9 SSH检查

概述

SSH checks are performed as agent-less monitoring. Zabbix agent is not needed for SSH checks.

SSH检查不依赖于Zabbix agent□可对无agent代理的设备进行监控。

To perform SSH checks Zabbix server must be initially configured with SSH2 support.

The minimum supported libssh2 library version is 1.0.0.

要执行SSH检查操作□Zabbix server必须支持SSH2□

libssh2库的最低版本是1. 0. 0.

Configuration

配置

Passphrase authentication

密码验证

SSH checks provide two authentication methods, a user/password pair and key-file based.

SSH检查提供了两种身份验证方式，一种是用户/密码对，另一种是基于密钥文件的验证方式。

If you do not intend to use keys, no additional configuration is required, besides linking libssh2 to Zabbix, if you're building from source.

如果你不打算使用密钥，除了将libssh2连接到Zabbix□就不需要额外的配置了（如果是源码安装）。

Key file authentication

密钥文件认证

To use key based authentication for SSH items, certain changes to the server configuration are required.

要对SSH监控项使用基于密钥的身份验证，需要对服务器配置进行某些更改。

Open the Zabbix server configuration file (zabbix_server.conf) as `root` and look for the following line:

以root身份打开Zabbix server的配置文件，查找以下行

```
# SSHKeyLocation=
```

```
# SSHKeyLocation=
```

Uncomment it and set full path to a folder where public and private keys will be located:

取消注释，配置公钥和私钥所在文件夹的完整路径：

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


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

Save the file and restart zabbix_server afterwards.

保存文件并重启zabbix_server服务

/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 a ssh-keygen command inside the home directory.

/home/zabbix 在这里是 *zabbix* 用户的主目录；*.ssh*是一个目录，由 ssh-keygen 这个命令产生的公钥和密钥将默认放到这个目录中。

Usually installation packages of zabbix-server from different OS distributions create the *zabbix* user account with a home directory in not very well-known places (as for system accounts). For example, for CentOS it's */var/lib/zabbix*, for Debian it's */var/run/zabbix*.

不同发行版操作系统的zabbix-server安装程序，会在不太明显的地方（与系统账户一样）创建一个带有主目录的zabbix用户账户。例如，对于CentOS系统，在 */var/lib/zabbix* 位置，而Debian系统则是在 */var/run/zabbix* 。

Before starting to generate the keys, an approach to reallocate the home directory to a better known place (intuitively expected) could be considered. This will correspond with the *SSHKeyLocation* Zabbix server configuration parameter mentioned above.

在生成密钥之前，可以考虑将主目录重新分配到更熟悉的地方（更为直观），与上述提到的 Zabbix server配置中 *SSHKeyLocation* 的参数对应。

These steps can be skipped if *zabbix* account has been added manually according to the installation section because in this case most likely the home directory is already located at */home/zabbix*.

如果根据 安装章节 手动添加了zabbix账户，则这些步骤可以省略，因为在这种情况下，主目录很可能已经是位于 */home/zabbix* 。

To change the setting for the *zabbix* user account all working processes which are using it have to be stopped:

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

要更改 *zabbix* 账户的设置，必须停止所有正在使用它的进程：

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

To change the home directory location with an attempt to move it (if it exists) a command should be executed:

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

要更改主目录的位置，以尝试移动它（如果存在），要执行一条命令：


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


It's absolutely possible that a home directory did not exist in the old place (in the CentOS for example), so it should be created at the new place. A safe attempt to do that is:

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

在旧的地方不存在主目录是完全可能的，因此需要在新的地方创建。一个安全的做法是：


```
# 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
```

为确保一切都是安全的，可以执行其他命令来设置主目录的权限：


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


Previously stopped processes now can be started again:

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

之前被停止的进程现在可以重新启动了：


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


Now steps to generate public and private keys can be performed by a command:

现在，可以通过如下命令来生成公钥和私钥：

```
# 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+        |
+-----------------+
```

Note: public and private keys (*id_rsa.pub* and *id_rsa* respectively) have been generated by default in the */home/zabbix/.ssh* directory which corresponds to the Zabbix server *SSHKeyLocation* configuration parameter.

请注意：在默认情况下，公钥和私钥(分别为 *id_rsa.pub* 和 *id_rsa*)生成在 */home/zabbix/.ssh* 目录，这与Zabbix server配置中 *SSHKeyLocation* 的参数是对应的。

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.
ssh-keygen工具和SSH服务器除了“rsa”之外，也可支持其他密钥类型，但Zabbix使用的libssh2可能不支持它们。

Shell configuration form

Shell配置方式

This step should be performed only once for every host that will be monitored by SSH checks.

对于每台被SSH检测的主机，此步骤只需要执行一次。

By using the following command the **public** key file can be installed on a remote host *10.10.10.10* so that then SSH checks can be performed with a *root* account:

通过使用以下命令，**公钥** 会安装到远程主机 *10.10.10.10* 上，以便可以使用 *root* 账户执行SSH检查：

```
# 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:
Now try logging into the machine, with "ssh 'root@10.10.10.10'", and check
in:
  .ssh/authorized_keys
to make sure we haven't added extra keys that you weren't expecting.
```

Now it's possible to check the SSH login using the default private key (*/home/zabbix/.ssh/id_rsa*) for *zabbix* user account:

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

现在可以使用 *zabbix* 用户的默认私钥（*/home/zabbix/.ssh/id_rsa*）检查SSH登陆了：

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

If the login is successful, then the configuration part in the shell is finished and remote SSH session can be closed.

如果登陆成功，那么Shell中的配置部分就完成了，并可以关闭远程SSH会话。

Item configuration

监控项配置

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 also will be formatted as multi lined.

要执行的实际命令必须放在监控项配置的 **执行脚本** 中。
如要执行多条命令，在执行脚本字段中一行写一条，命令将会逐条执行。这种情况下，返回值也将为多行显示。

All mandatory input fields are marked with a red asterisk.

所有标有红色星号的为必填项。

The fields that require specific information for SSH items are:

需要为SSH监控项提供特定信息的字段是：

Parameter	Description	Comments
Type	Select **SSH agent** here.	

Parameter	Description	Comments
Key	Unique (per host) item key in format **ssh.run[<unique short description>,<ip>,<port>,<encoding>]**	<unique short description> is required and should be unique for all SSH items per host Default port is 22, not the port specified in the interface to which this item is assigned
Authentication method	One of the “Password” or “Public key”	
User name	User name to authenticate on remote host. Required	
Public key file	File name of public key if *Authentication method* is “Public key”. Required	Example: *id_rsa.pub* - default public key file name generated by a command ssh-keygen
Private key file	File name of private key if *Authentication method* is “Public key”. Required	Example: *id_rsa* - default private key file name
Password or *Key passphrase*	Password to authenticate or Passphrase **if** it was used for the private key	Leave the *Key passphrase* field empty if passphrase was not used See also known issues regarding passphrase usage
Executed script	Executed shell command(s) using SSH remote session	Examples: *date +%s* *service mysql-server status* *ps auxww | grep httpd | wc -l*

参数	描述	注释
Type	在这里选择 **SSH agent**	
Key	格式为 **ssh.run[<unique short description>,<ip>,<port>,<encoding>]** 每台主机唯一的监控项键值	<unique short description> 参数是必须的，对于每台主机的所有SSH监控项都应该是唯一的 默认端口为22，而不是分配给该监控项的接口中指定的端口
Authentication method	“密码”认证或者“公钥”认证，两者选其一	
User name	在远程主机上进行身份验证的用户名 必填项	
Public key file	如果 *身份验证方式* 为“公钥”，此处则为公钥的文件名。 必填项	示例：*id_rsa.pub* – 由 ssh-keygen 命令生成的默认公钥文件名
Private key file	如果 *身份验证方式* 为 “公钥”，此处则为私钥的文件名. 必填项	示例：*id_rsa* – 默认私钥文件名

参数	描述	注释
Password or *Key passphrase*	如果密码用于私钥，则验证密码或密码短语	如果没有使用密码短语，则将 *密码短语* 字段留空 关于密码短语的使用，另请参阅 已知问题
Executed script	使用SSH远程会话执行shell命令	示例： *date +%s* *service mysql-server status* *ps auxww | grep httpd | wc -l*

libssh2 library may truncate executable scripts to ~32kB.
libssh2库可能会将可执行脚本截断到~32kB