Специфичные ключи элементов данных для Windows

Ключи элементов данных

В таблице приводится подробная информация о ключах элементов данных, которые вы можете использовать только с Zabbix Windows агентом.

Ключ				
▲	**Описание**	**Возвращаемое значение**	**Параметры**	**Комментарии**
eventlog[имя,<регулярное выражение>,<важность>,<источник>,<eventid>,<макс. кол-во строк>,<режим>]				
	Мониторинг журналов событий.	Журнал (лог)	**имя** - имя журнала событий **регулярное выражение** - регулярное выражение описывающее требуемый шаблон содержимого **важность** - регулярное выражение описывающее важность Параметр может принимать следующие значения: “Information”, “Warning”, “Error”, “Critical”, “Verbose” (начиная с Zabbix 2.2, работающих на Windows Vista или на более новых версиях) **источник** - регулярное выражение, описывающее идентификатор источника (регулярное выражение поддерживается начиная с версии Zabbix 2.2.0) **eventid** - регулярное выражение описывающее идентификатор(ы) событий **макс. кол-во строк** - максимальное количество новых строк в секунду, которое агент будет отправлять Zabbix серверу или прокси. Этот параметр заменяет значение 'MaxLinesPerSecond' в zabbix_agentd.win.conf **режим** - возможные значения: *all* (по умолчанию), *skip* - пропустить обработку старых данных (влияет только на недавно созданные элементы данных).	Элемент данных должен быть настроен активной проверкой. Примеры: ⇒ eventlog[Application] ⇒ eventlog[Security,,"Failure Audit",,529|680] ⇒ eventlog[System,,"Warning|Error"] ⇒ eventlog[System,,,,^1$] ⇒ eventlog[System,,,,@TWOSHORT] - здесь используется ссылка на пользовательское регулярное выражение с именем TWOSHORT (заданное с типом *Результат ИСТИНА*, само выражение равно ^1$|^70$). *Обратите внимание*, агент не может отправлять события из "Пересланные события" журнала. Параметр режим поддерживается начиная с версии 2.0.0. “Windows Eventing 6.0” поддерживается начиная с Zabbix 2.2.0. Обратите внимание, что выбор не журнального типа информации для этого элемента данных приведет к потере локального штампа времени, а также важности журнала и информации о источнике. Смотрите дополнительную информацию о мониторинге файлов журналов.
net.if.list				

Ключ				
▲	**Описание**	**Возвращаемое значение**	**Параметры**	**Комментарии**
	Список сетевых интерфейсов (включая тип, состояние, IPv4 адрес, описание интерфейса).	Текст		Поддерживается Zabbix агентом начиная с версии 1.8.1. Начиная с версии 1.8.6 Zabbix агента поддерживаются мультибайтные имена интерфейса. Отключенные интерфейсы не входят в список. Обратите внимание, что включение/отключение некоторых компонентов Windows могут изменить порядок имён интерфейсов в Windows. В некоторых версиях Windows (к примеру, Server 2008) может потребоваться установка последних обновления для поддержки не-ASCII символов в именах интерфейсов.
perf_counter[счетчик,<период>]				
	Значение любого счетчика производительности Windows.	Целое число, число с плавающией точкой, строка или текст (в зависимости от запроса)	**счетчик** - путь к счетчику **период** - последние N секунд для сохранения усредненного значения. Значение период должно быть равно значению с 1 до 900 секунд (включительно), значение по умолчанию 1.	Можно использовать Мониторинг производительности для получения списка счетчиков. До версии 1.6 этот параметр возвращал правильное значение только для счетчиков, которые возвращают только одно значение (например, \System\Threads). Параметр не будет работать со счетчиками, которые возвращают более одного значения - например утилизация CPU. Начиная с версии 1.6 используется период, такая проверка каждый раз возвращает среднее значение за последние “период” секунд. Смотрите также: Счетчики производительности в Windows.
proc_info[<процесс>,<атрибут>,<тип>]				

Ключ				
▲	**Описание**	**Возвращаемое значение**	**Параметры**	**Комментарии**
	Различная информация о указанном процессе(ах).	Число с плавающей точкой	**<процесс>** - имя процесса **<атрибут>** - запрашиваемый атрибут процесса. **<тип>** - тип представления (имеет смысл, когда есть более одного процесса с одним именем)	В настоящий момент поддерживаются следующие атрибуты: *vmsize* - размер виртуальной памяти процесса в Кбайтах *wkset* - размер working set процесса (количество физической памяти используемой процессом) в Кбайтах *pf* - Количество ошибок на страницах *ktime* - время ядра процесса в миллисекундах *utime* - пользовательское время процесса в миллисекундах *io_read_b* - количество байт чтения процессом в процессе I/O операций *io_read_op* - количество операций чтения выполненных процессом *io_write_b* - количество байт записи процессом в процессе I/O операций *io_write_op* - количество операций записи выполненных процессом *io_other_b* - количество байт переданных процессу в течении операций отличных от чтения и записи *io_other_op* - количество I/O операций выполненных процессов, отличных от операций чтения и записи *gdiobj* - количество объектов GDI используемых процессом *userobj* - количество объектов USER используемых процессом Допустимые типы: *min* - минимальное значение среди всех процессов с именем <процесс> *max* - максимальное значение среди всех процессов с именем <процесс> *avg* - среднее значение среди всех процессов с именем <процесс> *sum* - сумма значений для всех процессов с именем <процесс> Примеры: ⇒ proc_info[iexplore.exe,wkset,sum] - для получения общего количество физической памяти выделенной под все процессы Internet Explorer ⇒ proc_info[iexplore.exe,pf,avg] - для получения среднего количества ошибок на страницах для процессов Internet Explorer Обратите внимание, что для корректной работы этого элемента данных на 64-битной системе потребуется 64-битный Zabbix агент. Обратите внимание: Все атрибуты *io_**, *gdiobj* и *userobj* доступны только в Windows 2000 и более поздних версиях Windows, не в Windows NT 4.0.
service.discovery				

Ключ				
▲	**Описание**	**Возвращаемое значение**	**Параметры**	**Комментарии**
	Список служб Windows. Используется низкоуровневым обнаружением.	Объект JSON		Поддерживается Zabbix агентом начиная с версии 3.0.
service.info[служба,<парам>]				
	Информация о службе.	Целое число - с парам равным *state*, *startup* Строка - с парам равным *displayname*, *path*, *user* Текст - с парам равным *description* В частности при *state*: 0 - запущена, 1 - пауза, 2 - ожидание старта, 3 - ожидание паузы, 4 - ожидание продолжения, 5 - ожидание остановки, 6 - остановлена, 7 - неизвестно, 255 - такой службы не существует В частности при *startup*: 0 - автоматически, 1 - автоматически (отложенный запуск), 2 - вручную, 3 - отключена, 4 - неизвестно, 5 - автоматический запуск по триггеру, 6 - автоматический отложенный запуск по триггеру, 7 - ручной запуск по триггеру	**служба** - действительное имя службы или её отображаемое имя как в оснастке MMC Службы **парам** - *state* (по умолчанию), *displayname*, *path*, *user*, *startup* или *description*	Примеры: ⇒ service.info[SNMPTRAP] - состояние службы SNMPTRAP ⇒ service.info[SNMP Trap] - состояние этой же службы, но указано отображаемое имя ⇒ service.info[EventLog,startup] - состояние запуска при загрузке службы Журнала событий Элементы данных service.info[служба,state] and service.info[служба] вернут одинаковую информацию. Обратите внимание, что только парам равный *state* у этого элемента данных возвращает значение по несуществующим службам (255). Этот элемент данных поддерживается начиная с Zabbix 3.0.0. Его необходимо использовать вместо устаревшего элемента данных service_state[служба].
services[<тип>,<состояние>,<исключение>]				

Ключ				
▲	**Описание**	**Возвращаемое значение**	**Параметры**	**Комментарии**
	Список служб.	0 - если список служб пуст. Текст - список служб, разделенных новой строкой.	**тип** - *all* (по умолчанию), *automatic*, *manual*, *disabled* **состояние** - *all* (по умолчанию), *stopped*, *started*, *start_pending*, *stop_pending*, *running*, *continue_pending*, *pause_pending*, *paused* **исключение** - список служб исключенных из результата. Исключенные службы должны быть указаны в двойных кавычках, разделенные запятой, без пробелов.	Примеры: ⇒ services[,started] - список запущенных служб ⇒ services[automatic, stopped] - список остановленных служб, которые должны быть запущены ⇒ services[automatic, stopped, "service1,service2,service3"] - список остановленных служб, которые должны быть запущены, исключая службы с именами service1,service2 и service3 Параметр исключения поддерживается начиная с версии 1.8.1.
wmi.get[<пространство_имен>,<запрос>]				
	Выполнение WMI запроса и получение первого выбранного объекта.	Целое число, число с плавающей точкой, строка или текст(в зависимости от запроса.)	**пространство_имен** - название пространства имен WMI **запрос** - WMI запрос, возвращающий один объект	Пример: ⇒ wmi.get[root\cimv2,select status from Win32_DiskDrive where Name like '%PHYSICALDRIVE0%'] - возвращает состояние первого физического диска Этот ключ поддерживается начиная с Zabbix 2.2.0.
vm.vmemory.size[<тип>]				
	Размер виртуального пространства в байтах или в процентах от общего размера.	Целое исло - для байт Число с плвающей точкой - для процентов	**тип** - возможные значения: *available* (доступно виртуальной памяти), *pavailable* (доступно виртуальной памяти, в процентах), *pused* (использовано виртуальной памяти, в процентах), *total* (всего виртуальной памяти, по умолчанию), *used* (использовано виртуальной памяти)	Пример: ⇒ vm.vmemory.size[pavailable] → доступно виртуальной памяти, в процентах Мониторинг статистики виртуальной памяти на основе: Максимального количества памяти, которое может занять Zabbix агент. Текущий предел выделенной памяти в системе или Zabbix агенте, смотря что меньше. Этот ключ поддерживается начиная с Zabbix 3.0.7 и 3.2.3.

Мониторинг служб Windows

Это руководство содержит пошаговые инструкции по настройке мониторинга служб Windows. Предполагается, что Zabbix сервер и агент уже настроены и работают.

Шаг 1

Узнайте имя службы.

Вы можете получить имя, перейдя в оснастку MMC Службы и открыв свойства службы. На вкладке Общие вы должны увидеть поле называемое 'Имя службы'. Значение которого и будет именем желаемой службы, которое вы будете использовать при настройке элемента данных для наблюдения.

Например, если вы хотите наблюдать службу “workstation”, то ваша служба скорее всего будет: **lanmanworkstation**.

Шаг 2

Настройте элемент данных для наблюдения за службой.

Элемент данных service.info[служба,<парам>] возвращает информацию о указанной службе. В зависимости от требемой вам информации, укажите опцию *парам*, которая принимает следующие значения: *displayname*, *state*, *path*, *user*, *startup* или *description*. Значением по умолчанию является *state*, если *парам* не указан (service.info[служба]).

Тип возвращаемого значения зависит от выбранного *парам*: целое число при *state* и *startup*; строка символов при *displayname*, *path* и *user*; текст при *description*.

Пример:

- *Ключ*: serfice.info[lanmanworkstation]
- *Тип информации*: Целочисленное (положительное)
- *Отображение значений*: выберите преобразование значений *Windows service state*

Имеется два преобразования значений *Windows service state* и *Windows service startup type*, которые сопоставляют числовое значение в веб-интерфейсе его текстовому представлению.

Обнаружение служб Windows

Низкоуровневое обнаружение дает возможность автоматического создания элементов данных, триггеров и графиков по различных объектам на компьютере. Zabbix может автоматически начать наблюдение за службами Windows на вашей машине, без необходимости знания точного имени службы или создания элементов данных по каждой службе вручную. Можно использовать фильтр для генерирования реальных элементов данных, триггеров и графиков только по интересующим службам.