9 SSH检查

概述

运行SSH检查是作为无代理监控的SSH检查不需要Zabbix代理。

执行SSH检查Zabbix服务器必须初始化配置为SSH2支持。

最低支持的libssh2库版本为1.0.0

配置

密码验证

SSH检查提供两种身份验证方法，一种是用户/密码对，另一种是基于密钥文件。

如果你不打算使用密钥，则除了将libssh2连接到Zabbix你不需要额外的配置（如果从源代码构建）。

密钥文件认证

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。

以root身份打开Zabbix服务器配置文件(zabbix_server.conf)，并查找以下行：

```
# SSHKeyLocation=
```

取消注释，并设置完整路径到公钥和私钥所在的文件夹：

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

保存文件，然后重新启动zabbix_server

*/home/zabbix*在这里是zabbix用户帐户的主目录，而*.ssh*是一个目录，默认情况下，公钥和私钥将由主目录中的ssh-keygen命令生成。

通常来自不同操作系统发行版的zabbix-server的安装包在不太明显的地方（与系统帐户一样）创建了一个带有主目录的zabbix用户帐户。例如，对于CentOS它是*/var/lib/zabbix*，对于Debian它是*/var/run/zabbix*

在开始生成密钥之前，可以考虑将主目录重新分配到更熟悉的地方（更加直观）。与上面提到的*SSHKeyLocation* Zabbix server配置参数相对应。

如果根据安装章节手动添加了zabbix帐户，则可以跳过这些步骤，因为在这种情况下，最可能的主目录已经位于*/home/zabbix*

要更改*zabbix*用户帐户的设置，必须停止所有正在使用它的进程：

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

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

要更改主目录位置以尝试移动它（如果存在），应执行一个命令：

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

主目录绝对可能不存在于旧的地方（例如在CentOS中），所以应该在新的地方创建。 一个可靠的尝试是：

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

为了确保所有操作都是安全的，可以执行其它命令来设置主目录的权限：

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

以前被停止的进程现在可以重新启动：

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

现在可以通过命令执行生成公钥和私钥的步骤：

```
# 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: 默认情况下，在/home/zabbix/.ssh目录中生成公钥和私钥（分别为id_rsa.pub和id_rsa□□该目录对应于Zabbix服务器的SSHKeyLocation配置参数。

ssh-keygen工具和SSH服务器可以支持“rsa”以外的其它Key□但Zabbix使用的libssh2可能不支持。

Shell配置表

对于将通过SSH检查监视的每个主机，此步骤只应执行一次。

通过使用以下命令，在远程主机10.10.10.10上安装**公钥**文件，以便可以使用root帐户执行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.
```

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

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

如果登录成功，则shell中的配置部分完成，并且可以关闭远程SSH会话。

监控项配置

要执行的实际命令必须放在监控项配置中的**执行脚本**域中。
可以通过将多个命令放置在新行上来执行多个命令。在这种情况下，返回的值也将被格式化为多列。

需要SSH监控项特定信息的字段有：

参数	描述	说明
Type	在这里选择**SSH agent**	
Key	格式为ssh.run的唯一（每个主机）监控项Key**ssh.run[<unique short description>,<ip>,<port>,<encoding>]**	<unique short description> 是必需的，对于每个主机的所有SSH监控项都应该是唯一的。默认端口为22，而不是分配给该项目的接口中指定的端口
Authentication method	“密码”或者“公钥Key”的其中一个	
User name	用户名在远程主机上进行身份验证。 必需的	
Public key file	如果身份验证方法为“公钥”，则为公钥的文件名。必需的。	示例：*id_rsa.pub* - 由命令ssh-keygen生成的默认公钥文件名。
Private key file	如果身份验证方法为“私钥”，则为私钥的文件名。必需的。	示例：*id_rsa* - 默认私钥文件名

参数	描述	说明
Password or *Key passphrase*	验证密码，或者密码如果用于私钥密码	如果没有使用密码短语，则将密钥密码短字段留空。 另请参阅有关密码短语使用的已知问题
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库可能会将可执行脚本截断到~32kB。