Cisco Nexus 9000デバイスのAAA認証されたユーザアカウントのSSHパスワードレスファイルコピーの設定

内容

概要

このドキュメントでは、SSHの公開キーと秘密キーのペアを使用して、認証、許可、アカウンティング(AAA)プロトコル（RADIUSやTACACS+など）で認証されたCisco Nexus 9000ユーザアカウントのSSHパスワードレスファイルコピー機能を設定する方法について説明します。

前提条件

要件

- Cisco NexusデバイスでBashシェルを有効にする必要があります。Bashシェルを有効にする手順については、『Cisco Nexus 9000シリーズNX-OSプログラマビリティガイド』のBashの章の「Bashへのアクセス」セクションを参照してください。
- この手順は、「network-admin」ロールを持つユーザアカウントから実行する必要があります。
- インポートするには、既存のSSH公開キーと秘密キーのペアが必要です。**注**：SSHの公開キーと秘密キーのペアを生成する手順は、プラットフォームによって異なり、このドキュメントの範囲外です。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Nexus 9000プラットフォームNX-OSリリース7.0(3)I7(6)以降
- Nexus 3000プラットフォームNX-OSリリース7.0(3)I7(6)以降

このソフトウェアは、SCP/SFTPサーバとして動作するために使用されました。

- CentOS 7 Linux x86_64

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

背景説明

『Cisco Nexus 9000 Series NX-OS Security Configuration Guide』の「Configuring SSH and Telnet」の章で、Cisco NexusデバイスのNX-OS設定で作成されたユーザアカウントにSSHパスワードレスファイルコピー機能を設定する方法について説明します。この機能により、ローカルユーザアカウントは、Secure Copy Protocol(SCP)やSecure FTP(SFTP)などのSSHベースのプロトコルを使用して、リモートサーバからNexusデバイスにファイルをコピーできます。ただし、RADIUSやTACACS+などのAAAプロトコルを使用して認証されたユーザアカウントでは、この手順は想定どおりに動作しません。AAA認証されたユーザアカウントに対して実行すると、デバイスが何らかの理由でリロードされた場合、SSHの公開キーと秘密キーのペアは保持されません。このドキュメントでは、リロード時にキーペアが保持されるように、SSHの公開キーと秘密キーのペアをAAA認証されたユーザアカウントにインポートできるようにする手順を示します。

設定

AAA認証されたユーザアカウントのSSHパスワードレスファイルコピー機能の設定

この手順では、「foo」を使用して、AAA認証されたユーザアカウントの名前を表します。この手順の指示に従って、「foo」を、SSHパスワードレスファイルコピー機能で使用するように設定するAAA認証ユーザアカウントの実際の名前に置き換えます。

1. Bashシェルが有効になっていない場合は、有効にします。
   ```
   N9K(config)# feature bash-shell
   ```
   注：このアクションは無停止で実行できます。
2. Bashシェルを入力し、「foo」ユーザアカウントがすでに存在するかどうかを確認します。存在する場合は、"foo"ユーザアカウントを削除します。
   ```
   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：Bash内で、「foo」ユーザアカウントが作成されるのは、デバイスが最後にリブートされてから「foo」ユーザアカウントがリモートでNexusデバイスにログインした場合だけです。「foo」ユーザアカウントが最近デバイスにログインしていない場合、このステップで使用するコマンドの出力には表示されない可能性があります。コマンドの出力に「foo」ユーザアカウントがない場合は、ステップ3に進みます。

3. Bashシェル内に「foo」ユーザアカウントを作成します。

```
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. 「foo」ユーザアカウントを「network-admin」グループに追加します。 **注**：この操作により、「foo」ユーザアカウントがブートフラッシュにファイルを書き込むことができます。これは、SSHベースのプロトコル（SCPやSFTPなど）を使用してファイルのコピーを実行するために必要です。

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

5. Bashシェルを終了し、「foo」ユーザアカウントの設定がNX-OS実行コンフィギュレーションにあることを確認します。

```
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
```

注意：ステップ4で指定した「foo」ユーザアカウントを「network-admin」グループに追加しなかった場合、NX-OSの実行コンフィギュレーションでは、「foo」ユーザアカウントが「network-admin」ロールを継承していることがわかります。ただし、「foo」ユーザアカウントは、Linuxの観点から実際には「network-admin」グループのメンバーではなく、Nexusデバイスのブートフラッシュにファイルを書き込むことはできません。この問題を回避するには、ステップ4で指定したように「foo」ユーザアカウントを「network-admin」グループに追加し、Bashシェル内の「network-admin」グループに「foo」ユーザアカウントが追加されていることを確認します。**注**：上記の設定はNX-OSに存在しますが、このユーザアカウントはローカルユーザアカウントではありません。デバイスがAAA(RADIUS/TACACS+)サーバから切断されている場合でも、ローカルユーザアカウントとしてこのユーザアカウントにログインすることはできません。

6. SSHの公開キーと秘密キーのペアをリモートロケーションからNexusデバイスのブートフラッシュにコピーします。 **注**：この手順では、SSHの公開キーと秘密キーのペアがすでに存在することを前提としています。SSHの公開キーと秘密キーのペアを生成する手順は、プラットフォームによって異なり、このドキュメントの範囲外です。**注**：この例では、SSH公開キーのファイル名は「foo.pub」、SSH秘密キーのファイル名は「foo」です。 リモートロケーションは、管理Virtual Routing and Forwarding(VRF)経由で到達可能な192.0.2.10のSFTPサーバです。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. このアカウントに必要なSSH公開キーと秘密キーのペアをインポートします。

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

確認

AAA認証されたユーザアカウントのSSHパスワードレスファイルコピー機能を確認するには、次の手順に従います。

1. SSHキーペアが「foo」ユーザアカウントに正常にインポートされたことを確認します。

```
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. 「foo」ユーザアカウントのSSHキーペアを使用して、リモートサーバからファイルをコピーできることを確認します。 **注：**この例では、管理VRFの192.0.2.10からアクセス可能なSFTPサーバを使用します。このサーバには、「foo」ユーザアカウントの公開キーが許可キーとして追加されます。このSFTPサーバの絶対パス/home/foo/test.txtに「text.txt」ファイルが存在**します**。

```
[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. 「foo」ユーザアカウントにログインしていることを確認します。次に、上記のSFTPサーバから「test.txt」ファイルをコピーしてみます。NexusがSFTPサーバにログインし、ファイルをNexusのブートフラッシュに転送するためのパスワードを求めないことに注意してください。

```
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. （オプション）キーペアの持続性を確認します。 必要に応じて、Nexusデバイスの設定を保存し、デバイスをリロードします。Nexusデバイスがオンラインに戻ったら、SSHキーペアが「foo」ユーザアカウントに関連付けられていることを確認します。

```
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
**************************************
```

トラブルシューティング

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- 『Cisco Nexus 9000 Series NX-OS Security Configuration Guide:
  - リリース9.3(x)
  - リリース9.2(x)
  - リリース7.x
- Cisco Nexus 9000シリーズNX-OSプログラマビリティガイド：
  - リリース9.x
  - リリース7.x
  - リリース6.x
- Cisco Nexus 3600シリーズNX-OSプログラマビリティガイド：
  - リリース9.x
  - リリース7.x
- Cisco Nexus 3500シリーズNX-OSプログラマビリティガイド：
  - リリース9.x
  - リリース7.x
  - リリース6.x
- Cisco Nexus 3000シリーズNX-OSプログラマビリティガイド：
  - リリース9.x
  - リリース7.x
  - リリース6.x
- Cisco Open NX-OSによるプログラマビリティと自動化
- テクニカル サポートとドキュメント – Cisco Systems