuration form and a simple graph

**Using filter**

You may use the filter to display triggers by host group, host or trigger severity. Specifying a parent host group implicitly selects all nested host groups.

The filter is located below the 100 busiest triggers bar. It can be opened and collapsed by clicking on the Filter tab on the left.

**Time period selector**

The *time period selector* allows to select often required periods with one mouse click. The time period selector can be opened by clicking on the time period tab next to the filter.

### 4 Audit

**Overview**

In the Reports → Audit section users can view records of changes made in the frontend.

**Audit log**

In this screen the audit log of various changes made in the frontend can be seen.

**Displayed data:**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Timestamp of the audit record.</td>
</tr>
<tr>
<td>User</td>
<td>User of the activity.</td>
</tr>
<tr>
<td>IP</td>
<td>IP that was used in the activity.</td>
</tr>
<tr>
<td>Resource</td>
<td>Affected resource is displayed.</td>
</tr>
<tr>
<td>Action</td>
<td>Activity type is displayed - Login, Logout, Added, Updated, Deleted, Enabled or Disabled.</td>
</tr>
<tr>
<td>ID</td>
<td>ID of the affected resource is displayed.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the resource is displayed.</td>
</tr>
<tr>
<td>Details</td>
<td>Detailed information on the performed activity is displayed.</td>
</tr>
</tbody>
</table>

**Using filter**

You may use the filter to narrow down the records by user, activity type and affected resource.

The filter is located below the Audit log bar. It can be opened and collapsed by clicking on the Filter tab on the left.

**Time period selector**
The **time period selector** allows to select often required periods with one mouse click. The time period selector can be opened by clicking on the time period tab next to the filter.

### 5 Action log

#### Overview

In this screen details of operations (notifications, remote commands) executed within an action are displayed.

#### Displayed data:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Timestamp of the operation.</td>
</tr>
<tr>
<td>Action</td>
<td>Name of the action causing operations is displayed.</td>
</tr>
<tr>
<td>Type</td>
<td>Operation type is displayed - Email or Command.</td>
</tr>
<tr>
<td>Recipient(s)</td>
<td>User alias, name and surname (in parenthesis) and e-mail address of the notification recipient is displayed.</td>
</tr>
<tr>
<td>Message</td>
<td>The content of the message/remote command is displayed.</td>
</tr>
<tr>
<td>Status</td>
<td>Operation status is displayed:</td>
</tr>
<tr>
<td>Info</td>
<td>Error information (if any) regarding the action execution is displayed.</td>
</tr>
</tbody>
</table>

#### Using filter

You may use the filter to narrow down the records by the recipient of e-mail.

The filter is located below the Action log bar. It can be opened and collapsed by clicking on the Filter tab on the left.

#### Time period selector

The **time period selector** allows to select often required periods with one mouse click. The time period selector can be opened by clicking on the time period tab next to the filter.
6 Notifications

Overview

In the Reports → Notifications section a report on the number of notifications sent to each user is displayed.

From the dropdowns in the top right-hand corner you can choose the media type (or all), period (data for each day/week/month/year) and year for the notifications sent.

<table>
<thead>
<tr>
<th>DAY</th>
<th>Media type</th>
<th>Period</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-01-01</td>
<td>ADMIN (ZABBIX ADMINISTRATOR)</td>
<td>Daily</td>
<td>2016</td>
</tr>
<tr>
<td>2016-01-02</td>
<td>GUEST</td>
<td>Daily</td>
<td>2016</td>
</tr>
<tr>
<td>2016-01-03</td>
<td>USER (NEW USER)</td>
<td>Daily</td>
<td>2016</td>
</tr>
<tr>
<td>2016-01-04</td>
<td>ADMIN (ZABBIX ADMINISTRATOR)</td>
<td>Daily</td>
<td>2016</td>
</tr>
<tr>
<td>2016-01-05</td>
<td>GUEST</td>
<td>Daily</td>
<td>2016</td>
</tr>
<tr>
<td>2016-01-06</td>
<td>USER (NEW USER)</td>
<td>Daily</td>
<td>2016</td>
</tr>
<tr>
<td>2016-01-07</td>
<td>ADMIN (ZABBIX ADMINISTRATOR)</td>
<td>Daily</td>
<td>2016</td>
</tr>
<tr>
<td>2016-01-08</td>
<td>GUEST</td>
<td>Daily</td>
<td>2016</td>
</tr>
<tr>
<td>2016-01-09</td>
<td>USER (NEW USER)</td>
<td>Daily</td>
<td>2016</td>
</tr>
</tbody>
</table>

Each column displays totals per one system user.

4 Configuration

Overview

The Configuration menu contains sections for setting up major Zabbix functions, such as hosts and host groups, data gathering, data thresholds, sending problem notifications, creating data visualization and others.

1 Host groups

Overview

In the Configuration → Host groups section users can configure and maintain host groups. A host group can contain both templates and hosts.

A listing of existing host groups with their details is displayed. You can search and filter host groups by name.
### Column Description

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the host group. Clicking on the group name opens the host group configuration form.</td>
</tr>
<tr>
<td>Hosts</td>
<td>Number of hosts in the group (displayed in gray). Clicking on &quot;Hosts&quot; will, in the whole listing of hosts, filter out those that belong to the group.</td>
</tr>
<tr>
<td>Templates</td>
<td>Number of templates in the group (displayed in gray). Clicking on “Templates” will, in the whole listing of templates, filter out those that belong to the group.</td>
</tr>
<tr>
<td>Members</td>
<td>Names of group members. Template names are displayed in gray, monitored host names in blue and non-monitored host names in red. Clicking on a name will open the template/host configuration form.</td>
</tr>
<tr>
<td>Info</td>
<td>Error information (if any) regarding the host group is displayed.</td>
</tr>
</tbody>
</table>

### Mass editing options

Buttons below the list offer some mass-editing options:

- **Enable hosts** - change the status of all hosts in the group to “Monitored”
- **Disable hosts** - change the status of all hosts in the group to “Not monitored”
- **Delete** - delete the host groups

To use these options, mark the checkboxes before the respective host groups, then click on the required button.

---

### 2 Templates

### Overview

In the Configuration → Templates section users can configure and maintain templates.

A listing of existing templates with their details is displayed.
From the dropdown to the right in the title bar you can choose whether to display all templates or only those belonging to a group.

Displayed data:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Templates</td>
<td>Name of the template. Clicking on the template name opens the template</td>
</tr>
<tr>
<td></td>
<td>configuration form.</td>
</tr>
<tr>
<td>Entities (Applications,</td>
<td>Number of the respective entities in the template (displayed in gray). Clicking</td>
</tr>
<tr>
<td>Items, Triggers,</td>
<td>on the entity name will, in the whole listing of that entity, filter out those</td>
</tr>
<tr>
<td>Graphs, Screens,</td>
<td>that belong to the template.</td>
</tr>
<tr>
<td>Discovery, Web)</td>
<td></td>
</tr>
<tr>
<td>Linked templates</td>
<td>Templates that are linked to the template, in a nested setup where the</td>
</tr>
<tr>
<td></td>
<td>template will inherit all entities of the linked templates.</td>
</tr>
<tr>
<td>Linked to</td>
<td>The hosts and templates that the template is linked to.</td>
</tr>
</tbody>
</table>

To configure a new template, click on the Create template button in the top right-hand corner. To import a template from an XML file, click on the Import button in the top right-hand corner.

Mass editing options

Buttons below the list offer some mass-editing options:

- Export - export the template to an XML file
- Delete - delete the template while leaving its linked entities (items, triggers etc.) with the hosts
- Delete and clear - delete the template and its linked entities from the hosts

To use these options, mark the checkboxes before the respective templates, then click on the required button.

Filter

As the list may contain very many templates, it may be needed to filter out the ones you really need.

The Filter link is available above the list of templates. If you click on it, a filter becomes available where you can filter templates by name and directly linked templates (since 4.0.1).
Overview

In the Configuration → Hosts section users can configure and maintain hosts.

A listing of existing hosts with their details is displayed.

From the dropdown to the right in the Hosts bar you can choose whether to display all hosts or only those belonging to one particular group.

Displayed data:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the host. Clicking on the host name opens the host configuration form.</td>
</tr>
<tr>
<td>Elements (Applications, Items, Triggers, Graphs, Discovery, Web)</td>
<td>Clicking on the element name will display items, triggers etc. of the host. The number of the respective elements is displayed in gray.</td>
</tr>
<tr>
<td>Interface</td>
<td>The main interface of the host is displayed.</td>
</tr>
<tr>
<td>Templates</td>
<td>The templates linked to the host are displayed. If other templates are contained in the linked template, those are displayed in parentheses, separated by a comma. Clicking on a template name will open its configuration form.</td>
</tr>
<tr>
<td>Status</td>
<td>Host status is displayed - Enabled or Disabled. By clicking on the status you can change it. An orange wrench icon before the host status indicates that this host is in maintenance (since Zabbix 4.0.9). Maintenance details are displayed when the mouse pointer is positioned over the icon.</td>
</tr>
<tr>
<td>Availability</td>
<td>Availability of the host is displayed. Four icons each represent a supported interface (Zabbix agent, SNMP, IPMI, JMX). The current status of the interface is displayed by the respective color: Green - available Red - not available (upon mouseover, details of why the interface cannot be reached are displayed) Gray - unknown or not configured Note that active Zabbix agent items do not affect host availability.</td>
</tr>
<tr>
<td>Agent encryption</td>
<td>Encryption status for connections to the host is displayed: None - no encryption PSK - using pre-shared key Cert - using certificate</td>
</tr>
<tr>
<td>Info</td>
<td>Error information (if any) regarding the host is displayed.</td>
</tr>
</tbody>
</table>

To configure a new host, click on the Create host button in the top right-hand corner. To import a host from an XML file, click on the Import button in the top right-hand corner.

Mass editing options

Buttons below the list offer some mass-editing options:

- Enable - change host status to Monitored
- Disable - change host status to Not monitored
- Export - export the hosts to an XML file
- Mass update - update several properties for a number of hosts at once
- Delete - delete the hosts
To use these options, mark the checkboxes before the respective hosts, then click on the required button.

Filter

As the list may contain very many hosts, it may be needed to filter out the ones you really need.

The Filter link is available above the list of hosts. If you click on it, a filter becomes available where you can filter hosts by name, linked templates (since 4.0.1), if they are monitored by server or by proxy, proxy name, DNS, IP or port number.

Reading host availability

Host availability icons reflect the current host interface status on Zabbix server. Therefore, in the frontend:

- If you disable a host, availability icons will not immediately turn gray (unknown status), because the server has to synchronize the configuration changes first;
- If you enable a host, availability icons will not immediately turn green (available), because the server has to synchronize the configuration changes and start polling the host first.

Unknown host status

Zabbix server sets the host availability icon to gray (unknown status) for the corresponding agent interface (Zabbix, SNMP, IPMI, JMX) if:

- there are no enabled items on the interface (they were removed or disabled);
- there are only active Zabbix agent items;
- there are no pollers for that type of the interface (e.g. StartPollers=0);
- host is disabled;
- host is set to be monitored by proxy, a different proxy or by server if it was monitored by proxy;
- host is monitored by a proxy that appears to be offline (no updates received from the proxy during the maximum heartbeat interval - 1 hour).

Setting host availability to unknown is done after server configuration cache synchronization. Restoring host availability (available/unavailable) on hosts monitored by proxies is done after proxy configuration cache synchronization.

See also more details about host unreachability.

1 Applications

Overview

The application list for a template can be accessed from Configuration → Templates and then clicking on Applications for the respective template.

The application list for a host can be accessed from Configuration → Hosts and then clicking on Applications for the respective host.

A list of existing applications is displayed.
Displayed data:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Name of the application, displayed as a blue link for directly created applications. Clicking on the application name link opens the application configuration form. If the host application belongs to a template, the template name is displayed before the application name, as a gray link. Clicking on the template link will open the application list on the template level.</td>
</tr>
<tr>
<td>Items</td>
<td>Click on Items to view the items contained in the application. The number of items is displayed in gray.</td>
</tr>
<tr>
<td>Info</td>
<td>Error information (if any) regarding the application is displayed.</td>
</tr>
</tbody>
</table>

To configure a new application, click on the Create application button in the top right-hand corner.

Mass editing options

Buttons below the list offer some mass-editing options:

- Enable - change application status to Enabled
- Disable - change application status to Disabled
- Delete - delete the applications

To use these options, mark the checkboxes before the respective applications, then click on the required button.

2 Items

Overview

The item list for a template can be accessed from Configuration → Templates and then clicking on Items for the respective template.

The item list for a host can be accessed from Configuration → Hosts and then clicking on Items for the respective host.

A list of existing items is displayed.
Displayed data:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wizard</td>
<td>The wizard icon is a link to a wizard for creating a trigger based on the item. Name of the item, displayed as a blue link to item details. Clicking on the item name link opens the item configuration form. If the host item belongs to a template, the template name is displayed before the item name, as a gray link. Clicking on the template link will open the item list on the template level. If the item has been created from an item prototype, its name is preceded by the low level discovery rule name, in orange. Clicking on the discovery rule name will open the item prototype list.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the item, displayed as a blue link to item details.</td>
</tr>
<tr>
<td>Triggers</td>
<td>Moving the mouse over Triggers will display an info box displaying the triggers associated with the item. The number of the triggers is displayed in gray.</td>
</tr>
<tr>
<td>Key</td>
<td>Item key is displayed.</td>
</tr>
<tr>
<td>Interval</td>
<td>Frequency of the check is displayed. Note that passive items can also be checked immediately by pushing the Check now button.</td>
</tr>
<tr>
<td>History</td>
<td>How many days item data history will be kept is displayed.</td>
</tr>
<tr>
<td>Trends</td>
<td>How many days item trends history will be kept is displayed.</td>
</tr>
<tr>
<td>Type</td>
<td>Item type is displayed (Zabbix agent, SNMP agent, simple check, etc).</td>
</tr>
<tr>
<td>Applications</td>
<td>Item applications are displayed.</td>
</tr>
<tr>
<td>Status</td>
<td>Item status is displayed - Enabled, Disabled or Not supported. By clicking on the status you can change it - from Enabled to Disabled (and back); from Not supported to Disabled (and back).</td>
</tr>
<tr>
<td>Info</td>
<td>If everything is fine, no icon is displayed in this column. If there are errors, a red square icon with a cross is displayed. Move the mouse over the icon and you will see a tooltip with the error description.</td>
</tr>
</tbody>
</table>

To configure a new item, click on the Create item button in the top right-hand corner.

Mass editing options

Buttons below the list offer some mass-editing options:

- Enable - change item status to Enabled
- Disable - change item status to Disabled
- Check now - execute a check for new item values immediately. Supported for passive checks only (see more details). Note that when checking for values immediately, configuration cache is not updated, thus the values will not reflect very recent changes to item configuration.
- Clear history - delete history and trend data for items
- Copy - copy the items to other hosts or templates
- Mass update - update several properties for a number of items at once
- Delete - delete the items

To use these options, mark the checkboxes before the respective items, then click on the required button.

Filter
As the list may contain very many items, it may be needed to filter out the ones you really need.

The Filter link is available above the list. If you click on it, a filter becomes available where you can filter items by several properties.

The Subfilter below the filter offers further filtering options (for the data already filtered). You can select groups of items with a common parameter value. If you click on a group it gets highlighted and only the items with this parameter value remain in the list.

3 Triggers

Overview

The trigger list for a template can be accessed from Configuration → Templates and then clicking on Triggers for the respective template.

The trigger list for a host can be accessed from Configuration → Hosts and then clicking on Triggers for the respective host.

Displayed data:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity</td>
<td>Severity of the trigger is displayed by both name and cell background color.</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Value</td>
<td>Trigger value is displayed:&lt;br&gt;<strong>OK</strong> - trigger is in OK state&lt;br&gt;<strong>PROBLEM</strong> - trigger is in problem state&lt;br&gt;This column is available since Zabbix 4.0.0.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the trigger, displayed as a blue link to trigger details.&lt;br&gt;Clicking on the trigger name link opens the trigger configuration form.&lt;br&gt; If the host trigger belongs to a template, the template name is displayed before the trigger name, as a gray link. Clicking on the template link will open the trigger list on the template level.&lt;br&gt; If the trigger has been created from a trigger prototype, its name is preceded by the low level discovery rule name, in orange. Clicking on the discovery rule name will open the trigger prototype list.</td>
</tr>
<tr>
<td>Expression</td>
<td>Trigger expression is displayed. The host-item part of the expression is displayed as a link, leading to the item configuration form.</td>
</tr>
<tr>
<td>Status</td>
<td>Trigger status is displayed - Enabled, Disabled or Unknown. By clicking on the status you can change it - from Enabled to Disabled (and back); from Unknown to Disabled (and back).&lt;br&gt;Problems of a disabled trigger are no longer displayed in the frontend, but are not deleted.</td>
</tr>
<tr>
<td>Info</td>
<td>If everything is fine, no icon is displayed in this column. If there are errors, a red square icon with a cross is displayed. Move the mouse over the icon and you will see a tooltip with the error description.</td>
</tr>
<tr>
<td>Tags</td>
<td>If trigger contains tags, tag name and value are displayed in this column.</td>
</tr>
</tbody>
</table>

To configure a new trigger, click on the Create trigger button in the top right-hand corner.

Mass editing options

Buttons below the list offer some mass-editing options:

- Enable - change trigger status to Enabled
- Disable - change trigger status to Disabled
- Copy - copy the triggers to other hosts or templates
- Mass update - update several properties for a number of triggers at once
- Delete - delete the triggers

To use these options, mark the checkboxes before the respective triggers, then click on the required button.

Using filter

You can use the filter to display only the problems you are interested in. The filter is located above the table.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity</td>
<td>Filter by trigger severity.</td>
</tr>
<tr>
<td>State</td>
<td>Filter by trigger state.</td>
</tr>
<tr>
<td>Status</td>
<td>Filter by trigger status.</td>
</tr>
<tr>
<td>Value</td>
<td>Filter by trigger value.</td>
</tr>
</tbody>
</table>
Parameter Description

Tags Filter by trigger tag name and tag value.
Several conditions can be set. There are two calculation types for conditions:
- **And/Or** - all conditions must be met, conditions having same tag name will be grouped by Or condition
- **Or** - enough if one condition is met
There are two ways of matching the tag value:
- **Contains** - case-sensitive substring match (tag value contains the entered string)
- **Equals** - case-sensitive string match (tag value equals the entered string)
When filtered, the tags specified here will be displayed first with the trigger.
Macros and *macro functions* are supported both in tag name and tag value fields.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the custom graph, displayed as a blue link to graph details.</td>
</tr>
<tr>
<td>Width</td>
<td>Graph width is displayed.</td>
</tr>
<tr>
<td>Height</td>
<td>Graph height is displayed.</td>
</tr>
<tr>
<td>Graph type</td>
<td>Graph type is displayed - Normal, Stacked, Pie or Exploded.</td>
</tr>
</tbody>
</table>

4 Graphs

Overview

The custom graph list for a template can be accessed from Configuration → Templates and then clicking on Graphs for the respective template.

The custom graph list for a host can be accessed from Configuration → Hosts and then clicking on Graphs for the respective host.

A list of existing graphs is displayed.

Displayed data:

To configure a new graph, click on the Create graph button in the top right-hand corner.

Mass editing options

Buttons below the list offer some mass-editing options:
• Copy - copy the graphs to other hosts or templates
• Delete - delete the graphs

To use these options, mark the checkboxes before the respective graphs, then click on the required button.

5 Discovery rules

Overview

The list of low-level discovery rules for a template can be accessed from Configuration → Templates and then clicking on Discovery for the respective template.

The list of low-level discovery rules for a host can be accessed from Configuration → Hosts and then clicking on Discovery for the respective host.

A list of existing low-level discovery rules is displayed.

![Discovery rules table](image)

Displayed data:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the rule, displayed as a blue link. Clicking on the rule name opens the low-level discovery rule configuration form. If the discovery rule belongs to a template, the template name is displayed before the rule name, as a gray link. Clicking on the template link will open the rule list on the template level.</td>
</tr>
<tr>
<td>Items</td>
<td>A link to the list of item prototypes is displayed. The number of existing item prototypes is displayed in gray.</td>
</tr>
<tr>
<td>Triggers</td>
<td>A link to the list of trigger prototypes is displayed. The number of existing trigger prototypes is displayed in gray.</td>
</tr>
<tr>
<td>Graphs</td>
<td>A link to the list of graph prototypes displayed. The number of existing graph prototypes is displayed in gray.</td>
</tr>
<tr>
<td>Hosts</td>
<td>A link to the list of host prototypes displayed. The number of existing host prototypes is displayed in gray.</td>
</tr>
<tr>
<td>Key</td>
<td>The item key used for discovery is displayed.</td>
</tr>
<tr>
<td>Interval</td>
<td>The frequency of performing discovery is displayed. Note that discovery can also be performed immediately by pushing the Check now button below the list.</td>
</tr>
<tr>
<td>Type</td>
<td>The item type used for discovery is displayed (Zabbix agent, SNMP agent, etc.).</td>
</tr>
<tr>
<td>Status</td>
<td>Discovery rule status is displayed - Enabled, Disabled or Not supported. By clicking on the status you can change it - from Enabled to Disabled (and back); from Not supported to Disabled (and back).</td>
</tr>
<tr>
<td>Info</td>
<td>If everything is fine, no icon is displayed in this column. If there are errors, a red square icon with a cross is displayed. Move the mouse over the icon and you will see a tooltip with the error description.</td>
</tr>
</tbody>
</table>

To configure a new low-level discovery rule, click on the Create discovery rule button in the top right-hand corner.

Mass editing options

Buttons below the list offer some mass-editing options:

- Enable - change the low-level discovery rule status to Enabled
- Disable - change the low-level discovery rule status to Disabled
• Check now - perform discovery based on the discovery rules immediately. See more details. Note that when performing discovery immediately, the configuration cache is not updated, thus the result will not reflect very recent changes to discovery rule configuration
• Delete - delete the low-level discovery rules

To use these options, mark the checkboxes before the respective discovery rules, then click on the required button.

6 Web scenarios

Overview

The web scenario list for a template can be accessed from Configuration → Templates and then clicking on Web for the respective template.

The web scenario list for a host can be accessed from Configuration → Hosts and then clicking on Web for the respective host.

A list of existing web scenarios is displayed. From the dropdown to the right in the Scenarios bar you can choose whether to display all web scenarios or only those belonging to one particular group and host. Additionally you can choose to hide disabled scenarios (or show them again) by clicking on the respective link.

Displayed data:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the web scenario. Clicking on the web scenario name opens the web scenario configuration form.</td>
</tr>
<tr>
<td>Number of steps</td>
<td>The number of steps contained in the scenario.</td>
</tr>
<tr>
<td>Update interval</td>
<td>How often the scenario is performed.</td>
</tr>
<tr>
<td>Attempts</td>
<td>How many attempts for executing web scenario steps are performed.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Authentication method is displayed - Basic, NTLM or None.</td>
</tr>
<tr>
<td>HTTP proxy</td>
<td>Displays HTTP proxy or ‘No’ if not used.</td>
</tr>
<tr>
<td>Application</td>
<td>Web scenario application is displayed.</td>
</tr>
<tr>
<td>Status</td>
<td>Web scenario status is displayed - Enabled or Disabled.</td>
</tr>
<tr>
<td>Info</td>
<td>By clicking on the status you can change it.</td>
</tr>
<tr>
<td></td>
<td>If everything is fine, no icon is displayed in this column. If there are errors, a red square icon with a cross is displayed. Move the mouse over the icon and you will see a tooltip with the error description.</td>
</tr>
</tbody>
</table>

To configure a new web scenario, click on the Create web scenario button in the top right-hand corner.

Mass editing options

Buttons below the list offer some mass-editing options:

• Enable - change the scenario status to Enabled
• Disable - change the scenario status to Disabled
• Clear history - clear history and trend data for the scenarios
• Delete - delete the web scenarios

To use these options, mark the checkboxes before the respective web scenarios, then click on the required button.

4 Maintenance

Overview
In the Configuration → Maintenance section users can configure and maintain maintenance periods for hosts.

A listing of existing maintenance periods with their details is displayed.

From the dropdown to the right in the Maintenance periods bar you can choose whether to display all maintenance periods or only those belonging to one particular group.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the maintenance period. Clicking on the maintenance period name opens the maintenance period configuration form.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of maintenance is displayed: With data collection or No data collection</td>
</tr>
<tr>
<td>Active since</td>
<td>The date and time when executing maintenance periods becomes active.</td>
</tr>
<tr>
<td>Active till</td>
<td>The date and time when executing maintenance periods stops being active.</td>
</tr>
<tr>
<td>State</td>
<td>The state of the maintenance period:</td>
</tr>
<tr>
<td></td>
<td>Approaching - will become active soon</td>
</tr>
<tr>
<td></td>
<td>Active - is active</td>
</tr>
<tr>
<td></td>
<td>Expired - is not active any more</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the maintenance period is displayed.</td>
</tr>
</tbody>
</table>

Name, Type, Active since and Active till are sortable columns that can be sorted in ascending/descending order. To sort, click on the column name.

To configure a new maintenance period, click on the Create maintenance period button in the top right-hand corner.

Mass editing options

A button below the list offers one mass-editing option:

- Delete - delete the maintenance periods

To use this option, mark the checkboxes before the respective maintenance periods and click on Delete.

Filter

As the list may contain a number of maintenance periods, it may be needed to filter out the ones you really need.

The Filter link is available above the list of maintenance periods. If you click on it, a filter becomes available where you can filter maintenance periods by name and state.

5 Actions

Overview

In the Configuration → Actions section users can configure and maintain actions.

A listing of existing actions with their details is displayed. The actions displayed are actions assigned to the selected event source (triggers, discovery, auto-registration).

To view actions assigned to a different event source, change the source from the dropdown to the right in the Actions bar.
For users without Super-admin rights actions are displayed according to permission settings. That means in some cases a user without Super-admin rights isn’t able to view the complete action list because of certain permission restrictions. An action is displayed to the user without Super-admin rights if the following conditions are fulfilled:

- The user has read-write access to host groups, hosts, templates and triggers in action conditions
- The user has read-write access to host groups, hosts and templates in action operations, recovery operations and update operations
- The user has read access to user groups and users in action operations, recovery operations and update operations

Displayed data:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the action. Clicking on the action name opens the action configuration form.</td>
</tr>
<tr>
<td>Conditions</td>
<td>Action conditions are displayed.</td>
</tr>
<tr>
<td>Operations</td>
<td>Action operations are displayed. Since Zabbix 2.2, the operation list also displays the media type (e-mail, SMS, Jabber, etc) used for notification as well as the name and surname (in parentheses after the alias) of a notification recipient. Action operation can both be a notification or a remote command depending on the selected type of operation.</td>
</tr>
<tr>
<td>Status</td>
<td>Action status is displayed - Enabled or Disabled. By clicking on the status you can change it. See the Escalations section for more details as to what happens if an action is disabled during an escalation in progress.</td>
</tr>
</tbody>
</table>

To configure a new action, click on the Create action button in the top right-hand corner.

Mass editing options

Buttons below the list offer some mass-editing options:

- Enable - change the action status to Enabled
- Disable - change the action status to Disabled
- Delete - delete the actions

To use these options, mark the checkboxes before the respective actions, then click on the required button.

Filter

As the list may contain a number of actions, it may be needed to filter out the ones you really need.

The Filter link is available above the list of actions. If you click on it, a filter becomes available where you can filter actions by name and status.

6 Event correlation

Overview

In the Configuration → Event correlation section users can configure and maintain global correlation rules for Zabbix events.
Displayed data:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the correlation rule. Clicking on the correlation rule name opens the rule configuration form.</td>
</tr>
<tr>
<td>Conditions</td>
<td>Correlation rule conditions are displayed.</td>
</tr>
<tr>
<td>Operations</td>
<td>Correlation rule operations are displayed.</td>
</tr>
<tr>
<td>Status</td>
<td>Correlation rule status is displayed - Enabled or Disabled. By clicking on the status you can change it.</td>
</tr>
</tbody>
</table>

To configure a new correlation rule, click on the Create correlation button in the top right-hand corner.

Mass editing options

Buttons below the list offer some mass-editing options:

- Enable - change the correlation rule status to Enabled
- Disable - change the correlation rule status to Disabled
- Delete - delete the correlation rules

To use these options, mark the checkboxes before the respective correlation rules, then click on the required button.

Filter

As the list may contain a number of correlation rules, it may be needed to filter out the ones you really need.

The Filter link is available above the list of correlation rules. If you click on it, a filter becomes available where you can filter correlation rules by name and status.

7 Discovery

Overview

In the Configuration → Discovery section users can configure and maintain discovery rules.

A listing of existing discovery rules with their details is displayed.

Displayed data:
<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the discovery rule. Clicking on the discovery rule name opens the discovery rule <a href="#">configuration form</a>.</td>
</tr>
<tr>
<td>IP range</td>
<td>The range of IP addresses to use for network scanning is displayed.</td>
</tr>
<tr>
<td>Interval</td>
<td>The frequency of performing discovery displayed.</td>
</tr>
<tr>
<td>Checks</td>
<td>The types of checks used for discovery are displayed.</td>
</tr>
<tr>
<td>Status</td>
<td>Action status is displayed - Enabled or Disabled. By clicking on the status you can change it.</td>
</tr>
</tbody>
</table>

To configure a new discovery rule, click on the Create discovery rule button in the top right-hand corner.

Mass editing options

Buttons below the list offer some mass-editing options:

- Enable - change the discovery rule status to Enabled
- Disable - change the discovery rule status to Disabled
- Delete - delete the discovery rules

To use these options, mark the checkboxes before the respective discovery rules, then click on the required button.

Filter

As the list may contain a number of discovery rules, it may be needed to filter out the ones you really need.

The Filter link is available above the list of discovery rules. If you click on it, a filter becomes available where you can filter discovery rules by name and status.

---

**8 Services**

Overview

In the Configuration → Services section users can configure and maintain an IT services hierarchy.

When you first open this section it only contains a root entry.

You can use it as a starting point of building the hierarchy of monitored infrastructure. Click on Add child to add services and then other services below the ones you have added.

<table>
<thead>
<tr>
<th>SERVICE</th>
<th>ACTION</th>
<th>STATUS CALCULATION</th>
<th>TRIGGER</th>
</tr>
</thead>
<tbody>
<tr>
<td>root</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SLA by service</td>
<td>Add child</td>
<td>Problem, if all children have problems</td>
<td></td>
</tr>
<tr>
<td>Server 1</td>
<td>Add child Delete</td>
<td>Problem, if at least one child has a problem</td>
<td></td>
</tr>
<tr>
<td>Server 2</td>
<td>Add child Delete</td>
<td>Problem, if at least one child has a problem</td>
<td></td>
</tr>
<tr>
<td>Server 3</td>
<td>Add child Delete</td>
<td>Problem, if at least one child has a problem</td>
<td></td>
</tr>
<tr>
<td>Server 4</td>
<td>Add child Delete</td>
<td>Problem, if at least one child has a problem</td>
<td></td>
</tr>
<tr>
<td>Server 5</td>
<td>Add child Delete</td>
<td>Problem, if at least one child has a problem</td>
<td></td>
</tr>
</tbody>
</table>

For details on adding services, see the Service monitoring section.

**5 Administration**

Overview
The Administration menu is for administrative functions of Zabbix. This menu is available to users of Super Administrators type only.

1 General

Overview

The Administration → General section contains a number of screens for setting frontend-related defaults and customizing Zabbix. The dropdown to the right allows you to switch between different configuration screens.

GUI

This screen provides customization of several frontend-related defaults.

<table>
<thead>
<tr>
<th>Configuration parameters:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Default theme</td>
</tr>
<tr>
<td>Dropdown first entry</td>
</tr>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>------------------------------------------</td>
</tr>
<tr>
<td>Limit for search and filter results</td>
</tr>
<tr>
<td>Max count of elements&lt;br&gt;to show inside table cell</td>
</tr>
<tr>
<td>Show warning if Zabbix server is down</td>
</tr>
</tbody>
</table>

**Housekeeper**

The housekeeper is a periodical process, executed by Zabbix server. The process removes outdated information and information deleted by user.
## Events and alerts

<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable internal housekeeping</td>
<td>✔</td>
</tr>
<tr>
<td>Trigger data storage period</td>
<td>365d</td>
</tr>
<tr>
<td>Internal data storage period</td>
<td>1d</td>
</tr>
<tr>
<td>Network discovery data storage period</td>
<td>1d</td>
</tr>
<tr>
<td>Auto-registration data storage period</td>
<td>1d</td>
</tr>
</tbody>
</table>

## Services

<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable internal housekeeping</td>
<td>✔</td>
</tr>
<tr>
<td>Data storage period</td>
<td>365d</td>
</tr>
</tbody>
</table>

## Audit

<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable internal housekeeping</td>
<td>✔</td>
</tr>
<tr>
<td>Data storage period</td>
<td>365d</td>
</tr>
</tbody>
</table>

## User sessions

<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable internal housekeeping</td>
<td>✔</td>
</tr>
<tr>
<td>Data storage period</td>
<td>365d</td>
</tr>
</tbody>
</table>

## History

<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable internal housekeeping</td>
<td>✔</td>
</tr>
<tr>
<td>Override item history period</td>
<td>✔</td>
</tr>
<tr>
<td>Data storage period</td>
<td>90d</td>
</tr>
</tbody>
</table>

## Trends

<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable internal housekeeping</td>
<td>✔</td>
</tr>
<tr>
<td>Override item trend period</td>
<td>✔</td>
</tr>
<tr>
<td>Data storage period</td>
<td>365d</td>
</tr>
</tbody>
</table>
In this section housekeeping tasks can be enabled or disabled on a per-task basis separately for: events and alerts/IT services/audit/user sessions/history/trends. If housekeeping is enabled, it is possible to set for how many days data records will be kept before being removed by the housekeeper.

Deleting an item/trigger will also delete problems generated by that item/trigger.

Also, an event will only be deleted by the housekeeper if it is not associated with a problem in any way. This means that if an event is either a problem or recovery event, it will not be deleted until the related problem record is removed. The housekeeper will delete problems first and events after, to avoid potential problems with stale events or problem records.

For history and trends an additional option is available: Override item history period and Override item trend period. This option allows to globally set for how many days item history/trends will be kept (1 hour to 25 years; or "0"), in this case overriding the values set for individual items in History storage period/Trend storage period fields in item configuration. Note, that since Zabbix 4.0.11 the storage period will not be overridden for items that have configuration option Do not keep history and/or Do not keep trends enabled.

It is possible to override the history/trend storage period even if internal housekeeping is disabled. Thus, when using an external housekeeper, the history storage period could be set using the history Data storage period field.

**Time suffixes** are supported in the period fields, e.g. 1d (one day), 1w (one week). Minimum is 1 day (1 hour for history), maximum 25 years.

Reset defaults button allows to revert any changes made.

Images

The Images section displays all the images available in Zabbix. Images are stored in the database.

<table>
<thead>
<tr>
<th>Images</th>
<th>Images</th>
<th>Type</th>
<th>Image</th>
<th>Create icon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud (24)</td>
<td>Cloud (48)</td>
<td>Cloud (64)</td>
<td>Cloud (96)</td>
<td>Cloud (128)</td>
</tr>
<tr>
<td>Crypto-router (24)</td>
<td>Crypto-router (48)</td>
<td>Crypto-router (64)</td>
<td>Crypto-router (96)</td>
<td>Crypto-router (128)</td>
</tr>
<tr>
<td>Crypto-router_symbol (24)</td>
<td>Crypto-router_symbol (48)</td>
<td>Crypto-router_symbol (64)</td>
<td>Crypto-router_symbol (96)</td>
<td>Crypto-router_symbol (128)</td>
</tr>
<tr>
<td>Disk_array_2D (24)</td>
<td>Disk_array_2D (48)</td>
<td>Disk_array_2D (64)</td>
<td>Disk_array_2D (96)</td>
<td>Disk_array_2D (128)</td>
</tr>
<tr>
<td>Disk_array_3D (24)</td>
<td>Disk_array_3D (48)</td>
<td>Disk_array_3D (64)</td>
<td>Disk_array_3D (96)</td>
<td>Disk_array_3D (128)</td>
</tr>
<tr>
<td>Firewall (24)</td>
<td>Firewall (48)</td>
<td>Firewall (64)</td>
<td>Firewall (96)</td>
<td>Firewall (128)</td>
</tr>
</tbody>
</table>

The Type dropdown allows you to switch between icon and background images:

- Icons are used to display network map elements
- Backgrounds are used as background images of network maps

Adding image

You can add your own image by clicking on the Create icon or Create background button in the top right corner.
Image attributes:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name of an image.</td>
</tr>
<tr>
<td>Upload</td>
<td>Select the file (PNG, JPEG) from a local system to be uploaded to Zabbix.</td>
</tr>
</tbody>
</table>

**Note:**

Maximum size of the upload file is limited by value of ZBX_MAX_IMAGE_SIZE that is 1024x1024 bytes or 1 MB.

The upload of an image may fail if the image size is close to 1 MB and the `max_allowed_packet` MySQL configuration parameter is at a default of 1MB. In this case, increase the `max_allowed_packet` parameter.

Icon mapping

This section allows to create the mapping of certain hosts with certain icons. Host inventory field information is used to create the mapping.

The mappings can then be used in network map configuration to assign appropriate icons to matching hosts automatically.

To create a new icon map, click on Create icon map in the top right corner.

Configuration parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name of icon map.</td>
</tr>
<tr>
<td>Mappings</td>
<td>A list of mappings. The order of mappings determines which one will have priority. You can move mappings up and down the list with drag-and-drop.</td>
</tr>
<tr>
<td>Inventory field</td>
<td>Host inventory field that will be looked into to seek a match.</td>
</tr>
<tr>
<td>Expression</td>
<td>Regular expression describing the match.</td>
</tr>
<tr>
<td>Icon</td>
<td>Icon to use if a match for the expression is found.</td>
</tr>
<tr>
<td>Default</td>
<td>Default icon to use.</td>
</tr>
</tbody>
</table>

Regular expressions

This section allows to create custom regular expressions that can be used in several places in the frontend. See Regular expressions section for details.
Macros

This section allows to define system-wide macros.

Value mapping

This section allows to manage value maps that are useful for human-readable representation of incoming data in Zabbix frontend.

See Value mapping section for more details.

Working time

Working time is system-wide parameter, which defines working time. Working time is displayed as a white background in graphs, while non-working time is displayed in gray.

See Time period specification page for description of the time format. User macros are supported (since Zabbix 3.4.0).

Trigger severities
This section allows to customize trigger severity names and colors.

You can enter new names and color codes or click on the color to select another from the provided palette. See Customizing trigger severities page for more information.

Trigger displaying options

This section allows to customize how trigger status is displayed in the frontend.

The Use custom event status colors option allows to turn on the customization of colors for acknowledged/unacknowledged problems.

Also the time period for displaying OK triggers and for blinking upon trigger status change can be customized. The maximum value
is 86400 seconds (24 hours). *Time suffixes* are supported in the period fields, e.g. 5m, 2h, 1d.

Other parameters

This section allows to configure several other frontend parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh unsupported items</td>
<td>Some items may become unsupported due to errors in user parameters or because of an item not being supported by agent. Zabbix can be configured to periodically make unsupported items active. Zabbix server will activate unsupported item every N period set here (1 day maximum). If set to 0, the automatic activation will be disabled. Note that the first attempt to reactivate the unsupported item may occur earlier than the value configured here. <em>Time suffixes</em> are supported, e.g. 60s, 5m, 2h, 1d. The configured value also applies to how often Zabbix proxies reactivate unsupported items. This value is limited for active checks as it only postpones the item inclusion into the list of active checks, while afterwards the agent will poll that item according to the previously scheduled update interval. This value is not taken into account when items become unsupported because of a failed preprocessing step or data normalization.</td>
</tr>
<tr>
<td>Group for discovered hosts</td>
<td>Hosts discovered by network discovery and agent auto-registration will be automatically placed in the host group, selected here.</td>
</tr>
<tr>
<td>Default host inventory mode</td>
<td>Default mode for host inventory. It will be followed whenever a new host or host prototype is created by server or frontend, unless overridden during host discovery/auto registration by the Set host inventory mode operation.</td>
</tr>
</tbody>
</table>
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User group for database down message</td>
<td>User group for sending alarm message or ‘None’. Zabbix server depends on the availability of backend database. It cannot work without a database. If the database is down, selected users can be notified by Zabbix. Notifications will be sent to the user group set here using all configured user media entries. Zabbix server will not stop; it will wait until the database is back again to continue processing. Notification consists of the following content: `[MySQL][PostgreSQL][Oracle][IBM DB2] database &lt;DB Name&gt; [on &lt;DB Host&gt;:&lt;DB Port&gt;] is not available: &lt;error message depending on the type of DBMS (database)] &lt;DB Host&gt; is not added to the message if it is defined as an empty value and &lt;DB Port&gt; is not added if it is the default value (&quot;0&quot;). The alert manager (a special Zabbix server process) tries to establish a new connection to the database every 10 seconds. If the database is still down the alert manager repeats sending alerts, but not more often than every 15 minutes.</td>
</tr>
<tr>
<td>Log unmatched SNMP traps</td>
<td>Log SNMP trap if no corresponding SNMP interfaces have been found.</td>
</tr>
</tbody>
</table>

### 2 Proxies

#### Overview

In the Administration → Proxies section proxies for distributed monitoring can be configured in the Zabbix frontend.

#### Proxies

A listing of existing proxies with their details is displayed.

```
Proxies
```

<table>
<thead>
<tr>
<th>Name</th>
<th>Mode</th>
<th>Encryption</th>
<th>Compression</th>
<th>Last seen (age)</th>
<th>Host count</th>
<th>Item count</th>
<th>Required performance (vps)</th>
<th>Hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Active</td>
<td>None</td>
<td></td>
<td>21h 15m 15s</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Active</td>
<td>None</td>
<td></td>
<td>Never</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Displayed data:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the proxy. Clicking on the proxy name opens the proxy configuration form.</td>
</tr>
<tr>
<td>Mode</td>
<td>Proxy mode is displayed - Active or Passive.</td>
</tr>
<tr>
<td>Encryption</td>
<td>Encryption status for connections from the proxy is displayed: None - no encryption PSK - using pre-shared key Cert - using certificate</td>
</tr>
<tr>
<td>Last seen (age)</td>
<td>The time when the proxy was last seen by the server is displayed.</td>
</tr>
<tr>
<td>Host count</td>
<td>The number of enabled hosts assigned to the proxy is displayed.</td>
</tr>
<tr>
<td>Item count</td>
<td>The number of enabled items on enabled hosts assigned to the proxy is displayed.</td>
</tr>
<tr>
<td>Required performance (vps)</td>
<td>Required proxy performance is displayed (the number of values that need to be collected per second).</td>
</tr>
<tr>
<td>Hosts</td>
<td>All hosts monitored by the proxy are listed. Clicking on the host name opens the host configuration form.</td>
</tr>
</tbody>
</table>

To configure a new proxy, click on the Create proxy button in the top right-hand corner.
Mass editing options

Buttons below the list offer some mass-editing options:

- Enable hosts - change the status of hosts monitored by the proxy to Monitored
- Disable hosts - change the status of hosts monitored by the proxy to Not monitored
- Delete - delete the proxies

To use these options, mark the checkboxes before the respective proxies, then click on the required button.

Filter

As the list may contain many proxies, it may be needed to filter out the ones you really need.

The Filter link is available above the list of proxies. If you click on it, a filter becomes available where you can filter proxies by name and mode.

3 Authentication

Overview

In Administration → Authentication the global user authentication method to Zabbix can be specified. The available methods are internal, HTTP and LDAP authentication.

By default, Zabbix uses internal Zabbix authentication for all users. It is possible to change the default method to LDAP system-wide or enable LDAP authentication only for specific user groups.

To set LDAP as default authentication method for all users, navigate to the LDAP tab and configure authentication parameters, then return to the Authentication tab and switch Default authentication selector to LDAP.

Note that the authentication method can be fine-tuned on the user group level. Even if LDAP authentication is set globally, some user groups can still be authenticated by Zabbix. These groups must have frontend access set to Internal. Vice versa, if internal authentication is used globally, LDAP authentication details can be specified and used for specific user groups whose frontend access is set to LDAP. If a user is included into at least one user group with LDAP authentication, this user will not be able to use internal authentication method.

HTTP authentication method can be used in addition to the default authentication method.

HTTP authentication

HTTP or web server-based authentication (for example: Basic Authentication, NTLM/Kerberos) can be used to check user names and passwords. Note that a user must exist in Zabbix as well, however its Zabbix password will not be used.

**Attention:**

Be careful! Make sure that web server authentication is configured and works properly before switching it on.
**Configuration parameters:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable HTTP authentication</td>
<td>Mark the checkbox to enable HTTP authentication.</td>
</tr>
<tr>
<td>Default login form</td>
<td>Specify whether to direct non-authenticated users to:</td>
</tr>
<tr>
<td></td>
<td><strong>Zabbix login form</strong> - standard Zabbix login page.</td>
</tr>
<tr>
<td></td>
<td><strong>HTTP login form</strong> - HTTP login page.</td>
</tr>
<tr>
<td></td>
<td>It is recommended to enable web-server based authentication for the index_http.php page only. If Default login form is set to 'HTTP login page' the user will be logged in automatically if web server authentication module will set valid user login in the $_SERVER variable. Supported $_SERVER keys are PHP_AUTH_USER, REMOTE_USER, AUTH_USER.</td>
</tr>
<tr>
<td>Remove domain name</td>
<td>A comma-delimited list of domain names that should be removed from the username. E.g. comp, any - if username is 'Admin@any', 'comp\Admin', user will be logged in as 'Admin'; if username is 'notacompany\Admin', login will be denied.</td>
</tr>
<tr>
<td>Case sensitive login</td>
<td>Unmark the checkbox to disable case-sensitive login (enabled by default) for usernames. E.g. disable case-sensitive login and log in with, for example, 'ADMIN' user even if the Zabbix user is 'Admin'. Note that with case-sensitive login disabled the login will be denied if multiple users exist in Zabbix database with similar alias (e.g. Admin, admin).</td>
</tr>
</tbody>
</table>

**Note:**
In case of web server authentication all users (even with frontend access set to LDAP/Internal) will be authenticated by the web server, not by Zabbix!

**Note:**
For internal users who are unable to log in using HTTP credentials (with HTTP login form set as default) leading to the 401 error, you may want to add a ErrorDocument 401 /index.php?form=default line to basic authentication directives, which will redirect to the regular Zabbix login form.

**LDAP authentication**
External LDAP authentication can be used to check user names and passwords. Note that a user must exist in Zabbix as well, however its Zabbix password will not be used.

While LDAP authentication is set globally, some user groups can still be authenticated by Zabbix. These groups must have frontend access set to Internal. Vice versa, if internal authentication is used globally, LDAP authentication details can be specified and used for specific user groups whose frontend access is set to LDAP.
Zabbix LDAP authentication works at least with Microsoft Active Directory and OpenLDAP.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable LDAP authentication</td>
<td>Mark the checkbox to enable LDAP authentication.</td>
</tr>
<tr>
<td>LDAP host</td>
<td>Name of LDAP server. For example: ldap://ldap.zabbix.com</td>
</tr>
<tr>
<td></td>
<td>For secure LDAP server use ldaps protocol.</td>
</tr>
<tr>
<td></td>
<td>ldaps://ldap.zabbix.com</td>
</tr>
<tr>
<td></td>
<td>With OpenLDAP 2.x.x and later, a full LDAP URI of the form</td>
</tr>
<tr>
<td></td>
<td>ldap://hostname:port or ldaps://hostname:port may be used.</td>
</tr>
<tr>
<td>Port</td>
<td>Port of LDAP server. Default is 389.</td>
</tr>
<tr>
<td></td>
<td>For secure LDAP connection port number is normally 636.</td>
</tr>
<tr>
<td></td>
<td>Not used when using full LDAP URIs.</td>
</tr>
<tr>
<td>Base DN</td>
<td>Base path to search accounts:</td>
</tr>
<tr>
<td></td>
<td>ou=Users,ou=system (for OpenLDAP),</td>
</tr>
<tr>
<td></td>
<td>DC=company,DC=com (for Microsoft Active Directory)</td>
</tr>
<tr>
<td>Search attribute</td>
<td>LDAP account attribute used for search:</td>
</tr>
<tr>
<td></td>
<td>uid (for OpenLDAP),</td>
</tr>
<tr>
<td></td>
<td>sAMAccountName (for Microsoft Active Directory)</td>
</tr>
</tbody>
</table>
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bind DN</td>
<td>LDAP account for binding and searching over the LDAP server, examples: uid=ldap_search,ou=system (for OpenLDAP), CN=ldap_search,OU=user_group,DC=company,DC=com (for Microsoft Active Directory)</td>
</tr>
<tr>
<td></td>
<td>Anonymous binding is supported since Zabbix 4.0.4. Note that anonymous binding potentially opens up domain configuration to unauthorized users (information about users, computers, servers, groups, services, etc.). For security reasons, disable anonymous binds on LDAP hosts and use authenticated access instead.</td>
</tr>
<tr>
<td>Case-sensitive login</td>
<td>Unmark the checkbox to disable case-sensitive login (enabled by default) for usernames. E.g. disable case-sensitive login and log in with, for example, 'ADMIN' user even if the Zabbix user is 'Admin'. Note that with case-sensitive login disabled the login will be denied if multiple users exist in Zabbix database with similar alias (e.g. Admin, admin).</td>
</tr>
<tr>
<td>Bind password</td>
<td>LDAP password of the account for binding and searching over the LDAP server.</td>
</tr>
<tr>
<td>Test authentication</td>
<td>Header of a section for testing Login Name of a test user (which is currently logged in the Zabbix frontend). This user name must exist in the LDAP server. Zabbix will not activate LDAP authentication if it is unable to authenticate the test user.</td>
</tr>
<tr>
<td>User password</td>
<td>LDAP password of the test user.</td>
</tr>
</tbody>
</table>

**Warning:**

In case of trouble with certificates, to make a secure LDAP connection (ldaps) work you may need to add a `TLS_REQCERT allow` line to the `/etc/openldap/ldap.conf` configuration file. It may decrease the security of connection to the LDAP catalog.

**Note:**

It is recommended to create a separate LDAP account (Bind DN) to perform binding and searching over the LDAP server with minimal privileges in the LDAP instead of using real user accounts (used for logging in the Zabbix frontend). Such an approach provides more security and does not require changing the Bind password when the user changes his own password in the LDAP server.

In the table above it’s ldap_search account name.

### 4 User groups

**Overview**

In the Administration → User groups section user groups of the system are maintained.

**User groups**

A listing of existing user groups with their details is displayed.
### Displayed data:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the user group. Clicking on the user group name opens the user group configuration form.</td>
</tr>
<tr>
<td>#</td>
<td>The number of users in the group. Clicking on Users will display the respective users filtered out in the user list.</td>
</tr>
<tr>
<td>Members</td>
<td>Aliases of individual users in the user group (with name and surname in parentheses). Clicking on the alias will open the user configuration form. Users from disabled groups are displayed in red.</td>
</tr>
</tbody>
</table>
| Frontend access | Frontend access level is displayed:  
  - **System default** - Zabbix, LDAP or HTTP authentication; depending on the chosen authentication method  
  - **Internal** - the user is authenticated by Zabbix regardless of system settings  
  - **Disabled** - frontend access for this user is disabled. By clicking on the current level you can change it. |
| Debug mode   | **Debug mode** status is displayed - Enabled or Disabled. By clicking on the status you can change it.                                     |
| Status       | User group status is displayed - Enabled or Disabled. By clicking on the status you can change it.                                       |

To configure a new user group, click on the Create user group button in the top right-hand corner.

### Mass editing options

Buttons below the list offer some mass-editing options:

- Enable - change the user group status to Enabled
- Disable - change the user group status to Disabled
- Enable debug mode - enable debug mode for the user groups
- Disable debug mode - disable debug mode for the user groups
- Delete - delete the user groups

To use these options, mark the checkboxes before the respective user groups, then click on the required button.

### Filter

As the list may contain many user groups, it may be needed to filter out the ones you really need.

The Filter link is available above the list of user groups. If you click on it, a filter becomes available where you can filter user groups by name and status.
Overview

In the Administration → Users section users of the system are maintained.

Users

A listing of existing users with their details is displayed.

From the dropdown to the right in the Users bar you can choose whether to display all users or those belonging to one particular group.

Displayed data:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
<td>Alias of the user, used for logging into Zabbix. Clicking on the alias opens the user configuration form.</td>
</tr>
<tr>
<td>Name</td>
<td>First name of the user.</td>
</tr>
<tr>
<td>Surname</td>
<td>Second name of the user.</td>
</tr>
<tr>
<td>User type</td>
<td>User type is displayed - Zabbix Super Admin, Zabbix Admin or Zabbix User.</td>
</tr>
<tr>
<td>Groups</td>
<td>Groups that the user is member of are listed. Clicking on the user group name opens the user group configuration form. Disabled groups are displayed in red.</td>
</tr>
<tr>
<td>Is online?</td>
<td>The on-line status of the user is displayed - Yes or No. The time of last user activity is displayed in parentheses.</td>
</tr>
<tr>
<td>Login</td>
<td>The login status of the user is displayed - Ok or Blocked. A user can become temporarily blocked upon more than five unsuccessful login attempts. By clicking on Blocked you can unblock the user.</td>
</tr>
<tr>
<td>Frontend access</td>
<td>Frontend access level is displayed - System default, Internal or Disabled, depending on the one set for the whole user group.</td>
</tr>
<tr>
<td>Debug mode</td>
<td>Debug mode status is displayed - Enabled or Disabled, depending on the one set for the whole user group.</td>
</tr>
<tr>
<td>Status</td>
<td>User status is displayed - Enabled or Disabled, depending on the one set for the whole user group.</td>
</tr>
</tbody>
</table>

To configure a new user, click on the Create user button in the top right-hand corner.

Mass editing options

Buttons below the list offer some mass-editing options:

- Unblock - re-enable system access to blocked users
- Delete - delete the users

To use these options, mark the check-boxes before the respective users, then click on the required button.

Filter

As the list may contain many users, it may be needed to filter out the ones you really need.

The Filter link is available above the list of users. If you click on it, a filter becomes available where you can filter users by alias, name, surname and user type.
6 Media types

Overview

In the Administration → Media types section users can configure and maintain media type information.

Media type information contains general instructions for using a medium as delivery channel for notifications. Specific details, such as the individual e-mail addresses to send a notification to are kept with individual users.

A listing of existing media types with their details is displayed.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the media type. Clicking on the name opens the media type configuration form.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of the media (e-mail, SMS, etc) is displayed.</td>
</tr>
<tr>
<td>Status</td>
<td>Media type status is displayed - Enabled or Disabled. By clicking on the status you can change it.</td>
</tr>
<tr>
<td>Used in actions</td>
<td>All actions where the media type is used directly (selected in the Send only to dropdown) are displayed. Clicking on the action name opens the action configuration form.</td>
</tr>
<tr>
<td>Details</td>
<td>Detailed information of the media type is displayed.</td>
</tr>
</tbody>
</table>

To configure a new media type, click on the Create media type button in the top right-hand corner.

Mass editing options

Buttons below the list offer some mass-editing options:

- Enable - change the media type status to Enabled
- Disable - change the media type status to Disabled
- Delete - delete the media types

To use these options, mark the checkboxes before the respective media types, then click on the required button.

Filter

As the list may contain a number of media types, it may be needed to filter out the ones you really need.

The Filter link is available above the list of media types. If you click on it, a filter becomes available where you can filter media types by name and status.

7 Scripts

Overview

In the Administration → Scripts section user-defined global scripts can be configured and maintained.
These scripts, depending on the set user permissions, then become available for execution by clicking on the host in various frontend locations (Dashboard, Problems, Latest data, Maps) and can also be run as an action operation. The scripts are executed on the Zabbix server or agent.

A listing of existing scripts with their details is displayed.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Execute on</th>
<th>Commands</th>
<th>User group</th>
<th>Host group</th>
<th>Host access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detect operating system</td>
<td>Script</td>
<td>Server</td>
<td>sudo hostname</td>
<td>Zabbix administrators</td>
<td>All</td>
<td>Read</td>
</tr>
<tr>
<td>MyScripts/Check disk space</td>
<td>Script</td>
<td>Agent</td>
<td>sleep 5 df -h</td>
<td>All</td>
<td>All</td>
<td>Read</td>
</tr>
<tr>
<td>MyScripts/Check disk space no sleep</td>
<td>Script</td>
<td>Agent</td>
<td>df -h</td>
<td>All</td>
<td>All</td>
<td>Read</td>
</tr>
<tr>
<td>MyScripts/Check disk space S</td>
<td>Script</td>
<td>Server</td>
<td>sleep 11 df -h</td>
<td>All</td>
<td>All</td>
<td>Read</td>
</tr>
<tr>
<td>Ping</td>
<td>Script</td>
<td>Server</td>
<td>ping &lt; 3 (HOST.CONN)</td>
<td>All</td>
<td>All</td>
<td>Read</td>
</tr>
</tbody>
</table>

Displayed data:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the script. Clicking on the script name opens the script configuration form.</td>
</tr>
<tr>
<td>Type</td>
<td>Script type is displayed - Script or IPMI command.</td>
</tr>
<tr>
<td>Execute on</td>
<td>It is displayed whether the script will be executed on Zabbix server or agent.</td>
</tr>
<tr>
<td>Commands</td>
<td>All commands to be executed within the script are displayed.</td>
</tr>
<tr>
<td>User group</td>
<td>The user group that the script is available to is displayed (or All for all user groups).</td>
</tr>
<tr>
<td>Host group</td>
<td>The host group that the script is available for is displayed (or All for all host groups).</td>
</tr>
<tr>
<td>Host access</td>
<td>The permission level for the host group is displayed - Read or Write. Only users with the required permission level will have access to executing the script.</td>
</tr>
</tbody>
</table>

To configure a new script, click on the Create script button in the top right-hand corner.

Mass editing options

A button below the list offers one mass-editing option:

- Delete - delete the scripts

To use this option, mark the checkboxes before the respective scripts and click on Delete.

Filter

As the list may contain a number of scripts, it may be needed to filter out the ones you really need.

The Filter link is available above the list of scripts. If you click on it, a filter becomes available where you can filter scripts by name.

Configuring a global script
Script attributes:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Name**           | Unique name of the script. Since Zabbix 2.2 the name can be prefixed with the desired path, for example, Default/., putting the script into the respective directory. When accessing scripts through the menu in monitoring sections, they will be organized according to the given directories. A script cannot have the same name as an existing directory (and vice versa). A script name must be unique within its directory. Unescaped script names are validated for uniqueness, i.e. "Ping" and "\Ping" cannot be added in the same folder. A single backslash escapes any symbol directly after it. For example, characters '/' and '\' can be escaped by backslash, i.e. \ or \\.
| **Type**           | Click the respective button to select script type - **IPMI command** or **Script**. |

**Parameter Description**

* Name: Detect operating system
  - Type: IPMI | Script
  - Execute on: Zabbix agent | Zabbix server (proxy) | Zabbix server
  - Commands: sudo /usr/bin/nmap -O {HOST.CONN}
Parameter | Description
--- | ---
Execute on | Click the respective button to execute the script on:  
**Zabbix agent** - the script will be executed by Zabbix agent on the host  
**Zabbix server (proxy)** - the script will be executed by Zabbix server or proxy - depending on whether the host is monitored by server or proxy  
**Zabbix server** - the script will be executed by Zabbix server only  
The option to execute scripts on Zabbix agent is available since Zabbix 2.0 version (providing remote commands are enabled in the `EnableRemoteCommands` parameter in Zabbix agent configuration file).

Commands | Enter full path to the commands to be executed within the script.  
The following macros are supported in the commands:  
`{HOST.CONN}`, `{HOST.IP}`, `{HOST.DNS}`, `{HOST.HOST}`, `{HOST.NAME}`. If a macro may resolve to a value with spaces (for example, host name), don’t forget to quote as needed.  
Since Zabbix 2.2, **user macros** are supported in script commands.

Description | Enter a description for the script.

User group | Select the user group that the script will be available to (or All for all user groups).

Host group | Select the host group that the script will be available for (or All for all host groups).

Required host permissions | Select the permission level for the host group - Read or Write. Only users with the required permission level will have access to executing the script.

Enable confirmation | Mark the checkbox to display a confirmation message before executing the script. This feature might be especially useful with potentially dangerous operations (like a reboot script) or ones that might take a long time.

Confirmation text | Enter a custom confirmation text for the confirmation popup enabled with the checkbox above (for example, Remote system will be rebooted. Are you sure?). To see how the text will look like, click on Test confirmation next to the field.  
Since Zabbix 2.2, the confirmation text will expand host name macros - `{HOST.HOST}`, `{HOST.NAME}`, host connection macros - `{HOST.IP}`, `{HOST.DNS}`, `{HOST.CONN}` and user macros. Note: The macros will not be expanded when testing the confirmation message.

---

**Script execution and result**

Scripts run by Zabbix server are executed by the order described in **Command execution** section including exit code checking. The script result will be displayed in a pop-up window that will appear after the script is run.

**Note:** The return value of the script is standard output together with standard error.

See example of a script and the result window below:

```
uname
uname --non-existing-flag
/tmp/non_existing_script.sh
```
Script timeout

Zabbix agent

You may encounter a situation when timeout occurs while executing a script.

See example of a script running on Zabbix agent and the result window below:

```
uname
uname --non-existing-flag
/tmp/non_existing_script.sh
```

Linux

```
uname: unrecognized option '--non-existing-flag'
Try 'uname --help' for more information.
sh: 3: /tmp/non_existing_script.sh: not found
```

Error message in this case is the following:

Timeout while executing a shell script.

In order to avoid such a situation, it is advised to optimize the script itself (instead of adjusting Timeout parameter to a corresponding value (in our case, > '5') by modifying the Zabbix agent configuration and Zabbix server configuration).

In case still the Timeout parameter is changed in Zabbix agent configuration following error message appears:

Get value from agent failed: ZBX_TCP_READ() timed out.

It means that modification was made in Zabbix agent configuration and it is required to modify Timeout setting also in Zabbix server configuration.

Zabbix server/proxy

See example of a script running on Zabbix server and the result window below:
It is also advised to optimize the script itself (instead of adjusting TrapperTimeout parameter to a corresponding value (in our case, > '11') by modifying the Zabbix server configuration).

8 Queue

Overview

In the Administration → Queue section items that are waiting to be updated are displayed.

Ideally, when you open this section it should all be "green" meaning no items in the queue. If all items are updated without delay, there are none waiting. However, due to lacking server performance, connection problems or problems with agents, some items may get delayed and the information is displayed in this section. For more details, see the Queue section.

Note:
Queue is available only if Zabbix server is running.

From the dropdown in the upper right corner you can select:

- queue overview by item type
- queue overview by proxy
- list of delayed items

Overview by item type

In this screen it is easy to locate if the problem is related to one or several item types.

<table>
<thead>
<tr>
<th>ITEMS</th>
<th>5 SECONDS</th>
<th>10 SECONDS</th>
<th>30 SECONDS</th>
<th>1 MINUTE</th>
<th>5 MINUTES</th>
<th>OVERMORE THAN 10 MINUTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zabbix agent</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Zabbix agent (active)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Simple check</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SNMP agent</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SNMP agent (active)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Zabbix internal</td>
<td>4</td>
<td>14</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Zabbix aggregate</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Each line contains an item type. Each column shows the number of waiting items - waiting for 5-10 seconds/10-30 seconds/30-60 seconds/1-5 minutes/5-10 minutes or over 10 minutes respectively.

Overview by proxy

In this screen it is easy to locate if the problem is related to one of the proxies or the server.
Each line contains a proxy, with the server last in the list. Each column shows the number of waiting items - waiting for 5-10 seconds/10-30 seconds/30-60 seconds/1-5 minutes/5-10 minutes or over 10 minutes respectively.

List of waiting items

In this screen, each waiting item is listed.

<table>
<thead>
<tr>
<th>Scheduled check</th>
<th>Delayed by</th>
<th>Host</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-01-04 17:28:39</td>
<td>36s</td>
<td>Zabbix server 1</td>
<td>Zabbix busy discover processes, in %</td>
</tr>
<tr>
<td>2016-01-04 17:28:40</td>
<td>36s</td>
<td>Zabbix server 1</td>
<td>Zabbix busy discover processes, in %</td>
</tr>
<tr>
<td>2016-01-04 17:28:41</td>
<td>34s</td>
<td>Zabbix server 1</td>
<td>Zabbix busy discover processes, in %</td>
</tr>
<tr>
<td>2016-01-04 17:28:42</td>
<td>33s</td>
<td>Zabbix server 1</td>
<td>Zabbix busy discover processes, in %</td>
</tr>
<tr>
<td>2016-01-04 17:28:43</td>
<td>32s</td>
<td>Zabbix server 1</td>
<td>Zabbix busy discover processes, in %</td>
</tr>
<tr>
<td>2016-01-04 17:28:44</td>
<td>31s</td>
<td>Zabbix server 1</td>
<td>Zabbix busy discover processes, in %</td>
</tr>
</tbody>
</table>

In the host column, hosts monitored by proxy are prefixed with the proxy name (since Zabbix 2.4.0).

Displayed data:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next check</td>
<td>The time when the check was due is displayed.</td>
</tr>
<tr>
<td>Delayed by</td>
<td>The length of the delay is displayed.</td>
</tr>
<tr>
<td>Host</td>
<td>Host of the item is displayed.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the waiting item is displayed.</td>
</tr>
</tbody>
</table>

Possible error messages

You may encounter a situation when no data is displayed and the following error message appears:

**Cannot display item queue. Permission denied**

This happens when PHP configuration parameters $ZBX_SERVER_PORT or $ZBX_SERVER in zabbix.conf.php point to existing Zabbix server which uses different database.

**2 User profile**

Overview

In the user profile you can customize some Zabbix frontend features, such as the interface language, color theme, number of rows displayed in the lists etc. The changes made here will apply for the user only.

To access the user profile configuration form, click on the user profile link in the upper right corner of Zabbix window.

Configuration
The **User** tab allows you to set various user preferences.

### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Password</strong></td>
<td>Click on the link to display two fields for entering a new password. Select the interface language of your choice. For more information, see <a href="#">Installation of additional frontend languages</a>.</td>
</tr>
<tr>
<td><strong>Language</strong></td>
<td>Select the interface language of your choice.</td>
</tr>
</tbody>
</table>
| **Theme**       | Select a color theme specifically for your profile:  
|                 | **System default** - use default system settings  
|                 | **Blue** - standard blue theme  
|                 | **Dark** - alternative dark theme  
|                 | **High-contrast light** - light theme with high contrast  
|                 | **High-contrast dark** - dark theme with high contrast |
| **Auto-login**  | Mark this checkbox to make Zabbix remember you and log you in automatically for 30 days. Browser cookies are used for this. |
| **Auto-logout** | With this checkbox marked you will be logged out automatically, after the set amount of seconds (minimum 90 seconds, maximum 1 day).  
|                 | **Time suffixes** are supported, e.g. 90s, 5m, 2h, 1d.  
|                 | Note that this option will not work:  
|                 | * When Monitoring menu pages perform background information refreshes. In case pages refreshing data in a specific time interval (dashboards, graphs, screens, latest data, etc.) are left open session lifetime is extended, respectively disabling auto-logout feature;  
|                 | * If logging in with the Remember me for 30 days option checked. Auto-logout can accept 0, meaning that Auto-logout becomes disabled after profile settings update. |
| **Refresh**     | Set how often the information on the Monitoring menu pages will be refreshed (minimum 0 seconds, maximum 1 hour), except for **Dashboard**, which uses its own refresh parameters for every widget.  
<p>|                 | <strong>Time suffixes</strong> are supported, e.g. 30s, 90s, 1m, 1h. |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rows per page</td>
<td>You can set how many rows will be displayed per page in the lists. Fewer</td>
</tr>
<tr>
<td></td>
<td>rows (and fewer records to display) mean faster loading times.</td>
</tr>
<tr>
<td>URL (after login)</td>
<td>You can set a specific URL to be displayed after the login. Instead of</td>
</tr>
<tr>
<td></td>
<td>the default Monitoring → Dashboard it can be, for example, the URL of</td>
</tr>
<tr>
<td></td>
<td>Monitoring → Triggers.</td>
</tr>
</tbody>
</table>

The **Media** tab allows you to specify the media details for the user, such as the types, the addresses to use and when to use them to deliver notifications.

The **Messaging** tab allows you to set global notifications.

### 1 Global notifications

#### Overview

Global notifications are a way of displaying issues that are currently happening right on the screen you’re at in Zabbix frontend. Without global notifications, working in some other location than Host groups or Dashboard pages would not show any information regarding issues that are currently happening. Global notifications will display this information regardless of where you are.

Global notifications involve both showing a message and **playing a sound**.

**Attention:**
The auto play of sounds may be disabled in recent browser versions by default. In this case, you need to change this setting manually.

#### Configuration

Global notifications can be enabled per user in the Messaging tab of profile configuration.
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frontend messaging</td>
<td>Mark the checkbox to enable global notifications.</td>
</tr>
<tr>
<td>Message timeout</td>
<td>You can set for how long the message will be displayed. By default, messages will stay on screen for 60 seconds.</td>
</tr>
<tr>
<td></td>
<td><strong>Time suffixes</strong> are supported, e.g. 30s, 5m, 2h, 1d.</td>
</tr>
<tr>
<td>Play sound</td>
<td>You can set how long the sound will be played.</td>
</tr>
<tr>
<td></td>
<td><strong>Once</strong> - sound is played once and fully.</td>
</tr>
<tr>
<td></td>
<td><strong>10 seconds</strong> - sound is repeated for 10 seconds.</td>
</tr>
<tr>
<td></td>
<td><strong>Message timeout</strong> - sound is repeated while the message is visible.</td>
</tr>
<tr>
<td>Trigger severity</td>
<td>You can set the trigger severities that global notifications and sounds will be activated for. You can also select the sounds appropriate for various severities.</td>
</tr>
<tr>
<td></td>
<td>If no severity is marked then no messages will be displayed at all.</td>
</tr>
<tr>
<td></td>
<td>Also, recovery messages will only be displayed for those severities that are marked. So if you mark Recovery and Disaster, global notifications will be displayed for the problems and the recoveries of disaster severity triggers.</td>
</tr>
<tr>
<td>Show suppressed problems</td>
<td>Mark the checkbox to display notifications for problems which would otherwise be suppressed (not shown) because of host maintenance.</td>
</tr>
</tbody>
</table>

### Global messages displayed

As the messages arrive, they are displayed in a floating section on the right hand side. This section can be repositioned freely by dragging the section header.
For this section, several controls are available:

- **Snooze** button silences currently active alarm sound;
- **Mute/Unmute** button switches between playing and not playing the alarm sounds.

## 2 Sound in browsers

### Overview

Sound is used in global notifications.

For the sounds to be played in Zabbix frontend, Frontend messaging must be enabled in the user profile Messaging tab, with all trigger severities checked, and sounds should also be enabled in the global notification pop-up window.

If for some reasons audio cannot be played on the device, the **button** in the global notification popup window will permanently remain in the "mute" state and the message "Cannot support notification audio for this device." will be displayed upon hovering over the **button**.

Default audio clips are in:

- Wave format until Zabbix 4.0.11
- MP3 format since Zabbix 4.0.12

Note that since 4.0.16 sounds are supported in MP3 format only.

The sounds of Zabbix frontend have been successfully tested in recent Firefox/Opera browsers on Linux and Chrome, Firefox, Internet Explorer, Opera and Safari browsers on Windows.

**Attention:**
The auto play of sounds may be disabled in recent browser versions by default. In this case, you need to change this setting manually.
It is possible to search Zabbix frontend for hosts, host groups and templates.

The search input box is located in the upper right corner. The search can be started by pressing Enter or clicking on the search icon.

If there is a host that starts with the entered string, a dropdown will appear, listing all such hosts.

Starting with Zabbix 4.0.7, if there is a host that contains the entered string in any part of the name, a dropdown will appear, listing all such hosts (with the matching part highlighted in orange). The dropdown will also list a host if that host’s visible name is a match to the technical name entered as a search string; the matching host will be listed, but without any highlighting.

Properties searched

Hosts can be searched by the following properties:

- Host name
- Visible name
- IP address
- DNS name

Host groups can be searched by name. Specifying a parent host group implicitly selects all nested host groups.

Templates can be searched by name or visible name. If you search by a name that is different from the visible name (of a template/host), in the search results it is displayed below the visible name in parentheses.

Search results

Search results consist of three separate blocks for hosts, host groups and templates.

It is possible to collapse/expand each individual block. The entry count is displayed at the bottom of each block, for example, Displaying 13 of 13 found. Total entries displayed within one block are limited to 100.

Each entry provides links to monitoring and configuration data. See links available.

For all configuration data (such as items, triggers, graphs) the amount of entities found is displayed by a number next to the entity name, in gray. Note that if there are zero entities, no number is displayed.

Enabled hosts are displayed in blue, disabled hosts in red.
Links available

For each entry the following links are available:

• Hosts
  - Monitoring
    * Latest data
    * Triggers
    * Problems
    * Graphs
    * Host screens
    * Web scenarios
  - Configuration
    * Host properties
    * Applications
    * Items
    * Triggers
    * Graphs
    * Discovery rules
    * Web scenarios

• Host groups
  - Monitoring
    * Latest data
    * Triggers
    * Problems
    * Graphs
    * Web scenarios
  - Configuration
    * Host group properties
    * Host group members (hosts and templates)

• Templates
  - Configuration
    * Template properties
    * Applications
    * Items
    * Triggers
    * Graphs
    * Template screens
    * Discovery rules
    * Web scenarios

4 Frontend maintenance mode

Overview

Zabbix web frontend can be temporarily disabled in order to prohibit access to it. This can be useful for protecting the Zabbix database from any changes initiated by users, thus protecting the integrity of database.

Zabbix database can be stopped and maintenance tasks can be performed while Zabbix frontend is in maintenance mode.

Users from defined IP addresses will be able to work with the frontend normally during maintenance mode.

Configuration

In order to enable maintenance mode, the `maintenance.inc.php` file (located in `/conf` of the Zabbix HTML document directory on the webserver) must be modified to uncomment the following lines:

```php
// Maintenance mode.
define('ZBX_DENY_GUI_ACCESS', 1);
```

```php
// Array of IP addresses, which are allowed to connect to frontend (optional).
$ZBX_GUI_ACCESS_IP_RANGE = array('127.0.0.1');
```

```php
// Message shown on warning screen (optional).
```
$ZBX_GUI_ACCESS_MESSAGE = 'We are upgrading MySQL database till 15:00. Stay tuned...';

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZBX_DENY_GUI_ACCESS</td>
<td>Enable maintenance mode: 1 - maintenance mode is enabled, disabled otherwise</td>
</tr>
<tr>
<td>ZBX_GUI_ACCESS_IP_RANGE</td>
<td>Array of IP addresses, which are allowed to connect to frontend (optional). For example: array('192.168.1.1', '192.168.1.2')</td>
</tr>
<tr>
<td>ZBX_GUI_ACCESS_MESSAGE</td>
<td>A message you can enter to inform users about the maintenance (optional).</td>
</tr>
</tbody>
</table>

Display

The following screen will be displayed when trying to access the Zabbix frontend while in maintenance mode. The screen is refreshed every 30 seconds in order to return to a normal state without user intervention when the maintenance is over.

![Warning message]

IP addresses defined in ZBX_GUI_ACCESS_IP_RANGE will be able to access the frontend as always.

5 Page parameters

Overview

Most Zabbix web interface pages support various HTTP GET parameters that control what will be displayed. They may be passed by specifying parameter=value pairs after the URL, separated from the URL by a question mark (?) and from each other by ampersands (&).

Monitoring → Problems

The following parameters are supported:

- `sort` - sort column: clock, host, severity, name
- `sortorder` - sort order or results: DESC - descending, ASC - ascending
- `filter_set` - should be 'filter_set=1' to use "filter_*" parameters
- `filter_rst` - should be 'filter_rst=1' to reset filter elements
- `filter_show` - filter option "Show": 1 - recent problems, 2 - all, 3 - in problem state
- `filter_groupids` - filter option "Host groups": array of host groups IDs
- `filter_hostids` - filter option "Hosts": array of host IDs
- `filter_application` - filter option "Application": freeform string
- `filter_triggerids` - filter option "Triggers": array of trigger IDs
- `filter_name` - filter option "Problem": freeform string
- `filter_severity` - filter option "Minimum severity": 0 - not classified, 1 - information, 2 - warning, 3 - average, 4 - high, 5 - disaster
- `filter_age_state` - filter option "Age less than": should be 'filter_age_state=1' to enable 'filter_age'. Is used only when 'filter_show' equals 3.
- `filter_age` - filter option "Age less than": days
- `filter_inventory` - filter option "Host inventory": array of inventory fields: [field], [value]
- `filter_evaltype` - filter option "Tags", tag filtering strategy: 0 - And/Or, 2 - Or
- `filter_tags` - filter option "Tags": array of defined tags: [tag], [operator], [value]
- `filter_show_tags` - filter option "Show tags": 0 - none, 1 - one, 2 - two, 3 - three
- `filter_tag_name_format` - filter option "Tag name": 0 - full name, 1 - shortened, 2 - none
- `filter_tag_priority` - filter option "Tag display priority": comma-separated string of tag display priority
- `filter_show_suppressed` - filter option "Show suppressed problems": should be 'filter_show_suppressed=1' to show
- `filter_unacknowledged` - filter option "Show unacknowledged only": should be 'filter_unacknowledged=1' to show
• filter_compact_view - filter option "Compact view": should be 'filter_compact_view=1' to show
• filter_show_timeline - filter option "Show timeline": should be 'filter_show_timeline=1' to show
• filter_details - filter option "Show details": should be 'filter_details=1' to show
• filter_highlight_row - filter option "Highlight whole row" (use problem color as background color for every problem row): should be '1' to highlight; can be set only when 'filter_compact_view' is set
• from - date range start, can be 'relative' (e.g.: now-1m)
• to - date range end, can be 'relative' (e.g.: now-1m)

Fullscreen/kiosk mode

Fullscreen and kiosk modes in supported frontend pages can be activated using URL parameters. For example, in dashboards:
• /zabbix.php?action=dashboard.view&fullscreen=1 - activate fullscreen mode
• /zabbix.php?action=dashboard.view&kiosk=1 - activate kiosk mode
• /zabbix.php?action=dashboard.view&fullscreen=0 - activate normal mode

6 Definitions

Overview

While many things in the frontend can be configured using the frontend itself, some customisations are currently only possible by editing a definitions file.

This file is defines.inc.php located in /include of the Zabbix HTML document directory.

Parameters

Parameters in this file that could be of interest to users:

• ZBX_LOGIN_ATTEMPTS
  Number of unsuccessful login attempts that is allowed to an existing system user before a login block in applied (see ZBX_LOGIN_BLOCK). By default 5 attempts. Once the set number of login attempts is tried unsuccessfully, each additional unsuccessful attempt results in a login block. Used with internal authentication only.

• ZBX_LOGIN_BLOCK
  Number of seconds for blocking a user from accessing Zabbix frontend after a number of unsuccessful login attempts (see ZBX_LOGIN_ATTEMPTS). By default 30 seconds. Used with internal authentication only.

• ZBX_PERIOD_DEFAULT
  Default graph period, in seconds. One hour by default.

• ZBX_MIN_PERIOD
  Minimum graph period, in seconds. One minute by default.

• ZBX_MAX_PERIOD
  Maximum graph period, in seconds. Two years by default since 1.6.7, one year before that.

• ZBX_HISTORY_PERIOD
  The maximum period to display history data in Latest data, Web, Overview pages and Data overview screen element in seconds. By default set to 86400 seconds (24 hours). Unlimited period, if set to 0 seconds. This constant value also affects how far in the past the value is searched when {ITEM.VALUE} macro in trigger name is resolved.

• GRAPH_YAXIS_SIDE_DEFAULT
  Default location of Y axis in simple graphs and default value for drop down box when adding items to custom graphs. Possible values: 0 - left, 1 - right.
  Default: 0

• SCREEN_REFRESH_RESPONSIVENESS (available since 2.0.4)
  Used in screens and defines the number of seconds after which query skipping will be switched off. Otherwise, if a screen element is in update status all queries on update are skipped until a response is received. With this parameter in use, another update query might be sent after N seconds without having to wait for the response to the first one.
  Default: 10

• QUEUE_DETAIL_ITEM_COUNT
Defines retrieval limit of the total items queued. Since Zabbix 3.2.4 may be set higher than default value.

Default: 500

- **ZBX_SHOW_SQL_ERRORS** (available since 3.4.0)

  Show SQL errors in the frontend, if 'true'. If changed to 'false' then SQL errors will still be displayed to all users with Debug mode enabled. With Debug mode disabled, only Zabbix Super Admin users will see SQL errors. Others will see a generic message: "SQL error. Please contact Zabbix administrator."

  Default: true

- **VALIDATE_URI_SCHEMES** (available since 3.4.5)

  Validate a URI against the scheme whitelist defined in ZBX_URI_VALID_SCHEMES.

  Default: true

- **ZBX_URI_VALID_SCHEMES** (available since 3.4.2)

  A comma-separated list of allowed URI schemes. Affects all places in the frontend where URIs are used, for example, in map element URLs.

  Default: http,https,ftp,file,mailto,tel,ssh

  - **ZBX_SHOW_TECHNICAL_ERRORS** (available since 3.4.4)

    Show technical errors (PHP/SQL) to non-Zabbix Super admin users and to users that are not part of user groups with debug mode enabled.

    Default: false

- **ZBX_SESSION_NAME** (available since 4.0.0)

  String used as the name of the Zabbix frontend session cookie.

  Default: zbx_sessionid

### 7 Creating your own theme

**Overview**

By default, Zabbix provides a number of predefined themes. You may follow the step-by-step procedure provided here in order to create your own. Feel free to share the result of your work with Zabbix community if you created something nice.

**Step 1**

To define your own theme you’ll need to create a CSS file and save it in the `styles/` folder (for example, custom-theme.css). You can either copy the files from a different theme and create your theme based on it or start from scratch.

**Note:**

Since Zabbix 4.0.8, the CSS must be saved in `assets/styles`.

**Step 2**

Add your theme to the list of themes returned by the Z::getThemes() method. You can do this by overriding the ZBase::getThemes() method in the Z class. This can be done by adding the following code before the closing brace in include/classes/core/Z.php:

```php
public static function getThemes() {
    return array_merge(parent::getThemes(), array(
        'custom-theme' => _('Custom theme')
    ));
}
```

**Attention:**

Note that the name you specify within the first pair of quotes must match the name of the theme file without extension.

To add multiple themes, just list them under the first theme, for example:
public static function getThemes() {
    return array_merge(parent::getThemes(), array(
        'custom-theme' => _('Custom theme'),
        'anothertheme' => _('Another theme'),
        'onemoretheme' => _('One more theme')
    ));
}

Note that every theme except the last one must have a trailing comma.

**Note:**
To change graph colors, the entry must be added in the graph_theme database table.

Step 3
Activate the new theme.

In Zabbix frontend, you may either set this theme to be the default one or change your theme in the user profile.

Enjoy the new look and feel!

**8 Debug mode**

Overview
Debug mode may be used to diagnose performance problems with frontend pages.

Configuration
Debug mode can be activated for individual users who belong to a user group:

- when configuring a user group;
- when viewing configured user groups.

When Debug mode is enabled for a user group, its users will see a Debug button in the lower right corner of the browser window:

![Debug button](image)

Clicking on the Debug button opens a new window below the page contents which contains the SQL statistics of the page, along with a list of API calls and individual SQL statements:

```
*************** Script profiler *******************
Total time: 0.249625
Total SQL time: 0.139814
SQL count: 143 (selects: 117 | executes: 26)
Peak memory usage: 6M
Memory limit: 128M

1. hostgroup.get [latest.php:124]
Parameters: Array
            Result: Array
```

In case of performance problems with the page, this window may be used to search for the root cause of the problem.

**Warning:**
Enabled Debug mode negatively affects frontend performance.
# Cookies used by Zabbix

## Overview

This page provides a list of cookies used by Zabbix.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Values</th>
<th>Expires/Max-Age</th>
<th>Secure*</th>
</tr>
</thead>
<tbody>
<tr>
<td>PHPSESSID</td>
<td>Unique PHP session ID. The length can be set in php.ini - session.sid_length.</td>
<td>Example: kvlp5pu2ru1a2ccvff0g52m87a</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>ZBX_SESSION_NAME</td>
<td>Session cookie ID - a 32 character string. String used as the name of the Zabbix frontend session cookie.</td>
<td>Example: 004bc0213e7e8bca87fcc3919eca5270</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>Tab</td>
<td>Active tab number; this cookie is only used on pages with multiple tabs (e.g. Host, Trigger or Action configuration page) and is created, when a user navigates from a primary tab to another tab (such as Tags or Dependencies tab). 0 is used for the primary tab.</td>
<td>Example: 1</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>BrowserWarning</td>
<td>Whether a warning about using an outdated browser should be ignored.</td>
<td>yes</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

*Secure indicates that the cookie should only be transmitted over a secure HTTPS connection from the client. When set to 'true', the cookie will only be set if a secure connection exists.

According to specification these are voltages on chip pins and generally speaking may need scaling.
19. API

Overview  Zabbix API allows you to programmatically retrieve and modify the configuration of Zabbix and provides access to historical data. It is widely used to:

- Create new applications to work with Zabbix;
- Integrate Zabbix with third party software;
- Automate routine tasks.

The Zabbix API is a web based API and is shipped as part of the web frontend. It uses the JSON-RPC 2.0 protocol which means two things:

- The API consists of a set of separate methods;
- Requests and responses between the clients and the API are encoded using the JSON format.

More info about the protocol and JSON can be found in the JSON-RPC 2.0 specification and the JSON format homepage.

Structure  The API consists of a number of methods that are nominally grouped into separate APIs. Each of the methods performs one specific task. For example, the host.create method belongs to the host API and is used to create new hosts. Historically, APIs are sometimes referred to as "classes".

Note: Most APIs contain at least four methods: get, create, update and delete for retrieving, creating, updating and deleting data respectively, but some of the APIs may provide a totally different set of methods.

Performing requests  Once you’ve set up the frontend, you can use remote HTTP requests to call the API. To do that you need to send HTTP POST requests to the api_jsonrpc.php file located in the frontend directory. For example, if your Zabbix frontend is installed under http://example.com/zabbix, the HTTP request to call the apiinfo.version method may look like this:

```
POST http://example.com/zabbix/api_jsonrpc.php HTTP/1.1
Content-Type: application/json-rpc

{
    "jsonrpc": "2.0",
    "method": "apiinfo.version",
    "id": 1,
    "auth": null,
    "params": {}
}
```

The request must have the Content-Type header set to one of these values: application/json-rpc, application/json or application/jsonrequest.

Example workflow  The following section will walk you through some usage examples in more detail.

Authentication  Before you can access any data inside of Zabbix you’ll need to log in and obtain an authentication token. This can be done using the user.login method. Let us suppose that you want to log in as a standard Zabbix Admin user. Then your JSON request will look like this:

```
{
    "jsonrpc": "2.0",
    "method": "user.login",
    "params": {
        "user": "Admin",
        "password": "zabbix"
    },
    "id": 1,
}
```
Let's take a closer look at the request object. It has the following properties:

- `jsonrpc` - the version of the JSON-RPC protocol used by the API; the Zabbix API implements JSON-RPC version 2.0;
- `method` - the API method being called;
- `params` - parameters that will be passed to the API method;
- `id` - an arbitrary identifier of the request;
- `auth` - a user authentication token; since we don't have one yet, it's set to `null`.

If you provided the credentials correctly, the response returned by the API will contain the user authentication token:

```
{
    "jsonrpc": "2.0",
    "result": "0424bd59b807674191e7d77572075f33",
    "id": 1
}
```

The response object in turn contains the following properties:

- `jsonrpc` - again, the version of the JSON-RPC protocol;
- `result` - the data returned by the method;
- `id` - identifier of the corresponding request.

### Retrieving hosts

We now have a valid user authentication token that can be used to access the data in Zabbix. For example, let's use the `host.get` method to retrieve the IDs, host names and interfaces of all configured hosts:

```
{
    "jsonrpc": "2.0",
    "method": "host.get",
    "params": {
        "output": ["hostid", "host"],
        "selectInterfaces": ["interfaceid", "ip"]
    },
    "id": 2,
    "auth": "0424bd59b807674191e7d77572075f33"
}
```

**Attention:**

Note that the `auth` property is now set to the authentication token we've obtained by calling `user.login`.

The response object will contain the requested data about the hosts:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "hostid": "10084",
            "host": "Zabbix server",
            "interfaces": [
                {
                    "interfaceid": "1",
                    "ip": "127.0.0.1"
                }
            ]
        }
    ],
    "id": 2
}
```
Creating a new item  Let’s create a new item on “Zabbix server” using the data we’ve obtained from the previous `host.get` request. This can be done by using the `item.create` method:

```json
{
    "jsonrpc": "2.0",
    "method": "item.create",
    "params": {
        "name": "Free disk space on /home/joe/",
        "key_": "vfs.fs.size[/home/joe/,free]",
        "hostid": "10084",
        "value_type": 3,
        "interfaceid": "1",
        "delay": 30
    },
    "auth": "0424bd59b807674191e7d77572075f33",
    "id": 3
}
```

A successful response will contain the ID of the newly created item, which can be used to reference the item in the following requests:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "24759"
        ]
    },
    "id": 3
}
```

### Note:
The `item.create` method as well as other create methods can also accept arrays of objects and create multiple items with one API call.

Creating multiple triggers  So if create methods accept arrays, we can add multiple triggers like so:

```json
{
    "jsonrpc": "2.0",
    "method": "trigger.create",
    "params": [
        {
            "description": "Processor load is too high on {HOST.NAME}"
        },
        {
            "description": "Too many processes on {HOST.NAME}"
        }
    ],
    "auth": "0424bd59b807674191e7d77572075f33",
    "id": 4
}
```

A successful response will contain the IDs of the newly created triggers:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "triggerids": [
            "24759"
        ]
    },
    "id": 4
}
```
Updating an item  Enable an item, that is, set its status to “0”:

```
{
    "jsonrpc": "2.0",
    "method": "item.update",
    "params": {
        "itemid": "10092",
        "status": 0
    },
    "auth": "0424bd59b807674191e7d77572075f33",
    "id": 5
}
```

A successful response will contain the ID of the updated item:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": ["10092"
    ]
},
    "id": 5
}
```

Note: The item.update method as well as other update methods can also accept arrays of objects and update multiple items with one API call.

Updating multiple triggers  Enable multiple triggers, that is, set their status to 0:

```
{
    "jsonrpc": "2.0",
    "method": "trigger.update",
    "params": [
        {
            "triggerid": "13938",
            "status": 0
        },
        {
            "triggerid": "13939",
            "status": 0
        }
    ],
    "auth": "0424bd59b807674191e7d77572075f33",
    "id": 6
}
```

A successful response will contain the IDs of the updated triggers:

```
{
    "jsonrpc": "2.0",
    "result": {
        "triggerids": ["13938",
    ]
}
Note:
This is the preferred method of updating. Some API methods like host.massupdate allow to write more simple code, but it’s not recommended to use those methods, since they will be removed in the future releases.

Error handling  Up to that point everything we've tried has worked fine. But what happens if we try to make an incorrect call to the API? Let’s try to create another host by calling host.create but omitting the mandatory groups parameter.

```json
{
   "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"
         }
      ],
      "id": 7,
      "auth": "0424bd59b807674191e7d77572075f33"
   }
}
```

The response will then contain an error message:

```json
{
   "jsonrpc": "2.0",
   "error": {
      "code": -32602,
      "message": "Invalid params."
   },
   "id": 7
}
```

If an error occurred, instead of the result property, the response object will contain an error property with the following data:

- code  - an error code;
- message  - a short error summary;
- data  - a more detailed error message.

Errors can occur in different cases, such as, using incorrect input values, a session timeout or trying to access unexisting objects. Your application should be able to gracefully handle these kinds of errors.

API versions  To simplify API versioning, since Zabbix 2.0.4, the version of the API matches the version of Zabbix itself. You can use the apiinfo.version method to find out the version of the API you’re working with. This can be useful for adjusting your application to use version-specific features.

We guarantee feature backward compatibility inside of a major version. When making backward incompatible changes between major releases, we usually leave the old features as deprecated in the next release, and only remove them in the release after that. Occasionally, we may remove features between major releases without providing any backward compatibility. It is important that you never rely on any deprecated features and migrate to newer alternatives as soon as possible.
Further reading You now know enough to start working with the Zabbix API, but don’t stop here. For further reading we suggest you have a look at the list of available APIs.

Method reference

This section provides an overview of the functions provided by the Zabbix API and will help you find your way around the available classes and methods.

Monitoring The Zabbix API allows you to access history and other data gathered during monitoring.

History
Retrieve historical values gathered by Zabbix monitoring processes for presentation or further processing.

History API

Trends
Retrieve trend values calculated by Zabbix server for presentation or further processing.

Trend API

Events
Retrieve events generated by triggers, network discovery and other Zabbix systems for more flexible situation management or third-party tool integration.

Event API

Problems
Retrieve problems according to the given parameters.

Problem API

Service monitoring
Retrieve detailed service layer availability information about any service.

Service SLA calculation

Tasks
Task manager allows to check items or low-level discovery rules without config reload.

Task API

Configuration The Zabbix API allows you to manage the configuration of your monitoring system.

Hosts and host groups
Manage host groups, hosts and everything related to them, including host interfaces, host macros and maintenance periods.

Host API | Host group API | Host interface API | User macro API | Maintenance API

Items and applications
Define items to monitor. Create or remove applications and assign items to them.

Item API | Application API

Triggers
Configure triggers to notify you about problems in your system. Manage trigger dependencies.

Trigger API

Graphs
Edit graphs or separate graph items for better presentation of the gathered data.
Graph API | Graph item API

Templates
Manage templates and link them to hosts or other templates.

Template API

Export and import
Export and import Zabbix configuration data for configuration backups, migration or large-scale configuration updates.

Configuration API

Low-level discovery
Configure low-level discovery rules as well as item, trigger and graph prototypes to monitor dynamic entities.
LLD rule API | Item prototype API | Trigger prototype API | Graph prototype API | Host prototype API

Event correlation
Create custom event correlation rules.

Correlation API

Actions and alerts
Define actions and operations to notify users about certain events or automatically execute remote commands. Gain access to information about generated alerts and their receivers.
Action API | Alert API

Services
Manage services for service-level monitoring and retrieve detailed SLA information about any service.
Service API

Dashboards
Manage dashboards.
Dashboard API

Screens
Edit global and template-level screens or each screen item individually.
Screen API | Screen item API | Template screen API | Template screen item API

Maps
Configure maps to create detailed dynamic representations of your IT infrastructure.
Map API

Web monitoring
Configure web scenarios to monitor your web applications and services.
Web scenario API

Network discovery
Manage network-level discovery rules to automatically find and monitor new hosts. Gain full access to information about discovered services and hosts.
Discovery rule API | Discovery check API | Discovered host API | Discovered service API

Administration  With the Zabbix API you can change administration settings of your monitoring system.

Users
Add users that will have access to Zabbix, assign them to user groups and grant permissions. Configure media types and the ways users will receive alerts.
User API | User group API | Media type API

General
Change certain global configuration options.
Proxies
Manage the proxies used in your distributed monitoring setup.

Proxy API

Scripts
Configure and execute scripts to help you with your daily tasks.

Script API

**API information** Retrieve the version of the Zabbix API so that your application could use version-specific features.

**API info API**

**Action**

This class is designed to work with actions.

Object references:

- **Action**
- **Action condition**
- **Action operation**

Available methods:

- **action.create** - create new actions
- **action.delete** - delete actions
- **action.get** - retrieve actions
- **action.update** - update actions

---

**> Action object**

The following objects are directly related to the action API.

**Action**

The action object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>actionid</td>
<td>string</td>
<td>(readonly) ID of the action.</td>
</tr>
<tr>
<td><strong>esc_period</strong></td>
<td>string</td>
<td>Default operation step duration. Must be at least 60 seconds. Accepts seconds, time unit with suffix and user macro. Note that escalations are supported only for trigger and internal actions. In trigger actions, escalations are not supported in problem recovery and update operations.</td>
</tr>
<tr>
<td>(required)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>eventsource</strong></td>
<td>integer</td>
<td>(constant) Type of events that the action will handle. Refer to the event “source” property for a list of supported event types.</td>
</tr>
<tr>
<td>(required)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>name</strong></td>
<td>string</td>
<td>Name of the action.</td>
</tr>
<tr>
<td>(required)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>def_longdata</td>
<td>string</td>
<td>Problem message text.</td>
</tr>
<tr>
<td>def_shortdata</td>
<td>string</td>
<td>Problem message subject.</td>
</tr>
<tr>
<td>r_longdata</td>
<td>string</td>
<td>Recovery message text.</td>
</tr>
<tr>
<td>r_shortdata</td>
<td>string</td>
<td>Recovery message subject.</td>
</tr>
<tr>
<td>ack_longdata</td>
<td>string</td>
<td>Update operation message text.</td>
</tr>
<tr>
<td>ack_shortdata</td>
<td>string</td>
<td>Update operation message subject.</td>
</tr>
</tbody>
</table>
### Property | Type | Description
--- | --- | ---
Status | integer | Whether the action is enabled or disabled.
- Possible values:
  - 0 - (default) enabled;
  - 1 - disabled.

Pause suppressed | integer | Whether to pause escalation during maintenance periods or not.
- Possible values:
  - 0 - Don’t pause escalation;
  - 1 - (default) Pause escalation.

Note: This parameter is valid for trigger actions only.

---

Note that for some methods (update, delete) the required/optional parameter combination is different.

#### Action Operation

The action operation object defines an operation that will be performed when an action is executed. It has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation ID</td>
<td>string</td>
<td>(readonly) ID of the action operation.</td>
</tr>
<tr>
<td>Operation type</td>
<td>integer</td>
<td>Type of operation.</td>
</tr>
</tbody>
</table>
- Possible values:
  - 0 - send message;
  - 1 - remote command;
  - 2 - add host;
  - 3 - remove host;
  - 4 - add to host group;
  - 5 - remove from host group;
  - 6 - link to template;
  - 7 - unlink from template;
  - 8 - enable host;
  - 9 - disable host;
  - 10 - set host inventory mode.

- Note that only types ‘0’ and ‘1’ are supported for trigger actions, only ‘0’ is supported for internal actions. All types are supported for discovery and autoregistration actions.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action ID</td>
<td>string</td>
<td>ID of the action that the operation belongs to.</td>
</tr>
<tr>
<td>Esc period</td>
<td>string</td>
<td>Duration of an escalation step in seconds. Must be greater than 60 seconds. Accepts seconds, time unit with suffix and user macro. If set to 0 or 0s, the default action escalation period will be used.</td>
</tr>
</tbody>
</table>
- Default: 0s.

- Note that escalations are supported only for trigger and internal actions. In trigger actions, escalations are not supported in problem recovery and update operations.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Esc step from</td>
<td>integer</td>
<td>Step to start escalation from.</td>
</tr>
</tbody>
</table>
- Default: 1.

- Note that escalations are supported only for trigger and internal actions. In trigger actions, escalations are not supported in problem recovery and update operations.
<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>esc_step_to</td>
<td>integer</td>
<td>Step to end escalation at.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note that escalations are supported only for trigger and internal actions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In trigger actions, escalations are not supported in problem recovery and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>update operations.</td>
</tr>
<tr>
<td>evaltype</td>
<td>integer</td>
<td>Operation condition evaluation method.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values: 0 - (default) AND / OR; 1 - AND; 2 - OR.</td>
</tr>
<tr>
<td>opcommand</td>
<td>object</td>
<td>Object containing the data about the command run by the operation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The operation command object is described in detail below.</td>
</tr>
<tr>
<td>opcommand_grp</td>
<td>array</td>
<td>Host groups to run remote commands on.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Each object has the following properties:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>opcommand_grpid - (string, readonly) ID of the object;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>operationid - (string) ID of the operation;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>groupid - (string) ID of the host group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Required for remote command operations if opcommand_hst is not set.</td>
</tr>
<tr>
<td>opcommand_hst</td>
<td>array</td>
<td>Host to run remote commands on.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Each object has the following properties:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>opcommand_hstid - (string, readonly) ID of the object;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>operationid - (string) ID of the operation;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>hostid - (string) ID of the host; if set to 0 the command will be run on</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the current host.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Required for remote command operations if opcommand_grp is not set.</td>
</tr>
<tr>
<td>opconditions</td>
<td>array</td>
<td>Operation conditions used for trigger actions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The operation condition object is described in detail below.</td>
</tr>
<tr>
<td>opgroup</td>
<td>array</td>
<td>Host groups to add hosts to.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Each object has the following properties:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>operationid - (string) ID of the operation;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>groupid - (string) ID of the host group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Required for “add to host group” and “remove from host group” operations.</td>
</tr>
<tr>
<td>opmessage</td>
<td>object</td>
<td>Object containing the data about the message sent by the operation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The operation message object is described in detail below.</td>
</tr>
<tr>
<td>opmessage_grp</td>
<td>array</td>
<td>User groups to send messages to.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Each object has the following properties:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>operationid - (string) ID of the operation;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>usrgrpid - (string) ID of the user group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Required for message operations if opmessage_usr is not set.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>opmessage_usr</td>
<td>array</td>
<td>Users to send messages to. Each object has the following properties:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>operationid - (string) ID of the operation;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>userid - (string) ID of the user.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Required for message operations if opmessage_grp is not set.</td>
</tr>
<tr>
<td>optemplate</td>
<td>array</td>
<td>Templates to link the hosts to.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Each object has the following properties:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>operationid - (string) ID of the operation;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>templateid - (string) ID of the template.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Required for &quot;link to template&quot; and &quot;unlink from template&quot; operations.</td>
</tr>
<tr>
<td>opinventory</td>
<td>object</td>
<td>Inventory mode set host to.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Object has the following properties:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>operationid - (string) ID of the operation;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>inventory_mode - (string) Inventory mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Required for &quot;Set host inventory mode&quot; operations.</td>
</tr>
</tbody>
</table>

**Action operation command**

The operation command object contains data about the command that will be run by the operation.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>operationid</td>
<td>string</td>
<td>(readonly) ID of the operation.</td>
</tr>
<tr>
<td>command</td>
<td>string</td>
<td>Command to run. Required when type IN (0,1,2,3)</td>
</tr>
<tr>
<td>type</td>
<td>integer</td>
<td>Type of operation command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - custom script;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - IPMI;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 - SSH;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 - Telnet;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 - global script.</td>
</tr>
<tr>
<td>authtype</td>
<td>integer</td>
<td>Authentication method used for SSH commands.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - password;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - public key.</td>
</tr>
<tr>
<td>execute_on</td>
<td>integer</td>
<td>Target on which the custom script operation command will be executed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - Zabbix agent;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - Zabbix server;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 - Zabbix server (proxy).</td>
</tr>
<tr>
<td>password</td>
<td>string</td>
<td>Password used for SSH commands with password authentication and Telnet commands.</td>
</tr>
<tr>
<td>port</td>
<td>string</td>
<td>Port number used for SSH and Telnet commands.</td>
</tr>
<tr>
<td>privatekey</td>
<td>string</td>
<td>Name of the private key file used for SSH commands with public key authentication.</td>
</tr>
</tbody>
</table>

Required for SSH commands.

Required for custom script commands.

722
<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>publickey</td>
<td>string</td>
<td>Name of the public key file used for SSH commands with public key authentication.</td>
</tr>
<tr>
<td>scriptid</td>
<td>string</td>
<td>ID of the script used for global script commands.</td>
</tr>
<tr>
<td>username</td>
<td>string</td>
<td>User name used for authentication.</td>
</tr>
</tbody>
</table>

**Action operation message**

The operation message object contains data about the message that will be sent by the operation.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>operationid</td>
<td>string</td>
<td>(readonly) ID of the action operation.</td>
</tr>
<tr>
<td>default_msg</td>
<td>integer</td>
<td>Whether to use the default action message text and subject. Possible values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - (default) use the data from the operation; 1 - use the data from the action.</td>
</tr>
<tr>
<td>mediatypeid</td>
<td>string</td>
<td>ID of the media type that will be used to send the message.</td>
</tr>
<tr>
<td>message</td>
<td>string</td>
<td>Operation message text.</td>
</tr>
<tr>
<td>subject</td>
<td>string</td>
<td>Operation message subject.</td>
</tr>
</tbody>
</table>

**Action operation condition**

The action operation condition object defines a condition that must be met to perform the current operation. It has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>conditionid</td>
<td>string</td>
<td>(readonly) ID of the action operation condition Type of condition.</td>
</tr>
<tr>
<td>conditiontype</td>
<td>integer</td>
<td>Possible values: 14 - event acknowledged.</td>
</tr>
<tr>
<td>value</td>
<td>string</td>
<td>Value to compare with.</td>
</tr>
<tr>
<td>operationid</td>
<td>string</td>
<td>(readonly) ID of the operation.</td>
</tr>
<tr>
<td>operator</td>
<td>integer</td>
<td>Condition operator.</td>
</tr>
</tbody>
</table>

The following operators and values are supported for each operation condition type.

<table>
<thead>
<tr>
<th>Condition</th>
<th>Condition name</th>
<th>Supported operators</th>
<th>Expected value</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>Event acknowledged</td>
<td>=</td>
<td>Whether the event is acknowledged.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Possible values: 0 - not acknowledged;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - acknowledged.</td>
</tr>
</tbody>
</table>

**Action recovery operation**

The action recovery operation object defines an operation that will be performed when a problem is resolved. Recovery operations are possible for trigger actions and internal actions. It has the following properties.
<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>operationid</td>
<td>string</td>
<td>(readonly) ID of the action operation.</td>
</tr>
<tr>
<td>operationtype</td>
<td>integer</td>
<td>ID of the action operation.</td>
</tr>
<tr>
<td>actionid</td>
<td>string</td>
<td>ID of the action that the recovery operation belongs to.</td>
</tr>
<tr>
<td>opcommand</td>
<td>object</td>
<td>Object containing the data about the command run by the recovery operation.</td>
</tr>
<tr>
<td>opcommand_grp</td>
<td>array</td>
<td>Host groups to run remote commands on.</td>
</tr>
<tr>
<td>opcommand_hst</td>
<td>array</td>
<td>Host to run remote commands on.</td>
</tr>
<tr>
<td>opmessage</td>
<td>object</td>
<td>Object containing the data about the message sent by the recovery operation.</td>
</tr>
<tr>
<td>opmessage_grp</td>
<td>array</td>
<td>User groups to send messages to.</td>
</tr>
<tr>
<td>opmessage_usr</td>
<td>array</td>
<td>Users to send messages to.</td>
</tr>
</tbody>
</table>

**Operation update operation**

The action update operation object defines an operation that will be performed when a problem is updated (commented upon,
acknowledged, severity changed, or manually closed). Update operations are possible for trigger actions. It has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>operationid</td>
<td>string</td>
<td>(readonly) ID of the action operation.</td>
</tr>
<tr>
<td>operationtype</td>
<td>integer</td>
<td>Type of operation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values for trigger actions:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - send message;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - remote command;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>12 - notify all involved.</td>
</tr>
<tr>
<td>opcommand</td>
<td>object</td>
<td>Object containing the data about the command run by the recovery operation.</td>
</tr>
<tr>
<td>opcommand_grp</td>
<td>array</td>
<td>Required for remote command operations.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Host groups to run remote commands on.</td>
</tr>
<tr>
<td>opcommand_hst</td>
<td>array</td>
<td>Each object has the following properties:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>groupid - (string) ID of the host group.</td>
</tr>
<tr>
<td>opmessage</td>
<td>object</td>
<td>Object containing the data about the message sent by the recovery operation.</td>
</tr>
<tr>
<td>opmessage_grp</td>
<td>array</td>
<td>User groups to send messages to.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Each object has the following properties:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>usgrpid - (string) ID of the user group.</td>
</tr>
<tr>
<td>opmessage_usr</td>
<td>array</td>
<td>Users to send messages to.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Each object has the following properties:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>userid - (string) ID of the user.</td>
</tr>
</tbody>
</table>

Action filter

The action filter object defines a set of conditions that must be met to perform the configured action operations. It has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>conditions</td>
<td>array</td>
<td>Set of filter conditions to use for filtering results.</td>
</tr>
</tbody>
</table>
### Property

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>evaltype</strong></td>
<td>integer</td>
<td>Filter condition evaluation method.</td>
</tr>
<tr>
<td>(required)</td>
<td></td>
<td>Possible values: 0 - and/or; 1 - and; 2 - or; 3 - custom expression.</td>
</tr>
<tr>
<td><strong>eval_formula</strong></td>
<td>string</td>
<td>(readonly) Generated expression that will be used for evaluating filter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>conditions. The expression contains IDs that reference specific filter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>conditions by its formulaid. The value of eval_formula is equal to the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>value of formula for filters with a custom expression.</td>
</tr>
<tr>
<td><strong>formula</strong></td>
<td>string</td>
<td>User-defined expression to be used for evaluating conditions of filters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>with a custom expression. The expression must contain IDs that reference</td>
</tr>
<tr>
<td></td>
<td></td>
<td>specific filter conditions by its formulaid. The IDs used in the expression</td>
</tr>
<tr>
<td></td>
<td></td>
<td>must exactly match the ones defined in the filter conditions: no condition</td>
</tr>
<tr>
<td></td>
<td></td>
<td>can remain unused or omitted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Required for custom expression filters.</td>
</tr>
</tbody>
</table>

### Action filter condition

The action filter condition object defines a specific condition that must be checked before running the action operations.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>conditionid</td>
<td>string</td>
<td>(readonly) ID of the action condition.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>--------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>conditiontype</td>
<td>integer</td>
<td>Type of condition.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values for trigger actions:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - host group;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - host;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 - trigger;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 - trigger name;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 - trigger severity;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6 - time period;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>13 - host template;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>15 - application;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>16 - problem is suppressed;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>25 - event tag;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>26 - event tag value.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values for discovery actions:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7 - host IP;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8 - discovered service type;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9 - discovered service port;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10 - discovery status;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11 - uptime or downtime duration;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>12 - received value;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>18 - discovery rule;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>19 - discovery check;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>20 - proxy;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>21 - discovery object.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values for auto-registration actions:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>20 - proxy;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>22 - host name;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>24 - host metadata.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values for internal actions:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - host group;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - host;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>13 - host template;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>15 - application;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>23 - event type.</td>
</tr>
<tr>
<td>value</td>
<td>string</td>
<td>Value to compare with.</td>
</tr>
<tr>
<td></td>
<td>(required)</td>
<td></td>
</tr>
<tr>
<td>value2</td>
<td>string</td>
<td>Secondary value to compare with. Required for</td>
</tr>
<tr>
<td></td>
<td></td>
<td>trigger actions when condition type is 26.</td>
</tr>
<tr>
<td>actionid</td>
<td>string</td>
<td>(readonly) ID of the action that the condition</td>
</tr>
<tr>
<td></td>
<td></td>
<td>belongs to.</td>
</tr>
<tr>
<td>formulaid</td>
<td>string</td>
<td>Arbitrary unique ID that is used to reference</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the condition from a custom expression.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Can only contain capital-case letters. The ID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>must be defined by the user when modifying filter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>conditions, but will be generated anew when</td>
</tr>
<tr>
<td></td>
<td></td>
<td>requesting them afterward.</td>
</tr>
<tr>
<td>operator</td>
<td>integer</td>
<td>Condition operator.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - (default) equals;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - does not equal;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 - contains;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 - does not contain;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 - in;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5 - is greater than or equals;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6 - is less than or equals;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7 - not in;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10 - Yes;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11 - No.</td>
</tr>
</tbody>
</table>

727
The following operators and values are supported for each condition type.

<table>
<thead>
<tr>
<th>Condition</th>
<th>Condition name</th>
<th>Supported operators</th>
<th>Expected value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Host group</td>
<td>equals, does not equal</td>
<td>Host group ID.</td>
</tr>
<tr>
<td>1</td>
<td>Host</td>
<td>equals, does not equal</td>
<td>Host ID.</td>
</tr>
<tr>
<td>2</td>
<td>Trigger</td>
<td>equals, does not equal</td>
<td>Trigger ID.</td>
</tr>
<tr>
<td>3</td>
<td>Trigger name</td>
<td>contains, does not contain</td>
<td>Trigger name.</td>
</tr>
<tr>
<td>4</td>
<td>Trigger severity</td>
<td>equals, does not equal, is greater than or equals, is less than or equals</td>
<td>Trigger severity. Refer to the trigger &quot;severity&quot; property for a list of supported trigger severities.</td>
</tr>
<tr>
<td>5</td>
<td>Trigger value</td>
<td>equals, does not equal</td>
<td>Trigger value. Refer to the trigger &quot;value&quot; property for a list of supported trigger values.</td>
</tr>
<tr>
<td>6</td>
<td>Time period</td>
<td>in, not in</td>
<td>Time when the event was triggered as a time period.</td>
</tr>
<tr>
<td>7</td>
<td>Host IP</td>
<td>equals, does not equal</td>
<td>One or several IP ranges to check separated by commas. Refer to the network discovery configuration section for more information on supported formats of IP ranges.</td>
</tr>
<tr>
<td>8</td>
<td>Discovered service type</td>
<td>equals, does not equal</td>
<td>Type of discovered service. The type of service matches the type of the discovery check used to detect the service. Refer to the discovery check &quot;type&quot; property for a list of supported types.</td>
</tr>
<tr>
<td>9</td>
<td>Discovered service port</td>
<td>equals, does not equal</td>
<td>One or several port ranges separated by commas.</td>
</tr>
</tbody>
</table>
| 10        | Discovery status | equals | Status of a discovered object. Possible values: 
0 - host or service up; 
1 - host or service down; 
2 - host or service discovered; 
3 - host or service lost. |
| 11        | Uptime or downtime duration | is greater than or equals, is less than or equals | Time indicating how long has the discovered object been in the current status in seconds. |
| 12        | Received values | equals, does not equal, contains, does not contain | Value returned when performing a Zabbix agent, SNMPv1, SNMPv2 or SNMPv3 discovery check. |
| 13        | Host template  | equals, does not equal | Linked template ID. |
| 15        | Application    | equals, contains, does not contain | Name of the application. |
| 16        | Problem is suppressed | Yes, No | No value required: using the "Yes" operator means that problem must be suppressed, "No" - not suppressed. |
| 18        | Discovery rule | equals, does not equal | ID of the discovery rule. |
Condition | Condition name | Supported operators | Expected value
---|---|---|---
19 | Discovery check | equals, does not equal | ID of the discovery check.
20 | Proxy | equals, does not equal | ID of the proxy.
21 | Discovery object | equals | Type of object that triggered the discovery event.
Possible values:
1 - discovered host;
2 - discovered service.
Host name.
22 | Host name | contains, does not contain | Specific internal event.
23 | Event type | equals | Possible values:
0 - item in “not supported” state;
1 - item in “normal” state;
2 - LLD rule in “not supported” state;
3 - LLD rule in “normal” state;
4 - trigger in “unknown” state;
5 - trigger in “normal” state.
24 | Host metadata | contains, does not contain | Metadata of the auto-registered host.
25 | Tag | equals, does not equal, contains, does not contain | Event tag.
26 | Tag value | equals, does not equal, contains, does not contain | Event tag value.

**action.create**

**Description**

object action.create(object/array actions)

This method allows to create new actions.

**Parameters**

(object/array) Actions to create.

Additionally to the standard action properties, the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter</td>
<td>object</td>
<td>Action filter object for the action.</td>
</tr>
<tr>
<td>operations</td>
<td>array</td>
<td>Action operations to create for the action.</td>
</tr>
<tr>
<td>recovery_operations</td>
<td>array</td>
<td>Action recovery operations to create for the action.</td>
</tr>
<tr>
<td>acknowledge_operations</td>
<td>array</td>
<td>Action update operations to create for the action.</td>
</tr>
</tbody>
</table>

**Return values**

(object) Returns an object containing the IDs of the created actions under the actionids property. The order of the returned IDs matches the order of the passed actions.

**Examples**

Create a trigger action

Create a trigger action that will begin once a trigger (with the word “memory” in its name) from host “10084” goes into a PROBLEM state. The action will have 4 configured operations. The first and immediate operation will send a message to all users in user
group "7" via media type "1". If the event is not resolved in 30 minutes, the second operation will run script "3" on all hosts in group "2". If the event is resolved, a recovery operation will notify all users who received any messages regarding the problem. If the event is updated, an acknowledge/update operation will notify (with a custom subject and message) all users who received any messages regarding the problem.

Request:

```json
{
  "jsonrpc": "2.0",
  "method": "action.create",
  "params": {
    "name": "Trigger action",
    "eventsource": 0,
    "esc_period": "30m",
    "def_shortdata": "{TRIGGER.NAME}: {TRIGGER.STATUS}",
    "def_longdata": "{TRIGGER.NAME}: {TRIGGER.STATUS}\nLast value: {ITEM.LASTVALUE}\n{TRIGGER.URL}",
    "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": {
          "type": 4,
```
Create a discovery action

Create a discovery action that will link discovered hosts to template "10001".

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "action.create",
    "params": {
        "name": "Discovery action",
        "eventsource": 1,
        "filter": {
            "evaltype": 0,
            "conditions": [
                {"conditiontype": 21,
                "value": "1"},
                {"conditiontype": 10,
                "value": "2"}
            ]
        },
        "operations": [
        
```
```
Using a custom expression filter

Create a trigger action that uses a custom expression - "A and (B or C)" - for evaluating action conditions. Once a trigger with a severity higher or equal to "Warning" from host "10084" or host "10106" goes into a PROBLEM state, the action will send a message to all users in user group "7" via media type "1". The formula IDs "A", "B" and "C" have been chosen arbitrarily.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "action.create",
    "params": {
        "name": "Trigger action",
        "eventsource": 0,
        "esc_period": "15m",
        "def_shortdata": "{TRIGGER.NAME}: {TRIGGER.STATUS}\nLast value: {ITEM.LASTVALUE}\n{TRIGGER.URL}"
    },
    "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"
      }
    }
  ],
  "auth": "038e1d7b1735c6a5436ee9eae096879e",
  "id": 1
}
```

Response:

```
{
  "jsonrpc": "2.0",
  "result": {
    "actionIds": [
      "18"
    ]
  },
  "id": 1
}
```

See also

- Action filter
- Action operation
- Script

Source

CAction::create() in frontends/php/include/classes/api/services/CAction.php.

**action.delete**

Description

`object action.delete(array actionIds)`

This method allows to delete actions.

Parameters

(array) IDs of the actions to delete.

Return values

(object) Returns an object containing the IDs of the deleted actions under the `actionIds` property.

Examples

Delete multiple actions

Delete two actions.

Request:
Source
CAction::delete() in frontends/php/include/classes/api/services/CAction.php.

**action.get**

**Description**

`integer/array action.get(object parameters)`

The method allows to retrieve actions according to the given parameters.

**Parameters**

(object) Parameters defining the desired output.

The method supports the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>actionids</td>
<td>string/array</td>
<td>Return only actions with the given IDs.</td>
</tr>
<tr>
<td>groupids</td>
<td>string/array</td>
<td>Return only actions that use the given host groups in action conditions.</td>
</tr>
<tr>
<td>hostids</td>
<td>string/array</td>
<td>Return only actions that use the given hosts in action conditions.</td>
</tr>
<tr>
<td>triggerids</td>
<td>string/array</td>
<td>Return only actions that use the given triggers in action conditions.</td>
</tr>
<tr>
<td>mediatypeids</td>
<td>string/array</td>
<td>Return only actions that use the given media types to send messages.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>usrgrpids</td>
<td>string/array</td>
<td>Return only actions that are configured to send messages to the given user groups.</td>
</tr>
<tr>
<td>userids</td>
<td>string/array</td>
<td>Return only actions that are configured to send messages to the given users.</td>
</tr>
<tr>
<td>scriptids</td>
<td>string/array</td>
<td>Return only actions that are configured to run the given scripts.</td>
</tr>
<tr>
<td>selectFilter</td>
<td>query</td>
<td>Returns the action filter in the filter property.</td>
</tr>
<tr>
<td>selectOperations</td>
<td>query</td>
<td>Return action operations in the operations property.</td>
</tr>
<tr>
<td>selectRecoveryOperations</td>
<td></td>
<td>Return action recovery operations in the recoveryOperations property.</td>
</tr>
<tr>
<td>selectAcknowledgedOperations</td>
<td></td>
<td>Return action update operations in the acknowledgeOperations property.</td>
</tr>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Sort the result by the given properties.</td>
</tr>
<tr>
<td>countOutput</td>
<td>boolean</td>
<td>These parameters being common for all get methods are described in the reference commentary.</td>
</tr>
</tbody>
</table>

Return values:

(integer/array) Returns either:
• an array of objects;
• the count of retrieved objects, if the countOutput parameter has been used.

Examples

Retrieve discovery actions

Retrieve all configured discovery actions together with action conditions and operations. The filter uses the "and" evaluation type, so the formula property is empty and eval_formula is generated automatically.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "action.get",
    "params": {
        "output": "extend",
        "selectOperations": "extend",
        "selectRecoveryOperations": "extend",
        "selectFilter": "extend",
        "filter": {
            "eventsource": 1
        }
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": [
        {
            "actionid": "2",
            "name": "Auto discovery. Linux servers.",
            "eventsource": "1",
            "status": "1",
            "esc_period": "0s",
            "def_shortdata": "",
            "def_longdata": "",
            "r_shortdata": "",
            "r_longdata": "",
            "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": [
{
"operationid": "1",
"templateid": "10001"
}
]
},
{
"operationid": "2",
"actionid": "2",
"operationtype": "4",
"esc_period": "0s",
"esc_step_from": "1",
"esc_step_to": "1",
"evaltype": "0",
"opconditions": [],
"opgroup": [
{
"operationid": "2",
"groupid": "2"
}
]
}
],
"recoveryOperations": [
{
"operationid": "585",
"actionid": "2",
"operationtype": "11",
"evaltype": "0",
"opconditions": [],
"opmessage": {
"operationid": "585",
"default_msg": "1",
"subject": "{TRIGGER.STATUS}: {TRIGGER.NAME}\r\nTrigger status: {TRIGGER.SEVERITY}\r\nTrigger URL: {TRIGGER.URL}\r\nItem values: \r\n1. {ITEM.NAME1} ({HOST.NAME1}:{ITEM.KEY1}): {ITEM.VALUE1}\n2. {ITEM.NAME2} ({HOST.NAME2}:{ITEM.KEY2}): {ITEM.VALUE2}\n3. {ITEM.NAME3} ({HOST.NAME3}:{ITEM.KEY3}): {ITEM.VALUE3}\r\nOriginal event ID: {EVENT.ID}"
}
]
},
"acknowledgeOperations": [
{
"operationid": "585",
"operationtype": "12",
"evaltype": "0",
"opmessage": {

"default_msg": "1",
"subject": "Updated: {TRIGGER.NAME}",
"message": "{USER.FULLNAME} updated problem at {EVENT.UPDATE.DATE} {EVENT.UPDATE.TIME} with the following message:

{EVENT.UPDATE.MESSAGE}

Current problem status is {EVENT.STATUS}"
],
"mediatypeid": "0"
},
{
"operationid": "586",
"operationtype": "0",
"evaltype": "0",
"opmessage": {
  "default_msg": "1",
  "subject": "Updated: {TRIGGER.NAME}",
  "message": "{USER.FULLNAME} updated problem at {EVENT.UPDATE.DATE} {EVENT.UPDATE.TIME} with the following message:

{EVENT.UPDATE.MESSAGE}

Current problem status is {EVENT.STATUS}"
],
"mediatypeid": "0"
},
"opmessage_grp": [
  {
    "usrgrpid": "7"
  }
],
"opmessage_usr": []
},
{
"operationid": "587",
"operationtype": "1",
"evaltype": "0",
"opcommand": {
  "type": "0",
  "scriptid": "0",
  "execute_on": "0",
  "port": "",
  "authtype": "0",
  "username": "",
  "password": "",
  "publickey": "",
  "privatekey": "",
  "command": "notify.sh"
},
"opcommand_hst": [
  {
    "hostid": "0"
  }
],
"opcommand_grp": []
]}
"id": 1
}

See also

- Action filter
- Action operation

Source

CAction::get() in frontends/php/include/classes/api/services/CAction.php.

**action.update**

Description
object action.update(object/array actions)

This method allows to update existing actions.

Parameters
(object/array) Action properties to be updated.

The actionid property must be defined for each action, all other properties are optional. Only the passed properties will be updated, all others will remain unchanged.

Additionally to the standard action properties, the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter</td>
<td>object</td>
<td>Action filter object to replace the current filter.</td>
</tr>
<tr>
<td>operations</td>
<td>array</td>
<td>Action operations to replace existing operations.</td>
</tr>
<tr>
<td>recovery_operations</td>
<td>array</td>
<td>Action recovery operations to replace existing recovery operations.</td>
</tr>
<tr>
<td>acknowledge_operations</td>
<td>array</td>
<td>Action update operations to replace existing update operations.</td>
</tr>
</tbody>
</table>

Return values

(object) Returns an object containing the IDs of the updated actions under the actionids property.

Examples

Disable action

Disable an action, that is, set its status to "1".

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "action.update",
    "params": {
        "actionid": "2",
        "status": "1"
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "actionids": [
            "2"
        ],
        "id": 1
    }
}
```

See also

• Action filter
• Action operation

Source

CAction::update() in frontends/php/include/classes/api/services/CAction.php.

Alert

This class is designed to work with alerts.

Object references:
• Alert

Available methods:

• alert.get - retrieve alerts

> Alert object

The following objects are directly related to the alert API.

Alert

Note:
Alerts are created by the Zabbix server and cannot be modified via the API.

The alert object contains information about whether certain action operations have been executed successfully. It has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alertid</td>
<td>string</td>
<td>ID of the alert.</td>
</tr>
<tr>
<td>actionid</td>
<td>string</td>
<td>ID of the action that generated the alert.</td>
</tr>
<tr>
<td>alerttype</td>
<td>integer</td>
<td>Alert type. Possible values: 0 - message; 1 - remote command.</td>
</tr>
<tr>
<td>clock</td>
<td>timestamp</td>
<td>Time when the alert was generated.</td>
</tr>
<tr>
<td>error</td>
<td>string</td>
<td>Error text if there are problems sending a message or running a command.</td>
</tr>
<tr>
<td>esc_step</td>
<td>integer</td>
<td>Action escalation step during which the alert was generated.</td>
</tr>
<tr>
<td>eventid</td>
<td>string</td>
<td>ID of the event that triggered the action.</td>
</tr>
<tr>
<td>mediatypeid</td>
<td>string</td>
<td>ID of the media type that was used to send the message.</td>
</tr>
<tr>
<td>message</td>
<td>text</td>
<td>Message text. Used for message alerts.</td>
</tr>
<tr>
<td>retries</td>
<td>integer</td>
<td>Number of times Zabbix tried to send the message.</td>
</tr>
<tr>
<td>sendto</td>
<td>string</td>
<td>Address, user name or other identifier of the recipient. Used for message alerts.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>status</td>
<td>integer</td>
<td>Status indicating whether the action operation has been executed successfully. Possible values for message alerts: 0 - message not sent. 1 - message sent. 2 - failed after a number of retries. 3 - new alert is not yet processed by alert manager.</td>
</tr>
<tr>
<td>subject</td>
<td>string</td>
<td>Message subject. Used for message alerts.</td>
</tr>
<tr>
<td>userid</td>
<td>string</td>
<td>ID of the user that the message was sent to.</td>
</tr>
<tr>
<td>p_eventid</td>
<td>string</td>
<td>ID of problem event, which generated the alert.</td>
</tr>
<tr>
<td>acknowledgeid</td>
<td>string</td>
<td>ID of acknowledgment, which generated the alert.</td>
</tr>
</tbody>
</table>

**alert.get**

Description

integer/array alert.get(object parameters)

The method allows to retrieve alerts according to the given parameters.

Parameters

(object) Parameters defining the desired output.

The method supports the following parameters.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alertids</td>
<td>string/array</td>
<td>Return only alerts with the given IDs.</td>
</tr>
<tr>
<td>actionids</td>
<td>string/array</td>
<td>Return only alerts generated by the given actions.</td>
</tr>
<tr>
<td>eventids</td>
<td>string/array</td>
<td>Return only alerts generated by the given events.</td>
</tr>
<tr>
<td>groupids</td>
<td>string/array</td>
<td>Return only alerts generated by objects from the given host groups.</td>
</tr>
<tr>
<td>hostids</td>
<td>string/array</td>
<td>Return only alerts generated by objects from the given hosts.</td>
</tr>
<tr>
<td>mediatypeids</td>
<td>string/array</td>
<td>Return only message alerts that used the given media types.</td>
</tr>
<tr>
<td>objectids</td>
<td>string/array</td>
<td>Return only alerts generated by the given objects</td>
</tr>
<tr>
<td>userids</td>
<td>string/array</td>
<td>Return only message alerts that were sent to the given users.</td>
</tr>
<tr>
<td>eventobject</td>
<td>integer</td>
<td>Return only alerts generated by events related to objects of the given type.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Refer to the event &quot;object&quot; property for a list of supported object types.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 0 - trigger.</td>
</tr>
<tr>
<td>eventsource</td>
<td>integer</td>
<td>Return only alerts generated by events of the given type.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Refer to the event &quot;source&quot; property for a list of supported event types.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 0 - trigger events.</td>
</tr>
<tr>
<td>time_from</td>
<td>timestamp</td>
<td>Return only alerts that have been generated after the given time.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>time_till</td>
<td>timestamp</td>
<td>Return only alerts that have been generated before the given time.</td>
</tr>
<tr>
<td>selectHosts</td>
<td>query</td>
<td>Return the hosts that triggered the action operation in the hosts property.</td>
</tr>
<tr>
<td>selectMediatypes</td>
<td>query</td>
<td>Return the media type that was used for the message alert as an array in the mediatypes property.</td>
</tr>
<tr>
<td>selectUsers</td>
<td>query</td>
<td>Return the user that the message was addressed to as an array in the users property.</td>
</tr>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Sort the result by the given properties.</td>
</tr>
<tr>
<td>editable</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>excludeSearch</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>filter</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>limit</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>output</td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>preservekeys</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>search</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>searchByAny</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>searchWildcards</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>sortorder</td>
<td>string/array</td>
<td></td>
</tr>
<tr>
<td>startSearch</td>
<td>boolean</td>
<td></td>
</tr>
</tbody>
</table>

Return values

(integer/array) Returns either:

- an array of objects;
- the count of retrieved objects, if the countOutput parameter has been used.

Examples

Retrieve alerts by action ID

Retrieve all alerts generated by action "3".

Request:
{  "jsonrpc": "2.0",  "method": "alert.get",  "params": {    "output": "extend",    "actionids": "3"  },  "auth": "038e1d7b1735c6a5436ee9eae095879e",  "id": 1}

Response:
{
  "jsonrpc": "2.0",  "result": [
    {
      "alertid": "1",      "actionid": "3",      "eventid": "21243",      "userid": "1",      "clock": "1362128008",      "mediatypeid": "1",      "sendto": "support@company.com",      "subject": "PROBLEM: Zabbix agent on Linux server is unreachable for 5 minutes: ",      "message": "Trigger: Zabbix agent on Linux server is unreachable for 5 minutes: 
Trigger status: PROBLEM
Trigger severity: Not classified",
      "status": "0",
      "retries": "3",
      "error": "",
      "esc_step": "1",
      "alerttype": "0",
      "p_eventid": "0",
      "acknowledgeid": "0"
    },    {
      "id": 1
    }
  ],  "id": 1}

See also
- Host
- MediaType
- User

Source
CAAlert::get() in frontends/php/include/classes/api/services/CAAlert.php.

**API info**

This class is designed to retrieve meta information about the API.

Available methods:
- **apiinfo.version** - retrieving the version of the Zabbix API

**apiinfo.version**

Description
string apiinfo.version(array)

This method allows to retrieve the version of the Zabbix API.

Parameters
Attention: This method is available to unauthenticated users and must be called without the auth parameter in the JSON-RPC request.

(array) The method accepts an empty array.

Return values

(string) Returns the version of the Zabbix API.

Note: Starting from Zabbix 2.0.4 the version of the API matches the version of Zabbix.

Examples

Retrieving the version of the API

Retrieve the version of the Zabbix API.

Request:

```
{
    "jsonrpc": "2.0",
    "method": "apiinfo.version",
    "params": [],
    "id": 1
}
```

Response:

```
{
    "jsonrpc": "2.0",
    "result": "4.0.0",
    "id": 1
}
```

Source

CAPIInfo::version() in frontends/php/include/classes/api/services/CAPIInfo.php.

Application

This class is designed to work with applications.

Object references:

- Application

Available methods:

- application.create - creating new applications
- application.delete - deleting applications
- application.get - retrieving application
- application.massadd - updating application
- application.update - adding items to applications

> Application object

The following objects are directly related to the application API.

Application

The application object has the following properties.


<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>applicationid</td>
<td>string (readonly)</td>
<td>ID of the application.</td>
</tr>
<tr>
<td>hostid</td>
<td>string</td>
<td>ID of the host that the application belongs to. Cannot be updated.</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>Name of the application.</td>
</tr>
<tr>
<td>flags</td>
<td>integer (readonly)</td>
<td>Origin of the application. Possible values: 0 - a plain application; 4 - a discovered application.</td>
</tr>
<tr>
<td>templateids</td>
<td>array</td>
<td>(readonly) IDs of the parent template applications.</td>
</tr>
</tbody>
</table>

**application.create**

Description

object application.create(object/array applications)

This method allows to create new applications.

Parameters

(object/array) Applications to create.

The method accepts applications with the standard application properties.

Return values

(object) Returns an object containing the IDs of the created applications under the applicationids property. The order of the returned IDs matches the order of the passed applications.

Examples

Creating an application

Create an application to store SNMP items.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "application.create",
    "params": {
        "name": "SNMP Items",
        "hostid": "10050"
    },
    "auth": "038e1d7b1735c6a5436ee9eae095079e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "applicationids": [    ```
application.delete

Description

object application.delete(array applicationIds)

This method allows to delete applications.

Parameters

(array) IDs of the applications to delete.

Return values

(object) Returns an object containing the IDs of the deleted applications under the applicationids property.

Examples

Deleting multiple applications

Delete two applications.

Request:

```json
{
  "jsonrpc": "2.0",
  "method": "application.delete",
  "params": [
    "356",
    "358"
  ],
  "auth": "3a57200802b24cda67c4e4010b50c065",
  "id": 1
}
```

Response:

```json
{
  "jsonrpc": "2.0",
  "result": {
    "applicationids": [
      "356",
      "358"
    ],
    "id": 1
  }
}
```

Source

CApplication::create() in frontends/php/include/classes/api/services/CApplication.php.

application.get

Description

integer/array application.get(object parameters)

The method allows to retrieve applications according to the given parameters.

Parameters
Parameters defining the desired output.

The method supports the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>applicationids</td>
<td>string/array</td>
<td>Return only applications with the given IDs.</td>
</tr>
<tr>
<td>groupids</td>
<td>string/array</td>
<td>Return only applications that belong to hosts from the given host groups.</td>
</tr>
<tr>
<td>hostids</td>
<td>string/array</td>
<td>Return only applications that belong to the given hosts.</td>
</tr>
<tr>
<td>inherited</td>
<td>boolean</td>
<td>If set to true return only applications inherited from a template.</td>
</tr>
<tr>
<td>itemids</td>
<td>string/array</td>
<td>Return only applications that contain the given items.</td>
</tr>
<tr>
<td>templated</td>
<td>boolean</td>
<td>If set to true return only applications that belong to templates.</td>
</tr>
<tr>
<td>templateids</td>
<td>string/array</td>
<td>Return only applications that belong to the given templates.</td>
</tr>
<tr>
<td>selectHost</td>
<td>query</td>
<td>Return the host that the application belongs to in the host property.</td>
</tr>
<tr>
<td>selectItems</td>
<td>query</td>
<td>Return the items contained in the application in the items property.</td>
</tr>
<tr>
<td>selectDiscoveryRule</td>
<td>query</td>
<td>Return the LLD rule that created the application in the discoveryRule property.</td>
</tr>
<tr>
<td>selectApplicationDiscovery</td>
<td>query</td>
<td>Return the application discovery object in the applicationDiscovery property.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Sort the result by the given properties. Possible values: applicationid and name.</td>
</tr>
<tr>
<td>countOutput</td>
<td>boolean</td>
<td>These parameters being common for all get methods are described in detail in the reference commentary page.</td>
</tr>
<tr>
<td>editable</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>excludeSearch</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>filter</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>limit</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>output</td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>preservekeys</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>search</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>searchByAny</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>searchWildcardsEnabled</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>sortorder</td>
<td>string/array</td>
<td></td>
</tr>
<tr>
<td>startSearch</td>
<td>boolean</td>
<td></td>
</tr>
</tbody>
</table>

Return values
(integer/array) Returns either:
- an array of objects;
- the count of retrieved objects, if the countOutput parameter has been used.

Examples
Retrieving applications from a host
Retrieve all applications from a host sorted by name.

Request:
```json
{
   "jsonrpc": "2.0",
   "method": "application.get",
   "params": {
      "output": "extend",
      "hostids": ["10001"],
      "sortfield": "name"
   },
   "auth": "038e1d7b1735c6a5436ee9eae096879e",
   "id": 1
}
```

Response:
```json
{
   "jsonrpc": "2.0",
   "result": [
   {
      "applicationid": "13",
      "hostid": "10001",
      "name": "CPU",
      "templateids": []
   }
```
See also

- Host
- Item

Source

CApplication::get() in frontends/php/include/classes/api/services/CApplication.php.

**application.massadd**

**Description**

Object application.massadd(object parameters)

This method allows to simultaneously add multiple items to the given applications.

**Parameters**

(object) Parameters containing the IDs of the applications to update and the items to add to the applications.

The method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>applications</td>
<td>array/object</td>
<td>Applications to be updated. The applications must have the applicationid property defined.</td>
</tr>
<tr>
<td></td>
<td>(required)</td>
<td></td>
</tr>
<tr>
<td>items</td>
<td>array/object</td>
<td>Items to add to the given applications. The items must have the itemid property defined.</td>
</tr>
</tbody>
</table>

**Return values**

(object) Returns an object containing the IDs of the updated applications under the applicationids property.
Examples

Adding items to multiple applications

Add the given items to two applications.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "application.massadd",
    "params": {
        "applications": [
            {
                "applicationid": "247"
            },
            {
                "applicationid": "246"
            }
        ],
        "items": [
            {
                "itemid": "22800"
            },
            {
                "itemid": "22801"
            }
        ]
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "applicationids": [
            "247",
            "246"
        ]
    },
    "id": 1
}
```

See also

- Item

Source

CApplication::massAdd() in frontends/php/include/classes/api/services/CApplication.php.

**application.update**

Description

object application.update(object/array applications)

This method allows to update existing applications.

Parameters

(object/array) Application properties to be updated.

The applicationid property must be defined for each application, all other properties are optional. Only the passed properties will be updated, all others will remain unchanged.

Return values
Returns an object containing the IDs of the updated applications under the `applicationids` property.

**Examples**

**Changing the name of an application**

Change the name of the application to "Processes and performance".

**Request:**

```json
{
    "jsonrpc": "2.0",
    "method": "application.update",
    "params": {
        "applicationid": "13",
        "name": "Processes and performance"
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

**Response:**

```json
{
    "jsonrpc": "2.0",
    "result": {
        "applicationids": [
            "13"
        ]
    },
    "id": 1
}
```

**Source**

CApplication::update() in frontends/php/include/classes/api/services/CApplication.php.

**Configuration**

This class is designed to export and import Zabbix configuration data.

**Available methods:**

- `configuration.export` - exporting the configuration
- `configuration.import` - importing the configuration

**configuration.export**

**Description**

string `configuration.export(object parameters)`

This method allows to export configuration data as a serialized string.

**Parameters**

- `(object) Parameters defining the objects to be exported and the format to use.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>format</code></td>
<td>string</td>
<td>Format in which the data must be exported.</td>
</tr>
<tr>
<td>(required)</td>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>json - JSON;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>xml - XML.</td>
</tr>
</tbody>
</table>

752
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>options</td>
<td>object</td>
<td>Objects to be exported.</td>
</tr>
</tbody>
</table>

The options object has the following parameters:
- groups - (array) IDs of host groups to export;
- hosts - (array) IDs of hosts to export;
- images - (array) IDs of images to export;
- maps - (array) IDs of maps to export;
- screens - (array) IDs of screens to export;
- templates - (array) IDs of templates to export;
- valueMaps - (array) IDs of value maps to export;

Return values

(string) Returns a serialized string containing the requested configuration data.

Examples

Exporting a template

Export the configuration of template "10571" as an XML string.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "configuration.export",
    "params": {
        "options": {
            "templates": [
                "10571"
            ]
        },
        "format": "xml"
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
```
Source
CConfiguration::export() in frontends/php/include/classes/api/services/CConfiguration.php.

configuration.import

Description

boolean configuration.import(object parameters)

This method allows to import configuration data from a serialized string.

Parameters

(object) Parameters containing the data to import and rules how the data should be handled.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>format</td>
<td>string</td>
<td>Format of the serialized string. Possible values: json - JSON; xml - XML.</td>
</tr>
<tr>
<td>source</td>
<td>string</td>
<td>Serialized string containing the configuration data.</td>
</tr>
<tr>
<td>rules</td>
<td>object</td>
<td>Rules on how new and existing objects should be imported. The rules parameter is described in detail in the table below.</td>
</tr>
</tbody>
</table>

Note:
If no rules are given, the configuration will not be updated.

The rules object supports the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>applications</td>
<td>object</td>
<td>Rules on how to import applications. Supported parameters: createMissing - (boolean) if set to true, new applications will be created; default: false; deleteMissing - (boolean) if set to true, applications not present in the imported data will be deleted from the database; default: false.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>discoveryRules</td>
<td>object</td>
<td>Rules on how to import LLD rules.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Supported parameters:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>createMissing - (boolean) if set to true, new LLD rules will be created; default: false;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>updateExisting - (boolean) if set to true, existing LLD rules will be updated; default: false;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>deleteMissing - (boolean) if set to true, LLD rules not present in the imported data will be deleted from the database; default: false.</td>
</tr>
<tr>
<td>graphs</td>
<td>object</td>
<td>Rules on how to import graphs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Supported parameters:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>createMissing - (boolean) if set to true, new graphs will be created; default: false;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>updateExisting - (boolean) if set to true, existing graphs will be updated; default: false;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>deleteMissing - (boolean) if set to true, graphs not present in the imported data will be deleted from the database; default: false.</td>
</tr>
<tr>
<td>groups</td>
<td>object</td>
<td>Rules on how to import host groups.</td>
</tr>
<tr>
<td>hosts</td>
<td>object</td>
<td>Rules on how to import hosts.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Supported parameters:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>createMissing - (boolean) if set to true, new hosts will be created; default: false;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>updateExisting - (boolean) if set to true, existing hosts will be updated; default: false.</td>
</tr>
<tr>
<td>httptests</td>
<td>object</td>
<td>Rules on how to import web scenarios.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Supported parameters:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>createMissing - (boolean) if set to true, new web scenarios will be created; default: false;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>updateExisting - (boolean) if set to true, existing web scenarios will be updated; default: false;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>deleteMissing - (boolean) if set to true, web scenarios not present in the imported data will be deleted from the database; default: false.</td>
</tr>
<tr>
<td>images</td>
<td>object</td>
<td>Rules on how to import images.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Supported parameters:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>createMissing - (boolean) if set to true, new images will be created; default: false;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>updateExisting - (boolean) if set to true, existing images will be updated; default: false.</td>
</tr>
<tr>
<td>items</td>
<td>object</td>
<td>Rules on how to import items.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Supported parameters:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>createMissing - (boolean) if set to true, new items will be created; default: false;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>updateExisting - (boolean) if set to true, existing items will be updated; default: false;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>deleteMissing - (boolean) if set to true, items not present in the imported data will be deleted from the database; default: false.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>--------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| maps          | object | Rules on how to import maps.  
|               |        | Supported parameters:    
|               |        | createMissing - (boolean) if set to true, new maps will be created; default: false;    
|               |        | updateExisting - (boolean) if set to true, existing maps will be updated; default: false. |
| screens       | object | Rules on how to import screens.  
|               |        | Supported parameters:    
|               |        | createMissing - (boolean) if set to true, new screens will be created; default: false;    
|               |        | updateExisting - (boolean) if set to true, existing screens will be updated; default: false. |
| templateLinkage | object | Rules on how to import template links.  
|               |        | Supported parameters:    
|               |        | createMissing - (boolean) if set to true, new links between templates and host will be created; default: false;    
|               |        | deleteMissing - (boolean) if set to true, template links not present in the imported data will be deleted from the database; default: false. |
| templates     | object | Rules on how to import templates.  
|               |        | Supported parameters:    
|               |        | createMissing - (boolean) if set to true, new templates will be created; default: false;    
|               |        | updateExisting - (boolean) if set to true, existing templates will be updated; default: false. |
| templateScreens | object | Rules on how to import template screens.  
|               |        | Supported parameters:    
|               |        | createMissing - (boolean) if set to true, new template screens will be created; default: false;    
|               |        | updateExisting - (boolean) if set to true, existing template screens will be updated; default: false;    
|               |        | deleteMissing - (boolean) if set to true, template screens not present in the imported data will be deleted from the database; default: false. |
| triggers      | object | Rules on how to import triggers.  
|               |        | Supported parameters:    
|               |        | createMissing - (boolean) if set to true, new triggers will be created; default: false;    
|               |        | updateExisting - (boolean) if set to true, existing triggers will be updated; default: false;    
|               |        | deleteMissing - (boolean) if set to true, triggers not present in the imported data will be deleted from the database; default: false. |
| valueMaps     | object | Rules on how to import value maps.  
|               |        | Supported parameters:    
|               |        | createMissing - (boolean) if set to true, new value maps will be created; default: false;    
|               |        | updateExisting - (boolean) if set to true, existing value maps will be updated; default: false. |

Return values
(boolean) Returns true if importing has been successful.

Examples

Importing a template

Import the template configuration contained in the XML string. If any items or triggers in the XML string are missing, they will be deleted from the database, and everything else will be left unchanged.

Request:

```json
{  "jsonrpc": "2.0",  "method": "configuration.import",  "params": {    "format": "xml",    "rules": {      "applications": {        "createMissing": true      },      "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>4.0</version><date>2020-01-01T12:00:00Z</date><groups><group><name>Templates</name></group></groups><hosts><host><name>host1</name><items><item><application>app1</application><value>123</value><status>0</status><uptime: (.*)&lt;/dt&gt;\</item></items><triggers><trigger><eventSource>host1</eventSource><description>Trigger description</description><eventID>123</eventID><priority>1</priority><message>Trigger message</message></trigger></triggers><valueMaps><valueMap><value>1</value><newvalue>Available</newvalue></valueMap></valueMaps><jmx_endpoint/><timeout>3s</timeout><url/><query_fields/><posts/><status_codes>200</status_codes><mapping><value>1</value><newvalue>Available</newvalue></mapping></mappings></zabbix_export>\n</xml>"  },  "auth": "038e1d7b1735c6a5436ee9eae096879e",  "id": 1}
```

Response:

```json
{  "jsonrpc": "2.0",  "result": true,  "id": 1}
```

Source

CConfiguration::import() in frontends/php/include/classes/api/services/CConfiguration.php.

**Correlation**

This class is designed to work with correlations.

Object references:

- Correlation

Available methods:
• `correlation.create` - creating new correlations
• `correlation.delete` - deleting correlations
• `correlation.get` - retrieving correlations
• `correlation.update` - updating correlations

> **Correlation object**

The following objects are directly related to the correlation API.

**Correlation**

The correlation object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>correlationid</td>
<td>string</td>
<td>(readonly) ID of the correlation.</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>Name of the correlation.</td>
</tr>
<tr>
<td>description</td>
<td>string</td>
<td>Description of the correlation.</td>
</tr>
<tr>
<td>status</td>
<td>integer</td>
<td>Whether the correlation is enabled or disabled. Possible values are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - (default) enabled; 1 - disabled.</td>
</tr>
</tbody>
</table>

Note that for some methods (update, delete) the required/optional parameter combination is different.

**Correlation operation**

The correlation operation object defines an operation that will be performed when a correlation is executed. It has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>integer</td>
<td>Type of operation. Possible values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - close old events; 1 - close new event.</td>
</tr>
</tbody>
</table>

**Correlation filter**

The correlation filter object defines a set of conditions that must be met to perform the configured correlation operations. It has the following properties.
<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>evaltype</strong></td>
<td>integer</td>
<td>(required) Filter condition evaluation method. Possible values: 0 - and/or; 1 - and; 2 - or; 3 - custom expression.</td>
</tr>
<tr>
<td><strong>conditions</strong></td>
<td>array</td>
<td>(required) Set of filter conditions to use for filtering results. (readonly) Generated expression that will be used for evaluating filter conditions. The expression contains IDs that reference specific filter conditions by its formulaid. The value of <code>eval_formula</code> is equal to the value of <code>formula</code> for filters with a custom expression.</td>
</tr>
<tr>
<td><strong>eval_formula</strong></td>
<td>string</td>
<td>(readonly) Generated expression that will be used for evaluating filter conditions. The expression contains IDs that reference specific filter conditions by its formulaid. The value of <code>eval_formula</code> is equal to the value of <code>formula</code> for filters with a custom expression.</td>
</tr>
<tr>
<td><strong>formula</strong></td>
<td>string</td>
<td>User-defined expression to be used for evaluating conditions of filters with a custom expression. The expression must contain IDs that reference specific filter conditions by its formulaid. The IDs used in the expression must exactly match the ones defined in the filter conditions: no condition can remain unused or omitted. Required for custom expression filters.</td>
</tr>
</tbody>
</table>
Correlation filter condition

The correlation filter condition object defines a specific condition that must be checked before running the correlation operations.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>integer</td>
<td>Type of condition. Possible values: 0 - old event tag; 1 - new event tag; 2 - new event host group; 3 - event tag pair; 4 - old event tag value; 5 - new event tag value.</td>
</tr>
<tr>
<td>tag</td>
<td>string</td>
<td>Event tag (old or new). Required when type of condition is: 0, 1, 4, 5.</td>
</tr>
<tr>
<td>groupid</td>
<td>string</td>
<td>Host group ID. Required when type of condition is: 2.</td>
</tr>
<tr>
<td>oldtag</td>
<td>string</td>
<td>Old event tag. Required when type of condition is: 3.</td>
</tr>
<tr>
<td>newtag</td>
<td>string</td>
<td>New event tag. Required when type of condition is: 3.</td>
</tr>
<tr>
<td>value</td>
<td>string</td>
<td>Event tag (old or new) value. Required when type of condition is: 4, 5.</td>
</tr>
<tr>
<td>formulaid</td>
<td>string</td>
<td>Arbitrary unique ID that is used to reference the condition from a custom expression. Can only contain capital-case letters. The ID must be defined by the user when modifying filter conditions, but will be generated anew when requesting them afterward.</td>
</tr>
<tr>
<td>operator</td>
<td>integer</td>
<td>Condition operator. Required when type of condition is: 2, 4, 5.</td>
</tr>
</tbody>
</table>
The following operators and values are supported for each condition type.

<table>
<thead>
<tr>
<th>Condition</th>
<th>Condition name</th>
<th>Supported operators</th>
<th>Expected value</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Host group</td>
<td>=, &lt;&gt;</td>
<td>Host group ID.</td>
</tr>
<tr>
<td>4</td>
<td>Old event tag value</td>
<td>=, &lt;&gt;, like, not like</td>
<td>string</td>
</tr>
<tr>
<td>5</td>
<td>New event tag value</td>
<td>=, &lt;&gt;, like, not like</td>
<td>string</td>
</tr>
</tbody>
</table>

**correlation.create**

**Description**

object correlation.create(object/array correlations)

This method allows to create new correlations.

**Parameters**

(object/array) Correlations to create.

Additionally to the [standard correlation properties](#), the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>operations</td>
<td>array</td>
<td>Correlation operations to create for the correlation.</td>
</tr>
<tr>
<td>(required)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>filter</td>
<td>object</td>
<td>Correlation filter object for the correlation.</td>
</tr>
<tr>
<td>(required)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Return values**

(object) Returns an object containing the IDs of the created correlations under the correlationids property. The order of the returned IDs matches the order of the passed correlations.

**Examples**

Create a new event tag correlation

Create a correlation using evaluation method AND/OR with one condition and one operation. By default the correlation will be enabled.

**Request:**

```json
{
  "jsonrpc": "2.0",
  "method": "correlation.create",
  "params": {
    "name": "new event tag correlation",
    "filter": {
      "evaltype": 0,
      "conditions": [
        {
          "type": 1,
          "tag": "ok"
        }
      ]
    },
    "operations": [
      {
```
Using a custom expression filter

Create a correlation that will use a custom filter condition. The formula IDs "A" or "B" have been chosen arbitrarily. Condition type will be "Host group" with operator "<>".

Request:

```json
{
    "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
        }
    ],
    "auth": "343baad4f88b4106b9b5961e77437688",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "correlationids": [
        762
    ]
}
```
correlation.delete

Description

object correlation.delete(array correlationids)

This method allows to delete correlations.

Parameters

(array) IDs of the correlations to delete.

Return values

(object) Returns an object containing the IDs of the deleted correlations under the correlationids property.

Example

Delete multiple correlations

Delete two correlations.

Request:

```
{
    "jsonrpc": "2.0",
    "method": "correlation.delete",
    "params": [
        "1",
        "2"
    ],
    "auth": "343baad4f88b4106b9b5961e77437688",
    "id": 1
}
```

Response:

```
{
    "jsonrpc": "2.0",
    "result": {
        "correlationids": [
            "1",
            "2"
        ],
        "id": 1
    }
}
```

Source

CCorrelation::delete() in frontends/php/include/classes/api/services/CCorrelation.php.

correlation.get

Description
integer/array correlation.get(object parameters)

The method allows to retrieve correlations according to the given parameters.

Parameters

(object) Parameters defining the desired output.

The method supports the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>correlationids</td>
<td>string/array</td>
<td>Return only correlations with the given IDs.</td>
</tr>
<tr>
<td>selectFilter</td>
<td>query</td>
<td>Returns the correlation filter in the filter property.</td>
</tr>
<tr>
<td>selectOperations</td>
<td>query</td>
<td>Return correlation operations in the operations property.</td>
</tr>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Sort the result by the given properties.</td>
</tr>
<tr>
<td>countOutput</td>
<td>boolean</td>
<td>These parameters being common for all get methods are described in the reference commentary.</td>
</tr>
<tr>
<td>editable</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>excludeSearch</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>filter</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>limit</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>output</td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>preservekeys</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>search</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>searchByAny</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>searchWildcards</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>sortOrder</td>
<td>string/array</td>
<td></td>
</tr>
<tr>
<td>startSearch</td>
<td>boolean</td>
<td></td>
</tr>
</tbody>
</table>

Return values

(integer/array) Returns either:

- an array of objects;
- the count of retrieved objects, if the countOutput parameter has been used.

Examples

Retrieve correlations

Retrieve all configured correlations together with correlation conditions and operations. The filter uses the “and/or” evaluation type, so the formula property is empty and eval_formula is generated automatically.

Request:

```javascript
{
    "jsonrpc": "2.0",
    [code]
}
"method": "correlation.get",
"params": {
    "output": "extend",
    "selectOperations": "extend",
    "selectFilter": "extend"
},
"auth": "343baad4f88b4106b9b5961e77437688",
"id": 1
}

Response:
{
    "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
        }
    ],
    "id": 1
}

See also
- Correlation filter
- Correlation operation

Source
CCorrelation::get() in frontends/php/include/classes/api/services/CCorrelation.php.

**correlation.update**

Description

object correlation.update(object/array correlations)

This method allows to update existing correlations.

Parameters

(object/array) Correlation properties to be updated.

The **correlationid** property must be defined for each correlation, all other properties are optional. Only the passed properties will be updated, all others will remain unchanged.

Additionally to the **standard correlation properties**, the method accepts the following parameters.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter</td>
<td>object</td>
<td>Correlation filter object to replace the current filter.</td>
</tr>
<tr>
<td>operations</td>
<td>array</td>
<td>Correlation operations to replace existing operations.</td>
</tr>
</tbody>
</table>

Return values

(object) Returns an object containing the IDs of the updated correlations under the correlationids property.

Examples

Disable correlation

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "correlation.update",
    "params": {
        "correlationid": "1",
        "status": "1"
    },
    "auth": "343baad4f88b4106b9b5961e77437688",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "correlationids": [
            "1"
        ],
        "id": 1
    }
}
```

Replace conditions, but keep the evaluation method

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "correlation.update",
    "params": {
        "correlationid": "1",
        "filter": {
            "conditions": [
                {
                    "type": 3,
                    "oldtag": "error",
                    "newtag": "ok"
                }
            ],
        },
        "auth": "343baad4f88b4106b9b5961e77437688",
        "id": 1
    }
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "correlationids": [
            "1"
        ],
        "id": 1
    }
}
```
Dashboard

This class is designed to work with dashboards.

Object references:

- Dashboard
- Dashboard widget
- Dashboard widget field
- Dashboard user group
- Dashboard user

Available methods:

- dashboard.create - creating new dashboards
- dashboard.delete - deleting dashboards
- dashboard.get - retrieving dashboards
- dashboard.update - updating dashboards

> Dashboard object

The following objects are directly related to the dashboard API.

Dashboard

The dashboard object has the following properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dashboardid</td>
<td>string</td>
<td>(readonly) ID of the dashboard.</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>Name of the dashboard.</td>
</tr>
<tr>
<td>(required)</td>
<td></td>
<td>Name of the dashboard.</td>
</tr>
<tr>
<td>userid</td>
<td>string</td>
<td>Dashboard owner user ID.</td>
</tr>
<tr>
<td>private</td>
<td>integer</td>
<td>Type of dashboard sharing.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - public dashboard;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - (default) private dashboard.</td>
</tr>
</tbody>
</table>

Note that for some methods (update, delete) the required/optional parameter combination is different.

Dashboard widget

The dashboard widget object has the following properties:
<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>widgetid</td>
<td>string (readonly)</td>
<td>ID of the dashboard widget.</td>
</tr>
<tr>
<td>type</td>
<td>string</td>
<td>Type of the dashboard widget.</td>
</tr>
<tr>
<td></td>
<td>(required)</td>
<td></td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>Custom widget name.</td>
</tr>
<tr>
<td>x</td>
<td>integer</td>
<td>A horizontal position from the left side of the dashboard.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Valid values range from 0 to 11.</td>
</tr>
<tr>
<td>y</td>
<td>integer</td>
<td>A vertical position from the top of the dashboard.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Valid values range from 0 to 62.</td>
</tr>
</tbody>
</table>

Possible values:
- actionlog - Action log;
- clock - Clock;
- dataover - Data overview;
- discovery - Discovery status;
- favgraphs - Favorite graphs;
- favmaps - Favorite maps;
- favscreens - Favorite screens;
- graph - Graph (classic);
- problemhosts - Problem hosts;
- map - Map;
- navtree - Map Navigation Tree;
- plaintext - Plain text;
- problems - Problems;
- svggraph - Graph;
- systeminfo - System information;
- problemsbysv - Problems by severity;
- trigover - Trigger overview;
- url - URL;
- web - Web monitoring;
- monitoring;
<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>width</td>
<td>integer</td>
<td>The widget width.</td>
</tr>
<tr>
<td>height</td>
<td>integer</td>
<td>Valid values range from 1 to 12. The widget height.</td>
</tr>
<tr>
<td>fields</td>
<td>array</td>
<td>Valid values range from 2 to 32. Array of the dashboard widget field objects.</td>
</tr>
</tbody>
</table>

**Dashboard widget field**

The dashboard widget field object has the following properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>integer</td>
<td>Type of the widget field.</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>Widget field name.</td>
</tr>
<tr>
<td>value</td>
<td>mixed</td>
<td>Widget field value depending of type.</td>
</tr>
</tbody>
</table>

**Dashboard user group**

List of dashboard permissions based on user groups. It has the following properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>usgrpid</td>
<td>string</td>
<td>User group ID.</td>
</tr>
<tr>
<td>permission</td>
<td>integer</td>
<td>Type of permission level.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 - read only;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 - read-write;</td>
</tr>
</tbody>
</table>

**Dashboard user**

List of dashboard permissions based on users. It has the following properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>userid</td>
<td>string</td>
<td>User ID.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>permission</td>
<td>integer</td>
<td>Type of permission level. Possible values: 2 - read only; 3 - read-write;</td>
</tr>
</tbody>
</table>

**dashboard.create**

Description

object dashboard.create(object/array dashboards)

This method allows to create new dashboards.

Parameters

(object/array) Dashboards to create.

Additionally to the standard dashboard properties, the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>widgets</td>
<td>array</td>
<td>Dashboard widgets to be created for the dashboard.</td>
</tr>
<tr>
<td>users</td>
<td>array</td>
<td>Dashboard user shares to be created on the dashboard.</td>
</tr>
<tr>
<td>userGroups</td>
<td>array</td>
<td>Dashboard user group shares to be created on the dashboard.</td>
</tr>
</tbody>
</table>

Return values

(object) Returns an object containing the IDs of the created dashboards under the dashboardids property. The order of the returned IDs matches the order of the passed dashboards.

Examples

Creating a dashboard

Create a dashboard named "My dashboard" with one Problems widget with tags and using two types of sharing (user group and user).

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "dashboard.create",
    "params": {
        "name": "My dashboard",
        "widgets": [
            {
                "type": "problems",
                "x": 0,
                "y": 0,
                "width": 6,
                "height": 5,
                "fields": [
                    {
                        "type": 1,
                        "tag": "example"
                    }
                ]
            }
        ]
    }
}
```
"name": "tags.tag.0",
"value": "service"
},
{
"type": 0,
"name": "tags.operator.0",
"value": 1
},
{
"type": 1,
"name": "tags.value.0",
"value": "zabbix_server"
}
]
],
"userGroups": [
{
"usrgrpid": "7",
"permission": "2"
}
],
"users": [
{
"userid": "4",
"permission": "3"
}
],
"auth": "038e1d7b1735c6a5436ee9eae095879e",
"id": 1
}

Response:
{
"jsonrpc": "2.0",
"result": {
"dashboardids": [
"2"
],
"id": 1
}
}

See also
- Dashboard widget
- Dashboard widget field
- Dashboard user
- Dashboard user group

Source
CDashboard::create() in frontends/php/include/classes/api/services/CDashboard.php.

dashboard.delete

Description
object dashboard.delete(array dashboardids)

This method allows to delete dashboards.

Parameters
(array) IDs of the dashboards to delete.
Return values

(object) Returns an object containing the IDs of the deleted dashboards under the dashboardids property.

Examples

Deleting multiple dashboards

Delete two dashboards.

Request:

```
{
    "jsonrpc": "2.0",
    "method": "dashboard.delete",
    "params": [
        "2",
        "3"
    ],
    "auth": "3a57200802b24cda67c4e4010b50c065",
    "id": 1
}
```

Response:

```
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "2",
            "3"
        ]
    },
    "id": 1
}
```

Source

CDashboard::delete() in frontends/php/include/classes/api/services/CDashboard.php.

dashboard.get

description

integer/array dashboard.get(object parameters)

The method allows to retrieve dashboards according to the given parameters.

Parameters

(object) Parameters defining the desired output.

The method supports the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dashboardids</td>
<td>string/array</td>
<td>Return only dashboards with the given IDs.</td>
</tr>
<tr>
<td>selectWidgets</td>
<td>query</td>
<td>Return the dashboard widgets that are used in the dashboard with in widgets property.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>selectUsers</td>
<td>query</td>
<td>Returns users that the dashboard is shared with in users property.</td>
</tr>
<tr>
<td>selectUserGroups</td>
<td>query</td>
<td>Returns user groups that the dashboard is shared with in userGroups property.</td>
</tr>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Sort the result by the given properties.</td>
</tr>
<tr>
<td>countOutput</td>
<td>boolean</td>
<td>These parameters being common for all get methods are described in detail in the reference commentary page.</td>
</tr>
</tbody>
</table>

Return values
(integer/array) Returns either:
- an array of objects;
- the count of retrieved objects, if the countOutput parameter has been used.

Examples
Retrieving a dashboard by ID
Retrieve all data about dashboards "1" and "2".

Request:
```json
{
    "jsonrpc": "2.0",
    "method": "dashboard.get",
    "params": {
        "output": "extend",
        "selectWidgets": "extend",
        "selectUsers": "extend",
        "selectUserGroups": "extend",
        "dashboardids": ["1", "2"
    ]
}
```
Response:

```json
{
    "jsonrpc": "2.0",
    "result": [
        {
            "dashboardid": "1",
            "name": "Dashboard",
            "userid": "1",
            "private": "0",
            "users": [],
            "userGroups": [],
            "widgets": [
                {
                    "widgetid": "9",
                    "type": "systeminfo",
                    "name": "",
                    "x": "6",
                    "y": "8",
                    "width": "6",
                    "height": "5",
                    "fields": []
                },
                {
                    "widgetid": "8",
                    "type": "problemsbysv",
                    "name": "",
                    "x": "6",
                    "y": "4",
                    "width": "6",
                    "height": "4",
                    "fields": []
                },
                {
                    "widgetid": "7",
                    "type": "problemhosts",
                    "name": "",
                    "x": "6",
                    "y": "0",
                    "width": "6",
                    "height": "4",
                    "fields": []
                },
                {
                    "widgetid": "6",
                    "type": "discovery",
                    "name": "",
                    "x": "3",
                    "y": "9",
                    "width": "3",
                    "height": "4",
                    "fields": []
                },
                {
                    "widgetid": "5",
                    "type": "web",
                    "name": "",
                    "x": "0",
                    "y": "10",
                    "width": "6",
                    "height": "5",
                    "fields": []
                }
            ]
        }
    ]
}
```
"y": "9",
"width": "3",
"height": "4",
"fields": []
},
{
"widgetid": "4",
"type": "problems",
"name": "",
"x": "0",
"y": "3",
"width": "6",
"height": "6",
"fields": []
},
{
"widgetid": "3",
"type": "favmaps",
"name": "",
"x": "4",
"y": "0",
"width": "2",
"height": "3",
"fields": []
},
{
"widgetid": "2",
"type": "favscreens",
"name": "",
"x": "2",
"y": "0",
"width": "2",
"height": "3",
"fields": []
},
{
"widgetid": "1",
"type": "favgraphs",
"name": "",
"x": "0",
"y": "0",
"width": "2",
"height": "3",
"fields": []
}
],
{
"dashboardid": "2",
"name": "My dashboard",
"userid": "1",
"private": "1",
"users": [
{
"userid": "4",
"permission": "3"
}
],
"userGroups": [
{
"usrgrpid": "7",
"permission": "2"
}
See also

- Dashboard widget
- Dashboard widget field
- Dashboard user
- Dashboard user group

Source

CDashboard::get() in frontends/php/include/classes/api/services/CDashboard.php.

dashboard.update

description

object dashboard.update(object/array dashboards)

This method allows to update existing dashboards.

Parameters

(object/array) Dashboard properties to be updated.

The dashboardid property must be defined for each dashboard, all other properties are optional. Only the passed properties will be updated, all others will remain unchanged.

Additionally to the standard dashboard properties, the method accepts the following parameters.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>widgets</td>
<td>array</td>
<td>Dashboard widgets to replace existing dashboard widgets.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dashboard widgets are updated by widgetid property. Widgets without widgetid property will be created.</td>
</tr>
<tr>
<td>users</td>
<td>array</td>
<td>Dashboard user shares to replace the existing elements.</td>
</tr>
<tr>
<td>userGroups</td>
<td>array</td>
<td>Dashboard user group shares to replace the existing elements.</td>
</tr>
</tbody>
</table>

Return values

(object) Returns an object containing the IDs of the updated dashboards under the dashboardids property.

Examples

Renaming a dashboard

Rename a dashboard to "SQL server status".

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "dashboard.update",
    "params": {
        "dashboardid": "2",
        "name": "SQL server status"
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "dashboardids": [
            "2"
        ]
    },
    "id": 1
}
```

Change dashboard owner

Available only for admins and super admins.

Request:
See also

- Dashboard widget
- Dashboard widget field
- Dashboard user
- Dashboard user group

Source

CDashboard::update() in frontends/php/include/classes/api/services/CDashboard.php.

**Discovered host**

This class is designed to work with discovered hosts.

Object references:

- Discovered host

Available methods:

- dhost.get - retrieve discovered hosts

> **Discovered host object**

The following objects are directly related to the dhost API.

**Discovered host**

The discovered host object contains information about a host discovered by a network discovery rule. It has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhostid</td>
<td>string</td>
<td>ID of the discovered host.</td>
</tr>
<tr>
<td>druleid</td>
<td>string</td>
<td>ID of the discovery rule that detected the host.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>lastdown</td>
<td>timestamp</td>
<td>Time when the discovered host last went down.</td>
</tr>
<tr>
<td>lastup</td>
<td>timestamp</td>
<td>Time when the discovered host last went up.</td>
</tr>
<tr>
<td>status</td>
<td>integer</td>
<td>Whether the discovered host is up or down. A host is up if it has at least one active discovered service. Possible values: 0 - host up; 1 - host down.</td>
</tr>
</tbody>
</table>

**dhost.get**

Description

```dhost.get(object parameters)```

The method allows to retrieve discovered hosts according to the given parameters.

Parameters

(object) Parameters defining the desired output.

The method supports the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhostids</td>
<td>string/array</td>
<td>Return only discovered hosts with the given IDs.</td>
</tr>
<tr>
<td>druleids</td>
<td>string/array</td>
<td>Return only discovered hosts that have been created by the given discovery rules.</td>
</tr>
<tr>
<td>dserviceids</td>
<td>string/array</td>
<td>Return only discovered hosts that are running the given services.</td>
</tr>
<tr>
<td>selectDRules</td>
<td>query</td>
<td>Return the discovery rule that detected the host as an array in the drules property.</td>
</tr>
<tr>
<td>selectDServices</td>
<td>query</td>
<td>Return the discovered services running on the host in the dservices property.</td>
</tr>
</tbody>
</table>

Supports `count`.
### Parameter Descriptions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>limitSelects</td>
<td>integer</td>
<td>Limits the number of records returned by subselects.</td>
</tr>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Applies to the following subselects: <code>selectDServices</code>. Results will be sorted by <code>dserviceid</code>.</td>
</tr>
<tr>
<td>countOutput</td>
<td>boolean</td>
<td>Sort the result by the given properties.</td>
</tr>
<tr>
<td>editable</td>
<td>boolean</td>
<td>Possible values are: <code>dhostid</code> and <code>druleid</code>. These parameters being common for all get methods are described in detail in the reference commentary.</td>
</tr>
<tr>
<td>excludeSearch</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>filter</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>limit</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>output</td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>preservekeys</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>search</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>searchByAny</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>searchWildcardsEnabled</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>sortOrder</td>
<td>string/array</td>
<td></td>
</tr>
<tr>
<td>startSearch</td>
<td>boolean</td>
<td></td>
</tr>
</tbody>
</table>

#### Return Values

(integer/array) Returns either:

- an array of objects;
- the count of retrieved objects, if the `countOutput` parameter has been used.

#### Examples

**Retrieve discovered hosts by discovery rule**

Retrieve all hosts and the discovered services they are running that have been detected by discovery rule "4".

**Request:**

```json
{
  "jsonrpc": "2.0",
  "method": "dhost.get",
  "params": {
    "output": "extend",
    "selectDServices": "extend",
    "druleids": "4"
  },
  "auth": "038e1d7b1735c6a5436ee9eae095879e",
  "id": 1
}
```
Response:

{
  "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"
      }
    ],
    "dhostid": "3",
    "druleid": "4",
    "status": "0",
    "lastup": "1337697234",
    "lastdown": "0"
  }
]
See also

- Discovered service
- Discovery rule

Source

CDHost::get() in frontends/php/include/classes/api/services/CDHost.php.

Discovered service

This class is designed to work with discovered services.

Object references:

- Discovered service

Available methods:

- dservice.get - retrieve discovered services

> Discovered service object

The following objects are directly related to the dservice API.
The discovered service object contains information about a service discovered by a network discovery rule on a host. It has the following properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dserviceid</td>
<td>string</td>
<td>ID of the discovered service.</td>
</tr>
<tr>
<td>dcheckid</td>
<td>string</td>
<td>ID of the discovery check used to detect the service.</td>
</tr>
<tr>
<td>dhostid</td>
<td>string</td>
<td>ID of the discovered host running the service.</td>
</tr>
<tr>
<td>dns</td>
<td>string</td>
<td>DNS of the host running the service.</td>
</tr>
<tr>
<td>ip</td>
<td>string</td>
<td>IP address of the host running the service.</td>
</tr>
<tr>
<td>lastdown</td>
<td>timestamp</td>
<td>Time when the discovered service last went down.</td>
</tr>
<tr>
<td>lastup</td>
<td>timestamp</td>
<td>Time when the discovered service last went up.</td>
</tr>
<tr>
<td>port</td>
<td>integer</td>
<td>Service port number.</td>
</tr>
<tr>
<td>status</td>
<td>integer</td>
<td>Status of the service.</td>
</tr>
<tr>
<td>value</td>
<td>string</td>
<td>Value returned by the service when performing a Zabbix agent, SNMPv1, SNMPv2 or SNMPv3 discovery check.</td>
</tr>
</tbody>
</table>

**dservice.get**

**Description**

integer/array dservice.get(object parameters)

The method allows to retrieve discovered services according to the given parameters.

**Parameters**

(object) Parameters defining the desired output.

The method supports the following parameters.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dserviceids</td>
<td>string/array</td>
<td>Return only discovered services with the given IDs.</td>
</tr>
<tr>
<td>dhostids</td>
<td>string/array</td>
<td>Return only discovered services that belong to the given discovered hosts.</td>
</tr>
<tr>
<td>dcheckids</td>
<td>string/array</td>
<td>Return only discovered services that have been detected by the given discovery checks.</td>
</tr>
<tr>
<td>druleids</td>
<td>string/array</td>
<td>Return only discovered services that have been detected by the given discovery rules.</td>
</tr>
<tr>
<td>selectDRules</td>
<td>query</td>
<td>Return the discovery rule that detected the service as an array in the drules property.</td>
</tr>
<tr>
<td>selectDHosts</td>
<td>query</td>
<td>Return the discovered host that service belongs to as an array in the dhosts property.</td>
</tr>
<tr>
<td>selectHosts</td>
<td>query</td>
<td>Return the hosts with the same IP address and proxy as the service in the hosts property.</td>
</tr>
<tr>
<td>limitSelects</td>
<td>integer</td>
<td>Limits the number of records returned by subselects.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Applies to the following subselects: selectHosts - result will be sorted by hostid.</td>
</tr>
</tbody>
</table>
### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Sort the result by the given properties. Possible values are: dserviceid, dhostid and ip. These parameters being common for all get methods are described in detail in the reference commentary.</td>
</tr>
<tr>
<td>countOutput</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>editable</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>excludeSearch</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>filter</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>limit</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>output</td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>preservekeys</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>search</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>searchByAny</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>searchWildcards</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>sortorder</td>
<td>string/array</td>
<td></td>
</tr>
<tr>
<td>startSearch</td>
<td>boolean</td>
<td></td>
</tr>
</tbody>
</table>

### Return values

(integer/array) Returns either:

- an array of objects;
- the count of retrieved objects, if the countOutput parameter has been used.

### Examples

#### Retrieve services discovered on a host

Retrieve all discovered services detected on discovered host "11".

**Request:**

```json
{
    "jsonrpc": "2.0",
    "method": "dservice.get",
    "params": {
        "output": "extend",
        "dhostids": "11"
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

**Response:**

```json
{
    "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
}

See also

- Discovered host
- Discovery check
- Host

Source

CDService::get() in frontends/php/include/classes/api/services/CDService.php.

Discovery check

This class is designed to work with discovery checks.

Object references:

- Discovery check

Available methods:

- dcheck.get - retrieve discovery checks

> Discovery check object

The following objects are directly related to the dcheck API.

Discovery check

The discovery check object defines a specific check performed by a network discovery rule. It has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dcheckid</td>
<td>string</td>
<td>(readonly) ID of the discovery check.</td>
</tr>
<tr>
<td>druleid</td>
<td>string</td>
<td>(readonly) ID of the discovery rule that the check belongs to.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>key_</td>
<td>string</td>
<td>The value of this property differs depending on the type of the check: - key to query for Zabbix agent checks, required; - SNMP OID for SNMPv1, SNMPv2 and SNMPv3 checks, required.</td>
</tr>
<tr>
<td>ports</td>
<td>string</td>
<td>One or several port ranges to check separated by commas. Used for all checks except for ICMP. Default: 0.</td>
</tr>
<tr>
<td>snmp_community</td>
<td>string</td>
<td>SNMP community. Required for SNMPv1 and SNMPv2 agent checks.</td>
</tr>
<tr>
<td>snmpv3_authpasswd</td>
<td>string</td>
<td>Auth passphrase used for SNMPv3 agent checks with security level set to authNoPriv or authPriv.</td>
</tr>
<tr>
<td>snmpv3_authprotocol</td>
<td>integer</td>
<td>Authentication protocol used for SNMPv3 agent checks with security level set to authNoPriv or authPriv. Possible values: 0 - (default) MD5; 1 - SHA.</td>
</tr>
<tr>
<td>snmpv3_context</td>
<td>string</td>
<td>SNMPv3 context name. Used only by SNMPv3 checks.</td>
</tr>
<tr>
<td>snmpv3_privpasswd</td>
<td>string</td>
<td>Priv passphrase used for SNMPv3 agent checks with security level set to authPriv.</td>
</tr>
<tr>
<td>snmpv3_privprotocol</td>
<td>integer</td>
<td>Privacy protocol used for SNMPv3 agent checks with security level set to authPriv. Possible values: 0 - (default) DES; 1 - AES.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>snmpv3_securitylevel</td>
<td>string</td>
<td>Security level used for SNMPv3 agent checks.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values: 0 - noAuthNoPriv; 1 - authNoPriv; 2 - authPriv.</td>
</tr>
<tr>
<td>snmpv3_securityname</td>
<td>string</td>
<td>Security name used for SNMPv3 agent checks.</td>
</tr>
<tr>
<td>type</td>
<td>integer</td>
<td>Type of check.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values: 0 - SSH; 1 - LDAP; 2 - SMTP; 3 - FTP; 4 - HTTP; 5 - POP;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6 - NNTP; 7 - IMAP; 8 - TCP; 9 - Zabbix agent; 10 - SNMPv1 agent; 11 -</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SNMPv2 agent; 12 - ICMP ping; 13 - SNMPv3 agent; 14 - HTTPS; 15 - Telnet.</td>
</tr>
<tr>
<td>uniq</td>
<td>integer</td>
<td>Whether to use this check as a device uniqueness criteria. Only a single</td>
</tr>
<tr>
<td></td>
<td></td>
<td>unique check can be configured for a discovery rule. Used for Zabbix agent,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SNMPv1, SNMPv2 and SNMPv3 agent checks.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values: 0 - (default) do not use this check as a uniqueness</td>
</tr>
<tr>
<td></td>
<td></td>
<td>criteria; 1 - use this check as a uniqueness criteria.</td>
</tr>
</tbody>
</table>

**dcheck.get**

Description
integer/array dcheck.get(object parameters)

The method allows to retrieve discovery checks according to the given parameters.

Parameters

(object) Parameters defining the desired output.

The method supports the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dcheckids</td>
<td>string/array</td>
<td>Return only discovery checks with the given IDs.</td>
</tr>
<tr>
<td>druleids</td>
<td>string/array</td>
<td>Return only discovery checks that belong to the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>given discovery rules.</td>
</tr>
<tr>
<td>dserviceids</td>
<td>string/array</td>
<td>Return only discovery checks that have detected</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the given discovered services.</td>
</tr>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Sort the result by the given properties.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values are: dcheckid and druleid.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>These parameters being common for all get</td>
</tr>
<tr>
<td></td>
<td></td>
<td>methods are described in detail in the reference</td>
</tr>
<tr>
<td></td>
<td></td>
<td>commentary.</td>
</tr>
<tr>
<td>countOutput</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>editable</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>excludeSearch</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>filter</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>limit</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>output</td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>preservekeys</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>search</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>searchByAny</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>searchWildcardsEnabled</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>sortorder</td>
<td>string/array</td>
<td></td>
</tr>
<tr>
<td>startSearch</td>
<td>boolean</td>
<td></td>
</tr>
</tbody>
</table>

Return values

(integer/array) Returns either:

- an array of objects;
- the count of retrieved objects, if the countOutput parameter has been used.

Examples

Retrieve discovery checks for a discovery rule

Retrieve all discovery checks used by discovery rule "6".

Request:
CDCheck::get() in frontends/php/include/classes/api/services/CDCheck.php.

**Discovery rule**

This class is designed to work with network discovery rules.

> **Note:**
This API is meant to work with network discovery rules. For the low-level discovery rules see the [LLD rule API](#).

**Object references:**

- Discovery rule

**Available methods:**

- **drule.create** - create new discovery rules
- **drule.delete** - delete discovery rules
- **drule.get** - retrieve discovery rules
- **drule.update** - update discovery rules

> **Discovery rule object**

The following objects are directly related to the drule API.

Discovery rule
The discovery rule object defines a network discovery rule. It has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>druleid</td>
<td>string</td>
<td>(readonly) ID of the discovery rule.</td>
</tr>
<tr>
<td>iprange</td>
<td>string</td>
<td>One or several IP ranges to check separated by commas. Refer to the network discovery configuration section for more information on supported formats of IP ranges.</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>Name of the discovery rule.</td>
</tr>
<tr>
<td>delay</td>
<td>string</td>
<td>Execution interval of the discovery rule. Accepts seconds, time unit with suffix and user macro. Default: 1h.</td>
</tr>
<tr>
<td>nextcheck</td>
<td>timestamp</td>
<td>(readonly) Time when the discovery rule will be executed next.</td>
</tr>
<tr>
<td>proxy_hostid</td>
<td>string</td>
<td>ID of the proxy used for discovery.</td>
</tr>
<tr>
<td>status</td>
<td>integer</td>
<td>Whether the discovery rule is enabled. Possible values: 0 - (default) enabled; 1 - disabled.</td>
</tr>
</tbody>
</table>

Note that for some methods (update, delete) the required/optional parameter combination is different.

**drule.create**

Description

object drule.create(object/array discoveryRules)

This method allows to create new discovery rules.

Parameters

(object/array) Discovery rules to create.

Additionally to the standard discovery rule properties, the method accepts the following parameters.
### Parameter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dchecks</td>
<td>array</td>
<td>Discovery checks to create for the discovery rule.</td>
</tr>
</tbody>
</table>

**Return values**

(often) Returns an object containing the IDs of the created discovery rules under the `druleids` property. The order of the returned IDs matches the order of the passed discovery rules.

**Examples**

**Create a discovery rule**

Create a discovery rule to find machines running the Zabbix agent in the local network. The rule must use a single Zabbix agent check on port 10050.

**Request:**

```json
{
    "jsonrpc": "2.0",
    "method": "drule.create",
    "params": {
        "name": "Zabbix agent discovery",
        "iprange": "192.168.1.1-255",
        "dchecks": [
            {
                "type": "9",
                "key_": "system.uname",
                "ports": "10050",
                "uniq": "0"
            }
        ]
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

**Response:**

```json
{
    "jsonrpc": "2.0",
    "result": {
        "druleids": [
            "6"
        ]
    },
    "id": 1
}
```

**See also**

- [Discovery check](#)

**Source**

`CDRule::create()` in frontends/php/include/classes/api/services/CDRule.php.

### drule.delete

**Description**

object drule.delete(array discoveryRuleIds)

This method allows to delete discovery rules.

**Parameters**

(array) IDs of the discovery rules to delete.
Return values

(object) Returns an object containing the IDs of the deleted discovery rules under the druleids property.

Examples

Delete multiple discovery rules

Delete two discovery rules.

Request:

```
{
    "jsonrpc": "2.0",
    "method": "drule.delete",
    "params": [
        "4",
        "6"
    ],
    "auth": "3a57200802b24cda67c4e4010b50c065",
    "id": 1
}
```

Response:

```
{
    "jsonrpc": "2.0",
    "result": {
        "druleids": [
            "4",
            "6"
        ]
    },
    "id": 1
}
```

Source

CDRule::delete() in frontends/php/include/classes/api/services/CDRule.php.

drule.get

Description

integer/array drule.get(object parameters)

The method allows to retrieve discovery rules according to the given parameters.

Parameters

(object) Parameters defining the desired output.

The method supports the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhostids</td>
<td>string/array</td>
<td>Return only discovery rules that created the given discovered hosts.</td>
</tr>
<tr>
<td>druleids</td>
<td>string/array</td>
<td>Return only discovery rules with the given IDs.</td>
</tr>
<tr>
<td>dserviceids</td>
<td>string/array</td>
<td>Return only discovery rules that created the given discovered services.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>selectDChecks</td>
<td>query</td>
<td>Return discovery checks used by the discovery rule in the dchecks property. Supports count.</td>
</tr>
<tr>
<td>selectDHosts</td>
<td>query</td>
<td>Return the discovered hosts that the discovery rule created in the dhosts property. Supports count.</td>
</tr>
<tr>
<td>limitSelects</td>
<td>integer</td>
<td>Limits the number of records returned by subselects. Supports count.</td>
</tr>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Sort the result by the given properties. Possible values are: druleid and name. These parameters being common for all get methods are described in detail in the reference commentary.</td>
</tr>
<tr>
<td>countOutput</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>editable</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>excludeSearch</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>filter</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>limit</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>output</td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>preservekeys</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>search</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>searchByAny</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>searchWildcards</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>sortOrder</td>
<td>string/array</td>
<td></td>
</tr>
<tr>
<td>startSearch</td>
<td>boolean</td>
<td></td>
</tr>
</tbody>
</table>
• the count of retrieved objects, if the countOutput parameter has been used.

Examples

Retrieve all discovery rules

Retrieve all configured discovery rules and the discovery checks they use.

Request:

```
{  
  "jsonrpc": "2.0",
  "method": "drule.get",
  "params": {
    "output": "extend",
    "selectDChecks": "extend"
  },
  "auth": "038e1d7b1735c6a5436ee9eae095879e",
  "id": 1
}
```

Response:

```
{  
  "jsonrpc": "2.0",
  "result": [
    {
      "druleid": "2",
      "proxy_hostid": "0",
      "name": "Local network",
      "iprange": "192.168.3.1-255",
      "delay": "5s",
      "nextcheck": "1348754327",
      "status": "0",
      "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"
        },
        {
          "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"
        }
      ]
    }
  ]
}


See also

- Discovered host
- Discovery check

Source

CDRule::get() in frontends/php/include/classes/api/services/CDRule.php.

**drule.update**

**Description**

object drule.update(object/array discoveryRules)

This method allows to update existing discovery rules.

**Parameters**

(object/array) Discovery rule properties to be updated.

The druleid property must be defined for each discovery rule, all other properties are optional. Only the passed properties will be updated, all others will remain unchanged.

Additionally to the standard discovery rule properties, the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dchecks</td>
<td>array</td>
<td>Discovery checks to replace existing checks.</td>
</tr>
</tbody>
</table>

**Return values**

(object) Returns an object containing the IDs of the updated discovery rules under the druleids property.

**Examples**

Change the IP range of a discovery rule
Change the IP range of a discovery rule to "192.168.2.1-255".

Request:

```json
{
   "jsonrpc": "2.0",
   "method": "drule.update",
   "params": {
      "druleid": "6",
      "iprange": "192.168.2.1-255"
   },
   "auth": "038e1d7b1735c6a5436ee9eae096879e",
   "id": 1
}
```

Response:

```json
{
   "jsonrpc": "2.0",
   "result": {
      "druleids": ["6"]
   },
   "id": 1
}
```

See also

- Discovery check

Source

CDRule::update() in frontends/php/include/classes/api/services/CDRule.php.

**Event**

This class is designed to work with events.

Object references:

- Event

Available methods:

- `event.get` - retrieving events
- `event.acknowledge` - acknowledging events

> Event object

The following objects are directly related to the event API.

Event

**Note:**

Events are created by the Zabbix server and cannot be modified via the API.

The event object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eventid</td>
<td>string</td>
<td>ID of the event.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>source</td>
<td>integer</td>
<td>Type of the event.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - event created by a trigger;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - event created by a discovery rule;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 - event created by active agent auto-registration;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 - internal event.</td>
</tr>
<tr>
<td>object</td>
<td>integer</td>
<td>Type of object that is related to the event.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values for trigger events:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - trigger.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values for discovery events:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - discovered host;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 - discovered service.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values for auto-registration events:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 - auto-registered host.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values for internal events:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - trigger;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 - item;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5 - LLD rule.</td>
</tr>
<tr>
<td>objectid</td>
<td>string</td>
<td>ID of the related object.</td>
</tr>
<tr>
<td>acknowledged</td>
<td>integer</td>
<td>Whether the event has been acknowledged.</td>
</tr>
<tr>
<td>clock</td>
<td>timestamp</td>
<td>Time when the event was created.</td>
</tr>
<tr>
<td>ns</td>
<td>integer</td>
<td>Nanoseconds when the event was created.</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>Resolved event name.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>value</td>
<td>integer</td>
<td>State of the related object. Possible values for trigger events: 0 - OK; 1 - problem. Possible values for discovery events: 0 - host or service up; 1 - host or service down; 2 - host or service discovered; 3 - host or service lost. Possible values for internal events: 0 - &quot;normal&quot; state; 1 - &quot;unknown&quot; or &quot;not supported&quot; state. This parameter is not used for active agent auto-registration events.</td>
</tr>
<tr>
<td>severity</td>
<td>integer</td>
<td>Event current severity. Possible values: 0 - not classified; 1 - information; 2 - warning; 3 - average; 4 - high; 5 - disaster.</td>
</tr>
<tr>
<td>r_eventid</td>
<td>string</td>
<td>Recovery event ID</td>
</tr>
<tr>
<td>c_eventid</td>
<td>string</td>
<td>ID of the event that was used to override (close) current event under global correlation rule. See correlationid to identify exact correlation rule. This parameter is only defined when the event is closed by global correlation rule.</td>
</tr>
</tbody>
</table>
Event tag
The event tag object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tag</td>
<td>string</td>
<td>Event tag name.</td>
</tr>
<tr>
<td>value</td>
<td>string</td>
<td>Event tag value.</td>
</tr>
</tbody>
</table>

event.acknowledge

Description

object event.acknowledge(object/array parameters)

This method allows to update events. Following update actions can be performed:

- Close event. If event is already resolved, this action will be skipped.
- Acknowledge event. If event is already acknowledged, this action will be skipped.
- Add message.
- Change event severity. If event already has same severity, this action will be skipped.

**Attention:**
Only trigger events can be updated.
Only problem events can be updated.
Read/Write rights for trigger are required to close the event or to change event’s severity.
To close an event, manual close should be allowed in the trigger.

Parameters

(object/array) Parameters containing the IDs of the events and update operations that should be performed.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eventids</td>
<td>string/object</td>
<td>IDs of the events to update.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>action</strong></td>
<td>integer</td>
<td>Event update action(s). This is bitmask field, any combination of values is acceptable. Possible values: 1 - close problem; 2 - acknowledge event; 4 - add message; 8 - change severity.</td>
</tr>
<tr>
<td><strong>message</strong></td>
<td>string</td>
<td>Text of the message. <strong>Required</strong>, if action contains ‘add message’ flag.</td>
</tr>
<tr>
<td><strong>severity</strong></td>
<td>integer</td>
<td>New severity for events. <strong>Required</strong>, if action contains ‘change severity’ flag. Possible values: 0 - not classified; 1 - information; 2 - warning; 3 - average; 4 - high; 5 - disaster.</td>
</tr>
</tbody>
</table>

Return values

(object) Returns an object containing the IDs of the updated events under the eventids property.

Examples

Acknowledging an event

Acknowledge a single event and leave a message.

Request:

```json
{
   "jsonrpc": "2.0",
   "method": "event.acknowledge",
   "params": {
      "eventids": "20427",
      "action": 6,
      "message": "Problem resolved."
   },
   "auth": "038e1d7b1735c6a5436ee9ea095879e",
   "id": 1
}
```

Response:

```json
{
   "jsonrpc": "2.0",
   "result": {
```
Changing event’s severity

Change severity for multiple events and leave a message.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "event.acknowledge",
    "params": {
        "eventids": ["20427", "20428"],
        "action": 12,
        "message": "Maintenance required to fix it.",
        "severity": 4
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "eventids": ["20427", "20428"]
    },
    "id": 1
}
```

Source

CEvent::acknowledge() in frontends/php/include/classes/api/services/CEvent.php.

**event.get**

Description

integer/array event.get(object parameters)

The method allows to retrieve events according to the given parameters.

**Attention:**

This method may return events of a deleted entity if these events have not been removed by the housekeeper yet.

Parameters

(object) Parameters defining the desired output.

The method supports the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eventids</td>
<td>string/array</td>
<td>Return only events with the given IDs.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>groupids</td>
<td>string/array</td>
<td>Return only events created by objects that belong to the given host groups.</td>
</tr>
<tr>
<td>hostids</td>
<td>string/array</td>
<td>Return only events created by objects that belong to the given hosts.</td>
</tr>
<tr>
<td>objectids</td>
<td>string/array</td>
<td>Return only events created by the given objects.</td>
</tr>
<tr>
<td>applicationids</td>
<td>string/array</td>
<td>Return only events created by objects that belong to the given applications. Applies only if object is trigger or item.</td>
</tr>
<tr>
<td>source</td>
<td>integer</td>
<td>Return only events with the given type.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Refer to the event object page for a list of supported event types.</td>
</tr>
<tr>
<td>object</td>
<td>integer</td>
<td>Return only events created by objects of the given type.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Refer to the event object page for a list of supported object types.</td>
</tr>
<tr>
<td>acknowledged</td>
<td>boolean</td>
<td>If set to true return only acknowledged events.</td>
</tr>
<tr>
<td>suppressed</td>
<td>boolean</td>
<td>true - return only suppressed events; false - return events in the normal state.</td>
</tr>
<tr>
<td>severities</td>
<td>integer/array</td>
<td>Return only events with given event severities. Applies only if object is trigger.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>evaltype</td>
<td>integer</td>
<td>Rules for tag searching. Possible values: 0 - (default) And/Or; 2 - Or.</td>
</tr>
</tbody>
</table>
| tags          | array of objects          | Return only events with given tags. Exact match by tag and case-insensitive search by value and operator. Format: 
<p>|               |                           | An empty array returns all events. Possible operator types: 0 - (default) Like; 1 - Equal. |
| eventid_from  | string                    | Return only events with IDs greater or equal to the given ID.               |
| eventid_till  | string                    | Return only events with IDs less or equal to the given ID.                 |
| time_from     | timestamp                 | Return only events that have been created after or at the given time.      |
| time_till     | timestamp                 | Return only events that have been created before or at the given time.     |
| problem_time_from | timestamp               | Returns only events that were in the problem state starting with problem_time_from. Applies only if the source is trigger event and object is trigger. Mandatory if problem_time_till is specified. |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>problem_time_till</td>
<td>timestamp</td>
<td>Returns only events that were in the problem state until <code>problem_time_till</code>. Applies only if the source is trigger event and object is trigger. Mandatory if <code>problem_time_from</code> is specified.</td>
</tr>
<tr>
<td>value</td>
<td>integer/array</td>
<td>Return only events with the given values.</td>
</tr>
<tr>
<td>selectHosts</td>
<td>query</td>
<td>Return hosts containing the object that created the event in the <code>hosts</code> property. Supported only for events generated by triggers, items or LLD rules.</td>
</tr>
<tr>
<td>selectRelatedObj</td>
<td>query</td>
<td>Return the object that created the event in the <code>relatedObject</code> property. The type of object returned depends on the event type.</td>
</tr>
<tr>
<td>select_alerts</td>
<td>query</td>
<td>Return alerts generated by the event in the <code>alerts</code> property. Alerts are sorted in reverse chronological order.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>select_acknowledges</td>
<td></td>
<td>Return event’s updates in the acknowledges property. Event updates are sorted in reverse chronological order.</td>
</tr>
</tbody>
</table>

The event update object has the following properties:
- **acknowledgeid** - (string) acknowledgement’s ID;
- **userid** - (string) ID of the user that updated the event;
- **eventid** - (string) ID of the updated event;
- **clock** - (timestamp) time when the event was updated;
- **message** - (string) text of the message;
- **action** - (integer) update action that was performed see event.acknowledge;
- **old_severity** - (integer) event severity before this update action;
- **new_severity** - (integer) event severity after this update action;
- **alias** - (string) alias of the user that updated the event;
- **name** - (string) name of the user that updated the event;
- **surname** - (string) surname of the user that updated the event.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>selectTags</td>
<td>query</td>
<td>Return event tags in tags property.</td>
</tr>
<tr>
<td>selectSuppressionData</td>
<td>query</td>
<td>Return list of maintenances in the suppression_data property: maintenanceid - (string) ID of the maintenance; suppress_until - (integer) time until the event is suppressed.</td>
</tr>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Sort the result by the given properties.</td>
</tr>
<tr>
<td>countOutput</td>
<td>boolean</td>
<td>These parameters being common for all get methods are described in detail in the reference commentary page.</td>
</tr>
<tr>
<td>editable</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>excludeSearch</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>filter</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>limit</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>output</td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>preservekeys</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>search</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>searchByAny</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>searchWildcardsEnabled</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>sortorder</td>
<td>string/array</td>
<td></td>
</tr>
<tr>
<td>startSearch</td>
<td>boolean</td>
<td></td>
</tr>
</tbody>
</table>

Return values
(integer/array) Returns either:
- an array of objects;
- the count of retrieved objects, if the countOutput parameter has been used.

Examples

Retrieving trigger events

Retrieve the latest events from trigger "13926."

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "event.get",
    "params": {
        "output": "extend",
        "select_acknowledges": "extend",
        "selectTags": "extend",
    }
}
```
"selectSuppressionData": "extend",
"objectids": "13926",
"sortfield": ["clock", "eventid"],
"sortorder": "DESC"
},
"auth": "038e1d7b1735c6a5436ee9eae095879e",
"id": 1
}

Response:
{
  "jsonrpc": "2.0",
  "result": [
    {
      "acknowledges": [
        {
          "acknowledgeid": "1",
          "userid": "1",
          "eventid": "9695",
          "clock": "1350640590",
          "message": "Problem resolved.\n\n----[BULK ACKNOWLEDGE]----",
          "action": "6",
          "old_severity": "0",
          "new_severity": "0",
          "alias": "Admin",
          "name": "Zabbix",
          "surname": "Administrator"
        }
      ],
      "eventid": "9695",
      "source": "0",
      "object": "0",
      "objectid": "13926",
      "clock": "1347970410",
      "value": "1",
      "acknowledged": "1",
      "suppressed": "1",
      "ns": "413316245",
      "name": "MySQL is down",
      "severity": "5",
      "r_eventid": "0",
      "c_eventid": "0",
      "correlationid": "0",
      "userid": "0",
      "tags": [
        {
          "tag": "service",
          "value": "mysqld"
        },
        {
          "tag": "error",
          "value": ""
        }
      ],
      "suppression_data": [
        {
          "maintenanceid": "15",
          "suppress_until": "1472511600"
        }
      ]
    }
  ]
}
Retrieving events by time period

Retrieve all events that have been created between October 9 and 10, 2012, in reverse chronological order.

Request:

```json
{
  "jsonrpc": "2.0",
  "method": "event.get",
  "params": {
    "output": "extend",
    "time_from": "1349797228",
    "time_till": "1350661228",
    "sortfield": ["clock", "eventid"],
    "sortorder": "desc"
  },
  "auth": "038e1d7b1735c6a5436ee9eae095879e",
  "id": 1
}
```

Response:

```json
{
  "jsonrpc": "2.0",
  "result": [
    {
      "eventid": "20616",
      "source": "0",
      "object": "0",
      "objectid": "14282",
      "clock": "1350477814",
      "value": "1",
      "acknowledged": "0",
      "suppressed": "0",
      "ns": "0",
      "name": "Less than 25% free in the history cache",
      "severity": "3",
      "r_eventid": "0",
      "c_eventid": "0",
      "correlationid": "0",
      "userid": "0"
    }
  ]
}
```
See also

- Alert
- Item
- Host
- LLD rule
- Trigger

Source

CEvent::get() in frontends/php/include/classes/api/services/CEvent.php.

**Graph**

This class is designed to work with graphs.

Object references:

- Graph

Available methods:

- `graph.create` - creating new graphs
- `graph.delete` - deleting graphs
- `graph.get` - retrieving graphs
- `graph.update` - updating graphs
> **Graph object**

The following objects are directly related to the graph API.

**Graph**

The graph object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>graphid</td>
<td>string</td>
<td>(readonly) ID of the graph.</td>
</tr>
<tr>
<td>height</td>
<td>integer</td>
<td>Height of the graph in pixels.</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>Name of the graph</td>
</tr>
<tr>
<td>width</td>
<td>integer</td>
<td>Width of the graph in pixels.</td>
</tr>
<tr>
<td>flags</td>
<td>integer</td>
<td>(readonly) Origin of the graph.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - (default) a plain graph;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 - a discovered graph.</td>
</tr>
<tr>
<td>graphtype</td>
<td>integer</td>
<td>Graph’s layout type.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - (default) normal;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - stacked;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 - pie;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 - exploded.</td>
</tr>
<tr>
<td>percent_left</td>
<td>float</td>
<td>Left percentile.</td>
</tr>
<tr>
<td>percent_right</td>
<td>float</td>
<td>Right percentile.</td>
</tr>
<tr>
<td>show_3d</td>
<td>integer</td>
<td>Whether to show pie and exploded graphs in 3D.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - (default) show in 2D;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - show in 3D.</td>
</tr>
<tr>
<td>show_legend</td>
<td>integer</td>
<td>Whether to show the legend on the graph.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - hide;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - (default) show.</td>
</tr>
<tr>
<td>show_work_period</td>
<td>integer</td>
<td>Whether to show the working time on the graph.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - hide;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - (default) show.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>show_triggers</td>
<td>integer</td>
<td>Whether to show the trigger line on the graph. Possible values: 0 - hide; 1 - (default) show.</td>
</tr>
<tr>
<td>templateid</td>
<td>string</td>
<td>(readonly) ID of the parent template graph.</td>
</tr>
<tr>
<td>yaxismax</td>
<td>float</td>
<td>The fixed maximum value for the Y axis. Default: 100.</td>
</tr>
<tr>
<td>yaxismin</td>
<td>float</td>
<td>The fixed minimum value for the Y axis. Default: 0.</td>
</tr>
<tr>
<td>ymax_itemid</td>
<td>string</td>
<td>ID of the item that is used as the maximum value for the Y axis.</td>
</tr>
<tr>
<td>ymax_type</td>
<td>integer</td>
<td>Maximum value calculation method for the Y axis. Possible values: 0 - (default) calculated; 1 - fixed; 2 - item.</td>
</tr>
<tr>
<td>ymin_itemid</td>
<td>string</td>
<td>ID of the item that is used as the minimum value for the Y axis.</td>
</tr>
<tr>
<td>ymin_type</td>
<td>integer</td>
<td>Minimum value calculation method for the Y axis. Possible values: 0 - (default) calculated; 1 - fixed; 2 - item.</td>
</tr>
</tbody>
</table>

Note that for some methods (update, delete) the required/optional parameter combination is different.

**graph.create**

Description

object graph.create(object/array graphs)

This method allows to create new graphs.

Parameters

(object/array) Graphs to create.
Additionally to the **standard graph properties**, the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>gitems</td>
<td>array</td>
<td>Graph items to be created for the graph.</td>
</tr>
</tbody>
</table>

(Required)

**Return values**

(object) Returns an object containing the IDs of the created graphs under the graphIds property. The order of the returned IDs matches the order of the passed graphs.

**Examples**

Creating a graph

Create a graph with two items.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "graph.create",
    "params": {
        "name": "MySQL bandwidth",
        "width": 900,
        "height": 200,
        "gitems": [
            {
                "itemid": "22828",
                "color": "00AA00"
            },
            {
                "itemid": "22829",
                "color": "3333FF"
            }
        ]
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "graphIds": ["652"
    ]
    },
    "id": 1
}
```

See also

- **Graph item**

**Source**

CGraph::create() in frontends/php/include/classes/api/services/CGraph.php.

**graph.delete**

**Description**

Object graph.delete(array graphIds)

This method allows to delete graphs.
Parameters
(array) IDs of the graphs to delete.

Return values
(object) Returns an object containing the IDs of the deleted graphs under the graphids property.

Examples
Deleting multiple graphs
Delete two graphs.

Request:
{
    "jsonrpc": "2.0",
    "method": "graph.delete",
    "params": [
        "652",
        "653"
    ],
    "auth": "3a57200802b24cda67c4e4010b50c065",
    "id": 1
}

Response:
{
    "jsonrpc": "2.0",
    "result": {
        "graphids": [
            "652",
            "653"
        ]
    },
    "id": 1
}

Source
CGraph::delete() in frontends/php/include/classes/api/services/CGraph.php.

graph.get

Description
integer/array graph.get(object parameters)
The method allows to retrieve graphs according to the given parameters.

Parameters
(object) Parameters defining the desired output.
The method supports the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>graphids</td>
<td>string/array</td>
<td>Return only graphs with the given IDs.</td>
</tr>
<tr>
<td>groupids</td>
<td>string/array</td>
<td>Return only graphs that belong to hosts in the given host groups.</td>
</tr>
<tr>
<td>templateids</td>
<td>string/array</td>
<td>Return only graph that belong to the given templates.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>hostids</td>
<td>string/array</td>
<td>Return only graphs that belong to the given hosts.</td>
</tr>
<tr>
<td>itemids</td>
<td>string/array</td>
<td>Return only graphs that contain the given items.</td>
</tr>
<tr>
<td>templated</td>
<td>boolean</td>
<td>If set to true return only graphs that belong to templates.</td>
</tr>
<tr>
<td>inherited</td>
<td>boolean</td>
<td>If set to true return only graphs inherited from a template.</td>
</tr>
<tr>
<td>expandName</td>
<td>flag</td>
<td>Expand macros in the graph name.</td>
</tr>
<tr>
<td>selectGroups</td>
<td>query</td>
<td>Return the host groups that the graph belongs to in the groups property.</td>
</tr>
<tr>
<td>selectTemplates</td>
<td>query</td>
<td>Return the templates that the graph belongs to in the templates property.</td>
</tr>
<tr>
<td>selectHosts</td>
<td>query</td>
<td>Return the hosts that the graph belongs to in the hosts property.</td>
</tr>
<tr>
<td>selectItems</td>
<td>query</td>
<td>Return the items used in the graph in the items property.</td>
</tr>
<tr>
<td>selectGraphDiscovery</td>
<td>query</td>
<td>Return the graph discovery object in the graphDiscovery property. The graph discovery objects links the graph to a graph prototype from which it was created. It has the following properties: graphid - (string) ID of the graph; parent_graphid - (string) ID of the graph prototype from which the graph has been created.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>selectGraphItems</td>
<td>query</td>
<td>Return the graph items used in the graph in the gitems property.</td>
</tr>
<tr>
<td>selectDiscoveryRule</td>
<td>query</td>
<td>Return the low-level discovery rule that created the graph in the discoveryRule property.</td>
</tr>
<tr>
<td>filter</td>
<td>object</td>
<td>Return only those results that exactly match the given filter. Accepts an array, where the keys are property names, and the values are either a single value or an array of values to match against. Supports additional filters: host - technical name of the host that the graph belongs to; hostid - ID of the host that the graph belongs to. Sort the result by the given properties. Possible values are: graphid, name and graphtype. These parameters being common for all get methods are described in detail in the reference commentary page.</td>
</tr>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Sort the result by the given properties.</td>
</tr>
<tr>
<td>countOutput</td>
<td>boolean</td>
<td>These parameters being common for all get methods are described in detail in the reference commentary page.</td>
</tr>
<tr>
<td>editable</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>excludeSearch</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>limit</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>output</td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>preservekeys</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>search</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>searchByAny</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>searchWildcardsEnabled</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>sortOrder</td>
<td>string/array</td>
<td></td>
</tr>
<tr>
<td>startSearch</td>
<td>boolean</td>
<td></td>
</tr>
</tbody>
</table>
Return values

(integer/array) Returns either:

• an array of objects;
• the count of retrieved objects, if the countOutput parameter has been used.

Examples

Retrieving graphs from hosts

Retrieve all graphs from host "10107" and sort them by name.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "graph.get",
    "params": {
        "output": "extend",
        "hostids": 10107,
        "sortfield": "name"
    },
    "auth": "038e1d7b1735c6a5436ee9eae096879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": [
        {
            "graphid": "612",
            "name": "CPU jumps",
            "width": "900",
            "height": "200",
            "yaxismin": "0.0000",
            "yaxismax": "100.0000",
            "templateid": "439",
            "show_work_period": "1",
            "show_triggers": "1",
            "graphtype": "0",
            "show_legend": "1",
            "show_3d": "0",
            "percent_left": "0.0000",
            "percent_right": "0.0000",
            "ymin_type": "0",
            "ymax_type": "0",
            "ymin_itemid": "0",
            "ymax_itemid": "0",
            "flags": "0"
        },
        {
            "graphid": "613",
            "name": "CPU load",
            "width": "900",
            "height": "200",
            "yaxismin": "0.0000",
            "yaxismax": "100.0000",
            "templateid": "433",
            "show_work_period": "1",
            "show_triggers": "1",
            "graphtype": "0",
            "show_legend": "1",
            "show_3d": "0",
            "percent_left": "0.0000",
            "percent_right": "0.0000"
        }
    ]
}
```


See also

- Discovery rule
- Graph item
- Item
- Host
- Host group
- Template

Source
graph.update

Description

object graph.update(object/array graphs)

This method allows to update existing graphs.

Parameters

(object/array) Graph properties to be updated.

The graphid property must be defined for each graph, all other properties are optional. Only the passed properties will be updated, all others will remain unchanged.

Additionally to the standard graph properties the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>gitems</td>
<td>array</td>
<td>Graph items to replace existing graph items. If a graph item has the gitemid property defined it will be updated, otherwise a new graph item will be created.</td>
</tr>
</tbody>
</table>

Return values

(object) Returns an object containing the IDs of the updated graphs under the graphids property.

Examples

Setting the maximum for the Y scale

Set the maximum of the Y scale to a fixed value of 100.

Request:

```
{
    "jsonrpc": "2.0",
    "method": "graph.update",
    "params": {
        "graphid": "439",
        "yaxismax": 100
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```
{
    "jsonrpc": "2.0",
    "result": {
        "graphids": ["439"
    ],
    "id": 1
}
```
Graph item

This class is designed to work with graph items.

Object references:

- Graph item

Available methods:

- `graphitem.get` - retrieving graph items

> Graph item object

The following objects are directly related to the `graphitem` API.

Graph item

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>gitemid</td>
<td>string</td>
<td>(readonly) ID of the graph item.</td>
</tr>
<tr>
<td>color</td>
<td>string</td>
<td>Graph item's draw color as a hexadecimal color code.</td>
</tr>
<tr>
<td>itemid</td>
<td>string</td>
<td>ID of the item.</td>
</tr>
<tr>
<td>calc_fnc</td>
<td>integer</td>
<td>Value of the item that will be displayed.</td>
</tr>
<tr>
<td>drawtype</td>
<td>integer</td>
<td>Draw style of the graph item.</td>
</tr>
</tbody>
</table>

Possible values:

- 1 - minimum value;
- 2 - (default) average value;
- 4 - maximum value;
- 7 - all values;
- 9 - last value, used only by pie and exploded graphs.

Note: Graph items can only be modified via the graph API.
<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>graphid</td>
<td>string</td>
<td>ID of the graph that the graph item belongs to. Position of the item in the graph. Default: starts with 0 and increases by one with each entry.</td>
</tr>
<tr>
<td>sortorder</td>
<td>integer</td>
<td>Type of graph item. Possible values: 0 - (default) simple; 2 - graph sum, used only by pie and exploded graphs.</td>
</tr>
<tr>
<td>type</td>
<td>integer</td>
<td>Side of the graph where the graph item's Y scale will be drawn. Possible values: 0 - (default) left side; 1 - right side.</td>
</tr>
<tr>
<td>yaxisside</td>
<td>integer</td>
<td></td>
</tr>
</tbody>
</table>

**graphitem.get**

Description

integer/array graphitem.get(object parameters)

The method allows to retrieve graph items according to the given parameters.

Parameters

(object) Parameters defining the desired output.

The method supports the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>graphids</td>
<td>string/array</td>
<td>Return only graph items that belong to the given graphs.</td>
</tr>
<tr>
<td>itemids</td>
<td>string/array</td>
<td>Return only graph items with the given item IDs.</td>
</tr>
<tr>
<td>type</td>
<td>integer</td>
<td>Return only graph items with the given type. Refer to the <a href="#">graph item object page</a> for a list of supported graph item types.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>selectGraphs</td>
<td>query</td>
<td>Return the graph that the item belongs to as an array in the graphs property.</td>
</tr>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Sort the result by the given properties.</td>
</tr>
<tr>
<td>countOutput</td>
<td>boolean</td>
<td>Possible values are: gitemid. These parameters being common for all get methods are described in detail in the reference commentary page.</td>
</tr>
<tr>
<td>editable</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>limit</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>output</td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>preservekeys</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>sortorder</td>
<td>string/array</td>
<td></td>
</tr>
</tbody>
</table>

Return values
(integer/array) Returns either:
- an array of objects;
- the count of retrieved objects, if the countOutput parameter has been used.

Examples

Retrieving graph items from a graph

Retrieve all graph items used in a graph with additional information about the item and the host.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "graphitem.get",
    "params": {
        "output": "extend",
        "graphids": "387"
    },
    "auth": "038e1d7b1735c6a5436ee9eae096879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": [
        {
            "gitemid": "1242",
            "graphid": "387",
            "itemid": "22665",
            "drawtype": "1",
            "sortorder": "1",
            "color": "FF5555",
            "yaxisside": "0",
            "calc_fnc": "2"
        }
    ]
}
```
"type": "0",
"key_": "system.cpu.util[,steal]",
"hostid": "10001",
"flags": "0",
"host": "Template OS Linux"
},
{
    "gitemid": "1243",
    "graphid": "387",
    "itemid": "22668",
    "drawtype": "1",
    "sortorder": "2",
    "color": "55FF55",
    "yaxisside": "0",
    "calc_fnc": "2",
    "type": "0",
    "key_": "system.cpu.util[,softirq]",
    "hostid": "10001",
    "flags": "0",
    "host": "Template OS Linux"
},
{
    "gitemid": "1244",
    "graphid": "387",
    "itemid": "22671",
    "drawtype": "1",
    "sortorder": "3",
    "color": "009999",
    "yaxisside": "0",
    "calc_fnc": "2",
    "type": "0",
    "key_": "system.cpu.util[,interrupt]",
    "hostid": "10001",
    "flags": "0",
    "host": "Template OS Linux"
}
],
"id": 1}

See also

- Graph

Source

CGraphItem::get() in frontends/php/include/classes/api/services/CGraphItem.php.

**Graph prototype**

This class is designed to work with graph prototypes.

Object references:

- Graph prototype

Available methods:

- graphprototype.create - creating new graph prototypes
- graphprototype.delete - deleting graph prototypes
- graphprototype.get - retrieving graph prototypes
- graphprototype.update - updating graph prototypes
> Graph prototype object

The following objects are directly related to the graphprototype API.

Graph prototype

The graph prototype object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>graphid</td>
<td>string</td>
<td>(readonly) ID of the graph prototype.</td>
</tr>
<tr>
<td>height</td>
<td>integer</td>
<td>Height of the graph prototype in pixels.</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>Name of the graph prototype.</td>
</tr>
<tr>
<td>width</td>
<td>integer</td>
<td>Width of the graph prototype in pixels.</td>
</tr>
<tr>
<td>graphtype</td>
<td>integer</td>
<td>Graph prototypes's layout type.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values: 0 - (default) normal; 1 - stacked; 2 - pie; 3 - exploded.</td>
</tr>
<tr>
<td>percent_left</td>
<td>float</td>
<td>Left percentile.</td>
</tr>
<tr>
<td>percent_right</td>
<td>float</td>
<td>Right percentile.</td>
</tr>
<tr>
<td>show_3d</td>
<td>integer</td>
<td>Whether to show discovered pie and exploded graphs in 3D.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values: 0 - (default) show in 2D; 1 - show in 3D.</td>
</tr>
<tr>
<td>show_legend</td>
<td>integer</td>
<td>Whether to show the legend on the discovered graph.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values: 0 - hide; 1 - (default) show.</td>
</tr>
<tr>
<td>show_work_period</td>
<td>integer</td>
<td>Whether to show the working time on the discovered graph.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values: 0 - hide; 1 - (default) show.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>templateid</td>
<td>string</td>
<td>(readonly) ID of the parent template graph prototype.</td>
</tr>
<tr>
<td>yaxismax</td>
<td>float</td>
<td>The fixed maximum value for the Y axis.</td>
</tr>
<tr>
<td>yaxismin</td>
<td>float</td>
<td>The fixed minimum value for the Y axis.</td>
</tr>
<tr>
<td>ymax_itemid</td>
<td>string</td>
<td>ID of the item that is used as the maximum value for the Y axis.</td>
</tr>
<tr>
<td>ymax_type</td>
<td>integer</td>
<td>Maximum value calculation method for the Y axis.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values: 0 - (default) calculated; 1 - fixed; 2 - item.</td>
</tr>
<tr>
<td>ymin_itemid</td>
<td>string</td>
<td>ID of the item that is used as the minimum value for the Y axis.</td>
</tr>
<tr>
<td>ymin_type</td>
<td>integer</td>
<td>Minimum value calculation method for the Y axis.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values: 0 - (default) calculated; 1 - fixed; 2 - item.</td>
</tr>
</tbody>
</table>

Note that for some methods (update, delete) the required/optional parameter combination is different.

**graphprototype.create**

**Description**

*object* graphprototype.create(*object/array* graphPrototypes)

This method allows to create new graph prototypes.

**Parameters**

* (object/array) Graph prototypes to create.

Additionally to the standard graph prototype properties, the method accepts the following parameters.
Parameter | Type | Description
---|---|---
gitems | array | Graph items to be created for the graph prototypes. Graph items can reference both items and item prototypes, but at least one item prototype must be present.

Return values

(object) Returns an object containing the IDs of the created graph prototypes under the graphids property. The order of the returned IDs matches the order of the passed graph prototypes.

Examples

Creating a graph prototype

Create a graph prototype with two items.

Request:

```json
{
   "jsonrpc": "2.0",
   "method": "graphprototype.create",
   "params": {
      "name": "Disk space usage {#FSNAME}"
   },
   "gitems": [
      {
         "itemid": "22828",
         "color": "00AA00"
      },
      {
         "itemid": "22829",
         "color": "3333FF"
      }
   ],
   "width": 900,
   "height": 200,
   "auth": "038e1d7b1735c6a5436ee9eae095879e",
   "id": 1
}
```

Response:

```json
{
   "jsonrpc": "2.0",
   "result": {
      "graphids": [
         "652"
      ]
   },
   "id": 1
}
```

See also

- Graph item

Source

CGraphPrototype::create() in frontends/php/include/classes/api/services/CGraphPrototype.php.
**graphprototype.delete**

**Description**

object graphprototype.delete(array graphPrototypeIds)

This method allows to delete graph prototypes.

**Parameters**

(array) IDs of the graph prototypes to delete.

**Return values**

(object) Returns an object containing the IDs of the deleted graph prototypes under the `graphids` property.

**Examples**

Deleting multiple graph prototypes

Delete two graph prototypes.

**Request:**

```
{
    "jsonrpc": "2.0",
    "method": "graphprototype.delete",
    "params": [
        "652",
        "653"
    ],
    "auth": "3a57200802b24cda67c4e401b50c065",
    "id": 1
}
```

**Response:**

```
{
    "jsonrpc": "2.0",
    "result": {
        "graphids": [
            "652",
            "653"
        ]
    },
    "id": 1
}
```

**Source**

CGraphPrototype::delete() in frontends/php/include/classes/api/services/CGraphPrototype.php.

**graphprototype.get**

**Description**

integer/array graphprototype.get(object parameters)

The method allows to retrieve graph prototypes according to the given parameters.

**Parameters**

(object) Parameters defining the desired output.

The method supports the following parameters.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>discoveryids</td>
<td>string/array</td>
<td>Return only graph prototypes that belong to the given discovery rules.</td>
</tr>
<tr>
<td>graphids</td>
<td>string/array</td>
<td>Return only graph prototypes with the given IDs.</td>
</tr>
<tr>
<td>groupids</td>
<td>string/array</td>
<td>Return only graph prototypes that belong to hosts in the given host groups.</td>
</tr>
<tr>
<td>hostids</td>
<td>string/array</td>
<td>Return only graph prototypes that belong to the given hosts.</td>
</tr>
<tr>
<td>inherited</td>
<td>boolean</td>
<td>If set to true return only graph prototypes inherited from a template.</td>
</tr>
<tr>
<td>itemids</td>
<td>string/array</td>
<td>Return only graph prototypes that contain the given item prototypes.</td>
</tr>
<tr>
<td>templated</td>
<td>boolean</td>
<td>If set to true return only graph prototypes that belong to templates.</td>
</tr>
<tr>
<td>templateids</td>
<td>string/array</td>
<td>Return only graph prototypes that belong to the given templates.</td>
</tr>
<tr>
<td>selectDiscoveryRule</td>
<td>query</td>
<td>Return the LLD rule that the graph prototype belongs to in the discoveryRule property.</td>
</tr>
<tr>
<td>selectGraphItems</td>
<td>query</td>
<td>Return the graph items used in the graph prototype in the gitems property.</td>
</tr>
<tr>
<td>selectGroups</td>
<td>query</td>
<td>Return the host groups that the graph prototype belongs to in the groups property.</td>
</tr>
<tr>
<td>selectHosts</td>
<td>query</td>
<td>Return the hosts that the graph prototype belongs to in the hosts property.</td>
</tr>
<tr>
<td>selectItems</td>
<td>query</td>
<td>Return the items and item prototypes used in the graph prototype in the items property.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>selectTemplates</td>
<td>query</td>
<td>Return the templates that the graph prototype belongs to in the templates property.</td>
</tr>
<tr>
<td>filter</td>
<td>object</td>
<td>Return only those results that exactly match the given filter. Accepts an array, where the keys are property names, and the values are either a single value or an array of values to match against. Supports additional filters: host - technical name of the host that the graph prototype belongs to; hostid - ID of the host that the graph prototype belongs to. Sort the result by the given properties. Possible values are: graphid, name and graphtype. These parameters being common for all get methods are described in detail in the reference commentary.</td>
</tr>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Sort the result by the given properties. Possible values are: graphid, name and graphtype.</td>
</tr>
<tr>
<td>countOutput</td>
<td>boolean</td>
<td>These parameters being common for all get methods are described in detail in the reference commentary.</td>
</tr>
<tr>
<td>editable</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>excludeSearch</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>limit</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>output</td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>preservekeys</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>search</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>searchByAny</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>searchWildcards</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>sortorder</td>
<td>string/array</td>
<td></td>
</tr>
<tr>
<td>startSearch</td>
<td>boolean</td>
<td></td>
</tr>
</tbody>
</table>

Return values
(integer/array) Returns either:
• an array of objects;
• the count of retrieved objects, if the countOutput parameter has been used.

Examples

Retrieving graph prototypes from a LLD rule

Retrieve all graph prototypes from an LLD rule.

Request:

```json
{
   "jsonrpc": "2.0",
   "method": "graphprototype.get",
   "params": {
      "output": "extend",
      "discoveryids": "27426"
   },
   "auth": "038e1d7b1735c6a5436ee9eae095879e",
   "id": 1
}
```

Response:

```json
{
   "jsonrpc": "2.0",
   "result": [
      {
         "graphid": "1017",
         "parent_itemid": "27426",
         "name": "Disk space usage {#FSNAME}",
         "width": "600",
         "height": "340",
         "yaxismin": "0.0000",
         "yaxismsax": "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"
      }
   ],
   "id": 1
}
```

See also

- Discovery rule
- Graph item
- Item
- Host
- Host group
- Template

Source

CGraphPrototype::get() in frontends/php/include/classes/api/services/CGraphPrototype.php.

**graphprototype.update**

Description
object graphprototype.update(object/array graphPrototypes)

This method allows to update existing graph prototypes.

Parameters

(object/array) Graph prototype properties to be updated.

The graphid property must be defined for each graph prototype, all other properties are optional. Only the passed properties will be updated, all others will remain unchanged.

Additionally to the standard graph prototype properties, the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>gitems</td>
<td>array</td>
<td>Graph items to replace existing graph items. If a graph item has the gitemid property defined it will be updated, otherwise a new graph item will be created.</td>
</tr>
</tbody>
</table>

Return values

(object) Returns an object containing the IDs of the updated graph prototypes under the graphids property.

Examples

Changing the size of a graph prototype

Change the size of a graph prototype to 1100 to 400 pixels.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "graphprototype.update",
    "params": {
        "graphid": "439",
        "width": 1100,
        "height": 400
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "graphids": ["439"
    ],
    "id": 1
}
```

Source

CGraphPrototype::update() in frontends/php/include/classes/api/services/CGraphPrototype.php.

History

This class is designed to work with history data.
Object references:

- History

Available methods:

- history.get - retrieving history data.

> History object

The following objects are directly related to the history API.

**Note:**
History objects differ depending on the item's type of information. They are created by the Zabbix server and cannot be modified via the API.

Float history

The float history object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clock</td>
<td>timestamp</td>
<td>Time when that value was received.</td>
</tr>
<tr>
<td>itemid</td>
<td>string</td>
<td>ID of the related item.</td>
</tr>
<tr>
<td>ns</td>
<td>integer</td>
<td>Nanoseconds when the value was received.</td>
</tr>
<tr>
<td>value</td>
<td>float</td>
<td>Received value.</td>
</tr>
</tbody>
</table>

Integer history

The integer history object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clock</td>
<td>timestamp</td>
<td>Time when that value was received.</td>
</tr>
<tr>
<td>itemid</td>
<td>string</td>
<td>ID of the related item.</td>
</tr>
<tr>
<td>ns</td>
<td>integer</td>
<td>Nanoseconds when the value was received.</td>
</tr>
<tr>
<td>value</td>
<td>integer</td>
<td>Received value.</td>
</tr>
</tbody>
</table>

String history

The string history object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clock</td>
<td>timestamp</td>
<td>Time when that value was received.</td>
</tr>
<tr>
<td>itemid</td>
<td>string</td>
<td>ID of the related item.</td>
</tr>
<tr>
<td>ns</td>
<td>integer</td>
<td>Nanoseconds when the value was received.</td>
</tr>
<tr>
<td>value</td>
<td>string</td>
<td>Received value.</td>
</tr>
</tbody>
</table>

Text history

The text history object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>string</td>
<td>ID of the history entry.</td>
</tr>
<tr>
<td>clock</td>
<td>timestamp</td>
<td>Time when that value was received.</td>
</tr>
<tr>
<td>itemid</td>
<td>string</td>
<td>ID of the related item.</td>
</tr>
<tr>
<td>ns</td>
<td>integer</td>
<td>Nanoseconds when the value was received.</td>
</tr>
<tr>
<td>value</td>
<td>text</td>
<td>Received value.</td>
</tr>
</tbody>
</table>

Log history
The log history object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>string</td>
<td>ID of the history entry.</td>
</tr>
<tr>
<td>clock</td>
<td>timestamp</td>
<td>Time when that value was received.</td>
</tr>
<tr>
<td>itemid</td>
<td>string</td>
<td>ID of the related item.</td>
</tr>
<tr>
<td>logeventid</td>
<td>integer</td>
<td>Windows event log entry ID.</td>
</tr>
<tr>
<td>ns</td>
<td>integer</td>
<td>Nanoseconds when the value was received.</td>
</tr>
<tr>
<td>severity</td>
<td>integer</td>
<td>Windows event log entry level.</td>
</tr>
<tr>
<td>source</td>
<td>string</td>
<td>Windows event log entry source.</td>
</tr>
<tr>
<td>timestamp</td>
<td>timestamp</td>
<td>Windows event log entry time.</td>
</tr>
<tr>
<td>value</td>
<td>text</td>
<td>Received value.</td>
</tr>
</tbody>
</table>

**history.get**

Description

integer/array history.get(object parameters)

The method allows to retrieve history data according to the given parameters.

See also: known issues

Attention:
This method may return historical data of a deleted entity if this data has not been removed by the housekeeper yet.

Parameters

(object) Parameters defining the desired output.

The method supports the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>history</td>
<td>integer</td>
<td>History object types to return.</td>
</tr>
<tr>
<td>hostids</td>
<td>string/array</td>
<td>Return only history from the given hosts.</td>
</tr>
<tr>
<td>itemids</td>
<td>string/array</td>
<td>Return only history from the given items.</td>
</tr>
<tr>
<td>time_from</td>
<td>timestamp</td>
<td>Return only values that have been received after or at the given time.</td>
</tr>
<tr>
<td>time_till</td>
<td>timestamp</td>
<td>Return only values that have been received before or at the given time.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Sort the result by the given properties. Possible values are: itemid and clock.</td>
</tr>
<tr>
<td>countOutput</td>
<td>boolean</td>
<td>These parameters being common for all get methods are described in detail in the reference commentary page.</td>
</tr>
<tr>
<td>editable</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>excludeSearch</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>filter</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>limit</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>output</td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>search</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>searchByAny</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>searchWildcardsEnabled</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>sortorder</td>
<td>string/array</td>
<td></td>
</tr>
<tr>
<td>startSearch</td>
<td>boolean</td>
<td></td>
</tr>
</tbody>
</table>

Return values
(integer/array) Returns either:
- an array of objects;
- the count of retrieved objects, if the countOutput parameter has been used.

Examples

Retrieving item history data

Return 10 latest values received from a numeric(float) item.

Request:
```json
{
  "jsonrpc": "2.0",
  "method": "history.get",
  "params": {
    "output": "extend",
    "history": 0,
    "itemids": "23296",
    "sortfield": "clock",
    "sortorder": "DESC",
    "limit": 10
  },
  "auth": "038e1d7b1735c6a5436ee9eae095879e",
  "id": 1
}
```

Response:
```json
{
  "jsonrpc": "2.0",
  "result": [
    {
      "itemid": "23296",
      "clock": "1351090996",
      "value": "0.0850",
      834
```
CHistory::get() in frontends/php/include/classes/api/services/CHistory.php.
**Host**

This class is designed to work with hosts.

Object references:

- Host
- Host inventory

Available methods:

- **host.create** - creating new hosts
- **host.delete** - deleting hosts
- **host.get** - retrieving hosts
- **host.massadd** - adding related objects to hosts
- **host.massremove** - removing related objects from hosts
- **host.massupdate** - replacing or removing related objects from hosts
- **host.update** - updating hosts

> **Host object**

The following objects are directly related to the host API.

Host

The host object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostid</td>
<td>string</td>
<td>(readonly) ID of the host.</td>
</tr>
<tr>
<td>host</td>
<td>string</td>
<td>Technical name of the host.</td>
</tr>
<tr>
<td>(required)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>available</td>
<td>integer</td>
<td>(readonly) Availability of Zabbix agent.</td>
</tr>
<tr>
<td>description</td>
<td>text</td>
<td>Description of the host.</td>
</tr>
<tr>
<td>disable_until</td>
<td>timestamp</td>
<td>(readonly) The next polling time of an unavailable Zabbix agent.</td>
</tr>
<tr>
<td>error</td>
<td>string</td>
<td>(readonly) Error text if Zabbix agent is unavailable.</td>
</tr>
<tr>
<td>errors_from</td>
<td>timestamp</td>
<td>(readonly) Time when Zabbix agent became unavailable.</td>
</tr>
<tr>
<td>flags</td>
<td>integer</td>
<td>(readonly) Origin of the host.</td>
</tr>
<tr>
<td>inventory_mode</td>
<td>integer</td>
<td>(writeonly) Host inventory population mode.</td>
</tr>
<tr>
<td>ipmi_authype</td>
<td>integer</td>
<td>IPMI authentication algorithm.</td>
</tr>
</tbody>
</table>

Possible values:

- **hostid**
  - 0 - (default) unknown;
  - 1 - available;
  - 2 - unavailable.

- **description**
  - 0 - (default) unknown;
  - 1 - available;
  - 2 - unavailable.

- **disable_until**
  - 0 - (default) unknown;
  - 1 - available;
  - 2 - unavailable.

- **error**
  - 0 - (default) unknown;
  - 1 - available;
  - 2 - unavailable.

- **errors_from**
  - 0 - (default) unknown;
  - 1 - available;
  - 2 - unavailable.

- **flags**
  - 0 - (default) unknown;
  - 1 - available;
  - 2 - unavailable.

- **inventory_mode**
  - 0 - (default) unknown;
  - 1 - available;
  - 2 - unavailable.

- **ipmi_authype**
  - 0 - (default) unknown;
  - 1 - available;
  - 2 - unavailable.

836
<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipmi_available</td>
<td>integer</td>
<td>(readonly) Availability of IPMI agent. Possible values are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - (default) unknown;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - available;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 - unavailable.</td>
</tr>
<tr>
<td>ipmi_disable_until</td>
<td>timestamp</td>
<td>(readonly) The next polling time of an unavailable IPMI agent.</td>
</tr>
<tr>
<td>ipmi_error</td>
<td>string</td>
<td>(readonly) Error text if IPMI agent is unavailable.</td>
</tr>
<tr>
<td>ipmi_errors_from</td>
<td>timestamp</td>
<td>(readonly) Time when IPMI agent became unavailable.</td>
</tr>
<tr>
<td>ipmi_password</td>
<td>string</td>
<td>IPMI password.</td>
</tr>
<tr>
<td>ipmi_privilege</td>
<td>integer</td>
<td>IPMI privilege level. Possible values are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - callback;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 - (default) user;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 - operator;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 - admin;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5 - OEM.</td>
</tr>
<tr>
<td>ipmi_username</td>
<td>string</td>
<td>IPMI username.</td>
</tr>
<tr>
<td>jmx_available</td>
<td>integer</td>
<td>(readonly) Availability of JMX agent. Possible values are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - (default) unknown;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - available;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 - unavailable.</td>
</tr>
<tr>
<td>jmx_disable_until</td>
<td>timestamp</td>
<td>(readonly) The next polling time of an unavailable JMX agent.</td>
</tr>
<tr>
<td>jmx_error</td>
<td>string</td>
<td>(readonly) Error text if JMX agent is unavailable.</td>
</tr>
<tr>
<td>jmx_errors_from</td>
<td>timestamp</td>
<td>(readonly) Time when JMX agent became unavailable.</td>
</tr>
<tr>
<td>maintenance_from</td>
<td>timestamp</td>
<td>(readonly) Starting time of the effective maintenance.</td>
</tr>
<tr>
<td>maintenance_status</td>
<td>integer</td>
<td>(readonly) Effective maintenance status. Possible values are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - (default) no maintenance;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - maintenance in effect.</td>
</tr>
<tr>
<td>maintenance_type</td>
<td>integer</td>
<td>(readonly) Effective maintenance type. Possible values are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - (default) maintenance with data collection;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - maintenance without data collection.</td>
</tr>
<tr>
<td>maintenanceid</td>
<td>string</td>
<td>(readonly) ID of the maintenance that is currently in effect on the host.</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>Visible name of the host.</td>
</tr>
<tr>
<td>proxy_hostid</td>
<td>string</td>
<td>ID of the proxy that is used to monitor the host.</td>
</tr>
<tr>
<td>snmp_available</td>
<td>integer</td>
<td>(readonly) Availability of SNMP agent. Possible values are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - (default) unknown;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - available;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 - unavailable.</td>
</tr>
<tr>
<td>snmp_disable_until</td>
<td>timestamp</td>
<td>(readonly) The next polling time of an unavailable SNMP agent.</td>
</tr>
<tr>
<td>snmp_error</td>
<td>string</td>
<td>(readonly) Error text if SNMP agent is unavailable.</td>
</tr>
<tr>
<td>snmp_errors_from</td>
<td>timestamp</td>
<td>(readonly) Time when SNMP agent became unavailable.</td>
</tr>
<tr>
<td>status</td>
<td>integer</td>
<td>Status and function of the host.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - (default) monitored host;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - unmonitored host.</td>
</tr>
</tbody>
</table>
### Property Description

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tls_connect</td>
<td>integer</td>
<td>Connections to host.</td>
</tr>
<tr>
<td>tls_accept</td>
<td>integer</td>
<td>Connections from host.</td>
</tr>
<tr>
<td>tls_issuer</td>
<td>string</td>
<td>Certificate issuer.</td>
</tr>
<tr>
<td>tls_subject</td>
<td>string</td>
<td>Certificate subject.</td>
</tr>
<tr>
<td>tls_psk_identity</td>
<td>string</td>
<td>PSK identity. Required if either tls_connect or tls_accept has PSK enabled. Do not put sensitive information in the PSK identity, it is transmitted unencrypted over the network to inform a receiver which PSK to use.</td>
</tr>
<tr>
<td>tls_psk</td>
<td>string</td>
<td>The preshared key, at least 32 hex digits. Required if either tls_connect or tls_accept has PSK enabled.</td>
</tr>
</tbody>
</table>

Note that for some methods (update, delete) the required/optional parameter combination is different.

### Host inventory

The host inventory object has the following properties.

**Note:** Each property has it's own unique ID number, which is used to associate host inventory fields with items.

<table>
<thead>
<tr>
<th>ID</th>
<th>Property</th>
<th>Type</th>
<th>Description</th>
<th>Maximum length</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>alias</td>
<td>string</td>
<td>Alias.</td>
<td>64 characters</td>
</tr>
<tr>
<td>11</td>
<td>asset_tag</td>
<td>string</td>
<td>Asset tag.</td>
<td>64 characters</td>
</tr>
<tr>
<td>28</td>
<td>chassis</td>
<td>string</td>
<td>Chassis.</td>
<td>64 characters</td>
</tr>
<tr>
<td>23</td>
<td>contact</td>
<td>string</td>
<td>Contact person.</td>
<td>Dependson the database used:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- 65535 characters for SQL databases</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- 2048 characters for Oracle databases</td>
</tr>
<tr>
<td>32</td>
<td>contract_number</td>
<td>string</td>
<td>Contract number.</td>
<td>64 characters</td>
</tr>
<tr>
<td>47</td>
<td>date_hw_decomm</td>
<td>string</td>
<td>HW decommissioning date.</td>
<td>64 characters</td>
</tr>
<tr>
<td>46</td>
<td>date_hw_expiry</td>
<td>string</td>
<td>HW maintenance expiry date.</td>
<td>64 characters</td>
</tr>
<tr>
<td>45</td>
<td>date_hw_install</td>
<td>string</td>
<td>HW installation date.</td>
<td>64 characters</td>
</tr>
<tr>
<td>44</td>
<td>date_hw_purchase</td>
<td>string</td>
<td>HW purchase date.</td>
<td>64 characters</td>
</tr>
<tr>
<td>34</td>
<td>deployment_status</td>
<td>string</td>
<td>Deployment status.</td>
<td>64 characters</td>
</tr>
<tr>
<td>14</td>
<td>hardware</td>
<td>string</td>
<td>Hardware.</td>
<td>255 characters</td>
</tr>
<tr>
<td>15</td>
<td>hardware_full</td>
<td>string</td>
<td>Detailed hardware.</td>
<td>Dependson the database used:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- 65535 characters for SQL databases</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- 2048 characters for Oracle databases</td>
</tr>
<tr>
<td>39</td>
<td>host_netmask</td>
<td>string</td>
<td>Host subnet mask.</td>
<td>39 characters</td>
</tr>
<tr>
<td>38</td>
<td>host_networks</td>
<td>string</td>
<td>Host networks.</td>
<td>Dependson the database used:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- 65535 characters for SQL databases</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- 2048 characters for Oracle databases</td>
</tr>
<tr>
<td>40</td>
<td>host_router</td>
<td>string</td>
<td>Host router.</td>
<td>39 characters</td>
</tr>
<tr>
<td>30</td>
<td>hw_arch</td>
<td>string</td>
<td>HW architecture.</td>
<td>32 characters</td>
</tr>
<tr>
<td>ID</td>
<td>Property</td>
<td>Type</td>
<td>Description</td>
<td>Maximum length</td>
</tr>
<tr>
<td>----</td>
<td>-------------------</td>
<td>---------</td>
<td>------------------------------------------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td>33</td>
<td>installer_name</td>
<td>string</td>
<td>Installer name.</td>
<td>64 characters</td>
</tr>
<tr>
<td>24</td>
<td>location</td>
<td>string</td>
<td>Location.</td>
<td>64 characters</td>
</tr>
<tr>
<td>25</td>
<td>location_lat</td>
<td>string</td>
<td>Location latitude.</td>
<td>64 characters</td>
</tr>
<tr>
<td>26</td>
<td>location_lon</td>
<td>string</td>
<td>Location longitude.</td>
<td>64 characters</td>
</tr>
<tr>
<td>12</td>
<td>macaddress_a</td>
<td>string</td>
<td>MAC address A.</td>
<td>64 characters</td>
</tr>
<tr>
<td>13</td>
<td>macaddress_b</td>
<td>string</td>
<td>MAC address B.</td>
<td>64 characters</td>
</tr>
<tr>
<td>29</td>
<td>model</td>
<td>string</td>
<td>Model.</td>
<td>64 characters</td>
</tr>
<tr>
<td>3</td>
<td>name</td>
<td>string</td>
<td>Name.</td>
<td>64 characters</td>
</tr>
<tr>
<td>27</td>
<td>notes</td>
<td>string</td>
<td>Notes.</td>
<td>64 characters</td>
</tr>
<tr>
<td>41</td>
<td>oob_ip</td>
<td>string</td>
<td>OOB IP address.</td>
<td>39 characters</td>
</tr>
<tr>
<td>42</td>
<td>oob_netmask</td>
<td>string</td>
<td>OOB host subnet mask.</td>
<td>39 characters</td>
</tr>
<tr>
<td>43</td>
<td>oob_router</td>
<td>string</td>
<td>OOB router.</td>
<td>39 characters</td>
</tr>
<tr>
<td>5</td>
<td>os</td>
<td>string</td>
<td>OS name.</td>
<td>64 characters</td>
</tr>
<tr>
<td>6</td>
<td>os_full</td>
<td>string</td>
<td>Detailed OS name.</td>
<td>255 characters</td>
</tr>
<tr>
<td>7</td>
<td>os_short</td>
<td>string</td>
<td>Short OS name.</td>
<td>64 characters</td>
</tr>
<tr>
<td>58</td>
<td>poc_1_cell</td>
<td>string</td>
<td>Primary POC mobile number.</td>
<td>64 characters</td>
</tr>
<tr>
<td>57</td>
<td>poc_1_email</td>
<td>string</td>
<td>Primary email.</td>
<td>128 characters</td>
</tr>
<tr>
<td>55</td>
<td>site_address_a</td>
<td>string</td>
<td>Site address A.</td>
<td>128 characters</td>
</tr>
<tr>
<td>48</td>
<td>site_address_b</td>
<td>string</td>
<td>Site address B.</td>
<td>128 characters</td>
</tr>
<tr>
<td>50</td>
<td>site_address_c</td>
<td>string</td>
<td>Site address C.</td>
<td>128 characters</td>
</tr>
<tr>
<td>51</td>
<td>site_city</td>
<td>string</td>
<td>Site city.</td>
<td>64 characters</td>
</tr>
<tr>
<td>53</td>
<td>site_country</td>
<td>string</td>
<td>Site country.</td>
<td>128 characters</td>
</tr>
<tr>
<td>56</td>
<td>site_notes</td>
<td>string</td>
<td>Site notes.</td>
<td>128 characters</td>
</tr>
<tr>
<td>59</td>
<td>poc_1_phone_a</td>
<td>string</td>
<td>Primary POC phone A.</td>
<td>64 characters</td>
</tr>
<tr>
<td>60</td>
<td>poc_1_phone_b</td>
<td>string</td>
<td>Primary POC phone B.</td>
<td>64 characters</td>
</tr>
<tr>
<td>62</td>
<td>poc_1_screen</td>
<td>string</td>
<td>Primary POC screen name.</td>
<td>64 characters</td>
</tr>
<tr>
<td>68</td>
<td>poc_2_cell</td>
<td>string</td>
<td>Secondary POC mobile number.</td>
<td>64 characters</td>
</tr>
<tr>
<td>65</td>
<td>poc_2_email</td>
<td>string</td>
<td>Secondary POC email.</td>
<td>128 characters</td>
</tr>
<tr>
<td>64</td>
<td>poc_2_name</td>
<td>string</td>
<td>Secondary POC name.</td>
<td>128 characters</td>
</tr>
<tr>
<td>70</td>
<td>poc_2_notes</td>
<td>string</td>
<td>Secondary POC notes.</td>
<td>64 characters</td>
</tr>
<tr>
<td>66</td>
<td>poc_2_phone_a</td>
<td>string</td>
<td>Secondary POC phone A.</td>
<td>64 characters</td>
</tr>
<tr>
<td>67</td>
<td>poc_2_phone_b</td>
<td>string</td>
<td>Secondary POC phone B.</td>
<td>64 characters</td>
</tr>
<tr>
<td>69</td>
<td>poc_2_screen</td>
<td>string</td>
<td>Secondary POC screen name.</td>
<td>64 characters</td>
</tr>
<tr>
<td>8</td>
<td>serialno_a</td>
<td>string</td>
<td>Serial number A.</td>
<td>64 characters</td>
</tr>
<tr>
<td>9</td>
<td>serialno_b</td>
<td>string</td>
<td>Serial number B.</td>
<td>64 characters</td>
</tr>
<tr>
<td>49</td>
<td>site_state</td>
<td>string</td>
<td>Site state.</td>
<td>64 characters</td>
</tr>
<tr>
<td>54</td>
<td>site_zip</td>
<td>string</td>
<td>Site ZIP/postal code.</td>
<td>64 characters</td>
</tr>
<tr>
<td>16</td>
<td>software</td>
<td>string</td>
<td>Software.</td>
<td>64 characters</td>
</tr>
<tr>
<td>18</td>
<td>software_app_a</td>
<td>string</td>
<td>Software application A.</td>
<td>64 characters</td>
</tr>
<tr>
<td>19</td>
<td>software_app_b</td>
<td>string</td>
<td>Software application B.</td>
<td>64 characters</td>
</tr>
<tr>
<td>20</td>
<td>software_app_c</td>
<td>string</td>
<td>Software application C.</td>
<td>64 characters</td>
</tr>
<tr>
<td>21</td>
<td>software_app_d</td>
<td>string</td>
<td>Software application D.</td>
<td>64 characters</td>
</tr>
<tr>
<td>22</td>
<td>software_app_e</td>
<td>string</td>
<td>Software application E.</td>
<td>64 characters</td>
</tr>
<tr>
<td>17</td>
<td>software_full</td>
<td>string</td>
<td>Software details.</td>
<td>64 characters</td>
</tr>
<tr>
<td>10</td>
<td>tag</td>
<td>string</td>
<td>Tag.</td>
<td>64 characters</td>
</tr>
<tr>
<td>1</td>
<td>type</td>
<td>string</td>
<td>Type.</td>
<td>64 characters</td>
</tr>
</tbody>
</table>

- Depending on the database used:
  - 65535 characters for SQL databases
  - 2048 characters for Oracle databases
### host.create

**Description**

Object host.create(object/array hosts)

This method allows to create new hosts.

**Parameters**

(object/array) Hosts to create.

Additionally to the standard host properties, the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>groups</td>
<td>object/array</td>
<td>Host groups to add the host to. The host groups must have the groupid property defined. Interfaces to be created for the host. Templates to be linked to the host. User macros to be created for the host. Host inventory properties.</td>
</tr>
<tr>
<td>interfaces</td>
<td>object/array</td>
<td></td>
</tr>
<tr>
<td>templates</td>
<td>object/array</td>
<td></td>
</tr>
<tr>
<td>macros</td>
<td>object/array</td>
<td></td>
</tr>
<tr>
<td>inventory</td>
<td>object</td>
<td></td>
</tr>
</tbody>
</table>

**Return values**

(object) Returns an object containing the IDs of the created hosts under the hostids property. The order of the returned IDs matches the order of the passed hosts.

**Examples**

Creating a host

Create a host called "Linux server" with an IP interface, add it to a group, link a template to it and set the MAC addresses in the host inventory.

**Request:**

```json
{
    "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"
    }
],
"templates": [
    {
        "templateid": "20045"
    }
],
"macros": [
    {
        "macro": "{$USER_ID}"
    }
],
"inventory_mode": 0,
"inventory": {
    "macaddress_a": "01234",
    "macaddress_b": "56768"
}
},
"auth": "038e1d7b1735c6a5436ee9eae095879e",
"id": 1
}

Response:

{
    "jsonrpc": "2.0",
    "result": {
        "hostids": [
            "107819"
        ]
    },
    "id": 1
}

See also

- Host group
- Template
- User macro
- Host interface
- Host inventory

Source

CHost::create() in frontends/php/include/classes/api/services/CHost.php.

host.delete

Description

object host.delete(array hosts)

This method allows to delete hosts.
Parameters
(array) IDs of hosts to delete.

Return values
(object) Returns an object containing the IDs of the deleted hosts under the hostids property.

Examples
Deleting multiple hosts
Delete two hosts.

Request:
```json
{
    "jsonrpc": "2.0",
    "method": "host.delete",
    "params": [
        "13",
        "32"
    ],
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:
```json
{
    "jsonrpc": "2.0",
    "result": {
        "hostids": [
            "13",
            "32"
        ]
    },
    "id": 1
}
```

Source
CHost::delete() in frontends/php/include/classes/api/services/CHost.php.

**host.get**

Description
integer/array host.get(object parameters)

The method allows to retrieve hosts according to the given parameters.

Parameters
(object) Parameters defining the desired output.

The method supports the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>groupids</td>
<td>string/array</td>
<td>Return only hosts that belong to the given groups.</td>
</tr>
<tr>
<td>applicationids</td>
<td>string/array</td>
<td>Return only hosts that have the given applications.</td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dserviceids</td>
<td>string/array</td>
<td>Return only hosts that are related to the given discovered services.</td>
</tr>
<tr>
<td>graphids</td>
<td>string/array</td>
<td>Return only hosts that have the given graphs.</td>
</tr>
<tr>
<td>hostids</td>
<td>string/array</td>
<td>Return only hosts with the given host IDs.</td>
</tr>
<tr>
<td>httptestids</td>
<td>string/array</td>
<td>Return only hosts that have the given web checks.</td>
</tr>
<tr>
<td>interfaceids</td>
<td>string/array</td>
<td>Return only hosts that use the given interfaces.</td>
</tr>
<tr>
<td>itemids</td>
<td>string/array</td>
<td>Return only hosts that have the given items.</td>
</tr>
<tr>
<td>maintenanceids</td>
<td>string/array</td>
<td>Return only hosts that are affected by the given maintenances.</td>
</tr>
<tr>
<td>monitored_hosts</td>
<td>flag</td>
<td>Return only monitored hosts.</td>
</tr>
<tr>
<td>proxy_hosts</td>
<td>flag</td>
<td>Return only proxies.</td>
</tr>
<tr>
<td>proxyids</td>
<td>string/array</td>
<td>Return only hosts that are monitored by the given proxies.</td>
</tr>
<tr>
<td>templated_hosts</td>
<td>flag</td>
<td>Return both hosts and templates.</td>
</tr>
<tr>
<td>templateids</td>
<td>string/array</td>
<td>Return only hosts that are linked to the given templates.</td>
</tr>
<tr>
<td>triggerids</td>
<td>string/array</td>
<td>Return only hosts that have the given triggers.</td>
</tr>
<tr>
<td>with_items</td>
<td>flag</td>
<td>Return only hosts that have items.</td>
</tr>
<tr>
<td>with_applications</td>
<td>flag</td>
<td>Overrides the with_monitored_items and with_simple_graph_items parameters.</td>
</tr>
<tr>
<td>with_graphs</td>
<td>flag</td>
<td>Return only hosts that have applications.</td>
</tr>
<tr>
<td>with_httptests</td>
<td>flag</td>
<td>Return only hosts that have graphs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Overrides the with_monitored_httptests parameter.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-----------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>with_monitored_httpsts</td>
<td></td>
<td>Return only hosts that have enabled web checks.</td>
</tr>
<tr>
<td>with_monitored_items</td>
<td></td>
<td>Return only hosts that have enabled items.</td>
</tr>
<tr>
<td>with_monitored_triggers</td>
<td></td>
<td>Overrides the with_simple_graph_items parameter. Return only hosts that have enabled triggers. All of the items used in the trigger must also be enabled.</td>
</tr>
<tr>
<td>with_simple_graphflagms</td>
<td></td>
<td>Return only hosts that have items with numeric type of information.</td>
</tr>
<tr>
<td>with_triggers</td>
<td>flag</td>
<td>Return only hosts that have triggers.</td>
</tr>
<tr>
<td>withInventory</td>
<td>flag</td>
<td>Return only hosts that have inventory data.</td>
</tr>
<tr>
<td>selectGroups</td>
<td>query</td>
<td>Return a groups property with host groups that the host belongs to.</td>
</tr>
<tr>
<td>selectApplications</td>
<td>query</td>
<td>Return an applications property with host applications.</td>
</tr>
<tr>
<td>selectDiscoveries</td>
<td>query</td>
<td>Supports count. Return a discoveries property with host low-level discovery rules.</td>
</tr>
<tr>
<td>selectDiscoveryRule</td>
<td>query</td>
<td>Supports count. Return a discoveryRule property with the low-level discovery rule that created the host (from host prototype in VMware monitoring).</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>selectGraphs</td>
<td>query</td>
<td>Return a graphs property with host graphs. Supports count.</td>
</tr>
<tr>
<td>selectHostDiscovery</td>
<td>query</td>
<td>Return a hostDiscovery property with host discovery object data. The host discovery object links a discovered host to a host prototype or a host prototypes to an LLD rule and has the following properties: host, hostid, parent_hostid, parent_itemid, lastcheck, ts_delete.</td>
</tr>
<tr>
<td>selectHttpTests</td>
<td>query</td>
<td>Return an httpTests property with host web scenarios. Supports count.</td>
</tr>
<tr>
<td>selectInterfaces</td>
<td>query</td>
<td>Return an interfaces property with host interfaces. Supports count.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>selectInventory</td>
<td>query</td>
<td>Return an inventory property with host inventory data.</td>
</tr>
<tr>
<td>selectItems</td>
<td>query</td>
<td>Return an items property with host items. Supports count.</td>
</tr>
<tr>
<td>selectMacros</td>
<td>query</td>
<td>Return a macros property with host macros.</td>
</tr>
<tr>
<td>selectParentTemplates</td>
<td>query</td>
<td>Return a parentTemplates property with templates that the host is linked to. Supports count.</td>
</tr>
<tr>
<td>selectScreens</td>
<td>query</td>
<td>Return a screens property with host screens. Supports count.</td>
</tr>
<tr>
<td>selectTriggers</td>
<td>query</td>
<td>Return a triggers property with host triggers. Supports count.</td>
</tr>
<tr>
<td>filter</td>
<td>object</td>
<td>Return only those results that exactly match the given filter. Accepts an array, where the keys are property names, and the values are either a single value or an array of values to match against. Allows filtering by interface properties. Doesn’t work for text fields.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>limitSelects</td>
<td>integer</td>
<td>Limits the number of records returned by subselects. Applies to the following subselects: selectParentTemplates - results will be sorted by host; selectInterfaces; selectItems - sorted by name; selectDiscoveries - sorted by name; selectTriggers - sorted by description; selectGraphs - sorted by name; selectApplications - sorted by name; selectScreens - sorted by name.</td>
</tr>
<tr>
<td>search</td>
<td>object</td>
<td>Return results that match the given pattern (case-insensitive). Accepts an array, where the keys are property names, and the values are strings to search for. If no additional options are given, this will perform a LIKE &quot;%…%&quot; search. Allows searching by interface properties. Works only for string and text fields.</td>
</tr>
<tr>
<td>searchInventory</td>
<td>object</td>
<td>Return only hosts that have inventory data matching the given wildcard search. This parameter is affected by the same additional parameters as search.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Sort the result by the given properties. Possible values are: hostid, host, name, status.</td>
</tr>
<tr>
<td>countOutput</td>
<td>boolean</td>
<td>These parameters being common for all get methods are described in detail in the reference commentary.</td>
</tr>
<tr>
<td>editable</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>excludeSearch</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>limit</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>output</td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>preservekeys</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>searchByAny</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>searchWildcardsEnabled</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>sortorder</td>
<td>string/array</td>
<td></td>
</tr>
<tr>
<td>startSearch</td>
<td>boolean</td>
<td></td>
</tr>
</tbody>
</table>

Return values

(integer/array) Returns either:
- an array of objects;
- the count of retrieved objects, if the countOutput parameter has been used.

Examples

Retrieving data by name

Retrieve all data about two hosts named "Zabbix server" and "Linux server".

Request:
```json
{
    "jsonrpc": "2.0",
    "method": "host.get",
    "params": {
        "filter": {
            "host": ["Zabbix server", "Linux server"]
        }
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:
```json
{
    "jsonrpc": "2.0",
    "result": [
        {
            "maintenances": [],
            "hostid": "10160",
            "proxy_hostid": "0",
            "host": "Zabbix server",
```
"status": "0",
"disable_until": "0",
"error": "",
"available": "0",
"errors_from": "0",
"lastaccess": "0",
"ipmi_authtype": "-1",
"ipmi_privilege": "2",
"ipmi_username": "",
"ipmi_password": "",
"ipmi_disable_until": "0",
"ipmi_available": "0",
"snmp_disable_until": "0",
"snmp_available": "0",
"maintenanceid": "0",
"maintenance_status": "0",
"maintenance_type": "0",
"maintenance_from": "0",
"ipmi_errors_from": "0",
"snmp_errors_from": "0",
"ipmi_error": "",
"snmp_error": "",
"jmx_disable_until": "0",
"jmx_available": "0",
"jmx_errors_from": "0",
"jmx_error": "",
"name": "Zabbix server",
"description": "The Zabbix monitoring server.",
"tls_connect": "1",
"tls_accept": "1",
"tls_issuer": "",
"tls_subject": "",
"tls_psk_identity": "",
"tls_psk": "",

"hostid": "10167",
"proxy_hostid": "0",
"host": "Linux server",
"status": "0",
"disable_until": "0",
"error": "",
"available": "0",
"errors_from": "0",
"lastaccess": "0",
"ipmi_authtype": "-1",
"ipmi_privilege": "2",
"ipmi_username": "",
"ipmi_password": "",
"ipmi_disable_until": "0",
"ipmi_available": "0",
"snmp_disable_until": "0",
"snmp_available": "0",
"maintenanceid": "0",
"maintenance_status": "0",
"maintenance_type": "0",
"maintenance_from": "0",
"ipmi_errors_from": "0",
"snmp_errors_from": "0",
"ipmi_error": "",
"snmp_error": "",
"jmx_disable_until": "0",
"jmx_available": "0",
"jmx_errors_from": "0",
"jmx_error": "",
"name": "Linux server",
"description": "",
"tls_connect": "1",
"tls_accept": "1",
"tls_issuer": "",
"tls_subject": "",
"tls_psk_identity": "",
"tls_psk": "
},
"id": 1
}

Retrieving host groups

Retrieve names of the groups host "Zabbix server" is member of, but no host details themselves.

Request:
{
    "jsonrpc": "2.0",
    "method": "host.get",
    "params": {
        "output": ["hostid"],
        "selectGroups": "extend",
        "filter": {
            "host": [
                "Zabbix server"
            ]
        }
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 2
}

Response:
{
    "jsonrpc": "2.0",
    "result": [
        {
            "hostid": "10085",
            "groups": [
                {
                    "groupid": "2",
                    "name": "Linux servers",
                    "internal": "0",
                    "flags": "0"
                },
                {
                    "groupid": "4",
                    "name": "Zabbix servers",
                    "internal": "0",
                    "flags": "0"
                }
            ]
        },
        "id": 2
    }
}

Retrieving linked templates
Retrieve the IDs and names of templates linked to host "10084".

Request:

```
{  
"jsonrpc": "2.0",
"method": "host.get",
"params": {  
"output": ["hostid"],
"selectParentTemplates": [  
  "templateid",
  "name"
],
"hostids": "10084"
},
"id": 1,
"auth": "70785d2b494a7302309b48afcdb3a401"
}
```

Response:

```
{  
"jsonrpc": "2.0",
"result": [  
  {  
"hostid": "10084",
"parentTemplates": [  
  {  
"name": "Template OS Linux",
"templateid": "10001"
  },
  {  
"name": "Template App Zabbix Server",
"templateid": "10047"
  }
  
  ]
  
  },
  "id": 1
}
```

Searching by host inventory data

Retrieve hosts that contain "Linux" in the host inventory "OS" field.

Request:

```
{  
"jsonrpc": "2.0",
"method": "host.get",
"params": {  
"output": ["host"],
"selectInventory": [  
  "os"
],
"searchInventory": {  
  "os": "Linux"
}
},
"id": 2,
"auth": "7f9e00124c75e8f25facd5c093f3e9a0"
}
```

Response:

```
851
```
See also

- Host group
- Template
- User macro
- Host interface

Source

CHost::get() in frontends/php/include/classes/api/services/CHost.php.

**host.massadd**

**Description**

`object host.massadd(object parameters)`

This method allows to simultaneously add multiple related objects to all the given hosts.

**Parameters**

(object) Parameters containing the IDs of the hosts to update and the objects to add to all the hosts.

The method accepts the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>hosts</strong></td>
<td>object/array</td>
<td>Hosts to be updated. The hosts must have the hostid property defined.</td>
</tr>
<tr>
<td>(required)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>groups</td>
<td>object/array</td>
<td>Host groups to add to the given hosts. The host groups must have the groupid property defined.</td>
</tr>
<tr>
<td>interfaces</td>
<td>object/array</td>
<td>Host interfaces to be created for the given hosts.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>macros</td>
<td>object/array</td>
<td>User macros to be created for the given hosts.</td>
</tr>
<tr>
<td>templates</td>
<td>object/array</td>
<td>Templates to link to the given hosts.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The templates must have the <code>templateid</code> property defined.</td>
</tr>
</tbody>
</table>

Return values

(\textit{object}) Returns an object containing the IDs of the updated hosts under the `hostids` property.

Examples

Adding macros

Add two new macros to two hosts.

Request:

```json
{
   "jsonrpc": "2.0",
   "method": "host.massadd",
   "params": {
      "hosts": [
         {
            "hostid": "10160"
         },
         {
            "hostid": "10167"
         }
      ],
      "macros": [
         {
            "macro": "\{TEST1\}"
         },
         {
            "macro": "\{TEST2\}"
         }
      ]
   },
   "auth": "038e1d7b1735c6a5436ee9eae095879e",
   "id": 1
}
```

Response:

```json
{
   "jsonrpc": "2.0",
   "result": {
      "hostids": [
         "10160",
         "10167"
      ],
      "id": 1
   }
}
```

See also

853
host.update
Host group
Template
User macro
Host interface

Source
CHost::massAdd() in frontends/php/include/classes/api/services/CHost.php.

**host.massremove**

Description

object host.massremove(object parameters)

This method allows to remove related objects from multiple hosts.

Parameters

(object) Parameters containing the IDs of the hosts to update and the objects that should be removed.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostids</td>
<td>string/array</td>
<td>IDs of the hosts to be updated.</td>
</tr>
<tr>
<td>(required)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>groupids</td>
<td>string/array</td>
<td>Host groups to remove the given hosts from.</td>
</tr>
<tr>
<td>interfaces</td>
<td>object/array</td>
<td>Host interfaces to remove from the given hosts.</td>
</tr>
<tr>
<td>macros</td>
<td>string/array</td>
<td>User macros to delete from the given hosts.</td>
</tr>
<tr>
<td>templateids</td>
<td>string/array</td>
<td>Templates to unlink from the given hosts.</td>
</tr>
<tr>
<td>templateids_clear</td>
<td>string/array</td>
<td>Templates to unlink and clear from the given hosts.</td>
</tr>
</tbody>
</table>

Return values

(object) Returns an object containing the IDs of the updated hosts under the **hostids** property.

Examples

Unlinking templates

Unlink a template from two hosts and delete all of the templated entities.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "host.massremove",
    "params": {
        "hostids": ["69665", "69666"],
        "templateids_clear": "325"
    },
}
```
Response:
{
    "jsonrpc": "2.0",
    "result": {
        "hostids": [
            "69665",
            "69666"
        ],
        "id": 1
    }
}

See also
• host.update
• Usermacro
• Host interface

Source
CHost::massRemove() in frontends/php/include/classes/api/services/CHost.php.

host.massupdate

Description

object host.massupdate(object parameters)

This method allows to simultaneously replace or remove related objects and update properties on multiple hosts.

Parameters

(object) Parameters containing the IDs of the hosts to update and the properties that should be updated.

Additionally to the standard host properties, the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hosts</td>
<td>object/array</td>
<td>Hosts to be updated.</td>
</tr>
<tr>
<td>groups</td>
<td>object/array</td>
<td>Host groups to replace the current host groups the hosts belong to.</td>
</tr>
<tr>
<td>interfaces</td>
<td>object/array</td>
<td>Host interfaces to replace the current host interfaces on the given hosts.</td>
</tr>
</tbody>
</table>
### Parameter Table

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>inventory</td>
<td>object</td>
<td>Host inventory properties.</td>
</tr>
<tr>
<td>inventory_mode</td>
<td>integer</td>
<td>Host inventory mode cannot be updated using the inventory parameter, use inventory_mode instead.</td>
</tr>
<tr>
<td>macros</td>
<td>object/array</td>
<td>User macros to replace the current user macros on the given hosts.</td>
</tr>
<tr>
<td>templates</td>
<td>object/array</td>
<td>Templates to replace the currently linked templates on the given hosts.</td>
</tr>
<tr>
<td>templates_clear</td>
<td>object/array</td>
<td>Templates to unlink and clear from the given hosts.</td>
</tr>
</tbody>
</table>

### Return values

**(object)** Returns an object containing the IDs of the updated hosts under the `host_ids` property.

### Examples

**Enabling multiple hosts**

Enable monitoring of two hosts, i.e., set their status to 0.

**Request:**

```json
{
    "jsonrpc": "2.0",
    "method": "host.massupdate",
    "params": {
        "hosts": [
            {
                "hostid": "69665"
            },
            {
                "hostid": "69666"
            }
        ]
    }
}
```
"hostid": "69666"

],
"status": 0
},
"auth": "038e1d7b1735c6a5436ee9eae095879e",
"id": 1
}

Response:
{
  "jsonrpc": "2.0",
  "result": {
    "hostids": [
      "69665",
      "69666"
    ],
  },
  "id": 1
}

See also
• host.update
• host.massadd
• host.massremove
• Host group
• Template
• User macro
• Host interface

Source
CHost::massUpdate() in frontends/php/include/classes/api/services/CHost.php.

**host.update**

Description
object host.update(object/array hosts)

This method allows to update existing hosts.

Parameters
(object/array) Host properties to be updated.

The hostid property must be defined for each host, all other properties are optional. Only the given properties will be updated, all others will remain unchanged.

Note, however, that updating the host technical name will also update the host’s visible name (if not given or empty) by the host’s technical name value.

Additionally to the standard host properties, the method accepts the following parameters.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>groups</td>
<td>object/array</td>
<td>Host groups to replace the current host groups the host belongs to. The host groups must have the groupid property defined. All host groups that are not listed in the request will be unlinked.</td>
</tr>
<tr>
<td>interfaces</td>
<td>object/array</td>
<td>Host interfaces to replace the current host interfaces. All interfaces that are not listed in the request will be removed.</td>
</tr>
<tr>
<td>inventory</td>
<td>object</td>
<td>Host inventory properties.</td>
</tr>
<tr>
<td>macros</td>
<td>object/array</td>
<td>User macros to replace the current user macros. All macros that are not listed in the request will be removed.</td>
</tr>
<tr>
<td>templates</td>
<td>object/array</td>
<td>Templates to replace the currently linked templates. All templates that are not listed in the request will be only unlinked. The templates must have the templateid property defined.</td>
</tr>
<tr>
<td>templates_clear</td>
<td>object/array</td>
<td>Templates to unlink and clear from the host. The templates must have the templateid property defined.</td>
</tr>
</tbody>
</table>

**Note:**
As opposed to the Zabbix frontend, when name (visible host name) is the same as host (technical host name), updating host via API will not automatically update name. Both properties need to be updated explicitly.
Return values

(object) Returns an object containing the IDs of the updated hosts under the `hostids` property.

Examples

Enabling a host

Enable host monitoring, i.e. set its status to 0.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "host.update",
    "params": {
        "hostid": "10126",
        "status": 0
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "hostids": [
            "10126"
        ]
    },
    "id": 1
}
```

Unlinking templates

Unlink and clear two templates from host.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "host.update",
    "params": {
        "hostid": "10126",
        "templates_clear": [
            {
                "templateid": "10124"
            },
            {
                "templateid": "10125"
            }
        ]
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "hostids": [
            "10126"
        ]
    }
}
```
Updating host macros

Replace all host macros with two new ones.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "host.update",
    "params": {
        "hostid": "10126",
        "macros": [
            {
                "macro": "\{$PASS}\",
                "value": "password"
            },
            {
                "macro": "\{$DISC}\",
                "value": "sda"
            }
        ]
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "hostids": [
            "10126"
        ]
    },
    "id": 1
}
```

Updating host inventory

Change inventory mode and add location

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "host.update",
    "params": {
        "hostid": "10387",
        "inventory_mode": 0,
        "inventory": {
            "location": "Latvia, Riga"
        }
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "hostids": [
            "10387"
        ]
    },
    "id": 1
}
```
See also

- host.massadd
- host.massupdate
- host.massremove
- Host group
- Template
- User macro
- Host interface
- Host inventory

Source

CHost::update() in frontends/php/include/classes/api/services/CHost.php.

**Host group**

This class is designed to work with host groups.

Object references:

- Host group

Available methods:

- **hostgroup.create** - creating new host groups
- **hostgroup.delete** - deleting host groups
- **hostgroup.get** - retrieving host groups
- **hostgroup.massadd** - adding related objects to host groups
- **hostgroup.massremove** - removing related objects from host groups
- **hostgroup.massupdate** - replacing or removing related objects from host groups
- **hostgroup.update** - updating host groups

> **Host group object**

The following objects are directly related to the hostgroup API.

Host group

The host group object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>groupid</td>
<td>string</td>
<td>(readonly) ID of the host group.</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>Name of the host group.</td>
</tr>
<tr>
<td>(required)</td>
<td></td>
<td>(readonly) Origin of the host group.</td>
</tr>
<tr>
<td>flags</td>
<td>integer</td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - a plain host group;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 - a discovered host group.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>internal</td>
<td>integer</td>
<td>Whether the group is used internally by the system. An internal group cannot be deleted. (readonly) Possible values: 0 - (default) not internal; 1 - internal.</td>
</tr>
</tbody>
</table>

Note that for some methods (update, delete) the required/optional parameter combination is different.

**hostgroup.create**

Description

`object hostgroup.create(object/array hostGroups)`

This method allows to create new host groups.

Parameters

`(object/array)` Host groups to create. The method accepts host groups with the standard host group properties.

Return values

`(object)` Returns an object containing the IDs of the created host groups under the groupids property. The order of the returned IDs matches the order of the passed host groups.

Examples

Creating a host group

Create a host group called “Linux servers”.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "hostgroup.create",
    "params": {
        "name": "Linux servers"
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "groupids": [
            "107819"
        ],
    },
    "id": 1
}
```

Source

CHostGroup::create() in frontends/php/include/classes/api/services/CHostGroup.php.
**hostgroup.delete**

Description

object hostgroup.delete(array hostGroupIds)

This method allows to delete host groups.

A host group can not be deleted if:

- it contains hosts that belong to this group only;
- it is marked as internal;
- it is used by a host prototype;
- it is used in a global script;
- it is used in a correlation condition.

Parameters

(array) IDs of the host groups to delete.

Return values

(object) Returns an object containing the IDs of the deleted host groups under the `groupids` property.

Examples

Deleting multiple host groups

Delete two host groups.

Request:

```json
{
   "jsonrpc": "2.0",
   "method": "hostgroup.delete",
   "params": [
      "107824",
      "107825"
   ],
   "auth": "3a57200802b24cda67c4e4010b50c065",
   "id": 1
}
```

Response:

```json
{
   "jsonrpc": "2.0",
   "result": {
      "groupids": [
         "107824",
         "107825"
      ]
   },
   "id": 1
}
```

Source

CHostGroup::delete() in frontends/php/include/classes/api/services/CHostGroup.php.

**hostgroup.get**

Description

integer/array hostgroup.get(object parameters)

The method allows to retrieve host groups according to the given parameters.

Parameters

(object) Parameters defining the desired output.

The method supports the following parameters.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>graphids</td>
<td>string/array</td>
<td>Return only host groups that contain hosts or templates with the given graphs.</td>
</tr>
<tr>
<td>groupids</td>
<td>string/array</td>
<td>Return only host groups with the given host group IDs.</td>
</tr>
<tr>
<td>hostids</td>
<td>string/array</td>
<td>Return only host groups that contain the given hosts.</td>
</tr>
<tr>
<td>maintenanceids</td>
<td>string/array</td>
<td>Return only host groups that are affected by the given maintenance.</td>
</tr>
<tr>
<td>monitored_hosts</td>
<td>flag</td>
<td>Return only host groups that contain monitored hosts.</td>
</tr>
<tr>
<td>real_hosts</td>
<td>flag</td>
<td>Return only host groups that contain hosts.</td>
</tr>
<tr>
<td>templated_hosts</td>
<td>flag</td>
<td>Return only host groups that contain templates.</td>
</tr>
<tr>
<td>templateids</td>
<td>string/array</td>
<td>Return only host groups that contain the given templates.</td>
</tr>
<tr>
<td>triggerids</td>
<td>string/array</td>
<td>Return only host groups that contain hosts or templates with the given triggers.</td>
</tr>
<tr>
<td>with_applications</td>
<td>flag</td>
<td>Return only host groups that contain hosts with applications.</td>
</tr>
<tr>
<td>with_graphs</td>
<td>flag</td>
<td>Return only host groups that contain hosts with graphs.</td>
</tr>
<tr>
<td>with_hosts_and_templates</td>
<td>flag</td>
<td>Return only host groups that contain hosts or templates.</td>
</tr>
<tr>
<td>with_httptests</td>
<td>flag</td>
<td>Return only host groups that contain hosts with web checks.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Overrides the with_monitored_httptests parameter.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>with_items flag</td>
<td>flag</td>
<td>Return only host groups that contain hosts or templates with items. Overrides the with_monitored_items and with_simple_graph_items parameters.</td>
</tr>
<tr>
<td>with_monitored_http flag</td>
<td></td>
<td>Return only host groups that contain hosts with enabled web checks.</td>
</tr>
<tr>
<td>with_monitored_items flag</td>
<td></td>
<td>Return only host groups that contain hosts or templates with enabled items. Overrides the with_simple_graph_items parameter.</td>
</tr>
<tr>
<td>with_monitored_triggers flag</td>
<td></td>
<td>Return only host groups that contain hosts with enabled triggers. All of the items used in the trigger must also be enabled.</td>
</tr>
<tr>
<td>with_simple_graph_items flag</td>
<td></td>
<td>Return only host groups that contain hosts with numeric items.</td>
</tr>
<tr>
<td>with_triggers flag</td>
<td>flag</td>
<td>Return only host groups that contain hosts with triggers. Overrides the with_monitored_triggers parameter.</td>
</tr>
<tr>
<td>selectDiscoveryRule query</td>
<td></td>
<td>Return the LLD rule that created the host group in the discoveryRule property.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>selectGroupDiscovery</td>
<td>query</td>
<td>Return the host group discovery object in the groupDiscovery property.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The host group discovery object links a discovered host group to a host group prototype and has the following properties: groupid - (string)</td>
</tr>
<tr>
<td>selectHosts</td>
<td>query</td>
<td>Supports count. Return the hosts that belong to the host group in the hosts property.</td>
</tr>
<tr>
<td>selectTemplates</td>
<td>query</td>
<td>Supports count. Return the templates that belong to the host group in the templates property.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>limitSelects</td>
<td>integer</td>
<td>Limits the number of records returned by subselects.</td>
</tr>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Sort the result by the given properties. Possible values are: groupid, name.</td>
</tr>
<tr>
<td>countOutput</td>
<td>boolean</td>
<td>These parameters being common for all get methods are described in detail in the reference commentary page.</td>
</tr>
<tr>
<td>editable</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>excludeSearch</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>filter</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>limit</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>output</td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>preservekeys</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>search</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>searchByAny</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>searchWildcardsEnabled</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>sortOrder</td>
<td>string/array</td>
<td></td>
</tr>
<tr>
<td>startSearch</td>
<td>boolean</td>
<td></td>
</tr>
</tbody>
</table>

Return values

(integer/array) Returns either:

- an array of objects;
- the count of retrieved objects, if the countOutput parameter has been used.

Examples

Retrieving data by name

Retrieve all data about two host groups named “Zabbix servers” and “Linux servers”.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "hostgroup.get",
    "params": {
        "output": "extend",
        "filter": {
            "name": ["Zabbix servers",
```
Response:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "groupid": "2",
            "name": "Linux servers",
            "internal": "0"
        },
        {
            "groupid": "4",
            "name": "Zabbix servers",
            "internal": "0"
        }
    ],
    "id": 1
}
```

See also
- Host
- Template

Source
CHostGroup::get() in frontends/php/include/classes/api/services/CHostGroup.php.

**hostgroup.massadd**

Description
object hostgroup.massadd(object parameters)

This method allows to simultaneously add multiple related objects to all the given host groups.

Parameters
(object) Parameters containing the IDs of the host groups to update and the objects to add to all the host groups.

The method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>groups</td>
<td>object/array</td>
<td>Host groups to be updated. Host groups must have the groupid property defined.</td>
</tr>
<tr>
<td></td>
<td>(required)</td>
<td></td>
</tr>
<tr>
<td>hosts</td>
<td>object/array</td>
<td>Hosts to add to all host groups. The hosts must have the hostid property defined.</td>
</tr>
</tbody>
</table>
## Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>templates</td>
<td>object/array</td>
<td>Templates to add to all host groups. The templates must have the templateid property defined.</td>
</tr>
</tbody>
</table>

## Return values

(-object) Returns an object containing the IDs of the updated host groups under the groupids property.

## Examples

### Adding hosts to host groups

Add two hosts to host groups with IDs 5 and 6.

**Request:**

```json
{
    "jsonrpc": "2.0",
    "method": "hostgroup.massadd",
    "params": {
        "groups": [
            {
                "groupid": "5"
            },
            {
                "groupid": "6"
            }
        ],
        "hosts": [
            {
                "hostid": "30050"
            },
            {
                "hostid": "30001"
            }
        ]
    },
    "auth": "f223adf833b2bf2ff38574a67bba6372",
    "id": 1
}
```

**Response:**

```json
{
    "jsonrpc": "2.0",
    "result": {
        "groupids": [
            "5",
            "6"
        ]
    },
    "id": 1
}
```

## See also

- Host
- Template

## Source

CHostGroup::massAdd() in frontends/php/include/classes/api/services/CHostGroup.php.
hostgroup.massremove

Description

object hostgroup.massremove(object parameters)

This method allows to remove related objects from multiple host groups.

Parameters

(object) Parameters containing the IDs of the host groups to update and the objects that should be removed.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>groupids</td>
<td>string/array</td>
<td>IDs of the host groups to be updated.</td>
</tr>
<tr>
<td>hostids</td>
<td>string/array</td>
<td>Hosts to remove from all host groups.</td>
</tr>
<tr>
<td>templateids</td>
<td>string/array</td>
<td>Templates to remove from all host groups.</td>
</tr>
</tbody>
</table>

Return values

(object) Returns an object containing the IDs of the updated host groups under the groupids property.

Examples

Removing hosts from host groups

Remove two hosts from the given host groups.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "hostgroup.massremove",
    "params": {
        "groupids": [
            "5",
            "6"
        ],
        "hostids": [
            "30050",
            "30001"
        ]
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "groupids": [
            "5",
            "6"
        ]
    },
    "id": 1
}
```

Source

CHostGroup::massRemove() in frontends/php/include/classes/api/services/CHostGroup.php.

hostgroup.massupdate

Description
object hostgroup.massupdate(object parameters)

This method allows to simultaneously replace or remove related objects for multiple host groups.

Parameters

(object) Parameters containing the IDs of the host groups to update and the objects that should be updated.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>groups</td>
<td>object/array</td>
<td>Host groups to be updated. The host groups must have the groupid property defined.</td>
</tr>
<tr>
<td>hosts</td>
<td>object/array</td>
<td>Hosts to replace the current hosts on the given host groups. The hosts must have the hostid property defined.</td>
</tr>
<tr>
<td>templates</td>
<td>object/array</td>
<td>Templates to replace the current templates on the given host groups. The templates must have the templateid property defined.</td>
</tr>
</tbody>
</table>

Return values

(object) Returns an object containing the IDs of the updated host groups under the groupids property.

Examples

Replacing hosts in a host group

Replace all hosts in the host group with ID.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "hostgroup.massupdate",
    "params": {
        "groups": [
            {
                "groupid": "6"
            }
        ],
        "hosts": [
            {
                "hostid": "30050"
            }
        ],
        "auth": "f223adf833b2bf2ff38574a67bba6372",
        "id": 1
    }
}
```

Response:
See also

- hostgroup.update
- hostgroup.massadd
- Host
- Template

Source

CHostGroup::massUpdate() in frontends/php/include/classes/api/services/CHostGroup.php.

hostgroup.update

Description

object hostgroup.update(object/array hostGroups)

This method allows to update existing host groups.

Parameters

(object/array) **Host group properties** to be updated.

The **groupid** property must be defined for each host group, all other properties are optional. Only the given properties will be updated, all others will remain unchanged.

Return values

(object) Returns an object containing the IDs of the updated host groups under the groupids property.

Examples

Renaming a host group

Rename a host group to "Linux hosts."

Request:

```
{
   "jsonrpc": "2.0",
   "method": "hostgroup.update",
   "params": {
      "groupid": "7",
      "name": "Linux hosts"
   },
   "auth": "700ca65537074ec963db7efabda78259",
   "id": 1
}
```

Response:

```
{
   "jsonrpc": "2.0",
   "result": {
      "groupids": ["7"
   },
   "id": 1
}
```
Host interface

This class is designed to work with host interfaces.

Object references:

- Host interface

Available methods:

- hostinterface.create - creating new host interfaces
- hostinterface.delete - deleting host interfaces
- hostinterface.get - retrieving host interfaces
- hostinterface.massadd - adding host interfaces to hosts
- hostinterface.massremove - removing host interfaces from hosts
- hostinterface.replacehostinterfaces - replacing host interfaces on a host
- hostinterface.update - updating host interfaces

> Host interface object

The following objects are directly related to the hostinterface API.

Host interface

The host interface object has the following properties.

**Attention:**
Note that both IP and DNS are required. If you do not want to use DNS, set it to an empty string.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interfaceid</td>
<td>string</td>
<td>(readonly) ID of the interface.</td>
</tr>
<tr>
<td>dns</td>
<td>string</td>
<td>DNS name used by the interface. Can be empty if the connection is made via IP.</td>
</tr>
<tr>
<td>(required)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>hostid</td>
<td>string</td>
<td>ID of the host the interface belongs to.</td>
</tr>
<tr>
<td>(required)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ip</td>
<td>string</td>
<td>IP address used by the interface. Can be empty if the connection is made via DNS.</td>
</tr>
<tr>
<td>(required)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>main</td>
<td>integer</td>
<td>Whether the interface is used as default on the host. Only one interface of some type can be set as default on a host. Possible values are: 0 - not default; 1 - default.</td>
</tr>
<tr>
<td>port</td>
<td>string</td>
<td>Port number used by the interface. Can contain user macros. Interface type.</td>
</tr>
<tr>
<td>type</td>
<td>integer</td>
<td>Possible values are: 1 - agent; 2 - SNMP; 3 - IPMI; 4 - JMX.</td>
</tr>
<tr>
<td>useip</td>
<td>integer</td>
<td>Whether the connection should be made via IP. Possible values are: 0 - connect using host DNS name; 1 - connect using host IP address for this host interface.</td>
</tr>
<tr>
<td>bulk</td>
<td>integer</td>
<td>Whether to use bulk SNMP requests. Possible values are: 0 - don’t use bulk requests; 1 - (default) use bulk requests.</td>
</tr>
</tbody>
</table>

Note that for some methods (update, delete) the required/optional parameter combination is different.

**hostinterface.create**

Description

object hostinterface.create(object/array hostInterfaces)

This method allows to create new host interfaces.

Parameters

(object/array) Host interfaces to create. The method accepts host interfaces with the standard host interface properties.
Return values

(object) Returns an object containing the IDs of the created host interfaces under the `interfaceids` property. The order of the returned IDs matches the order of the passed host interfaces.

Examples

Create a new interface

Create a secondary IP agent interface on host "30052."

Request:

```json
{  "jsonrpc": "2.0",  "method": "hostinterface.create",  "params": {    "hostid": "30052",    "dns": "",    "ip": "127.0.0.1",    "main": 0,    "port": "10050",    "type": 1,    "useip": 1  },  "auth": "038e1d7b1735c6a5436ee9eae095879e",  "id": 1}
```

Response:

```json
{  "jsonrpc": "2.0",  "result": {    "interfaceids": [      "30062"    ]  },  "id": 1}
```

See also

- `hostinterface.massadd`
- `host.massadd`

Source

`CHostInterface::create()` in frontends/php/include/classes/api/services/CHostInterface.php.

### hostinterface.delete

Description

object hostinterface.delete(array hostInterfaceIds)

This method allows to delete host interfaces.

Parameters

(array) IDs of the host interfaces to delete.

Return values

(object) Returns an object containing the IDs of the deleted host interfaces under the `interfaceids` property.

Examples

Delete a host interface

Delete the host interface with ID 30062.

Request:
See also

- `hostinterface.massremove`
- `host.massremove`

Source

CHostInterface::delete() in frontends/php/include/classes/api/services/CHostInterface.php.

**hostinterface.get**

description

integer/array `hostinterface.get(object parameters)`

The method allows to retrieve host interfaces according to the given parameters.

parameters

(object) Parameters defining the desired output.

The method supports the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostids</td>
<td>string/array</td>
<td>Return only host interfaces used by the given hosts.</td>
</tr>
<tr>
<td>interfaceids</td>
<td>string/array</td>
<td>Return only host interfaces with the given IDs.</td>
</tr>
<tr>
<td>itemids</td>
<td>string/array</td>
<td>Return only host interfaces used by the given items.</td>
</tr>
<tr>
<td>triggerids</td>
<td>string/array</td>
<td>Return only host interfaces used by items in the given triggers.</td>
</tr>
<tr>
<td>selectItems</td>
<td>query</td>
<td>Return the items that use the interface in the <code>items</code> property. Supports count.</td>
</tr>
</tbody>
</table>
Parameter | Type | Description
---|---|---
selectHosts | query | Return the host that uses the interface as an array in the hosts property.
limitSelects | integer | Limits the number of records returned by subselects.
Applies to the following subselects: selectItems.
sortfield | string/array | Sort the result by the given properties.
Possible values are: interfaceid, dns, ip.
countOutput | boolean | These parameters being common for all get methods are described in detail in the reference commentary page.
editable | boolean | excludeSearch | boolean | filter | object | limit | integer | output | query | preservekeys | boolean | search | object | searchByAny | boolean | searchWildcardsEnabled | boolean | sortorder | string/array | startSearch | boolean

Return values

(integer/array) Returns either:

- an array of objects;
- the count of retrieved objects, if the countOutput parameter has been used.

Examples

Retrieve host interfaces

Retrieve all data about the interfaces used by host "30057."

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "hostinterface.get",
    "params": {
        "output": "extend",
        "hostids": "30057"
    }
}
```
"auth": "038e1d7b1735c6a5436ee9eae096879e",
"id": 1
}

Response:
{
  "jsonrpc": "2.0",
  "result": [
    {
      "interfaceid": "30050",
      "hostid": "30057",
      "main": "1",
      "type": "1",
      "useip": "1",
      "ip": "127.0.0.1",
      "dns": "",
      "port": "10050",
      "bulk": "1"
    },
    {
      "interfaceid": "30067",
      "hostid": "30057",
      "main": "0",
      "type": "1",
      "useip": "0",
      "ip": "",
      "dns": "localhost",
      "port": "10050",
      "bulk": "1"
    },
    {
      "interfaceid": "30068",
      "hostid": "30057",
      "main": "1",
      "type": "2",
      "useip": "1",
      "ip": "127.0.0.1",
      "dns": "",
      "port": "161",
      "bulk": "1"
    }
  ],
  "id": 1
}

See also
- Host
- Item

Source
CHostInterface::get() in frontends/php/include/classes/api/services/CHostInterface.php.

**hostinterface.massadd**

Description

object hostinterface.massadd(object parameters)

This method allows to simultaneously add host interfaces to multiple hosts.

Parameters

(object) Parameters containing the host interfaces to be created on the given hosts.
The method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hosts</td>
<td>object/array</td>
<td>(required) Hosts to be updated. The hosts must have the hostid property defined.</td>
</tr>
<tr>
<td>interfaces</td>
<td>object/array</td>
<td>(required) Host interfaces to create on the given hosts.</td>
</tr>
</tbody>
</table>

Return values

(object) Returns an object containing the IDs of the created host interfaces under the interfaceids property.

Examples

Creating interfaces

Create an interface on two hosts.

Request:

```json
{
    "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
        }
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "interfaceids": [
            "30069",
            "30070"
        ]
    },
    "id": 1
}
```

See also

- hostinterface.create
**hostinterface.massremove**

**Description**

object hostinterface.massremove(object parameters)

This method allows to remove host interfaces from the given hosts.

**Parameters**

(object) Parameters containing the IDs of the hosts to be updated and the interfaces to be removed.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostids</td>
<td>string/array</td>
<td>IDs of the hosts to be updated.</td>
</tr>
<tr>
<td>(required)</td>
<td></td>
<td>Host interfaces to remove from the given hosts.</td>
</tr>
<tr>
<td>interfaces</td>
<td>object/array</td>
<td>The host interface object must have the ip, dns and</td>
</tr>
<tr>
<td>(required)</td>
<td></td>
<td>port properties defined</td>
</tr>
</tbody>
</table>

**Return values**

(object) Returns an object containing the IDs of the deleted host interfaces under the interfaceids property.

**Examples**

**Removing interfaces**

Remove the "127.0.0.1" SNMP interface from two hosts.

**Request:**

```json
{
   "jsonrpc": "2.0",
   "method": "hostinterface.massremove",
   "params": {
      "hostids": [
         "30050",
         "30052"
      ],
      "interfaces": {
         "dns": ",",
         "ip": "127.0.0.1",
         "port": "161"
      }
   },
   "auth": "038e1d7b1735c6a5436ee9eae095879e",
   "id": 1
}
```

**Response:**

```json
{
   "jsonrpc": "2.0",
   "result": {
      "interfaceids": [
```

```
See also

- hostinterface.delete
- host.massremove

Source

CHostInterface::massRemove() in frontends/php/include/classes/api/services/CHostInterface.php.

**hostinterface.replacehostinterfaces**

**Description**

object hostinterface.replacehostinterfaces(object parameters)

This method allows to replace all host interfaces on a given host.

**Parameters**

(object) Parameters containing the ID of the host to be updated and the new host interfaces.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostid</td>
<td>string</td>
<td>ID of the host to be updated.</td>
</tr>
<tr>
<td>interfaces</td>
<td>object/array</td>
<td>Host interfaces to replace the current host interfaces with.</td>
</tr>
</tbody>
</table>

**Return values**

(object) Returns an object containing the IDs of the created host interfaces under the interfaceids property.

**Examples**

Replacing host interfaces

Replace all host interfaces with a single agent interface.

**Request:**

```json
{
    "jsonrpc": "2.0",
    "method": "hostinterface.replacehostinterfaces",
    "params": {
        "hostid": "30052",
        "interfaces": {
            "dns": "",
            "ip": "127.0.0.1",
            "main": 1,
            "port": "10050",
            "type": 1,
            "useip": 1
        }
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

**Response:**

881
hostinterface.update

Description

object hostinterface.update(object/array hostInterfaces)

This method allows to update existing host interfaces.

Parameters

(object/array) Host interface properties to be updated.

The interfaceid property must be defined for each host interface, all other properties are optional. Only the given properties will be updated, all others will remain unchanged.

Return values

(object) Returns an object containing the IDs of the updated host interfaces under the interfaceids property.

Examples

Changing a host interface port

Change the port of a host interface.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "hostinterface.update",
    "params": {
        "interfaceid": "30048",
        "port": "30050"
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "interfaceids": ["30048"
    ],
    "id": 1
}
```
Host prototype

This class is designed to work with host prototypes.

Object references:

- Host prototype
- Host prototype inventory
- Group link
- Group prototype

Available methods:

- `hostprototype.create` - creating new host prototypes
- `hostprototype.delete` - deleting host prototypes
- `hostprototype.get` - retrieving host prototypes
- `hostprototype.update` - updating host prototypes

> Host prototype object

The following objects are directly related to the `hostprototype` API.

Host prototype

The host prototype object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostid</td>
<td>string</td>
<td>(readonly) ID of the host prototype.</td>
</tr>
<tr>
<td>host</td>
<td>string</td>
<td>Technical name of the host prototype.</td>
</tr>
<tr>
<td>(required)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>Visible name of the host prototype.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: host property value.</td>
</tr>
<tr>
<td>status</td>
<td>integer</td>
<td>Status of the host prototype.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - (default) monitored host;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - unmonitored host.</td>
</tr>
<tr>
<td>templateid</td>
<td>string</td>
<td>(readonly) ID of the parent template host prototype.</td>
</tr>
</tbody>
</table>

Note that for some methods (update, delete) the required/optional parameter combination is different.

Host prototype inventory

The host prototype inventory object has the following properties.
<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>inventory_mode</td>
<td>integer</td>
<td>Host prototype inventory population mode.</td>
</tr>
<tr>
<td>population_mode</td>
<td>-1-disabled; 0-manual; 1-automatic.</td>
<td></td>
</tr>
</tbody>
</table>

**Group link**

The group link object links a host prototype with a host group and has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group_prototypeid</td>
<td>string</td>
<td>(readonly) ID of the group link.</td>
</tr>
<tr>
<td>groupid</td>
<td>string</td>
<td>ID of the host group.</td>
</tr>
<tr>
<td>hostid</td>
<td>string</td>
<td>(readonly) ID of the host prototype</td>
</tr>
<tr>
<td>templateid</td>
<td>string</td>
<td>(readonly) ID of the parent template group link.</td>
</tr>
</tbody>
</table>

**Group prototype**

The group prototype object defines a group that will be created for a discovered host and has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group_prototypeid</td>
<td>string</td>
<td>(readonly) ID of the group prototype.</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>Name of the group prototype.</td>
</tr>
<tr>
<td>hostid</td>
<td>string</td>
<td>(readonly) ID of the host prototype</td>
</tr>
<tr>
<td>templateid</td>
<td>string</td>
<td>(readonly) ID of the parent template group prototype.</td>
</tr>
</tbody>
</table>

**hostprototype.create**

Description

object hostprototype.create(object/array hostPrototypes)

This method allows to create new host prototypes.

Parameters

(object/array) Host prototypes to create.

Additionally to the standard host prototype properties, the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>groupLinks</td>
<td>array</td>
<td>Group links to be created for the host prototype.</td>
</tr>
<tr>
<td>ruleid</td>
<td>string</td>
<td>ID of the LLD rule that the host prototype belongs to.</td>
</tr>
<tr>
<td>groupPrototypes</td>
<td>array</td>
<td>Group prototypes to be created for the host prototype.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>inventory</td>
<td>object</td>
<td>Host prototype inventory properties.</td>
</tr>
<tr>
<td>templates</td>
<td>object/array</td>
<td>Templates to be linked to the host prototype.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The templates must have the templateid property defined.</td>
</tr>
</tbody>
</table>

Return values

(object) Returns an object containing the IDs of the created host prototypes under the hostids property. The order of the returned IDs matches the order of the passed host prototypes.

Examples

Creating a host prototype

Create a host prototype "(VM.NAME)" on LLD rule "23542" with a group prototype "(HV.NAME)". Link it to host group "2".

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "hostprototype.create",
    "params": {
        "host": "(VM.NAME)",
        "ruleid": "23542",
        "groupLinks": [
            {
                "groupid": "2"
            }
        ],
        "groupPrototypes": [
            {
                "name": "(HV.NAME)"
            }
        ],
        "auth": "038e1d7b1735c6a5436ee9eae095879e",
        "id": 1
    }
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "hostids": [
            "10103"
        ],
        "id": 1
    }
}
```

See also

- Group link
- Group prototype
- Host prototype inventory

Source

885
**hostprototype.delete**

**Description**

object hostprototype.delete(array hostPrototypeIds)

This method allows to delete host prototypes.

**Parameters**

(array) IDs of the host prototypes to delete.

**Return values**

(object) Returns an object containing the IDs of the deleted host prototypes under the hostids property.

**Examples**

Deleting multiple host prototypes

Delete two host prototypes.

**Request:**

```json
{
   "jsonrpc": "2.0",
   "method": "hostprototype.delete",
   "params": [
      "10103",
      "10105"
   ],
   "auth": "3a57200802b24cda67c4e4010b50c065",
   "id": 1
}
```

**Response:**

```json
{
   "jsonrpc": "2.0",
   "result": {
      "hostids": [
         "10103",
         "10105"
      ],
      "id": 1
   }
}
```

**Source**

CHostPrototype::delete() in frontends/php/include/classes/api/services/CHostPrototype.php.

**hostprototype.get**

**Description**

integer/array hostprototype.get(object parameters)

The method allows to retrieve host prototypes according to the given parameters.

**Parameters**

(object) Parameters defining the desired output.

The method supports the following parameters.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostids</td>
<td>string/array</td>
<td>Return only host prototypes with the given IDs.</td>
</tr>
<tr>
<td>discoveryids</td>
<td>string/array</td>
<td>Return only host prototype that belong to the given LLD rules.</td>
</tr>
<tr>
<td>inherited</td>
<td>boolean</td>
<td>If set to true return only items inherited from a template.</td>
</tr>
<tr>
<td>selectDiscoveryRule</td>
<td>query</td>
<td>Return the LLD rule that the host prototype belongs to in the discoveryRule property.</td>
</tr>
<tr>
<td>selectGroupLinks</td>
<td>query</td>
<td>Return the group links of the host prototype in the groupLinks property.</td>
</tr>
<tr>
<td>selectGroupPrototypes</td>
<td>query</td>
<td>Return the group prototypes of the host prototype in the groupPrototypes property.</td>
</tr>
<tr>
<td>selectInventory</td>
<td>query</td>
<td>Return the host prototype inventory in the inventory property.</td>
</tr>
<tr>
<td>selectParentHost</td>
<td>query</td>
<td>Return the host that the host prototype belongs to in the parentHost property.</td>
</tr>
<tr>
<td>selectTemplates</td>
<td>query</td>
<td>Return the templates linked to the host prototype in the templates property.</td>
</tr>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Sort the result by the given properties.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values are: hostid, host, name and status.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>countOutput</td>
<td>boolean</td>
<td>These parameters being common for all get methods are described in detail on the Generic Zabbix API information page.</td>
</tr>
<tr>
<td>editable</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>excludeSearch</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>filter</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>limit</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>output</td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>preservekeys</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>search</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>searchByAny</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>searchWildcardsEnabled</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>sortorder</td>
<td>string/array</td>
<td></td>
</tr>
<tr>
<td>startSearch</td>
<td>boolean</td>
<td></td>
</tr>
</tbody>
</table>

Return values

(integer/array) Returns either:

- an array of objects;
- the count of retrieved objects, if the countOutput parameter has been used.

Examples

Retrieving host prototypes from an LLD rule

Retrieve all host prototypes and their group links and group prototypes from an LLD rule.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "hostprototype.get",
    "params": {
        "output": "extend",
        "selectGroupLinks": "extend",
        "selectGroupPrototypes": "extend",
        "discoveryids": "23554"
    },
    "auth": "038e1d7b1735c6a5a436ee9eae095879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": [
        {  
            "hostid": "10092",
            "host": "{#HV.UUID}"
            "status": "0",
            "name": "{#HV.NAME}"
            "templateid": "0",
            "groupLinks": [
                {  
                    "group_prototypeid": "4",
                    "hostid": "10092",
                    "groupid": "7",
                    "templateid": "0"
```
See also

- Group link
- Group prototype
- Host prototype inventory

Source

CHostPrototype::get() in frontends/php/include/classes/api/services/CHostPrototype.php.

**hostprototype.update**

Description

**object hostprototype.update(object/array hostPrototypes)**

This method allows to update existing host prototypes.

Parameters

(object/array) Host prototype properties to be updated.

The **hostid** property must be defined for each host prototype, all other properties are optional. Only the passed properties will be updated, all others will remain unchanged.

Additionally to the standard host prototype properties, the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>groupLinks</td>
<td>array</td>
<td>Group links to replace the current group links on the host prototype.</td>
</tr>
<tr>
<td>groupPrototypes</td>
<td>array</td>
<td>Group prototypes to replace the existing group prototypes on the host prototype.</td>
</tr>
<tr>
<td>inventory</td>
<td>object</td>
<td>Host prototype inventory properties.</td>
</tr>
<tr>
<td>templates</td>
<td>object/array</td>
<td>Templates to replace the currently linked templates.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The templates must have the <strong>templateid</strong> property defined.</td>
</tr>
</tbody>
</table>
Return values

(object) Returns an object containing the IDs of the updated host prototypes under the hostids property.

Examples

Disabling a host prototype

Disable a host prototype, that is, set its status to 1.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "hostprototype.update",
    "params": {
        "hostid": "10092",
        "status": 1
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "hostids": [
            "10092"
        ],
    },
    "id": 1
}
```

See also

- Group link
- Group prototype
- Host prototype inventory

Source

CHostPrototype::update() in frontends/php/include/classes/api/services/CHostPrototype.php.

**Icon map**

This class is designed to work with icon maps.

Object references:

- Icon map
- Icon mapping

Available methods:

- `iconmap.create` - create new icon maps
- `iconmap.delete` - delete icon maps
- `iconmap.get` - retrieve icon maps
- `iconmap.update` - update icon maps

> **Icon map object**

The following objects are directly related to the iconmap API.

Icon map

The icon map object has the following properties.
### Icon mapping

The icon mapping object defines a specific icon to be used for hosts with a certain inventory field value. It has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>iconmapid</td>
<td>string</td>
<td>(readonly) ID of the icon map.</td>
</tr>
<tr>
<td>default_iconid</td>
<td>string</td>
<td>ID of the default icon.</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>Name of the icon map.</td>
</tr>
</tbody>
</table>

Note that for some methods (update, delete) the required/optional parameter combination is different.

### iconmap.create

**Description**

object iconmap.create(object/array iconMaps)

This method allows to create new icon maps.

**Parameters**

(object/array) Icon maps to create.

Additionally to the standard icon map properties, the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mappings</td>
<td>array</td>
<td>Icon mappings to be created for the icon map.</td>
</tr>
</tbody>
</table>

**Return values**

(object) Returns an object containing the IDs of the created icon maps under the iconmapids property. The order of the returned IDs matches the order of the passed icon maps.
Examples

Create an icon map

Create an icon map to display hosts of different types.

Request:

```
{
   "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"
         }
      ],
   },
   "auth": "038e1d7b1735c6a5436ee9eae095879e",
   "id": 1
}
```

Response:

```
{
   "jsonrpc": "2.0",
   "result": {
      "iconmapids": [
         "2"
      ],
   },
   "id": 1
}
```

See also

- Icon mapping

Source

CIconMap::create() in frontends/php/include/classes/api/services/CIconMap.php.

**iconmap.delete**

Description

Object iconmap.delete(array iconMapIds)

This method allows to delete icon maps.

Parameters

(array) IDs of the icon maps to delete.

Return values

(object) Returns an object containing the IDs of the deleted icon maps under the iconmapids property.

Examples

Delete multiple icon maps

Delete two icon maps.
Request:
{
    "jsonrpc": "2.0",
    "method": "iconmap.delete",
    "params": [
        "2",
        "5"
    ],
    "auth": "3a57200802b24cda67c4e4010b50c065",
    "id": 1
}

Response:
{
    "jsonrpc": "2.0",
    "result": {
        "iconmapids": [
            "2",
            "5"
        ]
    },
    "id": 1
}

Source
CIconMap::delete() in frontends/php/include/classes/api/services/CIconMap.php.

iconmap.get

Description

integer/array iconmap.get(object parameters)

The method allows to retrieve icon maps according to the given parameters.

Parameters

(object) Parameters defining the desired output.

The method supports the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>iconmapids</td>
<td>string/array</td>
<td>Return only icon maps with the given IDs.</td>
</tr>
<tr>
<td>sysmapids</td>
<td>string/array</td>
<td>Return only icon maps that are used in the given maps.</td>
</tr>
<tr>
<td>selectMappings</td>
<td>query</td>
<td>Return used icon mappings in the mappings property.</td>
</tr>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Sort the result by the given properties.</td>
</tr>
</tbody>
</table>

Possible values are: iconmapid and name.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>countOutput</td>
<td>boolean</td>
<td>These parameters being common for all get methods are described in detail in the reference commentary.</td>
</tr>
<tr>
<td>editable</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>excludeSearch</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>filter</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>limit</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>output</td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>preservekeys</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>search</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>searchByAny</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>searchWildcardsEnabled</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>sortorder</td>
<td>string/array</td>
<td></td>
</tr>
<tr>
<td>startSearch</td>
<td>boolean</td>
<td></td>
</tr>
</tbody>
</table>

Return values

(integer/array) Returns either:

- an array of objects;
- the count of retrieved objects, if the countOutput parameter has been used.

Examples

Retrieve all data about icon map "3".

Request:

```json
{
   "jsonrpc": "2.0",
   "method": "iconmap.get",
   "params": {
      "iconmapids": "3",
      "output": "extend",
      "selectMappings": "extend"
   },
   "auth": "038e1d7b1735c6a5436ee9eae095879e",
   "id": 1
}
```

Response:

```json
{
   "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": "server",
               "sortorder": "0"
            }
         
```
See also

• Icon mapping

Source

CIconMap::get() in frontends/php/include/classes/api/services/CIconMap.php.

**iconmap.update**

**Description**

object iconmap.update(object/array iconMaps)

This method allows to update existing icon maps.

**Parameters**

(object/array) Icon map properties to be updated.

The iconmapid property must be defined for each icon map, all other properties are optional. Only the passed properties will be updated, all others will remain unchanged.

Additionally to the standard icon map properties, the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mappings</td>
<td>array</td>
<td>Icon mappings to replace the existing icon mappings.</td>
</tr>
</tbody>
</table>

**Return values**

(object) Returns an object containing the IDs of the updated icon maps under the iconmapids property.

**Examples**

Rename icon map

Rename an icon map to “OS icons”.

**Request:**

```json
{
    "jsonrpc": "2.0",
    "method": "iconmap.update",
    "params": {
        "iconmapid": "1",
        "name": "OS icons"
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

**Response:**

```json
{
    "jsonrpc": "2.0",
    "result": {
```
See also

- Icon mapping

Source

CIconMap::update() in frontends/php/include/classes/api/services/CIconMap.php.

Image

This class is designed to work with images.

Object references:

- Image

Available methods:

- image.create - create new images
- image.delete - delete images
- image.get - retrieve images
- image.update - update images

> Image object

The following objects are directly related to the image API.

Image

The image object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>imageid</td>
<td>string</td>
<td>(readonly) ID of the image.</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>Name of the image.</td>
</tr>
<tr>
<td>imagetype</td>
<td>integer</td>
<td>Type of image.</td>
</tr>
</tbody>
</table>

Possible values:
1 - (default) icon;
2 - background image.

Note that for some methods (update, delete) the required/optional parameter combination is different.

image.create

Description

object image.create(object/array images)

This method allows to create new images.

Parameters

(object/array) images to create.

Additionally to the standard image properties, the method accepts the following parameters.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>image</strong></td>
<td>string</td>
<td>Base64 encoded image. The maximum size of the encoded image is 1 MB.</td>
</tr>
</tbody>
</table>

**Return values**

(object) Returns an object containing the IDs of the created images under the `imageids` property. The order of the returned IDs matches the order of the passed images.

**Examples**

Create an image

Create a cloud icon.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "image.create",
    "params": {
        "imagetype": 1,
        "name": "Cloud_(24)",
        "image": "iVBORw0KGgoAAAANSUhEUgAAABgAAAANCAYAAACzbK7QAAAABHNCSVQICAgIfAhkiAAAAAlwSFlzAAACmAAAApgBNtNH3wAAABl0RVh0U29mdHdhcmUAd3d3L...
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "imageids": [
            "188"
        ],
        "id": 1
    }
}
```

**Source**

CImage::create() in frontends/php/include/classes/api/services/CImage.php.

**image.delete**

**Description**

object image.delete(array imageIds)

This method allows to delete images.

**Parameters**

(array) IDs of the images to delete.

**Return values**

(object) Returns an object containing the IDs of the deleted images under the `imageids` property.

**Examples**

Delete multiple images

Delete two images.

Request:
{ "jsonrpc": "2.0", "method": "image.delete", "params": [ "188", "192" ], "auth": "3a57200802b24cda67c4e4010b50c065", "id": 1 }
}

Response:
{
  "jsonrpc": "2.0",
  "result": {
    "imageids": [
      "188",
      "192"
    ],
  },
  "id": 1
}

Source
CImage::delete() in frontends/php/include/classes/api/services/CImage.php.

**image.get**

Description

text

integer/array image.get(object parameters)

The method allows to retrieve images according to the given parameters.

Parameters

(object) Parameters defining the desired output.

The method supports the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>imageids</td>
<td>string/array</td>
<td>Return only images with the given IDs.</td>
</tr>
<tr>
<td>sysmapids</td>
<td>string/array</td>
<td>Return images that are used on the given maps.</td>
</tr>
<tr>
<td>select_image</td>
<td>flag</td>
<td>Return the Base64 encoded image in the image property.</td>
</tr>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Sort the result by the given properties.</td>
</tr>
</tbody>
</table>

Possible values are: imageid and name.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>countOutput</td>
<td>boolean</td>
<td>These parameters being common for all get methods are described in detail in the reference commentary.</td>
</tr>
<tr>
<td>editable</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>excludeSearch</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>filter</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>limit</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>output</td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>preservekeys</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>search</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>searchByAny</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>searchWildcardsEnabled</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>sortorder</td>
<td>string/array</td>
<td></td>
</tr>
<tr>
<td>startSearch</td>
<td>boolean</td>
<td></td>
</tr>
</tbody>
</table>

Return values

(integer/array) Returns either:

- an array of objects;
- the count of retrieved objects, if the countOutput parameter has been used.

Examples

Retrieve an image

Retrieve all data for image with ID "2".

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "image.get",
    "params": {
        "output": "extend",
        "select_image": true,
        "imageids": "2"
    },
    "auth": "038e1d7b1735c6a5436ee9eae096879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": [
        {
            "imageid": "2",
            "imagetype": "1",
            "name": "Cloud_(24)",
            "image": "iVBORw0KGgoAAAANSUhEUgAAABgAAAANCAYAAACzbK7QAAAABHNCSVQICAgI

Source

CImage::get() in frontends/php/include/classes/api/services/CImage.php.
**image.update**

Description

```object image.update(object/array images)```

This method allows to update existing images.

Parameters

**(object/array) Image properties to be updated.**

The `imageid` property must be defined for each image, all other properties are optional. Only the passed properties will be updated, all others will remain unchanged.

Additionally to the **standard image properties**, the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>image</td>
<td>string</td>
<td>Base64 encoded image. The maximum size of the encoded image is 1 MB.</td>
</tr>
</tbody>
</table>

Return values

**(object)** Returns an object containing the IDs of the updated images under the `imageids` property.

Examples

**Rename image**

Rename image to "Cloud icon".

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "image.update",
    "params": {
        "imageid": "2",
        "name": "Cloud icon"
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "imageids": [
            "2"
        ],
        "id": 1
    }
}
```

Source

CImage::update() in frontends/php/include/classes/api/services/CImage.php.

**Item**

This class is designed to work with items.

Object references:
Available methods:

- `item.create` - creating new items
- `item.delete` - deleting items
- `item.get` - retrieving items
- `item.update` - updating items

> Item object

The following objects are directly related to the `item API`.

Item

**Note:**
Web items cannot be directly created, updated or deleted via the Zabbix API.

The item object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>itemid</td>
<td>string</td>
<td>(readonly) ID of the item.</td>
</tr>
<tr>
<td>delay</td>
<td>string</td>
<td>Update interval of the item. Accepts seconds or a time unit with suffix (30s,1m,2h,1d). Optionally one or more <code>custom intervals</code> can be specified either as flexible intervals or scheduling. Multiple intervals are separated by a semicolon. User macros may be used. A single macro has to fill the whole field. Multiple macros in a field or macros mixed with text are not supported. Flexible intervals may be written as two macros separated by a forward slash (e.g. <code>{$FLEX_INTERVAL}/{$FLEX_PERIOD}</code>). Optional for Zabbix trapper or dependent items.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>hostid</td>
<td>string</td>
<td>ID of the host or template that the item belongs to. For update operations this field is readonly.</td>
</tr>
<tr>
<td>interfaceid</td>
<td>string</td>
<td>ID of the item’s host interface. Not required for template items. Optional for internal, active agent, trapper, aggregate, calculated, dependent and database monitor items.</td>
</tr>
<tr>
<td>key_</td>
<td>string</td>
<td>Item key.</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>Name of the item.</td>
</tr>
<tr>
<td>type</td>
<td>integer</td>
<td>Type of the item. Possible values: 0 - Zabbix agent; 1 - SNMPv1 agent; 2 - Zabbix trapper; 3 - Simple check; 4 - SNMPv2 agent; 5 - Zabbix internal; 6 - SNMPv3 agent; 7 - Zabbix agent (active); 8 - Zabbix aggregate; 9 - Web item; 10 - External check; 11 - Database monitor; 12 - IPMI agent; 13 - SSH agent; 14 - Telnet agent; 15 - Calculated; 16 - JMX agent; 17 - SNMP trap; 18 - Dependent item; 19 - HTTP agent</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>url</td>
<td>string</td>
<td>URL string, required only for HTTP agent item type. Supports user macros,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{HOST.IP}, {HOST.CONN}, {HOST.DNS}, {HOST.HOST}, {HOST.NAME},</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{ITEM.ID}, {ITEM.KEY}.</td>
</tr>
<tr>
<td>value_type</td>
<td>integer</td>
<td>Type of information of the item.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values: 0 - numeric float; 1 - character; 2 - log; 3 - numeric</td>
</tr>
<tr>
<td></td>
<td></td>
<td>unsigned; 4 - text.</td>
</tr>
<tr>
<td>allow_traps</td>
<td>integer</td>
<td>HTTP agent item field. Allow to populate value as in trapper item type also.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - (default) Do not allow to accept incoming data.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - Allow to accept incoming data.</td>
</tr>
<tr>
<td>auth_type</td>
<td>integer</td>
<td>Used only by SSH agent items or HTTP agent items.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SSH agent authentication method possible values: 0 - (default) password;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - public key.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HTTP agent authentication method possible values: 0 - (default) none 1 -</td>
</tr>
<tr>
<td></td>
<td></td>
<td>basic 2 - NTLM</td>
</tr>
<tr>
<td>description</td>
<td>string</td>
<td>Description of the item.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>error</td>
<td>string</td>
<td>(readonly) Error text if there are problems updating the item.</td>
</tr>
<tr>
<td>flags</td>
<td>integer</td>
<td>(readonly) Origin of the item.</td>
</tr>
<tr>
<td>follow_redirects</td>
<td>integer</td>
<td>HTTP agent item field. Follow response redirects while pooling data.</td>
</tr>
</tbody>
</table>
| headers       | object  | HTTP agent item field. Object with HTTP(S) request headers, where header name is used as key and header value as value. Example: 
|               |         | { "User-Agent": "Zabbix" }                                                 |
| history       | string  | A time unit of how long the history data should be stored. Also accepts user macro. 
|               |         | Default: 90d.                                                              |
| http_proxy    | string  | HTTP agent item field. HTTP(S) proxy connection string.                    |
| inventory_link | integer | ID of the host inventory field that is populated by the item. Refer to the host inventory page for a list of supported host inventory fields and their IDs. 
<p>|               |         | Default: 0.                                                                |
| ipmi_sensor   | string  | IPMI sensor. Used only by IPMI items.                                       |</p>
<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jmx_endpoint</td>
<td>string</td>
<td>JMX agent custom connection string. Default value: service:jmx:rmi:///jndi/rmi://{HOST.CONN}:{HOST.PORT}/jmxrmi (readonly) Time when the item was last updated.</td>
</tr>
<tr>
<td>lastclock</td>
<td>timestamp</td>
<td>(readonly) Time when the item was last updated. This property will only return a value for the period configured in ZBX_HISTORY_PERIOD.</td>
</tr>
<tr>
<td>lastns</td>
<td>integer</td>
<td>(readonly) Nanoseconds when the item was last updated. This property will only return a value for the period configured in ZBX_HISTORY_PERIOD.</td>
</tr>
<tr>
<td>lastvalue</td>
<td>string</td>
<td>(readonly) Last value of the item. This property will only return a value for the period configured in ZBX_HISTORY_PERIOD.</td>
</tr>
<tr>
<td>logtimefmt</td>
<td>string</td>
<td>Format of the time in log entries. Used only by log items. Master item ID. Recursion up to 3 dependent items and maximum count of dependent items equal to 999 are allowed. Required by dependent items. Time when the monitored log file was last updated. Used only by log items.</td>
</tr>
<tr>
<td>master_itemid</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>mtime</td>
<td>timestamp</td>
<td></td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>output_format</td>
<td>integer</td>
<td>HTTP agent item field. Should response be converted to JSON.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - (default) Store raw. 1 - Convert to JSON.</td>
</tr>
<tr>
<td>params</td>
<td>string</td>
<td>Additional parameters depending on the type of the item:</td>
</tr>
</tbody>
</table>
|               |          | - executed script for SSH and Telnet items;  
|               |          | - SQL query for database monitor items;  
<p>|               |          | - formula for calculated items. Password for authentication. Used by simple check, SSH, Telnet, database monitor, JMX and HTTP agent items.        |
|               |          | When used by JMX, username should also be specified together with password or both properties should be left blank.                                                                                     |
| port          | string   | Port monitored by the item. Used only by SNMP items.                                                                                                                                                      |
| post_type     | integer  | HTTP agent item field. Type of post data body stored in posts property.                                                                                                                                   |
|               |          | 0 - (default) Raw data. 2 - JSON data. 3 - XML data.                                                                                                                                                      |
| posts         | string   | HTTP agent item field. HTTP(S) request body data. Used with post_type.                                                                                                                                   |</p>
<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>prevvalue</td>
<td>string</td>
<td>(readonly) Previous value of the item. This property will only return a value for the period configured in ZBX_HISTORY_PERIOD.</td>
</tr>
<tr>
<td>privatekey</td>
<td>string</td>
<td>Name of the private key file.</td>
</tr>
<tr>
<td>publickey</td>
<td>string</td>
<td>Name of the public key file.</td>
</tr>
<tr>
<td>query_fields</td>
<td>array</td>
<td>HTTP agent item field. Query parameters. Array of objects with ‘key’:’value’ pairs, where value can be empty string.</td>
</tr>
<tr>
<td>request_method</td>
<td>integer</td>
<td>HTTP agent item field. Type of request method.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - (default) GET</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - POST</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 - PUT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 - HEAD</td>
</tr>
<tr>
<td>retrieve_mode</td>
<td>integer</td>
<td>HTTP agent item field. What part of response should be stored.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - (default) Body</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - Headers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 - Both body and headers will be stored.</td>
</tr>
<tr>
<td>snmp_community</td>
<td>string</td>
<td>SNMP community. Used only by SNMPv1 and SNMPv2 items.</td>
</tr>
<tr>
<td>snmp_oid</td>
<td>string</td>
<td>SNMP OID.                     SNMPv3 auth passphrase. Used only by SNMPv3 items.</td>
</tr>
<tr>
<td>snmpv3_authpassphrase</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>snmpv3_authprotocol</td>
<td>integer</td>
<td>SNMPv3 authentication protocol. Used only by SNMPv3 items. Possible values: 0 - (default) MD5; 1 - SHA.</td>
</tr>
<tr>
<td>snmpv3_contextname</td>
<td>string</td>
<td>SNMPv3 context name. Used only by SNMPv3 items.</td>
</tr>
<tr>
<td>snmpv3_privpassphrase</td>
<td>string</td>
<td>SNMPv3 privacy passphrase. Used only by SNMPv3 items.</td>
</tr>
<tr>
<td>snmpv3_privprotocol</td>
<td>integer</td>
<td>SNMPv3 privacy protocol. Used only by SNMPv3 items.</td>
</tr>
<tr>
<td>snmpv3_securityname</td>
<td>string</td>
<td>SNMPv3 security name. Used only by SNMPv3 items.</td>
</tr>
<tr>
<td>ssl_cert_file</td>
<td>string</td>
<td>HTTP agent item field. Public SSL Key file path.</td>
</tr>
<tr>
<td>ssl_key_file</td>
<td>string</td>
<td>HTTP agent item field. Private SSL Key file path.</td>
</tr>
<tr>
<td>ssl_key_password</td>
<td>string</td>
<td>HTTP agent item field. Password for SSL Key file.</td>
</tr>
<tr>
<td>state</td>
<td>integer</td>
<td>(readonly) State of the item.</td>
</tr>
<tr>
<td>status</td>
<td>integer</td>
<td>Status of the item.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values: 0 - (default) normal; 1 - not supported. Status of the item.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values: 0 - (default) enabled item; 1 - disabled item.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>status_codes</td>
<td>string</td>
<td>HTTP agent item field. Ranges of required HTTP status codes separated by commas. Also supports user macros as part of comma separated list. Example: 200,200-{$M},{$M},200-400</td>
</tr>
<tr>
<td>templateid</td>
<td>string</td>
<td>(readonly) ID of the parent template item.</td>
</tr>
<tr>
<td>timeout</td>
<td>string</td>
<td>HTTP agent item field. Item data polling request timeout. Support user macros. Default: 3s maximum value: 60s</td>
</tr>
<tr>
<td>trapper_hosts</td>
<td>string</td>
<td>Allowed hosts. Used by trapper items or HTTP agent items.</td>
</tr>
<tr>
<td>trends</td>
<td>string</td>
<td>A time unit of how long the trends data should be stored. Also accepts user macro. Default: 365d.</td>
</tr>
<tr>
<td>units</td>
<td>string</td>
<td>Value units.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>---------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>username</td>
<td>string</td>
<td>Username for authentication. Used by simple check, SSH, Telnet, database monitor, JMX and HTTP agent items. Required by SSH and Telnet items. When used by JMX, password should also be specified together with username or both properties should be left blank.</td>
</tr>
<tr>
<td>valuemapid</td>
<td>string</td>
<td>ID of the associated value map.</td>
</tr>
<tr>
<td>verify_host</td>
<td>integer</td>
<td>HTTP agent item field. Validate host name in URL is in Common Name field or a Subject Alternate Name field of host certificate.</td>
</tr>
<tr>
<td>verify_peer</td>
<td>integer</td>
<td>HTTP agent item field. Validate is host certificate authentic.</td>
</tr>
</tbody>
</table>

Note that for some methods (update, delete) the required/optional parameter combination is different.

Item preprocessing

The item preprocessing object has the following properties.
<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>integer</td>
<td>The preprocessing option type.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - Custom multiplier;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 - Right trim;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 - Left trim;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 - Trim;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5 - Regular expression matching;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6 - Boolean to decimal;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7 - Octal to decimal;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8 - Hexadecimal to decimal;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9 - Simple change;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10 - Change per second.</td>
</tr>
<tr>
<td>params</td>
<td>string</td>
<td>Additional parameters used by preprocessing option.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Multiple parameters are separated by LF (\n) character.</td>
</tr>
</tbody>
</table>

**item.create**

**Description**

`object item.create(object/array items)`

This method allows to create new items.

**Note:**

Web items cannot be created via the Zabbix API.

**Parameters**

(object/array) Items to create.

Additionally to the standard item properties, the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>applications</td>
<td>array</td>
<td>IDs of the applications to add the item to.</td>
</tr>
<tr>
<td>preprocessing</td>
<td>array</td>
<td>Item preprocessing options.</td>
</tr>
</tbody>
</table>

**Note:**

To add an item to a template, use ID of the template in the `hostid` property of the item.

**Return values**

(object) Returns an object containing the IDs of the created items under the `itemid` property. The order of the returned IDs matches the order of the passed items.

**Examples**
Creating an item

Create a numeric Zabbix agent item to monitor free disk space on host with ID "30074" and add it to two applications.

Request:

```
{   "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",       "applications": [           "609",           "610"       ],       "delay": "30s"   },   "auth": "038e1d7b1735c6a5436ee9eae095879e",   "id": 1 }
```

Response:

```
{   "jsonrpc": "2.0",   "result": {       "itemids": [           "24758"       ]   },   "id": 1 }
```

Creating a host inventory item

Create a Zabbix agent item to populate the host’s "OS" inventory field.

Request:

```
{   "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   },   "auth": "038e1d7b1735c6a5436ee9eae095879e",   "id": 1 }
```

Response:

```
{   "jsonrpc": "2.0",   "result": {       "itemids": [           "24759"       ]   },   "id": 1 }
```
Creating an item with preprocessing

Create an item using custom multiplier.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "item.create",
    "params": {
        "name": "Device uptime",
        "key_": "sysUpTime",
        "hostid": "11312",
        "type": 4,
        "snmp_community": "{$SNMP_COMMUNITY}"
    },
    "preprocessing": [
        {
            "type": "1",
            "params": "0.01"
        }
    ],
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": ["44210"]
    },
    "id": 1
}
```

Creating dependent item

Create a dependent item for the master item with ID 24759. Only dependencies on the same host are allowed, therefore master and the dependent item should have the same hostid.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "item.create",
    "params": {
        "hostid": "30074",
        "name": "Dependent test item",
        "key_": "dependent.item",
        "type": "18",
        "master_itemid": "24759",
        "value_type": "2"
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```
Create HTTP agent item

Create POST request method item with JSON response preprocessing.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "item.create",
    "params": {
        "url": "http://127.0.0.1/http.php",
        "query_fields": [
            {
                "mode": "json"
            },
            {
                "min": "10"
            },
            {
                "max": "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"
            }
        ],
        "auth": "038e1d7b1735c6a5436ee9eae095879e",
        "id": 2
    }
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "23865"
        ],
    },
    "id": 3
}
```
item.delete

Description

object item.delete(array itemIds)

This method allows to delete items.

Note:
Web items cannot be deleted via the Zabbix API.

Parameters

(array) IDs of the items to delete.

Return values

(object) Returns an object containing the IDs of the deleted items under the itemids property.

Examples

Deleting multiple items

Delete two items. Dependent items and item prototypes are removed automatically if master item is deleted.

Request:

```json
{
   "jsonrpc": "2.0",
   "method": "item.delete",
   "params": [
      "22982",
      "22986"
   ],
   "auth": "3a57200802b24cda67c4e4010b50c065",
   "id": 1
}
```

Response:

```json
{
   "jsonrpc": "2.0",
   "result": {
      "itemids": [
         "22982",
         "22986"
      ],
      "id": 1
   }
}
```

Source

CItem::create() in frontends/php/include/classes/api/services/CItem.php.

item.get

Description

integer/array item.get(object parameters)

The method allows to retrieve items according to the given parameters.
Parameters

(object) Parameters defining the desired output.

The method supports the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>itemids</td>
<td>string/array</td>
<td>Return only items with the given IDs.</td>
</tr>
<tr>
<td>groupids</td>
<td>string/array</td>
<td>Return only items that belong to the hosts from the given groups.</td>
</tr>
<tr>
<td>templateids</td>
<td>string/array</td>
<td>Return only items that belong to the given templates.</td>
</tr>
<tr>
<td>hostids</td>
<td>string/array</td>
<td>Return only items that belong to the given hosts.</td>
</tr>
<tr>
<td>proxyids</td>
<td>string/array</td>
<td>Return only items that are monitored by the given proxies.</td>
</tr>
<tr>
<td>interfaceids</td>
<td>string/array</td>
<td>Return only items that use the given host interfaces.</td>
</tr>
<tr>
<td>graphids</td>
<td>string/array</td>
<td>Return only items that are used in the given graphs.</td>
</tr>
<tr>
<td>triggerids</td>
<td>string/array</td>
<td>Return only items that are used in the given triggers.</td>
</tr>
<tr>
<td>applicationids</td>
<td>string/array</td>
<td>Return only items that belong to the given applications.</td>
</tr>
<tr>
<td>webitems</td>
<td>flag</td>
<td>Include web items in the result.</td>
</tr>
<tr>
<td>inherited</td>
<td>boolean</td>
<td>If set to <code>true</code> return only items inherited from a template.</td>
</tr>
<tr>
<td>templated</td>
<td>boolean</td>
<td>If set to <code>true</code> return only items that belong to templates.</td>
</tr>
<tr>
<td>monitored</td>
<td>boolean</td>
<td>If set to <code>true</code> return only enabled items that belong to monitored hosts.</td>
</tr>
<tr>
<td>group</td>
<td>string</td>
<td>Return only items that belong to a group with the given name.</td>
</tr>
<tr>
<td>host</td>
<td>string</td>
<td>Return only items that belong to a host with the given name.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>application</td>
<td>string</td>
<td>Return only items that belong to an application with the given name.</td>
</tr>
<tr>
<td>with_triggers</td>
<td>boolean</td>
<td>If set to true return only items that are used in triggers.</td>
</tr>
<tr>
<td>selectHosts</td>
<td>query</td>
<td>Returns the host that the item belongs to as an array in the hosts property.</td>
</tr>
<tr>
<td>selectInterfaces</td>
<td>query</td>
<td>Returns the host interface used by the item as an array in the interfaces property.</td>
</tr>
<tr>
<td>selectTriggers</td>
<td>query</td>
<td>Return triggers that the item is used in in the triggers property.</td>
</tr>
<tr>
<td>selectGraphs</td>
<td>query</td>
<td>Supports count. Return graphs that contain the item in the graphs property.</td>
</tr>
<tr>
<td>selectApplications</td>
<td>query</td>
<td>Return the applications that the item belongs to in the applications property.</td>
</tr>
<tr>
<td>selectDiscoveryRule</td>
<td>query</td>
<td>Return the LLD rule that created the item in the discoveryRule property.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>selectItemDiscovery</td>
<td>query</td>
<td>Return the item discovery object in the itemDiscovery property. The item discovery object links the item to an item prototype from which it was created.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>It has the following properties:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>itemdiscoveryid - (string) ID of the item discovery;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>itemid - (string) ID of the discovered item;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>parent_itemid - (string) ID of the item prototype from which the item has been created;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>key_ - (string) key of the item prototype;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>lastcheck - (timestamp) time when the item was last discovered;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ts_delete - (timestamp) time when an item that is no longer discovered will be deleted.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>selectPreprocessingquery</td>
<td></td>
<td>Return item preprocessing options in preprocessing property.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>It has the following properties:</td>
</tr>
<tr>
<td>type</td>
<td>(string)</td>
<td>The preprocessing option types:</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>- Custom multiplier;</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>- Right trim;</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>- Left trim;</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>- Trim;</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>- Regular expression matching;</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>- Boolean to decimal;</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>- Octal to decimal;</td>
</tr>
<tr>
<td>8</td>
<td></td>
<td>- Hexadecimal to decimal;</td>
</tr>
<tr>
<td>9</td>
<td></td>
<td>- Simple change;</td>
</tr>
<tr>
<td>10</td>
<td></td>
<td>- Change per second.</td>
</tr>
<tr>
<td>params</td>
<td>(string)</td>
<td>Additional parameters used by preprocessing option. Multiple parameters are</td>
</tr>
<tr>
<td></td>
<td></td>
<td>separated by LF (\n) character.</td>
</tr>
<tr>
<td>filter</td>
<td>object</td>
<td>Return only those results that exactly match the given filter.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Accepts an array, where the keys are property names, and the values are either</td>
</tr>
<tr>
<td></td>
<td></td>
<td>a single value or an array of values to match against.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Supports additional filters:</td>
</tr>
<tr>
<td>host</td>
<td>technical name</td>
<td>of the host that the item belongs to.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>limitSelects</td>
<td>integer</td>
<td>Limits the number of records returned by subselects.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Applies to the following subselects:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- selectGraphs - results will be sorted by name;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- selectTriggers - results will be sorted by description.</td>
</tr>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Sort the result by the given properties.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values are: itemid, name, key, delay, history, trends, type and status.</td>
</tr>
<tr>
<td>countOutput</td>
<td>boolean</td>
<td>These parameters being common for all get methods are described in detail in the reference commentary page.</td>
</tr>
<tr>
<td>editable</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>excludeSearch</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>limit</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>output</td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>preservekeys</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>search</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>searchByAny</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>searchWildcardsEnabled</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>sortorder</td>
<td>string/array</td>
<td></td>
</tr>
<tr>
<td>startSearch</td>
<td>boolean</td>
<td></td>
</tr>
</tbody>
</table>

Return values

(integer/array) Returns either:

- an array of objects;
- the count of retrieved objects, if the countOutput parameter has been used.

Examples

Finding items by key

Retrieve all items from host with ID "10084" that have the word "system" in the key and sort them by name.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "item.get",
    "params": {
        "output": "extend",
        "search": {
            "searchWildcardsEnabled": true,
            "searchByAny": true,
            "search": "system",
            "limit": 100
        }
    }
}
```
"hostids": "10084",
"search": {
    "key_": "system"
},
"sortfield": "name"
},
"auth": "038e1d7b1735c6a5436ee9eae095879e",
"id": 1
}

Response:
{
    "jsonrpc": "2.0",
    "result": [
        
        "itemid": "23298",
        "type": "0",
        "snmp_community": "",
        "snmp_oid": "",
        "hostid": "10084",
        "name": "Context switches per second",
        "key_": "system.cpu.switches",
        "delay": "1m",
        "history": "7d",
        "trends": "365d",
        "lastvalue": "2552",
        "lastclock": "1351090998",
        "prevvalue": "2641",
        "state": "0",
        "status": "0",
        "value_type": "3",
        "trapper_hosts": "",
        "units": "sps",
        "snmpv3_securityname": "",
        "snmpv3_securitylevel": "0",
        "snmpv3_authpassphrase": "",
        "snmpv3_privpassphrase": "",
        "snmpv3_authprotocol": "0",
        "snmpv3_privprotocol": "0",
        "snmpv3_contextname": "",
        "error": "",
        "lastlogsize": "0",
        "logtimefmt": "",
        "templateid": "22680",
        "valuemapid": "0",
        "params": "",
        "ipmi_sensor": "",
        "authtype": "0",
        "username": "",
        "password": "",
        "publickey": "",
        "privatekey": "",
        "mtime": "0",
        "lastns": "564054253",
        "flags": "0",
        "interfaceid": "1",
        "port": "",
        "description": "",
        "inventory_link": "0",
        "lifetime": "0s",
        "evaltype": "0",
        "jmx_endpoint": "",
    
    
    
}
"master_itemid": "0",
"timeout": "3s",
"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"
},
{
"itemid": "23299",
"type": "0",
"snmp_community": "",
"snmp_oid": "",
"hostid": "10084",
"name": "CPU $2 time",
"key_": "system.cpu.util[,idle]",
"delay": "1m",
"history": "7d",
"trends": "365d",
"lastvalue": "86.031879",
"lastclock": "1351090999",
"prevvalue": "85.306944",
"state": "0",
"status": "0",
"value_type": "0",
"trapper_hosts": "",
"units": "/\%",
"snmpv3_securityname": "",
"snmpv3_securitylevel": "0",
"snmpv3_authpassphrase": "",
"snmpv3_privpassphrase": "",
"snmpv3_authprotocol": "0",
"snmpv3_privprotocol": "0",
"snmpv3_contextname": "",
"error": "",
"lastlogsize": "0",
"logtimefmt": "",
"templateid": "17354",
"valuemapid": "0",
"params": "",
"ipmi_sensor": "",
"authtype": "0",
"username": "",
"password": "",
"publickey": "",
"privatekey": "",
"mtime": "0",
"lastns": "564256864",
"flags": "0",
"interfaceid": "1"
"port": "",
"description": "The time the CPU has spent doing nothing.",
"inventory_link": "0",
"lifetime": "0s",
"evaltype": "0",
"jmx_endpoint": "",
"master_itemid": "0",
"timeout": "3s",
"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"
},
{
"itemid": "23300",
"type": "0",
"snmp_community": "",
"snmp_oid": "",
"hostid": "10084",
"name": "CPU $2 time",
"key_": "system.cpu.util[,interrupt]",
"history": "7d",
"trends": "365d",
"lastvalue": "0.008389",
"lastclock": "1351091000",
"prevvalue": "0.000000",
"state": "0",
"status": "0",
"value_type": "0",
"trapper_hosts": "",
"units": "%
"snmpv3_securityname": "",
"snmpv3_securitylevel": "0",
"snmpv3_authpassphrase": "",
"snmpv3_privpassphrase": "",
"snmpv3_authprotocol": "0",
"snmpv3_privprotocol": "0",
"snmpv3_contextname": "",
"error": "",
"lastlogsize": "0",
"logtimefmt": "",
"templateid": "22671",
"valuemapid": "0",
"params": "",
"ipmi_sensor": "",
"authtype": "0",
"username": "",
"password": "",
"publickey": "",
"allow_traps": "0"}
Finding dependent items by key

Retrieve all dependent items from host with ID "10116" that have the word "apache" in the key.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "item.get",
    "params": {
        "output": "extend",
        "hostids": "10116",
        "search": {
            "key_": "apache"
        },
        "filter": {
            "type": "18"
        }
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": [
        {
            "itemid": "25550",
            "924
```
"type": "18",
"snmp_community": "",
"snmp_oid": "",
"hostid": "10116",
"name": "Days",
"key_": "apache.status.uptime.days",
"delay": "",
"history": "90d",
"trends": "365d",
"status": "0",
"value_type": "3",
"trapper_hosts": "",
"units": "",
"snmpv3_securityname": "",
"snmpv3_securitylevel": "0",
"snmpv3_authpassphrase": "",
"snmpv3_privpassphrase": "",
"formula": "",
"error": "",
"lastlogsize": "0",
"logtimefmt": "",
"templateid": "0",
"valuemapid": "0",
"params": "",
"ipmi_sensor": "",
"authtype": "0",
"username": "",
"password": "",
"publickey": "",
"privatekey": "",
"mtime": "0",
"flags": "0",
"interfaceid": "0",
"port": "",
"description": "",
"inventory_link": "0",
"lifetime": "30d",
"snmpv3_authprotocol": "0",
"snmpv3_privprotocol": "0",
"state": "0",
"snmpv3_contextname": "",
"evaltype": "0",
"master_itemid": "25545",
"jmx_endpoint": "",
"timeout": "3s",
"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"
"lastclock": "0",
"lastns": "0",
"lastvalue": "0",
"prevvalue": "0"
},
{
"itemid": "25555",
"type": "18",
"snmp_community": "",
"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": "",
"snmpv3_securityname": "",
"snmpv3_securitylevel": "0",
"snmpv3_authpassphrase": "",
"snmpv3_privpassphrase": "",
"formula": "",
"error": "",
"lastlogsize": "0",
"logtimefmt": "",
"templateid": "0",
"valuemapid": "0",
"params": "",
"ipmi_sensor": "",
"authtype": "0",
"username": "",
"password": "",
"publickey": "",
"privatekey": "",
"mtime": "0",
"flags": "0",
"interfaceid": "0",
"port": "",
"description": "",
"inventory_link": "0",
"lifetime": "30d",
"snmpv3_authprotocol": "0",
"snmpv3_privprotocol": "0",
"state": "0",
"snmpv3_contextname": "",
"evaltype": "0",
"master_itemid": "25545",
"jmx_endpoint": "",
"timeout": "3s",
"url": "",
"query_fields": [],
"posts": "",
"status_codes": "200",
"follow_redirects": "1",
"post_type": "0",
"http_proxy": "",
"headers": [],
"retrieve_mode": "0",
"request_method": "0"
Find HTTP agent item

Find HTTP agent item with post body type XML for specific host id.

Request:

```
{
   "jsonrpc": "2.0",
   "method": "item.get",
   "params": {
      "hostids": "10255",
      "filter": {
         "type": "19",
         "post_type": "3"
      }
   },
   "id": 3,
   "auth": "d678e0b85688ce578ff061bd29a20d3b"
}
```

Response:

```
{
   "jsonrpc": "2.0",
   "result": [
      {
         "itemid": "28252",
         "type": "19",
         "snmp_community": "",
         "snmp_oid": "",
         "hostid": "10255",
         "name": "template item",
         "key_": "ti",
         "delay": "30s",
         "history": "90d",
         "trends": "365d",
         "status": "0",
         "value_type": "3",
         "trapper_hosts": "",
         "units": "",
         "snmpv3_securityname": "",
         "snmpv3_securitylevel": "0",
         "snmpv3_authpassphrase": "",
         "snmpv3_privpassphrase": "",
         "formula": "",
         "error": "",
         "lastlogsize": "0",
         "logtimefmt": "",
         "templateid": "0"
      }
   ]
}
```
"valuemapid": "0",
"params": "",
"ipmi_sensor": "",
"authtype": "0",
"username": "",
"password": "",
"publickey": "",
"privatekey": "",
"mtime": "0",
"flags": "0",
"interfaceid": "0",
"port": "",
"description": "",
"inventory_link": "0",
"lifetime": "30d",
"snmpv3_authprotocol": "0",
"snmpv3_privprotocol": "0",
"state": "0",
"snmpv3_contextname": "",
"evaltype": "0",
"jmx_endpoint": "",
"master_itemid": "0",
"timeout": "3s",
"url": "localhost",
"query_fields": [ 
  { "mode": "xml" 
  },
  "posts": "<body><\n<![CDATA[{$MACRO}<foo></bar>]>\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",
  "lastclock": "0",
  "lastns": "0",
  "lastvalue": "0",
  "prevvalue": "0"
  }
],
"id": 3
}
CItem::get() in frontends/php/include/classes/api/services/CItem.php.

**item.update**

Description

object item.update(object/array items)

This method allows to update existing items.

**Note:**
Web items cannot be updated via the Zabbix API.

Parameters

(object/array) Item properties to be updated.

The `itemid` property must be defined for each item, all other properties are optional. Only the passed properties will be updated, all others will remain unchanged.

Additionally to the **standard item properties**, the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>applications</td>
<td>array</td>
<td>IDs of the applications to replace the current applications.</td>
</tr>
<tr>
<td>preprocessing</td>
<td>array</td>
<td>Item preprocessing options to replace the current preprocessing options.</td>
</tr>
</tbody>
</table>

Return values

(object) Returns an object containing the IDs of the updated items under the `itemids` property.

Examples

Enabling an item

Enable an item, that is, set its status to "0".

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "item.update",
    "params": {
        "itemid": "10092",
        "status": 0
    },
    "auth": "700ca65537074ec963db7efabda78259",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "10092"
        ]
    },
    "error": null
}
```
Update dependent item

Update Dependent item name and Master item ID. Only dependencies on same host are allowed, therefore Master and Dependent item should have same hostid.

Request:

```
{
    "jsonrpc": "2.0",
    "method": "item.update",
    "params": {
        "name": "Dependent item updated name",
        "master_itemid": "25562",
        "itemid": "189019"
    },
    "auth": "700ca65537074ec963db7efabda78259",
    "id": 1
}
```

Response:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "189019"
        ],
    },
    "id": 1
}
```

Update HTTP agent item

Enable item value trapping.

Request:

```
{
    "jsonrpc": "2.0",
    "method": "item.update",
    "params": {
        "itemid": "23856",
        "allow_traps": "1"
    },
    "auth": "700ca65537074ec963db7efabda78259",
    "id": 1
}
```

Response:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "23856"
        ],
    },
    "id": 1
}
```

Source

CItem::update() in frontends/php/include/classes/api/services/CItem.php.

Item prototype
This class is designed to work with item prototypes.

Object references:

- Item prototype

Available methods:

- `itemprototype.create` - creating new item prototypes
- `itemprototype.delete` - deleting item prototypes
- `itemprototype.get` - retrieving item prototypes
- `itemprototype.update` - updating item prototypes

> Item prototype object

The following objects are directly related to the `itemprototype` API.

Item prototype

The item prototype object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>itemid</td>
<td>string (readonly)</td>
<td>ID of the item prototype.</td>
</tr>
<tr>
<td>delay</td>
<td>string (required)</td>
<td>Update interval of the item prototype. Accepts seconds or a time unit with suffix (30s,1m,2h,1d). Optionally one or more custom intervals can be specified either as flexible intervals or scheduling. Multiple intervals are separated by a semicolon. User macros and LLD macros may be used. A single macro has to fill the whole field. Multiple macros in a field or macros mixed with text are not supported. Flexible intervals may be written as two macros separated by a forward slash (e.g. <code>{$FLEX_INTERVAL}/{$FLEX_PERIOD}</code>). Optional for Zabbix trapper or dependent item.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>hostid</td>
<td>string</td>
<td>ID of the host that the item prototype belongs to. For update operations this field is readonly.</td>
</tr>
<tr>
<td>ruleid</td>
<td>string</td>
<td>ID of the LLD rule that the item belongs to. For update operations this field is readonly.</td>
</tr>
<tr>
<td>interfaceid</td>
<td>string</td>
<td>ID of the item prototype’s host interface. Used only for host item prototypes. Optional for Zabbix agent (active), Zabbix internal, Zabbix trapper, Dependent item, Zabbix aggregate, database monitor and calculated item prototypes.</td>
</tr>
<tr>
<td>key_</td>
<td>string</td>
<td>Item prototype key.</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>Name of the item prototype.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>type</strong></td>
<td>integer</td>
<td>Type of the item prototype. Possible values: 0 - Zabbix agent; 1 - SNMPv1 agent; 2 - Zabbix trapper; 3 - simple check; 4 - SNMPv2 agent; 5 - Zabbix internal; 6 - SNMPv3 agent; 7 - Zabbix agent (active); 8 - Zabbix aggregate; 10 - external check; 11 - database monitor; 12 - IPMI agent; 13 - SSH agent; 14 - TELNET agent; 15 - calculated; 16 - JMX agent; 17 - SNMP trap; 18 - Dependent item; 19 - HTTP agent;</td>
</tr>
<tr>
<td><strong>url</strong></td>
<td>string</td>
<td>URL string required only for HTTP agent item prototypes. Supports LLD macros, user macros, {HOST.IP}, {HOST.CONN}, {HOST.DNS}, {HOST.HOST}, {HOST.NAME}, {ITEM.ID}, {ITEM.KEY}.</td>
</tr>
<tr>
<td><strong>value_type</strong></td>
<td>integer</td>
<td>Type of information of the item prototype. Possible values: 0 - numeric float; 1 - character; 2 - log; 3 - numeric unsigned; 4 - text.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>allow_traps</td>
<td>integer</td>
<td>HTTP agent item prototype field. Allow to populate value as in trapper item type also.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - (default) Do not allow to accept incoming data.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - Allow to accept incoming data.</td>
</tr>
<tr>
<td>authtype</td>
<td>integer</td>
<td>Used only by SSH agent item prototypes or HTTP agent item prototypes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SSH agent authentication method possible values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - (default) password;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - public key.</td>
</tr>
<tr>
<td>description</td>
<td>string</td>
<td>Description of the item prototype.</td>
</tr>
<tr>
<td>follow_redirects</td>
<td>integer</td>
<td>HTTP agent item prototype field. Follow response redirects while pooling data.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - Do not follow redirects.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - (default) Follow redirects.</td>
</tr>
<tr>
<td>headers</td>
<td>object</td>
<td>HTTP agent item prototype field. Object with HTTP(S) request headers, where header name is used as key and header value as value.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{ &quot;User-Agent&quot;: &quot;Zabbix&quot; }</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>history</td>
<td>string</td>
<td>A time unit of how long the history data should be stored. Also accepts user macro and LLD macro. Default: 90d.</td>
</tr>
<tr>
<td>http_proxy</td>
<td>string</td>
<td>HTTP agent item prototype field. HTTP(S) proxy connection string.</td>
</tr>
<tr>
<td>ipmi_sensor</td>
<td>string</td>
<td>IPMI sensor. Used only by IPMI item prototypes.</td>
</tr>
<tr>
<td>jmx_endpoint</td>
<td>string</td>
<td>JMX agent custom connection string. Default value: service:jmx:rmi:///jndi/rmi://{HOST.CONN}:{HOST.PORT}/jmxrmi</td>
</tr>
<tr>
<td>logtimefmt</td>
<td>string</td>
<td>Format of the time in log entries. Used only by log item prototypes.</td>
</tr>
<tr>
<td>master_itemid</td>
<td>integer</td>
<td>Master item ID. Recursion up to 3 dependent items and item prototypes and maximum count of dependent items and item prototypes equal to 999 are allowed. Required by Dependent items.</td>
</tr>
<tr>
<td>output_format</td>
<td>integer</td>
<td>HTTP agent item prototype field. Should response be converted to JSON. 0 - (default) Store raw. 1 - Convert to JSON.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>params</td>
<td>string</td>
<td>Additional parameters depending on the type of the item prototype: - executed script for SSH and Telnet item prototypes; - SQL query for database monitor item prototypes; - formula for calculated item prototypes.</td>
</tr>
<tr>
<td>password</td>
<td>string</td>
<td>Password for authentication. Used by simple check, SSH, Telnet, database monitor, JMX and HTTP agent item prototypes.</td>
</tr>
<tr>
<td>port</td>
<td>string</td>
<td>Port monitored by the item prototype. Used only by SNMP items prototype.</td>
</tr>
<tr>
<td>post_type</td>
<td>integer</td>
<td>HTTP agent item prototype field. Type of post data body stored in posts property. 0 - (default) Raw data. 2 - JSON data. 3 - XML data.</td>
</tr>
<tr>
<td>posts</td>
<td>string</td>
<td>HTTP agent item prototype field. HTTP(S) request body data. Used with post_type.</td>
</tr>
<tr>
<td>privatekey</td>
<td>string</td>
<td>Name of the private key file.</td>
</tr>
<tr>
<td>publickey</td>
<td>string</td>
<td>Name of the public key file.</td>
</tr>
<tr>
<td>query_fields</td>
<td>array</td>
<td>HTTP agent item prototype field. Query parameters. Array of objects with 'key':'value' pairs, where value can be empty string.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>request_method</td>
<td>integer</td>
<td>HTTP agent item prototype field. Type of request method.</td>
</tr>
<tr>
<td>retrieve_mode</td>
<td>integer</td>
<td>HTTP agent item prototype field. What part of response should be stored.</td>
</tr>
<tr>
<td>snmp_community</td>
<td>string</td>
<td>SNMP community. Used only by SNMPv1 and SNMPv2 item prototypes.</td>
</tr>
<tr>
<td>snmp_oid</td>
<td>string</td>
<td>SNMP OID. SNMPv3 auth passphrase. Used only by SNMPv3 item prototypes.</td>
</tr>
<tr>
<td>snmpv3_auth_passphase</td>
<td>string</td>
<td>SNMPv3 authentication protocol. Used only by SNMPv3 items.</td>
</tr>
<tr>
<td>snmpv3_auth_prot</td>
<td>integer</td>
<td>Possible values: 0 - (default) MD5; 1 - SHA. SNMPv3 context name. Used only by SNMPv3 item prototypes.</td>
</tr>
<tr>
<td>snmpv3_context</td>
<td>string</td>
<td>SNMPv3 priv passphrase. Used only by SNMPv3 item prototypes.</td>
</tr>
<tr>
<td>snmpv3_priv_passphase</td>
<td>string</td>
<td>SNMPv3 privacy protocol. Used only by SNMPv3 items.</td>
</tr>
<tr>
<td>snmpv3_priv_prot</td>
<td>integer</td>
<td>Possible values: 0 - (default) DES; 1 - AES.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>snmpv3_securitylevel</td>
<td>integer</td>
<td>SNMPv3 security level. Used only by SNMPv3 item prototypes. Possible values: 0 - noAuthNoPriv; 1 - authNoPriv; 2 - authPriv.</td>
</tr>
<tr>
<td>snmpv3_securityname</td>
<td>string</td>
<td>SNMPv3 security name. Used only by SNMPv3 item prototypes.</td>
</tr>
<tr>
<td>ssl_cert_file</td>
<td>string</td>
<td>HTTP agent item prototype field. Public SSL Key file path.</td>
</tr>
<tr>
<td>ssl_key_file</td>
<td>string</td>
<td>HTTP agent item prototype field. Private SSL Key file path.</td>
</tr>
<tr>
<td>ssl_key_password</td>
<td>string</td>
<td>HTTP agent item prototype field. Password for SSL Key file.</td>
</tr>
<tr>
<td>status</td>
<td>integer</td>
<td>Status of the item prototype. Possible values: 0 - (default) enabled item prototype; 1 - disabled item prototype; 3 - unsupported item prototype.</td>
</tr>
<tr>
<td>status_codes</td>
<td>string</td>
<td>HTTP agent item prototype field. Ranges of required HTTP status codes separated by commas. Also supports user macros or LLD macros as part of comma separated list. Example: 200,200-{$M},{$M},200-400</td>
</tr>
<tr>
<td>templateid</td>
<td>string</td>
<td>(readonly) ID of the parent template item prototype.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>timeout</td>
<td>string</td>
<td>HTTP agent item prototype field. Item data polling request timeout. Support user macros and LLD macros. default: 3s maximum value: 60s</td>
</tr>
<tr>
<td>trapper_hosts</td>
<td>string</td>
<td>Allowed hosts. Used by trapper item prototypes or HTTP item prototypes.</td>
</tr>
<tr>
<td>trends</td>
<td>string</td>
<td>A time unit of how long the trends data should be stored. Also accepts user macro and LLD macro. Default: 365d.</td>
</tr>
<tr>
<td>units</td>
<td>string</td>
<td>Value units.</td>
</tr>
<tr>
<td>username</td>
<td>string</td>
<td>Username for authentication. Used by simple check, SSH, Telnet, database monitor, JMX and HTTP agent item prototypes. Required by SSH and Telnet item prototypes.</td>
</tr>
<tr>
<td>valuemapid</td>
<td>string</td>
<td>ID of the associated value map.</td>
</tr>
<tr>
<td>verify_host</td>
<td>integer</td>
<td>HTTP agent item prototype field. Validate host name in URL is in Common Name field or a Subject Alternate Name field of host certificate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - (default) Do not validate. 1 - Validate.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>verify_peer</td>
<td>integer</td>
<td>HTTP agent item prototype field. Validate is host certificate authentic.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - (default) Do not validate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - Validate.</td>
</tr>
</tbody>
</table>

Note that for some methods (update, delete) the required/optional parameter combination is different.

**itemprototype.create**

**Description**

object itemprototype.create(object/array itemPrototypes)

This method allows to create new item prototypes.

**Parameters**

(object/array) Item prototype to create.

Additionally to the standard item prototype properties, the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ruleid</td>
<td>string</td>
<td>ID of the LLD rule that the item belongs to.</td>
</tr>
<tr>
<td>applications</td>
<td>array</td>
<td>IDs of applications to be assigned to the discovered items.</td>
</tr>
<tr>
<td>applicationPrototypes</td>
<td>array</td>
<td>Names of application prototypes to be assigned to the item prototype.</td>
</tr>
<tr>
<td>preprocessing</td>
<td>array</td>
<td>Item prototype preprocessing options.</td>
</tr>
</tbody>
</table>

**Return values**

(object) Returns an object containing the IDs of the created item prototypes under the itemids property. The order of the returned IDs matches the order of the passed item prototypes.

**Examples**

**Creating an item prototype**

Create an item prototype to monitor free disk space on a discovered file system. Discovered items should be numeric Zabbix agent items updated every 30 seconds.

**Request:**

```json
{
    "jsonrpc": "2.0",
    "method": "itemprototype.create",
    "params": {
        "name": "Free disk space on {#FSNAME}",
        "key_": "vfs.fs.size[#{FSNAME},free]",
        "hostid": "10197"
    }
}
```
Creating an item prototype with preprocessing

Create an item using change per second and a custom multiplier as a second step.

Request:

```
{
    "jsonrpc": "2.0",
    "method": "itemprototype.create",
    "params": {
        "name": "Incoming network traffic on {#IFNAME}\n", 
        "key_": "net.if.in[{#IFNAME}]\n",
        "hostid": "10001",
        "ruleid": "27665",
        "type": 0,
        "value_type": 3,
        "delay": "60s",
        "units": "bps",
        "interfaceid": "1155",
        "preprocessing": [
            {
                "type": "10",
                "params": ""
            },
            {
                "type": "1",
                "params": "8"
            }
        ],
        "auth": "038e1d7b1735c6a5436ee9eae095879e",
        "id": 1
    }
}
```

Response:

```
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "44211"
        ]
    },
    "id": 1
}
```
Creating dependent item prototype

Create dependent item prototype for Master item prototype with ID 44211. Only dependencies on same host (template/discovery rule) are allowed, therefore Master and Dependent item should have same hostid and ruleid.

Request:

```json
{
    "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"
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "44212"
        ]
    },
    "id": 1
}
```

Create HTTP agent item prototype

Create item prototype with URL using user macro, query fields and custom headers.

Request:

```json
{
    "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": [
        {
            "min": "10"
        },
        {
            "max": "100"
        }
    ],
    "headers": {
        "X-Source": "api"
    },
    "delay": "35"
}
```
Response:
{
   "jsonrpc": "2.0",
   "result": {
      "itemids": [
         "28305"
      ],
   },
   "id": 1
}

Source
CItemPrototype::create() in frontends/php/include/classes/api/services/CItemPrototype.php.

**itemprototype.delete**

Description

object itemprototype.delete(array itemPrototypeIds)

This method allows to delete item prototypes.

Parameters

(array) IDs of the item prototypes to delete.

Return values

(object) Returns an object containing the IDs of the deleted item prototypes under the prototypeIds property.

Examples

Deleting multiple item prototypes

Delete two item prototypes.

Dependent item prototypes are removed automatically if master item or item prototype is deleted.

Request:
{
   "jsonrpc": "2.0",
   "method": "itemprototype.delete",
   "params": [
      "27352",
      "27356"
   ],
   "auth": "3a57200802b24cda67c4e4010b50c065",
   "id": 1
}

Response:
{
   "jsonrpc": "2.0",
   "result": {
      "prototypeIds": [
         "27352",
         "27356"
      ]
   },
   "id": 1
}
## itemprototype.get

### Description

**integer/array itemprototype.get(object parameters)**

The method allows to retrieve item prototypes according to the given parameters.

### Parameters

**(object)** Parameters defining the desired output.

The method supports the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>discoveryids</td>
<td>string/array</td>
<td>Return only item prototypes that belong to the given LLD rules.</td>
</tr>
<tr>
<td>graphids</td>
<td>string/array</td>
<td>Return only item prototypes that are used in the given graph prototypes.</td>
</tr>
<tr>
<td>hostids</td>
<td>string/array</td>
<td>Return only item prototypes that belong to the given hosts.</td>
</tr>
<tr>
<td>inherited</td>
<td>boolean</td>
<td>If set to true return only item prototypes inherited from a template.</td>
</tr>
<tr>
<td>itemids</td>
<td>string/array</td>
<td>Return only item prototypes with the given IDs.</td>
</tr>
<tr>
<td>monitored</td>
<td>boolean</td>
<td>If set to true return only enabled item prototypes that belong to monitored hosts.</td>
</tr>
<tr>
<td>templated</td>
<td>boolean</td>
<td>If set to true return only item prototypes that belong to templates.</td>
</tr>
<tr>
<td>templateids</td>
<td>string/array</td>
<td>Return only item prototypes that belong to the given templates.</td>
</tr>
<tr>
<td>triggerids</td>
<td>string/array</td>
<td>Return only item prototypes that are used in the given trigger prototypes.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>selectApplications</td>
<td>query</td>
<td>Return applications that the item prototype belongs to in the applications property.</td>
</tr>
<tr>
<td>selectApplicationPrototypes</td>
<td></td>
<td>Return application prototypes linked to item prototype in applicationPrototypes property.</td>
</tr>
<tr>
<td>selectDiscoveryRule</td>
<td>query</td>
<td>Return the low-level discovery rule that the item prototype belongs to in the discoveryRule property.</td>
</tr>
<tr>
<td>selectGraphs</td>
<td>query</td>
<td>Return graph prototypes that the item prototype is used in the graphs property. Supports count.</td>
</tr>
<tr>
<td>selectHosts</td>
<td>query</td>
<td>Return the host that the item prototype belongs to as an array in the hosts property. Returns count.</td>
</tr>
<tr>
<td>selectTriggers</td>
<td>query</td>
<td>Return trigger prototypes that the item prototype is used in the triggers property. Supports count.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>selectPreprocessing</td>
<td>query</td>
<td>Return item preprocessing options in preprocessing property.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>It has the following properties:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>type - (string)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The preprocessing option types:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - Custom multiplier;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 - Right trim;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 - Left trim;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 - Trim;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5 - Regular expression matching;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6 - Boolean to decimal;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7 - Octal to decimal;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8 - Hexadecimal to decimal;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9 - Simple change;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10 - Change per second.</td>
</tr>
<tr>
<td>params</td>
<td>(string)</td>
<td>Additional parameters used by preprocessing option. Multiple parameters are separated by LF (\n) character.</td>
</tr>
<tr>
<td>filter</td>
<td>object</td>
<td>Return only those results that exactly match the given filter.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Accepts an array, where the keys are property names, and the values are either a single value or an array of values to match against.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Supports additional filters:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>host - technical name of the host that the item prototype belongs to.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>limitSelects</td>
<td>integer</td>
<td>Limits the number of records returned by subselects.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Applies to the following subselects:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>selectGraphs - results will be sorted by name; selectTriggers - results will be sorted by description.</td>
</tr>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Sort the result by the given properties.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values are: itemid, name, key_, delay, type and status.</td>
</tr>
<tr>
<td>countOutput</td>
<td>boolean</td>
<td>These parameters being common for all get methods are described in detail in the reference commentary.</td>
</tr>
<tr>
<td>editable</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>excludeSearch</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>limit</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>output</td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>preservekeys</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>search</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>searchByAny</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>searchWildcardsEnabled</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>sortOrder</td>
<td>string/array</td>
<td></td>
</tr>
<tr>
<td>startSearch</td>
<td>boolean</td>
<td></td>
</tr>
</tbody>
</table>

Return values

(integer/array) Returns either:

- an array of objects;
- the count of retrieved objects, if the countOutput parameter has been used.

Examples

Retrieving item prototypes from an LLD rule

Retrieve all item prototypes from an LLD rule.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "itemprototype.get",
    "params": {
        "output": "extend",
        "discoveryids": "27426"
    }
}
```
Response:

{
  "jsonrpc": "2.0",
  "result": [
    {
      "itemid": "23077",
      "type": "0",
      "snmp_community": "",
      "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",
      "snmpv3_securityname": "",
      "snmpv3_securitylevel": "0",
      "snmpv3_authpassphrase": "",
      "snmpv3_privpassphrase": "",
      "formula": "",
      "error": "",
      "lastlogsize": "0",
      "logtimefmt": "",
      "templateid": "0",
      "valuemapid": "0",
      "params": "",
      "ipmi_sensor": "",
      "authtype": "0",
      "username": "",
      "password": "",
      "publickey": "",
      "privatekey": "",
      "mtime": "0",
      "flags": "0",
      "interfaceid": "0",
      "port": "",
      "description": "",
      "inventory_link": "0",
      "lifetime": "30d",
      "snmpv3_authprotocol": "0",
      "snmpv3_privprotocol": "0",
      "state": "0",
      "snmpv3_contextname": "",
      "evaltype": "0",
      "jmx_endpoint": "",
      "master_itemid": "0",
      "timeout": "3s",
      "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",
"lastclock": "0",
"lastns": "0",
"lastvalue": "0",
"prevvalue": "0"
},
{
"itemid": "10010",
"type": "0",
"snmp_community": "",
"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": "",
"snmpv3_securityname": "",
"snmpv3_securitylevel": "0",
"snmpv3_authprotocol": "0",
"snmpv3_privprotocol": "0",
"snmpv3_authpassphrase": "",
"snmpv3_privpassphrase": "",
"formula": "",
"error": "",
"lastlogsize": "0",
"logtimefmt": "",
"templateid": "0",
"valuemapid": "0",
"params": "",
"ipmi_sensor": "",
"authtype": "0",
"username": "",
"password": "",
"publickey": "",
"privatekey": "",
"mtime": "0",
"flags": "0",
"interfaceid": "0",
"port": "",
"description": "The processor load is calculated as system CPU load divided by number of CPU cores.",
"inventory_link": "0",
"lifetime": "0",
"snmpv3_authprotocol": "0",
"snmpv3_privprotocol": "0",
"state": "0",
"snmpv3_contextname": "",
"evaltype": "0",
"jmx_endpoint": "",
"master_itemid": "0",
"timeout": "3s",
```
Finding dependent item

Find one Dependent item for item with ID "25545".

Request:

```
{  
    "jsonrpc": "2.0",  
    "method": "item.get",  
    "params": {  
        "output": "extend",  
        "filter": {  
            "type": "18",  
            "master_itemid": "25545"  
        },  
        "limit": "1"  
    },  
    "auth": "038e1d7b1735c6a5436ee9eae095879e",  
    "id": 1
}
```

Response:

```
{  
    "jsonrpc": "2.0",  
    "result": [  
        {  
            "itemid": "25547",  
            "type": "18",  
            "snmp_community": "",  
            "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": "",
"snmpv3_securityname": "",
"snmpv3_securitylevel": "0",
"snmpv3_authtype": "",
"snmpv3_privprotocol": "",
"evaltype": "",
"error": "",
"lastlogsize": "0",
"logtimefmt": "",
"templateid": "0",
"valuemapid": "0",
"params": "",
"ipmi_sensor": "",
"authtype": "0",
"username": "",
"password": "",
"publickey": "",
"privatekey": "",
"mtime": "0",
"flags": "0",
"interfaceid": "0",
"port": "",
"description": "",
"inventory_link": "0",
"lifetime": "30d",
"snmpv3_authprotocol": "0",
"snmpv3_privprotocol": "0",
"state": "0",
"snmpv3_contextname": "",
"evaltype": "0",
"master_itemid": "25545",
"jmx_endpoint": "",
"master_itemid": "0",
"timeout": "3s",
"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",
"lastclock": "0",
"lastns": "0",
"lastvalue": "0",
"prevvalue": "0"
}],
"id": 1
Find HTTP agent item prototype with request method HEAD for specific host id.

Request:

```json
{
  "jsonrpc": "2.0",
  "method": "itemprototype.get",
  "params": {
    "hostids": "10254",
    "filter": {
      "type": "19",
      "request_method": "3"
    }
  },
  "id": 17,
  "auth": "d678e0b85688ce578ff061bd29a20d3b"
}
```

Response:

```json
{
  "jsonrpc": "2.0",
  "result": [
    {
      "itemid": "28257",
      "type": "19",
      "snmp_community": "",
      "snmp_oid": "",
      "hostid": "10254",
      "name": "discovered",
      "key_": "item[#{INAME}]",
      "delay": "#{IUPDATE}'",
      "history": "90d",
      "trends": "30d",
      "status": "0",
      "value_type": "3",
      "trapper_hosts": "",
      "units": "",
      "snmpv3_securityname": "",
      "snmpv3_securitylevel": "0",
      "snmpv3_authpassphrase": "",
      "snmpv3_privpassphrase": "",
      "formula": "",
      "error": "",
      "lastlogsize": "0",
      "logtimefmt": "",
      "templateid": "28255",
      "valuemapid": "0",
      "params": "",
      "ipmi_sensor": "",
      "authtype": "0",
      "username": "",
      "password": "",
      "publickey": "",
      "privatekey": "",
      "mtime": "0",
      "flags": "2",
      "interfaceid": "2",
      "port": "",
      "description": "",
      "inventory_link": "0",
      "lifetime": "30d",
      "snmpv3_authprotocol": "0",
      "snmpv3_privprotocol": "0",
      "state": "0"
    }
  ]
}
```
See also

- Application
- Host
- Graph prototype
- Trigger prototype

Source

CItemPrototype::get() in frontends/php/include/classes/api/services/CItemPrototype.php.

**itemprototype.update**

**Description**

object itemprototype.update(object/array itemPrototypes)

This method allows to update existing item prototypes.

**Parameters**

(object/array) Item prototype properties to be updated.

The `itemid` property must be defined for each item prototype, all other properties are optional. Only the passed properties will be updated, all others will remain unchanged.

Additionally to the **standard item prototype properties**, the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>applications</td>
<td>array</td>
<td>IDs of the applications to replace the current applications.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>applicationPrototypes</td>
<td>array</td>
<td>Names of the application prototypes to replace the current application prototypes.</td>
</tr>
<tr>
<td>preprocessing</td>
<td>array</td>
<td>Item prototype preprocessing options to replace the current preprocessing options.</td>
</tr>
</tbody>
</table>

Return values

*(object)* Returns an object containing the IDs of the updated item prototypes under the *itemids* property.

Examples

Changing the interface of an item prototype

Change the host interface that will be used by discovered items.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "itemprototype.update",
    "params": {
        "itemid": "27428",
        "interfaceid": "132"
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "27428"
        ]
    },
    "id": 1
}
```

Update dependent item prototype

Update Dependent item prototype with new Master item prototype ID. Only dependencies on same host (template/discovery rule) are allowed, therefore Master and Dependent item should have same hostid and ruleid.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "itemprototype.update",
    "params": {
        "master_itemid": "25570",
        "itemid": "189030"
    },
    "auth": "700ca65537074ec963db7efabda78259",
    "id": 1
}
```
Response:
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "189030"
        ],
    },
    "id": 1
}

Update HTTP agent item prototype
Change query fields and remove all custom headers.
Request:
{
    "jsonrpc": "2.0",
    "method": "itemprototype.update",
    "params": {
        "itemid": "28305",
        "query_fields": [
            {
                "random": "qwertyuiopasdfghjklzxcvbnm"
            }
        ],
        "headers": []
    },
    "auth": "700ca65537074ec963db7efabda78259",
    "id": 1
}

Response:
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "28305"
        ],
    },
    "id": 1
}

Source
CItemPrototype::update() in frontends/php/include/classes/api/services/CItemPrototype.php.

**LLD rule**

This class is designed to work with low level discovery rules.

Object references:

- **LLD rule**

Available methods:

- **discoveryrule.copy** - copying LLD rules
- **discoveryrule.create** - creating new LLD rules
- **discoveryrule.delete** - deleting LLD rules
- **discoveryrule.get** - retrieving LLD rules
- **discoveryrule.update** - updating LLD rules
## LLD rule object

The following objects are directly related to the discoveryrule API.

**LLD rule**

The low-level discovery rule object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>itemid</td>
<td>string</td>
<td>(readonly) ID of the LLD rule.</td>
</tr>
<tr>
<td>delay</td>
<td>string</td>
<td>Update interval of the LLD rule.</td>
</tr>
<tr>
<td></td>
<td>(required)</td>
<td>Accepts seconds or time unit with suffix and with or without one or more custom intervals that consist of either flexible intervals and scheduling intervals as serialized strings. Also accepts user macros. Flexible intervals could be written as two macros separated by a forward slash. Intervals are separated by a semicolon.</td>
</tr>
<tr>
<td>hostid</td>
<td>string</td>
<td>ID of the host that the LLD rule belongs to.</td>
</tr>
<tr>
<td></td>
<td>(required)</td>
<td></td>
</tr>
<tr>
<td>interfaceid</td>
<td>string</td>
<td>ID of the LLD rule's host interface. Used only for host LLD rules.</td>
</tr>
<tr>
<td></td>
<td>(required)</td>
<td></td>
</tr>
<tr>
<td>key_</td>
<td>string</td>
<td>LLD rule key.</td>
</tr>
<tr>
<td></td>
<td>(required)</td>
<td></td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>Name of the LLD rule.</td>
</tr>
<tr>
<td></td>
<td>(required)</td>
<td></td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>type</td>
<td>integer</td>
<td>Type of the LLD rule. Possible values: 0 - Zabbix agent; 1 - SNMPv1 agent; 2 - Zabbix trapper; 3 - simple check; 4 - SNMPv2 agent; 5 - Zabbix internal; 6 - SNMPv3 agent; 7 - Zabbix agent (active); 10 - external check; 11 - database monitor; 12 - IPMI agent; 13 - SSH agent; 14 - TELNET agent; 16 - JMX agent; 19 - HTTP agent;</td>
</tr>
<tr>
<td>url</td>
<td>string</td>
<td>String URL string, required for HTTP agent LLD rule. Supports user macros, {HOST.IP}, {HOST.CONN}, {HOST.DNS}, {HOST.HOST}, {HOST.NAME}, {ITEM.ID}, {ITEM.KEY}.</td>
</tr>
<tr>
<td>allow_traps</td>
<td>integer</td>
<td>HTTP agent LLD rule field. Allow to populate value as in trapper item type also. 0 - (default) Do not allow to accept incoming data. 1 - Allow to accept incoming data.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>authtype</td>
<td>integer</td>
<td>Used only by SSH agent or HTTP agent LLD rules. SSH agent authentication method possible values: 0 - (default) password; 1 - public key.</td>
</tr>
<tr>
<td>description</td>
<td>string</td>
<td>Description of the LLD rule. (readonly) Error text if there are problems updating the LLD rule.</td>
</tr>
<tr>
<td>error</td>
<td>string</td>
<td>HTTP agent LLD rule field. Follow response redirects while pooling data. 0 - Do not follow redirects. 1 - (default) Follow redirects.</td>
</tr>
<tr>
<td>follow_redirects</td>
<td>integer</td>
<td>HTTP agent LLD rule field. Object with HTTP(S) request headers, where header name is used as key and header value as value. Example:</td>
</tr>
<tr>
<td>http_proxy</td>
<td>string</td>
<td>HTTP agent LLD rule field. HTTP(S) proxy connection string.</td>
</tr>
<tr>
<td>ipmi_sensor</td>
<td>string</td>
<td>IPMI sensor. Used only by IPMI LLD rules.</td>
</tr>
<tr>
<td>jmx_endpoint</td>
<td>string</td>
<td>JMX agent custom connection string.</td>
</tr>
</tbody>
</table>

Default value:
```
service:jmx:rmi:///jndi/rmi://{HOST.CONN}:{HOST.PORT}/jmxrmi
```
<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lifetime</td>
<td>string</td>
<td>Time period after which items that are no longer discovered will be deleted. Accepts seconds, time unit with suffix and user macro.</td>
</tr>
<tr>
<td>output_format</td>
<td>integer</td>
<td>Default: 30d. HTTP agent LLD rule field. Should response be converted to JSON.</td>
</tr>
<tr>
<td>params</td>
<td>string</td>
<td>Additional parameters depending on the type of the LLD rule:</td>
</tr>
<tr>
<td>password</td>
<td>string</td>
<td>Password for authentication. Used by simple check, SSH, Telnet, database monitor, JMX and HTTP agent LLD rules.</td>
</tr>
<tr>
<td>port</td>
<td>string</td>
<td>Port used by the LLD rule. Used only by SNMP LLD rules.</td>
</tr>
<tr>
<td>post_type</td>
<td>integer</td>
<td>HTTP agent LLD rule field. Type of post data body stored in posts property.</td>
</tr>
<tr>
<td>posts</td>
<td>string</td>
<td>HTTP agent LLD rule field. HTTP(S) request body data. Used with post_type.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>privatekey</td>
<td>string</td>
<td>Name of the private key file.</td>
</tr>
<tr>
<td>publickey</td>
<td>string</td>
<td>Name of the public key file.</td>
</tr>
<tr>
<td>query_fields</td>
<td>array</td>
<td>HTTP agent LLD rule field. Query parameters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Array of objects with 'key':'value' pairs, where value can be empty string.</td>
</tr>
<tr>
<td>request_method</td>
<td>integer</td>
<td>HTTP agent LLD rule field. Type of request method.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - (default) GET</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - POST</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 - PUT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 - HEAD</td>
</tr>
<tr>
<td>retrieve_mode</td>
<td>integer</td>
<td>HTTP agent LLD rule field. What part of response should be stored.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - (default) Body.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - Headers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 - Both body and headers will be stored.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For request_method HEAD only 1 is allowed value.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SNMP community.</td>
</tr>
<tr>
<td>snmp_community</td>
<td>string</td>
<td>Required for SNMPv1 and SNMPv2 LLD rules.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SNMP OID.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SNMPv3 auth passphrase. Used only by SNMPv3 LLD rules.</td>
</tr>
<tr>
<td>snmpv3_authpassphrase</td>
<td>string</td>
<td>SNMPv3 authentication protocol. Used only by SNMPv3 LLD rules.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - (default) MD5;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - SHA.</td>
</tr>
<tr>
<td>snmpv3_context</td>
<td>string</td>
<td>SNMPv3 context name. Used only by SNMPv3 checks.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>snmpv3_privpassphrasestring</td>
<td>string</td>
<td>SNMPv3 priv passphrase. Used only by SNMPv3 LLD rules.</td>
</tr>
<tr>
<td>snmpv3_privprotocolinteger</td>
<td>integer</td>
<td>SNMPv3 privacy protocol. Used only by SNMPv3 LLD rules. Possible values: 0 - (default) DES; 1 - AES.</td>
</tr>
<tr>
<td>snmpv3_securityinteger</td>
<td>integer</td>
<td>SNMPv3 security level. Used only by SNMPv3 LLD rules. Possible values: 0 - noAuthNoPriv; 1 - authNoPriv; 2 - authPriv.</td>
</tr>
<tr>
<td>snmpv3_securitystring</td>
<td>string</td>
<td>SNMPv3 security name. Used only by SNMPv3 LLD rules.</td>
</tr>
<tr>
<td>ssl_cert_filestring</td>
<td>string</td>
<td>HTTP agent LLD rule field. Public SSL Key file path.</td>
</tr>
<tr>
<td>ssl_key_filestring</td>
<td>string</td>
<td>HTTP agent LLD rule field. Private SSL Key file path.</td>
</tr>
<tr>
<td>ssl_key_passwordstring</td>
<td>string</td>
<td>HTTP agent LLD rule field. Password for SSL Key file. (readonly) State of the LLD rule.</td>
</tr>
<tr>
<td>stateinteger</td>
<td>integer</td>
<td>(readonly) State of the LLD rule. Possible values: 0 - (default) normal; 1 - not supported. Status of the LLD rule.</td>
</tr>
<tr>
<td>statusinteger</td>
<td>integer</td>
<td>Possible values: 0 - (default) enabled LLD rule; 1 - disabled LLD rule.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>status_codes</td>
<td>string</td>
<td>HTTP agent LLD rule field. Ranges of required HTTP status codes separated by commas. Also supports user macros as part of comma separated list. Example: 200,200-{$M},{$M},200-400</td>
</tr>
<tr>
<td>templateid</td>
<td>string</td>
<td>(readonly) ID of the parent template LLD rule.</td>
</tr>
<tr>
<td>timeout</td>
<td>string</td>
<td>HTTP agent LLD rule field. Item data polling request timeout. Support user macros. default: 3s maximum value: 60s</td>
</tr>
<tr>
<td>trapper_hosts</td>
<td>string</td>
<td>Allowed hosts. Used by trapper LLD rules or HTTP agent LLD rules.</td>
</tr>
<tr>
<td>username</td>
<td>string</td>
<td>Username for authentication. Used by simple check, SSH, Telnet, database monitor, JMX and HTTP agent LLD rules. Required by SSH and Telnet LLD rules.</td>
</tr>
<tr>
<td>verify_host</td>
<td>integer</td>
<td>HTTP agent LLD rule field. Validate host name in URL is in Common Name field or a Subject Alternate Name field of host certificate. 0 - (default) Do not validate. 1 - Validate.</td>
</tr>
</tbody>
</table>
### Property

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>verify_peer</td>
<td>integer</td>
<td>HTTP agent LLD rule field. Validate is host certificate authentic.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - (default) Do not validate. 1 - Validate.</td>
</tr>
</tbody>
</table>

Note that for some methods (update, delete) the required/optional parameter combination is different.

### LLD rule filter

The LLD rule filter object defines a set of conditions that can be used to filter discovered objects. It has the following properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>conditions</td>
<td>array</td>
<td>Set of filter conditions to use for filtering results.</td>
</tr>
<tr>
<td>evaltype</td>
<td>integer</td>
<td>Filter condition evaluation method.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values: 0 - and/or; 1 - and; 2 - or; 3 - custom expression.</td>
</tr>
<tr>
<td>eval_formula</td>
<td>string</td>
<td>Generated expression that will be used for evaluating filter conditions. The expression contains IDs that reference specific filter conditions by its formulaid. The value of eval_formula is equal to the value of formula for filters with a custom expression.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>formula</td>
<td>string</td>
<td>User-defined expression to be used for evaluating conditions of filters with a custom expression. The expression must contain IDs that reference specific filter conditions by its formulaid. The IDs used in the expression must exactly match the ones defined in the filter conditions: no condition can remain unused or omitted. Required for custom expression filters.</td>
</tr>
</tbody>
</table>

LLD rule filter condition

The LLD rule filter condition object defines a separate check to perform on the value of an LLD macro. It has the following properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>macro</td>
<td>string</td>
<td>LLD macro to perform the check on.</td>
</tr>
<tr>
<td>value</td>
<td>string</td>
<td>Value to compare with.</td>
</tr>
<tr>
<td>formulaid</td>
<td>string</td>
<td>Arbitrary unique ID that is used to reference the condition from a custom expression. Can only contain capital-case letters. The ID must be defined by the user when modifying filter conditions, but will be generated anew when requesting them afterward.</td>
</tr>
</tbody>
</table>
### discoveryrule.copy

**Description**

`object discoveryrule.copy(object parameters)`

This method allows to copy LLD rules with all of the prototypes to the given hosts.

**Parameters**

*(object)* Parameters defining the LLD rules to copy and the target hosts.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>discoveryids</td>
<td>array</td>
<td>IDs of the LLD rules to be copied.</td>
</tr>
<tr>
<td>hostids</td>
<td>array</td>
<td>IDs of the hosts to copy the LLD rules to.</td>
</tr>
</tbody>
</table>

**Return values**

*(boolean)* Returns `true` if the copying was successful.

**Examples**

Copy an LLD rule to multiple hosts

Copy an LLD rule to two hosts.

**Request:**

```json
{
    "jsonrpc": "2.0",
    "method": "discoveryrule.copy",
    "params": {
        "discoveryids": [27426],
        "hostids": [
            "10196",
            "10197"
        ]
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

**Response:**

Note:

To better understand how to use filters with various types of expressions, see examples on the `discoveryrule.get` and `discoveryrule.create` method pages.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>operator</td>
<td>integer</td>
<td>Condition operator.</td>
</tr>
</tbody>
</table>

Possible values:

- 8 - (default) matches regular expression;
- 9 - does not match regular expression.
discoveryrule.create

Description

object discoveryrule.create(object/array lldRules)

This method allows to create new LLD rules.

Parameters

(object/array) LLD rules to create.

Additionally to the standard LLD rule properties, the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter</td>
<td>object</td>
<td>LLD rule filter object for the LLD rule.</td>
</tr>
</tbody>
</table>

Return values

(object) Returns an object containing the IDs of the created LLD rules under the itemids property. The order of the returned IDs matches the order of the passed LLD rules.

Examples

Creating an LLD rule

Create a Zabbix agent LLD rule to discover mounted file systems. Discovered items will be updated every 30 seconds.

Request:

```json
{
   "jsonrpc": "2.0",
   "method": "discoveryrule.create",
   "params": {
      "name": "Mounted filesystem discovery",
      "key_": "vfs.fs.discovery",
      "hostid": "10197",
      "type": "0",
      "interfaceid": "112",
      "delay": "30s"
   },
   "auth": "038e1d7b1735c6a5436ee9eae095879e",
   "id": 1
}
```

Response:

```json
{
   "jsonrpc": "2.0",
   "result": {
      "itemids": [
         "27665"
      ]
   },
   "id": 1
}
```
Using a filter

Create an LLD rule with a set of conditions to filter the results by. The conditions will be grouped together using the logical "and" operator.

Request:

```json
{
    "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}"
                },
                {
                    "macro": "{#MACRO2}"
                },
                {
                    "macro": "{#MACRO3}"
                }
            ]
        }
    }
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "27665"
        ],
    },
    "id": 1
}
```

Using a custom expression filter

Create an LLD rule with a filter that will use a custom expression to evaluate the conditions. The LLD rule must only discover objects the "(#MACRO1)" macro value of which matches both regular expression "regex1" and "regex2", and the value of "(#MACRO2)" matches either "regex3" or "regex4". The formula IDs "A", "B", "C" and "D" have been chosen arbitrarily.

Request:

```json
{
    "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"
    }
  ]
},
"auth": "038e1d7b1735c6a5436ee9eae095879e",
"id": 1
}

Response:
{
  "jsonrpc": "2.0",
  "result": {
    "itemids": [27665]
  },
  "id": 1
}

Using custom query fields and headers
Create LLD rule with custom query fields and headers.

Request:
{
  "jsonrpc": "2.0",
  "method": "discoveryrule.create",
  "params": {
    "hostid": "10257",
    "interfaceid": "5",
    "type": "19",
    "name": "API HTTP agent",
    "key_": "api_discovery_rule",
    "value_type": "3",
    "delay": "5s",
    "url": "http://127.0.0.1?discoverer.php",
    "query_fields": []
  }
}
"mode": "json",
},

"elements": "2"
}
]
"headers": {
    "X-Type": "api",
    "Authorization": "Bearer mF_A.B5f-2.1JcM"
},
"allow_traps": "1",
"trapper_hosts": "127.0.0.1",
"id": 35,
"auth": "d678e0b85688ce578ff061bd29a20d3b",
}
}

Response:
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "28336"
        ]
    },
    "id": 35
}

See also
• LLD rule filter

Source
CDiscoveryRule::create() in frontends/php/include/classes/api/services/CDiscoveryRule.php.

discoveryrule.delete

Description
object discoveryrule.delete(array lldRuleIds)
This method allows to delete LLD rules.

Parameters
(array) IDs of the LLD rules to delete.

Return values
(object) Returns an object containing the IDs of the deleted LLD rules under the ruleids property.

Examples
Deleting multiple LLD rules
Delete two LLD rules.

Request:
{
    "jsonrpc": "2.0",
    "method": "discoveryrule.delete",
    "params": [
        "27665",
        "27668"
    ],
    "auth": "3a57200802b24cda67c4e4010b50c065",
}
Response:
{
  "jsonrpc": "2.0",
  "result": {
    "ruleids": [
      "27665",
      "27668"
    ]
  },
  "id": 1
}

Source
CDiscoveryRule::delete() in frontends/php/include/classes/api/services/CDiscoveryRule.php.

discoveryrule.get

Description
integer/array discoveryrule.get(object parameters)
The method allows to retrieve LLD rules according to the given parameters.

Parameters
(object) Parameters defining the desired output.
The method supports the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>itemids</td>
<td>string/array</td>
<td>Return only LLD rules with the given IDs.</td>
</tr>
<tr>
<td>hostids</td>
<td>string/array</td>
<td>Return only LLD rules that belong to the given hosts.</td>
</tr>
<tr>
<td>inherited</td>
<td>boolean</td>
<td>If set to true return only LLD rules inherited from a template.</td>
</tr>
<tr>
<td>interfaceids</td>
<td>string/array</td>
<td>Return only LLD rules use the given host interfaces.</td>
</tr>
<tr>
<td>monitored</td>
<td>boolean</td>
<td>If set to true return only enabled LLD rules that belong to monitored hosts.</td>
</tr>
<tr>
<td>templated</td>
<td>boolean</td>
<td>If set to true return only LLD rules that belong to templates.</td>
</tr>
<tr>
<td>templateids</td>
<td>string/array</td>
<td>Return only LLD rules that belong to the given templates.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>selectFilter</td>
<td>query</td>
<td>Returns the filter used by the LLD rule in the filter property.</td>
</tr>
<tr>
<td>selectGraphs</td>
<td>query</td>
<td>Returns graph prototypes that belong to the LLD rule in the graphs property.</td>
</tr>
<tr>
<td>selectHostPrototypes</td>
<td>query</td>
<td>Supports count. Returns host prototypes that belong to the LLD rule in the hostPrototypes property.</td>
</tr>
<tr>
<td>selectHosts</td>
<td>query</td>
<td>Supports count. Returns the host that the LLD rule belongs to as an array in the hosts property.</td>
</tr>
<tr>
<td>selectItems</td>
<td>query</td>
<td>Returns item prototypes that belong to the LLD rule in the items property.</td>
</tr>
<tr>
<td>selectTriggers</td>
<td>query</td>
<td>Supports count. Returns trigger prototypes that belong to the LLD rule in the triggers property.</td>
</tr>
<tr>
<td>filter</td>
<td>object</td>
<td>Return only those results that exactly match the given filter.</td>
</tr>
</tbody>
</table>

Accepts an array, where the keys are property names, and the values are either a single value or an array of values to match against.

Supports additional filters:
- host - technical name of the host that the LLD rule belongs to.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>limitSelects</td>
<td>integer</td>
<td>Limits the number of records returned by subselects. Applies to the following subselects: selectItems; selectGraphs; selectTriggers.</td>
</tr>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Sort the result by the given properties. Possible values are: itemid, name, key, delay, type and status.</td>
</tr>
<tr>
<td>countOutput</td>
<td>boolean</td>
<td>These parameters being common for all get methods are described in detail in the reference commentary.</td>
</tr>
<tr>
<td>editable</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>excludeSearch</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>limit</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>output</td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>preservekeys</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>search</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>searchByAny</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>searchWildcards</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>sortOrder</td>
<td>string/array</td>
<td></td>
</tr>
<tr>
<td>startSearch</td>
<td>boolean</td>
<td></td>
</tr>
</tbody>
</table>

Return values

(integer/array) Returns either:

- an array of objects;
- the count of retrieved objects, if the countOutput parameter has been used.

Examples

Retrieving discovery rules from a host

Retrieve all discovery rules from host "10202".

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "discoveryrule.get",
    "params": {
        "output": "extend",
        "hostids": "10202"
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

972
"jsonrpc": "2.0",
"result": [
{
"itemid": "27425",
"type": "0",
"snmp_community": "",
"snmp_oid": "",
"hostid": "10202",
"name": "Network interface discovery",
"key_": "net.if.discovery",
"delay": "1h",
"state": "0",
"status": "0",
"trapper_hosts": "",
"snmpv3_securityname": "",
"snmpv3_securitylevel": "0",
"snmpv3_authpassphrase": "",
"snmpv3_privpassphrase": "",
"error": "",
"templateid": "22444",
"params": "",
"ipmi_sensor": "",
"authtype": "0",
"username": "",
"password": "",
"publickey": "",
"privatekey": "",
"interfaceid": "119",
"port": "",
"description": "Discovery of network interfaces as defined in global regular expression "Network interfaces for discovery",
"lifetime": "30d",
"snmpv3_authprotocol": "0",
"snmpv3_privprotocol": "0",
"snmpv3_contextname": "",
"jmx_endpoint": "",
"master_itemid": "0",
"timeout": "3s",
"url": "",
"query_fields": [],
"posts": "",
"status_codes": "200",
"follow_redirects": "1",
"post_type": "0",
"http_proxy": "",
"headers": [],
"retrieve_mode": "0",
"request_method": "0",
"ssl_cert_file": "",
"ssl_key_file": "",
"ssl_key_password": "",
"verify_peer": "0",
"verify_host": "0",
"allow_traps": "0"
},
{
"itemid": "27426",
"type": "0",
"snmp_community": "",
"snmp_oid": "",
"hostid": "10202",
"name": "Mounted filesystem discovery",
"key_": "net.fs.discovery",
"delay": "1h",
"state": "0",
"status": "0",
"trapper_hosts": "",
"snmpv3_securityname": "",
"snmpv3_securitylevel": "0",
"snmpv3_authpassphrase": "",
"snmpv3_privpassphrase": "",
"error": "",
"templateid": "22444",
"params": "",
"ipmi_sensor": "",
"authtype": "0",
"username": "",
"password": "",
"publickey": "",
"privatekey": "",
"interfaceid": "119",
"port": "",
"description": "Discovery of mounted filesystems as defined in global regular expression "Mounted filesystem discovery",
"lifetime": "30d",
"snmpv3_authprotocol": "0",
"snmpv3_privprotocol": "0",
"snmpv3_contextname": "",
"jmx_endpoint": "",
"master_itemid": "0",
"timeout": "3s",
"url": "",
"query_fields": [],
"posts": "",
"status_codes": "200",
"follow_redirects": "1",
"post_type": "0",
"http_proxy": "",
"headers": [],
"retrieve_mode": "0",
"request_method": "0",
"ssl_cert_file": "",
"ssl_key_file": "",
"ssl_key_password": "",
"verify_peer": "0",
"verify_host": "0",
"allow_traps": "0"
}]}
Retrieving filter conditions

Retrieves the name of the LLD rule "24681" and its filter conditions. The filter uses the "and" evaluation type, so the formula property is empty and eval_formula is generated automatically.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "discoveryrule.get",
    "params": {
        "output": ["name"],
        "selectFilter": "extend",
```
Retrieve LLD rule by URL

Retrieve LLD rule for host by rule URL field value. Only exact match of URL string defined for LLD rule is supported.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "discoveryrule.get",
    "params": {
        "hostids": "10257",
        "filter": {
            "type": "19",
            "url": "http://127.0.0.1/discoverer.php"
        }
    },
    "id": 39,
    "auth": "d678e0b85688ce578ff061bd29a20d3b"
}
```

Response:

```json
975
```
{
"jsonrpc": "2.0",
"result": [
{
"itemid": "28336",
"type": "19",
"snmp_community": "",
"snmp_oid": "",
"hostid": "10257",
"name": "API HTTP agent",
"key_": "api_discovery_rule",
"delay": "5s",
"history": "90d",
"trends": "0",
"status": "0",
"value_type": "4",
"trapper_hosts": "",
"units": "",
"snmpv3_securityname": "",
"snmpv3_securitylevel": "0",
"snmpv3_authpassphrase": "",
"snmpv3_privpassphrase": "",
"error": "",
"lastlogsize": "0",
"logtimefmt": "",
"templateid": "0",
"valuemapid": "0",
"params": "",
"ipmi_sensor": "",
"authtype": "0",
"username": "",
"password": "",
"publickey": "",
"privatekey": "",
"mtime": "0",
"flags": "1",
"interfaceid": "5",
"port": "",
"description": "",
"inventory_link": "0",
"lifetime": "30d",
"snmpv3_authprotocol": "0",
"snmpv3_privprotocol": "0",
"state": "0",
"snmpv3_contextname": "",
"jmx_endpoint": "",
"master_itemid": "0",
"timeout": "3s",
"url": "http://127.0.0.1/discoverer.php",
"query_fields": [
{
"mode": "json"
},
{
"elements": "2"
}
],
"posts": "",
"status_codes": "200",
"follow_redirects": "1",
"post_type": "0",
"http_proxy": "",

976


See also

- Graph prototype
- Host
- Item prototype
- LLD rule filter
- Trigger prototype

Source

CDiscoveryRule::get() in frontends/php/include/classes/api/services/CDiscoveryRule.php.

discoveryrule.update

Description

object discoveryrule.update(object/array lldRules)

This method allows to update existing LLD rules.

Parameters

(object/array) LLD rule properties to be updated.

The itemid property must be defined for each LLD rule, all other properties are optional. Only the passed properties will be updated, all others will remain unchanged.

Additionally to the standard LLD rule properties, the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter</td>
<td>object</td>
<td>LLD rule filter object to replace the current filter.</td>
</tr>
</tbody>
</table>

Return values

(object) Returns an object containing the IDs of the updated LLD rules under the itemids property.

Examples

Adding a filter to an LLD rule

Add a filter so that the contents of the `{#FSTYPE}` macro would match the @File systems for discovery regexp.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "discoveryrule.update",
    "params": {
        "itemid": "22450",
        "filter": {
            "evaltype": 1,
```
"conditions": [
    {
        "macro": "#{FSTYPE}",
        "value": "@File systems for discovery"
    }
  ],
  "auth": "038e1d7b1735c6a5436ee9eae095879e",
  "id": 1
}

Response:
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "22450"
        ],
        "id": 1
    }
}

Disable trapping

Disable LLD trapping for discovery rule.

Request:
{
    "jsonrpc": "2.0",
    "method": "discoveryrule.update",
    "params": {
        "itemid": "28336",
        "allow_traps": "0"
    },
    "id": 36,
    "auth": "d678e0b85688ce578ff061bd29a20d3b"
}

Response:
{
    "jsonrpc": "2.0",
    "result": {
        "itemids": [
            "28336"
        ],
        "id": 36
    }
}

Source

CDiscoveryRule::update() in frontends/php/include/classes/api/services/CDiscoveryRule.php.

Maintenance

This class is designed to work with maintenances.

Object references:

- Maintenance
- Time period
Available methods:

- `maintenance.create` - creating new maintenances
- `maintenance.delete` - deleting maintenances
- `maintenance.get` - retrieving maintenances
- `maintenance.update` - updating maintenances

> **Maintenance object**

The following objects are directly related to the `maintenance` API.

**Maintenance**

The maintenance object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>maintenanceid</code></td>
<td>string</td>
<td>(readonly) ID of the maintenance.</td>
</tr>
<tr>
<td><code>name</code></td>
<td>string</td>
<td>Name of the maintenance.</td>
</tr>
<tr>
<td><code>active_since</code></td>
<td>timestamp</td>
<td>Time when the maintenance becomes active.</td>
</tr>
<tr>
<td><code>active_till</code></td>
<td>timestamp</td>
<td>Time when the maintenance stops being active.</td>
</tr>
<tr>
<td><code>description</code></td>
<td>string</td>
<td>Description of the maintenance.</td>
</tr>
<tr>
<td><code>maintenance_type</code></td>
<td>integer</td>
<td>Type of maintenance. Possible values: 0 - (default) with data collection; 1 - without data collection.</td>
</tr>
<tr>
<td><code>tags_evaltype</code></td>
<td>integer</td>
<td>Problem tag evaluation method. Possible values: 0 - (default) And/Or; 2 - Or.</td>
</tr>
</tbody>
</table>

Note that for some methods (update, delete) the required/optional parameter combination is different.

**Time period**

The time period object is used to define periods when the maintenance must come into effect. It has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>timeperiodid</code></td>
<td>string</td>
<td>(readonly) ID of the maintenance.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>day</td>
<td>integer</td>
<td>Day of the month when the maintenance must come into effect. Required only for monthly time periods.</td>
</tr>
<tr>
<td>dayofweek</td>
<td>integer</td>
<td>Days are stored in binary form with each bit representing the corresponding day. For example, 4 equals 100 in binary and means, that maintenance will be enabled on Wednesday. Used for weekly and monthly time periods. Required only for weekly time periods.</td>
</tr>
<tr>
<td>every</td>
<td>integer</td>
<td>For daily and weekly periods every defines day or week intervals at which the maintenance must come into effect. For monthly periods every defines the week of the month when the maintenance must come into effect. Possible values: 1 - first week; 2 - second week; 3 - third week; 4 - fourth week; 5 - last week.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>--------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>month</td>
<td>integer</td>
<td>Months when the maintenance must come into effect. Months are stored in binary form with each bit representing the corresponding month. For example, 5 equals 101 in binary and means, that maintenance will be enabled in January and March. Required only for monthly time periods.</td>
</tr>
<tr>
<td>period</td>
<td>integer</td>
<td>Duration of the maintenance period in seconds. Default: 3600.</td>
</tr>
<tr>
<td>start_date</td>
<td>timestamp</td>
<td>Date when the maintenance period must come into effect. Required only for one time periods. Default: current date.</td>
</tr>
<tr>
<td>start_time</td>
<td>integer</td>
<td>Time of day when the maintenance starts in seconds. Required for daily, weekly and monthly periods. Type of time period. Possible values: 0 - (default) one time only; 2 - daily; 3 - weekly; 4 - monthly.</td>
</tr>
</tbody>
</table>
### Property Types

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tag</td>
<td>string</td>
<td>Problem tag name.</td>
</tr>
<tr>
<td>operator</td>
<td>integer</td>
<td>Condition operator.</td>
</tr>
<tr>
<td>value</td>
<td>string</td>
<td>Problem tag value.</td>
</tr>
</tbody>
</table>

#### maintenance.create

**Description**

`object maintenance.create(object/array maintenances)`

This method allows to create new maintenances.

**Parameters**

- (object/array) Maintenances to create.

Additionally to the standard maintenance properties, the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>groupids</td>
<td>array</td>
<td>IDs of the host groups that will undergo maintenance.</td>
</tr>
<tr>
<td>hostids</td>
<td>array</td>
<td>IDs of the hosts that will undergo maintenance.</td>
</tr>
<tr>
<td>timeperiods</td>
<td>array</td>
<td>Maintenance time periods.</td>
</tr>
<tr>
<td>tags</td>
<td>array</td>
<td>Define what problems must be suppressed. If no tags are given, all active maintenance host problems will be suppressed.</td>
</tr>
</tbody>
</table>

**Attention:**

At least one host or host group must be defined for each maintenance.

**Return values**

- (object) Returns an object containing the IDs of the created maintenances under the `maintenanceids` property. The order of the returned IDs matches the order of the passed maintenances.

**Examples**

Creating a maintenance

Create a maintenance with data collection for host group “Z” with problem tags `service:mysqld` and `error`. It must be active from 22.01.2013 till 22.01.2014, come in effect each Sunday at 18:00 and last for one hour.

**Request:**
See also

• Time period

Source

CMaintenance::create() in frontends/php/include/classes/api/services/CMaintenance.php.

**maintenance.delete**

Description

object maintenance.delete(array maintenanceIds)

This method allows to delete maintenance periods.

Parameters
IDs of the maintenance periods to delete.

Return values

(obj) Returns an object containing the IDs of the deleted maintenance periods under the maintenanceids property.

Examples

Deleting multiple maintenance periods

Delete two maintenance periods.

Request:

```
{
    "jsonrpc": "2.0",
    "method": "maintenance.delete",
    "params": [
        3,
        1
    ],
    "auth": "3a57200802b24cda67c4e401b50c065",
    "id": 1
}
```

Response:

```
{
    "jsonrpc": "2.0",
    "result": {
        "maintenanceids": [3, 1]
    },
    "id": 1
}
```

Source

CMaintenance::delete() in frontends/php/include/classes/api/services/CMaintenance.php.

**maintenance.get**

Description

integer/array maintenance.get(object parameters)

The method allows to retrieve maintenances according to the given parameters.

Parameters

(obj) Parameters defining the desired output.

The method supports the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>groupids</td>
<td>string/array</td>
<td>Return only maintenances that are assigned to the given host groups.</td>
</tr>
<tr>
<td>hostids</td>
<td>string/array</td>
<td>Return only maintenances that are assigned to the given hosts.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>maintenanceids</td>
<td>string/array</td>
<td>Return only maintenance with the given IDs.</td>
</tr>
<tr>
<td>selectGroups</td>
<td>query</td>
<td>Return host groups assigned to the maintenance in the groups property.</td>
</tr>
<tr>
<td>selectHosts</td>
<td>query</td>
<td>Return hosts assigned to the maintenance in the hosts property.</td>
</tr>
<tr>
<td>selectTimeperiods</td>
<td>query</td>
<td>Return the maintenance’s time periods in the timeperiods property.</td>
</tr>
<tr>
<td>selectTags</td>
<td>query</td>
<td>Return the maintenance’s problem tags in the tags property.</td>
</tr>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Sort the result by the given properties.</td>
</tr>
<tr>
<td>countOutput</td>
<td>boolean</td>
<td>These parameters being common for all get methods are described in detail in the reference commentary.</td>
</tr>
<tr>
<td>editable</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>excludeSearch</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>filter</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>limit</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>output</td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>preservekeys</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>search</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>searchByAny</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>searchWildcards</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>sortorder</td>
<td>string/array</td>
<td></td>
</tr>
<tr>
<td>startSearch</td>
<td>boolean</td>
<td></td>
</tr>
</tbody>
</table>

**Return values**

*(integer/array)* Returns either:
- an array of objects;
- the count of retrieved objects, if the `countOutput` parameter has been used.

**Examples**
Retrieving maintenances

Retrieve all configured maintenances, and the data about the assigned host groups, defined time periods and problem tags.

Request:

```json
{
   "jsonrpc": "2.0",
   "method": "maintenance.get",
   "params": {
      "output": "extend",
      "selectGroups": "extend",
      "selectTimeperiods": "extend",
      "selectTags": "extend"
   },
   "auth": "038e1d7b1735c6a5436ee9eae095879e",
   "id": 1
}
```

Response:

```json
{
   "jsonrpc": "2.0",
   "result": [
      {
         "maintenanceid": "3",
         "name": "Sunday maintenance",
         "maintenance_type": "0",
         "description": "",
         "active_since": "1358844540",
         "active_till": "1390466940",
         "tags_evaltype": "0",
         "groups": [
            {
               "groupid": "4",
               "name": "Zabbix servers",
               "internal": "0"
            }
         ],
         "timeperiods": [
            {
               "timeperiodid": "4",
               "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": NULL
            }
         ]
      }
   ]
}
```
See also

- Host
- Host group
- Time period

Source

CMaintenance::get() in frontends/php/include/classes/api/services/CMaintenance.php.

**maintenance.update**

**Description**

object maintenance.update(object/array maintenances)

This method allows to update existing maintenances.

**Parameters**

(object/array) Maintenance properties to be updated.

The maintenanceid property must be defined for each maintenance, all other properties are optional. Only the passed properties will be updated, all others will remain unchanged.

Additionally to the standard maintenance properties, the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>groupids</td>
<td>array</td>
<td>IDs of the host groups to replace the current groups.</td>
</tr>
<tr>
<td>hostids</td>
<td>array</td>
<td>IDs of the hosts to replace the current hosts.</td>
</tr>
<tr>
<td>timeperiods</td>
<td>array</td>
<td>Maintenance time periods to replace the current periods.</td>
</tr>
<tr>
<td>tags</td>
<td>array</td>
<td>Problem tags.</td>
</tr>
</tbody>
</table>

**Attention:**

At least one host or host group must be defined for each maintenance.

**Return values**

(object) Returns an object containing the IDs of the updated maintenances under the maintenanceids property.

**Examples**

Assigning different hosts

Replace the hosts currently assigned to maintenance "3" with two different ones.

**Request:**

```json
{
    "jsonrpc": "2.0",
    "method": "maintenance.update",
    "params": {
        "maintenanceid": "3",
        "hostids": [
            "10085",
            "10084"
        ]
    },
    "auth": "038e1d7b1735c6a5436ee9eae096879e",
    "id": 1
}
```

**Response:**

```json
987
```
See also

- Time period

Source

CMaintenance::update() in frontends/php/include/classes/api/services/CMaintenance.php.

Map

This class is designed to work with maps.

Object references:

- Map
- Map element
- Map link
- Map URL
- Map user
- Map user group
- Map shape
- Map line

Available methods:

- map.create - create new maps
- map.delete - delete maps
- map.get - retrieve maps
- map.update - update maps

> Map object

The following objects are directly related to the map API.

Map

The map object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sysmapid</td>
<td>string</td>
<td>(readonly) ID of the map.</td>
</tr>
<tr>
<td>height</td>
<td>integer</td>
<td>Height of the map in pixels.</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>Name of the map.</td>
</tr>
<tr>
<td>width</td>
<td>integer</td>
<td>Width of the map in pixels.</td>
</tr>
<tr>
<td>backgroundid</td>
<td>string</td>
<td>ID of the image used as the background for the map.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>expand_macros</td>
<td>integer</td>
<td>Whether to expand macros in labels when configuring the map.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - (default) do not expand macros;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - expand macros.</td>
</tr>
<tr>
<td>expand_problem</td>
<td>integer</td>
<td>Whether the problem trigger will be displayed for elements with a single problem.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - always display the number of problems;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - (default) display the problem trigger if there’s only one problem.</td>
</tr>
<tr>
<td>grid_align</td>
<td>integer</td>
<td>Whether to enable grid aligning.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - disable grid aligning;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - (default) enable grid aligning.</td>
</tr>
<tr>
<td>grid_show</td>
<td>integer</td>
<td>Whether to show the grid on the map.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - do not show the grid;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - (default) show the grid.</td>
</tr>
<tr>
<td>grid_size</td>
<td>integer</td>
<td>Size of the map grid in pixels.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Supported values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>20, 40, 50, 75 and 100.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 50.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>highlight</td>
<td>integer</td>
<td>Whether icon highlighting is enabled. Possible values: 0 - highlighting disabled; 1 - (default) highlighting enabled.</td>
</tr>
<tr>
<td>iconmapid</td>
<td>string</td>
<td>ID of the icon map used on the map.</td>
</tr>
<tr>
<td>label_format</td>
<td>integer</td>
<td>Whether to enable advanced labels. Possible values: 0 - (default) disable advanced labels; 1 - enable advanced labels.</td>
</tr>
<tr>
<td>label_location</td>
<td>integer</td>
<td>Location of the map element label. Possible values: 0 - (default) bottom; 1 - left; 2 - right; 3 - top.</td>
</tr>
<tr>
<td>label_string_host</td>
<td>string</td>
<td>Custom label for host elements. Required for maps with custom host label type.</td>
</tr>
<tr>
<td>label_string_hostgroup</td>
<td>string</td>
<td>Custom label for host group elements. Required for maps with custom host group label type.</td>
</tr>
<tr>
<td>label_string_image</td>
<td>string</td>
<td>Custom label for image elements. Required for maps with custom image label type.</td>
</tr>
<tr>
<td>label_string_map</td>
<td>string</td>
<td>Custom label for map elements. Required for maps with custom map label type.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>label_string_trigger</td>
<td>string</td>
<td>Custom label for trigger elements. Required for maps with custom trigger label type.</td>
</tr>
<tr>
<td>label_type</td>
<td>integer</td>
<td>Map element label type. Possible values: 0 - label; 1 - IP address; 2 - (default) element name; 3 - status only; 4 - nothing.</td>
</tr>
<tr>
<td>label_type_host</td>
<td>integer</td>
<td>Host element label type. Possible values: 0 - label; 1 - IP address; 2 - (default) element name; 3 - status only; 4 - nothing; 5 - custom.</td>
</tr>
<tr>
<td>label_type_hostgroup</td>
<td>integer</td>
<td>Host group element label type. Possible values: 0 - label; 2 - (default) element name; 3 - status only; 4 - nothing; 5 - custom.</td>
</tr>
<tr>
<td>label_type_image</td>
<td>integer</td>
<td>Host group element label type. Possible values: 0 - label; 2 - (default) element name; 4 - nothing; 5 - custom.</td>
</tr>
<tr>
<td>label_type_map</td>
<td>integer</td>
<td>Map element label type. Possible values: 0 - label; 2 - (default) element name; 3 - status only; 4 - nothing; 5 - custom.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>label_type_trigger</td>
<td>integer</td>
<td>Label type for trigger elements.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - label;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 - (default) element name;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 - status only;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 - nothing;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5 - custom.</td>
</tr>
<tr>
<td>markelements</td>
<td>integer</td>
<td>Whether to highlight map elements that have recently changed their status.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - (default) do not highlight elements;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - highlight elements.</td>
</tr>
<tr>
<td>severity_min</td>
<td>integer</td>
<td>Minimum severity of the triggers that will be displayed on the map.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Refer to the <code>trigger &quot;severity&quot; property</code> for a list of supported trigger severities.</td>
</tr>
<tr>
<td>show_unack</td>
<td>integer</td>
<td>How problems should be displayed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - (default) display the count of all problems;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - display only the count of unacknowledged problems;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 - display the count of acknowledged and unacknowledged problems separately.</td>
</tr>
<tr>
<td>userid</td>
<td>string</td>
<td>Map owner user ID.</td>
</tr>
<tr>
<td>private</td>
<td>integer</td>
<td>Type of map sharing.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - public map;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - (default) private map.</td>
</tr>
</tbody>
</table>
show_suppressed integer
Whether suppressed problems are shown.
Possible values: 0 - (default) hide suppressed problems; 1 - show suppressed problems.

Note that for some methods (update, delete) the required/optional parameter combination is different.

Map element
The map element object defines an object displayed on a map. It has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>selementid string</td>
<td>(readonly) ID of the map element.</td>
<td></td>
</tr>
<tr>
<td>elements array</td>
<td>Element data object. Required for host, host group, trigger and map type elements.</td>
<td></td>
</tr>
<tr>
<td>areatype integer</td>
<td>How separate host group hosts should be displayed.</td>
<td></td>
</tr>
<tr>
<td>iconid_off string</td>
<td>ID of the image used to display the element in default state.</td>
<td></td>
</tr>
</tbody>
</table>

Possible values:
0 - host; 1 - map; 2 - trigger; 3 - host group; 4 - image.

Possible values:
0 - (default) the host group element will take up the whole map; 1 - the host group element will have a fixed size.
<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>application</td>
<td>string</td>
<td>Name of the application to display problems from. Used only for host and host group map elements.</td>
</tr>
<tr>
<td>elements subtype</td>
<td>integer</td>
<td>How a host group element should be displayed on a map.</td>
</tr>
<tr>
<td>height</td>
<td>integer</td>
<td>Height of the fixed size host group element in pixels. Default: 200.</td>
</tr>
<tr>
<td>iconid_disabled</td>
<td>string</td>
<td>ID of the image used to display disabled map elements. Unused for image elements.</td>
</tr>
<tr>
<td>iconid_maintenance</td>
<td>string</td>
<td>ID of the image used to display map elements in maintenance. Unused for image elements.</td>
</tr>
<tr>
<td>iconid_on</td>
<td>string</td>
<td>ID of the image used to display map elements with problems. Unused for image elements.</td>
</tr>
<tr>
<td>label</td>
<td>string</td>
<td>Label of the element.</td>
</tr>
<tr>
<td>label_location</td>
<td>integer</td>
<td>Location of the map element label.</td>
</tr>
</tbody>
</table>

Possible values:
-1 (default)
0 - display the host group as a single element;
1 - display each host in the group separately.

Possible values:
-1 (default)
default location;
0 - bottom;
1 - left;
2 - right;
3 - top.
<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>permission</td>
<td>integer</td>
<td>Type of permission level. Possible values: -1 - none; 2 - read only; 3 - read-write.</td>
</tr>
<tr>
<td>sysmapid</td>
<td>string</td>
<td>(readonly) ID of the map that the element belongs to.</td>
</tr>
<tr>
<td>urls</td>
<td>array</td>
<td>Map element URLs. The map element URL object is described in detail below.</td>
</tr>
<tr>
<td>use_iconmap</td>
<td>integer</td>
<td>Whether icon mapping must be used for host elements. Possible values: 0 - do not use icon mapping; 1 - (default) use icon mapping.</td>
</tr>
<tr>
<td>viewtype</td>
<td>integer</td>
<td>Host group element placing algorithm. Possible values: 0 - (default) grid.</td>
</tr>
<tr>
<td>width</td>
<td>integer</td>
<td>Width of the fixed size host group element in pixels. Default: 200.</td>
</tr>
<tr>
<td>x</td>
<td>integer</td>
<td>X-coordinates of the element in pixels. Default: 0.</td>
</tr>
<tr>
<td>y</td>
<td>integer</td>
<td>Y-coordinates of the element in pixels. Default: 0.</td>
</tr>
</tbody>
</table>

Map element Host

The map element Host object defines one host element.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostid</td>
<td>string</td>
<td>Host ID</td>
</tr>
</tbody>
</table>

Map element Host group

The map element Host group object defines one host group element.
Map element Map
The map element Map object defines one map element.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>groupid</td>
<td>string</td>
<td>Host group ID</td>
</tr>
</tbody>
</table>

Map element Trigger
The map element Trigger object defines one or more trigger elements.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sysmapid</td>
<td>string</td>
<td>Map ID</td>
</tr>
</tbody>
</table>

Map element URL
The map element URL object defines a clickable link that will be available for a specific map element. It has the following properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sysmapelementurlid</td>
<td>string</td>
<td>(readonly) ID of the map element URL.</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>Link caption.</td>
</tr>
<tr>
<td>url</td>
<td>string</td>
<td>Link URL.</td>
</tr>
<tr>
<td>selementid</td>
<td>string</td>
<td>ID of the map element that the URL belongs to.</td>
</tr>
</tbody>
</table>

Map link
The map link object defines a link between two map elements. It has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>linkid</td>
<td>string</td>
<td>(readonly) ID of the map link.</td>
</tr>
<tr>
<td>selementid1</td>
<td>string</td>
<td>ID of the first map element linked on one end.</td>
</tr>
<tr>
<td>selementid2</td>
<td>string</td>
<td>ID of the first map element linked on the other end.</td>
</tr>
<tr>
<td>color</td>
<td>string</td>
<td>Line color as a hexadecimal color code.</td>
</tr>
<tr>
<td>drawtype</td>
<td>integer</td>
<td>Link line draw style.</td>
</tr>
<tr>
<td>label</td>
<td>string</td>
<td>Link label.</td>
</tr>
</tbody>
</table>

| Possible values: | 0 - (default) line; | 2 - bold line; | 3 - dotted line; | 4 - dashed line. |

996
### Property | Type | Description
--- | --- | ---
linktriggers | array | Map link triggers to use as link status indicators. The map link trigger object is described in detail below. The map link trigger object defines a map link status indicator based on the state of a trigger. It has the following properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>linktriggerid</td>
<td>string</td>
<td>(readonly) ID of the map link trigger.</td>
</tr>
<tr>
<td>triggerid</td>
<td>string</td>
<td>(required) ID of the trigger used as a link indicator. Indicator color as a hexadecimal color code. Default: #D00000.</td>
</tr>
<tr>
<td>color</td>
<td>string</td>
<td>Indicator draw style. Possible values: 0 - (default) line; 2 - bold line; 3 - dotted line; 4 - dashed line.</td>
</tr>
<tr>
<td>drawtype</td>
<td>integer</td>
<td>ID of the map link that the link trigger belongs to.</td>
</tr>
<tr>
<td>linkid</td>
<td>string</td>
<td></td>
</tr>
</tbody>
</table>

### Map URL
The map URL object defines a clickable link that will be available for all elements of a specific type on the map. It has the following properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sysmapurlid</td>
<td>string</td>
<td>(readonly) ID of the map URL.</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>Link caption.</td>
</tr>
<tr>
<td>url</td>
<td>string</td>
<td>Link URL.</td>
</tr>
<tr>
<td>(required)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Property | Type | Description
---|---|---
**elementtype** | integer | Type of map element for which the URL will be available.  
Refer to the map element "type" property for a list of supported types.  
Default: 0.

**sysmapid** | string | ID of the map that the URL belongs to.

---

#### Map user

List of map permissions based on users. It has the following properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| sysmapuserid | string | (readonly) ID of the map user.  
User ID.                        |
| **userid**   | string | UserID.                  |
| (required)    |        |                          |
| **permission** | integer | Type of permission level.  
Possible values:  
2 - read only;  
3 - read-write; |
| (required)    |        |                          |

---

#### Map user group

List of map permissions based on user groups. It has the following properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| sysmapusrgrpid | string  | (readonly) ID of the map user group.  
User group ID.                             |
| **usrgrpid** | string | User group ID.            |
| (required)    |        |                          |
| **permission** | integer | Type of permission level.  
Possible values:  
2 - read only;  
3 - read-write; |
| (required)    |        |                          |

---

#### Map shapes

The map shape object defines an geometric shape (with or without text) displayed on a map. It has the following properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sysmap_shapeid</td>
<td>string</td>
<td>(readonly) ID of the map shape element.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>type</strong> (required)</td>
<td>integer</td>
<td>Type of map shape element. Possible values: 0 - rectangle; 1 - ellipse. Property is required when new shapes are created.</td>
</tr>
<tr>
<td>x</td>
<td>integer</td>
<td>X-coordinates of the shape in pixels. Default: 0.</td>
</tr>
<tr>
<td>y</td>
<td>integer</td>
<td>Y-coordinates of the shape in pixels. Default: 0.</td>
</tr>
<tr>
<td>width</td>
<td>integer</td>
<td>Width of the shape in pixels. Default: 200.</td>
</tr>
<tr>
<td>height</td>
<td>integer</td>
<td>Height of the shape in pixels. Default: 200.</td>
</tr>
<tr>
<td>text</td>
<td>string</td>
<td>Text of the shape. Default: 999</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>font_color</td>
<td>string</td>
<td>Font color. Default: ‘000000’. Horizontal alignment of text. Possible values: 0 - center; 1 - left; 2 - right. Default: 0.</td>
</tr>
<tr>
<td>text_halign</td>
<td>integer</td>
<td>Horizontal alignment of text. Possible values: 0 - center; 1 - left; 2 - right. Default: 0.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>text_align</td>
<td>integer</td>
<td>Vertical alignment of text.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values: 0 - middle; 1 - top; 2 - bottom.</td>
</tr>
<tr>
<td>border_type</td>
<td>integer</td>
<td>Type of the border.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values: 0 - none; 1 - ————; 2 - · · · · ·; 3 - - - - - - - - - - - -</td>
</tr>
<tr>
<td>border_width</td>
<td>integer</td>
<td>Width of the border in pixels.</td>
</tr>
<tr>
<td>border_color</td>
<td>string</td>
<td>Border color.</td>
</tr>
<tr>
<td>background_color</td>
<td>string</td>
<td>Background color (fill color).</td>
</tr>
<tr>
<td>zindex</td>
<td>integer</td>
<td>Value used to order shapes (z-index).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 0.</td>
</tr>
</tbody>
</table>

Map lines

The map line object defines an line displayed on a map. It has the following properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sysmap_shapeid</td>
<td>string</td>
<td>(readonly) ID of the map shape element.</td>
</tr>
<tr>
<td>x1</td>
<td>integer</td>
<td>X-coordinates of the line point 1 in pixels.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 0.</td>
</tr>
<tr>
<td>y1</td>
<td>integer</td>
<td>Y-coordinates of the line point 1 in pixels.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 0.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>x2</td>
<td>integer</td>
<td>X-coordinates of the line point 2 in pixels. Default: 200.</td>
</tr>
<tr>
<td>y2</td>
<td>integer</td>
<td>Y-coordinates of the line point 2 in pixels. Default: 200.</td>
</tr>
<tr>
<td>line_type</td>
<td>integer</td>
<td>Type of the border. Possible values: 0 - none; 1 - ——; 2 - · · · · ·; 3 - - - - -. Default: 0.</td>
</tr>
<tr>
<td>line_width</td>
<td>integer</td>
<td>Width of the border in pixels. Default: 0.</td>
</tr>
<tr>
<td>line_color</td>
<td>string</td>
<td>Border color. Default: '000000'.</td>
</tr>
<tr>
<td>zindex</td>
<td>integer</td>
<td>Value used to order shapes (z-index). Default: 0.</td>
</tr>
</tbody>
</table>

**map.create**

**Description**

*object map.create(object/array maps)*

This method allows to create new maps.

**Parameters**

*(object/array)* Maps to create.

Additionally to the standard map properties, the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>links</td>
<td>array</td>
<td>Map links to be created on the map.</td>
</tr>
<tr>
<td>elements</td>
<td>array</td>
<td>Map elements to be created on the map.</td>
</tr>
<tr>
<td>urls</td>
<td>array</td>
<td>Map URLs to be created on the map.</td>
</tr>
<tr>
<td>users</td>
<td>array</td>
<td>Map user shares to be created on the map.</td>
</tr>
<tr>
<td>userGroups</td>
<td>array</td>
<td>Map user group shares to be created on the map.</td>
</tr>
<tr>
<td>shapes</td>
<td>array</td>
<td>Map shapes to be created on the map.</td>
</tr>
<tr>
<td>lines</td>
<td>array</td>
<td>Map lines to be created on the map.</td>
</tr>
</tbody>
</table>

**Note:**

To create map links you’ll need to set a map elements selementid to an arbitrary value and then use this value to reference this element in the links selementid1 or selementid2 properties. When the element is created, this value will be replaced with the correct ID generated by Zabbix. See example.
Return values

(object) Returns an object containing the IDs of the created maps under the sysmapids property. The order of the returned IDs matches the order of the passed maps.

Examples

Create an empty map

Create a map with no elements.

Request:

```json
{
  "jsonrpc": "2.0",
  "method": "map.create",
  "params": {
    "name": "Map",
    "width": 600,
    "height": 600
  },
  "auth": "038e1d7b1735c6a5436ee9eae095879e",
  "id": 1
}
```

Response:

```json
{
  "jsonrpc": "2.0",
  "result": {
    "sysmapids": [
      "8"
    ],
  },
  "id": 1
}
```

Create a host map

Create a map with two host elements and a link between them. Note the use of temporary "selementid1" and "selementid2" values in the map link object to refer to map elements.

Request:

```json
{
  "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"
      }
    ]
  },
  "auth": "038e1d7b1735c6a5436ee9eae095879e",
  "id": 1
}
```
Create a trigger map

Create a map with trigger element, which contains two triggers.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "map.create",
    "params": {
        "name": "Trigger map",
        "width": 600,
        "height": 600,
        "selements": [
            {
                "elements": [
                    {"triggerid": "12345"},
                    {"triggerid": "67890"}
                ],
                "elementtype": 2,
                "iconid_off": "2"
            }
        ]
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "sysmapids": ["10"
    ],
    "id": 1
}
```

Map sharing

Create a map with two types of sharing (user and user group).
Map shapes

Create a map with map name title.

Request:

```json
{
    "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}"
            }
        ],
        "auth": "038e1d7b1735c6a5436ee9eae095879e",
        "id": 1
    }
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": { "sysmapids": [ "9" ] },
    "id": 1
}
```
Map lines

Create a map line.

Request:

```json
{
  "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"
      }
    ]
  },
  "auth": "038e1d7b1735c6a5436ee9095879e",
  "id": 1
}
```

Response:

```json
{
  "jsonrpc": "2.0",
  "result": {
    "sysmapids": ["11"
  ],
  },
  "id": 1
}
```

See also

- Map element
- Map link
- Map URL
- Map user
- Map user group
- Map shape
- Map line

Source

CMap::create() in frontends/php/include/classes/api/services/CMap.php.

map.delete
object map.delete(array mapIds)

This method allows to delete maps.

Parameters
(array) IDs of the maps to delete.

Return values
(object) Returns an object containing the IDs of the deleted maps under the sysmapids property.

Examples
Delete multiple maps
Delete two maps.

Request:
```
{
   "jsonrpc": "2.0",
   "method": "map.delete",
   "params": [
      "12",
      "34"
   ],
   "auth": "3a57200802b24cda67c4e4010b50c065",
   "id": 1
}
```

Response:
```
{
   "jsonrpc": "2.0",
   "result": {
      "sysmapids": [
         "12",
         "34"
      ]
   },
   "id": 1
}
```

Source
CMap::delete() in frontends/php/include/classes/api/services/CMap.php.

map.get

Description
integer/array map.get(object parameters)

The method allows to retrieve maps according to the given parameters.

Parameters
(object) Parameters defining the desired output.

The method supports the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sysmapids</td>
<td>string/array</td>
<td>Return only maps with the given IDs.</td>
</tr>
<tr>
<td>userids</td>
<td>string/array</td>
<td>Return only maps that belong to the given user IDs.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>expandUrls</td>
<td>flag</td>
<td>Adds global map URLs to the corresponding map elements and expands macros in all map element URLs.</td>
</tr>
<tr>
<td>selectIconMap</td>
<td>query</td>
<td>Returns the icon map used on the map in the iconmap property.</td>
</tr>
<tr>
<td>selectLinks</td>
<td>query</td>
<td>Returns map links between elements in the links property.</td>
</tr>
<tr>
<td>selectSelements</td>
<td>query</td>
<td>Returns the map elements from the map in the selements property.</td>
</tr>
<tr>
<td>selectUrls</td>
<td>query</td>
<td>Returns the map URLs in the urls property.</td>
</tr>
<tr>
<td>selectUsers</td>
<td>query</td>
<td>Returns users that the map is shared with in users property.</td>
</tr>
<tr>
<td>selectUserGroups</td>
<td>query</td>
<td>Returns user groups that the map is shared with in userGroups property.</td>
</tr>
<tr>
<td>selectShapes</td>
<td>query</td>
<td>Returns the map shapes from the map in the shapes property.</td>
</tr>
<tr>
<td>selectLines</td>
<td>query</td>
<td>Returns the map lines from the map in the lines property.</td>
</tr>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Sort the result by the given properties.</td>
</tr>
<tr>
<td>countOutput</td>
<td>boolean</td>
<td>These parameters being common for all get methods are described in detail in the reference commentary.</td>
</tr>
<tr>
<td>editable</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>excludeSearch</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>filter</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>limit</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>output</td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>preservekeys</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>search</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>searchByAny</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>searchWildcards</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>sortorder</td>
<td>string/array</td>
<td></td>
</tr>
<tr>
<td>startSearch</td>
<td>boolean</td>
<td></td>
</tr>
</tbody>
</table>

Return values

(integer/array) Returns either:

- an array of objects;
- the count of retrieved objects, if the countOutput parameter has been used.

Examples

Retrieve a map

Retrieve all data about map "3".

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "map.get",
    "params": {
        "output": "extend",
        "selectSelements": "extend",
        "selectLinks": "extend",
        "selectUsers": "extend",
        "selectUserGroups": "extend",
        "selectShapes": "extend",
        "selectLines": "extend",
        "sysmapids": "3"
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": [
        {
            "selements": [
                {
                    "selementid": "10",
                    "sysmapid": "3",
                    "elementtype": "4",
                    "iconid_off": "1",
                    "iconid_on": "0",
                    "label": "Zabbix server",
                    "label_location": "3",
                    "x": "11",
                    "y": "141",
                    "iconid_disabled": "0",
                    "iconid_maintenance": "0",
                    "elementssubtype": "0",
                    "areatype": "0",
                    "width": "200",
                    "height": "200",
                    "viewtype": "0",
                    "use_iconmap": "1",
                    "application": ""
                }
            ]
        }
    ]
}
```
See also

- Icon map
- Map element
- Map link
- Map URL
- Map user
- Map user group
- Map shapes
- Map lines

Source

CMap::get() in frontends/php/include/classes/api/services/CMap.php.

**map.update**

**Description**

object map.update(object/array maps)

This method allows to update existing maps.

**Parameters**

(object/array) Map properties to be updated.

The mapid property must be defined for each map, all other properties are optional. Only the passed properties will be updated, all others will remain unchanged.

Additionally to the standard map properties, the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>links</td>
<td>array</td>
<td>Map links to replace the existing links.</td>
</tr>
<tr>
<td>elements</td>
<td>array</td>
<td>Map elements to replace the existing elements.</td>
</tr>
<tr>
<td>urls</td>
<td>array</td>
<td>Map URLs to replace the existing URLs.</td>
</tr>
<tr>
<td>users</td>
<td>array</td>
<td>Map user shares to replace the existing elements.</td>
</tr>
<tr>
<td>userGroups</td>
<td>array</td>
<td>Map user group shares to replace the existing elements.</td>
</tr>
<tr>
<td>shapes</td>
<td>array</td>
<td>Map shapes to replace the existing shapes.</td>
</tr>
<tr>
<td>lines</td>
<td>array</td>
<td>Map lines to replace the existing lines.</td>
</tr>
</tbody>
</table>
Note:
To create map links between new map elements you’ll need to set an elements selementid to an arbitrary value and then use this value to reference this element in the links selementid1 or selementid2 properties. When the element is created, this value will be replaced with the correct ID generated by Zabbix. See example for map.create.

Return values

(object) Returns an object containing the IDs of the updated maps under the sysmapids property.

Examples

Resize a map

Change the size of the map to 1200x1200 pixels.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "map.update",
    "params": {
        "sysmapid": "8",
        "width": 1200,
        "height": 1200
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "sysmapids": [
            "8"
        ],
        "id": 1
    }
}
```

Change map owner

Available only for admins and super admins.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "map.update",
    "params": {
        "sysmapid": "9",
        "userid": "1"
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 2
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "sysmapids": [
            "9"
        ],
        "id": 2
    }
}
```
See also

- Map element
- Map link
- Map URL
- Map user
- Map user group
- Map shapes
- Map lines

Source

CMap::update() in frontends/php/include/classes/api/services/CMap.php.

**Media type**

This class is designed to work with media types.

Object references:

- Media type

Available methods:

- `mediatype.create` - creating new media types
- `mediatype.delete` - deleting media types
- `mediatype.get` - retrieving media types
- `mediatype.update` - updating media types

> **Media type object**

The following objects are directly related to the `mediatype` API.

Media type

The media type object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mediatypeid</td>
<td>string</td>
<td>(readonly) ID of the media type.</td>
</tr>
<tr>
<td>description</td>
<td>string</td>
<td>Name of the media type.</td>
</tr>
<tr>
<td>type</td>
<td>integer</td>
<td>Transport used by the media type.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - e-mail;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - script;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 - SMS;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 - Jabber;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>100 - Ez Texting.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>exec_path</td>
<td>string</td>
<td>For script media types exec_path contains the name of the executed script. For Ez Texting exec_path contains the message text limit. Possible text limit values: 0 - USA (160 characters); 1 - Canada (136 characters). Required for script and Ez Texting media types.</td>
</tr>
<tr>
<td>gsm_modem</td>
<td>string</td>
<td>Serial device name of the GSM modem. Required for SMS media types.</td>
</tr>
<tr>
<td>passwd</td>
<td>string</td>
<td>Authentication password. Required for Jabber and Ez Texting media types.</td>
</tr>
<tr>
<td>smtp_email</td>
<td>string</td>
<td>Email address from which notifications will be sent. Required for email media types.</td>
</tr>
<tr>
<td>smtp_helo</td>
<td>string</td>
<td>SMTP HELO. Required for email media types.</td>
</tr>
<tr>
<td>smtp_server</td>
<td>string</td>
<td>SMTP server. Required for email media types.</td>
</tr>
<tr>
<td>smtp_port</td>
<td>integer</td>
<td>SMTP server port to connect to.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>smtp_security</td>
<td>integer</td>
<td>SMTP connection security level to use.</td>
</tr>
<tr>
<td>smtp_verify_host</td>
<td>integer</td>
<td>SSL verify host for SMTP.</td>
</tr>
<tr>
<td>smtp_verify_peer</td>
<td>integer</td>
<td>SSL verify peer for SMTP.</td>
</tr>
<tr>
<td>smtp_authentication</td>
<td>integer</td>
<td>SMTP authentication method to use.</td>
</tr>
<tr>
<td>status</td>
<td>integer</td>
<td>Whether the media type is enabled.</td>
</tr>
<tr>
<td>username</td>
<td>string</td>
<td>Username or Jabber identifier. Required for Jabber and Ez Texting media types.</td>
</tr>
<tr>
<td>exec_params</td>
<td>string</td>
<td>Script parameters. Each parameter ends with a new line feed.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>maxsessions</td>
<td>integer</td>
<td>The maximum number of alerts that can be processed in parallel.</td>
</tr>
<tr>
<td>maxattempts</td>
<td>integer</td>
<td>The maximum number of attempts to send an alert.</td>
</tr>
<tr>
<td>attempt_interval</td>
<td>string</td>
<td>The interval between retry attempts. Accepts seconds and time unit with suffix.</td>
</tr>
</tbody>
</table>

Note that for some methods (update, delete) the required/optional parameter combination is different.

**mediatype.create**

**Description**

object mediatype.create(object/array mediaTypes)

This method allows to create new media types.

**Parameters**

(object/array) Media types to create.

The method accepts media types with the standard media type properties.

**Return values**

(object) Returns an object containing the IDs of the created media types under the mediatypeids property. The order of the returned IDs matches the order of the passed media types.

**Examples**

Creating a media type

Create a new e-mail media type.

Request:
Creating a media type with custom options

Create a new script media type with custom value for number of attempts and interval between them.

Request:

```
{
    "jsonrpc": "2.0",
    "method": "mediatype.create",
    "params": {
        "type": 1,
        "description": "Push notifications",
        "exec_path": "push-notification.sh",
        "exec_params": "{ALERT.SENDTO}\n{ALERT.SUBJECT}\n{ALERT.MESSAGE}\n",
        "maxattempts": "5",
        "attempt_interval": "11s"
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```
{
    "jsonrpc": "2.0",
    "result": {
        "mediatypeids": [
            "8"
        ]
    },
    "id": 1
}
```

Source
CMediaType::create() in frontends/php/include/classes/api/services/CMediaType.php.

mediatype.delete

Description
object mediatype.delete(array mediaTypeIds)

This method allows to delete media types.

Parameters

(array) IDs of the media types to delete.

Return values

(object) Returns an object containing the IDs of the deleted media types under the mediatypeids property.

Examples

Deleting multiple media types

Delete two media types.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "mediatype.delete",
    "params": [
        "3",
        "5"
    ],
    "auth": "3a57200802b24cda67c4e4010b50c065",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "mediatypeids": [
            "3",
            "5"
        ]
    },
    "id": 1
}
```

Source

CMediaType::delete() in frontends/php/include/classes/api/services/CMediaType.php.

mediatype.get

Description

integer/array mediatype.get(object parameters)

The method allows to retrieve media types according to the given parameters.

Parameters

(object) Parameters defining the desired output.

The method supports the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mediatypeids</td>
<td>string/array</td>
<td>Return only media types with the given IDs.</td>
</tr>
<tr>
<td>mediaids</td>
<td>string/array</td>
<td>Return only media types used by the given media.</td>
</tr>
</tbody>
</table>
### Parameter | Type          | Description
---|--------------|---
userids | string/array | Return only media types used by the given users.
selectUsers | query | Return the users that use the media type in the `users` property.
sortfield | string/array | Sort the result by the given properties.
Possible values are: `mediatypeid`.

countOutput | boolean | These parameters being common for all get methods are described in detail in the reference commentary.
editable | boolean |
excludeSearch | boolean |
filter | object |
limit | integer |
output | query |
preservekeys | boolean |
search | object |
searchByAny | boolean |
searchWildcardsEnabled | boolean |
sortorder | string/array |
startSearch | boolean |

**Return values**
(integer/array) Returns either:
- an array of objects;
- the count of retrieved objects, if the `countOutput` parameter has been used.

**Examples**

**Retrieving media types**

Retrieve all configured media types.

**Request:**

```json
{
   "jsonrpc": "2.0",
   "method": "mediatype.get",
   "params": {
      "output": "extend"
   },
   "auth": "038e1d7b1735c6a5436ee9eae095879e",
   "id": 1
}
```

**Response:**

```json
{
   "jsonrpc": "2.0",
   "result": [
      {
```
"mediatypeid": "1",
"type": "0",
"description": "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",
"exec_params": "",
"maxsessions": "1",
"maxattempts": "3",
"attempt_interval": "10s"
}
{
"mediatypeid": "2",
"type": "3",
"description": "Jabber",
"smtp_server": "",
"smtp_helo": "",
"smtp_email": "",
"exec_path": "",
"gsm_modem": "",
"username": "jabber@example.com",
"passwd": "zabbix",
"status": "0",
"smtp_port": "25",
"smtp_security": "0",
"smtp_verify_peer": "0",
"smtp_verify_host": "0",
"smtp_authentication": "0",
"exec_params": "",
"maxsessions": "1",
"maxattempts": "3",
"attempt_interval": "10s"
}
{
"mediatypeid": "3",
"type": "2",
"description": "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",
"exec_params": "",
"maxsessions": "1",
"maxattempts": "3"}
See also

- User

Source

CMediaType::get() in frontends/php/include/classes/api/services/CMediaType.php.

**mediatype.update**

Description

object mediatype.update(object/array mediaTypes)

This method allows to update existing media types.

Parameters

(object/array) **Media type properties** to be updated.

The `mediatypeid` property must be defined for each media type, all other properties are optional. Only the passed properties will be updated, all others will remain unchanged.

Return values

(object) Returns an object containing the IDs of the updated media types under the `mediatypeids` property.

Examples

Enabling a media type

Enable a media type, that is, set its status to 0.

Request:

```json
{
   "jsonrpc": "2.0",
   "method": "mediatype.update",
   "params": {
      "mediatypeid": "6",
      "status": 0
   },
   "auth": "038e1d7b1735c6a5436ee9eae096879e",
   "id": 1
}
```

Response:

```json
{
   "jsonrpc": "2.0",
   "result": {
      "mediatypeids": [
         "6"
      ]
   },
   "id": 1
}
```

Source

CMediaType::update() in frontends/php/include/classes/api/services/CMediaType.php.
Problem

This class is designed to work with problems.

Object references:

- Problem

Available methods:

- problem.get - retrieving problems

> Problem object

The following objects are directly related to the problem API.

Note:
Problems are created by the Zabbix server and cannot be modified via the API.

The problem object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eventid</td>
<td>string</td>
<td>ID of the problem event.</td>
</tr>
<tr>
<td>source</td>
<td>integer</td>
<td>Type of the problem event.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - event created by a trigger;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 - internal event.</td>
</tr>
<tr>
<td>object</td>
<td>integer</td>
<td>Type of object that is related to the problem event.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values for trigger events:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - trigger.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values for internal events:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - trigger;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 - item;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5 - LLD rule.</td>
</tr>
<tr>
<td>objectid</td>
<td>string</td>
<td>ID of the related object.</td>
</tr>
<tr>
<td>clock</td>
<td>timestamp</td>
<td>Time when the problem event was created.</td>
</tr>
<tr>
<td>ns</td>
<td>integer</td>
<td>Nanoseconds when the problem event was created.</td>
</tr>
<tr>
<td>r_eventid</td>
<td>string</td>
<td>Recovery event ID.</td>
</tr>
<tr>
<td>r_clock</td>
<td>timestamp</td>
<td>Time when the recovery event was created.</td>
</tr>
<tr>
<td>r_ns</td>
<td>integer</td>
<td>Nanoseconds when the recovery event was created.</td>
</tr>
<tr>
<td>correlationid</td>
<td>string</td>
<td>Correlation rule ID if this event was recovered by global correlation rule.</td>
</tr>
<tr>
<td>userid</td>
<td>string</td>
<td>User ID if the problem was manually closed.</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>Resolved problem name.</td>
</tr>
<tr>
<td>acknowledged</td>
<td>integer</td>
<td>Acknowledge state for problem.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - not acknowledged;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - acknowledged.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>severity</td>
<td>integer</td>
<td>Problem current severity.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - not classified;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - information;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 - warning;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 - average;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 - high;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5 - disaster.</td>
</tr>
<tr>
<td>suppressed</td>
<td>integer</td>
<td>Whether the problem is suppressed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - problem is in normal state;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - problem is suppressed.</td>
</tr>
</tbody>
</table>

Problem tag

The problem tag object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tag</td>
<td>string</td>
<td>Problem tag name.</td>
</tr>
<tr>
<td>value</td>
<td>string</td>
<td>Problem tag value.</td>
</tr>
</tbody>
</table>

**problem.get**

Description

integer/array problem.get(object parameters)

The method allows to retrieve problems according to the given parameters.

This method is for retrieving unresolved problems. It is also possible, if specified, to additionally retrieve recently resolved problems. The period that determines how old is "recently" is defined in Administration → General. Problems that were resolved prior to that period are not kept in the problem table. To retrieve problems that were resolved further back in the past, use the event.get method.

**Attention:**

This method may return problems of a deleted entity if these problems have not been removed by the housekeeper yet.

Parameters

(object) Parameters defining the desired output.

The method supports the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eventids</td>
<td>string/array</td>
<td>Return only problems with the given IDs.</td>
</tr>
<tr>
<td>groupids</td>
<td>string/array</td>
<td>Return only problems created by objects that belong to the given host groups.</td>
</tr>
<tr>
<td>hostids</td>
<td>string/array</td>
<td>Return only problems created by objects that belong to the given hosts.</td>
</tr>
<tr>
<td>objectids</td>
<td>string/array</td>
<td>Return only problems created by the given objects.</td>
</tr>
<tr>
<td>applicationids</td>
<td>string/array</td>
<td>Return only problems created by objects that belong to the given applications. Applies only if object is trigger or item.</td>
</tr>
<tr>
<td>source</td>
<td>integer</td>
<td>Return only problems with the given type.</td>
</tr>
</tbody>
</table>

Refer to the problem event object page for a list of supported event types.

Default: 0 - problem created by a trigger.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>object</td>
<td>integer</td>
<td>Return only problems created by objects of the given type. Refer to the problem event object page for a list of supported object types. Default: 0 - trigger.</td>
</tr>
<tr>
<td>acknowledged</td>
<td>boolean</td>
<td>true - return acknowledged problems only; false - unacknowledged only.</td>
</tr>
<tr>
<td>suppressed</td>
<td>boolean</td>
<td>true - return only suppressed problems; false - return problems in the normal state.</td>
</tr>
<tr>
<td>severities</td>
<td>integer/array</td>
<td>Return only problems with given event severities. Applies only if object is trigger.</td>
</tr>
<tr>
<td>evaltype</td>
<td>integer</td>
<td>Rules for tag searching. Possible values: 0 - (default) And/Or; 2 - Or.</td>
</tr>
<tr>
<td>tags</td>
<td>array of objects</td>
<td>Return only problems with given tags. Exact match by tag and case-insensitive search by value and operator. Format: [{&quot;tag&quot;: &quot;&lt;tag&gt;&quot;, &quot;value&quot;: &quot;&lt;value&gt;&quot;, &quot;operator&quot;: &quot;&lt;operator&gt;&quot;}, ..., ...]. An empty array returns all problems. Possible operator types: 0 - (default) Like; 1 - Equal.</td>
</tr>
<tr>
<td>recent</td>
<td>boolean</td>
<td>true - return PROBLEM and recently RESOLVED problems (depends on Display OK triggers for N seconds) Default: false - UNRESOLVED problems only</td>
</tr>
<tr>
<td>eventid_from</td>
<td>string</td>
<td>Return only problems with IDs greater or equal to the given ID.</td>
</tr>
<tr>
<td>eventid_till</td>
<td>string</td>
<td>Return only problems with IDs less or equal to the given ID.</td>
</tr>
<tr>
<td>time_from</td>
<td>timestamp</td>
<td>Return only problems that have been created after or at the given time.</td>
</tr>
<tr>
<td>time_till</td>
<td>timestamp</td>
<td>Return only problems that have been created before or at the given time.</td>
</tr>
<tr>
<td>selectAcknowledges</td>
<td>query</td>
<td>Return problem’s updates in the acknowledges property. Problem updates are sorted in reverse chronological order. The problem update object has the following properties: acknowledgeid - (string) update’s ID; userid - (string) ID of the user that updated the event; eventid - (string) ID of the updated event; clock - (timestamp) time when the event was updated; message - (string) text of the message; action - (integer) type of update action (see event.acknowledge); old_severity - (integer) event severity before this update action; new_severity - (integer) event severity after this update action;</td>
</tr>
</tbody>
</table>

Supports count.
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>selectTags</td>
<td>query</td>
<td>Return problem’s tags. Output format: [{&quot;tag&quot;: &quot;&lt;tag&gt;&quot;, &quot;value&quot;: &quot;&lt;value&gt;&quot;, ...}].</td>
</tr>
<tr>
<td>selectSuppressionData</td>
<td>query</td>
<td>Return list of maintenances in the suppression_data property: maintenanceid - (string) ID of the maintenance; suppress_until - (integer) time until the problem is suppressed.</td>
</tr>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Sort the result by the given properties.</td>
</tr>
<tr>
<td>countOutput</td>
<td>boolean</td>
<td>These parameters being common for all get methods are described in detail in the reference commentary page.</td>
</tr>
<tr>
<td>editable</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>excludeSearch</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>filter</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>limit</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>output</td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>preservekeys</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>search</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>searchByAny</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>searchWildcardsEnabled</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>sortorder</td>
<td>string/array</td>
<td></td>
</tr>
<tr>
<td>startSearch</td>
<td>boolean</td>
<td></td>
</tr>
</tbody>
</table>

Return values

(integer/array) Returns either:

- an array of objects;
- the count of retrieved objects, if the countOutput parameter has been used.

Examples

Retrieving trigger problem events

Retrieve recent events from trigger "15112."

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "problem.get",
    "params": {
        "output": "extend",
        "selectAcknowledges": "extend",
        "selectTags": "extend",
        "selectSuppressionData": "extend",
        "objectids": "15112",
        "recent": "true",
        "sortfield": ["eventid"],
        "sortorder": "DESC"
    },
    "auth": "67f45d3eb1173338e1b1647c4bdc1916",
    "id": 1
}
```

Response:

```json
{
    "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": "Zabbix agent on localhost is unreachable for 5 minutes",
"acknowledged": "1",
"suppressed": "1",
"severity": "3",
"acknowledges": [
  {
    "acknowledgeid": "14443",
    "userid": "1",
    "eventid": "1245463",
    "clock": "1472457281",
    "message": "problem solved",
    "action": "6",
    "old_severity": "0",
    "new_severity": "0"
  }
],
"tags": [
  {
    "tag": "test tag",
    "value": "test value"
  }
],
"suppression_data": [
  {
    "maintenanceid": "15",
    "suppress_until": "1472511600"
  }
]
],
"id": 1

See also

- Alert
- Item
- Host
- LLD rule
- Trigger

Source

CEvent::get() in frontends/php/include/classes/api/services/CProblem.php.

Proxy

This class is designed to work with proxies.

Object references:

- Proxy
- Proxy interface
Available methods:

- `proxy.create` - create new proxies
- `proxy.delete` - delete proxies
- `proxy.get` - retrieve proxies
- `proxy.update` - update proxies

> Proxy object

The following objects are directly related to the `proxy` API.

**Proxy**

The proxy object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>proxyid</code></td>
<td>string</td>
<td>(readonly) ID of the proxy.</td>
</tr>
<tr>
<td><code>host</code></td>
<td>string</td>
<td>Name of the proxy.</td>
</tr>
<tr>
<td><code>status</code></td>
<td>integer</td>
<td>Type of proxy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5 - active proxy;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6 - passive proxy.</td>
</tr>
<tr>
<td><code>description</code></td>
<td>text</td>
<td>Description of the proxy.</td>
</tr>
<tr>
<td><code>lastaccess</code></td>
<td>timestamp</td>
<td>(readonly) Time when the proxy last connected to the server.</td>
</tr>
<tr>
<td><code>tls_connect</code></td>
<td>integer</td>
<td>Connections to host.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - (default) No encryption;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 - PSK;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 - certificate.</td>
</tr>
<tr>
<td><code>tls_accept</code></td>
<td>integer</td>
<td>Connections from host.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible bitmap values are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - (default) No encryption;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 - PSK;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 - certificate.</td>
</tr>
<tr>
<td><code>tlsIssuer</code></td>
<td>string</td>
<td>Certificate issuer.</td>
</tr>
<tr>
<td><code>tlsSubject</code></td>
<td>string</td>
<td>Certificate subject.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>tls_psk_identity string</td>
<td></td>
<td>PSK identity. Required if either tls_connect or tls_accept has PSK enabled. Do not put sensitive information in the PSK identity, it is transmitted unencrypted over the network to inform a receiver which PSK to use.</td>
</tr>
<tr>
<td>tls_psk string</td>
<td></td>
<td>The preshared key, at least 32 hex digits. Required if either tls_connect or tls_accept has PSK enabled.</td>
</tr>
<tr>
<td>proxy_address string</td>
<td></td>
<td>Comma-delimited IP addresses or DNS names of active Zabbix proxy. (readonly) Indicates if communication between Zabbix server and proxy is compressed.</td>
</tr>
<tr>
<td>auto_compress integer</td>
<td></td>
<td>Possible values are: 0 - No compression; 1 - Compression enabled;</td>
</tr>
</tbody>
</table>

Note that for some methods (update, delete) the required/optional parameter combination is different.

Proxy interface

The proxy interface object defines the interface used to connect to a passive proxy. It has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interfaceid</td>
<td>string</td>
<td>(readonly) ID of the interface.</td>
</tr>
<tr>
<td>dns</td>
<td>string</td>
<td>DNS name to connect to. Can be empty if connections are made via IP address.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>ip</td>
<td>string</td>
<td>IP address to connect to. Can be empty if connections are made via DNS names.</td>
</tr>
<tr>
<td>port</td>
<td>string</td>
<td>Port number to connect to.</td>
</tr>
<tr>
<td>useip</td>
<td>integer</td>
<td>Whether the connection should be made via IP address. Possible values are: 0 - connect using DNS name; 1 - connect using IP address.</td>
</tr>
<tr>
<td>hostid</td>
<td>string</td>
<td>(readonly) ID of the proxy the interface belongs to.</td>
</tr>
</tbody>
</table>

**proxy.create**

Description

**object proxy.create(object/array proxies)**

This method allows to create new proxies.

Parameters

(object/array) Proxies to create.

Additionally to the standard proxy properties, the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hosts</td>
<td>array</td>
<td>Hosts to be monitored by the proxy. If a host is already monitored by a different proxy, it will be reassigned to the current proxy. The hosts must have the hostid property defined.</td>
</tr>
<tr>
<td>interface</td>
<td>object</td>
<td>Host interface to be created for the passive proxy. Required for passive proxies.</td>
</tr>
</tbody>
</table>
Returns an object containing the IDs of the created proxies under the `proxyids` property. The order of the returned IDs matches the order of the passed proxies.

Examples

Create an active proxy

Create an action proxy "Active proxy" and assign a host to be monitored by it.

Request:

```
{  
  "jsonrpc": "2.0",
  "method": "proxy.create",
  "params": {
    "host": "Active proxy",
    "status": "5",
    "hosts": [
      {
        "hostid": "10279"
      }
    ]
  },
  "auth": "ab9638041ec6922cb14b07982b268f47",
  "id": 1
}
```

Response:

```
{  
  "jsonrpc": "2.0",
  "result": {
    "proxyids": [  
      "10280"
    ]
  },
  "id": 1
}
```

Create a passive proxy

Create a passive proxy "Passive proxy" and assign two hosts to be monitored by it.

Request:

```
{  
  "jsonrpc": "2.0",
  "method": "proxy.create",
  "params": {
    "host": "Passive proxy",
    "status": "6",
    "interface": {
      "ip": "127.0.0.1",
      "dns": "",
      "useip": "1",
      "port": "10051"
    },
    "hosts": [
      {
        "hostid": "10192"
      },
      {
        "hostid": "10139"
      }
    ]
  },
  "auth": "ab9638041ec6922cb14b07982b268f47",
  "id": 1
}
```
See also

- Host
- Proxy interface

Source

CProxy::create() in frontends/php/include/classes/api/services/CProxy.php.

**proxy.delete**

Description

object proxy.delete(array proxies)

This method allows to delete proxies.

Parameters

(array) IDs of proxies to delete.

Return values

(object) Returns an object containing the IDs of the deleted proxies under the proxyids property.

Examples

Delete multiple proxies

Delete two proxies.

Request:

```
{
    "jsonrpc": "2.0",
    "method": "proxy.delete",
    "params": [
        "10286",
        "10285"
    ],
    "auth": "3a57200802b24cda67c4e4010b50c065",
    "id": 1
}
```

Response:

```
{
    "jsonrpc": "2.0",
    "result": {
        "proxyids": [
            "10286",
            "10285"
        ],
        "id": 1
    }
}
```
proxy.get

Description

type/array proxy.get(object parameters)

The method allows to retrieve proxies according to the given parameters.

Parameters

(object) Parameters defining the desired output.

The method supports the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>proxyids</td>
<td>string/array</td>
<td>Return only proxies with the given IDs.</td>
</tr>
<tr>
<td>selectHosts</td>
<td>query</td>
<td>Return hosts monitored by the proxy in the hosts property.</td>
</tr>
<tr>
<td>selectInterface</td>
<td>query</td>
<td>Return the proxy interface used by a passive proxy in the interface property.</td>
</tr>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Sort the result by the given properties.</td>
</tr>
<tr>
<td>countOutput</td>
<td>boolean</td>
<td>These parameters being common for all get methods are described in detail in the reference commentary.</td>
</tr>
<tr>
<td>editable</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>excludeSearch</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>filter</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>limit</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>output</td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>preservekeys</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>search</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>searchByAny</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>searchWildcards</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>sortOrder</td>
<td>string/array</td>
<td></td>
</tr>
<tr>
<td>startSearch</td>
<td>boolean</td>
<td></td>
</tr>
</tbody>
</table>

Return values

(integer/array) Returns either:

- an array of objects;
- the count of retrieved objects, if the countOutput parameter has been used.
Examples

Retrieve all proxies

Retrieve all configured proxies and their interfaces.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "proxy.get",
    "params": {
        "output": "extend",
        "selectInterface": "extend"
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": [
        {
            "host": "Active proxy",
            "lastaccess": "0",
            "description": "",
            "tls_connect": "1",
            "tls_accept": "1",
            "tlsIssuer": "",
            "tlsSubject": "",
            "tlsPskIdentity": "",
            "tls_psk": "",
            "proxy_address": "",
            "auto_compress": "0",
            "proxyid": "30091",
            "interface": []
        },
        {
            "host": "Passive proxy",
            "status": "6",
            "lastaccess": "0",
            "description": "",
            "tls_connect": "1",
            "tls_accept": "1",
            "tlsIssuer": "",
            "tlsSubject": "",
            "tlsPskIdentity": "",
            "tls_psk": "",
            "proxy_address": "",
            "auto_compress": "0",
            "proxyid": "30092",
            "interface": {
                "interfaceid": "30109",
                "hostid": "30092",
                "useip": "1",
                "ip": "127.0.0.1",
                "dns": "",
                "port": "10051"
            }
        }
    ],
    "id": 1
}
```
See also

- Host
- Proxy interface

Source

CProxy::get() in frontends/php/include/classes/api/services/CProxy.php.

**proxy.update**

Description

`object proxy.update(object/array proxies)`

This method allows to update existing proxies.

Parameters

`object/array` Proxy properties to be updated.

The `proxyid` property must be defined for each proxy, all other properties are optional. Only the passed properties will be updated, all others will remain unchanged.

Additionally to the **standard proxy properties**, the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hosts</td>
<td>array</td>
<td>Hosts to be monitored by the proxy. If a host is already monitored by a different proxy, it will be reassigned to the current proxy. The hosts must have the <code>hostid</code> property defined.</td>
</tr>
<tr>
<td>interface</td>
<td>object</td>
<td>Host interface to replace the existing interface for the passive proxy.</td>
</tr>
</tbody>
</table>

Return values

`object` Returns an object containing the IDs of the updated proxies under the `proxyids` property.

Examples

**Change hosts monitored by a proxy**

Update the proxy to monitor the two given hosts.

Request:

```json
{
   "jsonrpc": "2.0",
   "method": "proxy.update",
   "params": {
      "proxyid": "10293",
      "hosts": [
         "10294",
         "10295"
      ]
   }
}
```
Response:
{
    "jsonrpc": "2.0",
    "result": {
        "proxyids": [
            "10293"
        ]
    },
    "id": 1
}

Change proxy status

Change the proxy to an active proxy and rename it to "Active proxy".

Request:
{
    "jsonrpc": "2.0",
    "method": "proxy.update",
    "params": {
        "proxyid": "10293",
        "host": "Active proxy",
        "status": "5"
    },
    "auth": "038e1d7b1735c6a5436ee9eae096879e",
    "id": 1
}

Response:
{
    "jsonrpc": "2.0",
    "result": {
        "proxyids": [
            "10293"
        ]
    },
    "id": 1
}

See also
- Host
- Proxy interface

Source
CProxy::update() in frontends/php/include/classes/api/services/CProxy.php.

Screen

This class is designed to work with screen.

Object references:
- Screen
- Screen user
- Screen user group

Available methods:
> Screen object

The following objects are directly related to the screen API.

Screen

The screen object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>screenid</td>
<td>string</td>
<td>(readonly) ID of the screen.</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>Name of the screen.</td>
</tr>
<tr>
<td>hsize</td>
<td>integer</td>
<td>Width of the screen.</td>
</tr>
<tr>
<td>vsize</td>
<td>integer</td>
<td>Height of the screen.</td>
</tr>
<tr>
<td>userid</td>
<td>string</td>
<td>Screen owner user ID.</td>
</tr>
<tr>
<td>private</td>
<td>integer</td>
<td>Type of screen sharing.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values: 0 - public screen; 1 - (default) private screen.</td>
</tr>
</tbody>
</table>

Screen user

List of screen permissions based on users. It has the following properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>screenuserid</td>
<td>string</td>
<td>(readonly) ID of the screen user.</td>
</tr>
<tr>
<td>userid</td>
<td>string</td>
<td>User ID.</td>
</tr>
<tr>
<td>permission</td>
<td>integer</td>
<td>Type of permission level.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values: 2 - read only; 3 - read-write;</td>
</tr>
</tbody>
</table>

Screen user group

List of screen permissions based on user groups. It has the following properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>screenusrgrp</td>
<td>string</td>
<td>(readonly) ID of the screen user group.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>usgrpid</td>
<td>string</td>
<td>User group ID.</td>
</tr>
<tr>
<td>(required)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>permission</td>
<td>integer</td>
<td>Type of permission level.</td>
</tr>
<tr>
<td>(required)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**screen.create**

**Description**

object screen.create(object/array screens)

This method allows to create new screens.

**Parameters**

(object/array) Screens to create.

Additionally to the standard screen properties, the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>screenitems</td>
<td>array</td>
<td>Screen items to be created for the screen.</td>
</tr>
<tr>
<td>users</td>
<td>array</td>
<td>Screen user shares to be created on the screen.</td>
</tr>
<tr>
<td>userGroups</td>
<td>array</td>
<td>Screen user group shares to be created on the screen.</td>
</tr>
</tbody>
</table>

**Return values**

(object) Returns an object containing the IDs of the created screens under the screenids property. The order of the returned IDs matches the order of the passed screens.

**Examples**

**Creating a screen**

Create a screen named "Graphs" with 2 rows and 3 columns and add a graph to the upper-left cell.

**Request:**

```json
{
  "jsonrpc": "2.0",
  "method": "screen.create",
  "params": {
    "name": "Graphs",
    "hsize": 3,
    "vsize": 2,
    "screenitems": [
      {
        "resourcetype": 0,
        "resourceid": "612",
        "rowspan": 1,
        "colspan": 1,
        "x": 0,
        "y": 0
      }
    ]
  },
  "auth": "038e1d7b1735c6a5436ee9eae095879e",
  "id": 1
}
```

**Response:**

```json
1038
```
Screensharing
Create a screen with two types of sharing (user and user group).

Request:
```json
{"jsonrpc": "2.0",
 "method": "screen.create",
 "params": {
  "name": "Screen sharing",
  "hsize": 3,
  "vsize": 2,
  "users": [
    {
      "userid": "4",
      "permission": "3"
    }
  ],
  "userGroups": [
    {
      "usrgrpid": "7",
      "permission": "2"
    }
  ]
},
"auth": "038e1d7b1735c6a5436ee9eae095879e",
"id": 1}
```

Response:
```json
{"jsonrpc": "2.0",
 "result": {
  "screenIds": [
    "83"
  ],
  "id": 1
}
```

See also
- Screen item
- Screen user
- Screen user group

Source
CScreen::create() in frontends/php/include/classes/api/services/CScreen.php.

**screen.delete**

Description

object screen.delete(array screenIds)
This method allows to delete screens.

Parameters

(array) IDs of the screens to delete.

Return values

(object) Returns an object containing the IDs of the deleted screens under the `screenids` property.

Examples

Deleting multiple screens

Delete two screens.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "screen.delete",
    "params": [
        "25",
        "26"
    ],
    "auth": "3a57200802b24cda67c4e4010b50c065",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "screenids": [
            "25",
            "26"
        ],
        "id": 1
    }
}
```

Source

CScreen::delete() in frontends/php/include/classes/api/services/CScreen.php.

**screen.get**

Description

integer/array screen.get(object parameters)

The method allows to retrieve screens according to the given parameters.

Parameters

(object) Parameters defining the desired output.

The method supports the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>screenids</td>
<td>string/array</td>
<td>Return only screens with the given IDs.</td>
</tr>
<tr>
<td>userids</td>
<td>string/array</td>
<td>Return only screens that belong to the given user IDs.</td>
</tr>
</tbody>
</table>
### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>screenitemids</td>
<td>string/array</td>
<td>Return only screens that contain the given screen items.</td>
</tr>
<tr>
<td>selectUsers</td>
<td>query</td>
<td>Returns users that the screen is shared with in users property.</td>
</tr>
<tr>
<td>selectUserGroups</td>
<td>query</td>
<td>Returns user groups that the screen is shared with in userGroups property.</td>
</tr>
<tr>
<td>selectScreenItems</td>
<td>query</td>
<td>Return the screen items that are used in the screen.</td>
</tr>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Sort the result by the given properties.</td>
</tr>
<tr>
<td>countOutput</td>
<td>boolean</td>
<td>These parameters being common for all get methods are described in detail in the reference commentary page.</td>
</tr>
<tr>
<td>editable</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>excludeSearch</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>filter</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>limit</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>output</td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>preservekeys</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>search</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>searchByAny</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>searchWildcards</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>sortOrder</td>
<td>string/array</td>
<td></td>
</tr>
<tr>
<td>startSearch</td>
<td>boolean</td>
<td></td>
</tr>
</tbody>
</table>

### Return values

(integer/array) Returns either:

- an array of objects;
- the count of retrieved objects, if the countOutput parameter has been used.

### Examples

#### Retrieving a screen by ID

Retrieve all data about screen "26" and its screen items.

**Request:**

```json
{
    "jsonrpc": "2.0",
    "method": "screen.get",
    "params": {
```
"output": "extend",
"selectScreenItems": "extend",
"selectUsers": "extend",
"selectUserGroups": "extend",
"screenids": "26"
},
"auth": "038e1d7b1735c6a5436ee9eae095879e",
"id": 1
}

Response:
{
  "jsonrpc": "2.0",
  "result": [
    {
      "screenitems": [
        {
          "screenitemid": "67",
          "screenid": "26",
          "resourcetype": "0",
          "resourceid": "612",
          "width": "320",
          "height": "200",
          "x": "0",
          "y": "0",
          "colspan": "0",
          "rowspan": "0",
          "elements": "25",
          "valign": "0",
          "halign": "0",
          "style": "0",
          "url": "",
          "dynamic": "0",
          "sort_triggers": "0"
        }
      ],
      "users": [
        {
          "sysmapuserid": "1",
          "userid": "2",
          "permission": "2"
        }
      ],
      "userGroups": [
        {
          "screenusrgrpid": "1",
          "usrgrpid": "7",
          "permission": "3"
        }
      ],
      "screenid": "26",
      "name": "CPU Graphs",
      "hsize": "3",
      "vsize": "2",
      "userid": "1",
      "private": "1"
    }
  ],
  "id": 1
}

See also
• Screen item
• Screen user
• Screen user group

Source
CScreen::get() in frontends/php/include/classes/api/services/CScreen.php.

screen.update

Description
object screen.update(object/array screens)

This method allows to update existing screens.

Parameters
(object/array) Screen properties to be updated.

The screenid property must be defined for each screen, all other properties are optional. Only the passed properties will be updated, all others will remain unchanged.

Additionally to the standard screen properties, the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>screenitems</td>
<td>array</td>
<td>Screen items to replace existing screen items.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Screen items are updated by coordinates, so each screen item must have the x and y properties defined.</td>
</tr>
<tr>
<td>users</td>
<td>array</td>
<td>Screen user shares to replace the existing elements.</td>
</tr>
<tr>
<td>userGroups</td>
<td>array</td>
<td>Screen user group shares to replace the existing elements.</td>
</tr>
</tbody>
</table>

Return values
(object) Returns an object containing the IDs of the updated screens under the screenids property.

Examples
Renaming a screen

Rename a screen to “CPU Graphs”.

Request:
{
    "jsonrpc": "2.0",
    "method": "screen.update",
    "params": {
        "screenid": "26",
        "name": "CPU Graphs"
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "screenids": [
            "26"
        ],
        "id": 1
    }
}
```

Change screen owner

Available only for admins and super admins.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "screen.update",
    "params": {
        "screenid": "83",
        "userid": "1"
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 2
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "screenids": [
            "83"
        ],
        "id": 2
    }
}
```

See also

- Screen item
- `screenitem.create`
- `screenitem.update`
- `screenitem.updatebyposition`
- Screen user
- Screen user group

Source

`CScreen::update()` in `frontends/php/include/classes/api/services/CScreen.php`.

**Screen item**

This class is designed to work with screen items.

Object references:

- Screen item

Available methods:

- `screenitem.create` - creating new screen items
- `screenitem.delete` - deleting screen items
- `screenitem.get` - retrieving screen items
> Screen item object

The following objects are directly related to the `screenitem` API.

Screen item

The screen item object defines an element displayed on a screen. It has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>screenitemid</code></td>
<td>string</td>
<td>(readonly) ID of the screen item.</td>
</tr>
<tr>
<td><code>resourcetype</code></td>
<td>integer</td>
<td>Type of screen item. Possible values: 0 - graph; 1 - simple graph; 2 - map; 3 - plain text; 4 - hosts info; 5 - triggers info; 6 - system information; 7 - clock; 8 - screen; 9 - triggers overview; 10 - data overview; 11 - URL; 12 - history of actions; 13 - history of events; 14 - latest host group issues; 15 - problems by severity; 16 - latest host issues; 19 - simple graph prototype; 20 - graph prototype.</td>
</tr>
<tr>
<td><code>screenid</code></td>
<td>string</td>
<td>ID of the screen that the item belongs to.</td>
</tr>
<tr>
<td><code>application</code></td>
<td>string</td>
<td>Application or part of application name by which data in screen item can be filtered. Applies to resource types: “Data overview” and “Triggers overview”</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>colspan</td>
<td>integer</td>
<td>Number of columns the screen item will span across. Default: 1.</td>
</tr>
<tr>
<td>dynamic</td>
<td>integer</td>
<td>Whether the screen item is dynamic. Possible values: 0 - (default) not dynamic; 1 - dynamic.</td>
</tr>
<tr>
<td>elements</td>
<td>integer</td>
<td>Number of lines to display on the screen item. Default: 25.</td>
</tr>
<tr>
<td>halign</td>
<td>integer</td>
<td>Specifies how the screen item must be aligned horizontally in the cell. Possible values: 0 - (default) center; 1 - left; 2 - right.</td>
</tr>
<tr>
<td>height</td>
<td>integer</td>
<td>Height of the screen item in pixels. Default: 200.</td>
</tr>
<tr>
<td>max_columns</td>
<td>integer</td>
<td>Specifies the maximum amount of columns a graph prototype or simple graph prototype screen element can have. Default: 3.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>--------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>resourceid</td>
<td>string</td>
<td>ID of the object displayed on the screen item. Depending on the type of a screen item, the resourceid property can reference different objects. Required for data overview, graph, map, plain text, screen, simple graph and trigger overview screen items. Unused by local and server time clocks, history of actions, history of events, hosts info, system information, problems by severity and URL screen items. Number or rows the screen item will span across. Default: 1.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>sort_triggers</td>
<td>integer</td>
<td>Order in which actions or triggers must be sorted. Possible values for history of actions screen elements: 3 - time, ascending; 4 - time, descending; 5 - type, ascending; 6 - type, descending; 7 - status, ascending; 8 - status, descending; 9 - retries left, ascending; 10 - retries left, descending; 11 - recipient, ascending; 12 - recipient, descending. Possible values for latest host group issues and latest host issues screen items: 0 - (default) last change, descending; 1 - severity, descending; 2 - host, ascending.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>----------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>style</td>
<td>integer</td>
<td>Screen item display option.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values for data overview and triggers overview screen items:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - (default) display hosts on the left side;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - display hosts on the top.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values for hosts info and triggers info screen elements:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - (default) horizontal layout;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - vertical layout.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values for clock screen items:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - (default) local time;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - server time;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 - host time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values for plain text screen items:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - (default) display values as plain text;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - display values as HTML.</td>
</tr>
<tr>
<td>url</td>
<td>string</td>
<td>URL of the webpage to be displayed in the screen item.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Used by URL screen items.</td>
</tr>
<tr>
<td>valign</td>
<td>integer</td>
<td>Specifies how the screen item must be aligned vertically in the cell.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - (default) middle;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - top;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 - bottom.</td>
</tr>
<tr>
<td>width</td>
<td>integer</td>
<td>Width of the screen item in pixels.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 320.</td>
</tr>
</tbody>
</table>
### screenitem.create

**Description**

The `screenitem.create` method allows you to create new screen items.

**Parameters**

- `(object/array)` Screen items to create.

The method accepts screen items with the standard screen item properties.

**Return values**

- `(object)` Returns an object containing the IDs of the created screen items under the `screenitemids` property. The order of the returned IDs matches the order of the passed screen items.

**Examples**

#### Creating a screen item

Create a screen item displaying a graph in the left-upper cell of the screen.

**Request:**

```json
{
    "jsonrpc": "2.0",
    "method": "screenitem.create",
    "params": {
        "screenid": 16,
        "resourcetype": 0,
        "resourceid": 612,
        "x": 0,
        "y": 0
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

**Response:**

```json
{
    "jsonrpc": "2.0",
    "result": {
        "screenitemids": ["65"]
    },
    "id": 1
}
```
**screenitem.delete**

**Description**

`object screenitem.delete(array screenItemIds)`

This method allows to delete screen items.

**Parameters**

- **(array)** IDs of the screen items to delete.

**Return values**

- **(object)** Returns an object containing the IDs of the deleted screen items under the `screenitemids` property.

**Examples**

Deleting multiple screen items

Delete two screen items.

**Request:**

```json
{
   "jsonrpc": "2.0",
   "method": "screenitem.delete",
   "params": [
      "65",
      "63"
   ],
   "auth": "3a57200802b24cda67c4e4010b50c065",
   "id": 1
}
```

**Response:**

```json
{
   "jsonrpc": "2.0",
   "result": {
      "screenitemids": [
         "65",
         "63"
      ],
      "id": 1
   }
}
```

See also

- [screen.update](#)

Source

`CScreenItem::create()` in `frontends/php/include/classes/api/services/CScreenItem.php`.

**screenitem.get**

**Description**

`integer/array screenitem.get(object parameters)`

The method allows to retrieve screen items according to the given parameters.

**Parameters**
Parameters defining the desired output.

The method supports the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>screenitemids</td>
<td>string/array</td>
<td>Return only screen items with the given IDs.</td>
</tr>
<tr>
<td>screenids</td>
<td>string/array</td>
<td>Return only screen items that belong to the given screen.</td>
</tr>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Sort the result by the given properties.</td>
</tr>
<tr>
<td>countOutput</td>
<td>boolean</td>
<td>These parameters being common for all get methods are described in detail in the reference commentary page.</td>
</tr>
<tr>
<td>editable</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>excludeSearch</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>filter</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>limit</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>output</td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>preservekeys</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>search</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>searchByAny</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>searchWildcardsEnabled</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>sortorder</td>
<td>string/array</td>
<td></td>
</tr>
<tr>
<td>startSearch</td>
<td>boolean</td>
<td></td>
</tr>
</tbody>
</table>

Return values

(integer/array) Returns either:

- an array of objects;
- the count of retrieved objects, if the countOutput parameter has been used.

Examples

Retrieving screen items from screen

Retrieve all screen items from the given screen.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "screenitem.get",
    "params": {
        "output": "extend",
        "screenids": "3"
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```
Response:

{
"jsonrpc": "2.0",
"result": [
{
"screenitemid": "20",
"screenid": "3",
"resourcetype": "0",
"resourceid": "433",
"width": "500",
"height": "120",
"x": "0",
"y": "0",
"colspan": "1",
"rowspan": "1",
"elements": "0",
"valign": "1",
"halign": "0",
"style": "0",
"url": "",
"dynamic": "0",
"sort_triggers": "0",
"application": "",
"max_columns": "3"
},
{
"screenitemid": "21",
"screenid": "3",
"resourcetype": "0",
"resourceid": "387",
"width": "500",
"height": "100",
"x": "0",
"y": "1",
"colspan": "1",
"rowspan": "1",
"elements": "0",
"valign": "1",
"halign": "0",
"style": "0",
"url": "",
"dynamic": "0",
"sort_triggers": "0",
"application": "",
"max_columns": "3"
},
{
"screenitemid": "22",
"screenid": "3",
"resourcetype": "1",
"resourceid": "10013",
"width": "500",
"height": "148",
"x": "1",
"y": "0",
"colspan": "1",
"rowspan": "1",
"elements": "0",
"valign": "1",
"halign": "0",
"style": "0",
"url": "",

1053


Source
CScreenItem::get() in frontends/php/include/classes/api/services/CScreenItem.php.

**screenitem.update**

**Description**

object screenitem.update(object/array screenItems)

This method allows to update existing screen items.

**Parameters**

(object/array) Screen item properties to be updated.

The screenitemid property must be defined for each screen item, all other properties are optional. Only the passed properties will be updated, all others will remain unchanged.

**Return values**

(object) Returns an object containing the IDs of the updated screen items under the screenitemids property.

**Examples**

Setting the size of the screen item

Set the width of the screen item to 500px and height to 300px.

**Request:**

```json
{
    "jsonrpc": "2.0",
    "method": "screenitem.update",
    "params": {
        "screenitemid": "20",
        "width": 500,
        "height": 300
    }
}
```
Response:
{
    "jsonrpc": "2.0",
    "result": {
        "screenitemids": [
            "20"
        ],
        "id": 1
    },
    "id": 1
}

See also
- `screenitem.updatebyposition`

Source
CScreenItem::update() in frontends/php/include/classes/api/services/CScreenItem.php.

**screenitem.updatebyposition**

**Description**

object screenitem.updatebyposition(array screenItems)

This method allows to update screen items in the given screen cells. If a cell is empty, a new screen item will be created.

**Parameters**

(array) **Screen item properties** to be updated.

The x, y and screenid properties must be defined for each screen item, all other properties are optional. Only the passed properties will be updated, all others will remain unchanged.

**Return values**

(object) Returns an object containing the IDs of the updated and created screen items under the `screenitemids` property.

**Examples**

Changing a screen items resource ID

Change the resource ID for the screen element located in the upper-left cell of the screen.

**Request:**

```
{
    "jsonrpc": "2.0",
    "method": "screenitem.updatebyposition",
    "params": [
        {
            "screenid": "16",
            "x": 0,
            "y": 0,
            "resourceid": "644"
        }
    ],
    "auth": "038e1d7b1735c6a5436ee9eae096879e",
    "id": 1
}
```

**Response:**

```
{
    "jsonrpc": "2.0",
    "result": {
```
"screenitemids": [
  "66"
],
"id": 1
}

See also

- screenitem.update

Source

CScreenItem::update() in frontends/php/include/classes/api/services/CScreenItem.php.

**Script**

This class is designed to work with scripts.

Object references:

- **Script**

Available methods:

- script.create - create new scripts
- script.delete - delete scripts
- script.execute - run scripts
- script.get - retrieve scripts
- script.getscriptsbyhosts - retrieve scripts for hosts
- script.update - update scripts

> **Script object**

The following objects are directly related to the script API.

Script

The script object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scriptid</td>
<td>string</td>
<td>(readonly) ID of the script.</td>
</tr>
<tr>
<td>command</td>
<td>string</td>
<td>Command to run.</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>Name of the script.</td>
</tr>
<tr>
<td>confirmation</td>
<td>string</td>
<td>Confirmation pop up text. The pop up will appear when trying to run the script from the Zabbix frontend.</td>
</tr>
<tr>
<td>description</td>
<td>string</td>
<td>Description of the script.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>execute_on</td>
<td>integer</td>
<td>Where to run the script.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values: 0 - run on Zabbix agent; 1 - run on Zabbix server; 2 -(default) run on Zabbix server (proxy).</td>
</tr>
<tr>
<td>groupid</td>
<td>string</td>
<td>ID of the host group that the script can be run on. If set to 0, the script will be available on all host groups.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 0.</td>
</tr>
<tr>
<td>host_access</td>
<td>integer</td>
<td>Host permissions needed to run the script.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values: 2 -(default) read; 3 - write.</td>
</tr>
<tr>
<td>type</td>
<td>integer</td>
<td>Script type.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values: 0 -(default) script; 1 - IPMI.</td>
</tr>
<tr>
<td>usrgpid</td>
<td>string</td>
<td>ID of the user group that will be allowed to run the script. If set to 0, the script will be available for all user groups.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 0.</td>
</tr>
</tbody>
</table>

Note that for some methods (update, delete) the required/optional parameter combination is different.

**script.create**

Description

object script.create(object/array scripts)

This method allows to create new scripts.

Parameters

(object/array) Scripts to create.

The method accepts scripts with the standard script properties.

Return values

(object) Returns an object containing the IDs of the created scripts under the scriptids property. The order of the returned IDs matches the order of the passed scripts.
Examples

Create a script

Create a script that will reboot a server. The script will require write access to the host and will display a configuration message before running in the frontend.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "script.create",
    "params": {
        "name": "Reboot server",
        "command": "reboot server 1",
        "host_access": 3,
        "confirmation": "Are you sure you would like to reboot the server?"
    },
    "auth": "038e1d7b1735c6a5436ee9eae09b879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "scriptids": [
            "3"
        ]
    },
    "id": 1
}
```

Source

CScript::create() in frontends/php/include/classes/api/services/CScript.php.

**script.delete**

Description

object script.delete(array scriptIds)

This method allows to delete scripts.

Parameters

(array) IDs of the scripts to delete.

Return values

(object) Returns an object containing the IDs of the deleted scripts under the scriptIds property.

Examples

Delete multiple scripts

Delete two scripts.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "script.delete",
    "params": [
        "3",
        "4"
    ],
    "auth": "3a57200802b24cda67c4e010b50c065",
    "id": 1
}
```
Response:
{
    "jsonrpc": "2.0",
    "result": {
        "scriptids": ["3", "4"]
    },
    "id": 1
}

Source
CScript::delete() in frontends/php/include/classes/api/services/CScript.php.

**script.execute**

**Description**

object script.execute(object parameters)

This method allows to run a script on a host.

**Parameters**

(object) Parameters containing the ID of the script to run and the ID of the host.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostid</td>
<td>string</td>
<td>ID of the host to run the script on. (required)</td>
</tr>
<tr>
<td>scriptid</td>
<td>string</td>
<td>ID of the script to run. (required)</td>
</tr>
</tbody>
</table>

**Return values**

(object) Returns the result of script execution.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>response</td>
<td>string</td>
<td>Whether the script was run successfully. Possible values: success or failed.</td>
</tr>
<tr>
<td>value</td>
<td>string</td>
<td>Script output.</td>
</tr>
</tbody>
</table>

**Examples**

**Run a script**

Run a "ping" script on a host.

**Request:**
{
    "jsonrpc": "2.0",
    "method": "script.execute",
    "params": {
        "scriptid": "1",
        "hostid": "1"
    }
}
"hostid": "30079"
{
  "auth": "038e1d7b1735c6a5436ee9eae095879e",
  "id": 1
}

Response:
{
  "jsonrpc": "2.0",
  "result": {
    "response": "success",
    "value": "PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_req=1 ttl=64 time=0.074 ms
64 bytes from 127.0.0.1: icmp_req=2 ttl=64 time=0.030 ms
64 bytes from 127.0.0.1: icmp_req=3 ttl=64 time=0.030 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.030/0.044/0.074/0.022 ms"
  },
  "id": 1
}

Source

CScript::execute() in frontends/php/include/classes/api/services/CScript.php.

script.get

Description

integer/array script.get(object parameters)

The method allows to retrieve scripts according to the given parameters.

Parameters

(object) Parameters defining the desired output.

The method supports the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>groupids</td>
<td>string/array</td>
<td>Return only scripts that can be run on the given host groups.</td>
</tr>
<tr>
<td>hostids</td>
<td>string/array</td>
<td>Return only scripts that can be run on the given hosts.</td>
</tr>
<tr>
<td>scriptids</td>
<td>string/array</td>
<td>Return only scripts with the given IDs.</td>
</tr>
<tr>
<td>usrgrpids</td>
<td>string/array</td>
<td>Return only scripts that can be run by users in the given user groups.</td>
</tr>
<tr>
<td>selectGroups</td>
<td>query</td>
<td>Return host groups that the script can be run on in the groups property.</td>
</tr>
<tr>
<td>selectHosts</td>
<td>query</td>
<td>Return hosts that the script can be run on in the hosts property.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Sort the result by the given properties. Possible values are: scriptid and name.</td>
</tr>
<tr>
<td>countOutput</td>
<td>boolean</td>
<td>These parameters being common for all get methods are described in detail in the reference commentary.</td>
</tr>
<tr>
<td>editable</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>excludeSearch</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>filter</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>limit</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>output</td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>preservekeys</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>search</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>searchByAny</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>searchWildcardsEnabled</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>sortorder</td>
<td>string/array</td>
<td></td>
</tr>
<tr>
<td>startSearch</td>
<td>boolean</td>
<td></td>
</tr>
</tbody>
</table>

Return values
(integer/array) Returns either:
- an array of objects;
- the count of retrieved objects, if the countOutput parameter has been used.

Examples
Retrieve all scripts
Retrieve all configured scripts.

Request:
```json
{
    "jsonrpc": "2.0",
    "method": "script.get",
    "params": {
        "output": "extend"
    },
    "auth": "038e1d7b1735c6a5436ee9eae096879e",
    "id": 1
}
```

Response:
```json
{
    "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": ""
        }
    ]
}
```
See also

- Host
- Host group

Source

CScript::get() in frontends/php/include/classes/api/services/CScript.php.

**script.getscriptsbyhosts**

Description

object script.getscriptsbyhosts(array hostIds)

This method allows to retrieve scripts available on the given hosts.

Parameters

(string/array) IDs of hosts to return scripts for.

Return values

(object) Returns an object with host IDs as properties and arrays of available scripts as values.

**Note:**
The method will automatically expand macros in the confirmation text.

Examples

Retrieve scripts by host IDs

Retrieve all scripts available on hosts "30079" and "30073".

Request:
{
  "jsonrpc": "2.0",
  "method": "script.getscriptsbyhosts",
  "params": [
    "30079",
    "30073"
  ],
  "auth": "038e1d7b1735c6a5436ee9eae095879e",
  "id": 1
}

Response:
{
  "jsonrpc": "2.0",
  "result": [
    "30079": [
      {
        "scriptid": "3",
        "name": "Detect operating system",
        "command": "sudo /usr/bin/nmap -O {HOST.CONN} 2>&1",
        "host_access": "2",
        "usrgrp_id": "7",
        "group_id": "0",
        "description": "",
        "confirmation": "",
        "type": "0",
        "execute_on": "1",
        "host_id": "10001"
      },
      {
        "scriptid": "1",
        "name": "Ping",
        "command": "/bin/ping -c 3 {HOST.CONN} 2>&1",
        "host_access": "2",
        "usrgrp_id": "0",
        "group_id": "0",
        "description": "",
        "confirmation": "",
        "type": "0",
        "execute_on": "1",
        "host_id": "10001"
      },
      {
        "scriptid": "2",
        "name": "Traceroute",
        "command": "/usr/bin/traceroute {HOST.CONN} 2>&1",
        "host_access": "2",
        "usrgrp_id": "0",
        "group_id": "0",
        "description": "",
        "confirmation": "",
        "type": "0",
        "execute_on": "1",
        "host_id": "10001"
      }
    ],
    "30073": [
      {
        "scriptid": "3",
        "name": "Detect operating system",
        "command": "/usr/bin/nmap -O {HOST.CONN} 2>&1",
        "host_access": "2",
        "usrgrp_id": "0",
        "group_id": "0",
        "description": "",
        "confirmation": "",
        "type": "0",
        "execute_on": "1",
        "host_id": "10001"
      }
    ]
  ]
}
"usrgrpid": "7",
"groupid": "0",
"description": "",
"confirmation": "",
"type": "0",
"execute_on": "1",
"hostid": "10001"
},
{
  "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",
  "hostid": "10001"
},
{
  "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",
  "hostid": "10001"
}
],
"id": 1
}

Source
CScript::getScriptsByHosts() in frontends/php/include/classes/api/services/CScript.php.

**script.update**

**Description**

object script.update(object/array scripts)

This method allows to update existing scripts.

**Parameters**

(object/array) **Script properties** to be updated.

The scriptid property must be defined for each script, all other properties are optional. Only the passed properties will be updated, all others will remain unchanged.

**Return values**

(object) Returns an object containing the IDs of the updated scripts under the scriptids property.

**Examples**

Change script command

Change the command of the script to "/bin/ping -c 10 {HOST.CONN} 2>&1".
Source
CScript::update() in frontends/php/include/classes/api/services/CScript.php.

**Service**

This class is designed to work with services.

**Object references:**

- Service
- Service time
- Service dependency
- Service alarm

**Available methods:**

- service.adddependencies - adding dependencies between IT services
- service.addtimes - adding service times
- service.create - creating new IT services
- service.delete - deleting IT services
- service.deletedeclarations - deleting dependencies between IT services
- service.deletetimes - deleting service times
- service.get - retrieving IT services
- service.getsla - retrieving availability information about IT services
- service.update - updating IT services

**> Service object**

The following objects are directly related to the service API.

**Service**

The service object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>serviceid</td>
<td>string</td>
<td>(readonly) ID of the service.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>algorithm</strong></td>
<td>integer</td>
<td><strong>Algorithm</strong> used to calculate the state of the service. Possible values: 0 - do not calculate; 1 - problem, if at least one child has a problem; 2 - problem, if all children have problems.</td>
</tr>
<tr>
<td><strong>name</strong></td>
<td>string</td>
<td>Name of the service. Whether SLA should be calculated.</td>
</tr>
<tr>
<td><strong>showsla</strong></td>
<td>integer</td>
<td>Whether SLA should be calculated. Possible values: 0 - do not calculate; 1 - calculate.</td>
</tr>
<tr>
<td><strong>sortorder</strong></td>
<td>integer</td>
<td>Position of the service used for sorting.</td>
</tr>
<tr>
<td><strong>goodsla</strong></td>
<td>float</td>
<td>Minimum acceptable SLA value. If the SLA drops lower, the service is considered to be in problem state. Default: 99.9.</td>
</tr>
<tr>
<td><strong>status</strong></td>
<td>integer</td>
<td>Whether the service is in OK or problem state. If the service is in problem state, <strong>status</strong> is equal either to: - the priority of the linked trigger if it is set to 2, “Warning” or higher (priorities 0, &quot;Not classified&quot; and 1, “Information” are ignored); - the highest status of a child service in problem state. If the service is in OK state, <strong>status</strong> is equal to 0.</td>
</tr>
</tbody>
</table>
### Property | Type | Description
--- | --- | ---
triggerid | string | Trigger associated with the service. Can only be set for services that don't have children. Default: 0

Note that for some methods (update, delete) the required/optional parameter combination is different.

### Service time

The service time object defines periods, when an service is scheduled to be up or down. It has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>timeid</td>
<td>string</td>
<td>(readonly) ID of the service time.</td>
</tr>
<tr>
<td>serviceid</td>
<td>string</td>
<td>ID of the service. Cannot be updated.</td>
</tr>
<tr>
<td>ts_from</td>
<td>integer</td>
<td>Time when the service time comes into effect. For onetime downtimes ts_from must be set as a Unix timestamp, for other types - as a specific time in a week, in seconds, for example, 90000 for Mon, 1:00 AM.</td>
</tr>
<tr>
<td>ts_to</td>
<td>integer</td>
<td>Time when the service time ends. For onetime uptimes ts_to must be set as a Unix timestamp, for other types - as a specific time in a week, in seconds, for example, 90000 for Mon, 1:00 AM.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>type</td>
<td>integer</td>
<td>Service time type.</td>
</tr>
<tr>
<td></td>
<td>(required)</td>
<td>Possible values: 0 - planned uptime, repeated every week; 1 - planned downtime, repeated every week; 2 - one-time downtime.</td>
</tr>
<tr>
<td>note</td>
<td>string</td>
<td>Additional information about the service time.</td>
</tr>
</tbody>
</table>

Service dependency
The service dependency object represents a dependency between services. It has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>linkid</td>
<td>string</td>
<td>(readonly) ID of the service dependency.</td>
</tr>
<tr>
<td>servicedownid</td>
<td>string</td>
<td>ID of the service, that a service depends on, that is, the child service. An service can have multiple children.</td>
</tr>
<tr>
<td>serviceupid</td>
<td>string</td>
<td>ID of the service, that is dependent on a service, that is, the parent service. An service can have multiple parents forming a directed graph.</td>
</tr>
</tbody>
</table>
## Property

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>soft</td>
<td>integer</td>
<td>Type of dependency between services. Possible values: 0 - hard dependency; 1 - soft dependency. An service can have only one hard-dependent parent. This attribute has no effect on status or SLA calculation and is only used to create a core service tree. Additional parents can be added as soft dependencies forming a graph. An service can not be deleted if it has hard-dependent children.</td>
</tr>
</tbody>
</table>

### Service alarm

**Note:**
Service alarms cannot be directly created, updated or deleted via the Zabbix API.

The service alarm objects represents an service’s state change. It has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>servicealarmid</td>
<td>string</td>
<td>ID of the service alarm.</td>
</tr>
<tr>
<td>serviceid</td>
<td>string</td>
<td>ID of the service. Time when the service state change has happened.</td>
</tr>
<tr>
<td>clock</td>
<td>timestamp</td>
<td>Status of the service. Refer the service status property for a list of possible values.</td>
</tr>
<tr>
<td>value</td>
<td>integer</td>
<td></td>
</tr>
</tbody>
</table>
object service.adddependencies(object/array serviceDependencies)

This method allows to create dependencies between services.

Parameters

(object/array) Service dependencies to create.

Each service dependency has the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>serviceid</td>
<td>string</td>
<td>ID of the service that depends on a service, that is, the parent service.</td>
</tr>
<tr>
<td>dependsOnServiceid</td>
<td>string</td>
<td>ID of the service that a service depends on, that is, the child service.</td>
</tr>
<tr>
<td>soft</td>
<td>string</td>
<td>Type of dependency. Refer to the service dependency object page for more information on dependency types.</td>
</tr>
</tbody>
</table>

Return values

(object) Returns an object containing the IDs of the affected parent services under the serviceids property.

Examples

Creating a hard dependency

Make service “2” a hard-dependent child of service “3”.

Request:

{   "jsonrpc": "2.0",   "method": "service.adddependencies",   "params": {       "serviceid": "3",       "dependsOnServiceid": "2",       "soft": 0   },   "auth": "038e1d7b1735c6a5436ee9eae095879e",   "id": 1 }

Response:

{   "jsonrpc": "2.0",   "result": {       "serviceids": [ "3" ]   },   "id": 1 }
See also

- service.update

Source

CService::addDependencies() in frontends/php/include/classes/api/services/CService.php.

**service.addtimes**

Description

object service.addtimes(object/array serviceTimes)

This method allows to create new service times.

Parameters

(object/array) Service times to create.

The method accepts service times with the standard service time properties.

Return values

(object) Returns an object containing the IDs of the affected services under the serviceids property.

Examples

Adding a scheduled downtime

Add a downtime for service with ID "4" scheduled weekly from Monday 22:00 till Tuesday 10:00.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "service.addtimes",
    "params": {
        "serviceid": "4",
        "type": 1,
        "ts_from": 165600,
        "ts_to": 201600
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "serviceids": [
            "4"
        ]
    },
    "id": 1
}
```

See also

- service.update

Source

CService::addTimes() in frontends/php/include/classes/api/services/CService.php.

**service.create**

Description

object service.create(object/array services)
This method allows to create new services.

Parameters

(object/array) services to create.

Additionally to the standard service properties, the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dependencies</td>
<td>array</td>
<td>Service dependencies. Each service dependency has the following parameters:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- dependsOnServiceid - (string) ID of a service the service depends on, that is, the child service.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- soft - (integer) type of service dependency; refer to the service dependency object page for more information on dependency types.</td>
</tr>
<tr>
<td>parentid</td>
<td>string</td>
<td>ID of a hard-linked parent service.</td>
</tr>
<tr>
<td>times</td>
<td>array</td>
<td>Service times to be created for the service.</td>
</tr>
</tbody>
</table>

Return values

(object) Returns an object containing the IDs of the created services under the serviceids property. The order of the returned IDs matches the order of the passed services.

Examples

Creating an service

Create an service that will be switched to problem state, if at least one child has a problem. SLA calculation will be on and the minimum acceptable SLA is 99.99%.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "service.create",
    "params": {
        "name": "Server 1",
        "algorithm": 1,
        "showsla": 1,
        "goodsla": 99.99,
        "sortorder": 1
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e"
}
```
{  "jsonrpc": "2.0",
  "result": {
    "serviceids": [5]
  },
  "id": 1
}

Source
CService::create() in frontends/php/include/classes/api/services/CService.php.

**service.delete**

Description
object service.delete(array serviceIds)
This method allows to delete services.
Services with hard-dependent child services cannot be deleted.

Parameters
(array) IDs of the services to delete.

Return values
(object) Returns an object containing the IDs of the deleted services under the serviceids property.

Examples
Deleting multiple services
Delete two services.

Request:
{
  "jsonrpc": "2.0",
  "method": "service.delete",
  "params": [
    "4",
    "5"
  ],
  "auth": "3a57200802b24cda67c4e4010b50c065",
  "id": 1
}

Response:
{
  "jsonrpc": "2.0",
  "result": {
    "serviceids": [
      "4",
      "5"
    ]
  },
  "id": 1
}

Source
service.deletedependencies

Description

object service.deletedependencies(string/array serviceIds)

This method allows to delete all dependencies from services.

Parameters

(string/array) IDs of the services to delete all dependencies from.

Return values

(object) Returns an object containing the IDs of the affected services under the serviceids property.

Examples

Deleting dependencies from an service

Delete all dependencies from service "2".

Request:

```
{   "jsonrpc": "2.0",   "method": "service.deletedependencies",   "params": [     "2"   ],   "auth": "3a57200802b24cda67c4e4010b50c065",   "id": 1 }
```

Response:

```
{   "jsonrpc": "2.0",   "result": {     "serviceids": [       "2"     ]   },   "id": 1 }
```

See also

• service.update

Source

CService::delete() in frontends/php/include/classes/api/services/CService.php.

service.deletetimes

Description

object service.deletetimes(string/array serviceIds)

This method allows to delete all service times from services.

Parameters

(string/array) IDs of the services to delete all service times from.

Return values

(object) Returns an object containing the IDs of the affected services under the serviceids property.

Examples
Deletingservicetimesfromanservice

Delete all service times from service "2".

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "service.deletetimes",
    "params": [
        "2"
    ],
    "auth": "3a57200802b24cda67c4e4010b50c065",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "serviceids": [
            "2"
        ],
        "id": 1
    }
}
```

See also

- service.update

Source

CService::delete() in frontends/php/include/classes/api/services/CService.php.

**service.get**

Description

integer/array service.get(object parameters)

The method allows to retrieve services according to the given parameters.

Parameters

(object) Parameters defining the desired output.

The method supports the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>serviceids</td>
<td>string/array</td>
<td>Return only services with the given IDs.</td>
</tr>
<tr>
<td>parentids</td>
<td>string/array</td>
<td>Return only services with the given hard-dependent parent services.</td>
</tr>
<tr>
<td>childids</td>
<td>string/array</td>
<td>Return only services that are hard-dependent on the given child services.</td>
</tr>
<tr>
<td>selectParent</td>
<td>query</td>
<td>Return a parent property with the hard-dependent parent service.</td>
</tr>
</tbody>
</table>
Parameter | Type | Description
--- | --- | ---
selectDependencies query | | Return a dependencies property with child service dependencies.
selectParentDependencies query | | Return a parentDependencies property with parent service dependencies.
selectTimes query | | Return a times property with service times.
selectAlarms query | | Return an alarms property with service alarms.
selectTrigger query | | Return a trigger property with the associated trigger.
sortfield string/array | | Sort the result by the given properties. Possible values are: name and sortorder. These parameters being common for all get methods are described in detail in the reference commentary.
countOutput boolean | | The parameters being common for all get methods are described in detail in the reference commentary.
editable boolean | | 
excludeSearch boolean | | 
filter object | | 
limit integer | | 
output query | | 
preservekeys boolean | | 
search object | | 
searchByAny boolean | | 
searchWildcardsEnabled boolean | | 
sortorder string/array | | 
startSearch boolean | | 

Return values
(integer/array) Returns either:
• an array of objects;
• the count of retrieved objects, if the countOutput parameter has been used.

Examples
Retrieving all services
Retrieve all data about all services and their dependencies.
Request:
```json
{
  "jsonrpc": "2.0",
  "method": "service.get",
  ...}
```
"params": {
  "output": "extend",
  "selectDependencies": "extend"
},
"auth": "038e1d7b1735c6a5436ee9eae095879e",
"id": 1
}

Response:
{
  "jsonrpc": "2.0",
  "result": [
    {
      "serviceid": "2",
      "name": "Server 1",
      "status": "0",
      "algorithm": "1",
      "triggerid": "0",
      "showsla": "1",
      "goodsla": "99.9000",
      "sortorder": "0",
      "dependencies": []
    },
    {
      "serviceid": "3",
      "name": "Data center 1",
      "status": "0",
      "algorithm": "1",
      "triggerid": "0",
      "showsla": "1",
      "goodsla": "99.9000",
      "sortorder": "0",
      "dependencies": [
        {
          "linkid": "11",
          "serviceupid": "3",
          "servicedownid": "2",
          "soft": "0",
          "sortorder": "0",
          "serviceid": "2"
        },
        {
          "linkid": "10",
          "serviceupid": "3",
          "servicedownid": "5",
          "soft": "0",
          "sortorder": "1",
          "serviceid": "5"
        }
      ]
    },
    {
      "serviceid": "5",
      "name": "Server 2",
      "status": "0",
      "algorithm": "1",
      "triggerid": "0",
      "showsla": "1",
      "goodsla": "99.9900",
      "sortorder": "1",
      "dependencies": []
    }
  ]
}


Source
CService::get() in frontends/php/include/classes/api/services/CService.php.

**service.getsla**

Description

object service.getsla(object parameters)

This method allows to calculate availability information about services.

Parameters

(object) Parameters containing the IDs of the services and time intervals to calculate SLA.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>serviceids</td>
<td>string/array</td>
<td>IDs of services to return availability information for.</td>
</tr>
<tr>
<td>intervals</td>
<td>array</td>
<td>Time intervals to return service layer availability information about.</td>
</tr>
</tbody>
</table>

Each time interval must have the following parameters:
- **from** (timestamp) interval start time;
- **to** (timestamp) interval end time.

Return values

(object) Returns the following availability information about each service under the corresponding service ID.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status</td>
<td>integer</td>
<td>Current status of the service. Refer to the service object page for more information on service statuses.</td>
</tr>
<tr>
<td>problems</td>
<td>array</td>
<td>Triggers that are currently in problem state and are linked either to the service or one of its descendants.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>sla</td>
<td>array</td>
<td>SLA data about each time period.</td>
</tr>
</tbody>
</table>

Each SLA object has the following properties:
- `from` - (timestamp) interval start time;
- `to` - (timestamp) interval end time;
- `sla` - (float) SLA for the given time interval;
- `okTime` - (integer) time the service was in OK state, in seconds;
- `problemTime` - (integer) time the service was in problem state, in seconds;
- `downtimeTime` - (integer) time the service was in scheduled downtime, in seconds.

Examples

Retrieving availability information for an service

Retrieve availability information about a service during a week.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "service.getsla",
    "params": {
        "serviceids": "2",
        "intervals": [
            {
                "from": 1352452201,
                "to": 1353057001
            }
        ]
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "2": {
            "status": "3",
            "problems": {
```
"13904": {
  "triggerid": "13904",
  "expression": "\{13359\}=0",
  "description": "Service unavailable",
  "url": "",
  "status": "0",
  "value": "1",
  "priority": "3",
  "lastchange": "1352967420",
  "comments": "",
  "error": "",
  "templateid": "0",
  "type": "0",
  "value_flags": "0",
  "flags": "0"
},
"sla": [
  {
    "from": 1352452201,
    "to": 1353057001,
    "sla": 97.046296296296,
    "okTime": 586936,
    "problemTime": 17864,
    "downtimeTime": 0
  }
]
"id": 1

See also
  - Trigger

Source
CService::getSla() in frontends/php/include/classes/api/services/CService.php.

**service.update**

Description

object service.update(object/array services)

This method allows to update existing services.

Parameters

(object/array) service properties to be updated.

The serviceid property must be defined for each service, all other properties are optional. Only the passed properties will be updated, all others will remain unchanged.

Additionally to the standard service properties, the method accepts the following parameters.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dependencies</td>
<td>array</td>
<td>Service dependencies to replace the current service dependencies. Each service dependency has the following parameters: - dependsOnServiceid (string) ID of an service the service depends on, that is, the child service. - soft (integer) type of service dependency; refer to the service dependency object page for more information on dependency types.</td>
</tr>
<tr>
<td>parentid</td>
<td>string</td>
<td>ID of a hard-linked parent service.</td>
</tr>
<tr>
<td>times</td>
<td>array</td>
<td>Service times to replace the current service times.</td>
</tr>
</tbody>
</table>

Return values

(object) Returns an object containing the IDs of the updated services under the serviceids property.

Examples

Setting the parent of an service

Make service "3" the hard-linked parent of service "5".

Request:

```json
{
   "jsonrpc": "2.0",
   "method": "service.update",
   "params": {
      "serviceid": "5",
      "parentid": "3"
   },
   "auth": "038e1d7b1735c6a5436ee9eae095879e",
   "id": 1
}
```

Response:

```json
{
   "jsonrpc": "2.0",
   "result": {
      "serviceids": [
```

1081
See also

- service.adddependencies
- service.addtimes
- service.deletedependencies
- service.deletetimes

Source

CService::update() in frontends/php/include/classes/api/services/CService.php.

Task

This class is designed to work with tasks (such as checking items or low-level discovery rules without config reload).

Available methods:

- task.create - creating new tasks

**task.create**

Description

object task.create(object task)

This method allows to create a new task (such as checking items or low-level discovery rules without config reload).

Parameters

(object) A task to create.

The method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>type</strong></td>
<td>integer</td>
<td>Task type. Possible values: 6 - Check now.</td>
</tr>
<tr>
<td>(required)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>itemids</strong></td>
<td>string/array</td>
<td>IDs of items and low-level discovery rules.</td>
</tr>
<tr>
<td>(required)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note that tasks can be created for the following types of items/discovery rules:

- Zabbix agent
- SNMPv1/v2/v3 agent
- Simple check
- Internal check
- Aggregate check
- External check
- Database monitor
- HTTP agent
- IPMI agent
- SSH agent
- TELNET agent
- Calculated check
- JMX agent
Return values

*(object)* Returns an object containing the IDs of the created tasks under the *taskids* property. One task is created for each item and low-level discovery rule. The order of the returned IDs matches the order of the passed *itemids*.

Examples

Creating a task

Create a task check now for two items. One is an item, the other is a low-level discovery rule.

Request:

```json
{
   "jsonrpc": "2.0",
   "method": "task.create",
   "params": {
      "type": "6",
      "itemids": ["10092", "10093"]
   },
   "auth": "700ca65537074ec963db7efabda78259",
   "id": 1
}
```

Response:

```json
{
   "jsonrpc": "2.0",
   "result": {
      "taskids": ["1", "2"],
      "id": 1
   }
}
```

Source

CTask::create() in frontends/php/include/classes/api/services/CTask.php.

**Template**

This class is designed to work with templates.

Object references:

- **Template**

Available methods:

- template.create - creating new templates
- template.delete - deleting templates
- template.get - retrieving templates
- template.massadd - adding related objects to templates
- template.massremove - removing related objects from templates
- template.massupdate - replacing or removing related objects from templates
- template.update - updating templates

**Template object**

The following objects are directly related to the *template* API.

**Template**

The template object has the following properties.
<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>templateid</td>
<td>string</td>
<td>(readonly) ID of the template.</td>
</tr>
<tr>
<td>host</td>
<td>string</td>
<td>Technical name of the template.</td>
</tr>
<tr>
<td>description</td>
<td>text</td>
<td>Description of the template.</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>Visible name of the template.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: host property value.</td>
</tr>
</tbody>
</table>

Note that for some methods (update, delete) the required/optional parameter combination is different.

**template.create**

Description

object template.create(object/array templates)

This method allows to create new templates.

Parameters

(object/array) Templates to create.

Additionally to the standard template properties, the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>groups</td>
<td>object/array</td>
<td>Host groups to add the template to.</td>
</tr>
<tr>
<td>templates</td>
<td>object/array</td>
<td>Templates to be linked to the template.</td>
</tr>
<tr>
<td>macros</td>
<td>object/array</td>
<td>User macros to be created for the template.</td>
</tr>
<tr>
<td>hosts</td>
<td>object/array</td>
<td>Hosts to link the template to.</td>
</tr>
</tbody>
</table>

Return values

(object) Returns an object containing the IDs of the created templates under the templateIds property. The order of the returned IDs matches the order of the passed templates.

Examples

Creating a template
Create a template and link it to two hosts.

Request:

```
{
    "jsonrpc": "2.0",
    "method": "template.create",
    "params": {
        "host": "Linux template",
        "groups": {
            "groupid": 1
        },
        "hosts": [
            { "hostid": "10084" },
            { "hostid": "10090" }
        ],
        "auth": "038e1d7b1735c6a5436ee9eae095879e",
        "id": 1
    }
}
```

Response:

```
{
    "jsonrpc": "2.0",
    "result": {
        "templateids": [
            "10086"
        ],
        "id": 1
    }
}
```

Source

CTemplate::create() in frontends/php/include/classes/api/services/CTemplate.php.

**template.delete**

**Description**

object template.delete(array templateIds)

This method allows to delete templates.

**Note:**

Deleting a template will cause deletion of all template entities (items, triggers, graphs, etc.). To leave template entities with the hosts, but delete the template itself, first unlink the template from required hosts using one of these methods: template.update, template.massupdate, host.update, host.massupdate.

**Parameters**

(array) IDs of the templates to delete.

**Return values**

(object) Returns an object containing the IDs of the deleted templates under the templateids property.

**Examples**

Deleting multiple templates

Delete two templates.

Request:
Source

CTemplate::delete() in frontends/php/include/classes/api/services/CTemplate.php.

**template.get**

**Description**

integer/array template.get(object parameters)

The method allows to retrieve templates according to the given parameters.

**Parameters**

(object) Parameters defining the desired output.

The method supports the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>templateids</td>
<td>string/array</td>
<td>Return only templates with the given template IDs.</td>
</tr>
<tr>
<td>groupids</td>
<td>string/array</td>
<td>Return only templates that belong to the given host groups.</td>
</tr>
<tr>
<td>parentTemplateids</td>
<td>string/array</td>
<td>Return only templates that are parent to the given templates.</td>
</tr>
<tr>
<td>hostids</td>
<td>string/array</td>
<td>Return only templates that are linked to the given hosts/templates.</td>
</tr>
<tr>
<td>graphids</td>
<td>string/array</td>
<td>Return only templates that contain the given graphs.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>itemids</td>
<td>string/array</td>
<td>Return only templates that contain the given items.</td>
</tr>
<tr>
<td>triggerids</td>
<td>string/array</td>
<td>Return only templates that contain the given triggers.</td>
</tr>
<tr>
<td>with_items</td>
<td>flag</td>
<td>Return only templates that have items.</td>
</tr>
<tr>
<td>with_triggers</td>
<td>flag</td>
<td>Return only templates that have triggers.</td>
</tr>
<tr>
<td>with_graphs</td>
<td>flag</td>
<td>Return only templates that have graphs.</td>
</tr>
<tr>
<td>with_http_tests</td>
<td>flag</td>
<td>Return only templates that have web scenarios.</td>
</tr>
<tr>
<td>selectGroups</td>
<td>query</td>
<td>Return the host groups that the template belongs to in the groups property.</td>
</tr>
<tr>
<td>selectHosts</td>
<td>query</td>
<td>Return the hosts that are linked to the template in the hosts property.</td>
</tr>
<tr>
<td>selectTemplates</td>
<td>query</td>
<td>Return templates to which the template is a child, in the templates property.</td>
</tr>
<tr>
<td>selectParentTemplates</td>
<td>query</td>
<td>Return templates to which the template is a parent, in the parentTemplates property.</td>
</tr>
<tr>
<td>selectHttpTests</td>
<td>query</td>
<td>Return the web scenarios from the template in the httpTests property.</td>
</tr>
<tr>
<td>selectItems</td>
<td>query</td>
<td>Return items from the template in the items property.</td>
</tr>
</tbody>
</table>

Supports count.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>selectDiscoveries</td>
<td>query</td>
<td>Return low-level discoveries from the template in the <code>discoveries</code> property.</td>
</tr>
<tr>
<td>selectTriggers</td>
<td>query</td>
<td>Return triggers from the template in the <code>triggers</code> property. Supports count.</td>
</tr>
<tr>
<td>selectGraphs</td>
<td>query</td>
<td>Return graphs from the template in the <code>graphs</code> property. Supports count.</td>
</tr>
<tr>
<td>selectApplications</td>
<td>query</td>
<td>Return applications from the template in the <code>applications</code> property. Supports count.</td>
</tr>
<tr>
<td>selectMacros</td>
<td>query</td>
<td>Return the macros from the template in the <code>macros</code> property. Supports count.</td>
</tr>
<tr>
<td>selectScreens</td>
<td>query</td>
<td>Return screens from the template in the <code>screens</code> property. Supports count.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>limitSelects</td>
<td>integer</td>
<td>Limits the number of records returned by subselects.</td>
</tr>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Applies to the following subselects:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- selectTemplates: results will be sorted by name;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- selectHosts: sorted by host;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- selectParentTemplates: sorted by host;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- selectItems: sorted by name;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- selectDiscoveries: sorted by name;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- selectTriggers: sorted by description;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- selectGraphs: sorted by name;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- selectApplications: sorted by name;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- selectScreens: sorted by name.</td>
</tr>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Sort the result by the given properties.</td>
</tr>
<tr>
<td>countOutput</td>
<td>boolean</td>
<td>Possible values are: hostid, host, name, status.</td>
</tr>
<tr>
<td>editable</td>
<td>boolean</td>
<td>These parameters being common for all get methods are described in detail in the reference commentary.</td>
</tr>
<tr>
<td>excludeSearch</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>filter</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>limit</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>output</td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>preservekeys</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>search</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>searchByAny</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>searchWildcardsEnabled</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>sortorder</td>
<td>string/array</td>
<td></td>
</tr>
<tr>
<td>startSearch</td>
<td>boolean</td>
<td></td>
</tr>
</tbody>
</table>

Return values

(integer/array) Returns either:

- an array of objects;
- the count of retrieved objects, if the countOutput parameter has been used.
Examples

Retrieving templates by name

Retrieve all data about two templates named “Template OS Linux” and “Template OS Windows”.

Request:

```
{
   "jsonrpc": "2.0",
   "method": "template.get",
   "params": {
      "output": "extend",
      "filter": {
         "host": [
            "Template OS Linux",
            "Template OS Windows"
         ]
      }
   },
   "auth": "038e1d7b1735c6a5436ee9eae095879e",
   "id": 1
}
```

Response:

```
{
   "jsonrpc": "2.0",
   "result": [
      {
         "proxy_hostid": "0",
         "host": "Template OS Linux",
         "status": "3",
         "disable_until": "0",
         "error": "",
         "available": "0",
         "errors_from": "0",
         "lastaccess": "0",
         "ipmi_authtype": "0",
         "ipmi_privilege": "2",
         "ipmi_username": "",
         "ipmi_password": "",
         "ipmi_disable_until": "0",
         "ipmi_available": "0",
         "snmp_disable_until": "0",
         "snmp_available": "0",
         "maintenanceid": "0",
         "maintenance_status": "0",
         "maintenance_type": "0",
         "maintenance_from": "0",
         "ipmi_errors_from": "0",
         "snmp_errors_from": "0",
         "ipmi_error": "",
         "snmp_error": "",
         "jmx_disable_until": "0",
         "jmx_available": "0",
         "jmx_errors_from": "0",
         "jmx_error": "",
         "name": "Template OS Linux",
         "flags": "0",
         "templateid": "10001",
         "description": "",
         "tls_connect": "1",
         "tls_accept": "1",
         "tls_issuer": "",
         "tls_subject": "",
         "templateid": "10001",
      }
   ]
}
```
"tls_psk_identity": "", "tls_psk": "",
},
{
    "proxy_hostid": "0",
    "host": "Template OS Windows",
    "status": "3",
    "disable_until": "0",
    "error": "",
    "available": "0",
    "errors_from": "0",
    "lastaccess": "0",
    "ipmi_authtype": "0",
    "ipmi_privilege": "2",
    "ipmi_username": "",
    "ipmi_password": "",
    "ipmi_disable_until": "0",
    "ipmi_available": "0",
    "snmp_disable_until": "0",
    "snmp_available": "0",
    "maintenanceid": "0",
    "maintenance_status": "0",
    "maintenance_type": "0",
    "maintenance_from": "0",
    "ipmi_errors_from": "0",
    "snmp_errors_from": "0",
    "ipmi_error": "",
    "snmp_error": "",
    "jmx_disable_until": "0",
    "jmx_available": "0",
    "jmx_errors_from": "0",
    "jmx_error": "",
    "name": "Template OS Windows",
    "flags": "0",
    "templateid": "10081",
    "description": "",
    "tls_connect": "1",
    "tls_accept": "1",
    "tls_issuer": "",
    "tls_subject": "",
    "tls_psk_identity": "",
    "tls_psk": ""
}
]
"id": 1
}

See also

- Host group
- Template
- User macro
- Host interface

Source

CTemplate::get() in frontends/php/include/classes/api/services/CTemplate.php.

template.massadd

Description

object template.massadd(object parameters)

This method allows to simultaneously add multiple related objects to the given templates.
Parameters

(object) Parameters containing the IDs of the templates to update and the objects to add to the templates.

The method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>templates</td>
<td>object/array</td>
<td>Templates to be updated. The templates must have the templateid property defined.</td>
</tr>
<tr>
<td>groups</td>
<td>object/array</td>
<td>Host groups to add the given templates to. The host groups must have the groupid property defined.</td>
</tr>
<tr>
<td>hosts</td>
<td>object/array</td>
<td>Hosts and templates to link the given templates to. The hosts must have the hostid property defined.</td>
</tr>
<tr>
<td>macros</td>
<td>object/array</td>
<td>User macros to be created for the given templates.</td>
</tr>
<tr>
<td>templates_link</td>
<td>object/array</td>
<td>Templates to link to the given templates. The templates must have the templateid property defined.</td>
</tr>
</tbody>
</table>

Return values

(object) Returns an object containing the IDs of the updated templates under the templateids property.

Examples

Adding templates to a group

Add two templates to the host group "2".

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "template.massadd",
    "params": {
        "templates": [
            {
                "templateid": "10085"
            },
            {
                "templateid": "10086"
            }
        ]
    }
}
```
"groups": [  
  {  
    "groupid": "2"
  }
],  
"auth": "038e1d7b1735c6a5436ee9eae095879e",
"id": 1
}

Response:
{
  "jsonrpc": "2.0",
  "result": {
    "templateids": [
      "10085",
      "10086"
    ]
  },
  "id": 1
}

Linking a template to hosts

Link template "10073" to two hosts.

Request:
{
  "jsonrpc": "2.0",
  "method": "template.massadd",
  "params": {
    "templates": [
      {
        "templateid": "10073"
      }
    ],
    "hosts": [
      {
        "hostid": "10106"
      },
      {
        "hostid": "10104"
      }
    ]
  },
  "auth": "038e1d7b1735c6a5436ee9eae095879e",
  "id": 1
}

Response:
{
  "jsonrpc": "2.0",
  "result": {
    "templateids": ["10073"
  ]
  },
  "id": 1
}

See also
  • template.update
  • Host
Source
CTemplate::massAdd() in frontends/php/include/classes/api/services/CTemplate.php.

**template.massremove**

**Description**

```plaintext
object template.massremove(object parameters)
```

This method allows to remove related objects from multiple templates.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>templateids</strong></td>
<td>string/array</td>
<td>IDs of the templates to be updated.</td>
</tr>
<tr>
<td>(required)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>groupids</td>
<td>string/array</td>
<td>Host groups to remove the given templates from.</td>
</tr>
<tr>
<td>hostids</td>
<td>string/array</td>
<td>Hosts or templates to unlink the given templates from (downstream).</td>
</tr>
<tr>
<td>macros</td>
<td>string/array</td>
<td>User macros to delete from the given templates.</td>
</tr>
<tr>
<td>templateids_clear</td>
<td>string/array</td>
<td>Templates to unlink and clear from the given templates (upstream).</td>
</tr>
<tr>
<td>templateids_link</td>
<td>string/array</td>
<td>Templates to unlink from the given templates (upstream).</td>
</tr>
</tbody>
</table>

**Return values**

```plaintext
(object) Returns an object containing the IDs of the updated templates under the templateids property.
```

**Examples**

Removing templates from a group

Remove two templates from group "2".

**Request:**

```json
{
    "jsonrpc": "2.0",
    "method": "template.massremove",
    "params": {
        "templateids": [
            "10085",
            "10086"
        ],
        "groupids": "2"
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e"
}
```

1094
Unlinking templates from a host

Unlink template "10085" from two hosts.

Request:

```json
{
   "jsonrpc": "2.0",
   "method": "template.massremove",
   "params": {
      "templateids": "10085",
      "hostids": ["10106", "10104"]
   },
   "auth": "038e1d7b1735c6a5436ee9eae095879e",
   "id": 1
}
```

Response:

```json
{
   "jsonrpc": "2.0",
   "result": {
      "templateids": ["10085"]
   },
   "id": 1
}
```

See also

- template.update
- User macro

Source

CTemplate::massRemove() in frontends/php/include/classes/api/services/CTemplate.php.

**template.massupdate**

Description

object template.massupdate(object parameters)

This method allows to simultaneously replace or remove related objects and update properties on multiple templates.

Parameters

(object) Parameters containing the IDs of the templates to update and the properties that should be updated.

Additionally to the standard template properties, the method accepts the following parameters.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>templates</strong></td>
<td>object/array</td>
<td>Templates to be updated. The templates must have the <strong>templateid</strong> property defined.</td>
</tr>
<tr>
<td>(required)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>groups</strong></td>
<td>object/array</td>
<td>Host groups to replace the current host groups the templates belong to.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>hosts</strong></td>
<td>object/array</td>
<td>Hosts and templates to replace the ones the templates are currently linked to.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>macros</strong></td>
<td>object/array</td>
<td>User macros to replace the current user macros on the given templates.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>templates_clear</strong></td>
<td>object/array</td>
<td>Templates to unlink and clear from the given templates.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>templates_link</strong></td>
<td>object/array</td>
<td>Templates to replace the currently linked templates.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Return values**

*(object)* Returns an object containing the IDs of the updated templates under the **templateids** property.

**Examples**

Replacing host groups

Unlink and clear template “10091” from the given templates.
Request:

```json
{
  "jsonrpc": "2.0",
  "method": "template.massupdate",
  "params": {
    "templates": [
      {
        "templateid": "10085"
      },
      {
        "templateid": "10086"
      }
    ],
    "templates_clear": [
      {
        "templateid": "10091"
      }
    ]
  },
  "auth": "038e1d7b1735c6a5436ee9eae096879e",
  "id": 1
}
}
```

Response:

```json
{
  "jsonrpc": "2.0",
  "result": {
    "templateids": [
      "10085",
      "10086"
    ]
  },
  "id": 1
}
}
```

See also

- `template.update`
- `template.massadd`
- `Host group`
- `User macro`

Source

CTemplate::massUpdate() in frontends/php/include/classes/api/services/CTemplate.php.

**template.update**

Description

object template.update(object/array templates)

This method allows to update existing templates.

Parameters

(object/array) Template properties to be updated.

The `templateid` property must be defined for each template, all other properties are optional. Only the given properties will be updated, all others will remain unchanged.

Additionally to the standard template properties, the method accepts the following parameters.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>groups</td>
<td>object/array</td>
<td>Host groups to replace the current host groups the templates belong to. The host groups must have the groupid property defined.</td>
</tr>
<tr>
<td>hosts</td>
<td>object/array</td>
<td>Hosts and templates to replace the ones the templates are currently linked to. Both hosts and templates must use the hostid property to pass an ID.</td>
</tr>
<tr>
<td>macros</td>
<td>object/array</td>
<td>User macros to replace the current user macros on the given templates.</td>
</tr>
<tr>
<td>templates</td>
<td>object/array</td>
<td>Templates to replace the currently linked templates. Templates that are not passed are only unlinked. The templates must have the templateid property defined.</td>
</tr>
<tr>
<td>templates_clear</td>
<td>object/array</td>
<td>Templates to unlink and clear from the given templates. The templates must have the templateid property defined.</td>
</tr>
</tbody>
</table>

Return values
(object) Returns an object containing the IDs of the updated templates under the templateids property.

Examples
Renaming a template

Rename the template to “Template OS Linux”.

Request:
```json
{
    "jsonrpc": "2.0",
    "method": "template.update",
    "params": {
        "templateid": "10086",
        "name": "Template OS Linux"
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "templateids": ["10086"
    ],
    "id": 1
}
```

Source

CTemplate::update() in frontends/php/include/classes/api/services/CTemplate.php.

**Template screen**

This class is designed to work with template screens.

Object references:

- **Template screen**

Available methods:

- templatescreen.copy - copy template screens
- templatescreen.create - create new template screens
- templatescreen.delete - delete template screens
- templatescreen.get - retrieve template screens
- templatescreen.update - update template screens

> **Template screen object**

The following objects are directly related to the templatescreen API.

**Template screen**

The template screen object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>screenid</td>
<td>string</td>
<td>(readonly) ID of the template screen.</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>Name of the template screen.</td>
</tr>
<tr>
<td>templateid</td>
<td>string</td>
<td>ID of the template that the screen belongs to.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>---------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>hsize</td>
<td>integer</td>
<td>Width of the template screen.</td>
</tr>
<tr>
<td>vsize</td>
<td>integer</td>
<td>Height of the template screen.</td>
</tr>
</tbody>
</table>

**templatescreen.copy**

Description

```object templatescreen.copy(object parameters)```

This method allows to copy template screens to the given templates.

Parameters

```(object) Parameters defining the template screens to copy and the target templates.```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>screenIds</td>
<td>string/array</td>
<td>IDs of template screens to copy.</td>
</tr>
<tr>
<td>(required)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>templateIds</td>
<td>string/array</td>
<td>IDs of templates to copy the screens to.</td>
</tr>
<tr>
<td>(required)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Return values

```(boolean) Returns true if the copying was successful.```

Examples

Copy a template screen

Copy template screen "25" to template "30085".

Request:

```json
{
   "jsonrpc": "2.0",
   "method": "templatescreen.copy",
   "params": {
      "screenIds": "25",
      "templateIds": "30085"
   },
   "auth": "038e1d7b1735c6a5436ee9eae095879e",
   "id": 1
}
```

Response:

```json
{
   "jsonrpc": "2.0",
   "result": true,
   "id": 1
}
```

Source

CTemplateScreen::copy() in frontends/php/include/classes/api/services/CTemplateScreen.php.
**templatescreen.create**

Description

object templatescreen.create(object/array templateScreens)

This method allows to create new template screens.

Parameters

(object/array) Template screens to create.

Additionally to the standard template screen properties, the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>screenitems</td>
<td>array</td>
<td>Template screen items to create on the screen.</td>
</tr>
</tbody>
</table>

Return values

(object) Returns an object containing the IDs of the created template screens under the screenids property. The order of the returned IDs matches the order of the passed template screens.

Examples

Create a template screen

Create a template screen named “Graphs” with 2 rows and 3 columns and add a graph to the upper-left cell.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "templatescreen.create",
    "params": {
        "name": "Graphs",
        "templateid": "10047",
        "hsize": 3,
        "vsize": 2,
        "screenitems": [
            {
                "resourceid": "410",
                "x": 0,
                "y": 0
            }
        ]
    },
    "auth": "038e1d7b1735c6a5436ee9eaee095879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "screenids": [
            "45"
        ]
    },
    "id": 1
}
```

See also

- Template screen item

Source

CTemplateScreen::create() in frontends/php/include/classes/api/services/CTemplateScreen.php.
templatescreen.delete

Description

object templatescreen.delete(array templateScreenIds)

This method allows to delete template screens.

Parameters

(array) IDs of the template screens to delete.

Return values

(object) Returns an object containing the IDs of the deleted template screens under the screenids property.

Examples

Delete multiple template screens

Delete two template screens.

Request:

```json
{
   "jsonrpc": "2.0",
   "method": "templatescreen.delete",
   "params": [
      "45",
      "46"
   ],
   "auth": "3a57200802b24cda67c4e4010b50c065",
   "id": 1
}
```

Response:

```json
{
   "jsonrpc": "2.0",
   "result": {
      "screenids": [
         "45",
         "46"
      ]
   },
   "id": 1
}
```

Source

CTemplateScreen::delete() in frontends/php/include/classes/api/services/CTemplateScreen.php.

templatescreen.get

Description

integer/array templatescreen.get(object parameters)

The method allows to retrieve template screens according to the given parameters.

Parameters

(object) Parameters defining the desired output.

The method supports the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostids</td>
<td>string/array</td>
<td>Return only template screens that belong to the given hosts.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>screenids</td>
<td>string/array</td>
<td>Return only template screens with the given IDs.</td>
</tr>
<tr>
<td>screenitemids</td>
<td>string/array</td>
<td>Return only template screens that contain the given screen items.</td>
</tr>
<tr>
<td>templateids</td>
<td>string/array</td>
<td>Return only template screens that belong to the given templates.</td>
</tr>
<tr>
<td>noInheritance</td>
<td>flag</td>
<td>Do not return inherited template screens.</td>
</tr>
<tr>
<td>selectScreenItemsquery</td>
<td></td>
<td>Return the screen items that are used in the template screen in the screenitems property.</td>
</tr>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Sort the result by the given properties.</td>
</tr>
<tr>
<td>countOutput</td>
<td>boolean</td>
<td>These parameters being common for all get methods are described in detail in the reference commentary.</td>
</tr>
<tr>
<td>editable</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>excludeSearch</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>filter</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>limit</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>output</td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>preservekeys</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>search</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>searchByAny</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>searchWildcardsEnabled</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>sortOrder</td>
<td>string/array</td>
<td></td>
</tr>
<tr>
<td>startSearch</td>
<td>boolean</td>
<td></td>
</tr>
</tbody>
</table>

Return values

(integer/array) Returns either:

- an array of objects;
- the count of retrieved objects, if the countOutput parameter has been used.

Examples

Retrieve screens from template

Retrieve all screens from template “10001” and all of the screen items.

Request:
{
"jsonrpc": "2.0",
"method": "templatescreen.get",
"params": {
"output": "extend",
"selectScreenItems": "extend",
"templateids": "10001"
},
"auth": "038e1d7b1735c6a5436ee9eae095879e",
"id": 1
}
Response:

{
"jsonrpc": "2.0",
"result": [
{
"screenid": "3",
"name": "System performance",
"hsize": "2",
"vsize": "2",
"templateid": "10001",
"screenitems": [
{
"screenitemid": "20",
"screenid": "3",
"resourcetype": "0",
"resourceid": "433",
"width": "500",
"height": "120",
"x": "0",
"y": "0",
"colspan": "1",
"rowspan": "1",
"elements": "0",
"valign": "1",
"halign": "0",
"style": "0",
"url": ""
},
{
"screenitemid": "21",
"screenid": "3",
"resourcetype": "0",
"resourceid": "387",
"width": "500",
"height": "100",
"x": "0",
"y": "1",
"colspan": "1",
"rowspan": "1",
"elements": "0",
"valign": "1",
"halign": "0",
"style": "0",
"url": ""
},
{
"screenitemid": "22",
"screenid": "3",
"resourcetype": "1",
"resourceid": "10013",

1104


See also

- Template screen item

Source

CTemplateScreen::get() in frontends/php/include/classes/api/services/CTemplateScreen.php.

**templatescreen.update**

Description

object templatescreen.update(object/array templateScreens)

This method allows to update existing template screens.

Parameters

(object/array) Template screen properties to be updated.

The screenid property must be defined for each template screen, all other properties are optional. Only the passed properties will be updated, all others will remain unchanged.

Additionally to the standard template screen properties, the method accepts the following parameters.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>screenitems</td>
<td>array</td>
<td>Screen items to replace existing screen items. Screen items are updated by coordinates, so each screen item must have the x and y properties defined.</td>
</tr>
</tbody>
</table>

Return values

(object) Returns an object containing the IDs of the updated template screens under the screenids property.

Examples

Rename a template screen

Rename the template screen to "Performance graphs".

Request:

```
{
    "jsonrpc": "2.0",
    "method": "templatescreen.update",
    "params": {
        "screenid": "3",
        "name": "Performance graphs"
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```
{
    "jsonrpc": "2.0",
    "result": {
        "screenids": [
            "3"
        ],
        "id": 1
    }
}
```

Source

CTemplateScreen::update() in frontends/php/include/classes/api/services/CTemplateScreen.php.

**Template screen item**

This class is designed to work with template screen items.

Object references:

- Template screen item

Available methods:

- templatescreenitem.get - retrieve template screen items
Template screen item

The following objects are directly related to the templatescreenitem API.

The template screen item object defines an element displayed on a template screen. It has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>screenitemid</td>
<td>string</td>
<td>(readonly) ID of the template screen item.</td>
</tr>
</tbody>
</table>
| resourceid    | string | ID of the object from the parent template displayed on the template screen item. Depending on the type of screen item, the resourceid property can reference different objects. Unused by clock and URL template screen items. Note: the resourceid property always references an object used in the parent template object, even if the screen item itself is inherited on a host or template. Type of template screen item. Possible values:
  0 - graph;
  1 - simple graph;
  3 - plain text;
  7 - clock;
  11 - URL;
  19 - simple graph prototype;
  20 - graph prototype. ID of the template screen that the item belongs to. Number of columns the template screen item will span across. Default: 1. |
<p>| resourcetype  | integer| (required)                                                                  |
| screenid      | string | (required)                                                                  |
| colspan       | integer| (required)                                                                  |</p>
<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>elements</td>
<td>integer</td>
<td>Number of lines to display on the template screen item. Default: 25.</td>
</tr>
<tr>
<td>halign</td>
<td>integer</td>
<td>Specifies how the template screen item must be aligned horizontally in the cell. Possible values: 0 - (default) center; 1 - left; 2 - right.</td>
</tr>
<tr>
<td>height</td>
<td>integer</td>
<td>Height of the template screen item in pixels. Default: 200.</td>
</tr>
<tr>
<td>max_columns</td>
<td>integer</td>
<td>Specifies the maximum amount of columns a graph prototype or simple graph prototype screen element can have. Default: 3.</td>
</tr>
<tr>
<td>rowspan</td>
<td>integer</td>
<td>Number or rows the template screen item will span across. Default: 1.</td>
</tr>
<tr>
<td>style</td>
<td>integer</td>
<td>Template screen item display option. Possible values for clock screen items: 0 - (default) local time; 1 - server time; 2 - host time. Possible values for plain text screen items: 0 - (default) display values as plain text; 1 - display values as HTML.</td>
</tr>
</tbody>
</table>
### Property | Type | Description
--- | --- | ---
url | string | URL of the webpage to be displayed in the template screen item. Used by URL template screen items.

**valign** | integer | Specifies how the template screen item must be aligned vertically in the cell. Possible values: 0 - (default) middle; 1 - top; 2 - bottom.

**width** | integer | Width of the template screen item in pixels. Default: 320.

**x** | integer | X-coordinates of the template screen item on the screen, from left to right. Default: 0.

**y** | integer | Y-coordinates of the template screen item on the screen, from top to bottom. Default: 0.

---

#### templatescreenitem.get

**Description**

integer/array templatescreenitem.get(object parameters)

The method allows to retrieve template screen items according to the given parameters.

**Parameters**

(object) Parameters defining the desired output.

The method supports the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>screenids</td>
<td>string/array</td>
<td>Return only template screen items that belong to the given template screens.</td>
</tr>
</tbody>
</table>

<p>| screenitemids | string/array | Return only template screen items with the given IDs. |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostids</td>
<td>string/array</td>
<td>Returns an additional <strong>real_resourceid</strong> property for each template screen item, that belongs to a screen from the given hosts or templates. The <strong>real_resourceid</strong> property contains the ID of object displayed on the screen.</td>
</tr>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Sort the result by the given properties. Possible values are: <strong>screenitemid</strong> and <strong>screenid</strong>.</td>
</tr>
<tr>
<td>countOutput</td>
<td>boolean</td>
<td>These parameters being common for all get methods are described in detail in the reference commentary.</td>
</tr>
<tr>
<td>editable</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>excludeSearch</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>filter</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>limit</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>output</td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>preservekeys</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>search</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>searchByAny</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>searchWildcardsEnabled</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>sortorder</td>
<td>string/array</td>
<td></td>
</tr>
<tr>
<td>startSearch</td>
<td>boolean</td>
<td></td>
</tr>
</tbody>
</table>

**Return values**

(integer/array) Returns either:

- an array of objects;
- the count of retrieved objects, if the `countOutput` parameter has been used.

**Examples**

Retrieve template screen items for screen

Return all template screen items from template screen "15".

**Request:**

```json
{
    "jsonrpc": "2.0",
    "method": "templatescreenitem.get",
    "params": {
        "output": "extend",
        "screenids": "15"
    }
}
```
"auth": "038e1d7b1735c6a5436ee9eae095879e",
"id": 1
}

Response:
{
  "jsonrpc": "2.0",
  "result": [
    {
      "screenitemid": "42",
      "screenid": "15",
      "resourcetype": "0",
      "resourceid": "454",
      "width": "500",
      "height": "200",
      "x": "0",
      "y": "0",
      "colspan": "1",
      "rowspan": "1",
      "elements": "0",
      "valign": "1",
      "halign": "0",
      "style": "0",
      "url": "",
      "max_columns": "3"
    },
    {
      "screenitemid": "43",
      "screenid": "15",
      "resourcetype": "0",
      "resourceid": "455",
      "width": "500",
      "height": "270",
      "x": "1",
      "y": "0",
      "colspan": "1",
      "rowspan": "1",
      "elements": "0",
      "valign": "1",
      "halign": "0",
      "style": "0",
      "url": "",
      "max_columns": "3"
    }
  ],
  "id": 1
}

Source
CTemplateScreenItem::get() in frontends/php/include/classes/api/services/CTemplateScreenItem.php.

**Trend**

This class is designed to work with trend data.

Object references:

- Trend

Available methods:

- trend.get - retrieving trends
> **Trend object**

The following objects are directly related to the trend API.

**Note:**
Trend objects differ depending on the item’s type of information. They are created by the Zabbix server and cannot be modified via the API.

Float trend

The float trend object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clock</td>
<td>timestamp</td>
<td>Time when that value was received.</td>
</tr>
<tr>
<td>itemid</td>
<td>string</td>
<td>ID of the related item.</td>
</tr>
<tr>
<td>num</td>
<td>integer</td>
<td>Number of values within this hour.</td>
</tr>
<tr>
<td>value_min</td>
<td>float</td>
<td>Hourly minimum value.</td>
</tr>
<tr>
<td>value_avg</td>
<td>float</td>
<td>Hourly average value.</td>
</tr>
<tr>
<td>value_max</td>
<td>float</td>
<td>Hourly maximum value.</td>
</tr>
</tbody>
</table>

Integer trend

The integer trend object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clock</td>
<td>timestamp</td>
<td>Time when that value was received.</td>
</tr>
<tr>
<td>itemid</td>
<td>string</td>
<td>ID of the related item.</td>
</tr>
<tr>
<td>num</td>
<td>integer</td>
<td>Number of values within this hour.</td>
</tr>
<tr>
<td>value_min</td>
<td>integer</td>
<td>Hourly minimum value.</td>
</tr>
<tr>
<td>value_avg</td>
<td>integer</td>
<td>Hourly average value.</td>
</tr>
<tr>
<td>value_max</td>
<td>integer</td>
<td>Hourly maximum value.</td>
</tr>
</tbody>
</table>

**trend.get**

**Description**

integer/array trend.get(object parameters)

The method allows to retrieve trend data according to the given parameters.

**Parameters**

(object) Parameters defining the desired output.

The method supports the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>itemids</td>
<td>string/array</td>
<td>Return only trends with the given item IDs.</td>
</tr>
<tr>
<td>time_from</td>
<td>timestamp</td>
<td>Return only values that have been collected after or at the given time.</td>
</tr>
<tr>
<td>time_till</td>
<td>timestamp</td>
<td>Return only values that have been collected before or at the given time.</td>
</tr>
</tbody>
</table>
Parameter | Type | Description
--- | --- | ---
countOutput | boolean | Count the number of retrieved objects.
limit | integer | Limit the amount of retrieved objects.
output | query | Set fields to output.

Return values
(integer/array) Returns either:

- an array of objects;
- the count of retrieved objects, if the countOutput parameter has been used.

Examples

Retrieving item trend data

Request:

```json
{
   "jsonrpc": "2.0",
   "method": "trend.get",
   "params": {
      "output": [
         "itemid",
         "clock",
         "num",
         "value_min",
         "value_avg",
         "value_max",
      ],
      "itemids": [
         "23715"
      ],
      "limit": "1"
   },
   "auth": "038e1d7b1735c6a5436ee9eae095879e",
   "id": 1
}
```

Response:

```json
{
   "jsonrpc": "2.0",
   "result": [
      {
         "itemid": "23715",
         "clock": "1446199200",
         "num": "60",
         "value_min": "0.1650",
         "value_avg": "0.2168",
         "value_max": "0.3500",
      }
   ],
   "id": 1
}
```

Source

CTrend::get() in frontends/php/include/classes/api/services/CTrend.php.
Trigger

This class is designed to work with triggers.

Object references:

- Trigger

Available methods:

- `trigger.adddependencies` - adding new trigger dependencies
- `trigger.create` - creating new triggers
- `trigger.delete` - deleting triggers
- `trigger.deletedependencies` - deleting trigger dependencies
- `trigger.get` - retrieving triggers
- `trigger.update` - updating triggers

> Trigger object

The following objects are directly related to the trigger API.

Trigger

The trigger object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>triggerid</code></td>
<td>string</td>
<td>(readonly) ID of the trigger.</td>
</tr>
<tr>
<td><code>description</code></td>
<td>string</td>
<td>Name of the trigger.</td>
</tr>
<tr>
<td><code>expression</code></td>
<td>string</td>
<td>Reduced trigger expression.</td>
</tr>
<tr>
<td><code>comments</code></td>
<td>string</td>
<td>Additional description of the trigger.</td>
</tr>
<tr>
<td><code>error</code></td>
<td>string</td>
<td>(readonly) Error text if there have been any problems when updating the state of the trigger.</td>
</tr>
<tr>
<td><code>flags</code></td>
<td>integer</td>
<td>(readonly) Origin of the trigger. Possible values are:</td>
</tr>
<tr>
<td><code>lastchange</code></td>
<td>timestamp</td>
<td>Time when the trigger last changed its state.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>priority</td>
<td>integer</td>
<td>Severity of the trigger. Possible values are: 0 - (default) not classified; 1 - information; 2 - warning; 3 - average; 4 - high; 5 - disaster.</td>
</tr>
<tr>
<td>state</td>
<td>integer</td>
<td>(readonly) State of the trigger. Possible values: 0 - (default) trigger state is up to date; 1 - current trigger state is unknown.</td>
</tr>
<tr>
<td>status</td>
<td>integer</td>
<td>Whether the trigger is enabled or disabled. Possible values are: 0 - (default) enabled; 1 - disabled.</td>
</tr>
<tr>
<td>templateid</td>
<td>string</td>
<td>(readonly) ID of the parent template trigger.</td>
</tr>
<tr>
<td>type</td>
<td>integer</td>
<td>Whether the trigger can generate multiple problem events. Possible values are: 0 - (default) do not generate multiple events; 1 - generate multiple events.</td>
</tr>
<tr>
<td>url</td>
<td>string</td>
<td>URL associated with the trigger. (readonly)</td>
</tr>
<tr>
<td>value</td>
<td>integer</td>
<td>Whether the trigger is in OK or problem state. Possible values are: 0 - (default) OK; 1 - problem.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>recovery_mode</td>
<td>integer</td>
<td>OK event generation mode. Possible values are: 0 - (default) Expression; 1 - Recovery expression; 2 - None. Reduced trigger recovery expression.</td>
</tr>
<tr>
<td>recovery_expression</td>
<td>string</td>
<td>OK event closes. Possible values are: 0 - (default) All problems; 1 - All problems if tag values match. Tag for matching.</td>
</tr>
<tr>
<td>correlation_mode</td>
<td>integer</td>
<td>OK event closes. Possible values are: 0 - (default) No; 1 - Yes.</td>
</tr>
<tr>
<td>correlation_tag</td>
<td>string</td>
<td>Tag for matching.</td>
</tr>
<tr>
<td>manual_close</td>
<td>integer</td>
<td>Allow manual close. Possible values are: 0 - (default) No; 1 - Yes.</td>
</tr>
</tbody>
</table>

Note that for some methods (update, delete) the required/optional parameter combination is different.

**Trigger tag**

The trigger tag object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tag</td>
<td>string</td>
<td>(required) Trigger tag name.</td>
</tr>
<tr>
<td>value</td>
<td>string</td>
<td>Trigger tag value.</td>
</tr>
</tbody>
</table>

**trigger.adddependencies**

**Description**

object trigger.adddependencies(object/array triggerDependencies)

This method allows to create new trigger dependencies.

**Parameters**

(object/array) Trigger dependencies to create.

Each trigger dependency has the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>triggerid</td>
<td>string</td>
<td>(required) ID of the dependent trigger.</td>
</tr>
</tbody>
</table>
### Parameter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dependsOnTriggerid</code></td>
<td>string</td>
<td>ID of the trigger that the trigger depends on.</td>
</tr>
</tbody>
</table>

**Return values**

*(object)* Returns an object containing the IDs of the dependent triggers under the `triggerids` property.

**Examples**

**Add a trigger dependency**

Make trigger "14092" dependent on trigger "13565."

**Request:**

```json
{
  "jsonrpc": "2.0",
  "method": "trigger.adddependencies",
  "params": {
    "triggerid": "14092",
    "dependsOnTriggerid": "13565"
  },
  "auth": "038e1d7b1735c6a5436ee9eae095879e",
  "id": 1
}
```

**Response:**

```json
{
  "jsonrpc": "2.0",
  "result": {
    "triggerids": [{
      "14092"
    }],
  },
  "id": 1
}
```

**See also**

- `trigger.update`
- `Trigger dependencies`

**Source**

`CTrigger::addDependencies()` in `frontends/php/include/classes/api/services/CTrigger.php`.

### trigger.create

**Description**

`object trigger.create(object/array triggers)`

This method allows to create new triggers.

**Parameters**

*(object/array)* Triggers to create.

Additionally to the *standard trigger properties* the method accepts the following parameters.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dependencies</td>
<td>array</td>
<td>Triggers that the trigger is dependent on. The triggers must have the triggerid property defined.</td>
</tr>
<tr>
<td>tags</td>
<td>array</td>
<td>Trigger tags.</td>
</tr>
</tbody>
</table>

**Attention:**
The trigger expression has to be given in its expanded form.

**Return values**

(object) Returns an object containing the IDs of the created triggers under the triggerids property. The order of the returned IDs matches the order of the passed triggers.

**Examples**

**Creating a trigger**

Create a trigger with a single trigger dependency.

**Request:**

```json
{
   "jsonrpc": "2.0",
   "method": "trigger.create",
   "params": [
      {
         "description": "Processor load is too high on {HOST.NAME}"
      },
      {
         "description": "Service status",
         "expression": "{Linux server:log[/var/log/system,Service .* has stopped].strlen()}<>0",
         "dependencies": [
            {
               "triggerid": "17367"
            }
         ]
      }
   ],
   "auth": "038e1d7b1735c6a5436ee9eae095879e",
   "id": 1
}
```

1118
Response:

```json
{
   "jsonrpc": "2.0",
   "result": {
      "triggerids": [
         "17369",
         "17370"
      ],
      "id": 1
   }
}
```

Source

CTrigger::create() in frontends/php/include/classes/api/services/CTrigger.php.

trigger.delete

Description

object trigger.delete(array triggerIds)

This method allows to delete triggers.

Parameters

(array) IDs of the triggers to delete.

Return values

(object) Returns an object containing the IDs of the deleted triggers under the triggerids property.

Examples

Delete multiple triggers

Delete two triggers.

Request:

```json
{
   "jsonrpc": "2.0",
   "method": "trigger.delete",
   "params": [
      "12002",
      "12003"
   ],
   "auth": "3a57200802b24cda67c4e4010b50c065",
   "id": 1
}
```

Response:

```json
{
   "jsonrpc": "2.0",
   "result": {
      "triggerids": [
         "12002",
         "12003"
      ],
      "id": 1
   }
}
```

Source

CTrigger::delete() in frontends/php/include/classes/api/services/CTrigger.php.
**trigger.deletedependencies**

**Description**

object `trigger.deletedependencies(string/array triggers)`

This method allows to delete all trigger dependencies from the given triggers.

**Parameters**

(string/array) Triggers to delete the trigger dependencies from.

**Return values**

(object) Returns an object containing the IDs of the affected triggers under the `triggerids` property.

**Examples**

Deleting dependencies from multiple triggers

Delete all dependencies from two triggers.

**Request:**

```json
{
   "jsonrpc": "2.0",
   "method": "trigger.deleteDependencies",
   "params": [
      {
         "triggerid": "14544"
      },
      {
         "triggerid": "14545"
      }
   ],
   "auth": "038e1d7b1735c6a5436ee9eae095879e",
   "id": 1
}
```

**Response:**

```json
{
   "jsonrpc": "2.0",
   "result": {
      "triggerids": [
         "14544",
         "14545"
      ],
      "id": 1
   }
}
```

See also

- `trigger.update`

**Source**

CTrigger::deleteDependencies() in frontends/php/include/classes/api/services/CTrigger.php.

**trigger.get**

**Description**

integer/array `trigger.get(object parameters)`

The method allows to retrieve triggers according to the given parameters.

**Parameters**

(object) Parameters defining the desired output.

The method supports the following parameters.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>triggerids</td>
<td>string/array</td>
<td>Return only triggers with the given IDs.</td>
</tr>
<tr>
<td>groupids</td>
<td>string/array</td>
<td>Return only triggers that belong to hosts from the given host groups.</td>
</tr>
<tr>
<td>templateids</td>
<td>string/array</td>
<td>Return only triggers that belong to the given templates.</td>
</tr>
<tr>
<td>hostids</td>
<td>string/array</td>
<td>Return only triggers that belong to the given hosts.</td>
</tr>
<tr>
<td>itemids</td>
<td>string/array</td>
<td>Return only triggers that contain the given items.</td>
</tr>
<tr>
<td>applicationids</td>
<td>string/array</td>
<td>Return only triggers that contain items from the given applications.</td>
</tr>
<tr>
<td>functions</td>
<td>string/array</td>
<td>Return only triggers that use the given functions.</td>
</tr>
<tr>
<td>group</td>
<td>string</td>
<td>Return only triggers that belong to hosts from the host group with the given name.</td>
</tr>
<tr>
<td>host</td>
<td>string</td>
<td>Return only triggers that belong to host with the given name.</td>
</tr>
<tr>
<td>inherited</td>
<td>boolean</td>
<td>If set to true return only triggers inherited from a template.</td>
</tr>
<tr>
<td>templated</td>
<td>boolean</td>
<td>If set to true return only triggers that belong to templates.</td>
</tr>
<tr>
<td>monitored</td>
<td>flag</td>
<td>Return only enabled triggers that belong to monitored hosts and contain only enabled items.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>active</td>
<td>flag</td>
<td>Return only enabled triggers that belong to monitored hosts.</td>
</tr>
<tr>
<td>maintenance</td>
<td>boolean</td>
<td>If set to true, return only enabled triggers that belong to hosts in maintenance.</td>
</tr>
<tr>
<td>withUnacknowledgedEvents</td>
<td></td>
<td>Return only triggers that have unacknowledged events.</td>
</tr>
<tr>
<td>withAcknowledgedEvents</td>
<td></td>
<td>Return only triggers with all events acknowledged.</td>
</tr>
<tr>
<td>withLastEventUnacknowledged</td>
<td></td>
<td>Return only triggers with the last event unacknowledged.</td>
</tr>
<tr>
<td>skipDependent</td>
<td>flag</td>
<td>Skip triggers in a problem state that are dependent on other triggers. Note that the other triggers are ignored if disabled, have disabled items or disabled item hosts.</td>
</tr>
<tr>
<td>lastChangeSince</td>
<td>timestamp</td>
<td>Return only triggers that have changed their state after the given time.</td>
</tr>
<tr>
<td>lastChangeTill</td>
<td>timestamp</td>
<td>Return only triggers that have changed their state before the given time.</td>
</tr>
<tr>
<td>only_true</td>
<td>flag</td>
<td>Return only triggers that have recently been in a problem state.</td>
</tr>
<tr>
<td>min_severity</td>
<td>integer</td>
<td>Return only triggers with severity greater or equal than the given severity.</td>
</tr>
<tr>
<td>evaltype</td>
<td>integer</td>
<td>Rules for tag searching.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - (default)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>And/Or;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 - Or.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>tags</td>
<td>array of objects</td>
<td>Return only triggers with given tags. Exact match by tag and case-sensitive or case-insensitive search by tag value depending on operator value. Format: [{&quot;tag&quot;: &quot;&lt;tag&gt;&quot;, &quot;value&quot;: &quot;&lt;value&gt;&quot;, &quot;operator&quot;: &quot;&lt;operator&gt;&quot;}, ...]. An empty array returns all triggers. Possible operator types: 0 - (default) Like; 1 - Equal.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>selectFunctions</td>
<td>query</td>
<td>Return functions used in the trigger in the functions property. The function objects represent the functions used in the trigger expression and has the following properties: functionid - (string) ID of the function; itemid - (string) ID of the item used in the function; function - (string) name of the function; parameter - (string) parameter passed to the function.</td>
</tr>
<tr>
<td>selectDependencies</td>
<td>query</td>
<td>Return triggers that the trigger depends on in the dependencies property.</td>
</tr>
<tr>
<td>selectDiscoveryRule</td>
<td>query</td>
<td>Return the low-level discovery rule that created the trigger.</td>
</tr>
<tr>
<td>selectLastEvent</td>
<td>query</td>
<td>Return the last significant trigger event in the lastEvent property.</td>
</tr>
<tr>
<td>selectTags</td>
<td>query</td>
<td>Return the trigger tags in tags property.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| selectTriggerDiscovery | query   | Return the trigger discovery object in the triggerDiscovery property. The trigger discovery objects links the trigger to a trigger prototype from which it was created. It has the following properties:  
|                    |         | parent_triggerid - (string) ID of the trigger prototype from which the trigger has been created. Return only those results that exactly match the given filter.  
|                    |         | filter - object  
|                    |         | Accepts an array, where the keys are property names, and the values are either a single value or an array of values to match against. Supports additional filters:  
|                    |         | host - technical name of the host that the trigger belongs to;  
|                    |         | hostid - ID of the host that the trigger belongs to.  
|                    |         | limitSelects - integer  
|                    |         | Limits the number of records returned by subselects. Applies to the following subselects:  
<p>|                    |         | selectHosts - results will be sorted by host. |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Sort the result by the given properties. Possible values are: triggerid, description, status, priority, lastchange and hostname. These parameters being common for all get methods are described in detail in the reference Commentary page.</td>
</tr>
<tr>
<td>countOutput</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>editable</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>excludeSearch</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>limit</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>output</td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>preservekeys</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>search</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>searchByAny</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>searchWildcardsEnabled</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>sortorder</td>
<td>string/array</td>
<td></td>
</tr>
<tr>
<td>startSearch</td>
<td>boolean</td>
<td></td>
</tr>
</tbody>
</table>

**Return values**

(integer/array) Returns either:

- an array of objects;
- the count of retrieved objects, if the countOutput parameter has been used.

**Examples**

Retrieving data by trigger ID

Retrieve all data and the functions used in trigger "14062".

Request:

```json
{
  "jsonrpc": "2.0",
  "method": "trigger.get",
  "params": {
    "triggerids": "14062",
    "output": "extend",
    "selectFunctions": "extend"
  },
  "auth": "038e1d7b1735c6a5436ee9eae095879e",
  "id": 1
}
```

Response:

```json
{
  "jsonrpc": "2.0",
  "result": [
    {
      "functions": [
```

1126
Retrieving triggers in problem state

Retrieve the ID, name and severity of all triggers in problem state and sort them by severity in descending order.

Request:

```
{
   "jsonrpc": "2.0",
   "method": "trigger.get",
   "params": {
      "output": ["triggerid", "description", "priority"],
      "filter": {"value": 1},
      "sortfield": "priority",
      "sortorder": "DESC"
   },
   "auth": "038e1d7b1735c6a5436ee9f9ee096879e",
   "id": 1
}
```

Response:

```
{
   "jsonrpc": "2.0",
   "result": [
   {
      "triggerid": "13907",
      "description": "Zabbix self-monitoring processes < 100% busy",
      "priority": "4"
   }
   ]
}
```
Retrieving a specific trigger with tags

Retrieve a specific trigger with tags.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "trigger.get",
    "params": {
        "output": [
            "triggerid",
            "description"
        ],
        "selectTags": "extend",
        "triggerids": [
            "17578"
        ]
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": [
        {
            "triggerid": "17370",
            "description": "Service status",
            "tags": [
                {
                    "tag": "service",
                    "value": "{{ITEM.VALUE}.regsub("Service (.*) has stopped", \"\1\")}"},
                {
                    "tag": "error",
                    "value": ""
                }
            ]
        }
    ],
    "id": 1
}
```

See also

- Discovery rule
- Item
- Host
- Host group

Source

CTrigger::get() in frontends/php/include/classes/api/services/CTrigger.php.
**trigger.update**

**Description**

`object trigger.update(object/array triggers)`

This method allows to update existing triggers.

**Parameters**

(object/array) Trigger properties to be updated.

The `triggerid` property must be defined for each trigger, all other properties are optional. Only the passed properties will be updated, all others will remain unchanged.

Additionally to the standard trigger properties the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dependencies</td>
<td>array</td>
<td>Triggers that the trigger is dependent on. The triggers must have the <code>triggerid</code> property defined.</td>
</tr>
<tr>
<td>tags</td>
<td>array</td>
<td>Trigger tags.</td>
</tr>
</tbody>
</table>

**Attention:**
The trigger expression has to be given in its expanded form.

**Return values**

(object) Returns an object containing the IDs of the updated triggers under the `triggerids` property.

**Examples**

Enabling a trigger

Enable a trigger, that is, set its status to 0.

**Request:**

```json
{
    "jsonrpc": "2.0",
    "method": "trigger.update",
    "params": {
        "triggerid": "13938",
        "status": 0
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

**Response:**

```json
{
    "jsonrpc": "2.0",
    "result": {
        "triggerids": ["13938"
    ],
    "id": 1
}
```

Replacing triggers tags
Replace tags for trigger.

Request:

```json
{
   "jsonrpc": "2.0",
   "method": "trigger.update",
   "params": {
      "triggerid": "13938",
      "tags": [
         {
            "tag": "service",
            "value": "{{ITEM.VALUE}.regsub("Service (.*) has stopped\", \"\\\"")}"}
      ],
      "tag": "error",
      "value": ""
   }
},
"auth": "038e1d7b1735c6a5436ee9eae095879e",
"id": 1
}
```

Response:

```json
{
   "jsonrpc": "2.0",
   "result": {
      "triggerids": [
         "13938"
      ]
   },
   "id": 1
}
```

See also

- trigger.adddependencies
- trigger.deletedependencies

Source

CTrigger::update() in frontends/php/include/classes/api/services/CTrigger.php.

### Trigger prototype

This class is designed to work with trigger prototypes.

Object references:

- Trigger prototype

Available methods:

- triggerprototype.create - creating new trigger prototypes
- triggerprototype.delete - deleting trigger prototypes
- triggerprototype.get - retrieving trigger prototypes
- triggerprototype.update - updating trigger prototypes

> Trigger prototype object

The following objects are directly related to the triggerprototype API.

Trigger prototype
The trigger prototype object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>triggerid</td>
<td>string</td>
<td>(readonly) ID of the trigger prototype.</td>
</tr>
<tr>
<td>description</td>
<td>string</td>
<td>Name of the trigger prototype.</td>
</tr>
<tr>
<td>expression</td>
<td>string</td>
<td>Reduced trigger expression.</td>
</tr>
<tr>
<td>comments</td>
<td>string</td>
<td>Additional comments to the trigger prototype.</td>
</tr>
<tr>
<td>priority</td>
<td>integer</td>
<td>Severity of the trigger prototype. Possible values: 0 - (default) not classified; 1 - information; 2 - warning; 3 - average; 4 - high; 5 - disaster.</td>
</tr>
<tr>
<td>status</td>
<td>integer</td>
<td>Whether the trigger prototype is enabled or disabled. Possible values: 0 - (default) enabled; 1 - disabled.</td>
</tr>
<tr>
<td>templateid</td>
<td>string</td>
<td>(readonly) ID of the parent template trigger prototype.</td>
</tr>
<tr>
<td>type</td>
<td>integer</td>
<td>Whether the trigger prototype can generate multiple problem events. Possible values: 0 - (default) do not generate multiple events; 1 - generate multiple events.</td>
</tr>
<tr>
<td>url</td>
<td>string</td>
<td>URL associated with the trigger prototype. OK event generation mode.</td>
</tr>
<tr>
<td>recovery_mode</td>
<td>integer</td>
<td>Possible values are: 0 - (default) Expression; 1 - Recovery expression; 2 - None.</td>
</tr>
</tbody>
</table>
### Property | Type | Description
--- | --- | ---
recovery_expression | string | Reduced trigger recovery expression.
correlation_mode | integer | OK event closes. Possible values are:
| | 0 - (default) All problems; 1 - All problems if tag values match.
correlation_tag | string | Tag for matching. Allow manual close. Possible values are:
| | 0 - (default) No; 1 - Yes.
manual_close | integer | Allow manual close.

Note that for some methods (update, delete) the required/optional parameter combination is different.

**Trigger prototype tag**

The trigger prototype tag object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tag</td>
<td>string</td>
<td>Trigger prototype tag name.</td>
</tr>
<tr>
<td>(required)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>value</td>
<td>string</td>
<td>Trigger prototype tag value.</td>
</tr>
</tbody>
</table>

**triggerprototype.create**

Description

Object triggerprototype.create(object/array triggerPrototypes)

This method allows to create new trigger prototypes.

Parameters

(object/array) Trigger prototypes to create.

Additionally to the *standard trigger prototype properties* the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dependencies</td>
<td>array</td>
<td>Triggers and trigger prototypes that the trigger prototype is dependent on.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The triggers must have the triggerid property defined.</td>
</tr>
<tr>
<td>tags</td>
<td>array</td>
<td>Trigger prototype tags.</td>
</tr>
</tbody>
</table>
Attention:
The trigger expression has to be given in its expanded form and must contain at least one item prototype.

Return values

(object) Returns an object containing the IDs of the created trigger prototypes under the triggerids property. The order of the returned IDs matches the order of the passed trigger prototypes.

Examples

Creating a trigger prototype

Create a trigger prototype to detect when a file system has less than 20% free disk space.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "triggerprototype.create",
    "params": {
        "description": "Free disk space is less than 20% on volume \{#FSNAME\}"
        "expression": "{Zabbix server:vfs.fs.size[{#FSNAME},pfree].last()}<20",
        "tags": [
            {
                "tag": "volume",
                "value": "{#FSNAME}\"
            },
            {
                "tag": "type",
                "value": "{#FSTYPE}\"
            }
        ]
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "triggerids": [
            "17372"
        ]
    },
    "id": 1
}
```

Source

CTriggerPrototype::create() in frontends/php/include/classes/api/services/CTriggerPrototype.php.

triggerprototype.delete

Description

object triggerprototype.delete(array triggerPrototypeIds)

This method allows to delete trigger prototypes.

Parameters

(array) IDs of the trigger prototypes to delete.

Return values

(object) Returns an object containing the IDs of the deleted trigger prototypes under the triggerids property.

Examples
Deleting multiple trigger prototypes
Delete two trigger prototypes.

Request:
```json
{
   "jsonrpc": "2.0",
   "method": "triggerprototype.delete",
   "params": [
      "12002",
      "12003"
   ],
   "auth": "3a57200802b24cda67c4e4010b50c065",
   "id": 1
}
```

Response:
```json
{
   "jsonrpc": "2.0",
   "result": {
      "triggerids": [
         "12002",
         "12003"
      ]
   },
   "id": 1
}
```

Source
CTriggerPrototype::delete() in frontends/php/include/classes/api/services/CTriggerPrototype.php.

**triggerprototype.get**

Description
integer/array triggerprototype.get(object parameters)

The method allows to retrieve trigger prototypes according to the given parameters.

Parameters
(object) Parameters defining the desired output.

The method supports the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>active</td>
<td>flag</td>
<td>Return only enabled trigger prototypes that belong to monitored hosts.</td>
</tr>
<tr>
<td>applicationids</td>
<td>string/array</td>
<td>Return only trigger prototypes that contain items from the given applications.</td>
</tr>
<tr>
<td>discoveryids</td>
<td>string/array</td>
<td>Return only trigger prototypes that belong to the given LLD rules.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>functions</td>
<td>string/array</td>
<td>Return only triggers that use the given functions. Refer to the supported trigger functions page for a list of supported functions.</td>
</tr>
<tr>
<td>group</td>
<td>string</td>
<td>Return only trigger prototypes that belong to hosts from the host groups with the given name.</td>
</tr>
<tr>
<td>groupids</td>
<td>string/array</td>
<td>Return only trigger prototypes that belong to hosts from the given host groups.</td>
</tr>
<tr>
<td>host</td>
<td>string</td>
<td>Return only trigger prototypes that belong to hosts with the given name.</td>
</tr>
<tr>
<td>hostids</td>
<td>string/array</td>
<td>Return only trigger prototypes that belong to the given hosts.</td>
</tr>
<tr>
<td>inherited</td>
<td>boolean</td>
<td>If set to true return only trigger prototypes inherited from a template.</td>
</tr>
<tr>
<td>maintenance</td>
<td>boolean</td>
<td>If set to true return only enabled trigger prototypes that belong to hosts in maintenance.</td>
</tr>
<tr>
<td>min_severity</td>
<td>integer</td>
<td>Return only trigger prototypes with severity greater or equal than the given severity.</td>
</tr>
<tr>
<td>monitored</td>
<td>flag</td>
<td>Return only enabled trigger prototypes that belong to monitored hosts and contain only enabled items.</td>
</tr>
<tr>
<td>templated</td>
<td>boolean</td>
<td>If set to true return only trigger prototypes that belong to templates.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>templateids</td>
<td>string/array</td>
<td>Return only trigger prototypes that belong to the given templates.</td>
</tr>
<tr>
<td>triggerids</td>
<td>string/array</td>
<td>Return only trigger prototypes with the given IDs.</td>
</tr>
<tr>
<td>expandExpression</td>
<td>flag</td>
<td>Expand functions and macros in the trigger expression.</td>
</tr>
<tr>
<td>selectDiscoveryRule</td>
<td>query</td>
<td>Return the LLD rule that the trigger prototype belongs to.</td>
</tr>
<tr>
<td>selectFunctions</td>
<td>query</td>
<td>Return functions used in the trigger prototype in the functions property.</td>
</tr>
<tr>
<td>selectGroups</td>
<td>query</td>
<td>Return the host groups that the trigger prototype belongs to in the groups property.</td>
</tr>
<tr>
<td>selectHosts</td>
<td>query</td>
<td>Return the hosts that the trigger prototype belongs to in the hosts property.</td>
</tr>
<tr>
<td>selectItems</td>
<td>query</td>
<td>Return items and item prototypes used the trigger prototype in the items property.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>selectDependences</td>
<td>query</td>
<td>Return trigger prototypes and triggers that the trigger prototype depends on in the dependencies property.</td>
</tr>
<tr>
<td>selectTags</td>
<td>query</td>
<td>Return the trigger prototype tags in tags property.</td>
</tr>
<tr>
<td>filter</td>
<td>object</td>
<td>Return only those results that exactly match the given filter.</td>
</tr>
<tr>
<td>limitSelects</td>
<td>integer</td>
<td>Limits the number of records returned by subselects.</td>
</tr>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Sort the result by the given properties.</td>
</tr>
<tr>
<td>countOutput</td>
<td>boolean</td>
<td>These parameters being common for all get methods are described in detail in the reference commentary.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>editable</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>excludeSearch</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>limit</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>output</td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>preservekeys</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>search</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>searchByAny</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>searchWildcards</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>sortorder</td>
<td>string/array</td>
<td></td>
</tr>
<tr>
<td>startSearch</td>
<td>boolean</td>
<td></td>
</tr>
</tbody>
</table>

Return values

(integer/array) Returns either:

- an array of objects;
- the count of retrieved objects, if the countOutput parameter has been used.

Examples

Retrieve trigger prototypes from an LLD rule

Retrieve all trigger prototypes and their functions from an LLD rule.

Request:

```json
{
   "jsonrpc": "2.0",
   "method": "triggerprototype.get",
   "params": {
      "output": "extend",
      "selectFunctions": "extend",
      "discoveryids": "22450"
   },
   "auth": "038e1d7b1735c6a5436e9e9aae096879e",
   "id": 1
}
```

Response:

```json
{
   "jsonrpc": "2.0",
   "result": [
      {
         "functions": [
            {
               "functionid": "12598",
               "itemid": "22454",
               "function": "last",
               "parameter": "0"
            }
         ],
         "triggerid": "13272",
         "expression": "{12598}<20",
         "description": "Free inodes is less than 20% on volume {#FSNAME}",
         "url": "",
         "status": "0",
         "priority": "2",
         "comments": "",
         "templateid": "0",
         "type": "0",
         "flags": "2",
         "recovery_mode": "0",
         "recovery_expression": "",
         "correlation_mode": "0"
      }
   ]
}```
Retrieve a specific trigger prototype with tags

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "triggerprototype.get",
    "params": {
        "output": ["triggerid", "description"]
    },
    "selectTags": "extend",
    "triggerids": ["17373"]
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": [
        {
            "triggerid": "17373",
            "description": "Free disk space is less than 20% on volume {#FSNAME}"
        }
    ]
}
```


```
},
{
   "tag": "type",
   "value": "#{FSTYPE}"
}
}
],
"id": 1
}

See also

- Discovery rule
- Item
- Host
- Host group

Source

CTriggerPrototype::get() in frontends/php/include/classes/api/services/CTriggerPrototype.php.

triggerprototype.update

Description

object triggerprototype.update(object/array triggerPrototypes)

This method allows to update existing trigger prototypes.

Parameters

(object/array) Trigger prototype properties to be updated.

The triggerid property must be defined for each trigger prototype, all other properties are optional. Only the passed properties will be updated, all others will remain unchanged.

Additionally to the standard trigger prototype properties the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dependencies</td>
<td>array</td>
<td>Triggers and trigger prototypes that the trigger prototype is dependent on. The triggers must have the triggerid property defined.</td>
</tr>
<tr>
<td>tags</td>
<td>array</td>
<td>Trigger prototype tags.</td>
</tr>
</tbody>
</table>

Attention:
The trigger expression has to be given in its expanded form and must contain at least one item prototype.

Return values

(object) Returns an object containing the IDs of the updated trigger prototypes under the triggerids property.

Examples

Enabling a trigger prototype

Enable a trigger prototype, that is, set its status to 0.

Request:
{
    "jsonrpc": "2.0",
    "method": "triggerprototype.update",
    "params": {
        "triggerid": "13938",
        "status": 0
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}

Response:
{
    "jsonrpc": "2.0",
    "result": {
        "triggerids": ["13938"
    ],
    "id": 1
}

Replacing trigger prototype tags

Replace tags for one trigger prototype.

Request:
{
    "jsonrpc": "2.0",
    "method": "triggerprototype.update",
    "params": {
        "triggerid": "17373",
        "tags": [
            {
                "tag": "volume",
                "value": "{#FSNAME}"
            },
            {
                "tag": "type",
                "value": "{#FSTYPE}"            }
        ]
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}

Response:
{
    "jsonrpc": "2.0",
    "result": {
        "triggerids": ["17373"
    ],
    "id": 1
}

Source
CTriggerPrototype::update() in frontends/php/include/classes/api/services/CTriggerPrototype.php.

User
This class is designed to work with users.

Object references:

- User

Available methods:

- user.create - creating new users
- user.delete - deleting users
- user.get - retrieving users
- user.login - logging in to the API
- user.logout - logging out of the API
- user.update - updating users

> User object

The following objects are directly related to the user API.

User

The user object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>userid</td>
<td>string</td>
<td>(readonly) ID of the user.</td>
</tr>
<tr>
<td>alias</td>
<td>string</td>
<td>User alias.</td>
</tr>
<tr>
<td>attempt_clock</td>
<td>timestamp</td>
<td>(readonly) Time of the last unsuccessful login attempt.</td>
</tr>
<tr>
<td>attempt_failed</td>
<td>integer</td>
<td>(readonly) Recent failed login attempt count.</td>
</tr>
<tr>
<td>attempt_ip</td>
<td>string</td>
<td>(readonly) IP address from where the last unsuccessful login attempt came from.</td>
</tr>
<tr>
<td>autologin</td>
<td>integer</td>
<td>Whether to enable auto-login.</td>
</tr>
<tr>
<td>autologout</td>
<td>string</td>
<td>User session lifetime. Accepts seconds and time unit with suffix. If set to 0s, the session will never expire.</td>
</tr>
</tbody>
</table>

Possible values:
0 - (default) auto-login disabled;
1 - auto-login enabled.

Default: 15m.
<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lang</td>
<td>string</td>
<td>Language code of the user's language. Default: en_GB.</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>Name of the user.</td>
</tr>
<tr>
<td>refresh</td>
<td>string</td>
<td>Automatic refresh period. Accepts seconds or time unit with suffix (e.g., 30s, 90s, 1m, 1h). Default: 30s.</td>
</tr>
<tr>
<td>rows_per_page</td>
<td>integer</td>
<td>Amount of object rows to show per page. Default: 50.</td>
</tr>
<tr>
<td>surname</td>
<td>string</td>
<td>Surname of the user.</td>
</tr>
<tr>
<td>theme</td>
<td>string</td>
<td>User's theme. Possible values: default - (default) system default; blue-theme - Blue; dark-theme - Dark.</td>
</tr>
<tr>
<td>type</td>
<td>integer</td>
<td>Type of the user. Possible values: 1 - (default) Zabbix user; 2 - Zabbix admin; 3 - Zabbix super admin.</td>
</tr>
<tr>
<td>url</td>
<td>string</td>
<td>URL of the page to redirect the user to after logging in.</td>
</tr>
</tbody>
</table>

Note that for some methods (update, delete) the required/optional parameter combination is different.

Media

The media object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mediatypeid</td>
<td>string</td>
<td>ID of the media type used by the media. (required)</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>sendto</strong></td>
<td>string/array</td>
<td>Address, user name or other identifier of the recipient.</td>
</tr>
<tr>
<td>(required)</td>
<td></td>
<td>If type of <strong>Media type</strong> is e-mail, values are represented as array. For other types of <strong>Media types</strong>, value is represented as a string.</td>
</tr>
<tr>
<td><strong>active</strong></td>
<td>integer</td>
<td>Whether the media is enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values: 0 - (default) enabled; 1 - disabled.</td>
</tr>
<tr>
<td><strong>severity</strong></td>
<td>integer</td>
<td>Trigger severities to send notifications about.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Severities are stored in binary form with each bit representing the corresponding severity. For example, 12 equals 1100 in binary and means, that notifications will be sent from triggers with severities warning and average.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Refer to the <strong>trigger object page</strong> for a list of supported trigger severities.</td>
</tr>
<tr>
<td><strong>period</strong></td>
<td>string</td>
<td>Time when the notifications can be sent as a <strong>time period</strong> or user macros separated by a semicolon.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 63</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-7,00:00-24:00</td>
</tr>
</tbody>
</table>
user.checkAuthentication

Description

object user.checkAuthentication

This method checks and prolongs user session.

Parameters

The method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>extend</td>
<td>boolean</td>
<td>Default value: &quot;true&quot;. Setting it's value to &quot;false&quot; allows to check session without extending its lifetime. Supported since Zabbix 4.0.</td>
</tr>
<tr>
<td>sessionid</td>
<td>string</td>
<td>User session id.</td>
</tr>
</tbody>
</table>

Attention:
Calling user.checkAuthentication method prolongs user session by default.

Return values

(object) Returns an object containing information about user.

Examples

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "user.checkAuthentication",
    "params": {
        "sessionid": "8CB447FF6F61D134CEAC740CCA1BC90D"
    },
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "userid": "1",
        "alias": "Admin",
        "name": "Zabbix",
        "surname": "Administrator",
        "url": "",
        "autologin": "1",
        "autologout": "0",
        "lang": "ru_RU",
        "refresh": "0",
        "type": "3",
        "theme": "default",
        "attempt_failed": "0",
        "attempt_ip": "127.0.0.1",
        "attempt_clock": "1355919038",
        "rows_per_page": "50",
        "debug_mode": true
    }
}
```
"userip": "127.0.0.1",
"sessionid": "8C8447FF6F61D134CEAC740CCA1BC90D",
"gui_access": "0"
},
"id": 1
}

**Note:**
Response is similar to User.login call response with "userData" parameter set to true (the difference is that user data is retrieved by session id and not by username / password).

Source
CUser::checkAuthentication() in frontends/php/include/classes/api/services/CUser.php.

**user.create**

**Description**
object user.create(object/array users)

This method allows to create new users.

**Parameters**
(object/array) Users to create.

Additionally to the standard user properties, the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>passwd</td>
<td>string</td>
<td>User’s password.</td>
</tr>
<tr>
<td>(required)</td>
<td></td>
<td>Can be omitted if user is added only to groups that have LDAP access.</td>
</tr>
<tr>
<td>usrgrps</td>
<td>array</td>
<td>User groups to add the user to.</td>
</tr>
<tr>
<td>(required)</td>
<td></td>
<td>The user groups must have the usgrpid property defined.</td>
</tr>
<tr>
<td>user_medias</td>
<td>array</td>
<td>Medias to create for the user.</td>
</tr>
</tbody>
</table>

**Return values**
(object) Returns an object containing the IDs of the created users under the userids property. The order of the returned IDs matches the order of the passed users.

**Examples**

Creating a user

Create a new user, add him to a user group and create a new media for him.

**Request:**

```json
{
    "jsonrpc": "2.0",
    "method": "user.create",
    "params": {
        "alias": "John",
        "passwd": "Doe123",
```
"usrgrps": [
  {
    "usrgrpid": "7"
  }
],
"user_medias": [
  {
    "mediatypeid": "1",
    "sendto": [
      "support@company.com"
    ],
    "active": 0,
    "severity": 63,
    "period": "1-7,00:00-24:00"
  }
],
"auth": "038e1d7b1735c6a5436ee9eae095879e",
"id": 1
}

Response:
{
  "jsonrpc": "2.0",
  "result": {
    "userids": [
      "12"
    ],
    "id": 1
  }
}

See also
- Media
- User group

Source
CUser::create() in frontends/php/include/classes/api/services/CUser.php.

**user.delete**

Description

object user.delete(array users)

This method allows to delete users.

Parameters

(array) IDs of users to delete.

Return values

(object) Returns an object containing the IDs of the deleted users under the userids property.

Examples

Deleting multiple users

Delete two users.

Request:

{
  "jsonrpc": "2.0",
  "method": "user.delete",
  "params": [
"usrgrps": [
  {
    "usrgrpid": "7"
  }
],
"user_medias": [
  {
    "mediatypeid": "1",
    "sendto": [
      "support@company.com"
    ],
    "active": 0,
    "severity": 63,
    "period": "1-7,00:00-24:00"
  }
],
"auth": "038e1d7b1735c6a5436ee9eae095879e",
"id": 1
}
Response:

```
{
    "jsonrpc": "2.0",
    "result": {
        "userids": [
            "1",
            "5"
        ],
        "id": 1
    },
    "id": 1
}
```

Source

CUser::delete() in frontends/php/include/classes/api/services/CUser.php.

**user.get**

**Description**

**integer/array** **user.get**(object **parameters**)  
The method allows to retrieve users according to the given parameters.

**Parameters**

(object) Parameters defining the desired output.

The method supports the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mediaids</td>
<td>string/array</td>
<td>Return only users that use the given media.</td>
</tr>
<tr>
<td>mediatypeids</td>
<td>string/array</td>
<td>Return only users that use the given media types.</td>
</tr>
<tr>
<td>userids</td>
<td>string/array</td>
<td>Return only users with the given IDs.</td>
</tr>
<tr>
<td>usgrpid</td>
<td>string/array</td>
<td>Return only users that belong to the given user groups.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>getAccess</td>
<td>flag</td>
<td>Adds additional information about user permissions. Adds the following properties for each user: gui_access - (integer) user’s frontend authentication method. Refer to the gui_access property of the user group object for a list of possible values. debug_mode - (integer) indicates whether debug is enabled for the user. Possible values: 0 - debug disabled, 1 - debug enabled. users_status - (integer) indicates whether the user is disabled. Possible values: 0 - user enabled, 1 - user disabled.</td>
</tr>
</tbody>
</table>

selectMedias query

selectMediatypes query

selectUsrgrps query

sortfield string/array Sort the result by the given properties. Possible values are: userid and alias.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>countOutput</td>
<td>boolean</td>
<td>These parameters being common for all get methods are described in detail in the reference commentary.</td>
</tr>
<tr>
<td>editable</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>excludeSearch</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>filter</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>limit</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>output</td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>preservekeys</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>search</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>searchByAny</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>searchWildcardsEnabled</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>sortOrder</td>
<td>string/array</td>
<td></td>
</tr>
<tr>
<td>startSearch</td>
<td>boolean</td>
<td></td>
</tr>
</tbody>
</table>

Return values

(integer/array) Returns either:

- an array of objects;
- the count of retrieved objects, if the countOutput parameter has been used.

Examples

Retrieving users

Retrieve all of the configured users.

Request:

```json
{
  "jsonrpc": "2.0",
  "method": "user.get",
  "params": {
    "output": "extend"
  },
  "auth": "038e1d7b1735c6a5436ee9eae095879e",
  "id": 1
}
```

Response:

```json
{
  "jsonrpc": "2.0",
  "result": [
    {
      "userid": "1",
      "alias": "Admin",
      "name": "Zabbix",
      "surname": "Administrator",
      "url": "",
      "autologin": "1",
      "autologout": "0s",
      "lang": "ru_RU",
      "refresh": "0s",
      "type": "3",
      "theme": "default",
      "attempt_failed": "0",
      "attempt_ip": "",
      "attempt_clock": "0",
      "rows_per_page": "50"
    }
  ]
}
```
user.login

Description

string/object user.login(object parameters)

This method allows to log in to the API and generate an authentication token.

Warning:
When using this method, you also need to do user.logout to prevent the generation of a large number of open session records.

Parameters

Attention:
This method is available to unauthenticated users and must be called without the auth parameter in the JSON-RPC request.

(object) Parameters containing the user name and password.

The method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>password</td>
<td>string</td>
<td>User password.</td>
</tr>
<tr>
<td>(required)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>user</td>
<td>string</td>
<td>User name.</td>
</tr>
<tr>
<td>(required)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>userData</td>
<td>flag</td>
<td>Return information about the authenticated user.</td>
</tr>
</tbody>
</table>

Return values

(string/object) If the userData parameter is used, returns an object containing information about the authenticated user.

Additionally to the standard user properties, the following information is returned:
<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug_mode</td>
<td>boolean</td>
<td>Whether debug mode is enabled for the user.</td>
</tr>
<tr>
<td>gui_access</td>
<td>integer</td>
<td>User's authentication method to the frontend.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Refer to the gui_access property of the user group object for a list of possible values.</td>
</tr>
<tr>
<td>sessionid</td>
<td>string</td>
<td>Authentication token, which must be used in the following API requests.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IP address of the user.</td>
</tr>
</tbody>
</table>

**Note:**
If a user has been successfully authenticated after one or more failed attempts, the method will return the current values for the attempt_clock, attempt_failed and attempt_ip properties and then reset them.

If the userData parameter is not used, the method returns an authentication token.

**Note:**
The generated authentication token should be remembered and used in the auth parameter of the following JSON-RPC requests. It is also required when using HTTP authentication.

Examples

**Authenticating a user**

**Authenticate a user.**

**Request:**

```json
{   "jsonrpc": "2.0",   "method": "user.login",   "params": {     "user": "Admin",     "password": "zabbix"   },   "id": 1 }```

**Response:**

```json
{   "jsonrpc": "2.0",   "result": "0424bd59b807674191e7d77572075f33",   "id": 1 }```

**Requesting authenticated user’s information**

**Authenticate and return additional information about the user.**

**Request:**
See also

- user.logout

Source

CUser::login() in frontends/php/include/classes/api/services/CUser.php.

**user.logout**

Description

`string/object user.logout(array)`

This method allows to log out of the API and invalidates the current authentication token.

Parameters

(array) The method accepts an empty array.

Return values

(boolean) Returns true if the user has been logged out successfully.

Examples

Logging out

Log out from the API.

Request:
```json
{
   "jsonrpc": "2.0",
   "method": "user.logout",
   "params": [],
   "id": 1,
   "auth": "16a46baf181ef9602e1687f3110abf8a"
}
```

Response:

```json
{
   "jsonrpc": "2.0",
   "result": true,
   "id": 1
}
```

See also

- `user.login`

Source

CUser::login() in frontends/php/include/classes/api/services/CUser.php.

**user.update**

Description

`object user.update(object/array users)`

This method allows to update existing users.

Parameters

(object/array) User properties to be updated.

The `userid` property must be defined for each user, all other properties are optional. Only the passed properties will be updated, all others will remain unchanged.

Additionally to the **standard user properties**, the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>passwd</td>
<td>string</td>
<td>User’s password.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Can be empty string if user belongs to or is moved only to groups that have LDAP access.</td>
</tr>
<tr>
<td>usgrps</td>
<td>array</td>
<td>User groups to replace existing user groups.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The user groups must have the <code>usrgrpid</code> property defined.</td>
</tr>
<tr>
<td>user_medias</td>
<td>array</td>
<td>Medias to replace existing medias.</td>
</tr>
</tbody>
</table>

Return values

(object) Returns an object containing the IDs of the updated users under the `userids` property.

Examples

Renaming a user
Rename a user to John Doe.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "user.update",
    "params": {
        "userid": "1",
        "name": "John",
        "surname": "Doe"
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "userids": ["1"]
    },
    "id": 1
}
```

Source

CUser::update() in frontends/php/include/classes/api/services/CUser.php.

**User group**

This class is designed to work with user groups.

Object references:

- **User group**

Available methods:

- usergroup.create - creating new user groups
- usergroup.delete - deleting user groups
- usergroup.get - retrieving user groups
- usergroup.update - updating user groups

**User group object**

The following objects are directly related to the usergroup API.

User group

The user group object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>usgrpid</td>
<td>string</td>
<td>(readonly) ID of the user group.</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>Name of the user group.</td>
</tr>
</tbody>
</table>

(required)
<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug_mode</td>
<td>integer</td>
<td>Whether debug mode is enabled or disabled. Possible values are: 0 - (default) disabled; 1 - enabled.</td>
</tr>
<tr>
<td>gui_access</td>
<td>integer</td>
<td>Frontend authentication method of the users in the group. Possible values: 0 - (default) use the system default authentication method; 1 - use internal authentication; 2 - use LDAP authentication; 3 - disable access to the frontend.</td>
</tr>
<tr>
<td>users_status</td>
<td>integer</td>
<td>Whether the user group is enabled or disabled. Possible values are: 0 - (default) enabled; 1 - disabled.</td>
</tr>
</tbody>
</table>

Note that for some methods (update, delete) the required/optional parameter combination is different.

Permission

The permission object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>string</td>
<td>ID of the host group to add permission to. Access level to the host group. Possible values: 0 - access denied; 2 - read-only access; 3 - read-write access.</td>
</tr>
<tr>
<td>permission</td>
<td>integer</td>
<td>Access level to the host group. Possible values: 0 - access denied; 2 - read-only access; 3 - read-write access.</td>
</tr>
</tbody>
</table>

Tag based permission

The tag based permission object has the following properties.
<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>groupid</td>
<td>string</td>
<td>ID of the host group to add permission to. (required)</td>
</tr>
<tr>
<td>tag</td>
<td>string</td>
<td>Tag name.</td>
</tr>
<tr>
<td>value</td>
<td>string</td>
<td>Tag value.</td>
</tr>
</tbody>
</table>

usergroup.create

Description

object usergroup.create(object/array userGroups)

This method allows to create new user groups.

Parameters

(object/array) User groups to create.

Additionally to the standard user group properties, the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rights</td>
<td>object/array</td>
<td>Permissions to assign to the group</td>
</tr>
<tr>
<td>tag_filters</td>
<td>array</td>
<td>Tag based permissions to assign to the group</td>
</tr>
<tr>
<td>userids</td>
<td>string/array</td>
<td>IDs of users to add to the user group.</td>
</tr>
</tbody>
</table>

Return values

(object) Returns an object containing the IDs of the created user groups under the usgrpids property. The order of the returned IDs matches the order of the passed user groups.

Examples

Creating a user group

Create a user group, which denies access to host group “2”, and add a user to it.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "usergroup.create",
    "params": {
        "name": "Operation managers",
        "rights": {
            "permission": 0,
            "id": "2"
        },
        "userids": "12"
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "usgrpids": ["20"
        ],
        "id": 1
    }
}
```

See also
Permission
Source
CUserGroup::create() in frontends/php/include/classes/api/services/CUserGroup.php.

**usergroup.delete**

Description

object usergroup.delete(array userGroupIds)

This method allows to delete user groups.

Parameters

(array) IDs of the user groups to delete.

Return values

(object) Returns an object containing the IDs of the deleted user groups under the `usrgrpids` property.

Examples

Deleting multiple user groups

Delete two user groups.

Request:

```
{
    "jsonrpc": "2.0",
    "method": "usergroup.delete",
    "params": [
        "20",
        "21"
    ],
    "auth": "3a57200802b24cda67c4e4010b50c065",
    "id": 1
}
```

Response:

```
{
    "jsonrpc": "2.0",
    "result": {
        "usrgrpids": [
            "20",
            "21"
        ]
    },
    "id": 1
}
```

Source

CUserGroup::delete() in frontends/php/include/classes/api/services/CUserGroup.php.

**usergroup.get**

Description

integer/array usergroup.get(object parameters)

The method allows to retrieve user groups according to the given parameters.

Parameters

(object) Parameters defining the desired output.

The method supports the following parameters.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status</td>
<td>integer</td>
<td>Return only user groups with the given status. Refer to the user group page for a list of supported statuses.</td>
</tr>
<tr>
<td>userids</td>
<td>string/array</td>
<td>Return only user groups that contain the given users.</td>
</tr>
<tr>
<td>usrgrpids</td>
<td>string/array</td>
<td>Return only user groups with the given IDs.</td>
</tr>
<tr>
<td>selectTagFilters</td>
<td>query</td>
<td>Return user group tag based permissions in the tag_filters property. It has the following properties:</td>
</tr>
<tr>
<td>selectUsers</td>
<td>query</td>
<td>Return the users from the user group in the users property.</td>
</tr>
<tr>
<td>selectRights</td>
<td>query</td>
<td>Return user group rights in the rights property.</td>
</tr>
<tr>
<td>limitSelects</td>
<td>integer</td>
<td>Limits the number of records returned by subselects.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Sort the result by the given properties.</td>
</tr>
<tr>
<td>countOutput</td>
<td>boolean</td>
<td>Possible values are: usrgrpid, name. These parameters being common for all get methods are described in detail in the reference commentary.</td>
</tr>
<tr>
<td>editable</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>excludeSearch</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>filter</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>limit</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>output</td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>preservekeys</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>search</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>searchByAny</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>searchWildcardsEnabled</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>sortorder</td>
<td>string/array</td>
<td></td>
</tr>
<tr>
<td>startSearch</td>
<td>boolean</td>
<td></td>
</tr>
</tbody>
</table>

Return values
(integer/array) Returns either:
  • an array of objects;
  • the count of retrieved objects, if the countOutput parameter has been used.

Examples

Retrieving enabled user groups

Retrieve all enabled user groups.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "usergroup.get",
    "params": {
        "output": "extend",
        "status": 0
    },
    "auth": "038e1d7b1735c6a5436ee9eae096879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": [
        {
            "usrgrpid": "7",
            "name": "Zabbix administrators",
            "gui_access": "0",
            "users_status": "0",
            "debug_mode": "1"
        },
        {
```
<table>
<thead>
<tr>
<th>id</th>
<th>usrgrpid</th>
<th>name</th>
<th>gui_access</th>
<th>users_status</th>
<th>debug_mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>8</td>
<td>Guests</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>11</td>
<td>Enabled debug mode</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>No access to the frontend</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>Read only</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>18</td>
<td>Deny</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

See also

- **User**

Source

CUserGroup::get() in frontends/php/include/classes/api/services/CUserGroup.php.

### usergroup.update

**Description**

object usergroup.update(object/array userGroups)

This method allows to update existing user groups.

**Parameters**

(object/array) User group properties to be updated.

The **usrgrpid** property must be defined for each user group, all other properties are optional. Only the passed properties will be updated, all others will remain unchanged.

Additionally to the **standard user group properties**, the method accepts the following parameters.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rights</td>
<td>object/array</td>
<td>Permissions to replace the current permissions assigned to the user group.</td>
</tr>
<tr>
<td>tag_filters</td>
<td>array</td>
<td>Tag based permissions to replace the current permissions assigned to the user group.</td>
</tr>
<tr>
<td>userids</td>
<td>string/array</td>
<td>IDs of the users to replace the users in the user group.</td>
</tr>
</tbody>
</table>

Return values

(object) Returns an object containing the IDs of the updated user groups under the usrgrpids property.

Examples

Disabling a user group

Disable a user group.

Request:
```json
{
    "jsonrpc": "2.0",
    "method": "usergroup.update",
    "params": {
        "usrgrpid": "17",
        "users_status": "1"
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:
```json
{
    "jsonrpc": "2.0",
    "result": {
        "usrgrpids": [
            "17"
        ],
        "id": 1
    }
}
```

See also

- Permission

Source

CUserGroup::update() in frontends/php/include/classes/api/services/CUserGroup.php.

User macro

This class is designed to work with host and global macros.

Object references:
Global macro
Host macro

Available methods:

- `usermacro.create` - creating new host macros
- `usermacro.createglobal` - creating new global macros
- `usermacro.delete` - deleting host macros
- `usermacro.deleteglobal` - deleting global macros
- `usermacro.get` - retrieving host and global macros
- `usermacro.update` - updating host macros
- `usermacro.updateglobal` - updating global macros

> User macro object

The following objects are directly related to the `usermacro` API.

Global macro

The global macro object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>globalmacro</td>
<td>string</td>
<td>(readonly) ID of the global macro.</td>
</tr>
<tr>
<td>macro</td>
<td>string</td>
<td>Macro string.</td>
</tr>
<tr>
<td>value</td>
<td>string</td>
<td>Value of the macro.</td>
</tr>
</tbody>
</table>

Note that for some methods (update, delete) the required/optional parameter combination is different.

Host macro

The host macro object defines a macro available on a host or template. It has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostmacroid</td>
<td>string</td>
<td>(readonly) ID of the host macro.</td>
</tr>
<tr>
<td>hostid</td>
<td>string</td>
<td>ID of the host that the macro belongs to.</td>
</tr>
<tr>
<td>macro</td>
<td>string</td>
<td>Macro string.</td>
</tr>
<tr>
<td>value</td>
<td>string</td>
<td>Value of the macro.</td>
</tr>
</tbody>
</table>

Note that for some methods (update, delete) the required/optional parameter combination is different.

`usermacro.create`

Description

object `usermacro.create(object/array hostMacros)`

This method allows to create new host macros.

Parameters

(object/array) Host macros to create.

The method accepts host macros with the standard host macro properties.

Return values

(object) Returns an object containing the IDs of the created host macros under the `hostmacroids` property. The order of the returned IDs matches the order of the passed host macros.

Examples
Creating a host macro

Create a host macro "{$SNMP_COMMUNITY}" with the value "public" on host "10198".

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "usermacro.create",
    "params": {
        "hostid": "10198",
        "macro": "{$SNMP_COMMUNITY}"
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "hostmacroids": [
            "11"
        ]
    },
    "id": 1
}
```

Source

CUserMacro::create() in frontends/php/include/classes/api/services/CUserMacro.php.

**usermacro.createglobal**

Description

object usermacro.createglobal(object/array globalMacros)

This method allows to create new global macros.

Parameters

(object/array) Global macros to create.

The method accepts global macros with the standard global macro properties.

Return values

(object) Returns an object containing the IDs of the created global macros under the globalmacroids property. The order of the returned IDs matches the order of the passed global macros.

Examples

Creating a global macro

Create a global macro "{$SNMP_COMMUNITY}" with value "public".

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "usermacro.createglobal",
    "params": {
        "macro": "{$SNMP_COMMUNITY}"
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```
Response:
{
   "jsonrpc": "2.0",
   "result": {
      "globalmacroids": [
         "6"
      ],
   },
   "id": 1
}

Source
CUUserMacro::createGlobal() in frontends/php/include/classes/api/services/CUUserMacro.php.

usermacro.delete

Description
object usermacro.delete(array hostMacroIds)
This method allows to delete host macros.

Parameters
(array) IDs of the host macros to delete.

Return values
(object) Returns an object containing the IDs of the deleted host macros under the hostmacroids property.

Examples
Deleting multiple host macros
Delete two host macros.

Request:
{
   "jsonrpc": "2.0",
   "method": "usermacro.delete",
   "params": [
      "32",
      "11"
   ],
   "auth": "3a57200802b24cda67c4e4010b50c065",
   "id": 1
}

Response:
{
   "jsonrpc": "2.0",
   "result": {
      "hostmacroids": [
         "32",
         "11"
      ],
   },
   "id": 1
}

Source
CUUserMacro::delete() in frontends/php/include/classes/api/services/CUUserMacro.php.
usermacro.deleteglobal

Description

object usermacro.deleteglobal(array globalMacroIds)

This method allows to delete global macros.

Parameters

(array) IDs of the global macros to delete.

Return values

(object) Returns an object containing the IDs of the deleted global macros under the globalmacroids property.

Examples

Deleting multiple global macros

Delete two global macros.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "usermacro.deleteglobal",
    "params": [
        "32",
        "11"
    ],
    "auth": "3a57200802b24cda67c4e4010b50c065",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "globalmacroids": [
            "32",
            "11"
        ]
    },
    "id": 1
}
```

Source

CUserMacro::deleteGlobal() in frontends/php/include/classes/api/services/CUserMacro.php.

usermacro.get

Description

integer/array usermacro.get(object parameters)

The method allows to retrieve host and global macros according to the given parameters.

Parameters

(object) Parameters defining the desired output.

The method supports the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>globalmacro</td>
<td>flag</td>
<td>Return global macros instead of host macros.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>globalmacroids</td>
<td>string/array</td>
<td>Return only global macros with the given IDs.</td>
</tr>
<tr>
<td>groupids</td>
<td>string/array</td>
<td>Return only host macros that belong to hosts or templates from the given host groups.</td>
</tr>
<tr>
<td>hostids</td>
<td>string/array</td>
<td>Return only macros that belong to the given hosts or templates.</td>
</tr>
<tr>
<td>hostmacroids</td>
<td>string/array</td>
<td>Return only host macros with the given IDs.</td>
</tr>
<tr>
<td>selectGroups</td>
<td>query</td>
<td>Return host groups that the host macro belongs to in the groups property.</td>
</tr>
<tr>
<td>selectHosts</td>
<td>query</td>
<td>Return hosts that the host macro belongs to in the hosts property.</td>
</tr>
<tr>
<td>selectTemplates</td>
<td>query</td>
<td>Return templates that the host macro belongs to in the templates property.</td>
</tr>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Sort the result by the given properties.</td>
</tr>
<tr>
<td>countOutput</td>
<td>boolean</td>
<td>These parameters being common for all get methods are described in detail in the reference commentary page.</td>
</tr>
<tr>
<td>editable</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>excludeSearch</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>filter</td>
<td>object</td>
<td></td>
</tr>
</tbody>
</table>
### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>limit</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>output</td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>preservekeys</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>search</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>searchByAny</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>searchWildcardsEnabled</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>sortorder</td>
<td>string/array</td>
<td></td>
</tr>
<tr>
<td>startSearch</td>
<td>boolean</td>
<td></td>
</tr>
</tbody>
</table>

### Return Values

(integer/array) Returns either:

- an array of objects;
- the count of retrieved objects, if the `countOutput` parameter has been used.

### Examples

#### Retrieving host macros for a host

Retrieve all host macros defined for host "10198".

**Request:**

```json
{
    "jsonrpc": "2.0",
    "method": "usermacro.get",
    "params": {
        "output": "extend",
        "hostids": "10198"
    },
    "auth": "0381ed7b1735e6a5436ee9eae09e6879e",
    "id": 1
}
```

**Response:**

```json
{
    "jsonrpc": "2.0",
    "result": [
        {
            "hostmacroid": "9",
            "hostid": "10198",
            "macro": "{$INTERFACE}"
        },
        {
            "hostmacroid": "11",
            "hostid": "10198",
            "macro": "{$SNMP_COMMUNITY}"
        }
    ],
    "id": 1
}
```

#### Retrieving global macros

Retrieve all global macros.

**Request:**

```json
{
    "jsonrpc": "2.0",
    "method": "usermacro.get",
    "params": {
        "output": "extend",
    }
}
```
"globalmacro": true
},
"auth": "038e1d7b1735c6a5436ee9eae095879e",
"id": 1
}

Response:
{
  "jsonrpc": "2.0",
  "result": [
    {
      "globalmacroid": "6",
      "macro": "{$SNMP_COMMUNITY}",
      "value": "public"
    },
  ],
  "id": 1
}

Source
CUserMacro::get() in frontends/php/include/classes/api/services/CUserMacro.php.

**usermacro.update**

**Description**

object usermacro.update(object/array hostMacros)

This method allows to update existing host macros.

**Parameters**

(object/array) Host macro properties to be updated.

The hostmacroid property must be defined for each host macro, all other properties are optional. Only the passed properties will be updated, all others will remain unchanged.

**Return values**

(object) Returns an object containing the IDs of the updated host macros under the hostmacroids property.

**Examples**

Changing the value of a host macro

Change the value of a host macro to "public".

Request:

```json
{
  "jsonrpc": "2.0",
  "method": "usermacro.update",
  "params": {
    "hostmacroid": "1",
    "value": "public"
  },
  "auth": "038e1d7b1735c6a5436ee9eae095879e",
  "id": 1
}
```

Response:

```json
{
  "jsonrpc": "2.0",
  "result": {
    "hostmacroids": [
      "1"
    ]
  }
}
```
usermacro.updateglobal

Description

object usermacro.updateglobal(object/array globalMacros)

This method allows to update existing global macros.

Parameters

(object/array) Global macro properties to be updated.

The globalmacroid property must be defined for each global macro, all other properties are optional. Only the passed properties will be updated, all others will remain unchanged.

Return values

(object) Returns an object containing the IDs of the updated global macros under the globalmacroids property.

Examples

Changing the value of a global macro

Change the value of a global macro to "public".

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "usermacro.updateglobal",
    "params": {
        "globalmacroid": "1",
        "value": "public"
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "globalmacroids": [
            "1"
        ]
    },
    "id": 1
}
```

Source

CUserMacro::updateGlobal() in frontends/php/include/classes/api/services/CUserMacro.php.

Value map

This class is designed to work with value maps.

Object references:

- Value map
Available methods:

- `valuemap.create` - creating new value maps
- `valuemap.delete` - deleting value maps
- `valuemap.get` - retrieving value maps
- `valuemap.update` - updating value maps

> Value map object

The following objects are directly related to the `valuemap` API.

Value map

The value map object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>valuemapid</td>
<td>string</td>
<td>(readonly) ID of the value map.</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>Name of the value map.</td>
</tr>
<tr>
<td>mappings</td>
<td>array</td>
<td>Value mappings for current value map. The mapping object is described in detail below.</td>
</tr>
</tbody>
</table>

Note that for some methods (update, delete) the required/optional parameter combination is different.

Value mappings

The value mappings object defines value mappings of the value map. It has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>string</td>
<td>Original value.</td>
</tr>
<tr>
<td>newvalue</td>
<td>string</td>
<td>Value to which the original value is mapped to.</td>
</tr>
</tbody>
</table>

`valuemap.create`

Description

`object valuemap.create(object/array valuemaps)`

This method allows to create new value maps.

Parameters

(object/array) Value maps to create.

The method accepts value maps with the standard value map properties.

Return values

(object) Returns an object containing the IDs of the created value maps the `valuemapids` property. The order of the returned IDs matches the order of the passed value maps.

Examples

Creating a value map

Create one value map with two mappings.

Request:
```json
{
    "jsonrpc": "2.0",
    "method": "valuemap.create",
    "params": {
        "name": "Service state",
        "mappings": [
            {
                "value": "0",
                "newvalue": "Down"
            },
            {
                "value": "1",
                "newvalue": "Up"
            }
        ]
    },
    "auth": "57562fd409b3b3b9a4d916d45207bbcb",
    "id": 1
}
```

Response:
```json
{
    "jsonrpc": "2.0",
    "result": {
        "valuemapids": ["1"]
    },
    "id": 1
}
```

Source

CValueMap::create() in frontends/php/include/classes/api/services/CValueMap.php.

**valuemap.delete**

Description

object valuemap.delete(array valuemapids)

This method allows to delete value maps.

Parameters

(array) IDs of the value maps to delete.

Return values

(object) Returns an object containing the IDs of the deleted value maps under the valuemapids property.

Examples

Deleting multiple value maps

Delete two value maps.

Request:
```json
{
    "jsonrpc": "2.0",
    "method": "valuemap.delete",
    "params": [
        "1",
        "2"
    ],
    "auth": "57562fd409b3b3b9a4d916d45207bbcb",
    "id": 1
}
```
Response:
{
    "jsonrpc": "2.0",
    "result": {
        "valuemapids": [
            "1",
            "2"
        ]
    },
    "id": 1
}

Source
CValueMap::delete() in frontends/php/include/classes/api/services/CValueMap.php.

valuemap.get

Description
integer/array valuemap.get(object parameters)
The method allows to retrieve value maps according to the given parameters.

Parameters
(object) Parameters defining the desired output.

The method supports the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>valuemapids</td>
<td>string/array</td>
<td>Return only value maps with the given IDs.</td>
</tr>
<tr>
<td>selectMappings</td>
<td>query</td>
<td>Return the value mappings for current value map in the mappings property. Supports count.</td>
</tr>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Sort the result by the given properties. Possible values are: valuemapid, name.</td>
</tr>
<tr>
<td>countOutput</td>
<td>boolean</td>
<td>These parameters being common for all get methods are described in detail in the reference commentary.</td>
</tr>
<tr>
<td>editable</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>excludeSearch</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>filter</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>limit</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>output</td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>preservekeys</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>search</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>searchByAny</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>searchWildcards</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>sortorder</td>
<td>string/array</td>
<td></td>
</tr>
<tr>
<td>startSearch</td>
<td>boolean</td>
<td></td>
</tr>
</tbody>
</table>

Return values

(integer/array) Returns either:

- an array of objects;
- the count of retrieved objects, if the countOutput parameter has been used.

Examples

Retrieving value maps

Retrieve all configured value maps.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "valuemap.get",
    "params": {
        "output": "extend"
    },
    "auth": "57562fd409b3b3b9a4d916d45207bbcb",
    "id": 1
}
```

Response:

```json
{
    "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
}
```

Retrieve one value map with its mappings.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "valuemap.get",
    "params": {
        "output": "extend",
        "selectMappings": "extend",
        "valuemapids": ["4"]
    },
    "auth": "57562fd409b3b9a4d916d45207bbcb",
    "id": 1
}
```
Response:
{
    "jsonrpc": "2.0",
    "result": [
        {
            "valuemapid": "4",
            "name": "APC Battery Replacement Status",
            "mappings": [
                {
                    "value": "1",
                    "newvalue": "unknown"
                },
                {
                    "value": "2",
                    "newvalue": "notInstalled"
                },
                {
                    "value": "3",
                    "newvalue": "ok"
                },
                {
                    "value": "4",
                    "newvalue": "failed"
                },
                {
                    "value": "5",
                    "newvalue": "highTemperature"
                },
                {
                    "value": "6",
                    "newvalue": "replaceImmediately"
                },
                {
                    "value": "7",
                    "newvalue": "lowCapacity"
                }
            ]
        }
    ],
    "id": 1
}

Source
CValueMap::get() in frontends/php/include/classes/api/services/CValueMap.php.

valuemap.update

Description
object valuemap.update(object/array valuemaps)
This method allows to update existing value maps.

Parameters
(object/array) Value map properties to be updated.

The valuemapid property must be defined for each value map, all other properties are optional. Only the passed properties will be updated, all others will remain unchanged.

Return values
Returns an object containing the IDs of the updated value maps under the valuemapids property.

Examples

Changing value map name

Change value map name to "Device status".

Request:

```json
{
   "jsonrpc": "2.0",
   "method": "valuemap.update",
   "params": {
      "valuemapid": "2",
      "name": "Device status"
   },
   "auth": "57562fd409b3b3b9a4d916d45207bbcb",
   "id": 1
}
```

Response:

```json
{
   "jsonrpc": "2.0",
   "result": {
      "valuemapids": [
         "2"
      ],
      "id": 1
   }
}
```

Changing mappings for one value map.

Request:

```json
{
   "jsonrpc": "2.0",
   "method": "valuemap.update",
   "params": {
      "valuemapid": "2",
      "mappings": [
         {
            "value": "0",
            "newvalue": "Online"
         },
         {
            "value": "1",
            "newvalue": "Offline"
         }
      ],
      "auth": "57562fd409b3b3b9a4d916d45207bbcb",
      "id": 1
   }
}
```

Response:

```json
{
   "jsonrpc": "2.0",
   "result": {
      "valuemapids": [
         "2"
      ],
      "id": 1
   }
}
```
Web scenario

This class is designed to work with web scenarios.

Object references:

- Web scenario
- Scenario step

Available methods:

- `httptest.create` - creating new web scenarios
- `httptest.delete` - deleting web scenarios
- `httptest.get` - retrieving web scenarios
- `httptest.update` - updating web scenarios

> Web scenario object

The following objects are directly related to the webcheck API.

Web scenario

The web scenario object has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>httptestid</td>
<td>string</td>
<td>(readonly) ID of the web scenario.</td>
</tr>
<tr>
<td>hostid</td>
<td>string</td>
<td>ID of the host that the web scenario belongs to.</td>
</tr>
<tr>
<td>(required)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>Name of the web scenario.</td>
</tr>
<tr>
<td>(required)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>agent</td>
<td>string</td>
<td>User agent string that will be used by the web scenario.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: Zabbix</td>
</tr>
<tr>
<td>applicationid</td>
<td>string</td>
<td>ID of the application that the web scenario belongs to.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Authentication method that will be used by the web scenario.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - (default) none;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - basic HTTP authentication;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 - NTLM authentication.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>delay</td>
<td>string</td>
<td>Execution interval of the web scenario. Accepts seconds, time unit with suffix and user macro. Default: 1m.</td>
</tr>
<tr>
<td>headers</td>
<td>string (deprecated)</td>
<td>HTTP headers that will be sent when performing a request.</td>
</tr>
<tr>
<td>http_password</td>
<td>string</td>
<td>Password used for basic HTTP or NTLM authentication.</td>
</tr>
<tr>
<td>http_proxy</td>
<td>string</td>
<td>Proxy that will be used by the web scenario given as http://[username[:password]@]proxy.example.com[:port].</td>
</tr>
<tr>
<td>http_user</td>
<td>string</td>
<td>User name used for basic HTTP or NTLM authentication.</td>
</tr>
<tr>
<td>nextcheck</td>
<td>timestamp</td>
<td>(readonly) Time of the next web scenario execution. Number of times a web scenario will try to execute each step before failing.</td>
</tr>
<tr>
<td>retries</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>ssl_cert_file</td>
<td>string</td>
<td>Name of the SSL certificate file used for client authentication (must be in PEM format).</td>
</tr>
<tr>
<td>ssl_key_file</td>
<td>string</td>
<td>Name of the SSL private key file used for client authentication (must be in PEM format).</td>
</tr>
<tr>
<td>ssl_key_password</td>
<td>string</td>
<td>SSL private key password.</td>
</tr>
<tr>
<td>status</td>
<td>integer</td>
<td>Whether the web scenario is enabled. Possible values are: 0 - (default) enabled; 1 - disabled. (readonly) ID of the parent template web scenario.</td>
</tr>
<tr>
<td>templateid</td>
<td>string</td>
<td></td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>variables</td>
<td>string (deprecated)</td>
<td>Web scenario variables.</td>
</tr>
<tr>
<td>verify_host</td>
<td>integer</td>
<td>Whether to verify that the host name specified in the SSL certificate matches the one used in the scenario.</td>
</tr>
<tr>
<td></td>
<td>array of HTTP fields</td>
<td>Possible values are: 0 - (default) skip host verification; 1 - verify host.</td>
</tr>
<tr>
<td>verify_peer</td>
<td>integer</td>
<td>Whether to verify the SSL certificate of the web server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values are: 0 - (default) skip peer verification; 1 - verify peer.</td>
</tr>
</tbody>
</table>

Note that for some methods (update, delete) the required/optional parameter combination is different.

Scenario step

The scenario step object defines a specific web scenario check. It has the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpstepid</td>
<td>string (readonly)</td>
<td>(readonly) ID of the scenario step.</td>
</tr>
<tr>
<td>name</td>
<td>string (required)</td>
<td>Name of the scenario step.</td>
</tr>
<tr>
<td>no</td>
<td>integer (required)</td>
<td>Sequence number of the step in a web scenario.</td>
</tr>
<tr>
<td>url</td>
<td>string (required)</td>
<td>URL to be checked.</td>
</tr>
<tr>
<td>follow_redirects</td>
<td>integer</td>
<td>Whether to follow HTTP redirects.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Possible values are: 0 - don’t follow redirects; 1 - (default) follow redirects.</td>
</tr>
<tr>
<td>headers</td>
<td>string (deprecated)</td>
<td>HTTP headers that will be sent when performing a request.</td>
</tr>
<tr>
<td></td>
<td>array of HTTP fields</td>
<td>Scenario step headers will overwrite headers specified for the web scenario.</td>
</tr>
<tr>
<td>Property</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>httptestid</td>
<td>string</td>
<td>(readonly) ID of the web scenario that the step belongs to. HTTP POST variables as a string (raw post data) or as an array of HTTP fields.</td>
</tr>
<tr>
<td>posts</td>
<td>string array of</td>
<td>HTTP POST variables as a string (raw post data) or as an array of HTTP fields (form field data).</td>
</tr>
<tr>
<td>required</td>
<td>string</td>
<td>Text that must be present in the response.</td>
</tr>
<tr>
<td>retrieve_mode</td>
<td>integer</td>
<td>Part of the HTTP response that the scenario step must retrieve. Possible values are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 - (default) only body; 1 - only headers. Ranges of required HTTP status codes separated by commas.</td>
</tr>
<tr>
<td>status_codes</td>
<td>string</td>
<td>Request timeout in seconds. Accepts seconds, time unit with suffix and user macro. Default: 15s. Maximum: 1h. Minimum: 1s.</td>
</tr>
<tr>
<td>timeout</td>
<td>string</td>
<td></td>
</tr>
<tr>
<td>variables</td>
<td>string (deprecated)</td>
<td>Scenariostep variables. String data type for headers and variables is deprecated and will be removed in future versions.</td>
</tr>
<tr>
<td>query_fields</td>
<td>array of HTTP</td>
<td>Query fields - array of HTTP fields that will be added to URL when performing a request.</td>
</tr>
</tbody>
</table>

**Attention:**
Both string and array of HTTP fields types are allowed for headers and variables fields of both web scenario and web scenario step object.
String data type for headers and variables is deprecated and will be removed in future versions.

**HTTP field**
The HTTP field object defines a name and value that is used to specify variable, HTTP header, POST form field data of query field data. It has the following properties.
<table>
<thead>
<tr>
<th>Property</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>string</td>
<td>Name of header / variable / POST or GET field.</td>
</tr>
<tr>
<td>value</td>
<td>string</td>
<td>Value of header / variable / POST or GET field.</td>
</tr>
</tbody>
</table>

**httpertest.create**

**Description**

**object httpertest.create(object/array webScenarios)**

This method allows to create new web scenarios.

**Note:**
Creating a web scenario will automatically create a set of web monitoring items.

**Parameters**

(object/array) Web scenarios to create.

Additionally to the standard web scenario properties, the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>steps</td>
<td>array</td>
<td>Web scenario steps.</td>
</tr>
</tbody>
</table>

**Return values**

(object) Returns an object containing the IDs of the created web scenarios under the `httpertestids` property. The order of the returned IDs matches the order of the passed web scenarios.

**Examples**

**Creating a web scenario**

Create a web scenario to monitor the company home page. The scenario will have two steps, to check the home page and the "About" page and make sure they return the HTTP status code 200.

**Request:**

```json
{
   "jsonrpc": "2.0",
   "method": "httpertest.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
         }
      
   },
   "auth": "038e1d7b1735c6a5436ee9eae095879e",
   "id": 1
}
```
Response:
{
    "jsonrpc": "2.0",
    "result": {
        "httptestids": [
            "5"
        ]
    },
    "id": 1
}

See also
• Scenario step

Source
CHttpTest::create() in frontends/php/include/classes/api/services/CHttpTest.php.

**httptest.delete**

Description

**object httptest.delete(array webScenarioIds)**

This method allows to delete web scenarios.

Parameters

(array) IDs of the web scenarios to delete.

Return values

(object) Returns an object containing the IDs of the deleted web scenarios under the **httptestids** property.

Examples

Deleting multiple web scenarios

Delete two web scenarios.

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "httptest.delete",
    "params": [
        2,
        3
    ],
    "auth": "3a57200802b24cda67c4e4010b50c065",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": {
        "httptestids": [
            "2",
            "3"
        ]
    },
    "id": 1
}
```

Source

CHttpTest::delete() in frontends/php/include/classes/api/services/CHttpTest.php.
**httptest.get**

Description

integer/array `httptest.get(object parameters)`

The method allows to retrieve web scenarios according to the given parameters.

Parameters

(object) Parameters defining the desired output.

The method supports the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>applicationids</td>
<td>string/array</td>
<td>Return only web scenarios that belong to the given applications.</td>
</tr>
<tr>
<td>groupids</td>
<td>string/array</td>
<td>Return only web scenarios that belong to the given host groups.</td>
</tr>
<tr>
<td>hostids</td>
<td>string/array</td>
<td>Return only web scenarios that belong to the given hosts.</td>
</tr>
<tr>
<td>httptestids</td>
<td>string/array</td>
<td>Return only web scenarios with the given IDs.</td>
</tr>
<tr>
<td>inherited</td>
<td>boolean</td>
<td>If set to true return only web scenarios inherited from a template.</td>
</tr>
<tr>
<td>monitored</td>
<td>boolean</td>
<td>If set to true return only enabled web scenarios that belong to monitored hosts.</td>
</tr>
<tr>
<td>templated</td>
<td>boolean</td>
<td>If set to true return only web scenarios that belong to templates.</td>
</tr>
<tr>
<td>templateids</td>
<td>string/array</td>
<td>Return only web scenarios that belong to the given templates.</td>
</tr>
<tr>
<td>expandName</td>
<td>flag</td>
<td>Expand macros in the name of the web scenario.</td>
</tr>
<tr>
<td>expandStepName</td>
<td>flag</td>
<td>Expand macros in the names of scenario steps.</td>
</tr>
<tr>
<td>selectHosts</td>
<td>query</td>
<td>Return the host that the web scenario belongs to as an array in the hosts property.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>---------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>selectSteps</td>
<td>query</td>
<td>Return web scenario steps in the steps property.</td>
</tr>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Sort the result by the given properties. Possible values are: httptestid and name. These parameters being common for all get methods are described in detail in the reference commentary.</td>
</tr>
<tr>
<td>countOutput</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>editable</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>excludeSearch</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>filter</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>limit</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>output</td>
<td>query</td>
<td></td>
</tr>
<tr>
<td>preservekeys</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>search</td>
<td>object</td>
<td></td>
</tr>
<tr>
<td>searchByAny</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>searchWildcardsEnabled</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>sortorder</td>
<td>string/array</td>
<td></td>
</tr>
<tr>
<td>startSearch</td>
<td>boolean</td>
<td></td>
</tr>
</tbody>
</table>

Return values
(integer/array) Returns either:

- an array of objects;
- the count of retrieved objects, if the countOutput parameter has been used.

Examples

Retrieving a web scenario

Retrieve all data about web scenario "4".

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "httptest.get",
    "params": {
        "output": "extend",
        "selectSteps": "extend",
        "httptestids": "9"
    },
    "auth": "038e1d7b1735c6a5436ee9eae095879e",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": [
        
```
"httptestid": "9",
"name": "Homepage check",
"applicationid": "0",
"nextcheck": "0",
"delay": "1m",
"status": "0",
"variables": [],
"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",
"headers": [],
"steps": [
    {
        "httpstepid": "36",
        "httptestid": "9",
        "name": "Homepage",
        "no": "1",
        "url": "http://example.com",
        "timeout": "15s",
        "posts": "",
        "required": "",
        "status_codes": "200",
        "variables": [
            {
                "name": "\{var\}",
                "value": "12"
            }
        ],
        "follow_redirects": "1",
        "retrieve_mode": "0",
        "headers": [],
        "query_fields": []
    },
    {
        "httpstepid": "37",
        "httptestid": "9",
        "name": "Homepage / About",
        "no": "2",
        "url": "http://example.com/about",
        "timeout": "15s",
        "posts": "",
        "required": "",
        "status_codes": "200",
        "variables": [],
        "follow_redirects": "1",
        "retrieve_mode": "0",
        "headers": [],
        "query_fields": []
    }
],
See also

- Host
- Scenario step

Source

CHttpTest::get() in frontends/php/include/classes/api/services/CHttpTest.php.

**httpTest.update**

**Description**

object httpTest.update(object/array webScenarios)

This method allows to update existing web scenarios.

**Parameters**

(object/array) Web scenario properties to be updated.

The `httptestid` property must be defined for each web scenario, all other properties are optional. Only the passed properties will be updated, all others will remain unchanged.

Additionally to the standard web scenario properties, the method accepts the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>steps</td>
<td>array</td>
<td>Scenario steps to replace existing steps.</td>
</tr>
</tbody>
</table>

**Return values**

(object) Returns an object containing the IDs of the updated web scenarios under the `httptestid` property.

**Examples**

Enabling a web scenario

Enable a web scenario, that is, set its status to “0”.

**Request:**

```json
{
   "jsonrpc": "2.0",
   "method": "httpTest.update",
   "params": {
      "httptestid": "5",
      "status": 0
   },
   "auth": "700ca65537074ec963db7efabda78259",
   "id": 1
}
```

**Response:**

```json
{
   "jsonrpc": "2.0",
   "result": {
      "httptestids": [
      "5"
   ],
   "id": 1
}
```

See also

- Scenario step
Appendix 1. Reference commentary

Notation  Data types

The Zabbix API supports the following data types as input:

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>boolean</td>
<td>A boolean value, accepts either true or false.</td>
</tr>
<tr>
<td>flag</td>
<td>The value is considered to be true if it is passed and not equal to null; otherwise, it is considered to be false.</td>
</tr>
<tr>
<td>integer</td>
<td>A whole number.</td>
</tr>
<tr>
<td>float</td>
<td>A floating point number.</td>
</tr>
<tr>
<td>string</td>
<td>A text string.</td>
</tr>
<tr>
<td>text</td>
<td>A longer text string.</td>
</tr>
<tr>
<td>timestamp</td>
<td>A Unix timestamp.</td>
</tr>
<tr>
<td>array</td>
<td>An ordered sequence of values, that is, a plain array.</td>
</tr>
<tr>
<td>object</td>
<td>An associative array.</td>
</tr>
<tr>
<td>query</td>
<td>A value which defines, what data should be returned.</td>
</tr>
</tbody>
</table>

Can be defined as an array of property names to return only specific properties, or as one of the predefined values:
- extend - returns all object properties;
- count - returns the number of retrieved records, supported only by certain subselects.

Attention:
Zabbix API always returns values as strings or arrays only.

Property labels

Some of the objects properties are marked with short labels to describe their behavior. The following labels are used:

- readonly - the value of the property is set automatically and cannot be defined or changed by the client;
- constant - the value of the property can be set when creating an object, but cannot be changed after.

Reserved ID value “0”  Reserved ID value “0” can be used to filter elements and to remove referenced objects. For example, to remove a referenced proxy from a host, proxy_hostid should be set to 0 ("proxy_hostid": "0") or to filter hosts monitored by server option proxyids should be set to 0 ("proxyids": "0").

Common “get” method parameters  The following parameters are supported by all get methods:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>countOutput</td>
<td>boolean</td>
<td>Return the number of records in the result instead of the actual data.</td>
</tr>
<tr>
<td>editable</td>
<td>boolean</td>
<td>If set to true return only objects that the user has write permissions to.</td>
</tr>
<tr>
<td>excludeSearch</td>
<td>boolean</td>
<td>Return results that do not match the criteria given in the search parameter.</td>
</tr>
<tr>
<td>filter</td>
<td>object</td>
<td>Return only those results that exactly match the given filter.</td>
</tr>
<tr>
<td>limit</td>
<td>integer</td>
<td>Limit the number of records returned.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>output</td>
<td>query</td>
<td>Object properties to be returned.</td>
</tr>
<tr>
<td>preservekeys</td>
<td>boolean</td>
<td>Use IDs as keys in the resulting array.</td>
</tr>
<tr>
<td>search</td>
<td>object</td>
<td>Return results that match the given pattern (case-insensitive).</td>
</tr>
<tr>
<td>searchByAny</td>
<td>boolean</td>
<td>Supports only fields of string and text data type.</td>
</tr>
<tr>
<td>searchWildcardsEnabled</td>
<td>boolean</td>
<td>If set to true enables the use of &quot;*&quot; as a wildcard character in the search parameter.</td>
</tr>
<tr>
<td>sortfield</td>
<td>string/array</td>
<td>Sort the result by the given properties. Refer to a specific API get method description for a list of properties that can be used for sorting. Macros are not expanded before sorting.</td>
</tr>
<tr>
<td>sortOrder</td>
<td>string/array</td>
<td>Order of sorting. If an array is passed, each value will be matched to the corresponding property given in the sortfield parameter. Possible values are: ASC (default) ascending; DESC - descending.</td>
</tr>
<tr>
<td>startSearch</td>
<td>boolean</td>
<td>The search parameter will compare the beginning of fields, that is, perform a LIKE &quot;%%&quot; search instead. Ignored if searchWildcardsEnabled is set to true.</td>
</tr>
</tbody>
</table>

**Examples**  
User permission check

Does the user have permission to write to hosts whose names begin with "MySQL" or "Linux"?

**Request:**

```json
{
  "jsonrpc": "2.0",
  "method": "host.get",
  "params": {
    "countOutput": true,
    "search": {
      "host": ["MySQL", "Linux"]
    },
    "editable": true,
    "startSearch": true,
    "searchByAny": true
  },
  "auth": "766b71ee543230a1182ca5c44d353e36",
  "id": 1
}
```

**Response:**

```json
{
  "jsonrpc": "2.0",
  "result": "0",
  "id": 1
}
```
Mismatch counting

Count the number of hosts whose names do not contain the substring "ubuntu"

Request:

```json
{
    "jsonrpc": "2.0",
    "method": "host.get",
    "params": {
        "countOutput": true,
        "search": {
            "host": "ubuntu"
        },
        "excludeSearch": true,
        "auth": "766b71ee543230a1182ca5c44d353e36",
        "id": 1
    }
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": "44",
    "id": 1
}
```

Searching for hosts using wildcards

Find hosts whose name contains word "server" and have interface ports "10050" or "10071". Sort the result by host name in descending order and limit it to 5 hosts.

Request:

```json
{
    "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
    },
    "auth": "766b71ee543230a1182ca5c44d353e36",
    "id": 1
}
```

Response:

```json
{
    "jsonrpc": "2.0",
    "result": [
```
Searching for hosts using wildcards with "preservekeys"

If you add the parameter "preservekeys" to the previous request, the result is returned as an associative array, where the keys are the id of the objects.

Request:

```json
{
    "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
},
"auth": "766b71ee543230a1182ca5c44d353e36",
"id": 1
}

Response:
{
    "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"
            }
            ]
        }
    }
}
Appendix 2. Changes from 3.4 to 4.0

Backward incompatible changes  General

Changes:
*ZBXNEXT-4247* dropped support of the deprecated methods *user.updateprofile, user.addmedia, user.updatemedia, user.deletemedia, usergroup.massadd, usergroup.massupdate and usermedia.get*

*ZBXNEXT-4175* E-mail values in API methods *user.get, user.create and user.update* are represented as array if type of *Media type* is e-mail.

*ZBX-3783* proxy.delete: proxies cannot be deleted when are used in actions

*ZBX-18998* added more strict validation for JSON-RPC structure.

action

Changes:
*ZBXNEXT-413* renamed property *maintenance_mode* to *pause_suppressed*.

dashboard

Changes:
*ZBXNEXT-4516* renamed dashboard widget types: *actlog => actionlog, dscvry => discovery, favgrph => favgraphs, favmap => favmaps, favscr => favscreens, hoststat => problemhosts, navigationtree => navtree, stszbx => systeminfo, sysmap => map, syssum => problemsbysv and webovr => web*

*ZBXNEXT-4588* added new dashboard widget type: *svggraph*

drule

Changes:
*ZBX-3783* discovery rules cannot be deleted when are used in actions

user

Changes:
*ZBXNEXT-4573* user.login: password field is mandatory when HTTP authentication is enabled.

*ZBXNEXT-4573* user.create: password field can be omitted if user belongs only to groups that have LDAP access.

*ZBXNEXT-4573* user.update: password field can be empty string if user belongs only to groups that have LDAP access.

usergroup

Changes:
*ZBXNEXT-4573* changed *gui_access* type 2 → 3 - ”disable access to the frontend”.

*ZBXNEXT-4573* added *gui_access* type 2 - ”use LDAP authentication”.

Other changes and bug fixes  General

Changes:
*ZBXNEXT-4426* added a new task API introducing a new method *task.create*.

*ZBXNEXT-4152* added possibility to filter IDs by zero. For example: *host.get()* with option *{"proxyids": [0]}* will return hosts monitored by server.

apiinfo

Changes:
*ZBX-3783* added strict validation of input parameters for *version* method

action
Changes:
ZBXNEXT-413 changed supported operators for action condition 16: 4 - "in" and 7 - "not in" to new ones 10 - "Yes" and 11 - "No".
ZBXNEXT-2788 added support for not operator in custom expression filter formula
ZBX-3783 added strict validation of input parameters for delete method; added audit

correlation
Changes:
ZBXNEXT-2788 added support for not operator in custom expression filter formula
ZBX-3783 added strict validation of input parameters for delete method; added audit

discoveryrule
Changes:
ZBXNEXT-2788 added support for not operator in custom expression filter formula
ZBXNEXT-2788 added support of value 9 in the filter condition operator

drule
Changes:
ZBX-3783 added strict validation of input parameters for delete method

event
Changes:
ZBXNEXT-413 event.get: added new parameter suppressed.
ZBXNEXT-413 event.get: added new parameter selectSuppressionData that returns list of maintenances in the suppression_data property.
ZBXNEXT-4118 event.get: added a new property evaltype and extended tags property to support new value “<operator>”
ZBXNEXT-4119 event.get: returns only problems and corresponding recovery events that match the tag based permission filters
ZBXNEXT-4588 event.get: added new parameters problem_time_from and problem_time_till

hostprototype
ZBXNEXT-4656 hostprototype.create, hostprototype.update: added strict validation of input parameters and added audit.

item
Changes:
ZBXNEXT-4358 added new item type "HTTP agent".

itemprototype
Changes:
ZBXNEXT-4200 itemprototype.create, itemprototype.update: added possibility to add regular items and web items as master items in master_itemid property.

maintenance
Changes:
ZBXNEXT-413 added new property tags_evaltype.
ZBXNEXT-413 maintenance.create, maintenance.update: added new property tags.
ZBXNEXT-413 maintenance.get: added new option selectTags that returns maintenance problem tags in the tags property.

map
Changes:
ZBXNEXT-413 added new property show_suppressed.

mediatype
Changes:
ZBXNEXT-4144 password field for authentication type "Username and password" was made as optional.

problem
Changes:
ZBXNEXT-413 problem.get: added new parameter suppressed.
ZBXNEXT-413 problem.get: added new parameter selectSuppressionData that returns list of maintenances in the suppression_data property.
ZBXNEXT-4118 problem.get: added a property evaltype and extended tags property to support new value "<operator>"
ZBXNEXT-4119 problem.get: returns only those events that match the tag based permission filters

proxy
Changes:
ZBXNEXT-4411 added a new property auto_compress.

trigger
Changes:
ZBXNEXT-3860 trigger.get: added a new parameters evaltype and tags that allow to filter triggers by tags
ZBXNEXT-4357 trigger.get: added a new selectTriggerDiscovery option that returns the trigger discovery object in the triggerDiscovery property

usergroup
Changes:
ZBXNEXT-4119 usergroup.get: added a new selectTagFilters option that returns the array of the tag based permissions objects in the tag_filters property
ZBXNEXT-4119 usergroup.create and usergroup.update: added a new tag_filters property

Zabbix API changes in 4.0

4.0.34 usergroup
Bug fixes:
ZBX-19857 usergroup.get: dropped support for the non-working option web_gui_access

4.0.32 configuration
Bug fixes:
ZBX-8999 configuration.export: fixed exporting of images separately from other objects

graph
Bug fixes:
ZBX-19388 graph.update: fixed method to properly change values on template graph instead of making a new inherited graph if case user has no permissions to child host or template

graphprototype
Bug fixes:
ZBX-19388 graphprototype.update: fixed method to properly change values on template graph prototype instead of making a new inherited graph prototype if case user has no permissions to child host or template

trigger
Bug fixes:
ZBX-19424 trigger.create: fixed trigger creation on PostgreSQL with host name consisting of only numbers

4.0.17 script
Changes:
ZBX-3783 script.get: added strict validation of input parameters

4.0.16 configuration
Changes:
ZBXNEXT-5271 configuration.import: implemented deleteMissing option for templateLinkage

4.0.13 valuemap
Changes:
ZBX-3783 valuemap.get: added strict validation of input parameters

4.0.8 alert
Changes:
ZBX-11272 alert.get: added support of two new options mediatypeid and sendto in the sortfield parameter

4.0.7 discoveryrule
Bug fixes:
ZBX-10861 discoveryrule.create, discoveryrule.update: changed "username" and "password" fields to optional for HTTP agent type discovery rules and using authentication

httptest
Bug fixes:
ZBX-10861 httptest.create, httptest.update: changed "http_user" and "http_password" fields to optional when using authentication

item
Bug fixes:
ZBX-10861 item.create, item.update: changed "username" and "password" fields to optional for HTTP agent type items and using authentication

itemprototype
Bug fixes:
ZBX-10861 itemprototype.create, itemprototype.update: changed "username" and "password" fields to optional for HTTP agent type item prototypes and using authentication

4.0.2 dservice
Bug fixes:
ZBX-14833 dservice.get: fixed "selectHosts" option to return correct hosts that are monitored by current proxy or server

20. Appendixes

Please use the sidebar to access content in the Appendixes section.
1 Frequently asked questions / Troubleshooting

Frequently asked questions or FAQ.

1. Q: Can I flush/clear the queue (as depicted in Administration → Queue)?
   A: No.
2. Q: How do I migrate from one database to another?
   A: Dump data only (for MySQL, use flag -t or --no-create-info), create the new database using schema files from Zabbix and import the data.
3. Q: I would like to replace all spaces with underscores in my item keys because they worked in older versions but space is not a valid symbol for an item key in 3.0 (or any other reason to mass-modify item keys). How should I do it and what should I beware of?
   A: You may use a database query to replace all occurrences of spaces in item keys with underscores:
      
      update items set key_=replace(key_,'','_');

      Triggers will be able to use these items without any additional modifications, but you might have to change any item references in these locations:
      * Notifications (actions)
      * Map element and link labels
      * Calculated item formulas
4. Q: My graphs have dots instead of lines or empty areas. Why so?
   A: Data is missing. This can happen for a variety of reasons - performance problems on Zabbix database, Zabbix server, network, monitored devices...
5. Q: Zabbix daemons fail to start up with a message Listener failed with error: socket() for [-]:10050 failed with error 22: Invalid argument.
   A: This error arises at attempt to run Zabbix agent compiled on version 2.6.27 or above on a platform with a kernel 2.6.26 and lower. Note that static linking will not help in this case because it is the socket() system call that does not support SOCK_CLOEXEC flag on earlier kernels. ZBX-3395
6. Q: I try to set up a flexible user parameter (one that accepts parameters) with a command that uses a positional parameter like $1, but it doesn’t work (uses item parameter instead). How to solve this?
   A: Use a double dollar sign like \$\$1
7. Q: All dropdowns have a scrollbar and look ugly in Opera 11. Why so?
   A: It’s a known bug in Opera 11.00 and 11.01; see Zabbix issue tracker for more information.
8. Q: How can I change graph background color in a custom theme?
   A: See graph_theme table in the database and theming guide.
9. Q: With DebugLevel 4 I’m seeing messages “Trapper got [] len 0” in server/proxy log - what’s that?
   A: Most likely that is frontend, connecting and checking whether server is still running.
10. Q: My system had the time set in the future and now no data is coming in. How could this be solved?
    A: Clear values of database fields hosts.disable_until*, drules.nextcheck, httptest.nextcheck and restart the server/proxy.
11. Q: Text item values in frontend (when using {ITEM.VALUE} macro and in other cases) are cut/trimmed to 20 symbols. Is that normal?
    A: Yes, there is a hardcoded limit in include/items.inc.php currently. For more information, see Macro functions.

If you haven’t found an answer to your question try Zabbix forum.

2 Installation

1 Database creation

Overview

A Zabbix database must be created during the installation of Zabbix server or proxy.

This section provides instructions for creating a Zabbix database. A separate set of instructions is available for each supported database.

Note:

schema.sql, images.sql and data.sql files are located in the database subdirectory of Zabbix sources. If Zabbix was installed from distribution packages, refer to the distribution documentation.
**Attention:**
For a Zabbix proxy database, **only** `schema.sql` should be imported (no images.sql nor data.sql).

UTF-8 is the only encoding supported by Zabbix. It is known to work without any security flaws. Users should be aware that there are known security issues if using some of the other encodings.

**MySQL**

Character set utf8 and utf8_bin collation is required for Zabbix server to work properly with MySQL database.

```bash
mysql -u root -p<password>
```

```bash
mysql> create database zabbix character set utf8 collate utf8_bin;
mysql> create user 'zabbix'@'localhost' identified by '<password>';
mysql> grant all privileges on zabbix.* to 'zabbix'@'localhost';
mysql> quit;
```

**Attention:**
Zabbix server prior to 4.4 cannot work correctly with newer MariaDB versions out of the box. See [Known issues](#) for required database modifications.

**Warning:**
If you are installing from Zabbix packages, stop here and continue with instructions for Debian/Ubuntu or RHEL/CentOS to import the data into the database.

If you are installing Zabbix from sources, proceed to import the data into the database:

```bash
cd database/mysql
mysql -u zabbix -p<password> zabbix < schema.sql
# stop here if you are creating database for Zabbix proxy
mysql -u zabbix -p<password> zabbix < images.sql
mysql -u zabbix -p<password> zabbix < data.sql
```

**PostgreSQL**

You need to have database user with permissions to create database objects. The following shell command will create user zabbix. Specify password when prompted and repeat password (note, you may first be asked for `sudo` password):

```bash
sudo -u postgres createuser --pwprompt zabbix
```

Now we will setup the database zabbix (last parameter) with the previously created user as the owner (`-O zabbix`).

```bash
sudo -u postgres createdb -O zabbix -E Unicode -T template0 zabbix
```

**Warning:**
If you are installing from Zabbix packages, stop here and continue with instructions for Debian/Ubuntu or RHEL/CentOS to import the initial schema and data into the database.

If you are installing Zabbix from sources, proceed to import the initial schema and data (assuming you are in the root directory of Zabbix sources):

```bash
cd database/postgresql
cat schema.sql | sudo -u zabbix psql zabbix
# stop here if you are creating database for Zabbix proxy
cat images.sql | sudo -u zabbix psql zabbix
cat data.sql | sudo -u zabbix psql zabbix
```

**Attention:**
The above commands are provided as an example that will work in most of GNU/Linux installations. You can use different commands depending on how your system/database is configured, for example: `<br>` `<br>` `psql -U <username>` `<br>` `<br>` If you have troubles setting up the database, please consult your Database administrator.

**Oracle**
We assume that a zabbix database user with password password exists and has permissions to create database objects in ORCL service located on the host Oracle database server with a user shell user having write access to /tmp directory. Zabbix requires a Unicode database character set and a UTF8 national character set. Check current settings:

```sql
sqlplus> select parameter,value from v$nls_parameters where parameter='NLS_CHARACTERSET' or parameter='NLS_NCHAR_CHARACTERSET';
```

If you are creating a database for Zabbix server you need to have images from Zabbix sources on the host where Oracle is running. Copy them to a directory /tmp/zabbix_images on the Oracle host:

```bash
cd /path/to/zabbix-sources
ssh user@oracle_host "mkdir /tmp/zabbix_images"
scp -r misc/images/png_modern user@oracle_host:/tmp/zabbix_images/
```

Now prepare the database:

```bash
cd /path/to/zabbix-sources/database/oracle
sqlplus zabbix/password@oracle_host/ORCL
```

```sql
sqlplus> @schema.sql
# stop here if you are creating database for Zabbix proxy
sqlplus> @images.sql
sqlplus> @data.sql
```

**Note:**
Please set the initialization parameter CURSOR_SHARING=FORCE for best performance.

Now the temporary directory can be removed:

```bash
ssh user@oracle_host "rm -rf /tmp/zabbix_images"
```

### IBM DB2

```bash
db2 "create database zabbix using codeset utf-8 territory us pagesize 32768"
db2batch -d zabbix -f schema.sql
# stop here if you are creating database for Zabbix proxy
db2batch -d zabbix -f images.sql
db2batch -d zabbix -f data.sql
```

**Note:**
It is important to set UTF-8 locale for Zabbix server, Zabbix proxy and the web server running Zabbix frontend. Otherwise text information from Zabbix will be interpreted by IBM DB2 server as non-UTF-8 and will be additionally converted on the way from Zabbix to the database and back. The database will store corrupted non-ASCII characters.

Zabbix frontend uses OFFSET and LIMIT clauses in SQL queries. For this to work, IBM DB2 server must have DB2_COMPATIBILITY_VECTOR variable be set to 3. Run the following command before starting the database server:

```bash
db2set DB2_COMPATIBILITY_VECTOR=3
```

### SQLite

Using SQLite is supported for **Zabbix proxy** only!

The database will be automatically created if it does not exist.

Return to the [installation section](#).

### 2 Repairing Zabbix database character set and collation

MySQL/MariaDB

1. Check the database character set and collation.

For example:

```sql
mysql> SELECT @@character_set_database, @@collation_database;
```

<table>
<thead>
<tr>
<th>@@character_set_database</th>
<th>@@collation_database</th>
</tr>
</thead>
<tbody>
<tr>
<td>utf8mb4</td>
<td>utf8mb4_general_ci</td>
</tr>
</tbody>
</table>

1198
As we see, the character set here is not 'utf8' and collation is not 'utf8_bin', so we need to fix them.

2. Stop Zabbix.

3. Create a backup copy of the database!

4. Fix the character set and collation on database level:
   
   ```sql
   ALTER DATABASE <your DB name> CHARACTER SET utf8 COLLATE utf8_bin;
   ```

   Fixed values:

   ```sql
   mysql> SELECT @@character_set_database, @@collation_database;
   +--------------------------+----------------------+
   | @@character_set_database | @@collation_database |
   +--------------------------+----------------------+
   | utf8                    | utf8_bin             |
   +--------------------------+----------------------+
   ```

5. Load the script to fix character set and collation on table and column level:

   ```sql
   mysql <your DB name> < utf8_convert.sql
   ```

6. Execute the script:

   ```sql
   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;
   ```

   Note that data encoding will be changed on disk. For example, when converting characters like Æ, Ñ, Ö from 'latin1' to 'utf8' they will go from 1 byte to 2 bytes. Thus the repaired database may require more space than before.

7. If no errors - you may want to create a database backup copy with the fixed database.

8. Start Zabbix.

### 3 Elasticsearch setup

**Attention:**

Elasticsearch support is experimental!

Setup procedure considered in this section is applicable to the following Elasticsearch versions: 5.0.x → 6.1.x. In case an earlier or later version of Elasticsearch is used, some functionality may not work as intended.

Zabbix has recently started to support storage of historical data by means of Elasticsearch instead of a database. Users are now given the possibility to choose the storage place for historical data between a compatible database and Elasticsearch.

**Warning:**

If all history data is stored in Elasticsearch, trends are **not** calculated nor stored in the database. With no trends calculated and stored, the history storage period may need to be extended.

**Configuration**

To ensure proper communication between all elements involved make sure server configuration file and frontend configuration file parameters are properly configured.

Zabbix server and frontend

Zabbix server configuration file draft with parameters to be updated:

```yaml
### Option: HistoryStorageURL
# History storage HTTP(S) URL.
#
# Mandatory: no
# Default: HistoryStorageURL=
### Option: HistoryStorageTypes
```
# Comma separated list of value types to be sent to the history storage.
# Mandatory: no
# Default:
# HistoryStorageTypes=uint,dbl,str,log,text

Example parameter values to fill the Zabbix server configuration file with:

HistoryStorageURL=http://test.elasticsearch.lan:9200
HistoryStorageTypes=str,log,text

This configuration forces Zabbix Server to store history values of numeric types in the corresponding database and textual history data in Elasticsearch.

Elasticsearch supports the following item types:

uint,dbl,str,log,text

Supported item type explanation:

<table>
<thead>
<tr>
<th>Item value type</th>
<th>Database table</th>
<th>Elasticsearch type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Numeric (unsigned)</td>
<td>history_uint</td>
<td>uint</td>
</tr>
<tr>
<td>Numeric (float)</td>
<td>history</td>
<td>dbl</td>
</tr>
<tr>
<td>Character</td>
<td>history_str</td>
<td>str</td>
</tr>
<tr>
<td>Log</td>
<td>history_log</td>
<td>log</td>
</tr>
<tr>
<td>Text</td>
<td>history_text</td>
<td>text</td>
</tr>
</tbody>
</table>

Zabbix frontend configuration file (conf/zabbix.conf.php) draft with parameters to be updated:

// Elasticsearch url (can be string if same url is used for all types).
$HISTORY['url'] = [
    'uint' => 'http://localhost:9200',
    'text' => 'http://localhost:9200'
];

// Value types stored in Elasticsearch.
$HISTORY['types'] = ['uint', 'text'];

Example parameter values to fill the Zabbix frontend configuration file with:

$HISTORY['url'] = 'http://test.elasticsearch.lan:9200';
$HISTORY['types'] = ['str', 'text', 'log'];

This configuration forces to store Text, Character and Log history values in Elasticsearch.

It is also required to make $HISTORY global in conf/zabbix.conf.php to ensure everything is working properly (see conf/zabbix.conf.php.example for how to do it):

// Zabbix GUI configuration file.
global $DB, $HISTORY;

Installing Elasticsearch and creating mapping

Final two steps of making things work are installing Elasticsearch itself and creating mapping process.

To install Elasticsearch please refer to Elasticsearch installation guide.

**Note:**
Mapping is a data structure in Elasticsearch (similar to a table in a database). Mapping for all history data types is available here: database/elasticsearch/elasticsearch.map.

**Warning:**
Creating mapping is mandatory. Some functionality will be broken if mapping is not created according to the instruction.

To create mapping for text type send the following request to Elasticsearch:

curl -X PUT "http://your-elasticsearch.here:9200/text" -H 'content-type:application/json' -d '{"text": {"type": "text"}}'
"settings": {
  "index": {
    "number_of_replicas": 1,
    "number_of_shards": 5
  }
},
"mappings": {
  "values": {
    "properties": {
      "itemid": {
        "type": "long"
      },
      "clock": {
        "format": "epoch_second",
        "type": "date"
      },
      "value": {
        "fields": {
          "analyzed": {
            "index": true,
            "type": "text",
            "analyzer": "standard"
          }
        },
        "index": false,
        "type": "text"
      }
    }
  }
},
'

Similar request is required to be executed for Character and Log history values mapping creation with corresponding type correction.

**Note:**
To work with Elasticsearch please refer to [Requirement page](#) for additional information.

**Note:**
Housekeeper is not deleting any data from Elasticsearch.

Storing history data in multiple date-based indices

This section describes additional steps required to work with pipelines and ingest nodes.

To begin with, you must create templates for indices.

**Warning:**
Starting from **Elasticsearch version 5.6** the field "template" is no longer supported.

The example below shows a request for creating uint template (for ES 5.6 or newer delete "template": "uint*",
```
curl -X PUT \nhttp://your-elasticsearch.here:9200/_template/uint_template \n-H 'content-type:application/vnd.elasticsearch+json' \n-d '{
  "template": "uint*",
  "index_patterns": ["uint*"],
  "settings": {
    "index": {
      "number_of_replicas": 1,
      "number_of_shards": 5
    }
  }
}'
```
To create other templates, users should:

- **For ES versions below 5.6**: change the URL (last part is the name of template), change "template" and "index_patterns" fields to match index name and to set valid mapping, which can be taken from database/elasticsearch/elasticsearch.map.

- **For ES 5.6 and newer**: change the URL (last part is the name of template), change "index_patterns" field to match index name and to set valid mapping, which can be taken from database/elasticsearch/elasticsearch.map.

For example, the following command can be used to create a template for text index (for ES 5.6 or newer delete "template" : "text*",):

curl -X PUT \
http://your-elasticsearch.here:9200/_template/text_template \
-H 'content-type:application/json' \
-d '{
   "template": "text*",
   "index_patterns": ["text*"],
   "settings": { 
      "index": { 
         "number_of_replicas": 1,
         "number_of_shards": 5
      }
   },
   "mappings": { 
      "values": { 
         "properties": { 
            "itemid": { 
               "type": "long"
            },
            "clock": { 
               "format": "epoch_second",
               "type": "date"
            },
            "value": { 
               "type": "long"
            }
         }
      }
   }
}'
This is required to allow Elasticsearch to set valid mapping for indices created automatically. Then it is required to create the pipeline definition. Pipeline is some sort of preprocessing of data before putting data in indices. The following command can be used to create pipeline for uint index:

curl -X PUT \
http://your-elasticsearch.here:9200/_ingest/pipeline/uint-pipeline \
-H 'content-type:application/json' \
-d '{
    "description": "daily uint index naming",
    "processors": [
        {
            "date_index_name": {
                "field": "clock",
                "date_formats": ["UNIX"],
                "index_name_prefix": "uint-",
                "date_rounding": "d"
            }
        }
    ]
}'

User can change the rounding parameter ("date_rounding") to set a specific index rotation period. To create other pipelines, user should change the URL (last part is the name of pipeline) and change "index_name_prefix" field to match index name.

See also Elasticsearch documentation.

Additionally, storing history data in multiple date-based indices should also be enabled in the new parameter in Zabbix server configuration:

```
### Option: HistoryStorageDateIndex
# Enable preprocessing of history values in history storage to store values in different indices based on date.
# 0 - disable
# 1 - enable
# Mandatory: no
# Default: HistoryStorageDateIndex=0
```

Troubleshooting

The following steps may help you troubleshoot problems with Elasticsearch setup:

1. Check if the mapping is correct (GET request to required index URL like `http://localhost:9200/uint`).
2. Check if shards are not in failed state (restart of Elasticsearch should help).
3. Check the configuration of Elasticsearch. Configuration should allow access from the Zabbix frontend host and the Zabbix server host.
4. Check Elasticsearch logs.

If you are still experiencing problems with your installation then please create a bug report with all the information from this list (mapping, error logs, configuration, version, etc.)

4 Real-time export of events, item values, trends

Overview

It is possible to configure real-time exporting of trigger events, item values and trends in a newline-delimited JSON format.

Exporting is done into files, where each line of the export file is a JSON object. Value mappings are not applied.

In case of a write error (data cannot be written to the export file or the export file cannot be renamed or a new one cannot be created after renaming it), the data item is dropped and never written to the export file. It is written only in the Zabbix database. Writing data to the export file is resumed when the writing problem is resolved.

Note that before Zabbix 4.0.16, in case of a write error, Zabbix would retry with a 10 second interval until success. This behavior, while ensuring history data equivalence between database and export files resulted in actually stopping monitoring until
the problem with the export file was fixed. Since 4.0.16 the priority is given to continued monitoring rather than keeping the export file in sync with database at all cost.

For precise details on what information is exported, see the export protocol page.

Note that host/item can have no metadata (host groups, host name, item name) if the host/item was removed after the data was received, but before server exported data.

Configuration

Real-time export of trigger events, item values and trends is configured by specifying a directory for the export files - see the ExportDir parameter in server configuration.

Another parameter - ExportFileSize may be used to set the maximum allowed size of an individual export file. When a process needs to write to a file it checks the size of the file first. If it exceeds the configured size limit, the file is renamed by appending .old to its name and a new file with the original name is created.

**Attention:**
A file will be created per each process that will write data (i.e. approximately 4-30 files). As the default size per export file is 1G, keeping large export files may drain the disk space fast.

5 Running Agent as root

Starting with version 4.0.15 systemd service file for Zabbix agent in official packages (https://www.zabbix.com/download) was updated to explicitly include directives for User and Group. Both are set to zabbix.

This means that old functionality of configuring which user Zabbix agent runs as via zabbix_agentd.conf file is bypassed and agent will always run as the user specified in the systemd service file.

To override this new behavior create file /etc/systemd/system/zabbix-agent.service.d/override.conf with the following content.

```
[Service]
User=root
Group=root
```

Reload daemons and restart zabbix-agent service.

```
systemctl daemon-reload
grep restart zabbix-agent
```

For agent2 this completely determines the user that it runs as.

For old agent this only re-enables the functionality of configuring user in zabbix_agentd.conf file. Therefore in order to run zabbix agent as root you still have to edit zabbix_agentd.conf and specify User=root as well as AllowRoot=1 options. More on this here: https://www.zabbix.com/documentation/4.0/manual/appendix/config/zabbix_agentd.

6 Zabbix agent on Microsoft Windows

Configuring agent

Zabbix agent runs as a Windows service.

You can run a single instance of Zabbix agent or multiple instances of the agent on a Microsoft Windows host. A single instance can use the default configuration file C:\zabbix_agentd.conf or a configuration file specified in the command line. In case of multiple instances each agent instance must have its own configuration file (one of the instances can use the default configuration file).

An example configuration file is available in Zabbix source archive as conf/zabbix_agentd.win.conf.

See the configuration file options for details on configuring Zabbix Windows agent.

**Warning:**
Zabbix agent for Windows does not support non-standard Windows configurations where CPUs are distributed non-uniformly across NUMA nodes. If logical CPUs are distributed non-uniformly, then CPU performance metrics may not be available for some CPUs. For example, if there are 72 logical CPUs with 2 NUMA nodes, both nodes must have 36 CPUs each.

Hostname parameter
To perform active checks on a host Zabbix agent needs to have the hostname defined. Moreover, the hostname value set on the agent side should exactly match the "Host name" configured for the host in the frontend.

The hostname value on the agent side can be defined by either the Hostname or HostnameItem parameter in the agent configuration file - or the default values are used if any of these parameters are not specified.

The default value for HostnameItem parameter is the value returned by the "system.hostname" agent key and for Windows platform it returns the NetBIOS host name.

The default value for Hostname is the value returned by the HostnameItem parameter. So, in effect, if both these parameters are unspecified the actual hostname will be the host NetBIOS name; Zabbix agent will use NetBIOS host name to retrieve the list of active checks from Zabbix server and send results to it.

**Attention:**
The system.hostname key always returns the NetBIOS host name which is limited to 15 symbols and in UPPERCASE only - regardless of the length and lowercase/uppercase characters in the real host name.

Starting from Zabbix agent 1.8.6 version for Windows the "system.hostname" key supports an optional parameter - type of the name. The default value of this parameter is "netbios" (for backward compatibility) and the other possible value is "host".

**Attention:**
The system.hostname[host] key always returns the full, real (case sensitive) Windows host name.

So, to simplify the configuration of zabbix_agentd.conf file and make it unified, two different approaches could be used.

1. leave Hostname or HostnameItem parameters undefined and Zabbix agent will use NetBIOS host name as the hostname;
2. leave Hostname parameter undefined and define HostnameItem like this:

   HostnameItem=system.hostname[host]

   and Zabbix agent will use the full, (case sensitive) Windows host name as the hostname.

Host name is also used as part of Windows service name which is used for installing, starting, stopping and uninstalling the Windows service. For example, if Zabbix agent configuration file specifies Hostname=Windows_db_server, then the agent will be installed as a Windows service “Zabbix Agent [Windows_db_server]”. Therefore, to have a different Windows service name for each Zabbix agent instance, each instance must use a different host name.

Installing agent as Windows service

To install a single instance of Zabbix agent with the default configuration file c:\zabbix_agentd.conf:

zabbix_agentd.exe --install

**Attention:**
On a 64-bit system, a 64-bit Zabbix agent version is required for all checks related to running 64-bit processes to work correctly.

If you wish to use a configuration file other than c:\zabbix_agentd.conf, you should use the following command for service installation:

zabbix_agentd.exe --config <your_configuration_file> --install

A full path to the configuration file should be specified.

Multiple instances of Zabbix agent can be installed as services like this:

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

The installed service should now be visible in Control Panel.

Starting agent

To start the agent service, you can use Control Panel or do it from command line.

To start a single instance of Zabbix agent with the default configuration file:

zabbix_agentd.exe --start

To start a single instance of Zabbix agent with another configuration file:

zabbix_agentd.exe --config <your_configuration_file> --start
To start one of multiple instances of Zabbix agent:
```
zabbix_agentd.exe --config <configuration_file_for_this_instance> --start --multiple-agents
```

Stopping agent

To stop the agent service, you can use Control Panel or do it from command line.

To stop a single instance of Zabbix agent started with the default configuration file:
```
zabbix_agentd.exe --stop
```

To stop a single instance of Zabbix agent started with another configuration file:
```
zabbix_agentd.exe --config <your_configuration_file> --stop
```

To stop one of multiple instances of Zabbix agent:
```
zabbix_agentd.exe --config <configuration_file_for_this_instance> --stop --multiple-agents
```

Uninstalling agent Windows service

To uninstall a single instance of Zabbix agent using the default configuration file:
```
zabbix_agentd.exe --uninstall
```

To uninstall a single instance of Zabbix agent using a non-default configuration file:
```
zabbix_agentd.exe --config <your_configuration_file> --uninstall
```

To uninstall multiple instances of Zabbix agent from Windows services:
```
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
```

7 Additional frontend languages

Overview

In order to use any other language than English in Zabbix web interface, its locale should be installed on the web server. Additionally, the PHP gettext extension is required for the translations to work.

If a locale is installed, a language becomes available in the language selector in Zabbix web interface. Languages for which locales are not installed are greyed out and cannot be selected.

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.

Installing Zabbix

If installing Zabbix directly from Zabbix git repository, translation files should be generated manually. To generate translation files, run:
```
make gettext
locale/make_mo.sh
```

This step is not needed when installing Zabbix from packages or source tar.gz files.
3 Daemon configuration

1 Zabbix server

Overview

This section lists parameters supported in a Zabbix server configuration file (zabbix_server.conf). Note that:

- The default values reflect daemon defaults, not the values in the shipped configuration files;
- Zabbix supports configuration files only in UTF-8 encoding without BOM;
- Comments starting with “#” are only supported in the beginning of the line.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Mandatory</th>
<th>Range</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AlertScriptsPath</td>
<td>no</td>
<td>/usr/local/share/zabbix/alertscripts</td>
<td></td>
<td>Location of custom alert scripts (depends on compile-time installation variable datadir).</td>
</tr>
<tr>
<td>AllowRoot</td>
<td>no</td>
<td>0</td>
<td>0</td>
<td>Allow the server to run as 'root'. If disabled and the server is started by 'root', the server will try to switch to the 'zabbix' user instead. Has no effect if started under a regular user. 0 - do not allow 1 - allow</td>
</tr>
<tr>
<td>CacheSize</td>
<td>no</td>
<td>128K-64G</td>
<td>8M</td>
<td>Size of configuration cache, in bytes. Shared memory size for storing host, item and trigger data. The maximum value of this parameter was increased from 8GB to 64GB in Zabbix 4.0.21.</td>
</tr>
<tr>
<td>CacheUpdateFrequency</td>
<td>no</td>
<td>1-3600</td>
<td>60</td>
<td>How often Zabbix will perform update of configuration cache, in seconds. See also runtime control options.</td>
</tr>
<tr>
<td>DBHost</td>
<td>no</td>
<td>localhost</td>
<td></td>
<td>Database host name. In case of MySQL localhost or empty string results in using a socket. In case of PostgreSQL only empty string results in attempt to use socket.</td>
</tr>
<tr>
<td>DBName</td>
<td>yes</td>
<td></td>
<td></td>
<td>Database name.</td>
</tr>
<tr>
<td>DBPassword</td>
<td>no</td>
<td></td>
<td></td>
<td>Database password. Comment this line if no password is used.</td>
</tr>
<tr>
<td>DBPort</td>
<td>no</td>
<td>1024-65535</td>
<td></td>
<td>Database port when not using local socket.</td>
</tr>
<tr>
<td>DBSchema</td>
<td>no</td>
<td></td>
<td></td>
<td>Schema name. Used for IBM DB2 and PostgreSQL.</td>
</tr>
<tr>
<td>DBSocket</td>
<td>no</td>
<td></td>
<td></td>
<td>Path to MySQL socket file.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Mandatory</td>
<td>Range</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------</td>
<td>-----------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DBUser</td>
<td>no</td>
<td></td>
<td></td>
<td>Database user.</td>
</tr>
<tr>
<td>DebugLevel</td>
<td>no</td>
<td>0-5</td>
<td>3</td>
<td>Specifies debug level: 0 - basic information about starting and stopping of Zabbix processes, 1 - critical information, 2 - error information, 3 - warnings, 4 - for debugging (produces lots of information), 5 - extended debugging (produces even more information). See also runtime control options.</td>
</tr>
<tr>
<td>ExportDir</td>
<td>no</td>
<td></td>
<td></td>
<td>Directory for real-time export of events, history and trends in newline-delimited JSON format. If set, enables real-time export. This parameter is supported since Zabbix 4.0.0.</td>
</tr>
<tr>
<td>ExportFileSize</td>
<td>no</td>
<td>1M-1G</td>
<td>1G</td>
<td>Maximum size per export file in bytes. Only used for rotation if ExportDir is set. This parameter is supported since Zabbix 4.0.0.</td>
</tr>
<tr>
<td>ExternalScripts</td>
<td>no</td>
<td>/usr/local/share/zabbix/externalscripts</td>
<td></td>
<td>Location of external scripts (depends on compile-time installation variable datadir).</td>
</tr>
<tr>
<td>Fping6Location</td>
<td>no</td>
<td>/usr/sbin/fping6</td>
<td></td>
<td>Location of fping6. Make sure that fping6 binary has root ownership and SUID flag set. Make empty (&quot;Fping6Location=&quot;) if your fping utility is capable to process IPv6 addresses.</td>
</tr>
<tr>
<td>FpingLocation</td>
<td>no</td>
<td>/usr/sbin/fping</td>
<td></td>
<td>Location of fping. Make sure that fping binary has root ownership and SUID flag set!</td>
</tr>
<tr>
<td>HistoryCacheSize</td>
<td>no</td>
<td>128K-2G</td>
<td>16M</td>
<td>Size of history cache, in bytes. Shared memory size for storing history data.</td>
</tr>
<tr>
<td>HistoryIndexCacheSize</td>
<td>no</td>
<td>128K-2G</td>
<td>4M</td>
<td>Size of history index cache, in bytes. Shared memory size for indexing history data stored in history cache. The index cache size needs roughly 100 bytes to cache one item. This parameter is supported since Zabbix 3.0.0.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Mandatory</td>
<td>Range</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------</td>
<td>-------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>HistoryStorageDateIndex</td>
<td>no</td>
<td></td>
<td>0</td>
<td>Enable preprocessing of history values in history storage to store values in different indices based on date: 0 - disable 1 - enable</td>
</tr>
<tr>
<td>HistoryStorageURL</td>
<td>no</td>
<td></td>
<td></td>
<td>History storage HTTP[S] URL. This parameter is used for Elasticsearch setup.</td>
</tr>
<tr>
<td>HistoryStorageTypes</td>
<td>no</td>
<td>uint,dbl,str,log,text</td>
<td></td>
<td>Comma separated list of value types to be sent to the history storage. This parameter is used for Elasticsearch setup.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Mandatory</td>
<td>Range</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------</td>
<td>-------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>HousekeepingFrequency</td>
<td>no</td>
<td>0-24</td>
<td>1</td>
<td>How often Zabbix will perform housekeeping procedure (in hours). Housekeeping is removing outdated information from the database. Note: To prevent housekeeper from being overloaded (for example, when history and trend periods are greatly reduced), no more than 4 times HousekeepingFrequency hours of outdated information are deleted in one housekeeping cycle, for each item. Thus, if HousekeepingFrequency is 1, no more than 4 hours of outdated information (starting from the oldest entry) will be deleted per cycle. Note: To lower load on server startup housekeeping is postponed for 30 minutes after server start. Thus, if HousekeepingFrequency is 1, the very first housekeeping procedure after server start will run after 30 minutes, and will repeat with one hour delay thereafter. This postponing behavior is in place since Zabbix 2.4.0. Since Zabbix 3.0.0 it is possible to disable automatic housekeeping by setting HousekeepingFrequency to 0. In this case the housekeeping procedure can only be started by housekeeper_execute runtime control option and the period of outdated information deleted in one housekeeping cycle is 4 times the period since the last housekeeping cycle, but not less than 4 hours and not greater than 4 days. See also runtime control options.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Mandatory</td>
<td>Range</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------</td>
<td>----------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Include</td>
<td>no</td>
<td></td>
<td></td>
<td>You may include individual files or all files in a directory in the configuration file. To only include relevant files in the specified directory, the asterisk wildcard character is supported for pattern matching. For example: /absolute/path/to/config/files/*.conf. Pattern matching is supported since Zabbix 2.4.0. See special notes about limitations.</td>
</tr>
<tr>
<td>JavaGateway</td>
<td>no</td>
<td></td>
<td></td>
<td>IP address (or hostname) of Zabbix Java gateway. Only required if Java pollers are started. This parameter is supported since Zabbix 2.0.0.</td>
</tr>
<tr>
<td>JavaGatewayPort</td>
<td>no</td>
<td>1024-32767</td>
<td>10052</td>
<td>Port that Zabbix Java gateway listens on. This parameter is supported since Zabbix 2.0.0.</td>
</tr>
<tr>
<td>ListenIP</td>
<td>no</td>
<td>0.0.0.0</td>
<td></td>
<td>List of comma delimited IP addresses that the trapper should listen on. Trapper will listen on all network interfaces if this parameter is missing. Multiple IP addresses are supported since Zabbix 1.8.3.</td>
</tr>
<tr>
<td>ListenPort</td>
<td>no</td>
<td>1024-32767</td>
<td>10051</td>
<td>Listen port for trapper. Module to load at server startup. Modules are used to extend functionality of the server. Formats: LoadModule=&lt;module.so&gt; LoadModule=&lt;path/module.so&gt; (since 4.0.9) LoadModule=&lt;/abs_path/module.so&gt; Either the module must be located in directory specified by LoadModulePath or (since 4.0.9) the path must precede the module name. If the preceding path is absolute (starts with '/') then LoadModulePath is ignored. It is allowed to include multiple LoadModule parameters.</td>
</tr>
<tr>
<td>LoadModulePath</td>
<td>no</td>
<td></td>
<td></td>
<td>Full path to location of server modules. Default depends on compilation options.</td>
</tr>
<tr>
<td>LogFile</td>
<td>yes, if LogType is set to file, otherwise no</td>
<td></td>
<td></td>
<td>Name of log file.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Mandatory</td>
<td>Range</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------</td>
<td>-------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>LogFileSize</td>
<td>no</td>
<td>0-1024</td>
<td>1</td>
<td>Maximum size of log file in MB. 0 - disable automatic log rotation. Note: If the log file size limit is reached and file rotation fails, for whatever reason, the existing log file is truncated and started anew.</td>
</tr>
<tr>
<td>LogType</td>
<td>no</td>
<td>file</td>
<td></td>
<td>Log output type: file - write log to file specified by LogFile parameter, system - write log to syslog, console - write log to standard output. This parameter is supported since Zabbix 3.0.0.</td>
</tr>
<tr>
<td>LogSlowQueries</td>
<td>no</td>
<td>0-3600000</td>
<td>0</td>
<td>How long a database query may take before being logged (in milliseconds). 0 - don’t log slow queries. This option becomes enabled starting with DebugLevel=3. This parameter is supported since Zabbix 1.8.2.</td>
</tr>
<tr>
<td>MaxHousekeeperDelete</td>
<td>no</td>
<td>0-1000000</td>
<td>5000</td>
<td>No more than 'MaxHousekeeperDelete' rows (corresponding to [tablename], [field], [value]) will be deleted per one task in one housekeeping cycle. If set to 0 then no limit is used at all. In this case you must know what you are doing, so as not to overload the database! This parameter is supported since Zabbix 1.8.2 and applies only to deleting history and trends of already deleted items.</td>
</tr>
<tr>
<td>PidFile</td>
<td>no</td>
<td>/tmp/zabbix_server.pid</td>
<td></td>
<td>Name of PID file.</td>
</tr>
<tr>
<td>ProxyConfigFrequency</td>
<td>no</td>
<td>1-604800</td>
<td>3600</td>
<td>How often Zabbix server sends configuration data to a Zabbix proxy in seconds. Used only for proxies in a passive mode. This parameter is supported since Zabbix 1.8.3.</td>
</tr>
<tr>
<td>ProxyDataFrequency</td>
<td>no</td>
<td>1-3600</td>
<td>1</td>
<td>How often Zabbix server requests history data from a Zabbix proxy in seconds. Used only for proxies in a passive mode. This parameter is supported since Zabbix 1.8.3.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Mandatory</td>
<td>Range</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------</td>
<td>------------</td>
<td>---------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SNMPTrapperFile</td>
<td>no</td>
<td>/tmp</td>
<td>/tmp/zabbix_traps.tmp</td>
<td>Temporary file used for passing data from SNMP trap daemon to the server. Must be the same as in zabbix_trap_receiver.pl or SNMPTT configuration file. This parameter is supported since Zabbix 2.0.0.</td>
</tr>
<tr>
<td>SocketDir</td>
<td>no</td>
<td>/tmp</td>
<td></td>
<td>Directory to store IPC sockets used by internal Zabbix services. This parameter is supported since Zabbix 3.4.0.</td>
</tr>
<tr>
<td>SourceIP</td>
<td>no</td>
<td></td>
<td></td>
<td>Source IP address for: - outgoing connections to Zabbix proxy and Zabbix agent; - agentless connections (VMware, SSH, JMX, SNMP, Telnet and simple checks); - HTTP agent connections; - sending notification emails (connections to SMTP server)</td>
</tr>
<tr>
<td>SSHKeyLocation</td>
<td>no</td>
<td></td>
<td></td>
<td>Location of public and private keys for SSH checks and actions</td>
</tr>
<tr>
<td>SSLCertLocation</td>
<td>no</td>
<td></td>
<td></td>
<td>Location of SSL client certificate files for client authentication. This parameter is used in web monitoring only and is supported since Zabbix 2.4.</td>
</tr>
<tr>
<td>SSLKeyLocation</td>
<td>no</td>
<td></td>
<td></td>
<td>Location of SSL private key files for client authentication. This parameter is used in web monitoring only and is supported since Zabbix 2.4.</td>
</tr>
<tr>
<td>SSLLCAlocation</td>
<td>no</td>
<td></td>
<td></td>
<td>Override the location of certificate authority (CA) files for SSL server certificate verification. If not set, system-wide directory will be used. Note that the value of this parameter will be set as libcurl option CURLOPT_CAPATH. For libcurl versions before 7.42.0, this only has effect if libcurl was compiled to use OpenSSL. For more information see cURL web page. This parameter is used in web monitoring since Zabbix 2.4.0 and in SMTP authentication since Zabbix 3.0.0. Number of pre-forked instances of DB Syncers. The upper limit used to be 64 before version 1.8.5. This parameter is supported since Zabbix 1.8.3.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Mandatory</td>
<td>Range</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------</td>
<td>-------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>StartAlerters</td>
<td>no</td>
<td>1-100</td>
<td>3</td>
<td>Number of pre-forked instances of alerters. This parameter is supported since Zabbix 3.4.0.</td>
</tr>
<tr>
<td>StartDiscoverers</td>
<td>no</td>
<td>0-250</td>
<td>1</td>
<td>Number of pre-forked instances of discoverers. The upper limit used to be 255 before version 1.8.5.</td>
</tr>
<tr>
<td>StartEscalators</td>
<td>no</td>
<td>1-100</td>
<td>1</td>
<td>Number of pre-forked instances of escalators. This parameter is supported since Zabbix 3.0.0.</td>
</tr>
<tr>
<td>StartHTTPPollers</td>
<td>no</td>
<td>0-1000</td>
<td>1</td>
<td>Number of pre-forked instances of HTTP pollers. The upper limit used to be 255 before version 1.8.5.</td>
</tr>
<tr>
<td>StartIPMIPollers</td>
<td>no</td>
<td>0-1000</td>
<td>0</td>
<td>Number of pre-forked instances of IPMI pollers. The upper limit used to be 255 before version 1.8.5.</td>
</tr>
<tr>
<td>StartJavaPollers</td>
<td>no</td>
<td>0-1000</td>
<td>0</td>
<td>Number of pre-forked instances of Java pollers. This parameter is supported since Zabbix 2.0.0.</td>
</tr>
<tr>
<td>StartPingers</td>
<td>no</td>
<td>0-1000</td>
<td>1</td>
<td>Number of pre-forked instances of ICMP pingers. The upper limit used to be 255 before version 1.8.5.</td>
</tr>
<tr>
<td>StartPollersUnreachable</td>
<td>no</td>
<td>0-1000</td>
<td>1</td>
<td>Number of pre-forked instances of pollers for unreachable hosts (including IPMI and Java). Since Zabbix 2.4.0, at least one poller for unreachable hosts must be running if regular, IPMI or Java pollers are started. The upper limit used to be 255 before version 1.8.5. This option is missing in version 1.8.3.</td>
</tr>
<tr>
<td>StartPollers</td>
<td>no</td>
<td>0-1000</td>
<td>5</td>
<td>Number of pre-forked instances of pollers. Note that a non-zero value is required for internal, aggregated and calculated items to work.</td>
</tr>
<tr>
<td>StartPreprocessors</td>
<td>no</td>
<td>1-1000</td>
<td>3</td>
<td>Number of pre-forked instances of preprocessing workers. The preprocessing manager process is automatically started when a preprocessor worker is started. This parameter is supported since Zabbix 3.4.0.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Mandatory</td>
<td>Range</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------</td>
<td>--------</td>
<td>---------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>StartProxyPollers</td>
<td>no</td>
<td>0-250</td>
<td>1</td>
<td>Number of pre-forked instances of pollers for passive proxies. The upper limit used to be 255 before version 1.8.5. This parameter is supported since Zabbix 1.8.3.</td>
</tr>
<tr>
<td>StartSNMPTrapper</td>
<td>no</td>
<td>0-1</td>
<td>0</td>
<td>If set to 1, SNMP trap process will be started. This parameter is supported since Zabbix 2.0.0.</td>
</tr>
<tr>
<td>StartTimers</td>
<td>no</td>
<td>1-1000</td>
<td>1</td>
<td>Number of pre-forked instances of timers. Timers process maintenance periods. This parameter is supported since Zabbix 2.2.0.</td>
</tr>
<tr>
<td>StartTrappers</td>
<td>no</td>
<td>0-1000</td>
<td>5</td>
<td>Number of pre-forked instances of trappers. Trappers accept incoming connections from Zabbix sender, active agents and active proxies. At least one trapper process must be running to display server availability and view queue in the frontend. The upper limit used to be 255 before version 1.8.5.</td>
</tr>
<tr>
<td>StartVMwareCollectors</td>
<td>no</td>
<td>0-250</td>
<td>0</td>
<td>Number of pre-forked vmware collector instances. This parameter is supported since Zabbix 2.2.0.</td>
</tr>
<tr>
<td>StatsAllowedIP</td>
<td>no</td>
<td></td>
<td></td>
<td>List of comma delimited IP addresses, optionally in CIDR notation, or DNS names of external Zabbix instances. Stats request will be accepted only from the addresses listed here. If this parameter is not set no stats requests will be accepted. If IPv6 support is enabled then '127.0.0.1', '::1', '127.0.0.1', '::ffff:127.0.0.1' are treated equally and '::/0' will allow any IPv4 or IPv6 address. '0.0.0.0/0' can be used to allow any IPv4 address. Example: StatsAllowedIP=127.0.0.1,192.168.1.0/24,::1,2001::/32,zabbix.example.com This parameter is supported since Zabbix 4.0.5.</td>
</tr>
<tr>
<td>Timeout</td>
<td>no</td>
<td>1-30</td>
<td>3</td>
<td>Specifies how long we wait for agent, SNMP device or external check (in seconds).</td>
</tr>
<tr>
<td>Parameter</td>
<td>Mandatory</td>
<td>Range</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------</td>
<td>-------</td>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>TLSCAFile</td>
<td>no</td>
<td></td>
<td></td>
<td>Full pathname of a file containing the top-level CA(s) certificates for peer certificate verification, used for encrypted communications between Zabbix components. This parameter is supported since Zabbix 3.0.0.</td>
</tr>
<tr>
<td>TLS_certFile</td>
<td>no</td>
<td></td>
<td></td>
<td>Full pathname of a file containing the server certificate or certificate chain, used for encrypted communications between Zabbix components. This parameter is supported since Zabbix 3.0.0.</td>
</tr>
<tr>
<td>TLSCipherAll</td>
<td>no</td>
<td></td>
<td></td>
<td>GnuTLS priority string or OpenSSL (TLS 1.2) cipher string. Override the default ciphersuite selection criteria for certificate- and PSK-based encryption. Example: TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256. This parameter is supported since Zabbix 4.0.19.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Mandatory</td>
<td>Range</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------</td>
<td>------------------------</td>
<td>---------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TLSCipherCert13</td>
<td>no</td>
<td></td>
<td></td>
<td>Cipher string for OpenSSL 1.1.1 or newer in TLS 1.3. Override the default ciphersuite selection criteria for certificate-based encryption. This parameter is supported since Zabbix 4.0.19.</td>
</tr>
<tr>
<td>TLSCipherPSK13</td>
<td>no</td>
<td></td>
<td></td>
<td>Cipher string for OpenSSL 1.1.1 or newer in TLS 1.3. Override the default ciphersuite selection criteria for PSK-based encryption. Example: TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256 This parameter is supported since Zabbix 4.0.19.</td>
</tr>
<tr>
<td>TLSCRLFile</td>
<td>no</td>
<td></td>
<td></td>
<td>Full pathname of a file containing revoked certificates. This parameter is used for encrypted communications between Zabbix components. This parameter is supported since Zabbix 3.0.0.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Mandatory</td>
<td>Range</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------</td>
<td>--------------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TLSKeyFile</td>
<td>no</td>
<td>Full path name of a file containing the server private key, used for encrypted communications between Zabbix components. This parameter is supported since Zabbix 3.0.0.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TmpDir</td>
<td>no</td>
<td>/tmp</td>
<td></td>
<td>Temporary directory.</td>
</tr>
<tr>
<td>TrapperTimeout</td>
<td>no</td>
<td>1-300</td>
<td>300</td>
<td>Specifies how many seconds trapper may spend processing new data.</td>
</tr>
<tr>
<td>UnavailableDelay</td>
<td>no</td>
<td>1-3600</td>
<td>60</td>
<td>How often host is checked for availability during the unavailability period, in seconds.</td>
</tr>
<tr>
<td>UnreachableDelay</td>
<td>no</td>
<td>1-3600</td>
<td>15</td>
<td>How often host is checked for availability during the unreachable period, in seconds.</td>
</tr>
<tr>
<td>UnreachablePeriod</td>
<td>no</td>
<td>1-3600</td>
<td>45</td>
<td>After how many seconds of unreachability treat a host as unavailable.</td>
</tr>
<tr>
<td>User</td>
<td>no</td>
<td>zabbix</td>
<td></td>
<td>Drop privileges to a specific, existing user on the system. Only has effect if run as ‘root’ and AllowRoot is disabled. This parameter is supported since Zabbix 2.4.0.</td>
</tr>
<tr>
<td>ValueCacheSize</td>
<td>no</td>
<td>0,128K-64G</td>
<td>8M</td>
<td>Size of history value cache, in bytes. Shared memory size for caching item history data requests. Setting to 0 disables value cache (not recommended). When value cache runs out of the shared memory a warning message is written to the server log every 5 minutes. This parameter is supported since Zabbix 2.2.0.</td>
</tr>
<tr>
<td>VMwareCacheSize</td>
<td>no</td>
<td>256K-2G</td>
<td>8M</td>
<td>Shared memory size for storing VMware data. A VMware internal check zabbix[vmware,buffer,...] can be used to monitor the VMware cache usage (see Internal checks). Note that shared memory is not allocated if there are no VMware collector instances configured to start. This parameter is supported since Zabbix 2.2.0.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Mandatory</td>
<td>Range</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------</td>
<td>--------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>VMwareFrequency</td>
<td>no</td>
<td>10-86400</td>
<td>60</td>
<td>Delay in seconds between data gathering from a single VMware service. This delay should be set to the least update interval of any VMware monitoring item. This parameter is supported since Zabbix 2.2.0.</td>
</tr>
<tr>
<td>VMwarePerfFrequency</td>
<td>no</td>
<td>10-86400</td>
<td>60</td>
<td>Delay in seconds between performance counter statistics retrieval from a single VMware service. This delay should be set to the least update interval of any VMware monitoring item that uses VMware performance counters. This parameter is supported since Zabbix 2.2.9, 2.4.4</td>
</tr>
<tr>
<td>VMwareTimeout</td>
<td>no</td>
<td>1-300</td>
<td>10</td>
<td>The maximum number of seconds vmware collector will wait for a response from VMware service (vCenter or ESX hypervisor). This parameter is supported since Zabbix 2.2.9, 2.4.4</td>
</tr>
</tbody>
</table>

Footnotes

1 Note that too many data gathering processes (pollers, unreachable pollers, HTTP pollers, Java pollers, pingers, trappers, proxy-pollers) together with IPMI manager, SNMP trapper and preprocessing workers can exhaust the per-process file descriptor limit for the preprocessing manager.

2 When a lot of items are deleted it increases the load to the database, because the housekeeper will need to remove all the history data that these items had. For example, if we only have to remove 1 item prototype, but this prototype is linked to 50 hosts and for every host the prototype is expanded to 100 real items, 5000 items in total have to be removed (1*50*100). If 500 is set for MaxHousekeeperDelete (MaxHousekeeperDelete=500), the housekeeper process will have to remove up to 2500000 values (5000*500) for the deleted items from history and trends tables in one cycle.

2 Zabbix proxy

Overview

This section lists parameters supported in a Zabbix proxy configuration file (zabbix_proxy.conf). Note that:

- The default values reflect daemon defaults, not the values in the shipped configuration files;
- Zabbix supports configuration files only in UTF-8 encoding without BOM;
- Comments starting with “#” are only supported in the beginning of the line.

Parameters
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Mandatory</th>
<th>Range</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AllowRoot</td>
<td>no</td>
<td>0-1</td>
<td>0</td>
<td>Allow the proxy to run as 'root'. If disabled and the proxy is started by 'root', the proxy will try to switch to the 'zabbix' user instead. Has no effect if started under a regular user. 0 - do not allow 1 - allow  This parameter is supported since Zabbix 2.2.0.</td>
</tr>
<tr>
<td>CacheSize</td>
<td>no</td>
<td>128K-64G</td>
<td>8M</td>
<td>Size of configuration cache, in bytes. Shared memory size, for storing host and item data. The maximum value of this parameter was increased from 8GB to 64GB in Zabbix 4.0.21.</td>
</tr>
<tr>
<td>ConfigFrequency</td>
<td>no</td>
<td>1-604800</td>
<td>3600</td>
<td>How often proxy retrieves configuration data from Zabbix server in seconds. Active proxy parameter. Ignored for passive proxies (see ProxyMode parameter).</td>
</tr>
<tr>
<td>DBHost</td>
<td>no</td>
<td>localhost</td>
<td></td>
<td>Database host name. In case of MySQL localhost or empty string results in using a socket. In case of PostgreSQL only empty string results in attempt to use socket.</td>
</tr>
<tr>
<td>DBName</td>
<td>yes</td>
<td></td>
<td></td>
<td>Database name or path to database file for SQLite3 (multi-process architecture of Zabbix does not allow to use in-memory database, e.g. :memory:, file::memory:?cache=shared or file:memdb1?mode=memory&amp;cache=shared). Warning: Do not attempt to use the same database Zabbix server is using.</td>
</tr>
<tr>
<td>DBPassword</td>
<td>no</td>
<td></td>
<td></td>
<td>Database password. Ignored for SQLite. Comment this line if no password is used.</td>
</tr>
<tr>
<td>DBSchema</td>
<td>no</td>
<td></td>
<td></td>
<td>Schema name. Used for IBM DB2 and PostgreSQL.</td>
</tr>
<tr>
<td>DBSocket</td>
<td>no</td>
<td>3306</td>
<td></td>
<td>Path to MySQL socket. Database port when not using local socket. Ignored for SQLite.</td>
</tr>
<tr>
<td>DBUser</td>
<td></td>
<td></td>
<td></td>
<td>Database user. Ignored for SQLite.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Mandatory</td>
<td>Range</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------</td>
<td>----------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DataSenderFrequency</td>
<td>no</td>
<td>1-3600</td>
<td>1</td>
<td>Proxy will send collected data to the server every N seconds. Note that active proxy will still poll Zabbix server every second for remote command tasks. Active proxy parameter. Ignored for passive proxies (see ProxyMode parameter).</td>
</tr>
<tr>
<td>DebugLevel</td>
<td>no</td>
<td>0-5</td>
<td>3</td>
<td>Specifies debug level: 0 - basic information about starting and stopping of Zabbix processes 1 - critical information 2 - error information 3 - warnings 4 - for debugging (produces lots of information) 5 - extended debugging (produces even more information)</td>
</tr>
<tr>
<td>EnableRemoteCommands</td>
<td>no</td>
<td>0</td>
<td>0</td>
<td>Whether remote commands from Zabbix server are allowed. 0 - not allowed 1 - allowed This parameter is supported since Zabbix 3.4.0.</td>
</tr>
<tr>
<td>ExternalScripts</td>
<td>no</td>
<td>/usr/local/share/zabbix/externalscripts (depends on compile-time installation variable datadir)</td>
<td></td>
<td>Location of external scripts.</td>
</tr>
<tr>
<td>Fping6Location</td>
<td>no</td>
<td>/usr/sbin/fping6</td>
<td></td>
<td>Location of fping6. Make sure that fping6 binary has root ownership and SUID flag set. Make empty (&quot;Fping6Location=&quot;) if your fping utility is capable to process IPv6 addresses.</td>
</tr>
<tr>
<td>FpingLocation</td>
<td>no</td>
<td>/usr/sbin/fping</td>
<td></td>
<td>Location of fping. Make sure that fping binary has root ownership and SUID flag set!</td>
</tr>
<tr>
<td>HeartbeatFrequency</td>
<td>no</td>
<td>0-3600</td>
<td>60</td>
<td>Frequency of heartbeat messages in seconds. Used for monitoring availability of proxy on server side. 0 - heartbeat messages disabled. Active proxy parameter. Ignored for passive proxies (see ProxyMode parameter).</td>
</tr>
<tr>
<td>HistoryCacheSize</td>
<td>no</td>
<td>128K-2G</td>
<td>16M</td>
<td>Size of history cache, in bytes. Shared memory size for storing history data.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Mandatory</td>
<td>Range</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------</td>
<td>---------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>HistoryIndexCacheSize</td>
<td>no</td>
<td>128K-2G</td>
<td>4M</td>
<td>Size of history index cache, in bytes. Shared memory size for indexing history data stored in history cache. The index cache size needs roughly 100 bytes to cache one item. This parameter is supported since Zabbix 3.0.0.</td>
</tr>
</tbody>
</table>
| Hostname                   | no        | Set by  | HostnameItem | Unique, case sensitive Proxy name. Make sure the proxy name is known to the server! Allowed characters: alphanumeric, '.', ',', '_' and ':'.
<p>| HostnameItem               | no        | system.hostname |         | Maximum length: 64 Item used for setting Hostname if it is undefined (this will be run on the proxy similarly as on an agent). Does not support UserParameters, performance counters or aliases, but does support system.run[]. Ignored if Hostname is set. This parameter is supported since Zabbix 1.8.6. |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Mandatory</th>
<th>Range</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HousekeepingFrequency</td>
<td>no</td>
<td>0-24</td>
<td>1</td>
<td>How often Zabbix will perform housekeeping procedure (in hours). Housekeeping is removing outdated information from the database. Note: To prevent housekeeper from being overloaded (for example, when configuration parameters ProxyLocalBuffer or ProxyOfflineBuffer are greatly reduced), no more than 4 times HousekeepingFrequency hours of outdated information are deleted in one housekeeping cycle. Thus, if HousekeepingFrequency is 1, no more than 4 hours of outdated information (starting from the oldest entry) will be deleted per cycle. Note: To lower load on proxy startup housekeeping is postponed for 30 minutes after proxy start. Thus, if HousekeepingFrequency is 1, the very first housekeeping procedure after proxy start will run after 30 minutes, and will repeat every hour thereafter. This postponing behavior is in place since Zabbix 2.4.0. Since Zabbix 3.0.0 it is possible to disable automatic housekeeping by setting HousekeepingFrequency to 0. In this case the housekeeping procedure can only be started by housekeeper_execute runtime control option and the period of outdated information deleted in one housekeeping cycle is 4 times the period since the last housekeeping cycle, but not less than 4 hours and not greater than 4 days.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Mandatory</td>
<td>Range</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------</td>
<td>----------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Include</td>
<td>no</td>
<td></td>
<td></td>
<td>You may include individual files or all files in a directory in the configuration file. To only include relevant files in the specified directory, the asterisk wildcard character is supported for pattern matching. For example: /absolute/path/to/config/files/*.conf. Pattern matching is supported since Zabbix 2.4.0. See special notes about limitations.</td>
</tr>
<tr>
<td>JavaGateway</td>
<td>no</td>
<td></td>
<td></td>
<td>IP address (or hostname) of Zabbix Java gateway. Only required if Java pollers are started. This parameter is supported since Zabbix 2.0.0.</td>
</tr>
<tr>
<td>JavaGatewayPort</td>
<td>no</td>
<td>1024-32767</td>
<td>10052</td>
<td>Port that Zabbix Java gateway listens on. This parameter is supported since Zabbix 2.0.0.</td>
</tr>
<tr>
<td>ListenIP</td>
<td>no</td>
<td>0.0.0.0</td>
<td></td>
<td>List of comma delimited IP addresses that the trapper should listen on. Trapper will listen on all network interfaces if this parameter is missing. Multiple IP addresses are supported since Zabbix 1.8.3.</td>
</tr>
<tr>
<td>ListenPort</td>
<td>no</td>
<td>1024-32767</td>
<td>10051</td>
<td>Listen port for trapper. Module to load at proxy startup. Modules are used to extend functionality of the proxy. formats: LoadModule=&lt;module.so&gt; LoadModule=&lt;path/module.so&gt; (since 4.0.9) LoadModule=&lt;/abs_path/module.so&gt; Either the module must be located in directory specified by LoadModulePath or (since 4.0.9) the path must precede the module name. If the preceding path is absolute (starts with &quot;/&quot;) then LoadModulePath is ignored. It is allowed to include multiple LoadModule parameters.</td>
</tr>
<tr>
<td>LoadModulePath</td>
<td>no</td>
<td></td>
<td></td>
<td>Full path to location of proxy modules. Default depends on compilation options.</td>
</tr>
<tr>
<td>LogFile</td>
<td>yes, if LogType is set to file, otherwise no</td>
<td></td>
<td></td>
<td>Name of log file.</td>
</tr>
</tbody>
</table>

1224
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Mandatory</th>
<th>Range</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LogFileSize</td>
<td>no</td>
<td>0-1024</td>
<td>1</td>
<td>Maximum size of log file in MB. 0 - disable automatic log rotation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Note: If the log file size limit is reached and file rotation fails, for whatever reason, the existing log file is truncated and started anew.</td>
</tr>
<tr>
<td>LogRemoteCommands</td>
<td>no</td>
<td></td>
<td>0</td>
<td>Enable logging of executed shell commands as warnings. 0 - disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1 - enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>This parameter is supported since Zabbix 3.4.0.</td>
</tr>
<tr>
<td>LogType</td>
<td>no</td>
<td></td>
<td>file</td>
<td>Log output type: file - write log to file specified by LogFile parameter, system - write log to syslog, console - write log to standard output.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>This parameter is supported since Zabbix 3.0.0.</td>
</tr>
<tr>
<td>LogSlowQueries</td>
<td>no</td>
<td>0-3600000</td>
<td>0</td>
<td>How long a database query may take before being logged (in milliseconds). 0 - don't log slow queries.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>This option becomes enabled starting with DebugLevel=3.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>This parameter is supported since Zabbix 1.8.2.</td>
</tr>
<tr>
<td>PidFile</td>
<td>no</td>
<td></td>
<td>/tmp/zabbix_proxy.pid</td>
<td>Name of PID file.</td>
</tr>
<tr>
<td>ProxyLocalBuffer</td>
<td>no</td>
<td>0-720</td>
<td>0</td>
<td>Proxy will keep data locally for N hours, even if the data have already been synced with the server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>This parameter may be used if local data will be used by third party applications.</td>
</tr>
<tr>
<td>ProxyMode</td>
<td>no</td>
<td>0-1</td>
<td>0</td>
<td>Proxy operating mode. 0 - proxy in the active mode 1 - proxy in the passive mode</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>This parameter is supported since Zabbix 1.8.3.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Note that (sensitive) proxy configuration data may become available to parties having access to the Zabbix server trapper port when using an active proxy. This is possible because anyone may pretend to be an active proxy and request configuration data; authentication does not take place.</td>
</tr>
<tr>
<td>ProxyOfflineBuffer</td>
<td>no</td>
<td>1-720</td>
<td>1</td>
<td>Proxy will keep data for N hours in case of no connectivity with Zabbix server. Older data will be lost.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Mandatory</td>
<td>Range</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------</td>
<td>-------------</td>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>ServerPort</td>
<td>no</td>
<td>1024-32767</td>
<td>10051</td>
<td>Port of Zabbix trapper on Zabbix server. Active proxy parameter. Ignored for passive proxies (see ProxyMode parameter). If ProxyMode is set to active mode: IP address or DNS name of Zabbix server to get configuration data from and send data to. If ProxyMode is set to passive mode: List of comma delimited IP addresses, optionally in CIDR notation, or DNS names of Zabbix server. Incoming connections will be accepted only from the addresses listed here. If IPv6 support is enabled then '127.0.0.1', '::127.0.0.1', '::ffff:127.0.0.1' are treated equally and '::/0' will allow any IPv4 or IPv6 address. '0.0.0.0/0' can be used to allow any IPv4 address. Example: Server=127.0.0.1,192.168.1.0/24,::1,2001:db8::/32,zabbix.example.com</td>
</tr>
<tr>
<td>Server</td>
<td>yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SNMPTrapperFile</td>
<td>no</td>
<td>/tmp</td>
<td></td>
<td>Temporary file used for passing data from SNMP trap daemon to the proxy. Must be the same as in zabbix_trap_receiver.pl or SNMPTT configuration file. This parameter is supported since Zabbix 2.0.0.</td>
</tr>
<tr>
<td>SocketDir</td>
<td>no</td>
<td>/tmp</td>
<td></td>
<td>Directory to store IPC sockets used by internal Zabbix services. This parameter is supported since Zabbix 3.4.0.</td>
</tr>
<tr>
<td>SourceIP</td>
<td>no</td>
<td></td>
<td></td>
<td>Source IP address for: - outgoing connections to Zabbix server; - agentless connections (VMware, SSH, JMX, SNMP, Telnet and simple checks); - HTTP agent connections Location of public and private keys for SSH checks and actions SSLCertLocation</td>
</tr>
<tr>
<td>SSHKeyLocation</td>
<td>no</td>
<td></td>
<td></td>
<td>Location of public and private keys for SSH checks and actions</td>
</tr>
<tr>
<td>Parameter</td>
<td>Mandatory</td>
<td>Range</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------</td>
<td>---------</td>
<td>---------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SSLKeyLocation</td>
<td>no</td>
<td>Location of SSL private key files for client authentication. This parameter is used in web monitoring only and is supported since Zabbix 2.4.0.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSLCAlocation</td>
<td>no</td>
<td>Location of certificate authority (CA) files for SSL server certificate verification. Note that the value of this parameter will be set as libcurl option CURLOPT_CAPATH. For libcurl versions before 7.42.0, this only has effect if libcurl was compiled to use OpenSSL. For more information see cURL web page. This parameter is used in web monitoring since Zabbix 2.4.0 and in SMTP authentication since Zabbix 3.0.0.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>StartDBSyncers</td>
<td>no</td>
<td>1-100</td>
<td>4</td>
<td>Number of pre-forked instances of DB Syncers. The upper limit used to be 64 before version 1.8.5. This parameter is supported since Zabbix 1.8.3.</td>
</tr>
<tr>
<td>StartDiscoverers</td>
<td>no</td>
<td>0-250</td>
<td>1</td>
<td>Number of pre-forked instances of discoverers. The upper limit used to be 255 before version 1.8.5.</td>
</tr>
<tr>
<td>StartHTTPPollers</td>
<td>no</td>
<td>0-1000</td>
<td>1</td>
<td>Number of pre-forked instances of HTTP pollers.</td>
</tr>
<tr>
<td>StartIPMIPollers</td>
<td>no</td>
<td>0-1000</td>
<td>0</td>
<td>Number of pre-forked instances of IPMI pollers. The upper limit used to be 255 before version 1.8.5.</td>
</tr>
<tr>
<td>StartJavaPollers</td>
<td>no</td>
<td>0-1000</td>
<td>0</td>
<td>Number of pre-forked instances of Java pollers. This parameter is supported since Zabbix 2.0.0.</td>
</tr>
<tr>
<td>StartPingers</td>
<td>no</td>
<td>0-1000</td>
<td>1</td>
<td>Number of pre-forked instances of ICMP pingers. The upper limit used to be 255 before version 1.8.5.</td>
</tr>
<tr>
<td>StartPollersUnreachable</td>
<td>no</td>
<td>0-1000</td>
<td>1</td>
<td>Number of pre-forked instances of pollers for unreachable hosts (including IPMI and Java). Since Zabbix 2.4.0, at least one poller for unreachable hosts must be running if regular, IPMI or Java pollers are started. The upper limit used to be 255 before version 1.8.5. This option is missing in version 1.8.3.</td>
</tr>
<tr>
<td>StartPollers</td>
<td>no</td>
<td>0-1000</td>
<td>5</td>
<td>Number of pre-forked instances of pollers. The upper limit used to be 255 before version 1.8.5.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Mandatory</td>
<td>Range</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------</td>
<td>-------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>StartSNMPTrapper</td>
<td>no</td>
<td>0-1</td>
<td>0</td>
<td>If set to 1, SNMP trapper process will be started. This parameter is supported since Zabbix 2.0.0.</td>
</tr>
<tr>
<td>StartTrappers</td>
<td>no</td>
<td>0-1000</td>
<td>5</td>
<td>Number of pre-forked instances of trappers. Trappers accept incoming connections from Zabbix sender and active agents. The upper limit used to be 255 before version 1.8.5.</td>
</tr>
<tr>
<td>StartVMwareCollectors</td>
<td>no</td>
<td>0-250</td>
<td>0</td>
<td>Number of pre-forked vmware collector instances. This parameter is supported since Zabbix 2.2.0.</td>
</tr>
<tr>
<td>StatsAllowedIP</td>
<td>no</td>
<td>List of comma delimited IP addresses, optionally in CIDR notation, or DNS names of external Zabbix instances. Stats request will be accepted only from the addresses listed here. If this parameter is not set no stats requests will be accepted. If IPv6 support is enabled then '127.0.0.1', '::127.0.0.1', '::ffff:127.0.0.1' are treated equally and '::/0' will allow any IPv4 or IPv6 address. '0.0.0.0/0' can be used to allow any IPv4 address. Example: StatsAllowedIP=127.0.0.1,192.168.1.0/24,::1,2001:db8::/32,zabbix.example.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Timeout</td>
<td>no</td>
<td>1-30</td>
<td>3</td>
<td>Specifies how long we wait for agent, SNMP device or external check (in seconds).</td>
</tr>
<tr>
<td>TLSAccept</td>
<td>yes for passive proxy, if TLS certificate or PSK parameters are defined (even for unencrypted connection), otherwise no</td>
<td></td>
<td></td>
<td>Specifies incoming connections to accept from Zabbix server. Used for a passive proxy, ignored on an active proxy. Multiple values can be specified, separated by comma: unencrypted - accept connections without encryption (default) psk - accept connections with TLS and a pre-shared key (PSK) cert - accept connections with TLS and a certificate</td>
</tr>
<tr>
<td>Parameter</td>
<td>Mandatory</td>
<td>Range</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
<td>-------</td>
<td>---------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TLSCAFile</td>
<td>no</td>
<td></td>
<td></td>
<td>Full path name of a file containing the top-level CA(s) certificates for peer certificate verification, used for encrypted communications between Zabbix components.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>This parameter is supported since Zabbix 3.0.0.</td>
</tr>
<tr>
<td>TLSCertFile</td>
<td>no</td>
<td></td>
<td></td>
<td>Full path name of a file containing the proxy certificate or certificate chain, used for encrypted communications between Zabbix components.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>This parameter is supported since Zabbix 3.0.0.</td>
</tr>
<tr>
<td>TLSCipherAll</td>
<td>no</td>
<td></td>
<td></td>
<td>GnuTLS priority string or OpenSSL (TLS 1.2) cipher string. Override the default ciphersuite selection criteria for certificate- and PSK-based encryption.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Example: TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>This parameter is supported since Zabbix 4.0.19.</td>
</tr>
<tr>
<td>TLSCipherAll13</td>
<td>no</td>
<td></td>
<td></td>
<td>Cipher string for OpenSSL 1.1.1 or newer in TLS 1.3. Override the default ciphersuite selection criteria for certificate- and PSK-based encryption.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Example for OpenSSL: ECDH+aRSA+AES128:RSA+aRSA+AES128:kECDHEPSK+AES128:kPSK+AES128</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>This parameter is supported since Zabbix 4.0.19.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Mandatory</td>
<td>Range</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------</td>
<td>-------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TLSCipherCert13</td>
<td>no</td>
<td></td>
<td></td>
<td>Cipher string for OpenSSL 1.1.1 or newer in TLS 1.3. Override the default ciphersuite selection criteria for certificate-based encryption. This parameter is supported since Zabbix 4.0.19.</td>
</tr>
<tr>
<td>TLSCipherPSK13</td>
<td>no</td>
<td></td>
<td></td>
<td>Cipher string for OpenSSL 1.1.1 or newer in TLS 1.3. Override the default ciphersuite selection criteria for PSK-based encryption. Example: TLS_CHACHA20_POLY1305_SHA256-TLS_AES128_GCM_SHA256 This parameter is supported since Zabbix 4.0.19.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Mandatory</td>
<td>Range</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------</td>
<td>-----------</td>
<td>---------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TLSConnect</td>
<td>yes for active proxy, if TLS certificate or PSK parameters are defined (even for unencrypted connection), otherwise no</td>
<td></td>
<td></td>
<td>How the proxy should connect to Zabbix server. Used for an active proxy, ignored on a passive proxy. Only one value can be specified: unencrypted - connect without encryption (default) psk - connect using TLS and a pre-shared key (PSK) cert - connect using TLS and a certificate This parameter is supported since Zabbix 3.0.0.</td>
</tr>
<tr>
<td>TLSCRLFile</td>
<td>no</td>
<td>Full pathname of a file containing revoked certificates. This parameter is used for encrypted communications between Zabbix components. This parameter is supported since Zabbix 3.0.0.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TLSKeyFile</td>
<td>no</td>
<td>Full pathname of a file containing the proxy private key, used for encrypted communications between Zabbix components. This parameter is supported since Zabbix 3.0.0.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TLSPSKFile</td>
<td>no</td>
<td>Full pathname of a file containing the proxy pre-shared key. used for encrypted communications with Zabbix server. This parameter is supported since Zabbix 3.0.0.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TLSPSKIdentity</td>
<td>no</td>
<td>Pre-shared key identity string, used for encrypted communications with Zabbix server. This parameter is supported since Zabbix 3.0.0.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TLSServerCertIssuer</td>
<td>no</td>
<td>Allowed server certificate issuer. This parameter is supported since Zabbix 3.0.0.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TLSServerCertSubject</td>
<td>no</td>
<td>Allowed server certificate subject. This parameter is supported since Zabbix 3.0.0.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TmpDir</td>
<td>no</td>
<td>/tmp</td>
<td></td>
<td>Temporary directory.</td>
</tr>
<tr>
<td>TrapperTimeout</td>
<td>no</td>
<td>1-300</td>
<td>300</td>
<td>Specifies how many seconds trapper may spend processing new data.</td>
</tr>
<tr>
<td>User</td>
<td>no</td>
<td>zabbix</td>
<td></td>
<td>Drop privileges to a specific, existing user on the system. Only has effect if run as ‘root’ and AllowRoot is disabled. This parameter is supported since Zabbix 2.4.0.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Mandatory</td>
<td>Range</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------</td>
<td>-----------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>UnavailableDelay</td>
<td>no</td>
<td>1-3600</td>
<td>60</td>
<td>How often host is checked for availability during the unavailability period, in seconds.</td>
</tr>
<tr>
<td>UnreachableDelay</td>
<td>no</td>
<td>1-3600</td>
<td>15</td>
<td>How often host is checked for availability during the unreachability period, in seconds.</td>
</tr>
<tr>
<td>UnreachablePeriod</td>
<td>no</td>
<td>1-3600</td>
<td>45</td>
<td>After how many seconds of unreachability treat a host as unavailable.</td>
</tr>
<tr>
<td>VMwareCacheSize</td>
<td>no</td>
<td>256K-2G</td>
<td>8M</td>
<td>Shared memory size for storing VMware data. A VMware internal check zabbix[vmware,buffer,...] can be used to monitor the VMware cache usage (see Internal checks). Note that shared memory is not allocated if there are no vmware collector instances configured to start. This parameter is supported since Zabbix 2.2.0.</td>
</tr>
<tr>
<td>VMwareFrequency</td>
<td>no</td>
<td>10-86400</td>
<td>60</td>
<td>Delay in seconds between data gathering from a single VMware service. This delay should be set to the least update interval of any VMware monitoring item. This parameter is supported since Zabbix 2.2.0.</td>
</tr>
<tr>
<td>VMwarePerfFrequency</td>
<td>no</td>
<td>10-86400</td>
<td>60</td>
<td>Delay in seconds between performance counter statistics retrieval from a single VMware service. This delay should be set to the least update interval of any VMware monitoring item that uses VMware performance counters. This parameter is supported since Zabbix 2.2.9, 2.4.4</td>
</tr>
<tr>
<td>VMwareTimeout</td>
<td>no</td>
<td>1-300</td>
<td>10</td>
<td>The maximum number of seconds vmware collector will wait for a response from VMware service (vCenter or ESX hypervisor). This parameter is supported since Zabbix 2.2.9, 2.4.4</td>
</tr>
</tbody>
</table>

### 3 Zabbix agent (UNIX)

**Overview**

This section lists parameters supported in a Zabbix agent configuration file (zabbix_agentd.conf). Note that:

- The default values reflect daemon defaults, not the values in the shipped configuration files;
- Zabbix supports configuration files only in UTF-8 encoding without BOM;
- Comments starting with "#" are only supported in the beginning of the line.

**Parameters**
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Mandatory</th>
<th>Range</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
<td>no</td>
<td></td>
<td></td>
<td>Sets an alias for an item key. It can be used to substitute long and complex item key with a smaller and simpler one. Multiple Alias parameters may be present. Multiple parameters with the same Alias key are not allowed. Different Alias keys may reference the same item key. Aliases can be used in HostMetadataItem but not in HostnameItem parameters.</td>
</tr>
<tr>
<td>AllowRoot</td>
<td>no</td>
<td>0</td>
<td></td>
<td>Allows the agent to run as 'root'. If disabled and the agent is started by 'root', the agent will try to switch to user 'zabbix' instead. Has no effect if started under a regular user. 0 - do not allow 1 - allow</td>
</tr>
<tr>
<td>BufferSend</td>
<td>no</td>
<td>1-3600</td>
<td>5</td>
<td>Do not keep data longer than N seconds in buffer.</td>
</tr>
</tbody>
</table>

Examples:

1. Retrieving the ID of user ‘zabbix’.
   
   ```
   ```
   
   Now shorthand key `zabbix.userid` may be used to retrieve data.

2. Getting CPU utilization with default and custom parameters.
   
   ```
   Alias= cpu.util: system.cpu.util
   Alias= cpu.util[*]: system.cpu.util[*]
   ```
   
   This allows use `cpu.util` key to get CPU utilization percentage with default parameters as well as use `cpu.util[all, idle, avg15]` to get specific data about CPU utilization.

3. Running multiple low-level discovery rules processing the same discovery items.
   
   ```
   Alias= vfs.fs.discovery[*]: vfs.fs.discovery
   ```
   
   Now it is possible to set up several discovery rules using `vfs.fs.discovery` with different parameters for each rule, e.g.,
   `vfs.fs.discovery[foo]`, `vfs.fs.discovery[bar]`, etc.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Mandatory</th>
<th>Range</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BufferSize</td>
<td>no</td>
<td>2-65535</td>
<td>100</td>
<td>Maximum number of values in a memory buffer. The agent will send all collected data to Zabbix server or proxy if the buffer is full.</td>
</tr>
<tr>
<td>DebugLevel</td>
<td>no</td>
<td>0-5</td>
<td>3</td>
<td>Specifies debug level: 0 - basic information about starting and stopping of Zabbix processes 1 - critical information 2 - error information</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3 - warnings 4 - for debugging (produces lots of information) 5 - extended debugging (produces even more information)</td>
</tr>
<tr>
<td>EnableRemoteCommands</td>
<td>no</td>
<td></td>
<td>0</td>
<td>Whether remote commands from Zabbix server are allowed. 0 - not allowed 1 - allowed</td>
</tr>
<tr>
<td>HostMetadata</td>
<td>no</td>
<td>0-255</td>
<td></td>
<td>Optional parameter that defines host metadata. Host metadata is used only at host auto-registration process (active agent). If not defined, the value will be acquired from HostMetadataItem. An agent will issue an error and not start if the specified value is over the limit or a non-UTF-8 string. This option is supported in version 2.2.0 and higher.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Mandatory</td>
<td>Range</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------</td>
<td>----------------</td>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>HostMetadataItem</td>
<td>no</td>
<td>Optional</td>
<td>parameter</td>
<td>Optional parameter that defines a Zabbix agent item used for getting host metadata. This option is only used when HostMetadata is not defined.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>parameter</td>
<td></td>
<td>Supports UserParameters and aliases. Supports system.run[] regardless of EnableRemoteCommands value.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>HostMetadataItem value is retrieved on each auto-registration attempt and is used only at host auto-registration process (active agent).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>During an auto-registration request an agent will log a warning message if the value returned by the specified item is over the limit of 255 characters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>The value returned by the item must be a UTF-8 string otherwise it will be ignored. This option is supported in version 2.2.0 and higher.</td>
</tr>
<tr>
<td>Hostname</td>
<td>no</td>
<td>Set by</td>
<td>Hostnameltem</td>
<td>Optional parameter that defines a Zabbix agent item used for getting hostname. Required for active checks and must match hostname as configured on the server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Allowed characters: alphanumeric, '.', '-', '_'. and '·'.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Maximum length: 64</td>
</tr>
<tr>
<td>Hostnameltem</td>
<td>no</td>
<td>system.hostname</td>
<td></td>
<td>Optional parameter that defines a Zabbix agent item used for getting host name. This option is only used when Hostname is not defined.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Does not support UserParameters or aliases, but does support system.run[] regardless of EnableRemoteCommands value.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>This option is supported in version 1.8.6 and higher.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Mandatory</td>
<td>Range</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
<td>-----------</td>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>Include</td>
<td>no</td>
<td></td>
<td></td>
<td>You may include individual files or all files in a directory in the configuration file. To only include relevant files in the specified directory, the asterisk wildcard character is supported for pattern matching. For example: <code>/absolute/path/to/config/files/*.conf</code>. Pattern matching is supported since Zabbix 2.4.0. See special notes about limitations.</td>
</tr>
<tr>
<td>ListenIP</td>
<td>no</td>
<td>0.0.0.0</td>
<td></td>
<td>List of comma delimited IP addresses that the agent should listen on. Multiple IP addresses are supported in version 1.8.3 and higher.</td>
</tr>
<tr>
<td>ListenPort</td>
<td>no</td>
<td>1024-32767</td>
<td>10050</td>
<td>Agent will listen on this port for connections from the server.</td>
</tr>
</tbody>
</table>
| LoadModule   | no        |           |         | Module to load at agent startup. Modules are used to extend functionality of the agent. Formats: 
LoadModule=<module.so>
LoadModule=<path/module.so>
(since 4.0.9) LoadModule=</abs_path/module.so>
Either the module must be located in directory specified by LoadModulePath or (since 4.0.9) the path must precede the module name. If the preceding path is absolute (starts with '/') then LoadModulePath is ignored. It is allowed to include multiple LoadModule parameters. |
<p>| LoadModulePath| no        |           |         | Full path to location of agent modules. Default depends on compilation options. |
| LogFile      | yes, if LogType is set to file, otherwise no |         |         | Name of log file. |
| LogFileSize  | no        | 0-1024    | 1       | Maximum size of log file in MB. 0 - disable automatic log rotation. Note: If the log file size limit is reached and file rotation fails, for whatever reason, the existing log file is truncated and started anew. |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Mandatory</th>
<th>Range</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LogType</td>
<td>no</td>
<td>file</td>
<td></td>
<td>Log output type: file - write log to file specified by LogFile parameter,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>system - write log to syslog, console - write log to standard output.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>This parameter is supported since Zabbix 3.0.0.</td>
</tr>
<tr>
<td>LogRemoteCommands</td>
<td>no</td>
<td>0</td>
<td></td>
<td>Enable logging of executed shell commands as warnings. 0 - disabled 1 -</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>enabled</td>
</tr>
<tr>
<td>MaxLinesPerSecond</td>
<td>no</td>
<td>1-1000</td>
<td>20</td>
<td>Maximum number of new lines the agent will send per second to Zabbix</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>server or proxy when processing 'log' and 'eventlog' active checks.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>The provided value will be overridden by the parameter 'maxlines',</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>provided in 'log' or 'eventlog' item key.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Note: Zabbix will process 10 times more new lines than set in MaxLinesPerSecond to seek the required string in log items.</td>
</tr>
<tr>
<td>PidFile</td>
<td>no</td>
<td>/tmp/zabbix_agentd.pid</td>
<td></td>
<td>Name of PID file.</td>
</tr>
<tr>
<td>RefreshActiveChecks</td>
<td>no</td>
<td>60-3600</td>
<td>120</td>
<td>How often list of active checks is refreshed, in seconds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Note that after failing to refresh active checks the next refresh will be</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>attempted after 60 seconds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>List of comma delimited IP addresses, optionally in CIDR notation, or DNS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>names of Zabbix servers and Zabbix proxies.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Incoming connections will be accepted only from the hosts listed here.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>If IPv6 support is enabled then '127.0.0.1', ':127.0.0.1', '::127.0.0.1',</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>'::ffff:127.0.0.1' are treated equally and '::/0' will allow any IPv4 or</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>IPv6 address. '0.0.0.0/0' can be used to allow any IPv4 address. Note,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>that &quot;IPv4-compatible IPv6 addresses&quot; (0000::/96 prefix) are supported but</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>deprecated by RFC4291.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Example: Server=127.0.0.1,192.168.1.0/24,::1,2001:db8::/32,zabbix.example.com</td>
</tr>
<tr>
<td>Server</td>
<td>yes, if StartAgents is not explicitly set to 0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Mandatory</td>
<td>Range</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------</td>
<td>--------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ServerActive</td>
<td>no</td>
<td></td>
<td></td>
<td>IP:port (or hostname:port) of Zabbix server or Zabbix proxy for active checks. Multiple comma-delimited addresses can be provided to use several independent Zabbix servers in parallel. Spaces are allowed. If port is not specified, default port is used. IPv6 addresses must be enclosed in square brackets if port for that host is specified. If port is not specified, square brackets for IPv6 addresses are optional. If this parameter is not specified, active checks are disabled.</td>
</tr>
<tr>
<td>SourceIP</td>
<td>no</td>
<td></td>
<td></td>
<td>Source IP address for: - outgoing connections to Zabbix server or Zabbix proxy; - making connections while executing some items (web.page.get, net.tcp.port, etc.)</td>
</tr>
<tr>
<td>StartAgents</td>
<td>no</td>
<td>0-100</td>
<td>3</td>
<td>Number of pre-forked instances of zabbix_agentd that process passive checks. If set to 0, disables passive checks and the agent will not listen on any TCP port. The upper limit used to be 16 before version 1.8.5.</td>
</tr>
<tr>
<td>Timeout</td>
<td>no</td>
<td>1-30</td>
<td>3</td>
<td>Spend no more than Timeout seconds on processing What incoming connections to accept. Used for a passive checks. Multiple values can be specified, separated by comma: unencrypted - accept connections without encryption (default) psk - accept connections with TLS and a pre-shared key (PSK) cert - accept connections with TLS and a certificate</td>
</tr>
<tr>
<td>TLSAccept</td>
<td>yes, if TLS certificate or PSK parameters are defined (even for unencrypted connection), otherwise no</td>
<td></td>
<td></td>
<td>This parameter is supported since Zabbix 3.0.0. Full path name of a file containing the top-level CA(s) certificates for peer certificate verification, used for encrypted communications between Zabbix components. This parameter is supported since Zabbix 3.0.0.</td>
</tr>
<tr>
<td>TLSCAFile</td>
<td>no</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Mandatory</td>
<td>Range</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------</td>
<td>----------------------------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TLSCertFile</td>
<td>no</td>
<td>Full pathname of a file</td>
<td></td>
<td>Containing the agent certificate or certificate chain, used for encrypted communications with Zabbix components. This parameter is supported since Zabbix 3.0.0.</td>
</tr>
<tr>
<td>TLSCipherAll</td>
<td>no</td>
<td>GnuTLS priority string or</td>
<td></td>
<td>OpenSSL (TLS 1.2) cipher string. Override the default cipher suite selection criteria for certificate- and PSK-based encryption. Example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OpenSSL (TLS 1.2) cipher</td>
<td></td>
<td>string. Overridethedefault ciphersuiteselectioncriteriaforcertificate-andPSK-basedencryption.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>string. Overridethedefault</td>
<td></td>
<td>ciphersuiteselectioncriteriaforcertificate-andPSK-basedencryption. Example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ciphersuiteselectioncriteria</td>
<td></td>
<td>for certificate- and PSK-based encryption. Example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>for certificate- and PSK-based</td>
<td></td>
<td>encryption. Example for GnuTLS:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>encryption. Example for</td>
<td></td>
<td>GnuTLS:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example for OpenSSL:</td>
<td></td>
<td>ECDH+aRSA+AES128:RSA+aRSA+AES128</td>
</tr>
<tr>
<td>TLSCipherCert</td>
<td>no</td>
<td>GnuTLS priority string or</td>
<td></td>
<td>OpenSSL (TLS 1.2) cipher string. Override the default cipher suite selection criteria for certificate-based encryption.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OpenSSL (TLS 1.2) cipher</td>
<td></td>
<td>string. Override the default cipher suite selection criteria for certificate-based encryption.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>string. Override the default</td>
<td></td>
<td>cipher suite selection criteria for certificate-based encryption. Example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>cipher suite selection</td>
<td></td>
<td>criteria for certificate-based encryption. Example for GnuTLS:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>criteria for certificate-</td>
<td></td>
<td>and PSK-based encryption. Example for GnuTLS:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and PSK-based encryption.</td>
<td></td>
<td>Example for GnuTLS:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and PSK-based encryption.</td>
<td></td>
<td>Example for OpenSSL:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and PSK-based encryption.</td>
<td></td>
<td>ECDH+aRSA+AES128:RSA+aRSA+AES128</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and PSK-based encryption.</td>
<td></td>
<td>example supported since Zabbix 4.0.19.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and PSK-based encryption.</td>
<td></td>
<td>example supported since Zabbix 4.0.19.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and PSK-based encryption.</td>
<td></td>
<td>example supported since Zabbix 4.0.19.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Mandatory</td>
<td>Range</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------</td>
<td>-------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TLSCipherCert13</td>
<td>no</td>
<td></td>
<td></td>
<td>Cipher string for OpenSSL 1.1.1 or newer in TLS 1.3. Override the default ciphersuite selection criteria for certificate-based encryption. This parameter is supported since Zabbix 4.0.19.</td>
</tr>
<tr>
<td>TLSCipherPSK13</td>
<td>no</td>
<td></td>
<td></td>
<td>Cipher string for OpenSSL 1.1.1 or newer in TLS 1.3. Override the default ciphersuite selection criteria for PSK-based encryption. Example: TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256 This parameter is supported since Zabbix 4.0.19.</td>
</tr>
<tr>
<td>TLSCRLFile</td>
<td>no</td>
<td></td>
<td></td>
<td>Full pathname of a file containing revoked certificates. This parameter is used for encrypted communications with Zabbix components. This parameter is supported since Zabbix 3.0.0.</td>
</tr>
<tr>
<td>TLSKeyFile</td>
<td>no</td>
<td></td>
<td></td>
<td>Full pathname of a file containing the agent private key used for encrypted communications with Zabbix components. This parameter is supported since Zabbix 3.0.0.</td>
</tr>
</tbody>
</table>

**TLSConnect**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Mandatory</th>
<th>Range</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLSConnect</td>
<td>yes, if TLS certificate or PSK parameters are defined (even for unencrypted connection), otherwise no</td>
<td></td>
<td></td>
<td>How the agent should connect to Zabbix server or proxy. Used for active checks. Only one value can be specified: unencrypted - connect without encryption (default) psk - connect using TLS and a pre-shared key (PSK) cert - connect using TLS and a certificate This parameter is supported since Zabbix 4.0.19.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Mandatory</td>
<td>Range</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------</td>
<td>-------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TLSPSKFile</td>
<td>no</td>
<td></td>
<td></td>
<td>Full pathname of a file containing the agent pre-shared key used for encrypted communications with Zabbix components. This parameter is supported since Zabbix 3.0.0.</td>
</tr>
<tr>
<td>TLSPSKIdentity</td>
<td>no</td>
<td></td>
<td></td>
<td>Pre-shared key identity string, used for encrypted communications with Zabbix server. This parameter is supported since Zabbix 3.0.0.</td>
</tr>
<tr>
<td>TLSServerCertIssuer</td>
<td>no</td>
<td></td>
<td></td>
<td>Allowed server (proxy) certificate issuer. This parameter is supported since Zabbix 3.0.0.</td>
</tr>
<tr>
<td>TLSServerCertSubject</td>
<td>no</td>
<td></td>
<td></td>
<td>Allowed server (proxy) certificate subject. This parameter is supported since Zabbix 3.0.0.</td>
</tr>
</tbody>
</table>
| UnsafeUserParameters   | no        | 0,1   | 0       | Allow all characters to be passed in arguments to user-defined parameters. 0 - do not allow 1 - allow. The following characters are not allowed: 
\' " * ? [ ] { } ~ $ ! & ; > | # @ 
Additionally, newline characters are not allowed. Supported since Zabbix 1.8.2. |
| User                   | no        |       | zabbix  | Drop privileges to a specific, existing user on the system. Only has effect if run as ‘root’ and AllowRoot is disabled. This parameter is supported since Zabbix 2.4.0. |
| UserParameter          | no        |       |         | User-defined parameter to monitor. There can be several user-defined parameters. Format: UserParameter=<key>,<shell command> Note that shell command must not return empty string or EOL only. Example: UserParameter=sys:tem.test, who|wc -l |

See also

1. Differences in the Zabbix agent configuration for active and passive checks starting from version 2.0.0

4 Zabbix agent (Windows)

Overview

This section lists parameters supported in a Zabbix agent (Windows) configuration file (zabbix_agentd.conf). Note that:

- The default values reflect daemon defaults, not the values in the shipped configuration files;
Zabbix supports configuration files only in UTF-8 encoding without BOM;
Comments starting with "#" are only supported in the beginning of the line.

### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Mandatory</th>
<th>Range</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
<td>no</td>
<td></td>
<td></td>
<td>Sets an alias for an item key. It can be used to substitute long and complex item key with a smaller and simpler one. Multiple Alias parameters may be present. Multiple parameters with the same Alias key are not allowed. Different Alias keys may reference the same item key. Aliases can be used in HostMetadataItem but not in HostnameItem or PerfCounter parameters.</td>
</tr>
</tbody>
</table>

**Examples:**

1. Retrieving paging file usage in percents from the server.
   Alias=pg_usage:perf_counter[Paging File(_Total)% Usage]
   Now shorthand key **pg_usage** may be used to retrieve data.

2. Getting CPU load with default and custom parameters.
   Alias=cpu.load:system.cpu.load
   Alias=cpu.load[*]:system.cpu.load[*]
   This allows use **cpu.load** key to get CPU utilization percentage with default parameters as well as use **cpu.load[percpu,avg15]** to get specific data about CPU load.

3. Running multiple low-level discovery rules processing the same discovery items.
   Alias=vfs.fs.discovery[*]:vfs.fs.discovery
   Now it is possible to set up several discovery rules using **vfs.fs.discovery** with different parameters for each rule, e.g.,
   **vfs.fs.discovery[foo]**, **vfs.fs.discovery[bar]**, etc.
   Do not keep data longer than N seconds in buffer.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Mandatory</th>
<th>Range</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BufferSize</td>
<td>no</td>
<td>2-65535</td>
<td>100</td>
<td>Maximum number of values in a memory buffer. The agent will send all collected data to Zabbix server or proxy if the buffer is full.</td>
</tr>
<tr>
<td>DebugLevel</td>
<td>no</td>
<td>0-5</td>
<td>3</td>
<td>Specifies debug level: 0 - basic information about starting and stopping of Zabbix processes, 1 - critical information, 2 - error information, 3 - warnings, 4 - for debugging (produces lots of information), 5 - extended debugging (produces even more information)</td>
</tr>
<tr>
<td>EnableRemoteCommands</td>
<td>no</td>
<td>0</td>
<td>0</td>
<td>Whether remote commands from Zabbix server are allowed. 0 - not allowed, 1 - allowed</td>
</tr>
<tr>
<td>HostMetadata</td>
<td>no</td>
<td>0-255</td>
<td>characters</td>
<td>Optional parameter that defines host metadata. Host metadata is used only at host auto-registration process (active agent). If not defined, the value will be acquired from HostMetadataItem. An agent will issue an error and not start if the specified value is over the limit or a non-UTF-8 string. This option is supported in version 2.2.0 and higher.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Mandatory</td>
<td>Range</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------</td>
<td>-------</td>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>HostMetadataItem</td>
<td>no</td>
<td></td>
<td></td>
<td>Optional parameter that defines a Zabbix agent item used for getting host metadata. This option is only used when HostMetadata is not defined. Supports UserParameters, performance counters and aliases. Supports system.run[] regardless of EnableRemoteCommands value. HostMetadataItem value is retrieved on each auto-registration attempt and is used only at host auto-registration process (active agent). During an auto-registration request an agent will log a warning message if the value returned by the specified item is over the limit of 255 characters. The value returned by the item must be a UTF-8 string otherwise it will be ignored. This option is supported in version 2.2.0 and higher.</td>
</tr>
<tr>
<td>Hostname</td>
<td>no</td>
<td></td>
<td>Set by HostnameItem</td>
<td>Unique, case sensitive hostname. Required for active checks and must match hostname as configured on the server. Allowed characters: alphanumeric, '.', ',', '_' and '.'. Maximum length: 64</td>
</tr>
<tr>
<td>HostnameItem</td>
<td>no</td>
<td></td>
<td>system.hostname</td>
<td>Optional parameter that defines a Zabbix agent item used for getting host name. This option is only used when Hostname is not defined. Does not support UserParameters, performance counters or aliases, but does support system.run[] regardless of EnableRemoteCommands value. This option is supported in version 1.8.6 and higher. See also a more detailed description.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Mandatory</td>
<td>Range</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------</td>
<td>----------------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Include</td>
<td>no</td>
<td></td>
<td></td>
<td>You may include individual files or all files in a directory in the configuration file. To only include relevant files in the specified directory, the asterisk wildcard character is supported for pattern matching. For example: C:\Program Files\Zabbix Agent\zabbix_agentd.d*.conf. Pattern matching is supported since Zabbix 2.4.0. See special notes about limitations.</td>
</tr>
<tr>
<td>ListenIP</td>
<td>no</td>
<td>0.0.0.0</td>
<td></td>
<td>List of comma-delimited IP addresses that the agent should listen on. Multiple IP addresses are supported since Zabbix 1.8.3.</td>
</tr>
<tr>
<td>ListenPort</td>
<td>no</td>
<td>1024-32767</td>
<td>10050</td>
<td>Agent will listen on this port for connections from the server.</td>
</tr>
<tr>
<td>LogFile</td>
<td>yes, if LogType is set to file, otherwise no</td>
<td>C:\zabbix_agentd.log</td>
<td></td>
<td>Name of the agent log file.</td>
</tr>
<tr>
<td>LogFileSize</td>
<td>no</td>
<td>0-1024</td>
<td>1</td>
<td>Maximum size of log file in MB. 0 - disable automatic log rotation. Note: If the log file size limit is reached and file rotation fails, for whatever reason, the existing log file is truncated and started anew.</td>
</tr>
<tr>
<td>LogType</td>
<td>no</td>
<td>file</td>
<td></td>
<td>Log output type: file - write log to file specified by LogFile parameter, system - write log Windows Event Log, console - write log to standard output. This parameter is supported since Zabbix 3.0.0.</td>
</tr>
<tr>
<td>LogRemoteCommands</td>
<td>no</td>
<td>0</td>
<td></td>
<td>Enable logging of executed shell commands as warnings. 0 - disabled 1 - enabled</td>
</tr>
<tr>
<td>Parameter</td>
<td>Mandatory</td>
<td>Range</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------</td>
<td>--------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>MaxLinesPerSecond</td>
<td>no</td>
<td>1-1000</td>
<td>20</td>
<td>Maximum number of new lines the agent will send per second to Zabbix server or proxy processing 'log', 'logrt' and 'eventlog' active checks. The provided value will be overridden by the parameter 'maxlines', provided in 'log', 'logrt' or 'eventlog' item keys. Note: Zabbix will process 10 times more new lines than set in MaxLinesPerSecond to seek the required string in log items.</td>
</tr>
<tr>
<td>PerfCounter</td>
<td>no</td>
<td></td>
<td></td>
<td>Syntax: <code>&lt;parameter_name&gt;</code>, <code>&lt;perf_counter_path&gt;</code>, <code>&lt;period&gt;</code> Defines new parameter <code>&lt;parameter_name&gt;</code> which is an average value for system performance counter <code>&lt;perf_counter_path&gt;</code> for the specified time period <code>&lt;period&gt;</code> (in seconds). For example, if you wish to receive average number of processor interrupts per second for last minute, you can define new parameter &quot;interrupts&quot; as following: PerfCounter = interrupts,&quot;\Processor(0)\Interrupts/sec&quot;,60 Please note double quotes around performance counter path. The parameter name (interrupts) is to be used as the item key when creating an item. Samples for calculating average value will be taken every second. You may run &quot;typeperf -qx&quot; to get list of all performance counters available in Windows.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Mandatory</td>
<td>Range</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------</td>
<td>-------</td>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>PerfCounterEn</td>
<td>no</td>
<td></td>
<td></td>
<td>Syntax: <code>&lt;parameter_name&gt;,&quot;&lt;perf_counter_path&gt;&quot;,&lt;period&gt;</code>&lt;br&gt;Defines new parameter <code>&lt;parameter_name&gt;</code> which is an average value for system performance counter <code>&lt;perf_counter_path&gt;</code> for the specified time period <code>&lt;period&gt;</code> (in seconds). Compared to PerfCounter, perfcounter paths must be in English.&lt;br&gt;Supported only on <strong>Windows Server 2008/Vista</strong> and above.&lt;br&gt;For example, if you wish to receive average number of processor interrupts per second for last minute, you can define new parameter &quot;interrupts&quot; as following: <code>PerfCounterEn=interrupts,&quot;\Processor(0)\Interrupts/sec&quot;,60</code>&lt;br&gt;Please note double quotes around performance counter path.&lt;br&gt;The parameter name (interrupts) is to be used as the item key when creating an item.&lt;br&gt;Samples for calculating average value will be taken every second.&lt;br&gt;You can find the list of English strings by viewing the following registry key: <code>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\009</code>. This parameter is supported since Zabbix 4.0.13.&lt;br&gt;How often list of active checks is refreshed, in seconds.&lt;br&gt;Note that after failing to refresh active checks the next refresh will be attempted after 60 seconds.</td>
</tr>
<tr>
<td>RefreshActiveChecks</td>
<td>no</td>
<td>60-3600</td>
<td>120</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Mandatory</td>
<td>Range</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------</td>
<td>--------</td>
<td>---------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Server</td>
<td>yes, if StartAgents is not explicitly set to 0</td>
<td>List of comma delimited IP addresses, optionally in CIDR notation, or DNS names of Zabbix servers. Incoming connections will be accepted only from the hosts listed here. If IPv6 support is enabled then ‘127.0.0.1’, ‘::127.0.0.1’, ‘::ffff:127.0.0.1’ are treated equally and ‘::/0’ will allow any IPv4 or IPv6 address. ‘0.0.0.0/0’ can be used to allow any IPv4 address. Note, that “IPv4-compatible IPv6 addresses” (0000::/96 prefix) are supported but deprecated by RFC4291. Example: Server=127.0.0.1,192.168.1.0/24,::1,2001:db8::/32,zabbix.example.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ServerActive</td>
<td>no</td>
<td>(*)</td>
<td></td>
<td>IP:port (or hostname:port) of Zabbix server or Zabbix proxy for active checks. Multiple comma-delimited addresses can be provided to use several independent Zabbix servers in parallel. Spaces are allowed. If port is not specified, default port is used. IPv6 addresses must be enclosed in square brackets if port for that host is specified. If port is not specified, square brackets for IPv6 addresses are optional. If this parameter is not specified, active checks are disabled. Source IP address for: - outgoing connections to Zabbix server or Zabbix proxy; - making connections while executing some items (web.page.get, net.tcp.port, etc.)</td>
</tr>
<tr>
<td>SourceIP</td>
<td>no</td>
<td></td>
<td></td>
<td>Number of pre-forked instances of zabbix_agentd that process passive checks. If set to 0, disables passive checks and the agent will not listen on any TCP port. The upper limit used to be 16 before version 1.8.5.</td>
</tr>
<tr>
<td>Timeout</td>
<td>no</td>
<td>1-30</td>
<td>3</td>
<td>Spend no more than Timeout seconds on processing</td>
</tr>
<tr>
<td>Parameter</td>
<td>Mandatory</td>
<td>Range</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------------------</td>
<td>-------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TLSAccept</td>
<td>yes, if TLS certificate or PSK parameters are defined (even for unencrypted connection), otherwise no</td>
<td></td>
<td></td>
<td>What incoming connections to accept. Used for a passive checks. Multiple values can be specified, separated by comma: unencrypted - accept connections without encryption (default) psk - accept connections with TLS and a pre-shared key (PSK) cert - accept connections with TLS and a certificate This parameter is supported since Zabbix 3.0.0.</td>
</tr>
<tr>
<td>TLSCAFile</td>
<td>no</td>
<td></td>
<td></td>
<td>Full pathname of a file containing the top-level CA(s) certificates for peer certificate verification, used for encrypted communications between Zabbix components. This parameter is supported since Zabbix 3.0.0.</td>
</tr>
<tr>
<td>TLSCertFile</td>
<td>no</td>
<td></td>
<td></td>
<td>Full pathname of a file containing the agent certificate or certificate chain, used for encrypted communications with Zabbix components. This parameter is supported since Zabbix 3.0.0.</td>
</tr>
<tr>
<td>TLSConnect</td>
<td>yes, if TLS certificate or PSK parameters are defined (even for unencrypted connection), otherwise no</td>
<td></td>
<td></td>
<td>How the agent should connect to Zabbix server or proxy. Used for active checks. Only one value can be specified: unencrypted - connect without encryption (default) psk - connect using TLS and a pre-shared key (PSK) cert - connect using TLS and a certificate This parameter is supported since Zabbix 3.0.0.</td>
</tr>
<tr>
<td>TLSCRLFile</td>
<td>no</td>
<td></td>
<td></td>
<td>Full pathname of a file containing revoked certificates. This parameter is used for encrypted communications with Zabbix components. This parameter is supported since Zabbix 3.0.0.</td>
</tr>
<tr>
<td>TLSKeyFile</td>
<td>no</td>
<td></td>
<td></td>
<td>Full pathname of a file containing the agent private key used for encrypted communications with Zabbix components. This parameter is supported since Zabbix 3.0.0.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Mandatory</td>
<td>Range</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------</td>
<td>-------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TLSPSKFile</td>
<td>no</td>
<td></td>
<td>Full pathname of a file containing the agent pre-shared key used for encrypted communications with Zabbix components. This parameter is supported since Zabbix 3.0.0.</td>
<td></td>
</tr>
<tr>
<td>TLSPSKIdentity</td>
<td>no</td>
<td></td>
<td></td>
<td>Pre-shared key identity string, used for encrypted communications with Zabbix server. This parameter is supported since Zabbix 3.0.0.</td>
</tr>
<tr>
<td>TLSServerCertIssuer</td>
<td>no</td>
<td></td>
<td></td>
<td>Allowed server (proxy) certificate issuer. This parameter is supported since Zabbix 3.0.0.</td>
</tr>
<tr>
<td>TLSServerCertSubject</td>
<td>no</td>
<td></td>
<td></td>
<td>Allowed server (proxy) certificate subject. This parameter is supported since Zabbix 3.0.0.</td>
</tr>
<tr>
<td>UnsafeUserParameters</td>
<td>no</td>
<td>0-1</td>
<td>0</td>
<td>Allow all characters to be passed in arguments to user-defined parameters. 0 - do not allow 1 - allow The following characters are not allowed: \ ` &quot; ' * ? { } ~ $ ! &amp; ; () &gt;</td>
</tr>
<tr>
<td>UserParameter</td>
<td>no</td>
<td></td>
<td></td>
<td>User-defined parameter to monitor. There can be several user-defined parameters. Format: UserParameter=&lt;key&gt;,&lt;shell command&gt; Note that shell command must not return empty string or EOL only. Example: UserParameter=sys-tem.test,echo 1</td>
</tr>
</tbody>
</table>

**Note:**

(*) The number of active servers listed in ServerActive plus the number of pre-forked instances for passive checks specified in StartAgents must be less than 64.

See also

1. Differences in the Zabbix agent configuration for active and passive checks starting from version 2.0.0.

5 Zabbix Java gateway

If you use `startup.sh` and `shutdown.sh` scripts for starting Zabbix Java gateway, then you can specify the necessary configuration parameters in the `settings.sh` file. The startup and shutdown scripts source the settings file and take care of converting shell variables (listed in the first column) to Java properties (listed in the second column).

If you start Zabbix Java gateway manually by running `java` directly, then you specify the corresponding Java properties on the command line.
<table>
<thead>
<tr>
<th>Variable</th>
<th>Property</th>
<th>Mandatory</th>
<th>Range</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LISTEN_IP</td>
<td>zabbix.listenIP</td>
<td>no</td>
<td></td>
<td>0.0.0.0</td>
<td>IP address to listen on.</td>
</tr>
<tr>
<td>LISTEN_PORT</td>
<td>zabbix.listenPort</td>
<td>no</td>
<td>1024-3276</td>
<td>10052</td>
<td>Port to listen on.</td>
</tr>
<tr>
<td>PID_FILE</td>
<td>zabbix.pidFile</td>
<td>no</td>
<td>/tmp/zabbix_java.pid</td>
<td></td>
<td>Name of PID file. If omitted, Zabbix Java Gateway is started as a console application.</td>
</tr>
<tr>
<td>PROPERTIES_FILE</td>
<td>zabbix.propertiesFile</td>
<td>no</td>
<td></td>
<td></td>
<td>Name of properties file. Can be used to set additional properties using a key-value format in such a way that they are not visible on a command line or to overwrite existing ones. For example: &quot;javax.net.ssl.trustStorePassword=&lt;password&gt;&quot;. Supported since Zabbix 4.0.28.</td>
</tr>
<tr>
<td>START_POLLERS</td>
<td>zabbix.startPollers</td>
<td>no</td>
<td>1-1000</td>
<td>5</td>
<td>Number of worker threads to start.</td>
</tr>
<tr>
<td>TIMEOUT</td>
<td>zabbix.timeout</td>
<td>no</td>
<td>1-30</td>
<td>3</td>
<td>How long to wait for network operations.</td>
</tr>
</tbody>
</table>

**Warning:** Port 10052 is not IANA registered.

### 6 Special notes on “Include” parameter

If an Include parameter is used for including a file, the file must be readable.

If an Include parameter is used for including a directory:

- All files in the directory must be readable.
- No particular order of inclusion should be assumed (e.g. files are not included in alphabetical order). Therefore do not define one parameter in several “Include” files (e.g. to override a general setting with a specific one).
- All files in the directory are included into configuration.
- Beware of file backup copies automatically created by some text editors. For example, if editing the “include/my_specific.conf” file produces a backup copy “include/my_specific_conf.BAK” then both files will be included. Move “include/my_specific.conf.BAK” out of the “Include” directory. On Linux, contents of the “Include” directory can be checked with a “ls -al” command for unnecessary files.

If an Include parameter is used for including files using a pattern:

- All files matching the pattern must be readable.
- No particular order of inclusion should be assumed (e.g. files are not included in alphabetical order). Therefore do not define one parameter in several “Include” files (e.g. to override a general setting with a specific one).

### 4 Protocols

#### 1 Server-proxy data exchange protocol

Overview

Server - proxy data exchange is based on JSON format.
Request and response messages must begin with header and data length.

Passive proxy

Proxy config request

The proxy config request is sent by server to provide proxy configuration data. This request is sent every ProxyConfigFrequency (server configuration parameter) seconds.

<table>
<thead>
<tr>
<th>name</th>
<th>value type</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server→proxy:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>request</td>
<td>string</td>
<td>'proxy config'</td>
</tr>
<tr>
<td></td>
<td>object</td>
<td>one or more objects with &lt;table&gt; data</td>
</tr>
<tr>
<td></td>
<td>string</td>
<td>array of field names</td>
</tr>
<tr>
<td></td>
<td>string</td>
<td>field name</td>
</tr>
<tr>
<td></td>
<td>array</td>
<td>array of rows</td>
</tr>
<tr>
<td></td>
<td>string</td>
<td>column value with type depending on column type in database schema</td>
</tr>
<tr>
<td>proxy→server:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>response</td>
<td>string</td>
<td>the request success information ('success' or 'failed')</td>
</tr>
<tr>
<td>version</td>
<td>string</td>
<td>the proxy version (&lt;major&gt;,&lt;minor&gt;,&lt;build&gt;)</td>
</tr>
</tbody>
</table>

Example:

server→proxy:

```json
{
  "request": "proxy config",
  "globalmacro":{
    "fields":[
      "globalmacroid",
      "macro",
      "value"
    ],
    "data": [
      [2,
        "{$SNMP_COMMUNITY}",
        "public"
      ]
    ],
    "hosts":{
      "fields":[
        "hostid",
        "host",
        "status",
        "ipmi_authtype",
        "ipmi_privilage",
        "ipmi_username",
        "ipmi_password",
        "name",
        "tls_connect",
        "tls_accept",
        "tlsIssuer",
        "tls_subject",
        "tls_psk_identity",
        "tls_psk"
      ],
      "data": [
```
Proxy request

The proxy data request is used to obtain host availability, historical, discovery and autoregistration data from proxy. This request is sent every ProxyDataFrequency (server configuration parameter) seconds.

<table>
<thead>
<tr>
<th>name</th>
<th>value type</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server→proxy: request</td>
<td>string</td>
<td>'proxy data'</td>
</tr>
<tr>
<td>proxy→server: session</td>
<td>string</td>
<td>data session token</td>
</tr>
<tr>
<td>host availability</td>
<td>array</td>
<td>(optional) array of host availability data objects</td>
</tr>
<tr>
<td>hostid</td>
<td>number</td>
<td>host identifier</td>
</tr>
<tr>
<td>available</td>
<td>number</td>
<td>Zabbix agent availability</td>
</tr>
<tr>
<td>error</td>
<td>string</td>
<td>Zabbix agent error message or empty string</td>
</tr>
<tr>
<td>snmp_available</td>
<td>number</td>
<td>SNMP agent availability</td>
</tr>
<tr>
<td>snmp_string</td>
<td>string</td>
<td>SNMP agent error message or empty string</td>
</tr>
<tr>
<td>ipmi_available</td>
<td>number</td>
<td>IPMI agent availability</td>
</tr>
<tr>
<td>ipmi_error</td>
<td>string</td>
<td>IPMI agent error message or empty string</td>
</tr>
<tr>
<td>jmx_available</td>
<td>number</td>
<td>JMX agent availability</td>
</tr>
<tr>
<td>jmx_error</td>
<td>string</td>
<td>JMX agent error message or empty string</td>
</tr>
<tr>
<td>history data</td>
<td>array</td>
<td>(optional) array of history data objects</td>
</tr>
<tr>
<td>itemid</td>
<td>number</td>
<td>item identifier</td>
</tr>
<tr>
<td>clock</td>
<td>number</td>
<td>item value timestamp (seconds)</td>
</tr>
<tr>
<td>ns</td>
<td>number</td>
<td>item value timestamp (nanoseconds)</td>
</tr>
<tr>
<td>value</td>
<td>string</td>
<td>(optional) item value</td>
</tr>
<tr>
<td>name</td>
<td>value type</td>
<td>description</td>
</tr>
<tr>
<td>-----------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>id</td>
<td>number</td>
<td>value identifier (ascending counter, unique within one data session)</td>
</tr>
<tr>
<td>timestamp</td>
<td>number</td>
<td>(optional) timestamp of log type items</td>
</tr>
<tr>
<td>source</td>
<td>string</td>
<td>(optional) eventlog item source value</td>
</tr>
<tr>
<td>severity</td>
<td>number</td>
<td>(optional) eventlog item severity value</td>
</tr>
<tr>
<td>eventid</td>
<td>number</td>
<td>(optional) eventlog item eventid value</td>
</tr>
<tr>
<td>state</td>
<td>string</td>
<td>(optional) item state</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0, ITEM_STATE_NORMAL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1, ITEM_STATE_NOTSUPPORTED</td>
</tr>
<tr>
<td>lastlogsize</td>
<td>number</td>
<td>(optional) last log size of log type items</td>
</tr>
<tr>
<td>mtime</td>
<td>number</td>
<td>(optional) modify time of log type items</td>
</tr>
<tr>
<td></td>
<td></td>
<td>array (optional) array of discovery data objects</td>
</tr>
<tr>
<td>clock</td>
<td>number</td>
<td>the discovery data timestamp</td>
</tr>
<tr>
<td>druleid</td>
<td>number</td>
<td>the discovery rule identifier</td>
</tr>
<tr>
<td>dcheckid</td>
<td>number</td>
<td>the discovery check identifier or null for discovery rule data</td>
</tr>
<tr>
<td>type</td>
<td>number</td>
<td>the discovery check type:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-1 discovery rule data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0, SVC_SSH - SSH service check</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1, SVC_LDAP - LDAP service check</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2, SVC_SMTP - SMTP service check</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3, SVC_FTP - FTP service check</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4, SVC_HTTP - HTTP service check</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5, SVC_POP - POP service check</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6, SVC_NNTP - NNTP service check</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7, SVC_IMAP - IMAP service check</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8, SVC_TCP - TCP port availability check</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9, SVC_AGENT - Zabbix agent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10, SVC_SNMPv1 - SNMPv1 agent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11, SVC_SNMPv2 - SNMPv2 agent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>12, SVC_ICMPPING - ICMP ping</td>
</tr>
<tr>
<td></td>
<td></td>
<td>13, SVC_SNMPv3 - SNMPv3 agent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>14, SVC_HTTPS - HTTPS service check</td>
</tr>
<tr>
<td></td>
<td></td>
<td>15, SVC_TELNET - Telnet availability check</td>
</tr>
<tr>
<td>ip</td>
<td>string</td>
<td>the host IP address</td>
</tr>
<tr>
<td>dns</td>
<td>string</td>
<td>the host DNS name</td>
</tr>
<tr>
<td>port</td>
<td>number</td>
<td>(optional) service port number</td>
</tr>
<tr>
<td>key_</td>
<td>string</td>
<td>(optional) the item key for discovery check of type 9 SVC_AGENT</td>
</tr>
<tr>
<td>value</td>
<td>string</td>
<td>(optional) value received from the service, can be empty for most of services</td>
</tr>
<tr>
<td>status</td>
<td>number</td>
<td>(optional) service status:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0, DOBJECT_STATUS_UP - Service UP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1, DOBJECT_STATUS_DOWN - Service DOWN</td>
</tr>
<tr>
<td>auto</td>
<td>array</td>
<td>(optional) array of auto registration data objects</td>
</tr>
<tr>
<td>clock</td>
<td>number</td>
<td>the auto registration data timestamp</td>
</tr>
<tr>
<td>host</td>
<td>string</td>
<td>the host name</td>
</tr>
<tr>
<td>ip</td>
<td>string</td>
<td>(optional) the host IP address</td>
</tr>
<tr>
<td>dns</td>
<td>string</td>
<td>(optional) the resolved DNS name from IP address</td>
</tr>
<tr>
<td>port</td>
<td>string</td>
<td>(optional) the host port</td>
</tr>
<tr>
<td>host_metadata</td>
<td>string</td>
<td>(optional) the host metadata sent by agent (based on HostMetadata or HostMetadataItem agent configuration parameter)</td>
</tr>
<tr>
<td>tasks</td>
<td>array</td>
<td>(optional) array of tasks</td>
</tr>
<tr>
<td>name</td>
<td>value type</td>
<td>description</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>type</td>
<td>number</td>
<td>the task type:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0. ZBX_TM_TASK_PROCESS_REMOTE_COMMAND_RESULT - remote command result</td>
</tr>
<tr>
<td>status</td>
<td>number</td>
<td>the remote command execution status:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0. ZBX_TM_REMOTE_COMMAND_COMPLETED - the remote command completed successfully</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. ZBX_TM_REMOTE_COMMAND_FAILED - the remote command failed</td>
</tr>
<tr>
<td>error</td>
<td>string</td>
<td>(optional) the error message</td>
</tr>
<tr>
<td>parent_taskid</td>
<td>number</td>
<td>the parent task id</td>
</tr>
<tr>
<td>more</td>
<td>number</td>
<td>(optional) 1 - there are more history data to send</td>
</tr>
<tr>
<td>clock</td>
<td>number</td>
<td>(optional) data transfer timestamp (seconds)</td>
</tr>
<tr>
<td>ns</td>
<td>number</td>
<td>(optional) data transfer timestamp (nanoseconds)</td>
</tr>
<tr>
<td>version</td>
<td>string</td>
<td>the proxy version (&lt;major&gt;.&lt;minor&gt;.&lt;build&gt;)</td>
</tr>
<tr>
<td>server-proxy:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>response</td>
<td>string</td>
<td>the request success information ('success' or 'failed')</td>
</tr>
<tr>
<td>tasks</td>
<td>array</td>
<td>(optional) array of tasks</td>
</tr>
<tr>
<td>type</td>
<td>number</td>
<td>the task type:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. ZBX_TM_TASK_PROCESS_REMOTE_COMMAND - remote command</td>
</tr>
<tr>
<td>clock</td>
<td>number</td>
<td>the task creation time</td>
</tr>
<tr>
<td>ttl</td>
<td>number</td>
<td>the time in seconds after which task expires</td>
</tr>
<tr>
<td>command_type</td>
<td>number</td>
<td>the remote command type:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0. ZBX_SCRIPT_TYPE_CUSTOM_SCRIPT - use custom script</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. ZBX_SCRIPT_TYPE_IPMI - use IPMI</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. ZBX_SCRIPT_TYPE_SSH - use SSH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. ZBX_SCRIPT_TYPE_TELNET - use Telnet</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. ZBX_SCRIPT_TYPE_GLOBAL_SCRIPT - use global script (currently functionally equivalent to custom script)</td>
</tr>
<tr>
<td>command</td>
<td>string</td>
<td>the remote command to execute</td>
</tr>
<tr>
<td>execute_target</td>
<td>number</td>
<td>the execution target for custom scripts:</td>
</tr>
<tr>
<td>port</td>
<td>number</td>
<td>(optional) the port for telnet and ssh commands</td>
</tr>
<tr>
<td>authtype</td>
<td>number</td>
<td>(optional) the authentication type for ssh commands</td>
</tr>
<tr>
<td>username</td>
<td>string</td>
<td>(optional) the user name for telnet and ssh commands</td>
</tr>
<tr>
<td>password</td>
<td>string</td>
<td>(optional) the password for telnet and ssh commands</td>
</tr>
<tr>
<td>publickey</td>
<td>string</td>
<td>(optional) the public key for ssh commands</td>
</tr>
<tr>
<td>privatekey</td>
<td>string</td>
<td>(optional) the private key for ssh commands</td>
</tr>
<tr>
<td>parent_taskid</td>
<td>number</td>
<td>the parent task id</td>
</tr>
<tr>
<td>hostid</td>
<td>number</td>
<td>target host id</td>
</tr>
</tbody>
</table>
Example:

server→proxy:
```
{
   "request": "proxy data"
}
```

proxy→server:
```
{
   "session": "12345678901234567890123456789012"
   "host availability": [
      {
         "hostid": 10106,
         "available": 1,
         "error": "",
         "snmp_available": 0,
         "snmp_error": "",
         "ipmi_available": 0,
         "ipmi_error": "",
         "jmx_available": 0,
         "jmx_error": ""
      },
      {
         "hostid": 10107,
         "available": 1,
         "error": "",
         "snmp_available": 0,
         "snmp_error": "",
         "ipmi_available": 0,
         "ipmi_error": "",
         "jmx_available": 0,
         "jmx_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": "4.0.0"
}
}
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": "lsuusFncCzWBQ7RKNUSsemQRMSGkVb1/3j+skZ6UtW+5u09lHNsj6tQ5QCqKuk01De7zhd",
"parent_taskid": 10,
"hostid": 10070
},
{
"type": 1,
"}
Active proxy
Proxy heartbeat request
The proxy heartbeat request is sent by proxy to report that proxy is running. This request is sent every HeartbeatFrequency (proxy configuration parameter) seconds.

<table>
<thead>
<tr>
<th>name</th>
<th>value type</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>proxy-&gt;server:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>request</td>
<td>string</td>
<td>'proxy heartbeat'</td>
</tr>
<tr>
<td>host</td>
<td>string</td>
<td>the proxy name</td>
</tr>
<tr>
<td>version</td>
<td>string</td>
<td>the proxy version (&lt;major&gt;.&lt;minor&gt;.&lt;build&gt;)</td>
</tr>
</tbody>
</table>

proxy->server:
{
   "request": "proxy heartbeat",
   "host": "Proxy #12",
   "version": "4.0.0"
}

server->proxy:
{
   "response": "success"
}

Proxy config request
The proxy config request is sent by proxy to obtain proxy configuration data. This request is sent every ConfigFrequency (proxy configuration parameter) seconds.

<table>
<thead>
<tr>
<th>name</th>
<th>value type</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>proxy-&gt;server:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>request</td>
<td>string</td>
<td>'proxy config'</td>
</tr>
<tr>
<td>host</td>
<td>string</td>
<td>proxy name</td>
</tr>
<tr>
<td>version</td>
<td>string</td>
<td>the proxy version (&lt;major&gt;.&lt;minor&gt;.&lt;build&gt;)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>name</th>
<th>value type</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server-&gt;proxy:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>request</td>
<td>string</td>
<td>'proxy config'</td>
</tr>
<tr>
<td>&lt;table&gt;</td>
<td>object</td>
<td>one or more objects with &lt;table&gt; data</td>
</tr>
<tr>
<td>fields</td>
<td>array</td>
<td>array of field names</td>
</tr>
<tr>
<td></td>
<td>string</td>
<td>field name</td>
</tr>
<tr>
<td>data</td>
<td>array</td>
<td>array of rows</td>
</tr>
<tr>
<td></td>
<td>array</td>
<td>array of columns</td>
</tr>
<tr>
<td>name</td>
<td>value type</td>
<td>description</td>
</tr>
<tr>
<td>----------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>proxy→server:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>response</td>
<td>string</td>
<td>the request success information ('success' or 'failed')</td>
</tr>
</tbody>
</table>

Example:

```json
proxy→server:
{
    "request": "proxy config",
    "host": "Proxy #12",
    "version": "4.0.0"
}

server→proxy:
{
    "globalmacro": {
        "fields": ["globalmacroid", "macro", "value"],
        "data": [
            [2, "${SNMP_COMMUNITY}", "public"
        ]
    },
    "hosts": {
        "fields": ["hostid", "host", "status", "ipmi_authtype", "ipmi_privilege", "ipmi_username", "ipmi_password", "name", "tls_connect", "tls_accept", "tls_issuer", "tls_subject", "tls_psk_identity", "tls_psk"
        ],
        "data": [
            [10001, "Template OS Linux", 3, -1, 2, "", "", "Template OS Linux", 1, 1,
```
`,
[
  10050,
  "Template App Zabbix Agent",
  3,
  -1,
  2,
  "",
  "",
  "Template App Zabbix Agent",
  1,
  1,
  "",
  "",
  "",
  "",
]
],
[
  10105,
  "Logger",
  0,
  -1,
  2,
  "",
  "",
  "Logger",
  1,
  1,
  "",
  "",
  "",
  "",
]
],
"interface":{
  "fields":[
    "interfaceid",
    "hostid",
    "main",
    "type",
    "useip",
    "ip",
    "dns",
    "port",
    "bulk"
  ],
  "data":[
    [2,
     10105,
     1,
     1,
     127.0.0.1,
     "",
     "",
     "10050",
     1]
Proxy data request

The proxy data request is sent by proxy to provide host availability, history, discovery and autoregistration data. This request is sent every `DataSenderFrequency` (proxy configuration parameter) seconds. Note that active proxy will still poll Zabbix server every second for remote command tasks (with an empty proxy data request).

<table>
<thead>
<tr>
<th>name</th>
<th>value type</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>proxy→server:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>request</td>
<td>string</td>
<td>‘proxy data’</td>
</tr>
<tr>
<td>host</td>
<td>string</td>
<td>the proxy name</td>
</tr>
<tr>
<td>session</td>
<td>string</td>
<td>data session token</td>
</tr>
<tr>
<td>host availability</td>
<td>array</td>
<td>(optional) array of host availability data objects</td>
</tr>
<tr>
<td>hostid</td>
<td>number</td>
<td>host identifier</td>
</tr>
<tr>
<td>available</td>
<td>number</td>
<td>Zabbix agent availability</td>
</tr>
<tr>
<td>error</td>
<td>string</td>
<td>Zabbix agent error message or empty string</td>
</tr>
<tr>
<td>snmp_available</td>
<td>number</td>
<td>SNMP agent availability</td>
</tr>
<tr>
<td>snmp_string</td>
<td>number</td>
<td>SNMP agent error message or empty string</td>
</tr>
<tr>
<td>ipmi_available</td>
<td>number</td>
<td>IPMI agent availability</td>
</tr>
<tr>
<td>ipmi_error</td>
<td>string</td>
<td>IPMI agent error message or empty string</td>
</tr>
<tr>
<td>jmx_available</td>
<td>number</td>
<td>JMX agent availability</td>
</tr>
<tr>
<td>jmx_error</td>
<td>string</td>
<td>JMX agent error message or empty string</td>
</tr>
<tr>
<td>history data</td>
<td>array</td>
<td>(optional) array of history data objects</td>
</tr>
<tr>
<td>itemid</td>
<td>number</td>
<td>item identifier</td>
</tr>
<tr>
<td>clock</td>
<td>number</td>
<td>item value timestamp (seconds)</td>
</tr>
<tr>
<td>ns</td>
<td>number</td>
<td>item value timestamp (nanoseconds)</td>
</tr>
<tr>
<td>value</td>
<td>string</td>
<td>(optional) item value</td>
</tr>
<tr>
<td>id</td>
<td>number</td>
<td>value identifier (ascending counter, unique within one data session)</td>
</tr>
<tr>
<td>timestamp</td>
<td>number</td>
<td>(optional) timestamp of log type items</td>
</tr>
<tr>
<td>source</td>
<td>string</td>
<td>(optional) eventlog item source value</td>
</tr>
<tr>
<td>severity</td>
<td>number</td>
<td>(optional) eventlog item severity value</td>
</tr>
<tr>
<td>eventid</td>
<td>number</td>
<td>(optional) eventlog item eventid value</td>
</tr>
<tr>
<td>state</td>
<td>string</td>
<td>(optional) item state</td>
</tr>
<tr>
<td>lastlogsize</td>
<td>number</td>
<td>(optional) last log size of log type items</td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>name</th>
<th>value type</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mtime</td>
<td>number</td>
<td>(optional) modify time of log type items</td>
</tr>
<tr>
<td>clock</td>
<td>array</td>
<td>(optional) array of discovery data objects</td>
</tr>
<tr>
<td>druleid</td>
<td>number</td>
<td>the discovery rule identifier</td>
</tr>
<tr>
<td>dcheckid</td>
<td>number</td>
<td>the discovery check identifier or null for discovery rule data</td>
</tr>
<tr>
<td>type</td>
<td>number</td>
<td>the discovery check type:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-1 discovery rule data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0. SVC_SSH - SSH service check</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. SVC_LDAP - LDAP service check</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. SVC_SMTP - SMTP service check</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. SVC_FTP - FTP service check</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. SVC_HTTP - HTTP service check</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. SVC_POP - POP service check</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6. SVC_NNTP - NNTP service check</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7. SVC_IMAP - IMAP service check</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8. SVC_TCP - TCP port availability check</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9. SVC_AGENT - Zabbix agent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10, SVC_SNMPv1 - SNMPv1 agent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11, SVC_SNMPv2 - SNMPv2 agent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>12, SVC_ICMPPING - ICMP ping</td>
</tr>
<tr>
<td></td>
<td></td>
<td>13, SVC_SNMPv3 - SNMPv3 agent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>14, SVC_HTTPS - HTTPS service check</td>
</tr>
<tr>
<td></td>
<td></td>
<td>15, SVC_TELNET - Telnet availability check</td>
</tr>
<tr>
<td>ip</td>
<td>string</td>
<td>the host IP address</td>
</tr>
<tr>
<td>dns</td>
<td>string</td>
<td>the host DNS name</td>
</tr>
<tr>
<td>port</td>
<td>number</td>
<td>(optional) service port number</td>
</tr>
<tr>
<td>key_</td>
<td>string</td>
<td>(optional) the item key for discovery check of type 9 SVC_AGENT</td>
</tr>
<tr>
<td>value</td>
<td>string</td>
<td>(optional) value received from the service, can be empty for most of services</td>
</tr>
<tr>
<td>status</td>
<td>number</td>
<td>(optional) service status:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0. DOBJECT_STATUS_UP - Service UP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. DOBJECT_STATUS_DOWN - Service DOWN</td>
</tr>
<tr>
<td>auto registration</td>
<td>array</td>
<td>(optional) array of auto registration data objects</td>
</tr>
<tr>
<td>clock</td>
<td>number</td>
<td>the auto registration data timestamp</td>
</tr>
<tr>
<td>host</td>
<td>string</td>
<td>the host name</td>
</tr>
<tr>
<td>ip</td>
<td>string</td>
<td>(optional) the resolved IP address</td>
</tr>
<tr>
<td>dns</td>
<td>string</td>
<td>(optional) the resolved DNS name from IP address</td>
</tr>
<tr>
<td>port</td>
<td>string</td>
<td>(optional) the host port</td>
</tr>
<tr>
<td>host_metadata</td>
<td>string</td>
<td>(optional) the host metadata sent by agent (based on HostMetadata or HostMetadataItem agent configuration parameter)</td>
</tr>
<tr>
<td>tasks</td>
<td>array</td>
<td>(optional) array of tasks</td>
</tr>
<tr>
<td>type</td>
<td>number</td>
<td>the task type:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0. ZBX_TM_TASK_PROCESS_REMOTE_COMMAND_RESULT - remote command result</td>
</tr>
<tr>
<td>status</td>
<td>number</td>
<td>the remote command execution status:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0. ZBX_TM_REMOTE_COMMAND_COMPLETED - the remote command completed successfully</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. ZBX_TM_REMOTE_COMMAND_FAILED - the remote command failed</td>
</tr>
<tr>
<td>error</td>
<td>string</td>
<td>(optional) the error message</td>
</tr>
<tr>
<td>parent_taskid</td>
<td></td>
<td>the parent task id</td>
</tr>
<tr>
<td>name</td>
<td>value type</td>
<td>description</td>
</tr>
<tr>
<td>------------</td>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>more</td>
<td>number</td>
<td>(optional) 1 - there are more history data to send</td>
</tr>
<tr>
<td>clock</td>
<td>number</td>
<td>(optional) data transfer timestamp (seconds)</td>
</tr>
<tr>
<td>ns</td>
<td>number</td>
<td>(optional) data transfer timestamp (nanoseconds)</td>
</tr>
<tr>
<td>version</td>
<td>string</td>
<td>the proxy version (&lt;major&gt;.&lt;minor&gt;.&lt;build&gt;)</td>
</tr>
<tr>
<td>response</td>
<td>string</td>
<td>the request success information ('success' or 'failed')</td>
</tr>
<tr>
<td>tasks</td>
<td>array</td>
<td>(optional) array of tasks</td>
</tr>
<tr>
<td>type</td>
<td>number</td>
<td>the task type:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. ZBX_TM_TASK_PROCESS_REMOTE_COMMAND - remote command</td>
</tr>
<tr>
<td>clock</td>
<td>number</td>
<td>the task creation time</td>
</tr>
<tr>
<td>ttl</td>
<td>number</td>
<td>the time in seconds after which task expires</td>
</tr>
<tr>
<td>commandtype</td>
<td>number</td>
<td>the remote command type:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0. ZBX_SCRIPT_TYPE_CUSTOM_SCRIPT - use custom script</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. ZBX_SCRIPT_TYPE_IPMI - use IPMI</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. ZBX_SCRIPT_TYPE_SSH - use SSH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. ZBX_SCRIPT_TYPE_TELNET - use Telnet</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. ZBX_SCRIPT_TYPE_GLOBAL_SCRIPT - use global script (currently functionally equivalent to custom script)</td>
</tr>
<tr>
<td>command</td>
<td>string</td>
<td>the remote command to execute</td>
</tr>
<tr>
<td>executeon</td>
<td>number</td>
<td>the execution target for custom scripts:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0. ZBX_SCRIPT_EXECUTE_ON_AGENT - execute script on agent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. ZBX_SCRIPT_EXECUTE_ON_SERVER - execute script on server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. ZBX_SCRIPT_EXECUTE_ON_PROXY - execute script on proxy</td>
</tr>
<tr>
<td>port</td>
<td>number</td>
<td>(optional) the port for telnet and ssh commands</td>
</tr>
<tr>
<td>authtype</td>
<td>number</td>
<td>(optional) the authentication type for ssh commands</td>
</tr>
<tr>
<td>username</td>
<td>string</td>
<td>(optional) the user name for telnet and ssh commands</td>
</tr>
<tr>
<td>password</td>
<td>string</td>
<td>(optional) the password for telnet and ssh commands</td>
</tr>
<tr>
<td>publickey</td>
<td>string</td>
<td>(optional) the public key for ssh commands</td>
</tr>
<tr>
<td>privatekey</td>
<td>string</td>
<td>(optional) the private key for ssh commands</td>
</tr>
<tr>
<td>parentid</td>
<td>number</td>
<td>the parent task id</td>
</tr>
<tr>
<td>hostid</td>
<td>number</td>
<td>target hostid</td>
</tr>
</tbody>
</table>

Example:

proxy→server:

```json
{
    "request": "proxy data",
    "host": "Proxy #12",
    "session": "12345678901234567890123456789012",
    "host availability": [
        {
            "hostid": 10106,
            "available": 1,
            "error": "",
            "snmp_available": 0,
```
"clock":1478608381,
"host":"Logger2",
"ip":"10.3.0.2",
"dns":"localhost",
"port":"10050"
],
"tasks": [
{
"type": 2,
"clock":1478608371,
"ttl":600,
"commandtype": 2,
"command": "restart_service1.sh",
"execute_on": 2,
"port": 80,
"authtype": 0,
"username": "userA",
"password": "password",
"publickey": "MIIGMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCqGKukO1De7zhZj6+H0qtjTkVzuTCpvrKe",
"privatekey": "lsuusFncZwBQ7RKNUSesmQRMSGkVb1/3j++skZ6UtW+5u091HNa6J6tQ5QCgKuk01De7zhd",
"parent_taskid": 10,
"hostid": 10070
},
{
"type": 2,
"clock":1478608381,
"ttl":600,
"commandtype": 1,
"command": "restart_service2.sh",
"execute_on": 0,
"authtype": 0,
"username": "",
"password": "",
"publickey": "",
"privatekey": "",
"parent_taskid": 20,
"hostid": 10084
}
],
"tasks": [
{
"type": 0,
"status": 0,
"parent_taskid": 10
},
{
"type": 0,
"status": 1,
"error": "No permissions to execute task.",
"parent_taskid": 20
}
],
"version":"4.0.0"
}
server→proxy:
{
"response": "success",
"tasks": [
Backwards compatibility

Server supports partial backwards compatibility by accepting old host availability, history data, discovery data and auto registration requests.

2 Zabbix agent protocol

Please refer to Passive and active agent checks page for more information.

3 Zabbix sender protocol

Please refer to Trapper items page for more information.

4 Header

Overview

The header is present in all request and response messages between Zabbix components. It is required to determine the message length, if it is compressed or not, if it is a large packet or not.

Zabbix communications protocol has 1GB packet size limit per connection. The limit of 1GB is applied to both the received packet data length and the uncompressed data length.

When sending configuration to Zabbix proxy, the packet size limit is increased to 4GB to allow syncing large configurations. When data length before compression exceeds 4GB, Zabbix server automatically starts using the large packet format (0x04 flag) which increases the packet size limit to 16GB.

Note that while a large packet format can be used for sending any data, currently only the Zabbix proxy configuration syncer can handle packets that are larger than 1GB.
Structure

The header consists of four fields. All numbers in the header are formatted as little-endian.

<table>
<thead>
<tr>
<th>Field</th>
<th>Size (large packet)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;PROTOCOL&gt;</td>
<td>4</td>
<td>&quot;ZBXD&quot; or 5A 42 58 44</td>
</tr>
<tr>
<td>&lt;FLAGS&gt;</td>
<td>1</td>
<td>Protocol flags:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0x01 - Zabbix communications protocol</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0x02 - compression</td>
</tr>
<tr>
<td>&lt;DATALEN&gt;</td>
<td>4</td>
<td>Data length.</td>
</tr>
<tr>
<td>&lt;RESERVED&gt;</td>
<td>4</td>
<td>When compression is used (0x02 flag) - the length of uncompressed data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When compression is not used - 00 00 00 00</td>
</tr>
</tbody>
</table>

Examples

Here are some code snippets showing how to add Zabbix protocol header to the data you want to send in order to obtain the packet you should send to Zabbix so that it is interpreted correctly. These code snippets assume that the data is not larger than 1GB, thus the large packet format is not used.

Python

```python
packet = b"ZBXD\1" + struct.pack("<II", len(data), 0) + data
```

or

```python
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

```perl
my $packet = "ZBXD\1" . pack("(II)<", length($data), 0) . $data;
```

or

```perl
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
    {
```
5 Real-time export protocol

This section presents details of the real-time export protocol in a newline-delimited JSON format for:

- trigger events
- item values
- trends

All files have a .ndjson extension. Each line of the export file is a JSON object.

Trigger events

The following information is exported for a problem event:

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hosts</td>
<td>array</td>
<td>List of hosts involved in the trigger expression; there should be at least one element in array.</td>
</tr>
<tr>
<td>-</td>
<td>string</td>
<td>Visible host name.</td>
</tr>
<tr>
<td>groups</td>
<td>array</td>
<td>List of host groups of all hosts involved in the trigger expression; there should be at least one element in array.</td>
</tr>
<tr>
<td>-</td>
<td>string</td>
<td>Host group name.</td>
</tr>
<tr>
<td>tags</td>
<td>array</td>
<td>List of problem tags (can be empty).</td>
</tr>
<tr>
<td>-</td>
<td>object</td>
<td></td>
</tr>
</tbody>
</table>

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" "$data"
<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tag</td>
<td>string</td>
<td>Tag name.</td>
</tr>
<tr>
<td>value</td>
<td>string</td>
<td>Tag value (can be empty).</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>Problem event name.</td>
</tr>
<tr>
<td>clock</td>
<td>number</td>
<td>Number of seconds since Epoch to the moment when problem was detected (integer part).</td>
</tr>
<tr>
<td>ns</td>
<td>number</td>
<td>Number of nanoseconds to be added to clock to get a precise problem detection time.</td>
</tr>
<tr>
<td>eventid</td>
<td>number</td>
<td>Problem event ID.</td>
</tr>
<tr>
<td>value</td>
<td>number</td>
<td>1 (always).</td>
</tr>
</tbody>
</table>

The following information is exported for a recovery event:

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clock</td>
<td>number</td>
<td>Number of seconds since Epoch to the moment when problem was resolved (integer part).</td>
</tr>
<tr>
<td>ns</td>
<td>number</td>
<td>Number of nanoseconds to be added to clock to get a precise problem resolution time.</td>
</tr>
<tr>
<td>eventid</td>
<td>number</td>
<td>Recovery event ID.</td>
</tr>
<tr>
<td>p_eventid</td>
<td>number</td>
<td>Problem event ID.</td>
</tr>
<tr>
<td>value</td>
<td>number</td>
<td>0 (always).</td>
</tr>
</tbody>
</table>

Examples

Problem:

```json
{"hosts": ["Host B","Zabbix Server"], "groups": ["Group X","Group Y","Group Z","Zabbix servers"], "tags": [{"ta... on Host B or pollers are too busy on Zabbix Server"},
  "clock": 1519304285,
  "ns": 123456789,
  "eventid": 42,
  "value": 1}
```

Recovery:

```json
{"clock": 1519304345,
  "ns": 987654321,
  "eventid": 43,
  "p_eventid": 42,
  "value": 0}
```

Problem (multiple problem event generation):

```json
{"hosts": ["Host B","Zabbix Server"], "groups": ["Group X","Group Y","Group Z","Zabbix servers"], "tags": [{"tags... on Host B or pollers are too busy on Zabbix Server"},
  {"hosts": ["Host B","Zabbix Server"], "groups": ["Group X","Group Y","Group Z","Zabbix servers"], "tags": [{"tags... on Host B or pollers are too busy on Zabbix Server"},
  "clock": 1519304286,
  "ns": 123456789,
  "eventid": 43,
  "value": 1}]
```

Recovery:

```json
{"clock": 1519304346,
  "ns": 987654321,
  "eventid": 44,
  "p_eventid": 42,
  "value": 0}
```

```json
{"clock": 1519304346,
  "ns": 987654321,
  "eventid": 44,
  "p_eventid": 42,
  "value": 0}
```

Item values

The following information is exported for a collected item value:

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host</td>
<td>string</td>
<td>Visible host name of the item host.</td>
</tr>
<tr>
<td>groups</td>
<td>array</td>
<td>List of host groups of the item host; there should be at least one element in array.</td>
</tr>
<tr>
<td>applications</td>
<td>array</td>
<td>List of the item applications; empty if there are none.</td>
</tr>
<tr>
<td>itemid</td>
<td>number</td>
<td>Item ID.</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>Visible item name.</td>
</tr>
<tr>
<td>clock</td>
<td>number</td>
<td>Number of seconds since Epoch to the moment when value was collected (integer part).</td>
</tr>
<tr>
<td>ns</td>
<td>number</td>
<td>Number of nanoseconds to be added to clock to get a precise value collection time.</td>
</tr>
<tr>
<td>timestamp</td>
<td>number</td>
<td>0 if not available.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source</td>
<td>string</td>
<td>Empty string if not available.</td>
</tr>
<tr>
<td>severity</td>
<td>number</td>
<td>0 if not available.</td>
</tr>
<tr>
<td>eventid</td>
<td>number</td>
<td>0 if not available.</td>
</tr>
<tr>
<td>value</td>
<td>number (for numeric items) or string (for text items)</td>
<td>Collected item value.</td>
</tr>
</tbody>
</table>

### Examples

**Numeric (unsigned) value:**

```json
{"host":"Host B","groups":["Group X","Group Y","Group Z"],"applications":["Zabbix Agent","Availability"],"itemid":3,"name":"Agent availability","clock":1519304285,"ns":123456789,"value":1}
```

**Numeric (float) value:**

```json
{"host":"Host B","groups":["Group X","Group Y","Group Z"],"applications":["CPU","Performance"],"itemid":4,"name":"CPU Load","clock":1519304285,"ns":123456789,"value":0.1}
```

**Character, text value:**

```json
{"host":"Host B","groups":["Group X","Group Y","Group Z"],"applications":["Zabbix Agent","Installed software versions"],"itemid":2,"name":"Agent version","clock":1519304285,"ns":123456789,"value":"3.4.4"}
```

**Log value:**

```json
{"host":"Host A","groups":["Group X","Group Y","Group Z"],"applications":["Log files","Critical"],"itemid":5,"name":"Log file message"}
```

### Trends

The following information is exported for a calculated trend value:

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host</td>
<td>string</td>
<td>Visible host name of the item host.</td>
</tr>
<tr>
<td>groups</td>
<td>array</td>
<td>List of host groups of the item host; there should be at least one element in array.</td>
</tr>
<tr>
<td>-</td>
<td>string</td>
<td>Host group name.</td>
</tr>
<tr>
<td>applications</td>
<td>array</td>
<td>List of the item applications; empty if there are none.</td>
</tr>
<tr>
<td>-</td>
<td>string</td>
<td>Application name.</td>
</tr>
<tr>
<td>itemid</td>
<td>number</td>
<td>Item ID.</td>
</tr>
<tr>
<td>name</td>
<td>string</td>
<td>Visible item name.</td>
</tr>
<tr>
<td>clock</td>
<td>number</td>
<td>Number of seconds since Epoch to the moment when value was collected (integer part).</td>
</tr>
<tr>
<td>count</td>
<td>number</td>
<td>Number of values collected for a given hour.</td>
</tr>
<tr>
<td>min</td>
<td>number</td>
<td>Minimum item value for a given hour.</td>
</tr>
<tr>
<td>avg</td>
<td>number</td>
<td>Average item value for a given hour.</td>
</tr>
<tr>
<td>max</td>
<td>number</td>
<td>Maximum item value for a given hour.</td>
</tr>
</tbody>
</table>

**Examples**

**Numeric (unsigned) value:**

```json
{"host":"Host B","groups":["Group X","Group Y","Group Z"],"applications":["Zabbix Agent","Availability"],"itemid":3,"name":"Agent availability","clock":1519311600,"count":60,"min":1,"avg":1,"max":1}
```

**Numeric (float) value:**

```json
{"host":"Host B","groups":["Group X","Group Y","Group Z"],"applications":["CPU","Performance"],"itemid":4,"name":"CPU Load","clock":1519311600,"count":60,"min":0.01,"avg":0.15,"max":1.5}
```

5 Items
## 1 Items supported by platform

The table displays support for Zabbix agent items on various platforms:

- Items marked with "X" are supported, the ones marked with "-" are not supported.
- If an item is marked with "?", it is not known whether it is supported or not.
- If an item is marked with "r", it means that it requires root privileges.
- Parameters that are included in angle brackets <like_this> are optional.

[Note: Windows-only Zabbix agent items are not included in this table.]

<table>
<thead>
<tr>
<th>Platform</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>window</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mac</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OS X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tru64</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AIX</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HP-UX</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Solaris</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FreeBSD</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Linux</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.6 (and later)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Linux</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows</td>
<td>▼▼</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Parameters

<table>
<thead>
<tr>
<th>System</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Linux</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NetBSD</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OpenBSD</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AIX</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HP-UX</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Solaris</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FreeBSD</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Linux</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.6 (and later)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Linux</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>/ system</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>agent.hostname</strong></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>agent.ping</strong></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>agent.version</strong></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>kernel.maxfiles</strong></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>?</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>kernel.maxproc</strong></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>log[file, &lt;regexp&gt;, &lt;encoding&gt;, &lt;maxlines&gt;, &lt;mode&gt;, &lt;output&gt;, &lt;maxdelay&gt;]</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>log.count[file, &lt;regexp&gt;, &lt;encoding&gt;, &lt;maxproclines&gt;, &lt;mode&gt;, &lt;maxdelay&gt;]</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>logrt[file_regex, &lt;regexp&gt;, &lt;encoding&gt;, &lt;maxlines&gt;, &lt;mode&gt;, &lt;output&gt;, &lt;maxdelay&gt;, &lt;options&gt;]</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>logrt.count[file_regex, &lt;regexp&gt;, &lt;encoding&gt;, &lt;maxlines&gt;, &lt;mode&gt;, &lt;maxdelay&gt;, &lt;options&gt;]</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>net.dns[&lt;ip&gt;, zone, &lt;type&gt;, &lt;timeout&gt;, &lt;count&gt;]</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>net.dns.record[&lt;ip&gt;, zone, &lt;type&gt;, &lt;timeout&gt;, &lt;count&gt;]</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>net.if.discovery</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>net.if.in[if, &lt;mode&gt;]</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>mode</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>(default)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>packets</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>errors</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>dropped</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>overruns</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>frame</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>compressed</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>multicast</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>net.if.out[if, &lt;mode&gt;]</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>mode</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>(default)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>packets</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>errors</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Metric</td>
<td>Unit</td>
<td>Mode</td>
<td>Type</td>
<td>Value</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>-------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dropped</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>overruns</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>collision</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>carrier</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>compressed</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>net.if.total[if,&lt;mode&gt;]</td>
<td></td>
<td></td>
<td></td>
<td>X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>bytes</td>
<td></td>
<td></td>
<td></td>
<td>X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>packets</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>errors</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dropped</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>overruns</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>net.tcp.listen[port]</td>
<td></td>
<td></td>
<td></td>
<td>X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>net.tcp.port[ip, port]</td>
<td></td>
<td></td>
<td></td>
<td>X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>net.tcp.service[service,&lt;ip&gt;,&lt;port&gt;]</td>
<td></td>
<td></td>
<td></td>
<td>X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>net.tcp.service.perf[service,&lt;ip&gt;,&lt;port&gt;]</td>
<td></td>
<td></td>
<td></td>
<td>X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>net.udp.listen[port]</td>
<td></td>
<td></td>
<td></td>
<td>X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>net.udp.port[ip,&lt;ip&gt;,port]</td>
<td></td>
<td></td>
<td></td>
<td>X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>net.udp.service[service,&lt;ip&gt;,&lt;port&gt;]</td>
<td></td>
<td></td>
<td></td>
<td>X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>net.udp.service.perf[service,&lt;ip&gt;,&lt;port&gt;]</td>
<td></td>
<td></td>
<td></td>
<td>X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>proc.cpu.util[name, user, type, cmdline, &lt;mode&gt;, &lt;zone&gt;]</td>
<td></td>
<td></td>
<td></td>
<td>- - -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>type</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mode</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>type</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mode</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>zone</td>
<td></td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>proc.mem[name, user, mode, cmdline, memtype]</td>
<td></td>
<td></td>
<td></td>
<td>X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mode</td>
<td></td>
<td></td>
<td></td>
<td>X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>memtype</td>
<td></td>
<td></td>
<td></td>
<td>X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>proc.num[name, user, state, cmdline, &lt;zone&gt;]</td>
<td></td>
<td></td>
<td></td>
<td>X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>state</td>
<td></td>
<td></td>
<td></td>
<td>X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>command</td>
<td></td>
<td></td>
<td></td>
<td>X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>zone</td>
<td></td>
<td></td>
<td></td>
<td>X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sensor[device, sensor, &lt;mode&gt;]</td>
<td></td>
<td></td>
<td></td>
<td>X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Property</td>
<td>Values</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------------------------------------------------------------</td>
<td>--------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>system.boottime</td>
<td>X X X X X - - - X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>system.cpu.discovery</td>
<td>X X X X X X X X X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>system.cpu.intr</td>
<td>X X X X X - X - - X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>system.cpu.load[&lt;cpu&gt;,&lt;mode&gt;]</td>
<td>X X X X X X X X X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cpu ▲ (default)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>percpu</td>
<td>X X X X X X X X X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mode ▲ (default)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>avg1</td>
<td>X X X X X X X X X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>avg5</td>
<td>X X X X X X X X X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>avg15</td>
<td>X X X X X X X X X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>system.cpu.num[&lt;type&gt;]</td>
<td>X X X X X X X - X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>type-online</td>
<td>X X X X X X X - X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>max</td>
<td>- X X X X - - - X - -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>system.cpu.switches</td>
<td>X X X X X - X - - X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>system.cpu.util[&lt;cpu&gt;,&lt;type&gt;,&lt;mode&gt;]</td>
<td>X X X X X X X - X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>type-user</td>
<td>- X X X X X X X - X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>nice (default)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>idle (default)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>system</td>
<td>X X X X X X X - X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>for Windows</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iowait</td>
<td>- X X X X - X - - X -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>interrupt</td>
<td>- X X X - - - - - X -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>softirq</td>
<td>- X X - - - - - - -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>steal</td>
<td>- X X - - - - - - -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>guest</td>
<td>- X X - - - - - - -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>guest_nice</td>
<td>- X X - - - - - - -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mode ▲ (default)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>avg1</td>
<td>X X X X X X X - X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>avg5</td>
<td>X X X X X X X X X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>avg15</td>
<td>X X X X X X X X X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>system.hostname[&lt;type&gt;]</td>
<td>X X X X X X X X X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>system.hw.chassis[&lt;info&gt;]</td>
<td>X - - - - - - - - -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>system.hw.cpu[&lt;cpu&gt;,&lt;info&gt;]</td>
<td>X - - - - - - - - -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>system.hw.devices[&lt;type&gt;]</td>
<td>X - - - - - - - - -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>system.hw.macaddr[&lt;interface&gt;,&lt;format&gt;]</td>
<td>- - - - - - - - -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>system.localtime[&lt;type&gt;]</td>
<td>X X X X X X X X X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>type-utc</td>
<td>X X X X X X X X X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mode ▲ (default)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>local</td>
<td>X X X X X X X X X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>system.run[command,&lt;mode&gt;]</td>
<td>X X X X X X X X X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mode-wait</td>
<td>X X X X X X X X X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>system.stat[resource,&lt;type&gt;]</td>
<td>- - - - - X - - - -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>system.sw.arch</td>
<td>X X X X X X X X X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>system.sw.os[&lt;info&gt;]</td>
<td>X - - - - - - - - -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>system.sw.packages[&lt;package&gt;,&lt;manager&gt;,&lt;format&gt;]</td>
<td>- - - - - - - - -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1274
<table>
<thead>
<tr>
<th>system.swap.in[&lt;device&gt;,&lt;type&gt;]</th>
<th>-</th>
<th>X</th>
<th>-</th>
<th>-</th>
<th>-</th>
<th>-</th>
<th>-</th>
<th>X</th>
<th>-</th>
</tr>
</thead>
<tbody>
<tr>
<td>(specifying a device is only supported under Linux)</td>
<td>type</td>
<td>count</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>▲ (pages will under only all except if&lt;br&gt;device was not specified)</td>
<td>sectors</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>pages (default under Linux)</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>system.swap.out[&lt;device&gt;,&lt;type&gt;]</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td>(specifying a device is only supported under Linux)</td>
<td>type</td>
<td>count</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>▲ (pages will under only all except if&lt;br&gt;device was not specified)</td>
<td>sectors</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>pages (default under Linux)</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>system.swap.size[&lt;device&gt;,&lt;type&gt;]</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>(specifying)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a device is only supported under FreeBSD, for other platforms must be empty or &quot;all&quot;) type free</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td>▲ (default)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>total</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td>used</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td>pfree</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td>pused</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td>system.uname</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>system.uptime</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>?</td>
<td>X</td>
</tr>
<tr>
<td>system.users.num</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>vfs.dev.read[&lt;device&gt;,&lt;type&gt;,&lt;mode&gt;]</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>type</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>▲ (default for OpenBSD, AIX) operations</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>bytes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>(default for Solaris) sps</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>(default for Linux) ops</td>
<td>-</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>bps</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>X</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
| (default for FreeBSD)
<table>
<thead>
<tr>
<th>mode ▲ (compatible only with <code>&lt;br&gt;</code> type in: sps, ops, bps)</th>
<th>avg1 ▲ (default)</th>
<th>avg5 ▲ (default)</th>
<th>avg15 ▲ (default)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td><code>vfs.dev.write[&lt;device&gt;,&lt;type&gt;,&lt;mode&gt;]</code></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>type</td>
<td>X</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>sectors</td>
<td>X</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>operations</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><code>vfs.dir.count[dir,&lt;regex_incl&gt;,&lt;regex_excl&gt;,&lt;types_incl&gt;,&lt;types_excl&gt;,&lt;max_depth&gt;,&lt;min_size&gt;,&lt;max_size&gt;,&lt;min_age&gt;,&lt;max_age&gt;,&lt;regex_excl_dir&gt;]</code></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><code>vfs.dir.size[&lt;regex_incl&gt;,&lt;regex_excl&gt;,&lt;mode&gt;,&lt;max_depth&gt;,&lt;regex_excl_dir&gt;]</code></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><code>vfs.file.cksum[file]</code></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><code>vfs.file.contents[file, &lt;encoding&gt;]</code></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><code>vfs.file.exists[file]</code></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><code>vfs.file.md5sum[file]</code></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><code>vfs.file.regex[file, regexp, &lt;encoding&gt;, &lt;output&gt;]</code></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><code>vfs.file.regmatch[file, regexp, &lt;encoding&gt;]</code></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><code>vfs.file.size[file]</code></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><code>vfs.file.time[file, &lt;mode&gt;]</code></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><code>modify</code></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>access</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Command</td>
<td>Mode</td>
<td>Default</td>
<td>Total</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------</td>
<td>---------</td>
<td>-------</td>
</tr>
<tr>
<td>\texttt{vfs.fs.discovery}</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>\texttt{vfs.fs.get}</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>\texttt{vfs.fs.inode}</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>\texttt{vfs.fs.size}</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>\texttt{vm.memory.size}</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

\textbf{Note:}
See also a description of \texttt{vm.memory.size} parameters.

\textbf{Footnotes}

1. net.if.in, net.if.out and net.if.total items do not provide statistics of loopback interfaces (e.g. lo0).

2. These values for these items are not supported for loopback interfaces on Solaris systems up to and including Solaris 10 6/06 as byte, error and utilization statistics are not stored and/or reported by the kernel. However, if you’re monitoring a Solaris system via net-snmp, values may be returned as net-snmp carries legacy code from the cmu-snmp dated as old as 1997 that, upon failing to read byte values from the interface statistics returns the packet counter (which does exist on loopback interfaces) multiplied by an arbitrary value of 308. This makes the assumption that the average length of a packet is 308 octets, which is a very rough estimation as the MTU limit on Solaris systems for loopback interfaces is 8892 bytes.

These values should not be assumed to be correct or even closely accurate. They are guestimates. The Zabbix agent does not do any guess work, but net-snmp will return a value for these fields.

3. The command line on Solaris, obtained from \texttt{/proc/pid/psinfo}, is limited to 80 bytes and contains the command line as it was when the process was started.
Not supported on Windows Event Log.

On Windows XP vfs.file.time[file,change] may be equal to vfs.file.time[file,access].

2 vm.memory.size parameters

Overview

This section provides more details and platform-specific information on the parameters of the `vm.memory.size[<mode>]` agent item.

Parameters

The following parameters are available for this item:

- **active** - memory currently in use or very recently used, and so it is in RAM
- **anon** - memory not associated with a file (cannot be re-read from it)
- **available** - available memory, calculated differently depending on the platform (see the table below)
- **buffers** - cache for things like file system metadata
- **cached** - cache for various things
- **exec** - executable code, typically from a (program) file
- **file** - cache for contents of recently accessed files
- **free** - memory that is readily available to any entity requesting memory
- **inactive** - memory that is marked as not used
- **pavailable** - 'available' memory as percentage of 'total' (calculated as available/total*100)
- **pinned** - same as 'wired'
- **pused** - 'used' memory as percentage of 'total' (calculated as used/total*100)
- **shared** - memory that may be simultaneously accessed by multiple processes
- **slab** - total amount of memory used by the kernel to cache data structures for its own use
- **total** - total physical memory available
- **used** - used memory, calculated differently depending on the platform (see the table below)
- **wired** - memory that is marked to always stay in RAM. It is never moved to disk.

Attention:

Some of these parameters are platform-specific and might not be available on your platform. Please refer to this page for details.

Platform-specific calculation of available and used:

<table>
<thead>
<tr>
<th>Platform</th>
<th>&quot;available&quot;</th>
<th>&quot;used&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX</td>
<td>free + cached</td>
<td>real memory in use</td>
</tr>
<tr>
<td>FreeBSD</td>
<td>inactive + cached + free</td>
<td>active + wired + cached</td>
</tr>
<tr>
<td>HP UX</td>
<td>free</td>
<td>total - free</td>
</tr>
<tr>
<td>Linux&lt;3.14</td>
<td>free + buffers + cached</td>
<td>total - free</td>
</tr>
<tr>
<td>Linux 3.14+</td>
<td>/proc/meminfo, see &quot;MemAvailable&quot; in Linux kernel documentation for details. Note that free + buffers + cached is no longer equal to 'available' due to not all the page cache can be freed and low watermark being used in calculation.</td>
<td>total - free</td>
</tr>
<tr>
<td>NetBSD</td>
<td>inactive + execpages + file + free</td>
<td>total - free</td>
</tr>
<tr>
<td>OpenBSD</td>
<td>inactive + free + cached</td>
<td>active + wired</td>
</tr>
<tr>
<td>OSX</td>
<td>inactive + free</td>
<td>active + wired</td>
</tr>
<tr>
<td>Solaris</td>
<td>free</td>
<td>total - free</td>
</tr>
<tr>
<td>Win32</td>
<td>free</td>
<td>total - free</td>
</tr>
</tbody>
</table>
Attention:
The sum of `vm.memory.size[used]` and `vm.memory.size[available]` does not necessarily equal total. For instance, on FreeBSD:
* Active, inactive, wired, cached memories are considered used, because they store some useful information.
* At the same time inactive, cached, free memories are considered available, because these kinds of memories can be given instantly to processes that request more memory.

So inactive memory is both used and available simultaneously. Because of this, the `vm.memory.size[used]` item is designed for informational purposes only, while `vm.memory.size[available]` is designed to be used in triggers.

See the "See also" section at the bottom of this page to find more detailed information about memory calculation in different OS.

Platform-specific notes
- on Linux `shared` works only on kernel 2.4

See also
1. Detailed information about memory calculation in different OS

3 Passive and active agent checks

Overview
This section provides details on passive and active checks performed by Zabbix agent.
Zabbix uses a JSON based communication protocol for communicating with Zabbix agent.

Passive checks
A passive check is a simple data request. Zabbix server or proxy asks for some data (for example, CPU load) and Zabbix agent sends back the result to the server.

Server request
For definition of header and data length please refer to protocol details.

\(<\text{item key}>\)

Agent response

\(<\text{DATA}>[\0<\text{ERROR}>]\)\]

Above, the part in square brackets is optional and is only sent for not supported items.

For example, for supported items:
1. Server opens a TCP connection
2. Server sends `<HEADER><DATALEN>agent.ping`\]
3. Agent reads the request and responds with `<HEADER><DATALEN>1`\]
4. Server processes data to get the value, ‘1’ in our case
5. TCP connection is closed

For not supported items:
1. Server opens a TCP connection
2. Server sends `<HEADER><DATALEN>vfs.fs.size[/nono]`\]
3. Agent reads the request and responds with `<HEADER><DATALEN>ZBX_NOTSUPPORTED\0Cannot obtain filesystem information: [2] No such file or directory`\]
4. Server processes data, changes item state to not supported with the specified error message
5. TCP connection is closed

Active checks
Active checks require more complex processing. The agent must first retrieve from the server(s) a list of items for independent processing.

The servers to get the active checks from are listed in the ‘ServerActive’ parameter of the agent configuration file. The frequency of asking for these checks is set by the ‘RefreshActiveChecks’ parameter in the same configuration file. However, if refreshing active checks fails, it is retried after hardcoded 60 seconds.

The agent then periodically sends the new values to the server(s).
Getting the list of items

Agent request

```json
{  
"request":"active checks",
"host": "<hostname>"
}
```

Server response

```json
{
  "response":"success",
  "data": [
    {
      "key":"log[/home/zabbix/logs/zabbix_agentd.log]",
      "delay":30,
      "lastlogsize":0,
      "mtime":0
    },
    {
      "key":"agent.version",
      "delay":600,
      "lastlogsize":0,
      "mtime":0
    },
    {
      "key":"vfs.fs.size[/nono]",
      "delay":600,
      "lastlogsize":0,
      "mtime":0
    }
  ]
}
```

The server must respond with success. For each returned item, all properties `key`, `delay`, `lastlogsize` and `mtime` must exist, regardless of whether item is a log item or not.

For example:

1. Agent opens a TCP connection
2. Agent asks for the list of checks
3. Server responds with a list of items (item key, delay)
4. Agent parses the response
5. TCP connection is closed
6. Agent starts periodical collection of data

**Attention:**

Note that (sensitive) configuration data may become available to parties having access to the Zabbix server trapper port when using an active check. This is possible because anyone may pretend to be an active agent and request item configuration data; authentication does not take place unless you use encryption options.

Sending in collected data

Agent sends

```json
{
  "request":"agent data",
  "session": "12345678901234567890123456789012",
  "data": [
    {
      "host": "<hostname>",
      "key": "agent.version",
      "value": "2.4.0",
      "id": 1,
      "clock": "1400675595",
      "ns": "76808644"
    }
  ]
}
```
A virtual ID is assigned to each value. Value ID is a simple ascending counter, unique within one data session (identified by the session token). This ID is used to discard duplicate values that might be sent in poor connectivity environments.

**Server response**

```json
{
    "response": "success",
    "info": "processed: 3; failed: 0; total: 3; seconds spent: 0.003534"
}
```

**Attention:**

If sending of some values fails on the server (for example, because host or item has been disabled or deleted), agent will not retry sending of those values.

For example:

1. Agent opens a TCP connection
2. Agent sends a list of values
3. Server processes the data and sends the status back
4. TCP connection is closed

Note how in the example above the not supported status for vfs.fs.size[/nono] is indicated by the "state" value of 1 and the error message in "value" property.

**Attention:**

Error message will be trimmed to 2048 symbols on server side.

**Older XML protocol**

**Note:**

Zabbix will take up to 16 MB of XML Base64-encoded data, but a single decoded value should be no longer than 64 KB otherwise it will be truncated to 64 KB while decoding.

### 4 Trapper items

**Overview**

Zabbix server uses a JSON-based communication protocol for receiving data from Zabbix sender with the help of trapper item.

Request and response messages must begin with header and data length.
Zabbix sender request

```json
{   "request":"sender data",
    "data": [
        {
            "host":"<hostname>",
            "key":"trap",
            "value":"test value"
        }
    ]
}
```

Zabbix server response

```json
{   "response":"success",
    "info":"processed: 1; failed: 0; total: 1; seconds spent: 0.060753"
}
```

Alternatively Zabbix sender can send request with a timestamp

```json
{   "request":"sender data",
    "data": [
        {
            "host":"<hostname>",
            "key":"trap",
            "value":"test value",
            "clock":1516710794
        },
        {
            "host":"<hostname>",
            "key":"trap",
            "value":"test value",
            "clock":1516710795
        }
    ],
    "clock":1516712029,
    "ns":873386094
}
```

Zabbix server response

```json
{   "response":"success",
    "info":"processed: 2; failed: 0; total: 2; seconds spent: 0.060904"
}
```

5 Minimum permission level for Windows agent items

Overview

When monitoring systems using an agent, a good practice is to obtain metrics from the host on which the agent is installed. To use the principle of least privilege, it is necessary to determine what metrics are obtained from the agent.

The table in this document allows you to select the minimum rights for guaranteed correct operation of Zabbix agent.

If a different user is selected for the agent to work, rather than 'LocalSystem', then for the operation of agent as a Windows service, the new user must have the rights "Log on as a service" from "Local Policy→User Rights Assignment" and the right to create, write and delete the Zabbix agent log file.

**Note:**

When working with the rights of an agent based on the “minimum technically acceptable” group, prior provision of rights to objects for monitoring is required.
Common agent items supported on Windows

<table>
<thead>
<tr>
<th>Item key</th>
<th>User group</th>
<th>Minimum technically acceptable (functionality is limited)</th>
</tr>
</thead>
<tbody>
<tr>
<td>agent.hostname</td>
<td>Guests</td>
<td>Guests</td>
</tr>
<tr>
<td>agent.ping</td>
<td>Guests</td>
<td>Guests</td>
</tr>
<tr>
<td>agent.version</td>
<td>Guests</td>
<td>Guests</td>
</tr>
<tr>
<td>log</td>
<td>Administrators</td>
<td>Guests</td>
</tr>
<tr>
<td>log.count</td>
<td>Administrators</td>
<td>Guests</td>
</tr>
<tr>
<td>logrt</td>
<td>Administrators</td>
<td>Guests</td>
</tr>
<tr>
<td>logrt.count</td>
<td>Administrators</td>
<td>Guests</td>
</tr>
<tr>
<td>net.dns</td>
<td>Guests</td>
<td>Guests</td>
</tr>
<tr>
<td>net.dns.record</td>
<td>Guests</td>
<td>Guests</td>
</tr>
<tr>
<td>net.if.discovery</td>
<td>Guests</td>
<td>Guests</td>
</tr>
<tr>
<td>net.if.in</td>
<td>Guests</td>
<td>Guests</td>
</tr>
<tr>
<td>net.if.out</td>
<td>Guests</td>
<td>Guests</td>
</tr>
<tr>
<td>net.if.total</td>
<td>Guests</td>
<td>Guests</td>
</tr>
<tr>
<td>net.tcp.listen</td>
<td>Guests</td>
<td>Guests</td>
</tr>
<tr>
<td>net.tcp.port</td>
<td>Guests</td>
<td>Guests</td>
</tr>
<tr>
<td>net.tcp.service</td>
<td>Guests</td>
<td>Guests</td>
</tr>
<tr>
<td>net.tcp.service.perf</td>
<td>Guests</td>
<td>Guests</td>
</tr>
<tr>
<td>net.udp.service</td>
<td>Guests</td>
<td>Guests</td>
</tr>
<tr>
<td>net.udp.service.perf</td>
<td>Guests</td>
<td>Guests</td>
</tr>
<tr>
<td>proc.num</td>
<td>Administrators</td>
<td>Guests</td>
</tr>
<tr>
<td>system.cpu.discovery</td>
<td>Performance Monitor Users</td>
<td>Performance Monitor Users</td>
</tr>
<tr>
<td>system.cpu.load</td>
<td>Guests</td>
<td>Guests</td>
</tr>
<tr>
<td>system.cpu.num</td>
<td>Guests</td>
<td>Guests</td>
</tr>
<tr>
<td>system.cpu.util</td>
<td>Performance Monitor Users</td>
<td>Performance Monitor Users</td>
</tr>
<tr>
<td>system.hostname</td>
<td>Guests</td>
<td>Guests</td>
</tr>
<tr>
<td>system.localtime</td>
<td>Guests</td>
<td>Guests</td>
</tr>
<tr>
<td>system.run</td>
<td>Administrators</td>
<td>Guests</td>
</tr>
<tr>
<td>system.sw.arch</td>
<td>Guests</td>
<td>Guests</td>
</tr>
<tr>
<td>system.swap.size</td>
<td>Guests</td>
<td>Guests</td>
</tr>
<tr>
<td>system.uname</td>
<td>Guests</td>
<td>Guests</td>
</tr>
<tr>
<td>system.uptime</td>
<td>Performance Monitor Users</td>
<td>Performance Monitor Users</td>
</tr>
<tr>
<td>vfs.dir.count</td>
<td>Administrators</td>
<td>Guests</td>
</tr>
<tr>
<td>vfs.dir.size</td>
<td>Administrators</td>
<td>Guests</td>
</tr>
<tr>
<td>vfs.file.cksum</td>
<td>Administrators</td>
<td>Guests</td>
</tr>
<tr>
<td>vfs.file.contents</td>
<td>Administrators</td>
<td>Guests</td>
</tr>
<tr>
<td>vfs.file.exists</td>
<td>Administrators</td>
<td>Guests</td>
</tr>
<tr>
<td>vfs.file.md5sum</td>
<td>Administrators</td>
<td>Guests</td>
</tr>
<tr>
<td>vfs.file.regexp</td>
<td>Administrators</td>
<td>Guests</td>
</tr>
<tr>
<td>vfs.file.regmatch</td>
<td>Administrators</td>
<td>Guests</td>
</tr>
<tr>
<td>vfs.file.size</td>
<td>Administrators</td>
<td>Guests</td>
</tr>
<tr>
<td>vfs.file.time</td>
<td>Administrators</td>
<td>Guests</td>
</tr>
<tr>
<td>vfs.fs.discovery</td>
<td>Administrators</td>
<td>Guests</td>
</tr>
<tr>
<td>vfs.fs.size</td>
<td>Administrators</td>
<td>Guests</td>
</tr>
<tr>
<td>vm.memory.size</td>
<td>Guests</td>
<td>Guests</td>
</tr>
<tr>
<td>web.page.get</td>
<td>Guests</td>
<td>Guests</td>
</tr>
<tr>
<td>web.page.perf</td>
<td>Guests</td>
<td>Guests</td>
</tr>
<tr>
<td>web.page.regexp</td>
<td>Guests</td>
<td>Guests</td>
</tr>
<tr>
<td>zabbix.stats</td>
<td>Guests</td>
<td>Guests</td>
</tr>
</tbody>
</table>

Windows-specific item keys

<table>
<thead>
<tr>
<th>Item key</th>
<th>User group</th>
<th>Minimum technically acceptable (functionality is limited)</th>
</tr>
</thead>
<tbody>
<tr>
<td>eventlog</td>
<td>Event Log Readers</td>
<td>Guests</td>
</tr>
<tr>
<td>net.if.list</td>
<td>Guests</td>
<td>Guests</td>
</tr>
<tr>
<td>perf_counter</td>
<td>Performance Monitor Users</td>
<td>Performance Monitor Users</td>
</tr>
<tr>
<td>proc_info</td>
<td>Administrators</td>
<td>Guests</td>
</tr>
</tbody>
</table>
### 6 Encoding of returned values

Zabbix server expects every returned text value in the UTF8 encoding. This is related to any type of checks: zabbix agent, ssh, telnet, etc.

Different monitored systems/devices and checks can return non-ASCII characters in the value. For such cases, almost all possible zabbix keys contain an additional item key parameter - `<encoding>`. This key parameter is optional but it should be specified if the returned value is not in the UTF8 encoding and it contains non-ASCII characters. Otherwise the result can be unexpected and unpredictable.

A description of behavior with different database back-ends in such cases follows.

**MySQL**

If a value contains a non-ASCII character in non UTF8 encoding - this character and the following will be discarded when the database stores this value. No warning messages will be written to the zabbix_server.log.

Relevant for at least MySQL version 5.1.61

**PostgreSQL**

If a value contains a non-ASCII character in non UTF8 encoding - this will lead to a failed SQL query (PGRES_FATAL_ERROR:ERROR invalid byte sequence for encoding) and data will not be stored. An appropriate warning message will be written to the zabbix_server.log.

Relevant for at least PostgreSQL version 9.1.3

### 7 Large file support

Large file support, often abbreviated to LFS, is the term applied to the ability to work with files larger than 2 GB on 32-bit operating systems. Since Zabbix 2.0 support for large files has been added. This change affects at least log file monitoring and all vfs.file.* items. Large file support depends on the capabilities of a system at Zabbix compilation time, but is completely disabled on a 32-bit Solaris due to its incompatibility with procfs and swapctl.

### 8 Sensor

Each sensor chip gets its own directory in the sysfs /sys/devices tree. To find all sensor chips, it is easier to follow the device symlinks from /sys/class/hwmon(hwmon*, where * is a real number (0,1,2,...)).

The sensor readings are located either in /sys/class/hwmon(hwmon*) directory for virtual devices, or in /sys/class/hwmon(hwmon*)/device directory for non-virtual devices. A file, called name, located inside hwmon* or hwmon*/device directories contains the name of the chip, which corresponds to the name of the kernel driver used by the sensor chip.

There is only one sensor reading value per file. The common scheme for naming the files that contain sensor readings inside any of the directories mentioned above is: `<type><number>_<item>`, where

- **type** - for sensor chips is "in" (voltage), "temp" (temperature), "fan" (fan), etc.,
- **item** - "input" (measured value), "max" (high threshold), "min" (low threshold), etc.,
- **number** - always used for elements that can be present more than once (usually starts from 1, except for voltages which start from 0). If files do not refer to a specific element they have a simple name with no number.

The information regarding sensors available on the host can be acquired using `sensor-detect` and `sensors` tools (lm-sensors package: [http://lm-sensors.org/]). `Sensors-detect` helps to determine which modules are necessary for available sensors. When modules are loaded the `sensors` program can be used to show the readings of all sensor chips. The labeling of sensor readings, used by this program, can be different from the common naming scheme (`<type><number>_<item>`):

- if there is a file called `<type><number>_<item>_label`, then the label inside this file will be used instead of `<type><number>_<item>` name;
- if there is no `<type><number>_<item>_label` file, then the program searches inside the `/etc/sensors.conf` (could be also `/etc/sensors3.conf`, or different) for the name substitution.
This labeling allows user to determine what kind of hardware is used. If there is neither `<type><number>_label` file nor label inside the configuration file the type of hardware can be determined by the name attribute (hwmon*/device/name). The actual names of sensors, which zabbix_agent accepts, can be obtained by running `sensors` program with `-u` parameter (`sensors -u`).

In `sensor` program the available sensors are separated by the bus type (ISA adapter, PCI adapter, SPI adapter, Virtual device, ACPI interface, HID adapter).

On Linux 2.4:

(Sensor readings are obtained from `/proc/sys/dev/sensors` directory)
- **device** - device name (if `<mode>` is used, it is a regular expression);
- **sensor** - sensor name (if `<mode>` is used, it is a regular expression);
- **mode** - possible values: avg, max, min (if this parameter is omitted, device and sensor are treated verbatim).

Example key: `sensor[w83781d-i2c-0-2d,temp1]`

Prior to Zabbix 1.8.4, the `sensor[temp1]` format was used.

On Linux 2.6+:

(Sensor readings are obtained from `/sys/class/hwmon` directory)
- **device** - device name (non regular expression). The device name could be the actual name of the device (e.g 0000:00:18.3) or the name acquired using sensors program (e.g. k8temp-pci-00c3). It is up to the user to choose which name to use;
- **sensor** - sensor name (non regular expression);
- **mode** - possible values: avg, max, min (if this parameter is omitted, device and sensor are treated verbatim).

Example key:

`sensor[k8temp-pci-00c3,temp,max]` or `sensor[0000:00:18.3,temp1]`

`sensor[smsc47b397-isa-0880,in,avg]` or `sensor[smsc47b397.2176,in1]`

Obtaining sensor names

Sensor labels, as printed by the `sensors` command, cannot always be used directly because the naming of labels may be different for each sensor chip vendor. For example, sensors output might contain the following lines:

```
$ 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)
```

Out of these, only one label may be used directly:

```
$ zabbix_get -s 127.0.0.1 -k sensor[lm85-i2c-0-2e,in0]
2.240000
```

Attempting to use other labels (like Vcore or +12V) will not work.

```
$ zabbix_get -s 127.0.0.1 -k sensor[lm85-i2c-0-2e,Vcore]
ZBX_NOTSUPPORTED
```

To find out the actual sensor name, which can be used by Zabbix to retrieve the sensor readings, run `sensors -u`. In the output, the following may be observed:

```
$ 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
...
```
So Vcore should be queried as in1, and +12V should be queried as in4.\(^5\)

$ zabbix_get -s 127.0.0.1 -k sensor[lm85-i2c-0-2e,in1]
1.301000

Not only voltage (in), but also current (curr), temperature (temp) and fan speed (fan) readings can be retrieved by Zabbix.

9 Notes on memtype parameter in proc.mem items

Overview

The **memtype** parameter is supported on Linux, AIX, FreeBSD, and Solaris platforms.

Three common values of 'memtype' are supported on all of these platforms: pmem, rss and vsize. Additionally, platform-specific 'memtype' values are supported on some platforms.

AIX

See values supported for ‘memtype’ parameter on AIX in the table.

<table>
<thead>
<tr>
<th>Supported value</th>
<th>Description</th>
<th>Source in procentry64 structure</th>
<th>Tries to be compatible with</th>
</tr>
</thead>
<tbody>
<tr>
<td>vsize (^1)</td>
<td>Virtual memory size</td>
<td>pi_size</td>
<td>ps -o vmem</td>
</tr>
<tr>
<td>pmem</td>
<td>Percentage of real memory</td>
<td>pi_prm</td>
<td>ps -o pmem</td>
</tr>
<tr>
<td>rss</td>
<td>Resident set size</td>
<td>pi_trss + pi_drss</td>
<td>ps -o rss</td>
</tr>
<tr>
<td>size</td>
<td>Size of process (code + data)</td>
<td>pi_dvm</td>
<td>&quot;ps gvw&quot; SIZE column</td>
</tr>
<tr>
<td>dsize</td>
<td>Data size</td>
<td>pi_dsize</td>
<td></td>
</tr>
<tr>
<td>tsize</td>
<td>Text (code) size</td>
<td>pi_tsize</td>
<td>&quot;ps gvw&quot; TSZ column</td>
</tr>
<tr>
<td>sdsizese</td>
<td>Data size from shared library</td>
<td>pi_sdsizese</td>
<td></td>
</tr>
<tr>
<td>drss</td>
<td>Data resident set size</td>
<td>pi_drss</td>
<td></td>
</tr>
<tr>
<td>trss</td>
<td>Text resident set size</td>
<td>pi_trss</td>
<td></td>
</tr>
</tbody>
</table>

FreeBSD

See values supported for ‘memtype’ parameter on FreeBSD in the table.

<table>
<thead>
<tr>
<th>Supported value</th>
<th>Description</th>
<th>Source in kinfo_proc structure</th>
<th>Tries to be compatible with</th>
</tr>
</thead>
<tbody>
<tr>
<td>vsize</td>
<td>Virtual memory size</td>
<td>kp_eproc.e_vm.vm_map.size or ki_size</td>
<td>ps -o vsz</td>
</tr>
<tr>
<td>pmem</td>
<td>Percentage of real memory</td>
<td>calculated from rss</td>
<td>ps -o pmem</td>
</tr>
<tr>
<td>rss</td>
<td>Resident set size</td>
<td>kp_eproc.e_vm.vm_rssize or ki_rssize</td>
<td>ps -o rss</td>
</tr>
<tr>
<td>size (^1)</td>
<td>Size of process (code + data + stack)</td>
<td>tsize + dsize + ssize</td>
<td></td>
</tr>
<tr>
<td>tsize</td>
<td>Text (code) size</td>
<td>kp_eproc.e_vm.vm_tsizese or ki_tsizese</td>
<td>ps -o tsiz</td>
</tr>
<tr>
<td>dsize</td>
<td>Data size</td>
<td>kp_eproc.e_vm.vm_dsizese or ki_dsizese</td>
<td>ps -o dsiz</td>
</tr>
<tr>
<td>ssize</td>
<td>Stack size</td>
<td>kp_eproc.e_vm.vm_sssize or ki_sssize</td>
<td>ps -o ssiz</td>
</tr>
</tbody>
</table>

Linux

See values supported for ‘memtype’ parameter on Linux in the table.

\(^5\) According to specification these are voltages on chip pins and generally speaking may need scaling.
<table>
<thead>
<tr>
<th>Supported value</th>
<th>Description</th>
<th>Source in /proc/&lt;pid&gt;/status file</th>
</tr>
</thead>
<tbody>
<tr>
<td>vsize (^1)</td>
<td>Virtual memory size</td>
<td>VmSize</td>
</tr>
<tr>
<td>pmem</td>
<td>Percentage of real memory</td>
<td>(VmRSS/total_memory) * 100</td>
</tr>
<tr>
<td>rss</td>
<td>Resident set size</td>
<td>VmRSS</td>
</tr>
<tr>
<td>data</td>
<td>Size of data segment</td>
<td>VmData</td>
</tr>
<tr>
<td>exe</td>
<td>Size of code segment</td>
<td>VmExe</td>
</tr>
<tr>
<td>hwm</td>
<td>Peak resident set size</td>
<td>VmHWM</td>
</tr>
<tr>
<td>lck</td>
<td>Size of locked memory</td>
<td>VmLck</td>
</tr>
<tr>
<td>lib</td>
<td>Size of shared libraries</td>
<td>VmLib</td>
</tr>
<tr>
<td>peak</td>
<td>Peak virtual memory size</td>
<td>VmPeak</td>
</tr>
<tr>
<td>pin</td>
<td>Size of pinned pages</td>
<td>VmPin</td>
</tr>
<tr>
<td>pte</td>
<td>Size of page table entries</td>
<td>VmPTE</td>
</tr>
<tr>
<td>size</td>
<td>Size of process code + data + stack segments</td>
<td>VmExe + VmData + VmStk</td>
</tr>
<tr>
<td>stk</td>
<td>Size of stack segment</td>
<td>VmStk</td>
</tr>
<tr>
<td>swap</td>
<td>Size of swap space used</td>
<td>VmSwap</td>
</tr>
</tbody>
</table>

Notes for Linux:

1. Not all ‘memtype’ values are supported by older Linux kernels. For example, Linux 2.4 kernels do not support hwm, pin, peak, pte and swap values.

2. We have noticed that self-monitoring of the Zabbix agent active check process with `proc.mem[...,...,...,...,data]` shows a value that is 4 kB larger than reported by VmData line in the agent’s `/proc/<pid>/status file`. At the time of self-measurement the agent’s data segment increases by 4 kB and then returns to the previous size.

Solaris

See values supported for ‘memtype’ parameter on Solaris in the table.

<table>
<thead>
<tr>
<th>Supported value</th>
<th>Description</th>
<th>Source in psinfo structure</th>
<th>Tries to be compatible with</th>
</tr>
</thead>
<tbody>
<tr>
<td>vsize (^1)</td>
<td>Size of process image</td>
<td>pr_size</td>
<td>ps -o vsz</td>
</tr>
<tr>
<td>pmem</td>
<td>Percentage of real memory</td>
<td>pr_pctmem</td>
<td>ps -o pmem</td>
</tr>
<tr>
<td>rss</td>
<td>Resident set size</td>
<td>pr_rssize</td>
<td>ps -o rss</td>
</tr>
<tr>
<td>data</td>
<td>Size of data segment</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Footnotes

\(^1\) Default value.

10 Notes on selecting processes in `proc.mem` and `proc.num` items

Processes modifying their commandline

Some programs use modifying their commandline as a method for displaying their current activity. A user can see the activity by running `ps` and `top` commands. Examples of such programs include PostgreSQL, Sendmail, Zabbix.

Let’s see an example from Linux. Let’s assume we want to monitor a number of Zabbix agent processes.

`ps` command shows processes of interest as

```
$ 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/ZBXNEXT-1078/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]

Selecting processes by name and user does the job:

$ zabbix_get -s localhost -k 'proc.num[zabbix_agentd,zabbix]'
6

Now let's rename zabbix_agentd executable to zabbix_agentd_30 and restart it.

ps now shows

$ ps -fu zabbix

<table>
<thead>
<tr>
<th>UID</th>
<th>PID</th>
<th>PPID</th>
<th>C</th>
<th>STIME</th>
<th>TTY</th>
<th>TIME</th>
<th>CMD</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6715</td>
<td>1</td>
<td>0</td>
<td>12:53</td>
<td>?</td>
<td>00:00:00</td>
<td>sbin/zabbix_agentd_30 -c /home/zabbix/ZBXNEXT-1078/zabbix_agentd.conf</td>
</tr>
<tr>
<td></td>
<td>6716</td>
<td>6715</td>
<td>0</td>
<td>12:53</td>
<td>?</td>
<td>00:00:00</td>
<td>sbin/zabbix_agentd_30: collector [idle 1 sec]</td>
</tr>
<tr>
<td></td>
<td>6717</td>
<td>6715</td>
<td>0</td>
<td>12:53</td>
<td>?</td>
<td>00:00:00</td>
<td>sbin/zabbix_agentd_30: listener #1 [waiting for connection]</td>
</tr>
<tr>
<td></td>
<td>6718</td>
<td>6715</td>
<td>0</td>
<td>12:53</td>
<td>?</td>
<td>00:00:00</td>
<td>sbin/zabbix_agentd_30: listener #2 [waiting for connection]</td>
</tr>
<tr>
<td></td>
<td>6719</td>
<td>6715</td>
<td>0</td>
<td>12:53</td>
<td>?</td>
<td>00:00:00</td>
<td>sbin/zabbix_agentd_30: listener #3 [waiting for connection]</td>
</tr>
<tr>
<td></td>
<td>6720</td>
<td>6715</td>
<td>0</td>
<td>12:53</td>
<td>?</td>
<td>00:00:00</td>
<td>sbin/zabbix_agentd_30: active checks #1 [idle 1 sec]</td>
</tr>
</tbody>
</table>

Now selecting processes by name and user produces an incorrect result:

$ zabbix_get -s localhost -k 'proc.num[zabbix_agentd_30,zabbix]'
1

Why a simple renaming of executable to a longer name lead to quite different result?

Zabbix agent starts with checking the process name. /proc/<pid>/status file is opened and the line Name is checked. In our case the Name lines are:

$ 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
```

The process name in status file is truncated to 15 characters.

A similar result can be seen with ps command:

$ ps -u zabbix

<table>
<thead>
<tr>
<th>PID</th>
<th>TTY</th>
<th>TIME</th>
<th>CMD</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6715</td>
<td>00:00:00</td>
<td>sbin/zabbix_agentd_3</td>
</tr>
<tr>
<td></td>
<td>6716</td>
<td>00:00:01</td>
<td>sbin/zabbix_agentd_3</td>
</tr>
<tr>
<td></td>
<td>6717</td>
<td>00:00:00</td>
<td>sbin/zabbix_agentd_3</td>
</tr>
<tr>
<td></td>
<td>6718</td>
<td>00:00:00</td>
<td>sbin/zabbix_agentd_3</td>
</tr>
<tr>
<td></td>
<td>6719</td>
<td>00:00:00</td>
<td>sbin/zabbix_agentd_3</td>
</tr>
<tr>
<td></td>
<td>6720</td>
<td>00:00:00</td>
<td>sbin/zabbix_agentd_3</td>
</tr>
</tbody>
</table>

Obviously, that is not equal to our proc.num[] name parameter value zabbix_agentd_30. Having failed to match the process name from status file the Zabbix agent turns to /proc/<pid>/cmdline file.

How the agent sees the "cmdline" file can be illustrated with running a command

$ for i in 6715 6716 6717 6718 6719 6720; do cat /proc/$i/cmdline | awk '{gsub(/\x0/,"<NUL>"); print}'; done

```
sbin/zabbix_agentd_30
sbin/zabbix_agentd_30: collector [idle 1 sec]
sbin/zabbix_agentd_30: listener #1 [waiting for connection]
sbin/zabbix_agentd_30: listener #2 [waiting for connection]
sbin/zabbix_agentd_30: listener #3 [waiting for connection]
sbin/zabbix_agentd_30: active checks #1 [idle 1 sec]
```

1289
/proc/<pid>/cmdline files in our case contain invisible, non-printable null bytes, used to terminate strings in C language. The null bytes are shown as "<NUL>" in this example.

Zabbix agent checks "cmdline" for the main process and takes a zabbix-agentd_30, which matches our name parameter value zabbix-agentd_30. So, the main process is counted by item proc.num[zabbix_agentd_30,zabbix].

When checking the next process, the agent takes zabbix-agentd_30: collector [idle 1 sec] from the cmdline file and it does not meet our name parameter zabbix-agentd_30. So, only the main process which does not modify its commandline, gets counted. Other agent processes modify their command line and are ignored.

This example shows that the name parameter cannot be used in proc.mem[] and proc.num[] for selecting processes in this case.

Using cmdline parameter with a proper regular expression produces a correct result:

```
$ zabbix_get -s localhost -k 'proc.num[,zabbix,,zabbix_agentd_30[ :]]'
6
```

Be careful when using proc.mem[] and proc.num[] items for monitoring programs which modify their commandlines.

Before putting name and cmdline parameters into proc.mem[] and proc.num[] items, you may want to test the parameters using proc.num[] item and ps command.

Linux kernel threads

Threads cannot be selected with cmdline parameter in proc.mem[] and proc.num[] items

Let's take as an example one of kernel threads:

```
$ ps -ef | grep kthreadd
root 2 0 0 09:33 ? 00:00:00 [kthreadd]
```

It can be selected with process name parameter:

```
$ zabbix_get -s localhost -k 'proc.num[kthreadd,root]'
1
```

But selection by process cmdline parameter does not work:

```
$ zabbix_get -s localhost -k 'proc.num[,root,,kthreadd]'
0
```

The reason is that Zabbix agent takes the regular expression specified in cmdline parameter and applies it to contents of process /proc/<pid>/cmdline. For kernel threads their /proc/<pid>/cmdline files are empty. So, cmdline parameter never matches.

Counting of threads in proc.mem[] and proc.num[] items

Linux kernel threads are counted by proc.num[] item but do not report memory in proc.mem[] item. For example:

```
$ 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.
```

But what happens if there is a user process with the same name as a kernel thread? Then it could look like this:

```
$ 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[] counted both the kernel thread and the user process. proc.mem[] reports memory for the user process only and counts the kernel thread memory as if it was 0. This is different from the case above when ZBX_NOTSUPPORTED was reported.
Be careful when using `proc.mem[]` and `proc.num[]` items if the program name happens to match one of the thread.

Before putting parameters into `proc.mem[]` and `proc.num[]` items, you may want to test the parameters using `proc.num[]` item and `ps` command.

11 Implementation details of net.tcp.service and net.udp.service checks

Implementation of net.tcp.service and net.udp.service checks is detailed on this page for various services specified in the service parameter.

Item net.tcp.service parameters

**ftp**

Creates a TCP connection and expects the first 4 characters of the response to be “220 “, then sends “QUIT\n”. Default port 21 is used if not specified.

**http**

Creates a TCP connection without expecting and sending anything. Default port 80 is used if not specified.

**https**

Uses (and only works with) libcurl, does not verify the authenticity of the certificate, does not verify the host name in the SSL certificate, only fetches the response header (HEAD request). Default port 443 is used if not specified.

**imap**

Creates a TCP connection and expects the first 4 characters of the response to be “* OK”, then sends “a1 LOGOUT\n”. Default port 143 is used if not specified.

**ldap**

Opens a connection to an LDAP server and performs an LDAP search operation with filter set to (objectClass=*). Expects successful retrieval of the first attribute of the first entry. Default port 389 is used if not specified.

**nntp**

Creates a TCP connection and expects the first 3 characters of the response to be “200” or “201”, then sends “QUIT\n”. Default port 119 is used if not specified.

**pop**

Creates a TCP connection and expects the first 3 characters of the response to be “+OK”, then sends “QUIT\n”. Default port 110 is used if not specified.

**smtp**

Creates a TCP connection and expects the first 3 characters of the response to be “220”, followed by a space, the line ending or a dash. The lines containing a dash belong to a multiline response and the response will be re-read until a line without the dash is received. Then sends “QUIT\n”. Default port 25 is used if not specified.

**ssh**

Creates a TCP connection. If the connection has been established, both sides exchange an identification string (SSH-major.minor-XXXX), where major and minor are protocol versions and XXXX is a string. Zabbix checks if the string matching the specification is found and then sends back the string “SSH-major.minor-zabbix_agent\n” or “0\n” on mismatch. Default port 22 is used if not specified.

**tcp**

Creates a TCP connection without expecting and sending anything. Unlike the other checks requires the port parameter to be specified.

**telnet**

Creates a TCP connection and expects a login prompt (’:*’ at the end). Default port 23 is used if not specified.

Item net.udp.service parameters

**ntp**

Sends an SNTP packet over UDP and validates the response according to [RFC 4330, section 5](https://tools.ietf.org/html/rfc4330). Default port 123 is used if not specified.
12 Item value preprocessing details

Overview

This section provides item value preprocessing details. Item value preprocessing allows to define and execute transformation rules for the received item values.

To learn about configuring basic preprocessing steps, see: Item value preprocessing.

Preprocessing is managed by a preprocessing manager process, which was added in Zabbix 3.4, along with preprocessing workers that perform the preprocessing steps. All values (with or without preprocessing) from different data gatherers pass through the preprocessing manager before being added to the history cache. Socket-based IPC communication is used between data gatherers (pollers, trappers, etc) and the preprocessing process. Only Zabbix server is performing preprocessing steps.

Item value processing

To visualize the data flow from data source to the Zabbix database, we can use the following simplified diagram:
Data gathering

Data gathering is performed by: poller, trapper, and other processes

Configuration cache

Configuration cache acts as a buffer between Zabbix processes and Zabbix DB (where configuration is stored).

Data preprocessing

Data preprocessing is performed by: preprocessing manager and preprocessing worker processes

History cache

History cache acts as a buffer between data source (from where data is gathered) and Zabbix DB (where data is stored).

Data processing

Data processing starts with data synchronization (transferring data from history cache to Zabbix database) and proceeds with trigger processing, item configuration updates, etc.

Data processing is performed by: history syncer processes
The diagram above shows only processes, objects and actions related to item value processing in a simplified form. The diagram does not show conditional direction changes, error handling or loops. Local data cache of preprocessing manager is not shown either because it doesn’t affect data flow directly. The aim of this diagram is to show processes involved in item value processing and the way they interact.

- Data gathering starts with raw data from a data source. At this point, data contains only ID, timestamp and value (can be multiple values as well)
- No matter what type of data gatherer is used, the idea is the same for active or passive checks, for trapper items and etc, as it only changes the data format and the communication starter (either data gatherer is waiting for a connection and data, or data gatherer initiates the communication and requests the data). Raw data is validated, item configuration is retrieved from configuration cache (data is enriched with the configuration data).
- Socket-based IPC mechanism is used to pass data from data gatherers to preprocessing manager. At this point data gatherer continue to gather data without waiting for the response from preprocessing manager.
- Data preprocessing is performed. This includes execution of preprocessing steps and dependent item processing.

**Note:**
Item can change its state to NOT SUPPORTED while preprocessing is performed if any of preprocessing steps fail.

- History data from local data cache of preprocessing manager is being flushed into history cache.
- At this point data flow stops until the next synchronization of history cache (when history syncer process performs data synchronization).
- Synchronization process starts with data normalization storing data in Zabbix database. Data normalization performs conversions to desired item type (type defined in item configuration), including truncation of textual data based on pre-defined sizes allowed for those types (HISTORY_STR_VALUE_LEN for string, HISTORY_TEXT_VALUE_LEN for text and HISTORY_LOG_VALUE_LEN for log values). Data is being sent to Zabbix database after normalization is done.

**Note:**
Item can change its state to NOT SUPPORTED if data normalization fails (for example, when textual value cannot be converted to number).

- Gathered data is being processed - triggers are checked, item configuration is updated if item becomes NOT SUPPORTED, etc.
- This is considered the end of data flow from the point of view of item value processing.

### Item value preprocessing

To visualize the data preprocessing process, we can use the following simplified diagram:
The diagram above shows only processes, objects and main actions related to item value preprocessing in a simplified form. The diagram does not show conditional direction changes, error handling or loops. Only one preprocessing worker is shown on this diagram (multiple preprocessing workers can be used in real-life scenarios), only one item value is being processed and we assume that this item requires to execute at least one preprocessing step. The aim of this diagram is to show the idea behind item value preprocessing pipeline.

- Item data and item value is passed to preprocessing manager using socket-based IPC mechanism.
- Item is placed in the preprocessing queue.

**Note:**
Item can be placed at the end or at the beginning of the preprocessing queue. Zabbix internal items are always placed at the beginning of preprocessing queue, while other item types are enqueued at the end.

- At this point data flow stops until there is at least one unoccupied (that is not executing any tasks) preprocessing worker.
- When preprocessing worker is available, preprocessing task is being sent to it.
- After preprocessing is done (both failed and successful execution of preprocessing steps), preprocessed value is being passed back to preprocessing manager.
- Preprocessing manager converts result to desired format (defined by item value type) and places result in preprocessing queue. If there are dependent items for current item, then dependent items are added to preprocessing queue as well. Dependent items are enqueued in preprocessing queue right after the master item, but only for master items with value set and not in NOT SUPPORTED state.

**Value processing pipeline**

Item value processing is executed in multiple steps (or phases) by multiple processes. This can cause:

- Dependent item can receive values, while THE master value cannot. This can be achieved by using the following use case:
- Master item has value type UINT, (trapper item can be used), dependent item has value type TEXT.
- No preprocessing steps are required for both master and dependent items.
- Textual value (like, “abc”) should be passed to master item.
- As there are no preprocessing steps to execute, preprocessing manager checks if master item is not in NOT SUPPORTED state and if value is set (both are true) and enqueues dependent item with the same value as master item (as there are no preprocessing steps).

* When both master and dependent items reach history synchronization phase, master item becomes NOT SUPPORTED.

As a result, dependent item receives a value, while master item changes its state to NOT SUPPORTED.

- Dependent item receives value that is not present in master item history. The use case is very similar to the previous one, except for the master item type. For example, if CHAR type is used for master item, then master item value will be truncated at the history synchronization phase, while dependent items will receive their value from the initial (not truncated) value of master item.

Preprocessing queue

Preprocessing queue is a FIFO data structure that stores values preserving the order in which values are reviewed by preprocessing manager. There are multiple exceptions to FIFO logic:

- Internal items are enqueued at the beginning of the queue
- Dependent items are always enqueued after the master item

To visualize the logic of preprocessing queue, we can use the following diagram:

![Preprocessing queue diagram](image)

Values from the preprocessing queue are flushed from the beginning of the queue to the first unprocessed value. So, for example, preprocessing manager will flush values 1, 2 and 3, but will not flush value 5 as value 4 is not processed yet:

![Preprocessing queue values](image)

Only two values will be left in queue (4 and 5) after flushing, values are added into local data cache of preprocessing manager and then values are transferred from local cache into history cache. Preprocessing manager can flush values from local data cache in single item mode or in bulk mode (used for dependent items and values received in bulk).
Preprocessing workers

Zabbix server configuration file allows users to set count of preprocessing worker processes. StartPreprocessors configuration parameter should be used to set number of pre-forked instances of preprocessing workers. Optimal number of preprocessing workers can be determined by many factors, including the count of “preprocessable” items (items that require to execute any preprocessing steps), count of data gathering processes, average step count for item preprocessing, etc.

But assuming that there is no heavy preprocessing operations like parsing of large XML / JSON chunks, number of preprocessing workers can match total number of data gatherers. This way, there will mostly (except for the cases when data from gatherer comes in bulk) be at least one unoccupied preprocessing worker for collected data.

**Warning:**
Too many data gathering processes (pollers, unreachable pollers, HTTP pollers, Java pollers, pingers, trappers, proxypollers) together with IPMI manager, SNMP trapper and preprocessing workers can exhaust the per-process file descriptor limit for the preprocessing manager. This will cause Zabbix server to stop (usually shortly after the start, but sometimes it can take more time). The configuration file should be revised or the limit should be raised to avoid this situation.

13 Supported JSONPath functionality

**Attention:**
The full JSONPath functionality as described in this page is available starting with Zabbix 4.0.11.

Overview

JSONPath consists of segments separated with dots. A segment can be either a simple word like a JSON value name, * or a more complex construct enclosed within square brackets `[ ]`. The separating dot before bracket segment is optional and can be omitted. For example:

<table>
<thead>
<tr>
<th>Path</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$.object.name</td>
<td>Return the object.name contents.</td>
</tr>
<tr>
<td>$.object['name']</td>
<td>Return the object.name contents.</td>
</tr>
<tr>
<td>$.object.['name']</td>
<td>Return the object.name contents.</td>
</tr>
<tr>
<td>$['object'] ['name']</td>
<td>Return the object.name contents.</td>
</tr>
<tr>
<td>$.['object'].['name']</td>
<td>Return the object.name contents.</td>
</tr>
<tr>
<td>$.object.history.length()</td>
<td>Return the number of object.history array elements.</td>
</tr>
<tr>
<td>$[@@name == 'object'].price.first()</td>
<td>Return the price field of the first object with name ‘Object’.</td>
</tr>
<tr>
<td>$[@@name == 'object'].history.first().length()</td>
<td>Return the number of history array elements of the first object with name ‘Object’.</td>
</tr>
<tr>
<td>$[@@price &gt; 10].length()</td>
<td>Return the number of objects with price being greater than 10.</td>
</tr>
</tbody>
</table>

Supported segments

<table>
<thead>
<tr>
<th>Segment</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;name&gt;</td>
<td>Match object property by name.</td>
</tr>
<tr>
<td>*</td>
<td>Match all object properties.</td>
</tr>
<tr>
<td>['&lt;name&gt;']</td>
<td>Match object property by name.</td>
</tr>
<tr>
<td>['&lt;name&gt;', '&lt;name&gt;', ...]</td>
<td>Match object property by any of the listed names.</td>
</tr>
<tr>
<td>[index]</td>
<td>Match array element by the index.</td>
</tr>
<tr>
<td>[&lt;number&gt;, &lt;number&gt;, ...]</td>
<td>Match array element by any of the listed indexes.</td>
</tr>
<tr>
<td>[*]</td>
<td>Match all object properties or array elements.</td>
</tr>
<tr>
<td>[&lt;start&gt;:&lt;end&gt;]</td>
<td>Match array elements by the defined range: <code>&lt;start&gt;</code> - the first index to match (including). If not specified matches all array elements from the beginning. If negative specifies starting offset from the end of array. <code>&lt;end&gt;</code> - the last index to match (excluding). If not specified matches all array elements to the end. If negative specifies starting offset from the end of array.</td>
</tr>
<tr>
<td>[?(&lt;expression&gt;)]</td>
<td>Match objects/array elements by applying filter expression.</td>
</tr>
</tbody>
</table>
To find a matching segment ignoring its ancestry (detached segment) it must be prefixed with `..`, for example `$..name` or `$..['name']` return values of all `name` properties.

Since Zabbix 4.0.19 matched element names can be extracted by adding a `~` suffix to the JSONPath. It returns the name of the matched object or an index in string format of the matched array item. The output format follows the same rules as other JSONPath queries - definite path results are returned `as is` and indefinite path results are returned in array. However there is not much point of extracting the name of an element matching a definite path - it’s already known.

Filter expression

Filter expression is a arithmetical expression in infix notation.

Supported operands:

<table>
<thead>
<tr>
<th>Operand</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;&lt;text&gt;&quot;</td>
<td>Text constant.</td>
<td>‘value: ‘1’”</td>
</tr>
<tr>
<td>'&lt;text&gt;'</td>
<td></td>
<td>“value: ‘1’”</td>
</tr>
<tr>
<td>&lt;number&gt;</td>
<td>Numeric constant supporting scientific notation.</td>
<td>123</td>
</tr>
<tr>
<td>&lt;jsonpath starting with $&gt;</td>
<td>Value referred to by the JSONPath from the input document root node; only definite paths are supported.</td>
<td>$.object.name</td>
</tr>
<tr>
<td>&lt;jsonpath starting with @&gt;</td>
<td>Value referred to by the JSONPath from the current object/element; only definite paths are supported.</td>
<td>@.name</td>
</tr>
</tbody>
</table>

Supported operators:

<table>
<thead>
<tr>
<th>Operator</th>
<th>Type</th>
<th>Description</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>binary</td>
<td>Subtraction.</td>
<td>Number.</td>
</tr>
<tr>
<td>+</td>
<td>binary</td>
<td>Addition.</td>
<td>Number.</td>
</tr>
<tr>
<td>/</td>
<td>binary</td>
<td>Division.</td>
<td>Number.</td>
</tr>
<tr>
<td>*</td>
<td>binary</td>
<td>Multiplication.</td>
<td>Number.</td>
</tr>
<tr>
<td>==</td>
<td>binary</td>
<td>Is equal to.</td>
<td>Boolean (1 or 0).</td>
</tr>
<tr>
<td>!=</td>
<td>binary</td>
<td>Is not equal to.</td>
<td>Boolean (1 or 0).</td>
</tr>
<tr>
<td>&lt;</td>
<td>binary</td>
<td>Is less than.</td>
<td>Boolean (1 or 0).</td>
</tr>
<tr>
<td>&lt;=</td>
<td>binary</td>
<td>Is less than or equal to.</td>
<td>Boolean (1 or 0).</td>
</tr>
<tr>
<td>&gt;</td>
<td>binary</td>
<td>Is greater than.</td>
<td>Boolean (1 or 0).</td>
</tr>
<tr>
<td>&gt;=</td>
<td>binary</td>
<td>Is greater than or equal to.</td>
<td>Boolean (1 or 0).</td>
</tr>
<tr>
<td>=~</td>
<td>binary</td>
<td>Matches regular expression.</td>
<td>Boolean (1 or 0).</td>
</tr>
<tr>
<td>!</td>
<td>unary</td>
<td>Boolean not.</td>
<td>Boolean (1 or 0).</td>
</tr>
<tr>
<td>||</td>
<td>binary</td>
<td>Boolean or.</td>
<td>Boolean (1 or 0).</td>
</tr>
<tr>
<td>&amp; &amp;</td>
<td>binary</td>
<td>Boolean and.</td>
<td>Boolean (1 or 0).</td>
</tr>
</tbody>
</table>

Functions

Functions can be used at the end of JSONPath. Multiple functions can be chained if the preceding function returns value that is accepted by the following function.

Supported functions:

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
<th>Input</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>avg</td>
<td>Average value of numbers in input array.</td>
<td>Array of numbers.</td>
<td>Number.</td>
</tr>
<tr>
<td>min</td>
<td>Minimum value of numbers in input array.</td>
<td>Array of numbers.</td>
<td>Number.</td>
</tr>
<tr>
<td>max</td>
<td>Maximum value of numbers in input array.</td>
<td>Array of numbers.</td>
<td>Number.</td>
</tr>
<tr>
<td>sum</td>
<td>Sum of numbers in input array.</td>
<td>Array of numbers.</td>
<td>Number.</td>
</tr>
<tr>
<td>length</td>
<td>Number of elements in input array.</td>
<td>Array.</td>
<td>Number.</td>
</tr>
<tr>
<td>first</td>
<td>The first array element.</td>
<td>Array.</td>
<td>A JSON construct (object, array, value) depending on input array contents.</td>
</tr>
</tbody>
</table>

Quoted numeric values are accepted by the JSONPath aggregate functions since Zabbix 4.0.14. It means that the values are converted from string type to numeric if aggregation is required.
Incompatible input will cause the function to generate error.

Output value

JSONPaths can be divided in definite and indefinite paths. A definite path can return only null or a single match. An indefinite path can return multiple matches, basically JSONPaths with detached, multiple name/index list, array slice or expression segments. However, when a function is used the JSONPath becomes definite, as functions always output single value.

A definite path returns the object/array/value it's referencing, while indefinite path returns an array of the matched objects/arrays/values.

Whitespace

Whitespace (space, tab characters) can be freely used in bracket notation segments and expressions, for example, ${ 'a' [ 0 ][ ?( $.b == 'c' ) ][ : -1 ].first( ).

Strings

Strings should be enclosed with single ' or double " quotes. Inside the strings, single or double quotes (depending on which are used to enclose it) and backslashes \ are escaped with the backslash \ character.

Examples

Input data

```json
{
  "books": [
    {
      "category": "reference",
      "author": "Nigel Rees",
      "title": "Sayings of the Century",
      "price": 8.95,
      "id": 1
    },
    {
      "category": "fiction",
      "author": "Evelyn Waugh",
      "title": "Sword of Honour",
      "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": "The Lord of the Rings",
      "isbn": "0-395-19395-8",
      "price": 22.99,
      "id": 4
    }
  ],
  "services": {
    "delivery": {
      "servicegroup": 1000,
      "description": "Next day delivery in local town",
      "active": true,
      "price": 5
    },
    "bookbinding": {
      "servicegroup": 1001,
      "description": "Printing and assembling book in A5 format",
    }
  }
}
```
"active": true,
"price": 154.99
},
"restoration": {
"servicegroup": 1002,
"description": "Various restoration methods",
"active": false,
"methods": [
{
"description": "Chemical cleaning",
"price": 46
},
{
"description": "Pressing pages damaged by moisture",
"price": 24.5
},
{
"description": "Rebinding torn book",
"price": 99.49
}
]
},
"filters": {
"price": 10,
"category": "fiction",
"no filters": "no "filters"
},
"closed message": "Store is closed",
"tags": [
"a",
"b",
"c",
"d",
"e"
]}

<table>
<thead>
<tr>
<th>JSONPath</th>
<th>Type</th>
<th>Result</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>$.filters.price</td>
<td>definite</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>$.filters.category</td>
<td>definite</td>
<td>fiction</td>
<td></td>
</tr>
<tr>
<td>$.filters['no filters']</td>
<td>definite</td>
<td>no &quot;filters&quot;</td>
<td></td>
</tr>
<tr>
<td>$.filters</td>
<td>definite</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$.books[1].title</td>
<td>definite</td>
<td>Sword of Honour</td>
<td></td>
</tr>
<tr>
<td>$.books[-1].author</td>
<td>definite</td>
<td>J. R. Tolkien</td>
<td></td>
</tr>
<tr>
<td>$.books.length()</td>
<td>definite</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>$.tags[:]</td>
<td>indefinite</td>
<td>[&quot;a&quot;, &quot;b&quot;, &quot;c&quot;, &quot;d&quot;, &quot;e&quot;]</td>
<td></td>
</tr>
<tr>
<td>$.tags[2:]</td>
<td>indefinite</td>
<td>[&quot;c&quot;, &quot;d&quot;, &quot;e&quot;]</td>
<td></td>
</tr>
<tr>
<td>$.tags[:3]</td>
<td>indefinite</td>
<td>[&quot;a&quot;, &quot;b&quot;, &quot;c&quot;]</td>
<td></td>
</tr>
<tr>
<td>$.tags[1:4]</td>
<td>indefinite</td>
<td>[&quot;b&quot;, &quot;c&quot;, &quot;d&quot;]</td>
<td></td>
</tr>
<tr>
<td>$.tags[-2:]</td>
<td>indefinite</td>
<td>[&quot;d&quot;, &quot;e&quot;]</td>
<td></td>
</tr>
<tr>
<td>$.tags[3:]</td>
<td>indefinite</td>
<td>[&quot;a&quot;, &quot;b&quot;]</td>
<td></td>
</tr>
<tr>
<td>$.tags[:3].length()</td>
<td>definite</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>
| $.books[0, 2].title | indefinite | ["Sayings of the
Century", "Moby Dick"] |                           |
| $.books[1]['author',
"title"] | indefinite | ["Evelyn Waugh", "Sword
of Honour"] |                           |
<table>
<thead>
<tr>
<th>JSONPath</th>
<th>Type</th>
<th>Result</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>$..id</td>
<td>indefinite</td>
<td>[1, 2, 3, 4]</td>
<td></td>
</tr>
<tr>
<td>$.services..price</td>
<td>indefinite</td>
<td>[5, 154.99, 46, 24.5, 99.49]</td>
<td></td>
</tr>
<tr>
<td>$.books[?(@.id == 4 - 0.4 * 5)].title</td>
<td>indefinite</td>
<td>[&quot;Sword of Honour&quot;]</td>
<td>This query shows that arithmetical operations can be used in queries.</td>
</tr>
<tr>
<td>$books[?(@.id == 2</td>
<td></td>
<td>@.id == 4)].title</td>
<td>indefinite</td>
</tr>
<tr>
<td>$.books[?(!(@.id == 2)].title</td>
<td>indefinite</td>
<td>[&quot;SayingsoftheCentury&quot;, &quot;Moby Dick&quot;, &quot;The Lord of the Rings&quot;]</td>
<td></td>
</tr>
<tr>
<td>$.books[?(@.title =~ &quot; of &quot;)].title</td>
<td>indefinite</td>
<td>[&quot;SayingsoftheCentury&quot;, &quot;Sword of Honour&quot;, &quot;The Lord of the Rings&quot;]</td>
<td></td>
</tr>
<tr>
<td>$.books[?(@.price &gt; 12.99)].title</td>
<td>indefinite</td>
<td>[&quot;The Lord of the Rings&quot;]</td>
<td></td>
</tr>
<tr>
<td>$.books[?(@.author &gt; &quot;Herman Melville&quot;).title</td>
<td>indefinite</td>
<td>[&quot;SayingsoftheCentury&quot;, &quot;The Lord of the Rings&quot;]</td>
<td></td>
</tr>
<tr>
<td>$.books[?(@.price &gt; $.filters.price)].title</td>
<td>indefinite</td>
<td>[&quot;Sword of Honour&quot;, &quot;The Lord of the Rings&quot;]</td>
<td></td>
</tr>
<tr>
<td>$.books[?(@.category == $.filters.category)].title</td>
<td>indefinite</td>
<td>[&quot;Sword of Honour&quot;, &quot;Moby Dick&quot;, &quot;The Lord of the Rings&quot;]</td>
<td></td>
</tr>
<tr>
<td>JSONPath</td>
<td>Type</td>
<td>Result</td>
<td>Comments</td>
</tr>
<tr>
<td>----------</td>
<td>--------</td>
<td>----------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>$[..[?(@.id)]</td>
<td>indefinite</td>
<td>[</td>
<td>A query without match returns NULL for definite and indefinite paths. Text constants must be used in boolean value comparisons.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>{</td>
<td></td>
</tr>
</tbody>
</table>
14 Unreachable/unavailable host settings

Overview

Several configuration parameters define how Zabbix server should behave when an agent check (Zabbix, SNMP, IPMI, JMX) fails and a host becomes unreachable.

Unreachable host

A host is treated as unreachable after a failed check (network error, timeout) by Zabbix, SNMP, IPMI or JMX agents. Note that Zabbix agent active checks do not influence host availability in any way.

From that moment UnreachableDelay defines how often a host is rechecked using one of the items (including LLD rules) in this unreachability situation and such rechecks will be performed already by unreachable pollers (or IPMI pollers for IPMI checks). By default it is 15 seconds before the next check.

In the Zabbix server log unreachability is indicated by messages like these:

Zabbix agent item "system.cpu.load[percpu,avg1]" on host "New host" failed: first network error, wait for 15 seconds
Zabbix agent item "system.cpu.load[percpu,avg15]" on host "New host" failed: another network error, wait for 30 seconds

Note that the exact item that failed is indicated and the item type (Zabbix agent).

The Timeout parameter will also affect how early a host is rechecked during unreachability. If the Timeout is 20 seconds and UnreachableDelay 30 seconds, the next check will be in 50 seconds after the first attempt.

The UnreachablePeriod parameter defines how long the unreachability period is in total. By default UnreachablePeriod is 45 seconds. UnreachablePeriod should be several times bigger than UnreachableDelay, so that a host is rechecked more than once before a host becomes unavailable.

Switching host back to available

When unreachability period is over, the host is polled again, decreasing priority for item, that turned host into unreachable state. If the unreachable host reappears, the monitoring returns to normal automatically:

resuming Zabbix agent checks on host "New host": connection restored

Note:

Once host becomes available, it does not poll all its items immediately for two reasons:
- It might overload the host.
- The host restore time is not always matching planned item polling schedule time.

So, after the host becomes available, items are not polled immediately, but they are getting rescheduled to their next polling round.

Unavailable host

After the UnreachablePeriod ends and the host has not reappeared, the host is treated as unavailable.

In the server log it is indicated by messages like these:

temporarily disabling Zabbix agent checks on host "New host": host unavailable

and in the frontend the host availability icon for the respective interface goes from green (or gray) to red (note that on mouseover a tooltip with the error description is displayed):

Get value from agent failed: cannot connect to [192.168.3.31]:32050: [111] Connection refused
The **UnavailableDelay** parameter defines how often a host is checked during host unavailability. By default it is 60 seconds (so in this case “temporarily disabling”, from the log message above, will mean disabling checks for one minute).

When the connection to the host is restored, the monitoring returns to normal automatically, too:

enabling Zabbix agent checks on host "New host": host became available

### 15 Remote monitoring of Zabbix stats

**Overview**

Starting with Zabbix 4.0.5, it is possible to make some internal metrics of Zabbix server and proxy accessible remotely by another Zabbix instance or a third party tool. This can be useful so that supporters/service providers can monitor their client Zabbix servers/proxies remotely or, in organizations where Zabbix is not the main monitoring tool, that Zabbix internal metrics can be monitored by a third party system in an umbrella-monitoring setup.

Zabbix internal stats are exposed to a configurable set of addresses listed in the new `StatsAllowedIP` server/proxy parameter. Requests will be accepted only from these addresses.

**Items**

To configure querying of internal stats on another Zabbix instance, you may use two items:

- `zabbix[stats,<ip>,<port>]` internal item - for direct remote queries of Zabbix server/proxy. `<ip>` and `<port>` are used to identify the target instance.
- `zabbix.stats[<ip>,<port>]` agent item - for agent-based remote queries of Zabbix server/proxy. `<ip>` and `<port>` are used to identify the target instance.

See also: [Internal items](#), [Zabbix agent items](#)

The following diagram illustrates the use of either item depending on the context.
To make sure that the target instance allows querying it by the external instance, list the address of the external instance in the 'StatsAllowedIP' parameter on the target instance.

Exposed metrics

The stats items gather the statistics in bulk and return a JSON, which is the basis for dependent items to get their data from. The following internal metrics are returned by either of the two items:

- `zabbix[boottime]`
- `zabbix[hosts]`
- `zabbix[items]`
- `zabbix[items_unsupported]`
- `zabbix[preprocessing_queue]` (server only)
- `zabbix[process,<type>,<mode>,<state>]` (only process type based statistics)
- `zabbix[rcache,<cache>,<mode>]`
- `zabbix[requiredperformance]`
- `zabbix[triggers]` (server only)
- `zabbix[uptime]`
- `zabbix[vcache,buffer,<mode>]` (server only)
- `zabbix[vcache,cache,<parameter>]`
Templates

Templates are available for remote monitoring of Zabbix server or proxy internal metrics from an external instance:

- Template App Remote Zabbix server
- Template App Remote Zabbix proxy

Note that in order to use a template for remote monitoring of multiple external instances, a separate host is required for each external instance monitoring.

Trapper process

Receiving internal metric requests from an external Zabbix instance is handled by the trapper process that validates the request, gathers the metrics, creates the JSON data buffer and sends the prepared JSON back, for example, from server:

```json
{
  "response": "success",
  "data": {
    "boottime": N,
    "hosts": N,
    "items": N,
    "items_unsupported": 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
```
Internal queue items

There are also another two items specifically allowing to remote query internal queue stats on another Zabbix instance:

- `zabbix[stats,<ip>,<port>,queue,<from>,<to>]` internal item - for direct internal queue queries to remote Zabbix server/proxy
- `zabbix.stats[<ip>,<port>,queue,<from>,<to>]` agent item - for agent-based internal queue queries to remote Zabbix server/proxy

See also: Internal items, Zabbix agent items

6 Triggers

1 Supported trigger functions

All functions supported in trigger expressions are listed here.
<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>abschange</td>
<td>The amount of absolute difference between last and previous values.</td>
<td>Supported value types: float, int, str, text, log.</td>
<td>For example: ((\text{previous value};\text{last value})=\text{abschange}) (1;5=4) (3;1=2) (0;-=2.5). For strings returns: 0 - values are equal 1 - values differ.</td>
</tr>
</tbody>
</table>

**avg** (sec|num,<time_shift>)
**FUNCTION**

Average value of an item within the defined evaluation period.

**sec**

-supported value types: float, int

Examples:

- `avg(#5)` → average value for the five latest values
- `avg(1h)` → average value for an hour
- `avg(1h,1d)` → average value for an hour one day ago.

The `time_shift` parameter is supported since Zabbix 1.8.2. It is useful when there is a need to compare the current average value with the average value `time_shift` seconds back.

```plaintext
band (<sec|#num>,mask,<time_shift>)
```
Value of "bitwise AND" of an item value and mask.

**sec**
(ignored, equals #1) or

**#num**
(optional)
- the Nth most recent value

**mask**
(mandatory) - 64-bit unsigned integer (0 - 18446744073709551615)

**time_shift**
(optional)
- evaluation point is moved the number of seconds back in time

Supported value types: int

Take note that #num works differently here than with many other functions (see last()).

Although the comparison is done in a bitwise manner, all the values must be supplied and are returned in decimal. For example, checking for the 3rd bit is done by comparing to 4, not 100.

Examples:

```plaintext
=>
band(,12)=8 or band(,12)=4 → 3rd or 4th bit set, but not both at the same time
=>
band(,20)=16 → 3rd bit not set and 5th bit set.
```

This function is supported since Zabbix 2.2.0.
FUNCTION

change

The amount of difference between last and previous values.

Supported value types: float, int, str, text, log

For example:
(previous value;last value=change)
1;5=+4
3;1=-2
0;-2.5=-2.5

See also:
abschange for comparison

For strings returns:
0 - values are equal
1 - values differ

count (sec|#num,<pattern>,<operator>,<time_shift>)
FUNCTION

Number of values within the defined evaluation period.

sec or
#num - maximum evaluation period in seconds or in latest collected values (preceded by a hash mark)

Supported value types: float, integer, string, text, log

pattern (optional) - required pattern

operator (optional)

Supported operators:
eq - equal
ne - not equal
gt - greater
gle - greater or equal
lt - less
le - less or equal
like - matches if contains pattern (case-sensitive)
binary - bitwise AND
regexp - case sensitive match of regular expression given in pattern

regexp - case insensitive match of regular expression given in pattern

With band as third parameter, the second pattern parameter can be specified as two numbers, separated by '/':

num-number_to_compare_with/
count() calculates “bitwise AND” from the value and the mask and compares the result to num-number_to_compare_with.

If the result of “bitwise AND” is equal to num-number_to_compare_with, the value is counted. If num-number_to_compare_with and mask are equal, only the mask need be specified (without '/').

Note that: With regexp or

1.8.2.
1.6.1.
3.2.0.
**FUNCTION**

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
<th>Supported value types</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>date</strong></td>
<td>Current date in YYYYMMDD format.</td>
<td>any</td>
</tr>
<tr>
<td><strong>dayofmonth</strong></td>
<td>Day of month in range of 1 to 31.</td>
<td>any</td>
</tr>
<tr>
<td><strong>dayofweek</strong></td>
<td>Day of week in range of 1 to 7 (Mon - 1, Sun - 7).</td>
<td>any</td>
</tr>
<tr>
<td>**delta (sec</td>
<td>#num,&lt;time_shift&gt;)**</td>
<td>Difference between the maximum and minimum values within the defined evaluation period (‘max()’ minus ‘min()’).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>float, int</td>
</tr>
</tbody>
</table>

1. The time_shift parameter is supported since Zabbix 1.8.2.
FUNCTION

Checking if last and previous values differ.

Supported value types: float, int, str, text, log

Returns:
1 - last and previous values differ
0 - otherwise

forecast (sec|num,<time_shift>,time,<fit>,<mode>)
**FUNCTION**

Future value, max, min, delta or avg of the item.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>sec</strong> or <strong>#num</strong></td>
<td>Maximum evaluation period in seconds or in latest collected values specified (preceded by a hash mark)</td>
</tr>
<tr>
<td><strong>max, min</strong></td>
<td>If value to return is larger than 999999999999.9999 or less than -999999999999.9999, return value is cropped to 999999999999.9999 or -999999999999.9999 correspondingly.</td>
</tr>
<tr>
<td><strong>delta or avg of the item.</strong></td>
<td>Becomes not supported only if misused in expression (wrong item type, invalid parameters), otherwise returns -1 in case of errors.</td>
</tr>
</tbody>
</table>

**time_shift** (optional) - evaluation point is moved the number of seconds back in time

**time** - forecasting horizon in seconds

**fit** (optional) - function used to fit historical data

Supported fits:
- linear
- polynomial of degree N (1 <= N <= 6)
- exponential
- logarithmic
- power

Examples:
- linear => forecast
- polynomial of degree 3 => forecast
- exponential based on last 10 values => forecast
- logarithmic function of item => forecast
- power function after 30 minutes based on data => forecast
- Note that: linear is default, polynomial1 is

Supported value types: float, int

Examples:
- forecast(#10"1h) → forecast of item value after one hour based on last 10 values
- forecast(1h"30m) → forecast of item value after 30 minutes based on latest hour data
- forecast(1h,1d,12h) → forecast of item value after 12 hours based on one hour, one day ago
- forecast(1h"10m,exponential) → forecast of item value after 10 minutes based on last hour data and exponential function
- forecast(1h"2h,polynomial3,max) → forecast of maximum value item can reach in next two hours based on last hour data and cubic (third degree) polynomial

=> forecast(#2"-20m) → estimate the value of an item which was 20 minutes ago based on last two values (this can be more precise than using last() or prev(), especially if item is updated rarely, say, once an hour)

This function is supported since Zabbix 3.0.0. Negative time values are supported since Zabbix 3.0.6 and 3.2.2. See also additional information on predictive trigger functions.
FUNCTION
fuzzytime (sec)
Checking how much the passive agent time differs from the Zabbix server/proxy time.

**sec** - seconds

Supported value types: float, int

Returns:
1 - difference between the passive item value (as times-tamp) and Zabbix server/proxy times-tamp (clock of value collection) is less than or equal to T seconds
0 - otherwise

Usually used with the ‘system.localtime’ item to check that local time is in sync with the local time of Zabbix server. Note that ‘system.localtime’ must be configured as a [passive check](#).

Can be used also with vfs.file.time[/path/file,modify] key to check that file didn’t get updates for long time.

Example:
=> fuzzy-time(60)=0 → detect a problem if time difference is over 60 seconds

This function is not recommended for use in complex trigger expressions (with multiple items involved), because it may cause unexpected results (time difference will be measured with the most recent metric), e.g. in Host:system.localtime.fuzzytime(60)=0 or {Host:trap.last()}<>0
FUNCTION

iregexp (<pattern>,<sec|#num>)

This function is a non-case-sensitive analog of regexp().

Supported value types: str, log, text

last (<sec|#num>,<time_shift>)
<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
<th>Supported value types</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>last()</strong></td>
<td>The most recent value.</td>
<td>float, int, str, text, log</td>
<td>Take note that <strong>#num</strong> works differently here than with many other functions. For example: last() is always equal to last(#1) last(#3) - third most recent value (not three latest values) Zabbix does not guarantee exact order of values if more than two values exist within one second in history. The <strong>#num</strong> parameter is supported since Zabbix 1.6.2. The <strong>time_shift</strong> parameter is supported since Zabbix 1.8.2.</td>
</tr>
</tbody>
</table>

**logeventid (<pattern>)**
### FUNCTION

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
<th>Supported value types</th>
<th>Returns</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>logseverity</strong></td>
<td>Log severity of the last log entry.</td>
<td>log</td>
<td>0 - default severity N - severity (integer, useful for Windows event logs: 1 - Information, 2 - Warning, 4 - Error, 7 - Failure Audit, 8 - Success Audit, 9 - Critical, 10 - Verbose). Zabbix takes log severity from Information field of Windows event log.</td>
</tr>
<tr>
<td><strong>logsource</strong> (&lt;pattern&gt;)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### max (sec|num,<time_shift>)

Highest value of an item within the defined evaluation period.

- **sec or #num** - maximum evaluation period in seconds or in latest collected values (preceded by a hash mark)
- **time_shift** (optional) - evaluation point is moved the number of seconds back in time

Supported value types: float, int

Normally used for Windows event logs. For example, log-source("VMware Server").

### min (sec|num,<time_shift>)
**FUNCTION**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sec or #num - maximum evaluation period[^1] in seconds or in latest collected values (preceded by a hash mark)</td>
<td>The time_shift parameter is supported since Zabbix 1.8.2.</td>
</tr>
<tr>
<td>time_shift (optional)</td>
<td>- Evaluation point is moved the number of seconds back in time</td>
</tr>
<tr>
<td>nodata (sec)</td>
<td>Supported value types: float, int</td>
</tr>
</tbody>
</table>

[^1]: Evaluation period is defined as the time_shift parameter.
Checking for no data received.

**Function: Checking for data received.**

**sec** - evaluation period in seconds. The period should not be less than 30 seconds because the history syncer process calculates this function only every 30 seconds.

**nodata(0) is disallowed.**

**Supported value types:** any

**Returns:**
- 1 - if no data received during the defined period of time
- 0 - otherwise

Note that this function will display an error if, within the period of the 1st parameter:
- there's no data and Zabbix server was restarted
- there's no data and maintenance was completed
- there's no data and the item was added or re-enabled

Errors are displayed in the Info column in trigger configuration.

This function may not work properly if there are time differences between Zabbix server, proxy and agent.

See also: Time synchronization requirement.
now

Number of seconds since the Epoch (00:00:00 UTC, January 1, 1970).

Supported value types: any

percentile (sec|#num,<time_shift>,percentage)

P-th percentile of a period, where P (percentage) is specified by the third parameter.

Supported value types: float, int

This function is supported since Zabbix 3.0.0.

time_shift (optional)
- evaluation point is moved the number of seconds back in time
- a floating-point number between 0 and 100 (inclusive) with up to 4 digits after the decimal point

prev

Previous value.

Supported value types: float, int, str, text, log

Returns the same as last(#2).

regexp (<pattern>,<sec|#num>)
Checking if the latest (most recent) value matches regular expression.

**pattern** (optional) - regular expression, **Perl Compatible Regular Expression** (PCRE) style.

**sec** or **#num** (optional) - maximum evaluation period \(^1\) in seconds or in latest collected values (preceded by a hash mark). In this case, more than one value may be processed.

Supported value types: str, text, log

Returns:
1 - found
0 - otherwise

If more than one value is processed, ‘1’ is returned if there is at least one matching value.

This function is case-sensitive.

\[\text{str (<pattern>,<sec|#num>)}\]
Finding a string in the latest (most recent) value.

<table>
<thead>
<tr>
<th><strong>Pattern</strong> (optional)</th>
<th>Supported value types: str, text, log</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>sec</code> or <code>#num</code> (optional)</td>
<td>maximum evaluation period in seconds or in latest collected values (preceded by a hash mark). In this case, more than one value may be processed.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Returns</strong></th>
<th>If more than one value is processed, ‘1’ is returned if there is at least one matching value.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - found</td>
<td>0 - otherwise</td>
</tr>
</tbody>
</table>

If more than one value is processed, ‘1’ is returned if there is at least one matching value.

This function is case-sensitive.

Tip: You may use the 'count' function with the like operator to count string values that match a pattern.

`strlen(<sec|#num>,<time_shift>)`
Length of the latest (most recent) value in characters (not bytes).

**sec** (ignored, equals #1) or **num** (optional) - the Nth most recent value

**time_shift** (optional) - evaluation point is moved the number of seconds back in time

Supported value types: str, text, log

Take note that **num** works differently here than with many other functions.

Examples:

- `strlen()` (is equal to `strlen(#1)`)
  → length of the latest value
- `strlen(#3)`
  → length of the third most recent value
- `strlen(,1d)`
  → length of the most recent value one day ago.

This function is supported since Zabbix 1.8.4.

**sum** (sec|num,<time_shift>)
## FUNCTION

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sum</strong></td>
<td>Sum of collected values within the defined evaluation period.</td>
</tr>
<tr>
<td><strong>sec or #num</strong></td>
<td>Maximum evaluation period in seconds or in latest collected values (preceded by a hash mark).</td>
</tr>
<tr>
<td><strong>time_shift</strong></td>
<td>Parameter is supported since Zabbix 1.8.2.</td>
</tr>
</tbody>
</table>

### time

Current time in HHMMSS format. Supported value types: any.

Example of returned value: 123055

### timeleft (sec,#num,<time_shift>,threshold,<fit>)
FUNCTION

Time in seconds needed for an item to reach a specified threshold.

**sec** or **#num** - maximum evaluation period\(^1\) in seconds or in latest collected values (preceded by a hash mark)

**time_shift** (optional)
- evaluation point is moved the number of seconds back in time

**threshold** - value to reach

**fit** (optional)
- see forecast()

Supported value types: float, int

If value to return is larger than 999999999999.9999, return value is cropped to 999999999999.9999.

Returns 999999999999.9999 if threshold cannot be reached.

Becomes not supported only if misused in expression (wrong item type, invalid parameters), otherwise returns -1 in case of errors.

Examples:

\[ \text{timeleft(#10,0)} \]
\[ \rightarrow \text{time} \]
\[ \rightarrow \text{time until item value reaches zero based on last 10 values} \]

\[ \text{timeleft(1h,100)} \]
\[ \rightarrow \text{time} \]
\[ \rightarrow \text{time until item value reaches 100 based on last hour data} \]

1329
**Warning:**
Important notes:
1) All functions return numeric values only. Comparison to strings is not supported.
2) Some of the functions cannot be used for non-numeric values!
3) String arguments should be double quoted. Otherwise, they might get misinterpreted.
4) For all trigger functions sec and time_shift must be an integer with an optional time unit suffix and has absolutely nothing to do with the item’s data type.

Footnotes

1 The evaluation period is up to the latest collected value (not the server ‘now’ time). A function is evaluated as soon as at least one value is received (unless the time_shift parameter is used), i.e. Zabbix will not wait for all the values within the defined evaluation period before evaluating the function.

Functions and unsupported items

Since Zabbix 3.2, nodata(), date(), dayofmonth(), dayofweek(), now() and time() functions are calculated for unsupported items, too. Other functions require that the referenced item is in a supported state.

7 Macros

1 Supported macros

Overview

The table contains a complete list of macros supported by Zabbix out-of-the-box.

**Note:**
To see all macros supported in a location (for example, in "map URL"), you may paste the location name into the search box at the bottom of your browser window (accessible by pressing CTRL+F) and do a search for next.

<table>
<thead>
<tr>
<th>Macro</th>
<th>Supported in</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>{ACTION.ID}</td>
<td>→ Trigger-based notifications and commands</td>
<td>Numeric ID of the triggered action. Supported since 2.2.0.</td>
</tr>
<tr>
<td></td>
<td>→ Problem update notifications and commands</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Discovery notifications and commands</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Autoregistration notifications and commands</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Internal notifications</td>
<td></td>
</tr>
<tr>
<td>{ACTION.NAME}</td>
<td>→ Trigger-based notifications and commands</td>
<td>Name of the triggered action. Supported since 2.2.0.</td>
</tr>
<tr>
<td></td>
<td>→ Problem update notifications and commands</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Discovery notifications and commands</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Autoregistration notifications and commands</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Internal notifications</td>
<td></td>
</tr>
<tr>
<td>{ALERT.MESSAGE}</td>
<td>→ Alert script parameters</td>
<td>'Default message' value from action configuration. Supported since 3.0.0.</td>
</tr>
<tr>
<td>{ALERT.SENDTO}</td>
<td>→ Alert script parameters</td>
<td>'Send to' value from user media configuration. Supported since 3.0.0.</td>
</tr>
<tr>
<td>{ALERT.SUBJECT}</td>
<td>→ Alert script parameters</td>
<td>'Default subject' value from action configuration. Supported since 3.0.0.</td>
</tr>
<tr>
<td>{DATE}</td>
<td>→ Trigger-based notifications and commands</td>
<td>Current date in yyyy.mm.dd format.</td>
</tr>
<tr>
<td></td>
<td>→ Problem update notifications and commands</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Discovery notifications and commands</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Autoregistration notifications and commands</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Internal notifications</td>
<td></td>
</tr>
</tbody>
</table>
## Supported Macros

<table>
<thead>
<tr>
<th>Macro</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>{DISCOVERY.DEVICE.IP ADDRESS}</td>
<td>IP address of the discovered device. Available always, does not depend on host being added.</td>
</tr>
<tr>
<td>{DISCOVERY.DEVICE.DNS}</td>
<td>DNS name of the discovered device. Available always, does not depend on host being added.</td>
</tr>
<tr>
<td>{DISCOVERY.DEVICE.STATUS}</td>
<td>Status of the discovered device: can be either UP or DOWN.</td>
</tr>
<tr>
<td>{DISCOVERY.DEVICE.UPTIME}</td>
<td>Time since the last change of discovery status for a particular device, with precision down to a second since Zabbix 4.0.25 (down to a minute before that). For example: 1h29m01s. For devices with status DOWN, this is the period of their downtime.</td>
</tr>
<tr>
<td>{DISCOVERY.RULE.NAME}</td>
<td>Name of the discovery rule that discovered the presence or absence of the device or service.</td>
</tr>
<tr>
<td>{DISCOVERY.SERVICE.NAME}</td>
<td>Name of the service that was discovered. For example: HTTP.</td>
</tr>
<tr>
<td>{DISCOVERY.SERVICE.PORT}</td>
<td>Port of the service that was discovered. For example: 80.</td>
</tr>
<tr>
<td>{DISCOVERY.SERVICE.STATUS}</td>
<td>Status of the discovered service: can be either UP or DOWN.</td>
</tr>
<tr>
<td>{DISCOVERY.SERVICE.UPTIME}</td>
<td>Time since the last change of discovery status for a particular service, with precision down to a second since Zabbix 4.0.25 (down to a minute before that). For example: 1h29m01s. For services with status DOWN, this is the period of their downtime.</td>
</tr>
<tr>
<td>{ESC.HISTORY}</td>
<td>Trigger-based notifications and commands&lt;br&gt;→ Problem update notifications and commands&lt;br&gt;→ Discovery notifications and commands&lt;br&gt;→ Autoregistration notifications and commands&lt;br&gt;→ Internal notifications&lt;br&gt;Escalation history. Log of previously sent messages. Shows previously sent notifications, on which escalation step they were sent and their status (sent//, in progress or failed).</td>
</tr>
<tr>
<td>{EVENT.ACK.STATUS}</td>
<td>Acknowledgment status of the event (Yes/No).</td>
</tr>
<tr>
<td>{EVENT.AGE}</td>
<td>Age of the event that triggered an action, with precision down to a second since Zabbix 4.0.25 (down to a minute before that). Useful in escalated messages.</td>
</tr>
<tr>
<td>{EVENT.DATE}</td>
<td>Date of the event that triggered an action.</td>
</tr>
<tr>
<td>{EVENT.ID}</td>
<td>Numeric ID of the event that triggered an action.</td>
</tr>
<tr>
<td>{EVENT.NAME}</td>
<td>Name of the problem event that triggered an action. Supported since 4.0.0.</td>
</tr>
<tr>
<td>Macro</td>
<td>Supported in</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>{EVENT.SEVERITY}</td>
<td>→ Trigger-based notifications and commands</td>
</tr>
<tr>
<td></td>
<td>→ Problem update notifications and commands</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>{EVENT.NSEVERITY}</td>
<td>→ Trigger-based notifications and commands</td>
</tr>
<tr>
<td></td>
<td>→ Problem update notifications and commands</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>{EVENT.RECOVERY.DATE}</td>
<td>Problem recovery notifications and commands</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>{EVENT.RECOVERY.ID}</td>
<td>Problem recovery notifications and commands</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>{EVENT.RECOVERY.NAME}</td>
<td>Problem recovery notifications and commands</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>{EVENT.RECOVERY.STATUS}</td>
<td>Problem recovery notifications and commands</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>{EVENT.RECOVERY.TAGS}</td>
<td>Problem recovery notifications and commands</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>{EVENT.RECOVERY.TIME}</td>
<td>Problem recovery notifications and commands</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>{EVENT.RECOVERY.VALUE}</td>
<td>Problem recovery notifications and commands</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>{EVENT.SEVERITY}</td>
<td>→ Trigger-based notifications and commands</td>
</tr>
<tr>
<td></td>
<td>→ Problem update notifications and commands</td>
</tr>
<tr>
<td>{EVENT.STATUS}</td>
<td>→ Trigger-based notifications and commands</td>
</tr>
<tr>
<td></td>
<td>→ Discovery notifications and commands</td>
</tr>
<tr>
<td></td>
<td>→ Autoregistration notifications and commands</td>
</tr>
<tr>
<td></td>
<td>→ Internal notifications</td>
</tr>
<tr>
<td>{EVENT.TAGS}</td>
<td>→ Trigger-based notifications and commands</td>
</tr>
<tr>
<td></td>
<td>→ Problem update notifications and commands</td>
</tr>
<tr>
<td>{EVENT.TIME}</td>
<td>→ Trigger-based notifications and commands</td>
</tr>
<tr>
<td></td>
<td>→ Problem update notifications and commands</td>
</tr>
<tr>
<td></td>
<td>→ Discovery notifications and commands</td>
</tr>
<tr>
<td></td>
<td>→ Autoregistration notifications and commands</td>
</tr>
<tr>
<td></td>
<td>→ Internal notifications</td>
</tr>
<tr>
<td>{EVENT.UPDATE.DATE}</td>
<td>Problem update notifications and commands</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>{EVENT.UPDATE.HISTORY}</td>
<td>Trigger-based notifications and commands</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>{EVENT.UPDATE.MESSAGE}</td>
<td>Problem update notifications and commands</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>{EVENT.UPDATE.TIME}</td>
<td>Problem update notifications and commands</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>{EVENT.VALUE}</td>
<td>→ Trigger-based notifications and commands</td>
</tr>
<tr>
<td></td>
<td>→ Discovery notifications and commands</td>
</tr>
<tr>
<td></td>
<td>→ Autoregistration notifications and commands</td>
</tr>
<tr>
<td></td>
<td>→ Internal notifications</td>
</tr>
<tr>
<td>Macro</td>
<td>Supported in</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>{HOST.CONN&lt;1-9&gt;}</td>
<td>→ Trigger-based notifications and commands&lt;br&gt;→ Problem update notifications and commands&lt;br&gt;→ Internal notifications&lt;br&gt;→ Global scripts (including confirmation text)&lt;br&gt;→ Icon labels in maps&lt;sup&gt;1&lt;/sup&gt;&lt;br&gt;→ Item key parameters&lt;sup&gt;2&lt;/sup&gt;&lt;br&gt;→ Host interface IP/DNS&lt;br&gt;→ Trapper item “Allowed hosts” field&lt;sup&gt;12&lt;/sup&gt;&lt;br&gt;→ Database monitoring additional parameters&lt;sup&gt;5&lt;/sup&gt;&lt;br&gt;→ SSH and Telnet scripts&lt;sup&gt;5&lt;/sup&gt;&lt;br&gt;→ JMX item endpoint field&lt;br&gt;→ Web monitoring&lt;sup&gt;6&lt;/sup&gt;&lt;br&gt;→ Low-level discovery rule filter regular expressions&lt;sup&gt;8&lt;/sup&gt;&lt;br&gt;→ URL field of dynamic URL dashboard widget/screen element&lt;sup&gt;8&lt;/sup&gt;&lt;br&gt;→ Trigger names and descriptions&lt;br&gt;→ Trigger URLs&lt;sup&gt;10&lt;/sup&gt;&lt;br&gt;→ Event tags and values&lt;br&gt;→ HTTP agent type item, item prototype and discovery rule fields:&lt;br&gt; URL, Query fields, Request body, Headers, Proxy, SSL certificate file, SSL key file, Allowed hosts&lt;sup&gt;12&lt;/sup&gt;.</td>
</tr>
<tr>
<td>{HOST.DESCRIPTION&lt;1-9&gt;}</td>
<td>→ Trigger-based notifications and commands&lt;br&gt;→ Problem update notifications and commands&lt;br&gt;→ Internal notifications&lt;br&gt;→ Icon labels in maps&lt;sup&gt;1&lt;/sup&gt;&lt;br&gt;→ Item key parameters&lt;sup&gt;2&lt;/sup&gt;&lt;br&gt;→ Host interface IP/DNS&lt;br&gt;→ Trapper item “Allowed hosts” field&lt;sup&gt;12&lt;/sup&gt;&lt;br&gt;→ Database monitoring additional parameters&lt;sup&gt;5&lt;/sup&gt;&lt;br&gt;→ SSH and Telnet scripts&lt;sup&gt;5&lt;/sup&gt;&lt;br&gt;→ JMX item endpoint field&lt;br&gt;→ Web monitoring&lt;sup&gt;6&lt;/sup&gt;&lt;br&gt;→ Low-level discovery rule filter regular expressions&lt;sup&gt;8&lt;/sup&gt;&lt;br&gt;→ URL field of dynamic URL dashboard widget/screen element&lt;sup&gt;8&lt;/sup&gt;&lt;br&gt;→ Trigger names and descriptions&lt;br&gt;→ Trigger URLs&lt;sup&gt;10&lt;/sup&gt;&lt;br&gt;→ Event tags and values&lt;br&gt;→ HTTP agent type item, item prototype and discovery rule fields:&lt;br&gt; URL, Query fields, Request body, Headers, Proxy, SSL certificate file, SSL key file, Allowed hosts&lt;sup&gt;12&lt;/sup&gt;.</td>
</tr>
<tr>
<td>{HOST.DNS&lt;1-9&gt;}</td>
<td>→ Trigger-based notifications and commands&lt;br&gt;→ Problem update notifications and commands&lt;br&gt;→ Internal notifications&lt;br&gt;→ Icon labels in maps&lt;sup&gt;1&lt;/sup&gt;&lt;br&gt;→ Item key parameters&lt;sup&gt;2&lt;/sup&gt;&lt;br&gt;→ Host interface IP/DNS&lt;br&gt;→ Trapper item “Allowed hosts” field&lt;sup&gt;12&lt;/sup&gt;&lt;br&gt;→ Database monitoring additional parameters&lt;sup&gt;5&lt;/sup&gt;&lt;br&gt;→ SSH and Telnet scripts&lt;sup&gt;5&lt;/sup&gt;&lt;br&gt;→ JMX item endpoint field&lt;br&gt;→ Web monitoring&lt;sup&gt;6&lt;/sup&gt;&lt;br&gt;→ Low-level discovery rule filter regular expressions&lt;sup&gt;8&lt;/sup&gt;&lt;br&gt;→ URL field of dynamic URL dashboard widget/screen element&lt;sup&gt;8&lt;/sup&gt;&lt;br&gt;→ Trigger names and descriptions&lt;br&gt;→ Trigger URLs&lt;sup&gt;10&lt;/sup&gt;&lt;br&gt;→ Event tags and values&lt;br&gt;→ HTTP agent type item, item prototype and discovery rule fields:&lt;br&gt; URL, Query fields, Request body, Headers, Proxy, SSL certificate file, SSL key file, Allowed hosts&lt;sup&gt;12&lt;/sup&gt;.</td>
</tr>
<tr>
<td>Macro</td>
<td>Supported in</td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>{HOST.HOST&lt;1-9&gt;}</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>{HOST.ID&lt;1-9&gt;}</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>{HOST.IP&lt;1-9&gt;}</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>{HOST.METADATA}</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\(^1\) {HOSTNAME<1-9>} is deprecated.

\(^2\) {HOST.IP<1-9>} is deprecated.
<table>
<thead>
<tr>
<th>Macro</th>
<th>Supported in</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>{HOST.NAME&lt;1-9&gt;}</td>
<td>→ Trigger-based notifications and commands</td>
<td>Visible host name.</td>
</tr>
<tr>
<td></td>
<td>→ Problem update notifications and commands</td>
<td>Supported since 2.0.0.</td>
</tr>
<tr>
<td></td>
<td>→ Internal notifications</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Global scripts (including confirmation text)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Icon labels in maps</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Item key parameters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Host interface IP/DNS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Trapper item “Allowed hosts” field</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Database monitoring additional parameters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ SSH and Telnet scripts</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Web monitoring</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Low-level discovery rule filter regular expressions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ URL field of dynamic URL dashboard widget/screen element</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Trigger names and descriptions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Trigger URLs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Event tags and values</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ HTTP agent type item, item prototype and discovery rule fields:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ URL, Query fields, Request body, Headers, Proxy, SSL certificate file, SSL</td>
<td></td>
</tr>
<tr>
<td></td>
<td>key file, Allowed hosts</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Trigger names and descriptions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Trigger URLs</td>
<td></td>
</tr>
<tr>
<td>{HOST.PORT&lt;1-9&gt;}</td>
<td>→ Trigger-based notifications and commands</td>
<td>Host (agent) port.</td>
</tr>
<tr>
<td></td>
<td>→ Problem update notifications and commands</td>
<td>Supported in auto-registration since 2.0.0.</td>
</tr>
<tr>
<td></td>
<td>→ Autoregistration notifications and commands</td>
<td>Supported in trigger names, trigger descriptions, internal and trigger-based</td>
</tr>
<tr>
<td></td>
<td>→ Internal notifications</td>
<td>notifications since 2.2.2.</td>
</tr>
<tr>
<td></td>
<td>→ Trigger names and descriptions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Trigger URLs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ JMX item endpoint field</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Event tags and values</td>
<td></td>
</tr>
<tr>
<td>{HOSTGROUP.ID}</td>
<td>→ Map URLs</td>
<td>Host group ID.</td>
</tr>
<tr>
<td>{INVENTORY.ALIAS&lt;1-9&gt;}</td>
<td>→ Trigger-based notifications and commands</td>
<td>Alias field in host inventory.</td>
</tr>
<tr>
<td></td>
<td>→ Problem update notifications and commands</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Internal notifications</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Tag names and values</td>
<td></td>
</tr>
<tr>
<td>{INVENTORY.ASSET.TAG&lt;1-9&gt;}</td>
<td>→ Trigger-based notifications and commands</td>
<td>Asset tag field in host inventory.</td>
</tr>
<tr>
<td></td>
<td>→ Problem update notifications and commands</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Internal notifications</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Tag names and values</td>
<td></td>
</tr>
<tr>
<td>{INVENTORY.CHASSIS&lt;1-9&gt;}</td>
<td>→ Trigger-based notifications and commands</td>
<td>Chassis field in host inventory.</td>
</tr>
<tr>
<td></td>
<td>→ Problem update notifications and commands</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Internal notifications</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Tag names and values</td>
<td></td>
</tr>
<tr>
<td>{INVENTORY.CONTACT&lt;1-9&gt;}</td>
<td>→ Trigger-based notifications and commands</td>
<td>Contact field in host inventory.</td>
</tr>
<tr>
<td></td>
<td>→ Problem update notifications and commands</td>
<td>{PROFILE.CONTACT&lt;1-9&gt;} is deprecated.</td>
</tr>
<tr>
<td></td>
<td>→ Internal notifications</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Tag names and values</td>
<td></td>
</tr>
<tr>
<td>{INVENTORY.NUMBER&lt;1-9&gt;}</td>
<td>→ Trigger-based notifications and commands</td>
<td>Contract number field in host inventory.</td>
</tr>
<tr>
<td></td>
<td>→ Problem update notifications and commands</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Internal notifications</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Tag names and values</td>
<td></td>
</tr>
<tr>
<td>{INVENTORY.DEPLOYMENT&lt;1-9&gt;}</td>
<td>→ Trigger-based notifications and commands</td>
<td>Deployment status field in host inventory.</td>
</tr>
<tr>
<td></td>
<td>→ Problem update notifications and commands</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Internal notifications</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Tag names and values</td>
<td></td>
</tr>
<tr>
<td>{INVENTORY.HARDWARE&lt;1-9&gt;}</td>
<td>→ Trigger-based notifications and commands</td>
<td>Hardware field in host inventory.</td>
</tr>
<tr>
<td></td>
<td>→ Problem update notifications and commands</td>
<td>{PROFILE.HARDWARE&lt;1-9&gt;} is deprecated.</td>
</tr>
<tr>
<td></td>
<td>→ Internal notifications</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Tag names and values</td>
<td></td>
</tr>
<tr>
<td>Macro</td>
<td>Supported in</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>{INVENTORY.HARDWARE.FULL}</td>
<td>Trigger-based notifications and commands</td>
<td>Hardware (Full details) field in host inventory.</td>
</tr>
<tr>
<td>9&gt; }</td>
<td>→ Problem update notifications and commands</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Internal notifications</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Tag names and values</td>
<td></td>
</tr>
<tr>
<td>{INVENTORY.HOST.NETMASK}</td>
<td>Trigger-based notifications and commands</td>
<td>Host subnet mask field in host inventory.</td>
</tr>
<tr>
<td>9&gt; }</td>
<td>→ Problem update notifications and commands</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Internal notifications</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Tag names and values</td>
<td></td>
</tr>
<tr>
<td>{INVENTORY.HOST.NETWORKS}</td>
<td>Trigger-based notifications and commands</td>
<td>Host networks field in host inventory.</td>
</tr>
<tr>
<td>9&gt; }</td>
<td>→ Problem update notifications and commands</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Internal notifications</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Tag names and values</td>
<td></td>
</tr>
<tr>
<td>{INVENTORY.HOST.ROUTER}</td>
<td>Trigger-based notifications and commands</td>
<td>Host router field in host inventory.</td>
</tr>
<tr>
<td>9&gt; }</td>
<td>→ Problem update notifications and commands</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Internal notifications</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Tag names and values</td>
<td></td>
</tr>
<tr>
<td>{INVENTORY.HW.ARCH}</td>
<td>Trigger-based notifications and commands</td>
<td>Hardware architecture field in host inventory.</td>
</tr>
<tr>
<td>9&gt; }</td>
<td>→ Problem update notifications and commands</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Internal notifications</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Tag names and values</td>
<td></td>
</tr>
<tr>
<td>{INVENTORY.HW.DATE.DECOMM}</td>
<td>Trigger-based notifications and commands</td>
<td>Date hardware decommissioned field in host inventory.</td>
</tr>
<tr>
<td>9&gt; }</td>
<td>→ Problem update notifications and commands</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Internal notifications</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Tag names and values</td>
<td></td>
</tr>
<tr>
<td>{INVENTORY.HW.DATE.EXPIRY}</td>
<td>Trigger-based notifications and commands</td>
<td>Date hardware maintenance expires field in host inventory.</td>
</tr>
<tr>
<td>9&gt; }</td>
<td>→ Problem update notifications and commands</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Internal notifications</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Tag names and values</td>
<td></td>
</tr>
<tr>
<td>{INVENTORY.HW.DATE.INSTALL}</td>
<td>Trigger-based notifications and commands</td>
<td>Date hardware installed field in host inventory.</td>
</tr>
<tr>
<td>9&gt; }</td>
<td>→ Problem update notifications and commands</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Internal notifications</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Tag names and values</td>
<td></td>
</tr>
<tr>
<td>{INVENTORY.HW.DATE.PURCHASE}</td>
<td>Trigger-based notifications and commands</td>
<td>Date hardware purchased field in host inventory.</td>
</tr>
<tr>
<td>9&gt; }</td>
<td>→ Problem update notifications and commands</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Internal notifications</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Tag names and values</td>
<td></td>
</tr>
<tr>
<td>{INVENTORY.INSTALLER.NAME}</td>
<td>Trigger-based notifications and commands</td>
<td>Installer name field in host inventory.</td>
</tr>
<tr>
<td>9&gt; }</td>
<td>→ Problem update notifications and commands</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Internal notifications</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Tag names and values</td>
<td></td>
</tr>
<tr>
<td>{INVENTORY.LOCATION}</td>
<td>Trigger-based notifications and commands</td>
<td>Location field in host inventory.</td>
</tr>
<tr>
<td>9&gt; }</td>
<td>→ Problem update notifications and commands</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Internal notifications</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Tag names and values</td>
<td></td>
</tr>
<tr>
<td>{PROFILE.LOCATION&lt;1-9&gt;} is deprecated.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>{INVENTORY.LOCATION.LAT}</td>
<td>Trigger-based notifications and commands</td>
<td>Location latitude field in host inventory.</td>
</tr>
<tr>
<td>9&gt; }</td>
<td>→ Problem update notifications and commands</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Internal notifications</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Tag names and values</td>
<td></td>
</tr>
<tr>
<td>{INVENTORY.LOCATION.LON}</td>
<td>Trigger-based notifications and commands</td>
<td>Location longitude field in host inventory.</td>
</tr>
<tr>
<td>9&gt; }</td>
<td>→ Problem update notifications and commands</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Internal notifications</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Tag names and values</td>
<td></td>
</tr>
<tr>
<td>{INVENTORY.MACADDRESS.A}</td>
<td>Trigger-based notifications and commands</td>
<td>MAC address A field in host inventory.</td>
</tr>
<tr>
<td>9&gt; }</td>
<td>→ Problem update notifications and commands</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Internal notifications</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Tag names and values</td>
<td></td>
</tr>
<tr>
<td>{PROFILE.MACADDRESS&lt;1-9&gt;} is deprecated.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>{INVENTORY.MACADDRESS.B}</td>
<td>Trigger-based notifications and commands</td>
<td>MAC address B field in host inventory.</td>
</tr>
<tr>
<td>9&gt; }</td>
<td>→ Problem update notifications and commands</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Internal notifications</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Tag names and values</td>
<td></td>
</tr>
<tr>
<td>Macro</td>
<td>Supported in</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>{INVENTORY.MODEL&lt;1-9&gt;}</td>
<td></td>
<td>Model field in host inventory.</td>
</tr>
<tr>
<td>{INVENTORY.NAME&lt;1-9&gt;}</td>
<td></td>
<td>Name field in host inventory.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{PROFILE.NAME&lt;1-9&gt;} is deprecated.</td>
</tr>
<tr>
<td>{INVENTORY.NOTES&lt;1-9&gt;}</td>
<td></td>
<td>Notes field in host inventory.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{PROFILE.NOTES&lt;1-9&gt;} is deprecated.</td>
</tr>
<tr>
<td>{INVENTORY.OOB.IP&lt;1-9&gt;}</td>
<td></td>
<td>OOB IP address field in host inventory.</td>
</tr>
<tr>
<td>{INVENTORY.OOB.NETMASK&lt;1-9&gt;}</td>
<td></td>
<td>OOB subnet mask field in host inventory.</td>
</tr>
<tr>
<td>{INVENTORY.OOB.ROUTER&lt;1-9&gt;}</td>
<td></td>
<td>OOB router field in host inventory.</td>
</tr>
<tr>
<td>{INVENTORY.OS&lt;1-9&gt;}</td>
<td></td>
<td>OS field in host inventory.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{PROFILE.OS&lt;1-9&gt;} is deprecated.</td>
</tr>
<tr>
<td>{INVENTORY.OS.FULL&lt;1-9&gt;}</td>
<td></td>
<td>OS (Full details) field in host inventory.</td>
</tr>
<tr>
<td>{INVENTORY.OS.SHORT&lt;1-9&gt;}</td>
<td></td>
<td>OS (Short) field in host inventory.</td>
</tr>
<tr>
<td>{INVENTORY.POC.PRIMARY.CELL&lt;1-9&gt;}</td>
<td></td>
<td>Primary POC cell field in host inventory.</td>
</tr>
<tr>
<td>{INVENTORY.POC.PRIMARY.EMAIL&lt;1-9&gt;}</td>
<td></td>
<td>Primary POC email field in host inventory.</td>
</tr>
<tr>
<td>{INVENTORY.POC.PRIMARY.NAME&lt;1-9&gt;}</td>
<td></td>
<td>Primary POC name field in host inventory.</td>
</tr>
<tr>
<td>{INVENTORY.POC.PRIMARY.NOTES&lt;1-9&gt;}</td>
<td></td>
<td>Primary POC notes field in host inventory.</td>
</tr>
<tr>
<td>{INVENTORY.POC.PRIMARYPHONE.A&lt;1-9&gt;}</td>
<td></td>
<td>Primary POC phone A field in host inventory.</td>
</tr>
<tr>
<td>{INVENTORY.POC.PRIMARYPHONE.B&lt;1-9&gt;}</td>
<td></td>
<td>Primary POC phone B field in host inventory.</td>
</tr>
<tr>
<td>Macro</td>
<td>Supported in</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td><code>{INVENTORY:POC.PRIMARY.SCREEN&lt;1-9&gt;}</code></td>
<td>Trigger-based notifications and commands</td>
<td>Primary POC screen name field in host inventory.</td>
</tr>
<tr>
<td><code>{INVENTORY:POC.SECONDARY.CELL&lt;1-9&gt;}</code></td>
<td>Trigger-based notifications and commands</td>
<td>Secondary POC cell field in host inventory.</td>
</tr>
<tr>
<td><code>{INVENTORY:POC.SECONDARY.EMAIL&lt;1-9&gt;}</code></td>
<td>Trigger-based notifications and commands</td>
<td>Secondary POC email field in host inventory.</td>
</tr>
<tr>
<td><code>{INVENTORY:POC.SECONDARY.NAME&lt;1-9&gt;}</code></td>
<td>Trigger-based notifications and commands</td>
<td>Secondary POC name field in host inventory.</td>
</tr>
<tr>
<td><code>{INVENTORY:POC.SECONDARY.NOTES&lt;1-9&gt;}</code></td>
<td>Trigger-based notifications and commands</td>
<td>Secondary POC notes field in host inventory.</td>
</tr>
<tr>
<td><code>{INVENTORY:SERIALNO.A&lt;1-9&gt;}</code></td>
<td>Trigger-based notifications and commands</td>
<td>Serial number A field in host inventory.</td>
</tr>
<tr>
<td><code>{INVENTORY:SERIALNO.B&lt;1-9&gt;}</code></td>
<td>Trigger-based notifications and commands</td>
<td>Serial number B field in host inventory.</td>
</tr>
<tr>
<td><code>{INVENTORY:SITE.ADDRESS.A&lt;1-9&gt;}</code></td>
<td>Trigger-based notifications and commands</td>
<td>Site address A field in host inventory.</td>
</tr>
<tr>
<td><code>{INVENTORY:SITE.ADDRESS.B&lt;1-9&gt;}</code></td>
<td>Trigger-based notifications and commands</td>
<td>Site address B field in host inventory.</td>
</tr>
<tr>
<td><code>{INVENTORY:SITE.ADDRESS.C&lt;1-9&gt;}</code></td>
<td>Trigger-based notifications and commands</td>
<td>Site address C field in host inventory.</td>
</tr>
<tr>
<td><code>{INVENTORY:SITE.CITY&lt;1-9&gt;}</code></td>
<td>Trigger-based notifications and commands</td>
<td>Site city field in host inventory.</td>
</tr>
<tr>
<td><code>{INVENTORY:SITE.COUNTRY&lt;1-9&gt;}</code></td>
<td>Trigger-based notifications and commands</td>
<td>Site country field in host inventory.</td>
</tr>
<tr>
<td>Macro</td>
<td>Supported in</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| `{INVENTORY:SITE.NOTES<9>` | Trigger-based notifications and commands  
   → Problem update notifications and commands  
   → Internal notifications  
   → Tag names and values | Site notes field in host inventory. |
| `{INVENTORY:SITE.RACK<9>` | Trigger-based notifications and commands  
   → Problem update notifications and commands  
   → Internal notifications  
   → Tag names and values | Site rack location field in host inventory. |
| `{INVENTORY:SITE.STATE<9>` | Trigger-based notifications and commands  
   → Problem update notifications and commands  
   → Internal notifications  
   → Tag names and values | Site state/province field in host inventory. |
| `{INVENTORY:SITE.ZIP<9>` | Trigger-based notifications and commands  
   → Problem update notifications and commands  
   → Internal notifications  
   → Tag names and values | Site ZIP/postal field in host inventory. |
| `{INVENTORY:SOFTWARE<9>` | Trigger-based notifications and commands  
   → Problem update notifications and commands  
   → Internal notifications  
   → Tag names and values | Software field in host inventory.  
   {PROFILE.SOFTWARE<1-9> is deprecated.} |
| `{INVENTORY:SOFTWARE.APP.A<9>` | Trigger-based notifications and commands  
   → Problem update notifications and commands  
   → Internal notifications  
   → Tag names and values | Software application A field in host inventory. |
| `{INVENTORY:SOFTWARE.APP.B<9>` | Trigger-based notifications and commands  
   → Problem update notifications and commands  
   → Internal notifications  
   → Tag names and values | Software application B field in host inventory. |
| `{INVENTORY:SOFTWARE.APP.C<9>` | Trigger-based notifications and commands  
   → Problem update notifications and commands  
   → Internal notifications  
   → Tag names and values | Software application C field in host inventory. |
| `{INVENTORY:SOFTWARE.APP.D<9>` | Trigger-based notifications and commands  
   → Problem update notifications and commands  
   → Internal notifications  
   → Tag names and values | Software application D field in host inventory. |
| `{INVENTORY:SOFTWARE.APP.E<9>` | Trigger-based notifications and commands  
   → Problem update notifications and commands  
   → Internal notifications  
   → Tag names and values | Software application E field in host inventory. |
| `{INVENTORY:SOFTWARE.FULL<9>` | Trigger-based notifications and commands  
   → Problem update notifications and commands  
   → Internal notifications  
   → Tag names and values | Software (Full details) field in host inventory. |
| `{INVENTORY:TAG<9>` | Trigger-based notifications and commands  
   → Problem update notifications and commands  
   → Internal notifications  
   → Tag names and values | Tag field in host inventory.  
   {PROFILE.TAG<1-9> is deprecated.} |
| `{INVENTORY:TYPE<9>` | Trigger-based notifications and commands  
   → Problem update notifications and commands  
   → Internal notifications  
   → Tag names and values | Type field in host inventory.  
   {PROFILE.DEVICETYPE<1-9> is deprecated.} |
| `{INVENTORY:TYPE.FULL<9>` | Trigger-based notifications and commands  
   → Problem update notifications and commands  
   → Internal notifications  
   → Tag names and values | Type (Full details) field in host inventory. |
| `{INVENTORY:URL.A<9>` | Trigger-based notifications and commands  
   → Problem update notifications and commands  
   → Internal notifications  
   → Tag names and values | URL A field in host inventory. |
<table>
<thead>
<tr>
<th>Macro</th>
<th>Supported in</th>
<th>Description</th>
</tr>
</thead>
</table>
| `{INVENTORY.URL.B<1-9>}`          | Trigger-based notifications and commands  
→ Trigger-based notifications and commands  
→ Problem update notifications and commands  
→ Internal notifications  
→ Tag names and values          | URL B field in host inventory.                                                                                                                |
| `{INVENTORY.URL.C<1-9>}`          | Trigger-based notifications and commands  
→ Trigger-based notifications and commands  
→ Problem update notifications and commands  
→ Internal notifications  
→ Tag names and values          | URL C field in host inventory.                                                                                                                |
| `{INVENTORY.VENDOR<1-9>}`         | Trigger-based notifications and commands  
→ Trigger-based notifications and commands  
→ Problem update notifications and commands  
→ Internal notifications  
→ Tag names and values          | Vendor field in host inventory.                                                                                                              |
| `{ITEM.DESCRIPTION<1-9>}`         | Trigger-based notifications and commands  
→ Trigger-based notifications and commands  
→ Problem update notifications and commands  
→ Internal notifications                                                                                               | Description of the Nth item in the trigger expression that caused a notification. Supported since 2.0.0. |
| `{ITEM.ID<1-9>}`                  | Trigger-based notifications and commands  
→ Trigger-based notifications and commands  
→ Problem update notifications and commands  
→ Internal notifications  
→ HTTP agent type item, item prototype and discovery rule fields:  
URL, query fields, request body, headers, proxy, SSL certificate file, SSL key file. | Numeric ID of the Nth item in the trigger expression that caused a notification. Supported since 1.8.12. |
| `{ITEM.KEY<1-9>}`                 | Trigger-based notifications and commands  
→ Trigger-based notifications and commands  
→ Problem update notifications and commands  
→ Internal notifications  
→ HTTP agent type item, item prototype and discovery rule fields:  
URL, query fields, request body, headers, proxy, SSL certificate file, SSL key file. | Key of the Nth item in the trigger expression that caused a notification. Supported since 2.0.0.  
\{TRIGGER.KEY\} is deprecated.                                                                                                    |
| `{ITEM.KEY.ORIG<1-9>}`            | Trigger-based notifications and commands  
→ Trigger-based notifications and commands  
→ Problem update notifications and commands  
→ Internal notifications                                                                                               | Original key (with macros not expanded) of the Nth item in the trigger expression that caused a notification. Supported since 2.0.6. |
| `{ITEM.LASTVALUE<1-9>}`           | Trigger-based notifications and commands  
→ Trigger-based notifications and commands  
→ Problem update notifications and commands  
→ Internal notifications  
→ HTTP agent type item, item prototype and discovery rule fields:  
URL, query fields, request body, headers, proxy, SSL certificate file, SSL key file. | The latest value of the Nth item in the trigger expression that caused a notification. Supported since 2.0.6.  
The latest value of the Nth item in the trigger expression that caused a notification. It will resolve to "UNKNOWN" in the frontend if the latest history value has been collected more than the ZBX_HISTORY_PERIOD time ago (defined in defines.inc.php). Note that since 4.0, when used in the problem name, it will not resolve to the latest item value when viewing problem events, instead it will keep the item value from the time of problem happening. Supported since 1.4.3. It is alias to \{HOST.HOST\}::\{ITEM.KEY\}.last(). \nNote that since 4.0, when used in the problem name, it will not resolve to the latest item value when viewing problem events, instead it will keep the item value from the time of problem happening. Supported since 1.4.3. It is alias to \{HOST.HOST\}::\{ITEM.KEY\}.last(). |
| `{ITEM.LOGL.0ADG<1-9>}`           | Trigger-based notifications and commands  
→ Trigger-based notifications and commands  
→ Problem update notifications and commands  
→ Trigger names and descriptions  
→ Event tags and values  
→ Trigger URLs\(^\text{11}\) | The resolved value for text/log items is truncated to 20 characters by the frontend in the following locations:  
- Operational data;  
- Trigger description;  
- Trigger URLs.  
To resolve to a full value, you may use macro functions. No values are truncated by the server.  
\nCustomizing the macro value is supported for this macro; starting with Zabbix 3.2.0.  
Age of the log item event.                                                                                                    |
| `{ITEM.LOGL.DATE<1-9>}`           | Trigger-based notifications and commands  
→ Problem update notifications and commands  
→ Trigger-based notifications and commands  
→ Problem update notifications and commands | Date of the log item event.                                                                                                                 |
ID of the event in the event log. For Windows event log monitoring only.

Numeric severity of the event in the event log. For Windows event log monitoring only.

Verbal severity of the event in the event log. For Windows event log monitoring only.

Source of the event in the event log. For Windows event log monitoring only.

Time of the log item event.

Name of the Nth item (with macros resolved) in the trigger expression that caused a notification.

Original name (i.e. without macros resolved) of the Nth item in the trigger expression that caused a notification. Supported since 2.0.6.

The latest state of the Nth item in the trigger expression that caused a notification. Possible values: Not supported and Normal. Supported since 2.2.0.

Resolved to either:
1) the historical (at-the-time-of-event) value of the Nth item in the trigger expression, if used in the context of trigger status change, for example, when displaying events or sending notifications.
2) the latest value of the Nth item in the trigger expression, if used without the context of trigger status change, for example, when displaying a list of triggers in a pop-up selection window. In this case works the same as {ITEM.LASTVALUE}
In the first case it will resolve to *UNKNOWN* if the history value has already been deleted or has never been stored.
In the second case, and in the frontend only, it will resolve to *UNKNOWN* if the latest history value has been collected more than the ZBX_HISTORY_PERIOD time ago (defined in defines.inc.php).

The resolved value for text/log items is truncated to 20 characters by the frontend in the following locations:
- Operational data;
- Trigger description;
- Trigger URLs.
To resolve to a full value, you may use macro functions. No values are truncated by the server.

Customizing the macro value is supported for this macro, starting with Zabbix 3.2.0.
Description of the low-level discovery rule which caused a notification. Supported since 2.2.0.

Numeric ID of the low-level discovery rule which caused a notification. Supported since 2.2.0.
<table>
<thead>
<tr>
<th>Macro</th>
<th>Supported in</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>{LLDRULE.KEY}</td>
<td>→ LLD-rule based internal notifications</td>
<td>Key of the low-level discovery rule which caused a notification. Supported since 2.2.0.</td>
</tr>
<tr>
<td>{LLDRULE.KEY.ORIG}</td>
<td>→ LLD-rule based internal notifications</td>
<td>Original key (with macros not expanded) of the low-level discovery rule which caused a notification. Supported since 2.2.0.</td>
</tr>
<tr>
<td>{LLDRULE.NAME}</td>
<td>→ LLD-rule based internal notifications</td>
<td>Name of the low-level discovery rule (with macros resolved) that caused a notification. Supported since 2.2.0.</td>
</tr>
<tr>
<td>{LLDRULE.NAME.ORIG}</td>
<td>→ LLD-rule based internal notifications</td>
<td>Original name (i.e. without macros resolved) of the low-level discovery rule that caused a notification. Supported since 2.2.0.</td>
</tr>
<tr>
<td>{LLDRULE.STATE}</td>
<td>→ LLD-rule based internal notifications</td>
<td>The latest state of the low-level discovery rule. Possible values: Not supported and Normal. Supported since 2.2.0.</td>
</tr>
<tr>
<td>{MAP.ID}</td>
<td>→ Map URLs</td>
<td>Network map ID. Supported since 2.2.0.</td>
</tr>
<tr>
<td>{MAP.NAME}</td>
<td>→ Text field in map shapes</td>
<td>Network map name. Supported since 2.2.0.</td>
</tr>
<tr>
<td>{PROXY.DESCRIPTION&lt;1-9&gt;}</td>
<td>→ Trigger-based notifications and commands</td>
<td>Description of the proxy. Resolves to either: 1) proxy of the Nth item in the trigger expression (in trigger-based notifications). You may use indexed macros here. 2) proxy, which executed discovery (in discovery notifications). Use {PROXY.DESCRIPTION} here, without indexing. 3) proxy to which an active agent registered (in auto-registration notifications). Use {PROXY.DESCRIPTION} here, without indexing. Supported since 2.4.0.</td>
</tr>
<tr>
<td>{PROXY.NAME&lt;1-9&gt;}</td>
<td>→ Trigger-based notifications and commands</td>
<td>Name of the proxy. Resolves to either: 1) proxy of the Nth item in the trigger expression (in trigger-based notifications). You may use indexed macros here. 2) proxy, which executed discovery (in discovery notifications). Use {PROXY.NAME} here, without indexing. 3) proxy to which an active agent registered (in auto-registration notifications). Use {PROXY.NAME} here, without indexing. Supported since 1.8.4.</td>
</tr>
<tr>
<td>{TIME}</td>
<td>→ Trigger-based notifications and commands</td>
<td>Current time in hh:mm:ss.</td>
</tr>
<tr>
<td>{TRIGGER.DESCRIPTION}</td>
<td>→ Trigger-based notifications and commands</td>
<td>Trigger description. Supported since 2.0.4. Starting with 2.2.0, all macros supported in a trigger description will be expanded if {TRIGGER.DESCRIPTION} is used in notification text. {TRIGGER.COMMENT} is deprecated.</td>
</tr>
<tr>
<td>{TRIGGER.EVENTS.ACK}</td>
<td>→ Trigger-based notifications and commands</td>
<td>Number of acknowledged events for a map element in maps, or for the trigger which generated current event in notifications. Supported since 1.8.3.</td>
</tr>
<tr>
<td>{TRIGGER.EVENTS.PROBLEM.ACK}</td>
<td>→ Trigger-based notifications and commands</td>
<td>Number of acknowledged PROBLEM events for all triggers disregarding their state. Supported since 1.8.3.</td>
</tr>
</tbody>
</table>

1. Depending on the trigger type and the notification settings.
<table>
<thead>
<tr>
<th>Macro</th>
<th>Supported in</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>{TRIGGER.EVENTS.PROBLEM.UNACK}</code></td>
<td>→ Problem update notifications and commands</td>
<td>Number of unacknowledged PROBLEM events for all triggers disregarding their state. Supported since 1.8.3.</td>
</tr>
<tr>
<td><code>{TRIGGER.EVENTS.PROBLEM.UNACK}</code></td>
<td>→ Icon labels in maps</td>
<td>Number of unacknowledged events for a map element in maps, or for the trigger which generated current event in notifications. Supported in map element labels since 1.8.3.</td>
</tr>
<tr>
<td><code>{TRIGGER.HOSTGROUP.NAME}</code></td>
<td>→ Problem update notifications and commands</td>
<td>A sorted (by SQL query), comma-space separated list of host groups in which the trigger is defined. Supported since 2.0.6.</td>
</tr>
<tr>
<td><code>{TRIGGER.PROBLEM.EVENTS.PROBLEM.ACK}</code></td>
<td>→ Problem update notifications and commands</td>
<td>Number of acknowledged PROBLEM events for triggers in PROBLEM state. Supported since 1.8.3.</td>
</tr>
<tr>
<td><code>{TRIGGER.PROBLEM.EVENTS.PROBLEM.UNACK}</code></td>
<td>→ Problem update notifications and commands</td>
<td>Number of unacknowledged PROBLEM events for triggers in PROBLEM state. Supported since 1.8.3.</td>
</tr>
<tr>
<td><code>{TRIGGER.EXPRESSION}</code></td>
<td>→ Problem update notifications and commands</td>
<td>Trigger expression. Supported since 1.8.12.</td>
</tr>
<tr>
<td><code>{TRIGGER.EXPRESSION.RECOVERY}</code></td>
<td>→ Problem update notifications and commands</td>
<td>Trigger recovery expression if OK event generation in trigger configuration is set to ‘Recovery expression’; otherwise an empty string is returned. Supported since 3.2.0.</td>
</tr>
<tr>
<td><code>{TRIGGER.ID}</code></td>
<td>→ Problem update notifications and commands</td>
<td>Numeric trigger ID which triggered this action. Supported in trigger URLs since Zabbix 1.8.8, in trigger tag values since 4.0.14.</td>
</tr>
<tr>
<td><code>{TRIGGER.NAME}</code></td>
<td>→ Problem update notifications and commands</td>
<td>Name of the trigger (with macros resolved). Note that since 4.0.0 <code>{EVENT.NAME}</code> can be used in actions to display the triggered event/problem name with macros resolved. Supported since 2.0.6.</td>
</tr>
<tr>
<td><code>{TRIGGER.NAME.ORG}</code></td>
<td>→ Problem update notifications and commands</td>
<td>Original name of the trigger (i.e. without macros resolved).</td>
</tr>
<tr>
<td><code>{TRIGGER.NSEVERITY}</code></td>
<td>→ Problem update notifications and commands</td>
<td>Numerical trigger severity. Possible values: 0 - Not classified, 1 - Information, 2 - Warning, 3 - Average, 4 - High, 5 - Disaster. Supported starting from Zabbix 1.6.2.</td>
</tr>
<tr>
<td><code>{TRIGGER.SEVERITY}</code></td>
<td>→ Problem update notifications and commands</td>
<td>Trigger severity name. Can be defined in Administration → General → Trigger severities.</td>
</tr>
<tr>
<td><code>{TRIGGER.STATE}</code></td>
<td>→ Problem update notifications and commands</td>
<td>The latest state of the trigger. Possible values: Unknown and Normal. Supported since 2.2.0.</td>
</tr>
<tr>
<td><code>{TRIGGER.STATUS}</code></td>
<td>→ Problem update notifications and commands</td>
<td>Current trigger value. Can be either PROBLEM or OK. <code>{STATUS}</code> is deprecated.</td>
</tr>
<tr>
<td><code>{TRIGGER.TEMPLATE.NAME}</code></td>
<td>→ Problem update notifications and commands</td>
<td>A sorted (by SQL query), comma-space separated list of templates in which the trigger is defined, or <em>UNKNOWN</em> if the trigger is defined in a host. Supported since 2.0.6.</td>
</tr>
<tr>
<td><code>{TRIGGER.URL}</code></td>
<td>→ Problem update notifications and commands</td>
<td>Trigger URL.</td>
</tr>
<tr>
<td><code>{TRIGGER.VALUE}</code></td>
<td>→ Problem update notifications and commands</td>
<td>Current trigger numeric value: 0 - trigger is in OK state, 1 - trigger is in PROBLEM state.</td>
</tr>
<tr>
<td>Macro</td>
<td>Supported in</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>{TRIGGERS.UNACK}</td>
<td>→ Icon labels in maps$^1$</td>
<td>Number of unacknowledged triggers for a map element, disregarding trigger state. A trigger is considered to be unacknowledged if at least one of its PROBLEM events is unacknowledged.</td>
</tr>
<tr>
<td>{TRIGGERS.PROBLEM.UNACK}</td>
<td>→ Icon labels in maps$^1$</td>
<td>Number of unacknowledged PROBLEM triggers for a map element. A trigger is considered to be unacknowledged if at least one of its PROBLEM events is unacknowledged. Supported since 1.8.3.</td>
</tr>
<tr>
<td>{TRIGGERS.ACK}</td>
<td>→ Icon labels in maps$^1$</td>
<td>Number of acknowledged triggers for a map element, disregarding trigger state. A trigger is considered to be acknowledged if all of it’s PROBLEM events are acknowledged. Supported since 1.8.3.</td>
</tr>
<tr>
<td>{TRIGGERS.PROBLEM.ACK}</td>
<td>→ Icon labels in maps$^1$</td>
<td>Number of acknowledged PROBLEM triggers for a map element. A trigger is considered to be acknowledged if all of it’s PROBLEM events are acknowledged. Supported since 1.8.3.</td>
</tr>
<tr>
<td>{USER.FULLNAME}</td>
<td>→ Problem update notifications and commands</td>
<td>Name and surname of the user who added event acknowledgment. Supported since 1.8.3.</td>
</tr>
<tr>
<td>{host:key.func(param)}</td>
<td>→ Trigger-based notifications and commands</td>
<td>Simple macros, as used in building trigger expressions. Supported for shape labels in maps since 3.4.2.</td>
</tr>
<tr>
<td></td>
<td>→ Problem update notifications and commands</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Icon/shape labels in maps$^{1,4}$</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Link labels in maps$^4$</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Graph names$^7$</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ Trigger expressions$^9$</td>
<td></td>
</tr>
<tr>
<td>{$MACRO}</td>
<td>→ See: User macros supported by location</td>
<td>User-definable macros.</td>
</tr>
<tr>
<td>{#MACRO}</td>
<td>→ See: Low-level discovery macros</td>
<td>Low-level discovery macros. Supported since 2.0.0.</td>
</tr>
<tr>
<td>$1...$9</td>
<td>→ Trigger names</td>
<td></td>
</tr>
<tr>
<td></td>
<td>→ User parameter commands</td>
<td></td>
</tr>
</tbody>
</table>

Footnotes

$^1$ Macros for map labels are supported since 1.8.

$^2$ The {HOST.*} macros supported in item key parameters will resolve to the interface that is selected for the item. When used in items without interfaces they will resolve to either the Zabbix agent, SNMP, JMX or IPMI interface of the host in this order of priority.

$^3$ In remote commands, global scripts, interface IP/DNS fields and web scenarios the macro will resolve to the main agent interface, however, if it is not present, the main SNMP interface will be used. If SNMP is also not present, the main JMX interface will be used. If JMX is not present either, the main IPMI interface will be used.

$^4$ Only the avg, last, max and min functions, with seconds as parameter are supported in this macro in map labels.

$^5$ Supported since 2.0.3.

$^6$ Supported since Zabbix 2.2.0, {HOST.*} macros are supported in web scenario Variables, Headers, SSL certificate file and SSL key field fields and in scenario step URL, Post, Headers and Required string fields. Macros {HOST.*} in web scenario Name and web scenario step Name are not supported since Zabbix 4.0.27.

$^7$ Supported since Zabbix 2.2.0. Only the avg, last, max and min functions, with seconds as parameter are supported within this macro in graph names. The {HOST.HOST<1-9>} macro can be used as host within the macro. For example:

```
* {Cisco switch:ifAlias[#SNMPINDEX].last()}
* {{HOST.HOST}:ifAlias[#SNMPINDEX].last()}
```

$^8$ Supported since 2.4.0.
9 While supported to build trigger expressions, simple macros may not be used inside each other.

10 Supported since 3.0.0.

11 Supported since 4.0.0.

12 Supported in "Allowed hosts" field since 4.0.2.

Indexed macros

The indexed macro syntax of \{MACRO\<1-9>\} works only in the context of trigger expressions. It can be used to reference hosts in the order in which they appear in the expression. Macros like \{HOST.IP1\}, \{HOST.IP2\}, \{HOST.IP3\} will resolve to the IP of the first, second and third host in the trigger expression (providing the trigger expression contains those hosts).

Additionally the \{HOST.HOST<1-9>\} macro is also supported within the \{host:key.func(param)\} macro in graph names. For example, \{\{HOST.HOST2\}:key.func()\} in the graph name will refer to the host of the second item in the graph.

Warning:
Indexed macros will not resolve in any other context, except the two cases mentioned here. For other contexts, use macros without index (i.e., \{HOST.HOST\}, \{HOST.IP\}, etc) instead.

2 User macros supported by location

Overview

This section contains a list of locations, where user-definable macros are supported.

Note:
Only global-level user macros are supported for Actions, Network discovery, Proxies and all locations listed under Other locations section of this page. In the mentioned locations, host-level and template-level macros will not be resolved.

Actions

In actions, user macros can be used in the following fields:

<table>
<thead>
<tr>
<th>Location</th>
<th>Multiple macros/mix with text</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trigger-based notifications and commands</td>
<td>yes</td>
</tr>
<tr>
<td>Trigger-based internal notifications</td>
<td>yes</td>
</tr>
<tr>
<td>Problem update notifications</td>
<td>yes</td>
</tr>
<tr>
<td>Time period condition</td>
<td>no</td>
</tr>
<tr>
<td>Operations</td>
<td></td>
</tr>
<tr>
<td>Default operation step duration</td>
<td>no</td>
</tr>
<tr>
<td>Step duration</td>
<td>no</td>
</tr>
</tbody>
</table>

Hosts

In a host configuration, user macros can be used in the following fields:

<table>
<thead>
<tr>
<th>Location</th>
<th>Multiple macros/mix with text</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface IP/DNS</td>
<td>DNS only</td>
</tr>
<tr>
<td>Interface port</td>
<td>no</td>
</tr>
<tr>
<td>SNMP v1, v2</td>
<td></td>
</tr>
<tr>
<td>SNMP v3</td>
<td>Interface community yes</td>
</tr>
<tr>
<td></td>
<td>Interface context name yes</td>
</tr>
<tr>
<td></td>
<td>Security name yes</td>
</tr>
<tr>
<td></td>
<td>Authentication passphrase yes</td>
</tr>
<tr>
<td></td>
<td>Privacy passphrase yes</td>
</tr>
<tr>
<td>IPMI</td>
<td>Username yes</td>
</tr>
<tr>
<td></td>
<td>Password yes</td>
</tr>
<tr>
<td>//Tags //</td>
<td>Tag names yes</td>
</tr>
</tbody>
</table>
Items / item prototypes

In an item or an item prototype configuration, user macros can be used in the following fields:

<table>
<thead>
<tr>
<th>Location</th>
<th>Multiple macros/mix with text¹</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name (deprecated)</td>
<td>yes</td>
</tr>
<tr>
<td>Item key parameters</td>
<td>yes</td>
</tr>
<tr>
<td>Update interval</td>
<td>no</td>
</tr>
<tr>
<td>Custom intervals</td>
<td>no</td>
</tr>
<tr>
<td>History storage period</td>
<td>no</td>
</tr>
<tr>
<td>Trend storage period</td>
<td>no</td>
</tr>
<tr>
<td>Formula</td>
<td>yes</td>
</tr>
<tr>
<td>Username</td>
<td>yes</td>
</tr>
<tr>
<td>Password</td>
<td>yes</td>
</tr>
<tr>
<td>SQL query</td>
<td>yes</td>
</tr>
<tr>
<td>URL</td>
<td>yes</td>
</tr>
<tr>
<td>Query fields</td>
<td>yes</td>
</tr>
<tr>
<td>Timeout</td>
<td>no</td>
</tr>
<tr>
<td>Request body</td>
<td>yes</td>
</tr>
<tr>
<td>Headers (names and values)</td>
<td>yes</td>
</tr>
<tr>
<td>Required status codes</td>
<td>yes</td>
</tr>
<tr>
<td>HTTP proxy</td>
<td>yes</td>
</tr>
<tr>
<td>HTTP authentication username</td>
<td>yes</td>
</tr>
<tr>
<td>HTTP authentication password</td>
<td>yes</td>
</tr>
<tr>
<td>SSI certificate file</td>
<td>yes</td>
</tr>
<tr>
<td>SSI key file</td>
<td>yes</td>
</tr>
<tr>
<td>SSI key password</td>
<td>yes</td>
</tr>
<tr>
<td>Allowed hosts</td>
<td>yes</td>
</tr>
<tr>
<td>JMX endpoint</td>
<td>yes</td>
</tr>
<tr>
<td>SNMP OID</td>
<td>yes</td>
</tr>
<tr>
<td>Username</td>
<td>yes</td>
</tr>
<tr>
<td>Public key file</td>
<td>yes</td>
</tr>
<tr>
<td>Private key file</td>
<td>yes</td>
</tr>
<tr>
<td>Password</td>
<td>yes</td>
</tr>
<tr>
<td>Script</td>
<td>yes</td>
</tr>
<tr>
<td>Username</td>
<td>yes</td>
</tr>
<tr>
<td>Password</td>
<td>yes</td>
</tr>
<tr>
<td>Script</td>
<td>yes</td>
</tr>
<tr>
<td>Allowed hosts</td>
<td>yes</td>
</tr>
<tr>
<td>Step parameters</td>
<td>yes</td>
</tr>
</tbody>
</table>

Low-level discovery

In a low-level discovery rule, user macros can be used in the following fields:

<table>
<thead>
<tr>
<th>Location</th>
<th>Multiple macros/mix with text¹</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name (deprecated)</td>
<td>yes</td>
</tr>
<tr>
<td>Key parameters</td>
<td>yes</td>
</tr>
<tr>
<td>Location</td>
<td>Multiple macros/mix with text</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Update interval</td>
<td>no</td>
</tr>
<tr>
<td>Custom interval</td>
<td>no</td>
</tr>
<tr>
<td>Keep lost resources period</td>
<td>no</td>
</tr>
<tr>
<td>SNMP agent</td>
<td>SNMP OID: yes</td>
</tr>
<tr>
<td>SSH agent</td>
<td>Username: yes</td>
</tr>
<tr>
<td></td>
<td>Public key file: yes</td>
</tr>
<tr>
<td></td>
<td>Private key file: yes</td>
</tr>
<tr>
<td></td>
<td>Password: yes</td>
</tr>
<tr>
<td></td>
<td>Script: yes</td>
</tr>
<tr>
<td>TELNET agent</td>
<td>Username: yes</td>
</tr>
<tr>
<td></td>
<td>Password: yes</td>
</tr>
<tr>
<td></td>
<td>Script: yes</td>
</tr>
<tr>
<td>Zabbix trapper</td>
<td>Allowed hosts: yes</td>
</tr>
<tr>
<td>Database monitor</td>
<td>Additional parameters: yes</td>
</tr>
<tr>
<td>JMX agent</td>
<td>JMX endpoint: yes</td>
</tr>
<tr>
<td>HTTP agent</td>
<td>URL: yes</td>
</tr>
<tr>
<td></td>
<td>Query fields: yes</td>
</tr>
<tr>
<td></td>
<td>Timeout: no</td>
</tr>
<tr>
<td></td>
<td>Request body: yes</td>
</tr>
<tr>
<td></td>
<td>Headers (names and values):</td>
</tr>
<tr>
<td></td>
<td>Required status codes:</td>
</tr>
<tr>
<td></td>
<td>HTTP authentication username:</td>
</tr>
<tr>
<td></td>
<td>HTTP authentication password:</td>
</tr>
<tr>
<td>//Filters //</td>
<td>Regular expression: yes</td>
</tr>
</tbody>
</table>

Network discovery

In a network discovery rule, user macros can be used in the following fields:

<table>
<thead>
<tr>
<th>Location</th>
<th>Multiple macros/mix with text</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update interval</td>
<td>no</td>
</tr>
<tr>
<td>SNMP v1, v2</td>
<td>SNMP community: yes</td>
</tr>
<tr>
<td></td>
<td>SNMP OID: yes</td>
</tr>
<tr>
<td>SNMP v3</td>
<td>Context name: yes</td>
</tr>
<tr>
<td></td>
<td>Security name: yes</td>
</tr>
<tr>
<td></td>
<td>Authentication passphrase:</td>
</tr>
<tr>
<td></td>
<td>Privacy passphrase: yes</td>
</tr>
<tr>
<td></td>
<td>SNMP OID: yes</td>
</tr>
</tbody>
</table>

Proxies

In a proxy configuration, user macros can be used in the following field:

<table>
<thead>
<tr>
<th>Location</th>
<th>Multiple macros/mix with text</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface port (for passive proxy)</td>
<td>no</td>
</tr>
</tbody>
</table>

Templates

In a template configuration, user macros can be used in the following fields:
Triggers

In a trigger configuration, user macros can be used in the following fields:

<table>
<thead>
<tr>
<th>Location</th>
<th>Multiple macros/mix with text¹</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>yes</td>
</tr>
<tr>
<td>Operational data</td>
<td>yes</td>
</tr>
<tr>
<td>Expression</td>
<td>yes</td>
</tr>
<tr>
<td>(only in constants and function parameters; secret macros are not supported)</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>yes</td>
</tr>
<tr>
<td>URL</td>
<td>yes</td>
</tr>
<tr>
<td>Tag for matching</td>
<td>yes</td>
</tr>
</tbody>
</table>

//Tags //

| Tag names     | yes |
| Tag values    | yes |

Web scenario

In a web scenario configuration, user macros can be used in the following fields:

<table>
<thead>
<tr>
<th>Location</th>
<th>Multiple macros/mix with text¹</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>yes</td>
</tr>
<tr>
<td>Update interval</td>
<td>no</td>
</tr>
<tr>
<td>Agent</td>
<td>yes</td>
</tr>
<tr>
<td>HTTP proxy</td>
<td>yes</td>
</tr>
<tr>
<td>Variables (values only)</td>
<td>yes</td>
</tr>
<tr>
<td>Headers (names and values)</td>
<td>yes</td>
</tr>
</tbody>
</table>

//Steps //

| Name                        | yes |
| URL                         | yes |
| Variables (values only)     | yes |
| Headers (names and values)  | yes |
| Timeout                     | no  |
| Required string             | yes |
| Required status codes       | no  |

//Authentication //

| User                         | yes |
| Password                     | yes |
| SSL certificate              | yes |
| SSL key file                 | yes |
| SSL key password             | yes |
Other locations

In addition to the locations listed here, user macros can be used in the following fields:

<table>
<thead>
<tr>
<th>Location</th>
<th>Multiple macros/mix with text</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global scripts (including confirmation text)</td>
<td>yes</td>
</tr>
<tr>
<td>Monitoring → Screens</td>
<td>URL field of dynamic URL screen element yes</td>
</tr>
<tr>
<td>Administration → Users → Media</td>
<td>When active no</td>
</tr>
<tr>
<td>Administration → General → Working time</td>
<td>Working time no</td>
</tr>
</tbody>
</table>

For a complete list of all macros supported in Zabbix, see supported macros.

Footnotes

1 If multiple macros in a field or macros mixed with text are not supported for the location, a single macro has to fill the whole field.

8 Unit symbols

Overview

Having to use some large numbers, for example ‘86400’ to represent the number of seconds in one day, is both difficult and error-prone. This is why you can use some appropriate unit symbols (or suffixes) to simplify Zabbix trigger expressions and item keys.

Instead of ‘86400’ for the number of seconds you can simply enter ‘1d’. Suffixes function as multipliers.

Time suffixes

For time you can use:

- **s** - seconds (when used, works the same as the raw value)
- **m** - minutes
- **h** - hours
- **d** - days
- **w** - weeks

Time suffixes support only integer numbers (so ‘1h’ is supported, ‘1.5h’ or ‘1.5h’ are not; use ‘90m’ instead).

Time suffixes are supported in:

- trigger expression constants and function parameters
- constants of calculated item formulas (see also known issues for 4.0.0-4.0.3)
- parameters of the \texttt{zabbix\{queue,\langle from\rangle,\langle to\rangle\}} internal item
- last parameter of aggregate checks
- item configuration (‘Update interval’, ‘Custom intervals’, ‘History storage period’ and ‘Trend storage period’ fields)
- item prototype configuration (‘Update interval’, ‘Custom intervals’, ‘History storage period’ and ‘Trend storage period’ fields)
- low-level discovery rule configuration (‘Update interval’, ‘Custom intervals’, ‘Keep lost resources’ fields)
- network discovery configuration (‘Update interval’ field)
- web scenario configuration (‘Update interval’, ‘Timeout’ fields)
- action operation configuration (‘Default operation step duration’, ‘Step duration’ fields)
- slide show configuration (‘Default delay’ field)
- user profile settings (‘Auto-login’, ‘Refresh’, ‘Message timeout’ fields)
- graph widget of Monitoring → Dashboard (‘Time shift’ field)
- Administration → General → Housekeeping (storage period fields)
- Administration → General → Trigger displaying options (‘Display OK triggers for’, ‘On status change triggers blink for’ fields)
- Administration → General → Other (‘Refresh unsupported items’ field)

Memory suffixes

Memory size suffixes are supported in:

- trigger expression constants and function parameters
- constants of calculated item formulas
For memory size you can use:

- K - kilobyte
- M - megabyte
- G - gigabyte
- T - terabyte

Other uses

Unit symbols are also used for a human-readable representation of data in the frontend.

In both Zabbix server and frontend these symbols are supported:

- K - kilo
- M - mega
- G - giga
- T - tera

When item values in B, Bps are displayed in the frontend, base 2 is applied (1K = 1024). Otherwise a base of 10 is used (1K = 1000).

Additionally the frontend also supports the display of:

- P - peta
- E - exa
- Z - zetta
- Y - yotta

Usage examples

By using some appropriate suffixes you can write trigger expressions that are easier to understand and maintain, for example these expressions:

{host:zabbix[proxy,zabbix_proxy,lastaccess]}>120
{host:system.uptime[]}.last()<86400
{host:system.cpu.load.avg(600)}<10
{host:vm.memory.size[available].last()}<20971520

could be changed to:

{host:zabbix[proxy,zabbix_proxy,lastaccess]}>2m
{host:system.uptime.last()}<1d
{host:system.cpu.load.avg(10m)}<10
{host:vm.memory.size[available].last()}<20M

9 Setting time periods

Overview

To set a time period, the following format has to be used:

d-d, hh:mm-hh:mm

where the symbols stand for the following:

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>d</td>
<td>Day of the week: 1 - Monday, 2 - Tuesday, ..., 7 - Sunday</td>
</tr>
<tr>
<td>hh</td>
<td>Hours: 00-24</td>
</tr>
<tr>
<td>mm</td>
<td>Minutes: 00-59</td>
</tr>
</tbody>
</table>

You can specify more than one time period using a semicolon (;) separator:

d-d, hh:mm-hh:mm; d-d, hh:mm-hh:mm...

Leaving the time period empty equals 01-07, 00:00-24:00, which is the default value.
Attention: The upper limit of a time period is not included. Thus, if you specify 09:00-18:00 the last second included in the time period is 17:59:59. This is true starting from version 1.8.7, for everything, while Working time has always worked this way.

Examples

Working hours. Monday - Friday from 9:00 till 18:00:
1-5, 09:00-18:00

Working hours plus weekend. Monday - Friday from 9:00 till 18:00 and Saturday, Sunday from 10:00 till 16:00:
1-5, 09:00-18:00; 6-7, 10:00-16:00

10 Command execution

Zabbix uses common functionality for external checks, user parameters, system.run items, custom alert scripts, remote commands and user scripts.

Execution steps

The command/script is executed similarly on both Unix and Windows platforms:

1. Zabbix (the parent process) creates a pipe for communication
2. Zabbix sets the pipe as the output for the to-be-created child process
3. Zabbix creates the child process (runs the command/script)
4. A new process group (in Unix) or a job (in Windows) is created for the child process
5. Zabbix reads from the pipe until timeout occurs or no one is writing to the other end (ALL handles/file descriptors have been closed). Note that the child process can create more processes and exit before they exit or close the handle/file descriptor.
6. If the timeout has not been reached, Zabbix waits until the initial child process exits or timeout occurs
7. If the initial child process exited and the timeout has not been reached, Zabbix checks exit code of the initial child process and compares it to 0 (non-zero value is considered as execution failure, only for custom alert scripts, remote commands and user scripts executed on Zabbix server and Zabbix proxy)
8. At this point it is assumed that everything is done and the whole process tree (i.e. the process group or the job) is terminated

Attention: Zabbix assumes that a command/script has done processing when the initial child process has exited AND no other process is still keeping the output handle/file descriptor open. When processing is done, ALL created processes are terminated.

All double quotes and backslashes in the command are escaped with backslashes and the command is enclosed in double quotes.

Exit code checking

Exit code are checked with the following conditions:

- Only for custom alert scripts, remote commands and user scripts executed on Zabbix server and Zabbix proxy.
- Any exit code that is different from 0 is considered as execution failure.
- Contents of standard error and standard output for failed executions are collected and available in frontend (where execution result is displayed).
- Additional log entry is created for remote commands on Zabbix server to save script execution output and can be enabled using LogRemoteCommands agent parameter.

Possible frontend messages and log entries for failed commands/scripts:

- Contents of standard error and standard output for failed executions (if any).
- "Process exited with code: N." (for empty output, and exit code not equal to 0).
- "Process killed by signal: N." (for process terminated by a signal, on Linux only).
- "Process terminated unexpectedly." (for process terminated for unknown reasons).

Read more about:

- External checks
- User parameters
- system.run items
- Custom alert scripts
11 Version compatibility

Supported agents

Zabbix agents starting with version 1.4 are compatible with Zabbix 4.0. However, you may need to review the configuration of older agents as some parameters have changed, for example, parameters related to logging for versions before 3.0.

To take full advantage of new and improved items, improved performance and reduced memory usage, use the latest 4.0 agent.

Note that Zabbix agent newer than 4.0 cannot be used with Zabbix server 4.0.

Supported Zabbix proxies

Zabbix 4.0.x server can only work with Zabbix 4.0.x proxies. Zabbix 4.0.x proxies can only work with Zabbix 4.0.x server.

Attention:
It is known to be possible to start an upgraded server and have older and unupgraded proxies report data to a newer server (the proxies can’t refresh their configuration though). This approach, however, is not recommended and not supported by Zabbix and choosing it is entirely at your own risk. For more information, see the upgrade procedure.

Warnings about using incompatible Zabbix daemon versions are logged since Zabbix 4.0.8.

Supported XML files

XML files, exported with 1.8, 2.0, 2.2, 2.4, 3.0, 3.2 and 3.4 are supported for import in Zabbix 4.0.

Attention:
In Zabbix 1.8 XML export format, trigger dependencies are stored by name only. If there are several triggers with the same name (for example, having different severities and expressions) that have a dependency defined between them, it is not possible to import them. Such dependencies must be manually removed from the XML file and re-added after import.

12 Database error handling

If Zabbix detects that the backend database is not accessible, it will send a notification message and continue the attempts to connect to the database. For some database engines, specific error codes are recognized.

MySQL

- 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

13 Zabbix sender dynamic link library for Windows

In a Windows environment applications can send data to Zabbix server-proxy directly by using the Zabbix sender dynamic link library (zabbix_sender.dll) instead of having to launch an external process (zabbix_sender.exe).

The dynamic link library with the development files is located in bin\winXX\dev folders. To use it, include the zabbix_sender.h header file and link with the zabbix_sender.lib library. An example file with Zabbix sender API usage can be found in build\win32\examples\zabbix_sender folder.
The following functionality is provided by the Zabbix sender dynamic link library:

```c
int zabbix_sender_send_values(const char *address, unsigned short port, const char *source, const zabbix_sender_value_t *values, int count, char **result);
```

The following data structures are used by the Zabbix sender dynamic link library:

```c
typedef struct {
    /* host name, must match the name of target host in Zabbix */
    char *host;
    /* the item key */
    char *key;
    /* the item value */
    char *value;
} zabbix_sender_value_t;

typedef struct {
    /* number of total values processed */
    int total;
    /* number of failed values */
    int failed;
    /* time in seconds the server spent processing the sent values */
    double time_spent;
} zabbix_sender_info_t;
```

14 Issues with SELinux

Socket-based inter-process communication has been added since Zabbix 3.4. On systems where SELinux is enabled it may be required to add SELinux rules to allow Zabbix create/use UNIX domain sockets in the SocketDir directory. Currently socket files are used by server (alerter, preprocessing, IPMI) and proxy (IPMI). Socket files are persistent, meaning are present while the process is running.

15 Other issues

Login and systemd

We recommend creating a zabbix user as system user, that is, without ability to log in. Some users ignore this recommendation and use the same account to log in (e.g. using SSH) to host running Zabbix. This might crash Zabbix daemon on log out. In this case you will get something like the following in Zabbix server log:

```
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
```

and in Zabbix agent log:

```
zabbix_agentd [27796]: [file: 'log.c', line: 238] lock failed: [22] Invalid argument
```

This happens because of default systemd setting RemoveIPC=yes configured in `/etc/systemd/logind.conf`. When you log out of the system the semaphores created by Zabbix previously are removed which causes the crash.

A quote from systemd documentation:

RemoveIPC=

Controls whether System V and POSIX IPC objects belonging to the user shall be removed when the user fully logs out. Takes a boolean argument. If enabled, the user may not consume IPC resources.
after the last of the user's sessions terminated. This covers System V semaphores, shared memory and message queues, as well as POSIX shared memory and message queues. Note that IPC objects of the root user and other system users are excluded from the effect of this setting. Defaults to "yes".

There are 2 solutions to this problem:

1. (recommended) Stop using zabbix account for anything else than Zabbix processes, create a dedicated account for other things.
2. (not recommended) Set RemoveIPC=no in /etc/systemd/logind.conf and reboot the system. Note that RemoveIPC is a system-wide parameter, changing it will affect the whole system.

Using Zabbix frontend behind proxy

If Zabbix frontend runs behind proxy server, the cookie path in the proxy configuration file needs to be rewritten in order to match the reverse-proxied path. See examples below. If the cookie path is not rewritten, users may experience authorization issues, when trying to login to Zabbix frontend.

Example configuration for nginx

```plaintext
# ...
location / {
    # ...
    proxy_cookie_path /zabbix /;
    proxy_pass http://192.168.0.94/zabbix/;
    # ...
```

Example configuration for Apache

```plaintext
# ...
ProxyPass "/" http://host/zabbix/
ProxyPassReverse "/" http://host/zabbix/
ProxyPassReverseCookiePath /zabbix /
ProxyPassReverseCookieDomain host zabbix.example.com
# ...
```

Zabbix manpages

These are Zabbix manpages for Zabbix processes.

zabbix_agentd

Section: Maintenance Commands (8)
Updated: 2018-10-11
Index Return to Main Contents

NAME

zabbix_agentd - Zabbix agent daemon

SYNOPSIS

zabbix_agentd [-c config-file]
zabbix_agentd [-c config-file] -p
zabbix_agentd [-c config-file] -t item-key
zabbix_agentd [-c config-file] -R runtime-option
zabbix_agentd -h
zabbix_agentd -V

DESCRIPTION

zabbix_agentd is a daemon for monitoring of various server parameters.
OPTIONS

-\(c\), \(--\text{config}\) config-file
Use the alternate config-file instead of the default one.

-\(f\), \(--\text{foreground}\)
Run Zabbix agent in foreground.

-\(R\), \(--\text{runtime-control}\) runtime-option
Perform administrative functions according to runtime-option.

Runtime control options

\text{log\_level\_increase}[\text{=target}]
Increase log level, affects all processes if target is not specified

\text{log\_level\_decrease}[\text{=target}]
Decrease log level, affects all processes if target is not specified

Log level control targets

\text{process-type}
All processes of specified type (active checks, collector, listener)

\text{process-type,N}
Process type and number (e.g., listener,3)

\text{pid}
Process identifier, up to 65535. For larger values specify target as “process-type,N”

\(-p\), \(--\text{print}\)
Print known items and exit. For each item either generic defaults are used, or specific defaults for testing are supplied. These defaults are listed in square brackets as item key parameters. Returned values are enclosed in square brackets and prefixed with the type of the returned value, separated by a pipe character. For user parameters type is always \text{t}, as the agent can not determine all possible return values. Items, displayed as working, are not guaranteed to work from the Zabbix server or zabbix_get when querying a running agent daemon as permissions or environment may be different. Returned value types are:

\text{d}
Number with a decimal part.

\text{m}
Not supported. This could be caused by querying an item that only works in the active mode like a log monitoring item or an item that requires multiple collected values. Permission issues or incorrect user parameters could also result in the not supported state.

\text{s}
Text. Maximum length not limited.

\text{t}
Text. Same as \text{s}.

\text{u}
Unsigned integer.

\(-t\), \(--\text{test}\) item-key
Test single item and exit. See \(--\text{print}\) for output description.

\(-h\), \(--\text{help}\)
Display this help and exit.

\(-V\), \(--\text{version}\)
Output version information and exit.

FILES

/usr/local/etc/zabbix_agentd.conf
Default location of Zabbix agent configuration file (if not modified during compile time).
NAME
zabbix_get - Zabbix get utility

SYNOPSIS
zabbix_get -s host-name-or-IP [-p port-number] [-I IP-address] -k item-key
zabbix_get -h
zabbix_get -V

DESCRIPTION
zabbix_get is a command line utility for getting data from Zabbix agent.

OPTIONS
- -s, --host host-name-or-IP
  Specify host name or IP address of a host.
- -p, --port port-number
  Specify port number of agent running on the host. Default is 10050.
-l --source-address IP-address
Specify source IP address.

-k, --key item-key
Specify key of item to retrieve value for.

--tls-connect value
How to connect to agent. Values:

  unencrypted
  connect without encryption (default)

  psk
  connect using TLS and a pre-shared key

  cert
  connect using TLS and a certificate

  --tls-ca-file CA-file
  Full pathname of a file containing the top-level CA(s) certificates for peer certificate verification.

  --tls-crl-file CRL-file
  Full pathname of a file containing revoked certificates.

  --tls-agent-cert-issuer cert-issuer
  Allowed agent certificate issuer.

  --tls-agent-cert-subject cert-subject
  Allowed agent certificate subject.

  --tls-cert-file cert-file
  Full pathname of a file containing the certificate or certificate chain.

  --tls-key-file key-file
  Full pathname of a file containing the private key.

  --tls-psk-identity PSK-identity
  PSK-identity string.

  --tls-psk-file PSK-file
  Full pathname of a file containing the pre-shared key.

  --tls-cipher13 cipher-string
  Cipher string for OpenSSL 1.1.1 or newer for TLS 1.3. Override the default ciphersuite selection criteria. This option is not available if OpenSSL version is less than 1.1.1.

  --tls-cipher cipher-string
  GnuTLS priority string (for TLS 1.2 and up) or OpenSSL cipher string (only for TLS 1.2). Override the default ciphersuite selection criteria.

-h, --help
Display this help and exit.

-V, --version
Output version information and exit.

EXAMPLES

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
NAME
zabbix_proxy - Zabbix proxy daemon

SYNOPSIS
zabbix_proxy [-c config-file]
zabbix_proxy [-c config-file] -R runtime-option
zabbix_proxy -h
zabbix_proxy -V

DESCRIPTION
zabbix_proxy is a daemon that collects monitoring data from devices and sends it to Zabbix server.

OPTIONS
-c, --config config-file
Use the alternate config-file instead of the default one.

-f, --foreground
Run Zabbix proxy in foreground.

-R, --runtime-control runtime-option
Perform administrative functions according to runtime-option.
Runtime control options

**config_cache_reload**
Reload configuration cache. Ignored if cache is being currently loaded. Active Zabbix proxy will connect to the Zabbix server and request configuration data. Default configuration file (unless `-c` option is specified) will be used to find PID file and signal will be sent to process, listed in PID file.

**housekeeper_execute**
Execute the housekeeper. Ignored if housekeeper is being currently executed.

**log_level_increase[=target]**
Increase log level, affects all processes if target is not specified

**log_level_decrease[=target]**
Decrease log level, affects all processes if target is not specified

Log level control targets

**process-type**
All processes of specified type (configuration syncer, data sender, discoverer, heartbeat sender, history syncer, housekeeper, http poller, icmp pinger, ipmi manager, ipmi poller, java poller, poller, self-monitoring, snmp trapper, task manager, trapper, unreachable poller, vmware collector)

**process-type,N**
Process type and number (e.g., poller,3)

**pid**
Process identifier, up to 65535. For larger values specify target as "process-type,N"

**-h, --help**
Display this help and exit.

**-V, --version**
Output version information and exit.

**FILES**

/usr/local/etc/zabbix_proxy.conf
Default location of Zabbix proxy configuration file (if not modified during compile time).

**SEE ALSO**

zabbix_agentd(8), zabbix_get(1), zabbix_sender(1), zabbix_server(8)

**AUTHOR**

Alexei Vladishev <alex@zabbix.com>

Index

NAME
SYNOPSIS
DESCRIPTION
OPTIONS
FILES
SEE ALSO
This document was created by man2html, using the manual pages.
Time: 15:28:13 GMT, October 18, 2018

zabbix_sender

Section: User Commands (1)
Updated: 2020-02-29

NAME

zabbix_sender - Zabbix sender utility

SYNOPSIS

zabbix_sender [-v] [-z server [-p port] [-I IP-address] -s host -k key -o value
zabbix_sender [-v] [-c config-file [-z server] [-p port] [-L IP-address] [-s host] -k key -o value
zabbix_sender -h
zabbix_sender -V

DESCRIPTION

zabbix_sender is a command line utility for sending monitoring data to Zabbix server or proxy. On the Zabbix server an item of type Zabbix trapper should be created with corresponding key. Note that incoming values will only be accepted from hosts specified in Allowed hosts field for this item.

OPTIONS

-c, --config config-file
Use config-file. zabbix_sender reads server details from the agentd configuration file. By default zabbix_sender does not read any configuration file. Only parameters Hostname, ServerActive, SourceIP, TLSSocket, TLSCertificate, TLSCRFile, TLSServerCertIssuer, TLSServerCertSubject, TLSCertificate, TLSKeyFile, TLSPSKIdentity and TLSPSKFile are supported. First entry from the ServerActive parameter is used.
-z, --zabbix-server server
Hostname or IP address of Zabbix server. If a host is monitored by a proxy, proxy hostname or IP address should be used instead. When used together with --config, overrides the entries of ServerActive parameter specified in agentd configuration file.

-p, --port port
Specify port number of Zabbix server trapper running on the server. Default is 10051. When used together with --config, overrides the port entries of ServerActive parameter specified in agentd configuration file.

-I, --source-address IP-address
Specify source IP address. When used together with --config, overrides SourceIP parameter specified in agentd configuration file.

-s, --host host
Specify host name the item belongs to (as registered in Zabbix front end). Host IP address and DNS name will not work. When used together with --config, overrides Hostname parameter specified in agentd configuration file.

-k, --key key
Specify item key to send value to.

-o, --value value
Specify item value.

-l, --input-file input-file
Load values from input file. Specify - as <input-file> to read values from standard input. Each line of file contains whitespace delimited: <hostname> <key> <value>. Each value must be specified on its own line. Each line must contain 3 whitespace delimited entries: <hostname> <key> <value>, where "hostname" is the name of monitored host as registered in Zabbix frontend, "key" is target item key and "value" - the value to send. Specify - as <hostname> to use hostname from agent configuration file or from --host argument.

An example of a line of an input file:
"Linux DB3" db.connections 43

The value type must be correctly set in item configuration of Zabbix frontend. Zabbix sender will send up to 250 values in one connection. Size limit for sending values from an input file depends on the size described in Zabbix communication protocol. Contents of the input file must be in the UTF-8 encoding. All values from the input file are sent in a sequential order top-down. Entries must be formatted using the following rules:

- Quoted and non-quoted entries are supported.
- Double-quote is the quoting character.
- Entries with whitespace must be quoted.
- Double-quote and backslash characters inside quoted entry must be escaped with a backslash.
- Escaping is not supported in non-quoted entries.
- Linefeed escape sequences (\n) are supported in quoted strings.
- Linefeed escape sequences are trimmed from the end of an entry.

-T, --with-timestamps
This option can be only used with --input-file option.

Each line of the input file must contain 4 whitespace delimited entries: <hostname> <key> <timestamp> <value>. Timestamp should be specified in Unix timestamp format. If target item has triggers referencing it, all timestamps must be in an increasing order, otherwise event calculation will not be correct.

An example of a line of the input file:
"Linux DB3" db.connections 1429533600 43

For more details please see option --input-file.

If a timestamped value is sent for a host that is in a "no data" maintenance type then this value will be dropped; however, it is possible to send a timestamped value in for an expired maintenance period and it will be accepted.

-r, --real-time
Send values one by one as soon as they are received. This can be used when reading from standard input.

--tls-connect value
How to connect to server or proxy. Values:
connect without encryption (default)

psk
connect using TLS and a pre-shared key

cert
connect using TLS and a certificate

--tls-ca-file CA-file
Full pathname of a file containing the top-level CA(s) certificates for peer certificate verification.

--tls-crl-file CRL-file
Full pathname of a file containing revoked certificates.

--tls-server-cert-issuer cert-issuer
Allowed server certificate issuer.

--tls-server-cert-subject cert-subject
Allowed server certificate subject.

--tls-cert-file cert-file
Full pathname of a file containing the certificate or certificate chain.

--tls-key-file key-file
Full pathname of a file containing the private key.

--tls-psk-identity PSK-identity
PSK-identity string.

--tls-psk-file PSK-file
Full pathname of a file containing the pre-shared key.

--tls-cipher13 cipher-string
Cipher string for OpenSSL 1.1.1 or newer for TLS 1.3. Override the default ciphersuite selection criteria. This option is not available if OpenSSL version is less than 1.1.1.

--tls-cipher cipher-string
GnuTLS priority string (for TLS 1.2 and up) or OpenSSL cipher string (only for TLS 1.2). Override the default ciphersuite selection criteria.

-v, --verbose
Verbose mode, -vv for more details.

-h, --help
Display this help and exit.

-V, --version
Output version information and exit.

EXIT STATUS
The exit status is 0 if the values were sent and all of them were successfully processed by server. If data was sent, but processing of at least one of the values failed, the exit status is 2. If data sending failed, the exit status is 1.

EXAMPLES
zabbix_sender -c /etc/zabbix/zabbix_agentd.conf -k mysql.queries -o 342.45

Send 342.45 as the value for mysql.queries item of monitored host. Use monitored host and Zabbix server defined in agent configuration file.

zabbix_sender -c /etc/zabbix/zabbix_agentd.conf -s "Monitored Host" -k mysql.queries -o 342.45

Send 342.45 as the value for mysql.queries item of Monitored Host host using Zabbix server defined in agent configuration file.
zabbix_sender -z 192.168.1.113 -i data_values.txt

Send values from file data_values.txt to Zabbix server with IP 192.168.1.113. Host names and keys are defined in the file.

```
echo "-hw.serial.number1287872261SQ4321ASDF" | zabbix_sender -c /usr/local/etc/zabbix_agentd.conf -T -i -
```

Send a timestamped value from the commandline to Zabbix server, specified in the agent configuration file. Dash in the input data indicates that hostname also should be used from the same configuration file.

```
echo ""Zabbix server" trapper.item """ | zabbix_sender -z 192.168.1.113 -p 10000 -i -
```

Send empty value of an item to the Zabbix server with IP address 192.168.1.113 on port 10000 from the commandline. Empty values must be indicated by empty double quotes.

```
zabbix_sender -z 192.168.1.113 -s "Monitored 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
```

Send 342.45 as the value for mysql.queries item in Monitored Host host to server with IP 192.168.1.113 using TLS with certificate.

```
zabbix_sender -z 192.168.1.113 -s "Monitored 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
```

Send 342.45 as the value for mysql.queries item in Monitored Host host to server with IP 192.168.1.113 using TLS with pre-shared key (PSK).

SEE ALSO

Documentation https://www.zabbix.com/manuals

zabbix_agentd(8), zabbix_get(1), zabbix_proxy(8), zabbix_server(8)

AUTHOR

Alexei Vladishev <alex@zabbix.com>
zabbix_server

NAME
zabbix_server - Zabbix server daemon

SYNOPSIS
zabbix_server [-c config-file]
zabbix_server [-c config-file] -R runtime-option
zabbix_server -h
zabbix_server -V

DESCRIPTION
zabbix_server is the core daemon of Zabbix software.

OPTIONS
-c, --config config-file
Use the alternate config-file instead of the default one.

-f, --foreground
Run Zabbix server in foreground.

-R, --runtime-control runtime-option
Perform administrative functions according to runtime-option.

Runtime control options
config_cache_reload
Reload configuration cache. Ignored if cache is being currently loaded. Default configuration file (unless -c option is specified) will be used to find PID file and signal will be sent to process, listed in PID file.

housekeeper_execute
Execute the housekeeper. Ignored if housekeeper is being currently executed.

log_level_increase[=target]
Increase log level, affects all processes if target is not specified

log_level_decrease[=target]
Decrease log level, affects all processes if target is not specified

Log level control targets
process-type
All processes of specified type (alerter, alert manager, configuration syncer, discoverer, escalator, history syncer, housekeeper, http poller, icmp pinger, ipmi manager, ipmi poller, java poller, poller, preprocessing manager, preprocessing worker, proxy poller, self-monitoring, snmp trapper, task manager, timer, trapper, unreachable poller, vmware collector)

process-type,N
Process type and number (e.g., poller,3)

pid
Process identifier, up to 65535. For larger values specify target as "process-type,N"
-h, --help
Display this help and exit.

-V, --version
Output version information and exit.

FILES
/usr/local/etc/zabbix_server.conf
Default location of Zabbix server configuration file (if not modified during compile time).

SEE ALSO
zabbix_agentd(8), zabbix_get(1), zabbix_proxy(8), zabbix_sender(1)

AUTHOR
Alexei Vladishev <alex@zabbix.com>