9 Проверки через SSH

Обзор

SSH проверки выполняются без какого-либо агента. Zabbix агент не требуется для проверок выполняемых по SSH.

Для выполнения SSH проверок Zabbix сервер должен быть изначально сконфигурирован с поддержкой SSH2.

Минимально поддерживаемой версией библиотеки libssh2 является версия 1.0.0.

Настройка

Аутентификация парольной фразой

Проверки SSH предоставляют два метода аутентификации, пара логин пользователя/пароль и на основе ключа-файла.

Если вы не собираетесь использовать ключ, то никакой дополнительной настройки не требуется, при компиляции из исходных кодов, необходима также привязка библиотеки libssh2 к Zabbix.

Аутентификация на базе ключа

Для использования элементов данных SSH на основе аутентификации по ключу необходимо произвести некоторые изменения в конфигурации сервера.

Откройте файл конфигурации Zabbix сервера (zabbix_server.conf) из под `root` и найдите следующую строку:

```
# SSHKeyLocation=
```

Раскомментируйте её и укажите полный путь к папке, где размещены публичные и приватные ключи:

```
SSHKeyLocation=/home/zabbix/.ssh
```

Затем сохраните файл и перезапустите zabbix_server.

Где */home/zabbix* домашняя папка для аккаунта *zabbix* пользователя и *.ssh* папка, куда будут по умолчанию сгенерированы с помощью команды ssh-keygen публичные и приватные ключи.

Обычно при установке пакетов zabbix-server на разных дистрибутивах ОС создается аккаунт *zabbix* пользователя с домашней папкой в не очень известных местах (как для системных аккаунтов). Например, для CentOS папка */var/lib/zabbix*, для Debian она */var/run/zabbix*.

До начала генерирования ключей, рассмотрите вариант перемещения домашней папки в более

известное место (интуитивно ожидаемое). Этот вариант будет соответствовать параметру *SSHKeyLocation* конфигурации Zabbix сервера, упомянутого выше.

Эти шаги можно пропустить, если аккаунт *zabbix* добавлен вручную в соответствии с разделом установки, потому что в этом случае домашняя папка, скорее всего, уже расположена в */home/zabbix*.

Для изменения этой настройки у аккаунта *zabbix* пользователя все работающие процессы, которые его используют должны быть остановлены:

```
# service zabbix-agent stop
# service zabbix-server stop
```

Для изменения размещения домашней папки с попыткой переместить её (если папка существует),вы должны выполнить команду:

```
# usermod -m -d /home/zabbix zabbix
```

Вполне возможно, что домашняя папка не существует в старом месте (в CentOS, например), поэтому её необходимо создать в новом месте. Безопасная попытка, чтобы сделать это:

```
# test -d /home/zabbix || mkdir /home/zabbix
```

Чтобы быть уверенным что всё безопасно, можно выполнить дополнительные команды для установки разрешений к домашней папке:

```
# chown zabbix:zabbix /home/zabbix
# chmod 700 /home/zabbix
```

Теперь можно запустить ранее остановленные процессы:

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

Теперь шаги генерирования публичных и приватных ключей можно выполнить командой:

```
# 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):
Created directory '/home/zabbix/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/zabbix/.ssh/id_rsa.
Your public key has been saved in /home/zabbix/.ssh/id_rsa.pub.
The key fingerprint is:
90:af:e4:c7:e3:f0:2e:5a:8d:ab:48:a2:0c:92:30:b9 zabbix@it0
The key's randomart image is:
+--[ RSA 2048]----+
|                 |
```

```
|       .         |
|      o          |
| .     o         |
|+     . S        |
|.+   o =         |
|E .   * =        |
|=o . ..* .       |
|... oo.o+        |
+-----------------+
```

Возьмите на заметку: публичные и приватные ключи (*id_rsa.pub* и *id_rsa* соответственно) генерируются по умолчанию в папку */home/zabbix/.ssh*, которая соответствует параметру конфигурации *SSHKeyLocation* Zabbix сервера.

Ключи других типов кроме “rsa” могут быть использованы, если поддерживаются утилитой ssh-keygen и библиотекой libssh2, которая используется Zabbix.

Диалог настройки командной строки

Этот шаг необходимо выполнить только один раз на каждом хосте, который будет наблюдаться с использованием SSH проверок.

При использовании следующей команды, файл **публичного** ключа будет установлен на удаленный хост *10.10.10.10*, для того чтобы потом можно было выполнять SSH проверки при помощи аккаунта *root*:

```
# sudo -u zabbix ssh-copy-id root@10.10.10.10
The authenticity of host '10.10.10.10 (10.10.10.10)' can't be established.
RSA key fingerprint is 38:ba:f2:a4:b5:d9:8f:52:00:09:f7:1f:75:cc:0b:46.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.10.10' (RSA) to the list of known hosts.
root@10.10.10.10's password:
Теперь попытайтесь зайти на машину с помощью "ssh 'root@10.10.10.10'" и проверьте там:
  .ssh/authorized_keys
чтобы убедиться, что мы не добавили дополнительные ключи, которые нежелательны.
```

Теперь можно проверить вход по SSH с использованием приватного ключа по умолчанию (*/home/zabbix/.ssh/id_rsa*) у аккаунта *zabbix* пользователя:

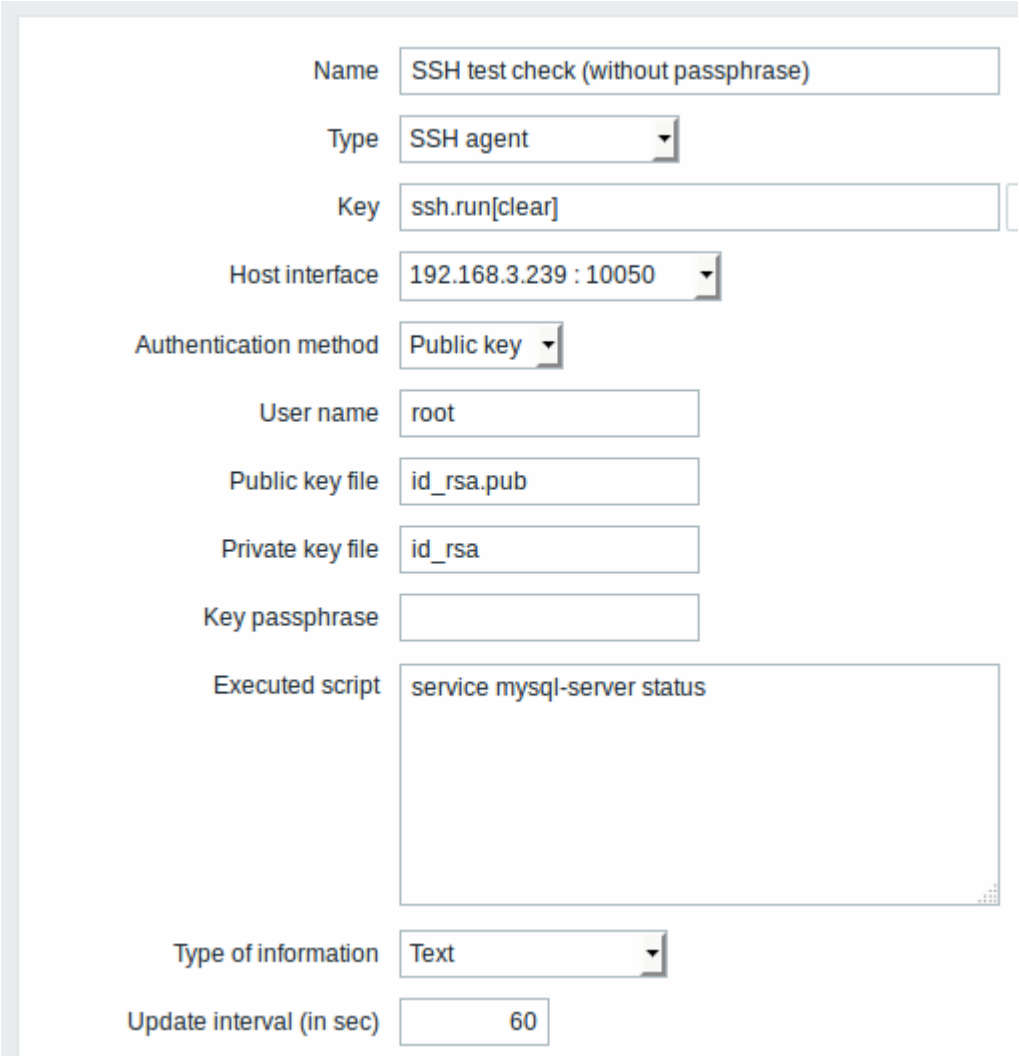
```
# sudo -u zabbix ssh root@10.10.10.10
```

Если вход успешен, то часть настройки в командной строке завершена и удаленное соединение по SSH можно закрыть.

Настройка элемента данных

Фактически выполняемые команда(ы) необходимо поместить в поле **Выполняемый скрипт** при настройке элемента данных.

Можно выполнять несколько команд одну за другой, размещая каждую на новой строке. В этом случае возвращаемые значения также будет отформатированы как многострочные.



Поля, которые требуют специфичную информацию SSH элементов данных:

Параметр элемента данных	Описание	Комментарии
Тип	Здесь выберите **SSH агент**.	
Ключ	Уникальный (в пределах узла сети) ключ элемента данных в формате **ssh.run[<уникальное короткое описание>,<ip>,<порт>,<кодировка>]**	<уникальное короткое описание> обязательно и должно быть уникальным у всех элементов данных типа SSH в рамках одного узла сети Порт 22 по умолчанию, а не порт указанный в интерфейсе узла сети к которому этот элемент данных назначен
Метод аутентификации	Один из “Пароль” или “Публичный ключ”	

Параметр элемента данных	Описание	Комментарии
Имя пользователя	Имя пользователя для аутентификации на удаленном хосте. Требуется	
Файл публичного ключа	Имя файла публичного ключа, если *Метод аутентификации* “Публичный ключ”. Требуется	Пример: *id_rsa.pub* - имя файла публичного ключа по умолчанию сгенерированного командой ssh-keygen
Файл приватного ключа	Имя файла приватного ключа, если *Метод аутентификации* “Публичный ключ”. Требуется	Пример: *id_rsa* - имя файла приватного ключа
Пароль или *Парольная фраза*	Пароль при аутентификации или Парольная фраза, **если** была использована фраза для приватного ключа	Оставьте поле *Парольная фраза* пустым, если фраза не используется Смотрите также известные проблемы по поводу использования парольных фраз
Выполняемый скрипт	Выполняемые команды командной строки при использовании удаленной сессии SSH	Примеры: *date +%s* *service mysql-server status* *ps auxww | grep httpd | wc -l*

Библиотека libssh2 может обрезать выполняемые скрипты до ~32КБ