# 為Cisco Nexus 9000裝置上的AAA驗證使用者帳戶配置SSH無密碼檔案副本

## 目錄



## 簡介

本檔案介紹如何使用SSH公用和私人金鑰對，為使用驗證、授權和計量(AAA)通訊協定（例如RADIUS和TACACS+）驗證的Cisco Nexus 9000使用者帳戶設定SSH無密碼檔案複製功能。

## 必要條件

### 需求

- 必須在Cisco Nexus裝置上啟用Bash外殼。有關啟用Bash shell的說明，請參閱Cisco Nexus 9000系列NX-OS可程式設計性指南中Bash一章的「訪問Bash」一節。
- 您必須使用具有「network-admin」角色的使用者帳戶執行此過程。
- 您必須具有現有的SSH公鑰和私鑰對才能匯入。**附註**：產生SSH公共金鑰對和私有金鑰對的過程取決於平台，不屬於本檔案的範圍。

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 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

此軟體用作SCP/SFTP伺服器：

- CentOS 7 Linux x86_64

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

## 背景資訊

Cisco Nexus 9000系列NX-OS安全配置指南的「配置SSH和Telnet」一章介紹了如何為通過Cisco Nexus裝置上的NX-OS配置建立的使用者帳戶配置SSH無密碼檔案複製功能。此功能允許本地使用者帳戶使用基於SSH的協定（如安全複製協定[SCP]和安全FTP[SFTP]）將檔案從遠端伺服器複製到Nexus裝置。但是，對於通過AAA協定（例如RADIUS或TACACS+）進行身份驗證的使用者帳戶，此過程沒有按預期運行。對通過AAA身份驗證的使用者帳戶執行時，如果由於任何原因重新載入裝置，SSH公共金鑰對和私有金鑰對將不會持續。本文檔演示了一個過程，該過程允許將SSH公共金鑰對和私有金鑰對匯入到經過AAA身份驗證的使用者帳戶中，以便在重新載入時金鑰對仍然存在。

# 設定

## 為AAA驗證的使用者帳戶配置SSH無密碼檔案複製功能

此過程使用「foo」表示AAA驗證的使用者帳戶的名稱。按照此過程中的說明進行操作時，請將「foo」替換為要配置以與SSH無密碼檔案複製功能配合使用的AAA驗證使用者帳戶的實際名稱。

1. 啟用Bash shell（如果尚未啟用）。
   ```
   N9K(config)# feature bash-shell
   ```
   **附註**：此操作不會造成中斷。
2. 輸入Bash shell並驗證「foo」使用者帳戶是否存在。如果存在，請刪除「foo」使用者帳戶。
   ```
   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
   ```

   **附註**：在Bash中，僅當自上次重新啟動裝置後，「foo」使用者帳戶已遠端登入到Nexus裝置時，才會建立「foo」使用者帳戶。如果「foo」使用者帳戶最近未登入到裝置，則它可能未出

現在此步驟中使用的命令的輸出中。如果命令輸出中沒有「foo」使用者帳戶，請繼續執行步驟3。

3. 在Bash shell中建立「foo」使用者帳戶。

```
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. 將「foo」使用者帳戶新增到「network-admin」組。 **附註**：此操作允許「foo」使用者帳戶將檔案寫入bootflash，這是使用基於SSH的協定（如SCP和SFTP）執行檔案複製所必需的。

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

5. 退出Bash shell並確認「foo」使用者帳戶的配置存在於NX-OS運行配置中。

```
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**：如果您沒有按照步驟4中的說明將「foo」使用者帳戶新增到「network-admin」組，則NX-OS運行配置仍會顯示「foo」使用者帳戶繼承了「network-admin」角色。但是，從Linux的角度來看，「foo」使用者帳戶實際上不是「network-admin」組的成員，它無法將檔案寫入Nexus裝置的bootflash。要避免此問題，請確保按照步驟4中的說明將「foo」使用者帳戶新增到「network-admin」組，並確認已將「foo」使用者帳戶新增到Bash shell中的「network-admin」組。**附註**：即使上述配置存在於NX-OS中，此使用者帳戶也不是本地使用者帳戶。您不能以本地使用者帳戶登入此使用者帳戶，即使裝置與任何AAA(RADIUS/TACACS+)伺服器斷開連線也是如此。

6. 將SSH公鑰和私鑰對從遠端位置複製到Nexus裝置的bootflash。 **附註**：此步驟假設SSH公鑰

和私鑰對已存在。產生SSH公共金鑰對和私有金鑰對的過程取決於平台，不屬於本檔案的範圍。**附註**：在本例中，SSH公鑰的檔案名稱為「foo.pub」，SSH私鑰的檔案名稱為「foo」。 遠端位置是通過管理虛擬路由和轉發(VRF)可訪問的192.0.2.10上的SFTP伺服器。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. 為此帳戶匯入所需的SSH公鑰和私鑰對。

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

# 驗證

按照以下步驟驗證通過AAA驗證的使用者帳戶的SSH無密碼檔案複製功能。

1. 驗證SSH金鑰對是否已成功匯入到「foo」使用者帳戶。

```
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. 確認可以使用「foo」使用者帳戶的SSH金鑰對從遠端伺服器複製檔案。 **附註**：此示例使用在管理VRF中可訪問192.0.2.10的SFTP伺服器，並將「foo」使用者帳戶的公鑰新增為授權金鑰。此SFTP伺服器的**/home/foo/test.txt**絕對路徑上有一個「text.txt」檔案。

```
[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. 確認您已登入到「foo」使用者帳戶；然後嘗試從上述SFTP伺服器複製「test.txt」檔案。請注意，Nexus不會提示輸入密碼以登入到SFTP伺服器並將檔案傳輸到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. （可選）驗證金鑰對永續性。 如果需要，請儲存Nexus裝置的配置並重新載入裝置。Nexus裝置恢復聯機後，驗證SSH金鑰對是否繼續與「foo」使用者帳戶關聯。

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

# 疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

# 相關資訊

- 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可程式設計性指南：
  - 版本9.x
  - 版本7.x
  - 版本6.x
- Cisco Nexus 3600系列NX-OS可程式設計性指南：
  - 版本9.x
  - 版本7.x
- Cisco Nexus 3500系列NX-OS可程式設計性指南：
  - 版本9.x
  - 版本7.x
  - 版本6.x
- Cisco Nexus 3000系列NX-OS可程式設計性指南：
  - 版本9.x
  - 版本7.x
  - 版本6.x

- Cisco Open NX-OS的可程式設計性和自動化
- 技術支援與文件 - Cisco Systems