Средства централизованного протоколирования и аудита

Данная статья применима к:

- ОС ОН Орёл 2.12;
- ОС СН Смоленск 1.6;
- ОС СН Ленинград 8.1.

Введение

Для решения задач централизованного протоколирования и анализа журналов аудита, а также для организации распределенного мониторинга сети, жизнеспособности и целостности серверов в ОС ОН Орёл 2.12 и ОС СН Смоленск 1.6 используется программное решение Zabbix, реализованное на web-сервере Apache, СУБД (MySQL, Oracle, PostgreSQL, SQLite) и языке сценариев PHP.

Zabbix предоставляет гибкий механизм сбора данных. Все отчеты и статистика Zabbix, а также параметры настройки компонентов Zabbix доступны через web-интерфейс. В web-интерфейсе реализован следующий функционал:

- Вывод отчетности и визуализация собранных данных;
- Создание правил и шаблонов мониторинга состояния сети и узлов;
- Определение допустимых границ значений заданных параметров;
- Настройка оповещений;
- Настройка автоматического реагирования на события безопасности.

Архитектура

Zabbix состоит из следующих основных программных компонентов:

- **Сервер** --- является основным компонентом, который выполняет мониторинг, взаимодействует с прокси и агентами, вычисляет триггеры, отправляет оповещения. Является главным хранилищем данных конфигурации, статистики, а также оперативных данных;
- **Агенты** --- разворачиваются на наблюдаемых системах для активного мониторинга за локальными ресурсами и приложениями и для отправки собранных данных серверу или прокси;
- **Прокси** --- может собирать данные о производительности и доступности от имени сервера. Прокси является опциональной частью Zabbix и может использоваться для снижения нагрузки на сервер;
- **База данных** --- вся информация о конфигурации, а также собранные Zabbix данные, хранятся в базе данных;
- **Web-интерфейс** --- используется для доступа к Zabbix из любого места и с любой платформы.

Zabbix может использоваться с СУБД PostgreSQL или с СУБД MySQL. Выбор СУБД осуществляется при установке пакета
Установку пакета Zabbix можно осуществить с помощью графического менеджера пакетов или из командной строки.

Установка пакета

Установка сервера Zabbix с СУБД PostgreSQL выполняется командой:

```
apt-get install zabbix-server-pgsql zabbix-frontend-php
```

Установка сервера Zabbix с СУБД MySQL выполняется командой:

```
apt-get install zabbix-server-mysql zabbix-frontend-php
```

Создание базы данных

Для создания базы данных сервера используются скрипты по созданию базы данных для PostgreSQL, например:

```
psql -U <username>
create database zabbix;

cd database/postgresql
psql -U <username> zabbix < schema.sql
psql -U <username> zabbix < images.sql
psql -U <username> zabbix < data.sql
```

Далее необходимо импортировать исходную схему и данные сервера на PostgreSQL:

```
zcat /usr/share/doc/zabbix-server-pgsql/create.sql.gz | psql -U <username>
zabbix
```

Для настройки базы данных сервера откорректировать конфигурационный файл zabbix_server.conf:

```
DBHost=localhost
DBName=zabbix
DBUser=zabbix
DBPassword=<пароль>
```

При эттом в параметре DBPassword указывается пароль пользователя PosgreSQL.

Основные параметры конфигурационного файла сервера приведены в таблице:

Параметр	Описание
AllowRoot	Разрешение серверу запускаться от имени пользователя root. Если запуск от имени root не разрешен (значение "0"), а сервер запускается от имени root, то сервер попробует переключиться на пользователя zabbix. Если сервер запускается от имени обычного пользователя, то параметр игнорируется. Значение по умолчанию --- 0.
CacheSize	Размер кэша конфигурации в байтах для хранения данных узлов сети, элементов данных и триггеров. Возможные значения от 128КБ до 8ГБ, значение по умолчанию - 8МБ.
CacheUpdateFrequency	Частота выполнения процедуры обновления кэша конфигурации, в секундах. Возможные значения от 1 до 3600 сек, значение по умолчанию --- 60 сек.
DBHost	Имя хоста базы данных. В случае пустой строки PostgreSQL будет использовать сокет. Значение по умолчанию --- localhost.
DBName	Обязательный параметр. Имя базы данных.
DBPassword	Пароль к базе данных.
DBPort	Порт базы данных, когда не используется localhost. Значение по умолчанию --- 3306.
DBSchema	Имя схемы.
DBUser	Пользователь базы данных.
HousekeepingFrequency	Частота выполнения автоматической процедуры очистки базы данных от устаревшей информации, в часах. Возможные значения от 0 до 24 ч., значение по умолчанию --- 1 ч.

Запуск сервера и управление сервером

Сервер работает как демон. Для запуска сервера выполнить команду:

```
systemctl start zabbix-server
```

Соответственно для остановки, перезапуска и просмотра состояния сервера используются следующие команды:

```
systemctl stop zabbix-server
systemctl restart zabbix-server
systemctl status zabbix-server
```

Для нормальной работы сервера необходимо использовать локаль UTF-8, иначе некоторые текстовые элементы данных могут интерпретироваться некорректно.

В следующей таблице приведены основные параметры, используемые при управлении сервером.

Параметр	Описание
-c --config <файл>	Путь к файлу конфигурации. Значение по умолчанию /usr/local/etc/zabbix_server.conf.
-R --runtime-control <опция>	Выполнение административных функций
config_cache_reload	Перезагрузка кэша конфигурации. Игнорируется, если кэш загружается в данный момент. Пример: zabbix_server -c /usr/local/etc/zabbix_server.conf -R config_cache_reload
housekeeper_execute	Запуск процедуры очистки базы данных. Игнорируется, если процедура очистки выполняется в данный момент. Пример: zabbix_server -c /usr/local/etc/zabbix_server.conf -R housekeeper_execute
log_level_increase[=<цель>]	Увеличение уровня журналирования, действует на все процессы, если цель не указана. В качестве цели может быть указан идентификатор процесса, тип процесса или тип и номер процесса, например: zabbix_server -c /usr/local/etc/zabbix_server.conf -R log_level_increase zabbix_server -c /usr/local/etc/zabbix_server.conf -R log_level_increase=1234 zabbix_server -c /usr/local/etc/zabbix_server.conf -R log_level_increase=poller,2
log_level_decrease[=<цель>]	Уменьшение уровня журналирования, действует на все процессы, если цель не указана. В качестве цели может быть указан идентификатор процесса, тип процесса или тип и номер процесса, например: zabbix_server -c /usr/local/etc/zabbix_server.conf -R log_level_decrease="http poller"

Агенты

Агенты устанавливаются на контролируемые компьютеры и могут выполнять пассивные и активные проверки:

- При пассивной проверке агент отвечает на запрос от сервера или прокси;
- При активной проверке агент получает от сервера перечень данных для мониторинга, затем осуществляет периодический сбор и отправку данных серверу согласно полученному перечню.

Выбор между пассивной и активной проверкой осуществляется выбором соответствующего типа элемента данных. Агент обрабатывает элементы данных типов <<Zabbix агент>> и <<Zabbix агент (активный)>>.

Установка и настройка агента в UNIX

Для установки агента в UNIX-системах выполнить команду:

```
apt-get install zabbix-agent
```

Агент UNIX работает как демон, для запуска выполнить команду:

```
systemctl start zabbix-agent
```

Соответственно для остановки, перезапуска и просмотра состояния агента UNIX используются следующие команды:

```
systemctl stop zabbix-agent
systemctl restart zabbix-agent
systemctl status zabbix-agent
```

Установка и настройка агента в Windows

В среде Windows агент работает как служба Windows. Агент Windows распространяется в виде zip-архива.
Файл агента bin\win64\zabbix_agentd.exe и файл конфигурации conf\zabbix_agentd.win.conf из zip-архива необходимо скопировать в один каталог, например, в C:\zabbix.

При необходимости - откорректировать конфигурационный файл c:\zabbix\zabbix_agentd.win.conf.

Для установки агента Windows как службы используется следующая команда:

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

Основные параметры конфигурационного файла агента.

Основные параметры конфигурационного файла агента приведены в таблице:

Параметр	Описание
AllowRoot	Параметр используется только для агентов UNIX. Разрешение агенту запускаться от имени пользователя root. Если запускаться от имени root не разрешено (значение "0") , а агент запускается от имени root, то он попробует переключиться на пользователя zabbix. Если агент запускается от имени обычного пользователя, то параметр игнорируется. Значение по умолчанию --- 0.
EnableRemoteCommands	Указывает, разрешены ли удаленные команды с сервера: • 0 — Не разрешены; • 1 --- Разрешены.
Hostname	Уникальное регистрозависимое имя машины. Требуется для активных проверок и должно совпадать с именем машины, указанным на сервере.
ListenIP	Список IP-адресов, разделенных запятой, которые агент должен слушать.
ListenPort	Порт, который необходимо слушать для подключений с сервера.
LogFile	Имя файла журнала. Обязательный параметр, если тип журнала указан как file (см. параметр LogType).
LogType	Тип вывода журнала: • file --- запись журнала в файл, указанный в параметре LogFile; • system--- запись журнала в syslog (для агентов UNIX) или в журнал событий Windows (для агентов Windows); • console --- вывод журнала в стандартный вывод
Server	Список IP-адресов или имен серверов, разделенных запятой. Входящие соединения будут приниматься только с адресов, указанных в этом параметре.
TLSAccept	Обязательный параметр если заданы TLS-сертификат или параметры PSK, в противном случае --- нет. Указывает, какие входящие подключения принимаются. Используется пассивными проверками. Можно указывать несколько значений, разделенных запятой: • unencrypted --- принимать подключения без защитного преобразования данных (по умолчанию); • psk --- принимать подключения с TLS и pre-shared ключом (PSK); • cert --- принимать подключения с TLS и сертификатом

TLSConnect	Обязательный параметр если заданы TLS-сертификат или параметры PSK, в противном случае --- нет. Как агент должен соединяться с сервером или прокси. Используется активными проверками. Можно указать только одно из значений: • unencrypted --- подключаться без использования защитного преобразования данных (по умолчанию); • psk --- подключаться, используя TLS и pre-shared ключом (PSK); • cert --- подключаться, используя TLS и сертификат
User	Использование привилегий указанного (существующего) пользователя системы. Значение по умолчанию --- zabbix. Используется только если запускается от имени пользователя root, когда такой запуск запрещенпараметром AllowRoot не разрешен

Управление агентом

Основные параметры, используемые при управлении агентом, приведены в таблице:

Параметр	Описание
Агенты Unix и Windows	
-c --config <файл_конфигурации>|	Путь к файлу конфигурации, размещенному в каталоге, отличном от заданного по умолчанию. В UNIX путь по умолчанию /usr/local/etc/zabbix_agentd.conf. В Windows --- c:\zabbix_agentd.conf.
-p --print	Вывод известных данных и выход
-t --test <ключ_элемента_данных>	Тестирование указанного элемента данных и выход.
Агент UNIX	
-R --runtime-control <опция>	Выполнение административных функций для изменения уровня журналирования у процессов агента.
log_level_increase[=<цель>]	Увеличение уровня журналирования, действует на все процессы, если цель не указана. В качестве цели может быть указан идентификатор процесса, тип процесса или тип и номер процесса, например: zabbix_agentd -R log_level_increase zabbix_agentd -R log_level_increase=1234| zabbix_agentd -R log_level_increase=listener,2
log_level_decrease[=<цель>]	Уменьшение уровня журналирования, действует на все процессы, если цель не указана. В качестве цели может быть указан идентификатор процесса, тип процесса или тип и номер процесса, например: zabbix_agentd -R log_level_decrease="active checks"
Агент Windows	
-m --multiple-agents	Использование нескольких экземпляров агента (с -i,-d,-s,-x функциями). Для отделения имени экземпляров служб каждое имя службы будет в значении Hostvalue из указанного файла конфигурации
-i --install	Установка агента как службы
-d --uninstall	Удаление службы агента
-s --start	Запуск службы агента
-x --stop	Остановка службы агента

Прокси

Для прокси требуется отдельная база данных. Для установки прокси с PostgreSQL выполнить команду:

```
apt-get install zabbix-proxy-pgsql
```

Для создания базы данных прокси используются скрипты по созданию базы данных для PostgreSQL, например:

```
psql -U <username>
create database zabbix;
\q
cd database/postgresql
psql -U <username> zabbix < schema.sql
```

Далее необходимо импортировать исходную схему и данные прокси на PostgreSQL:

```
zcat /usr/share/doc/zabbix-proxy-pgsql/create.sql.gz | psql -U <username>
zabbix
```

Для настройки базы данных прокси изменить конфигурационный файл zabbix_proxy.conf.

DBHost=localhost
DBName=zabbix
DBUser=zabbix
DBPassword=<пароль>

В параметре DBPassword указать пароль пользователя PosgreSQL.

Основные параметры конфигурационного файла прокси приведены в таблице:

Параметр	Описание
AllowRoot	Разрешение прокси запускаться от имени пользователя root. Если запуск от иемни root не разрешен (значение <<0>>), а прокси запускается от имени root, прокси попробует переключиться на пользователя zabbix. Если прокси запускается от имени обычного пользователя параметр игнорируется. Значение по умолчанию --- 0.
CacheSize	Размер кэша конфигурации в байтах для хранения данных узлов сети, элементов данных и триггеров. Возможные значения от 128КБ до 8ГБ, значение по умолчанию --- 8МБ.
ConfigFrequency	Частота получения данных конфигурации от сервера, в секундах. Параметр активного прокси, игнорируется пассивными прокси (см. параметр ProxyMode). Возможные значения от 1 до 604800 сек., значение по умолчанию --- 3600 сек.
DBHost	Имя хоста базы данных. В случае пустой строки PostgreSQL будет использовать сокет. Значение по умолчанию --- localhost.
DBName	Обязательный параметр. Имя базы данных. Должна отличаться от базы данных сервера.
DBPassword	Пароль к базе данных.
DBPort	Порт базы данных, когда не используется localhost. Значение по умолчанию --- 3306.
DBSchema	Имя схемы базы данных.
DBUser	Имя пользователя базы данных.
DataSenderFrequency	Частота отправки собранных значений серверу, в секундах. Параметр активного прокси, игнорируется пассивными прокси (см. параметр ProxyMode|). Возможные значения от 1 до 3600 сек., значение по умолчанию --- 1 сек.
Hostname	Уникальное регистрозависимое имя прокси.
HousekeepingFrequency	Частота выполнения автоматической процедуры очистки базы данных от устаревшей информации, в часах. Возможные значения от 0 до 24 ч., значение по умолчанию --- 1 ч.
ProxyMode	Режим работы прокси: • 0 --- прокси в активном режиме; • 1 --- прокси в пассивном режиме

Server	IP-адрес или имя сервера для доступа к данным конфигурации с сервера. Параметр активного прокси, игнорируется пассивными прокси (см. ProxyMode).
TLSAccept	Обязательный параметр если заданы TLS-сертификат или параметры PSK, в противном случае --- нет. Указывает, какие входящие подключения принимаются от сервера. Используется пассивным прокси, игнорируется активным прокси. Можно указывать несколько значений, разделенных запятой: • unencrypted --- принимать подключения без использования защитного преобразования данных (по умолчанию); • psk --- принимать подключения с TLS и pre-shared ключом (PSK); • cert --- принимать подключения с TLS и сертификатом
TLSConnect	Обязательный параметр если заданы TLS-сертификат или параметры PSK, в противном случае --- нет. Как прокси должен соединяться с сервером. Используется активным прокси, игнорируется пассивным прокси. Можно указать только одно из значений: • unencrypted --- подключаться без использования защитного преобразования данных (по умолчанию); • psk --- подключаться, используя TLS и pre-shared ключом (PSK); • cert --- подключаться, используя TLS и сертификат

Прокси работает как демон. Для запуска прокси выполнить команду:

```
systemctl start zabbix-proxy
```

Соответственно для остановки, перезапуска и просмотра состояния прокси используются следующие команды:

```
systemctl stop zabbix-proxy
systemctl restart zabbix-proxy
systemctl status zabbix-proxy
```

В таблице приведены основные параметры командной строки zabbix-proxy:

Параметр	Описание
-c --config <файл>	Путь к файлу конфигурации. Значение по умолчанию /etc/zabbix/zabbix_proxy.conf.
-R --runtime-control <опция>	Выполнение административных функций
config_cache_reload	Перезагрузка кэша конфигурации. Игнорируется, если кэш загружается в данный момент. Активный прокси подключится к серверу и запросит данные конфигурации: zabbix_proxy -c /usr/local/etc/zabbix_proxy.conf -R config_cache_reload
housekeeper_execute	Запуск процедуры очистки базы данных. Игнорируется, если процедура очистки выполняется в данный момент: zabbix_proxy -c /usr/local/etc/zabbix_proxy.conf -R housekeeper_execute
log_level_increase[=<цель>]	Увеличение уровня журналирования, действует на все процессы, если цель не указана. В качестве цели может быть указан идентификатор процесса, тип процесса или тип и номера процесса, например: zabbix_proxy -c /usr/local/etc/zabbix_proxy.conf -R log_level_increase zabbix_proxy -c /usr/local/etc/zabbix_proxy.conf -R log_level_increase=1234 zabbix_proxy -c /usr/local/etc/zabbix_proxy.conf -R log_level_increase=poller,2
log_level_decrease[=<цель>]	Уменьшение уровня журналирования, действует на все процессы, если цель не указана. В качестве цели может быть указан идентификатор процесса, тип процесса или тип и номера процесса, например: zabbix_proxy -c /usr/local/etc/zabbix_proxy.conf -R log_level_decrease="http poller"

Web-интерфейс

Настройка и управление работой Zabbix осуществляется посредством web-интерфейса.

Установка web-интерфейса производится путем копирования php-файлов в папку HTML web-сервера.
После копирования необходимо:

- Ввести URL Zabbix http://<ip_или_имя_сервера>/zabbix в браузере, после чего откроется первая страница помощника установки web-интерфейса;
- Указать данные для подключения к базе данных. База данных должна быть создана;
- Указать данные сервера;
- Подтвердить данные для настройки;
- Скачать конфигурационный файл и поместить его в каталог conf (если web-сервер имеет право на запись в каталог conf, файл будет сохранен автоматически);
- Завершить установку.

Для входа по умолчанию используется имя пользователя Admin и пароль zabbix.