在Cisco Nexus 9000设备上为AAA身份验证用户帐户配置SSH无密码文件副本

目录

简介

本文档介绍如何使用SSH公钥和私钥对为使用身份验证、授权和记帐(AAA)协议（如RADIUS和TACACS+）进行身份验证的Cisco Nexus 9000用户帐户配置SSH无密码文件复制功能。

先决条件

要求

- 必须在Cisco Nexus设备上启用Bash外壳。有关启用Bash外壳的说明，请参阅Cisco Nexus 9000系列NX-OS可编程性指南中Bash一章的“访问Bash”部分。
- 您必须从具有“network-admin”角色的用户帐户执行此步骤。
- 必须有现有的SSH公钥和私钥对才能导入。**注意：**生成SSH公钥和私钥对的过程与平台相关，不在本文档的范围内。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Nexus 9000平台NX-OS版本7.0(3)I7(6)或更高版本
- Nexus 3000平台NX-OS版本7.0(3)I7(6)或更高版本

此软件用作SCP/SFTP服务器：

- CentOS 7 Linux x86_64

本文档中的信息在特定实验室环境设备上创建。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解任何命令的潜在影响。

背景信息

Cisco Nexus 9000系列NX-OS安全配置指南的“配置SSH和Telnet”一章介绍如何为通过Cisco Nexus设备上的NX-OS配置创建的用户帐户配置SSH无密码文件复制功能。此功能使本地用户帐户能够使用基于SSH的协议(如安全复制协议(SCP)和安全FTP(SFTP))将文件从远程服务器复制到Nexus设备。但是，此过程不能按预期对通过AAA协议（如RADIUS或TACACS+）进行身份验证的用户帐户起作用。对通过AAA身份验证的用户帐户执行时，如果因任何原因重新加载设备，SSH公钥和私钥对将不会持续。本文档演示了允许将SSH公钥和私钥对导入到经AAA身份验证的用户帐户中，以使密钥对在重新加载时继续存在的过程。

配置

为AAA身份验证用户帐户配置SSH无密码文件复制功能

此过程使用“foo”表示经AAA身份验证的用户帐户的名称。按照本步骤中的说明，将“foo”替换为要配置以用于SSH无密码文件复制功能的AAA身份验证用户帐户的实际名称。

1. 如果尚未启用Bash外壳，请启用它。
   ```
   N9K(config)# feature bash-shell
   ```
   注意：此操作不会造成中断。
2. 输入Bash外壳并验证“foo”用户帐户是否已存在。如果存在，请删除“foo”用户帐户。
   ```
   N9K# run bash sudo su -
   root@N9K# cat /etc/passwd
   root:x:0:0:root:/root:/bin/bash
   bin:*:1:1:bin:/bin:
   daemon:*:2:2:daemon:/usr/sbin:
   sys:*:3:3:sys:/dev:
   ftp:*:15:14:ftp:/var/ftp:/isanboot/bin/nobash
   ftpuser:*:99:14:ftpuser:/var/ftp:/isanboot/bin/nobash
   sshd:x:15:6:sshd:/var/sshd:/isanboot/bin/nobash
   __eemuser:*:101:100:eemuser:/var/home/__eemuser:/isanboot/bin/nobash
   nobody:*:65534:65534:nobody:/home:/bin/false
   svc-nxapi:*:498:501::/var/home/svc-nxapi:/isan/bin/vsh_perm
   svc-isan:*:499:501::/var/home/svc-isan:/isan/bin/vsh_perm
   svc-nxsdk:*:500:501::/var/home/svc-nxsdk:/isan/bin/vsh_perm
   dockremap:x:999:498::/var/home/dockremap:/bin/false
   admin:x:2002:503::/var/home/admin:/isan/bin/vsh_perm
   foo:x:2004:504::/var/home/foo:/isan/bin/vsh_perm    <<<

   root@N9K# userdel foo
   root@N9K# cat /etc/passwd
   root:x:0:0:root:/root:/bin/bash
   bin:*:1:1:bin:/bin:
   daemon:*:2:2:daemon:/usr/sbin:
   sys:*:3:3:sys:/dev:
   ftp:*:15:14:ftp:/var/ftp:/isanboot/bin/nobash
   ftpuser:*:99:14:ftpuser:/var/ftp:/isanboot/bin/nobash
   sshd:x:15:6:sshd:/var/sshd:/isanboot/bin/nobash
   __eemuser:*:101:100:eemuser:/var/home/__eemuser:/isanboot/bin/nobash
   nobody:*:65534:65534:nobody:/home:/bin/false
   svc-nxapi:*:498:501::/var/home/svc-nxapi:/isan/bin/vsh_perm
   svc-isan:*:499:501::/var/home/svc-isan:/isan/bin/vsh_perm
   svc-nxsdk:*:500:501::/var/home/svc-nxsdk:/isan/bin/vsh_perm
   dockremap:x:999:498::/var/home/dockremap:/bin/false
   admin:x:2002:503::/var/home/admin:/isan/bin/vsh_perm
   ```

   注意：在Bash中，仅当“foo”用户帐户自上次重新启动设备后远程登录Nexus设备时，才会创建“foo”用户帐户。如果“foo”用户帐户最近未登录到设备，则此步骤中使用的命令输出中可能不存在该帐户。如果命令输出中不存在“foo”用户帐户，请继续步骤3。

3. 在Bash外壳中创建“foo”用户帐户。

```
root@N9K# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:*:1:1:bin:/bin:
daemon:*:2:2:daemon:/usr/sbin:
sys:*:3:3:sys:/dev:
ftp:*:15:14:ftp:/var/ftp:/isanboot/bin/nobash
ftpuser:*:99:14:ftpuser:/var/ftp:/isanboot/bin/nobash
sshd:x:15:6:sshd:/var/sshd:/isanboot/bin/nobash
__eemuser:*:101:100:eemuser:/var/home/__eemuser:/isanboot/bin/nobash
nobody:*:65534:65534:nobody:/home:/bin/false
svc-nxapi:*:498:501::/var/home/svc-nxapi:/isan/bin/vsh_perm
svc-isan:*:499:501::/var/home/svc-isan:/isan/bin/vsh_perm
svc-nxsdk:*:500:501::/var/home/svc-nxsdk:/isan/bin/vsh_perm
dockremap:x:999:498::/var/home/dockremap:/bin/false
admin:x:2002:503::/var/home/admin:/isan/bin/vsh_perm

root@N9K# useradd foo
root@N9K# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:*:1:1:bin:/bin:
daemon:*:2:2:daemon:/usr/sbin:
sys:*:3:3:sys:/dev:
ftp:*:15:14:ftp:/var/ftp:/isanboot/bin/nobash
ftpuser:*:99:14:ftpuser:/var/ftp:/isanboot/bin/nobash
sshd:x:15:6:sshd:/var/sshd:/isanboot/bin/nobash
__eemuser:*:101:100:eemuser:/var/home/__eemuser:/isanboot/bin/nobash
nobody:*:65534:65534:nobody:/home:/bin/false
svc-nxapi:*:498:501::/var/home/svc-nxapi:/isan/bin/vsh_perm
svc-isan:*:499:501::/var/home/svc-isan:/isan/bin/vsh_perm
svc-nxsdk:*:500:501::/var/home/svc-nxsdk:/isan/bin/vsh_perm
dockremap:x:999:498::/var/home/dockremap:/bin/false
admin:x:2002:503::/var/home/admin:/isan/bin/vsh_perm
foo:x:2004:504::/var/home/foo:/isan/bin/vsh_perm    <<<
```

4. 将“foo”用户帐户添加到“network-admin”组。 **注意：**此操作允许“foo”用户帐户将文件写入bootflash，这是使用基于SSH的协议（如SCP和SFTP）执行文件复制所必需的。

```
root@N9K# usermod -a -G network-admin foo
```

5. 退出Bash外壳，确认NX-OS运行配置中存在“foo”用户帐户的配置。

```
root@N9K# exit
N9K# show run | i foo
username foo password 5 !  role network-admin
username foo keypair generate rsa
username foo passphrase  lifetime 99999 warntime 7
```

警告：如果您没有按照步骤4的说明将“foo”用户帐户添加到“network-admin”组，则NX-OS运行配置仍将显示“foo”用户帐户继承了“network-admin”角色。但是，从Linux的角度来看，“foo”用户帐户实际上不是“network-admin”组的成员，它将无法将文件写入Nexus设备的bootflash。要避免此问题，请确保按照步骤4的说明将“foo”用户帐户添加到“network-admin”组，并确认“foo”用户帐户已添加到Bash外壳中的“network-admin”组。**注意：**即使上述配置在NX-OS中存在，此用户帐户也不是本地用户帐户。您无法以本地用户帐户身份登录此用户帐户，即使设备与任何AAA(RADIUS/TACACS+)服务器断开连接也是如此。

6. 将SSH公钥和私钥对从远程位置复制到Nexus设备的bootflash。 **注意：**此步骤假设SSH公钥和私钥对已存在。生成SSH公钥和私钥对的过程与平台相关，不在本文档的范围内。**注意：**在本例中，SSH公钥的文件名为“foo.pub”，而SSH私钥的文件名为“foo”。 远程位置是SFTP服务器，地址为192.0.2.10，可通过管理虚拟路由和转发(VRF)访问。N9K# **copy sftp://foo@192.0.2.10/home/foo/foo* bootflash: vrf management**

```
The authenticity of host '192.0.2.10 (192.0.2.10)' can't be established.
ECDSA key fingerprint is SHA256:TwkQiylhtFDFPPwqh3U2Oq9ugrDuTQ50bB3boV5DkXM.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.0.2.10' (ECDSA) to the list of known hosts.
foo@192.0.2.10's password:
sftp> progress
Progress meter enabled
sftp> get /home/foo/foo* /bootflash
/home/foo/foo
100% 1766 1.7KB/s 00:00
/home/foo/foo.pub
100% 415 0.4KB/s 00:00
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.

N9K# dir bootflash: | i foo
1766 Sep 23 23:30:02 2019 foo
415 Sep 23 23:30:02 2019 foo.pub
```

7. 导入此帐户所需的SSH公钥和私钥对。

```
N9K# configure
N9K(config)# username foo keypair import bootflash:foo rsa force
N9K(config)# exit
```

验证

按照此步骤验证AAA身份验证用户帐户的SSH无密码文件复制功能。

1. 验证SSH密钥对是否已成功导入到“foo”用户帐户。

```
N9K# show username foo keypair
**************************************

rsa Keys generated:Thu Sep 5 01:50:43 2019

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDn+7nOJN8aF0i2NHSnmChHi+lujltuxf6MHtSfiKQWYCz7N13of0U4quIDGOD
LZEXzic+N655me3MsnxzvyUwXz2XNQtjqdbmPVfWnmoXiSmWQ82qfDADtnWBEX8krVhypS5ny4+lG6m0S+yMtNuAvpp
BgLpT4weSUUFWnU7DcxOzlebe9ku/0Y4JARhOZlR0bAVC0qknsd/4+2ngmcXjKqMBtNPuVESAaddFS5enED0RJRveqY
/mte/h6NUQfuzGk2COk4hh4LCslRtEsxB1+QhCasN7u7o+MJR3nV9pfKwj3qwjWt2iL5gRukj/c6UdMZ4d0+QLEoftt
BMp/y2NV

bitcount:2048
fingerprint:
MD5:9b:d8:7e:dd:32:9c:ae:32:07:b6:9b:64:34:ef:9a:af**************************************

could not retrieve dsa key information
**************************************

could not retrieve ecdsa key information
**************************************
```

2. 确认您可以使用“foo”用户帐户的SSH密钥对从远程服务器复制文件。 **注意：**本示例使用在管理VRF中可访问192.0.2.10的SFTP服务器，其中“foo”用户帐户的公钥添加为授权密钥。此SFTP服务器在绝对路径/home/foo/test.txt上存在“text.txt”**文件**。

```
[admin@server ~]$ cat .ssh/authorized_keys
```

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDn+7nOJN8aF0i2NHSnmChHi+lujltuxf6MHtSfiKQWYCz7N13of0U4quIDGOD
LZEXzic+N655me3MsnxzvyUwXz2XNQtjqdbmPVfWnmoXiSmWQ82qfDADtnWBEX8krVhypS5ny4+lG6m0S+yMtNuAvpp
BgLpT4weSUUFWnU7DcxOzlebe9ku/0Y4JARhOZlR0bAVC0qknsd/4+2ngmcXjKqMBtNPuVESAaddFS5enED0RJRveqY
/mte/h6NUQfuzGk2COk4hh4LCslRtEsxB1+QhCasN7u7o+MJR3nV9pfKwj3qwjWt2iL5gRukj/c6UdMZ4d0+QLEoftt
BMp/y2NV

[admin@server ~]$ hostname -I
192.0.2.10

[admin@server ~]$ pwd
/home/foo

[admin@server ~]$ ls | grep test.txt
test.txt
```

3. 确认您已登录“foo”用户帐户；然后尝试从上述SFTP服务器复制“test.txt”文件。请注意，Nexus不提示输入密码以登录SFTP服务器并将文件传输到Nexus的bootflash。

```
N9K# show users
NAME LINE TIME IDLE PID COMMENT
foo pts/0 Sep 19 23:18 . 4863 (192.0.2.100) session=ssh *

N9K# copy sftp://foo@192.0.2.10/home/foo/test.txt bootflash: vrf management

Outbound-ReKey for 192.0.2.10:22
Inbound-ReKey for 192.0.2.10:22
sftp> progress
Progress meter enabled
sftp> get /home/foo/test.txt /bootflash/test.txt
/home/foo/test.txt
100% 15 6.8KB/s 00:00
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

4. （可选）检验密钥对持久性。 如果需要，请保存Nexus设备的配置并重新加载设备。在Nexus设备恢复联机后，验证SSH密钥对是否继续与“foo”用户帐户关联。

```
N9K# show username foo keypair
**************************************

rsa Keys generated:Thu Sep 5 01:50:43 2019

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDn+7nOJN8aF0i2NHSnmChHi+lujltuxf6MHtSfiKQWYCz7N13of0U4quIDGOD
LZEXzic+N655me3MsnxzvyUwXz2XNQtjqdbmPVfWnmoXiSmWQ82qfDADtnWBEX8krVhypS5ny4+lG6m0S+yMtNuAvpp
BgLpT4weSUUFWnU7DcxOzlebe9ku/0Y4JARhOZlR0bAVC0qknsd/4+2ngmcXjKqMBtNPuVESAaddFS5enED0RJRveqY
/mte/h6NUQfuzGk2COk4hh4LCslRtEsxB1+QhCasN7u7o+MJR3nV9pfKwj3qwjWt2iL5gRukj/c6UdMZ4d0+QLEoftt
BMp/y2NV

bitcount:2048
fingerprint:
MD5:9b:d8:7e:dd:32:9c:ae:32:07:b6:9b:64:34:ef:9a:af**************************************

could not retrieve dsa key information
**************************************

could not retrieve ecdsa key information
**************************************

N9K# reload
This command will reboot the system. (y/n)? [n] y
```

```
N9K# show username foo keypair
**************************************

rsa Keys generated:Thu Sep 5 01:50:43 2019

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDn+7nOJN8aF0i2NHSnmChHi+lujltuxf6MHtSfiKQWYCz7N13of0U4quIDGOD
LZEXzic+N655me3MsnxzvyUwXz2XNQtjqdbmPVfWnmoXiSmWQ82qfDADtnWBEX8krVhypS5ny4+lG6m0S+yMtNuAvpp
BgLpT4weSUUFWnU7DcxOzlebe9ku/0Y4JARhOZlR0bAVC0qknsd/4+2ngmcXjKqMBtNPuVESAaddFS5enED0RJRveqY
/mte/h6NUQfuzGk2COk4hh4LCslRtEsxB1+QhCasN7u7o+MJR3nV9pfKwj3qwjWt2iL5gRukj/c6UdMZ4d0+QLEoftt
BMp/y2NV

bitcount:2048
fingerprint:
MD5:9b:d8:7e:dd:32:9c:ae:32:07:b6:9b:64:34:ef:9a:af**************************************

could not retrieve dsa key information
**************************************

could not retrieve ecdsa key information
**************************************
```

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- Cisco Nexus 9000系列NX-OS安全配置指南的“配置SSH和Telnet”一章：
  - 版本9.3(x)
  - 版本9.2(x)
  - 版本7.x
- Cisco Nexus 9000系列NX-OS可编程性指南：
  - 版本9.x
  - 版本7.x
  - 6.x 版
- Cisco Nexus 3600系列NX-OS可编程性指南：
  - 版本9.x
  - 版本7.x
- Cisco Nexus 3500系列NX-OS可编程性指南：
  - 版本9.x
  - 版本7.x
  - 6.x 版
- Cisco Nexus 3000系列NX-OS可编程性指南：
  - 版本9.x
  - 版本7.x
  - 6.x 版
- 借助思科开放式NX-OS实现可编程性和自动化
- 技术支持和文档 - Cisco Systems