# Configurazione della copia dei file senza password SSH per gli account utente autenticati AAA sui dispositivi Cisco Nexus 9000

## Sommario



## Introduzione

In questo documento viene descritto come usare una coppia di chiavi pubblica e privata SSH per configurare la funzione di copia dei file senza password SSH per gli account utente Cisco Nexus 9000 autenticati con i protocolli di autenticazione, autorizzazione e accounting (AAA) (ad esempio RADIUS e TACACS+).

## Prerequisiti

### Requisiti

- La shell Bash deve essere abilitata sul dispositivo Cisco Nexus. Per le istruzioni su come abilitare Bash Shell, consultare la sezione "Accesso a Bash" del capitolo Bash nella Guida alla programmabilità di Cisco Nexus serie 9000 NX-OS.
- Ènecessario eseguire questa procedura da un account utente con il ruolo "network-admin".
- Ènecessario avere una coppia di chiavi pubblica e privata SSH esistente da importare.**Nota:** La procedura per generare una coppia di chiavi pubblica e privata SSH è dipendente dalla piattaforma e non rientra nell'ambito di questo documento.

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Piattaforma Nexus 9000 NX-OS release 7.0(3)I7(6) o successive
- Piattaforma Nexus 3000 NX-OS release 7.0(3)I7(6) o successive

Questo software è stato utilizzato come server SCP/SFTP:

- CentOS 7 Linux x86_64

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

# Premesse

Nel capitolo "Configuring SSH and Telnet" della guida alla configurazione della sicurezza di Cisco Nexus serie 9000 NX-OS viene descritto come configurare la funzione di copia dei file senza password SSH per gli account utente creati tramite la configurazione di NX-OS sui dispositivi Cisco Nexus. Questa funzionalità consente a un account utente locale di utilizzare protocolli basati su SSH, quali SCP (Secure Copy Protocol) e SFTP (Secure FTP), per copiare i file da un server remoto al dispositivo Nexus. Tuttavia, questa procedura non funziona come previsto per gli account utente autenticati tramite un protocollo AAA, ad esempio RADIUS o TACACS+. Se eseguita su account utente autenticati AAA, la coppia di chiavi pubblica e privata SSH non persiste se il dispositivo viene ricaricato per qualsiasi motivo. In questo documento viene illustrata una procedura che consente di importare una coppia di chiavi pubblica e privata SSH in un account utente autenticato AAA, in modo che la coppia di chiavi persista al ricaricamento.

# Configurazione

## Configurazione della funzione di copia dei file senza password SSH per gli account utente autenticati AAA

In questa procedura viene utilizzato "foo" per rappresentare il nome di un account utente autenticato AAA. Seguendo le istruzioni riportate in questa procedura, sostituire "foo" con il nome effettivo dell'account utente autenticato AAA che si desidera configurare per l'uso con la funzione di copia dei file senza password SSH.

1. Abilitare la shell Bash se non è già abilitata.
   ```
   N9K(config)# feature bash-shell
   ```
   **Nota:** Questa azione non comporta interruzioni.
2. Immettere la shell Bash e verificare se l'account utente "foo" esiste già. Se esiste, eliminare l'account utente "foo".
   ```
   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
```

**Nota:** All'interno di Bash, l'account utente "foo" viene creato solo se l'account utente "foo" ha effettuato l'accesso remoto al dispositivo Nexus dall'ultimo riavvio del dispositivo. Se l'account utente "foo" non ha eseguito di recente l'accesso al dispositivo, potrebbe non essere presente nell'output dei comandi utilizzati in questo passaggio. Se l'account utente "foo" non è presente nell'output dei comandi, andare al passaggio 3.

3. Creare l'account utente "foo" all'interno della shell Bash.

```
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. Aggiungere l'account utente "foo" al gruppo "network-admin". **Nota:** Questa azione consente

all'account utente "foo" di scrivere file nella memoria flash, necessaria per usare i protocolli basati su SSH (come SCP e SFTP) per eseguire una copia dei file.

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

5. Uscire dalla shell Bash e verificare che la configurazione per l'account utente "foo" sia presente nella configurazione NX-OS in esecuzione.

```
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
```

**Attenzione:** Se l'account utente "foo" non è stato aggiunto al gruppo "network-admin" come indicato al passaggio 4, la configurazione di esecuzione di NX-OS mostrerà comunque che l'account utente "foo" eredita il ruolo "network-admin". Tuttavia, l'account utente "foo" non è in realtà un membro del gruppo "network-admin" da una prospettiva Linux, e non sarà in grado di scrivere file nella bootflash del dispositivo Nexus. Per evitare questo problema, accertarsi di aver aggiunto l'account utente "foo" al gruppo "network-admin" come indicato al punto 4 e confermare che l'account utente "foo" sia stato aggiunto al gruppo "network-admin" all'interno della shell Bash.**Nota:** Anche se la configurazione precedente è presente in NX-OS, questo account utente *non* è un account utente locale. Non è possibile accedere a questo account utente come account utente locale, anche se il dispositivo è disconnesso da qualsiasi server AAA (RADIUS/TACACS+).

6. Copiare la coppia di chiavi SSH pubblica e privata da una postazione remota sulla memoria flash del dispositivo Nexus. **Nota:** In questo passaggio si presume che la coppia di chiavi pubblica e privata SSH esista già. La procedura per generare una coppia di chiavi pubblica e privata SSH è dipendente dalla piattaforma e non rientra nell'ambito di questo documento.**Nota:** Nell'esempio, la chiave pubblica SSH ha il nome file "foo.pub" e la chiave privata SSH il nome file "foo". La posizione remota è un server SFTP a 192.0.2.10 raggiungibile tramite il VRF (Virtual Routing and Forwarding) di gestione.

```
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. Importare la coppia di chiavi pubblica e privata SSH desiderata per questo account.

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

```
N9K(config)# exit
```

# Verifica

Seguire questa procedura per verificare la funzionalità di copia dei file senza password SSH per gli account utente autenticati con AAA.

1. Verificare che la coppia di chiavi SSH sia stata importata nell'account utente "foo" correttamente.

```
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. Confermare che è possibile usare la coppia di chiavi SSH dell'account utente "foo" per copiare i file da un server remoto. **Nota:** In questo esempio viene usato un server SFTP accessibile dalla versione 192.0.2.10 nel VRF di gestione con la chiave pubblica dell'account utente "foo" aggiunta come chiave autorizzata. Questo server SFTP ha un file "text.txt" presente nel percorso assoluto **/home/foo/test.txt**.

```
[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. Confermare di aver effettuato l'accesso all'account utente "foo"; quindi provate a copiare il file "test.txt" dal server SFTP sopraindicato. Notare che Nexus non richiede una password per accedere al server SFTP e trasferire il file nella bootflash di Nexus.

```
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. (Facoltativo) Verificare la persistenza della coppia di chiavi. Se lo si desidera, salvare la configurazione del dispositivo Nexus e ricaricarlo. Dopo che il dispositivo Nexus è tornato online, verificare che la coppia di chiavi SSH continui a essere associata all'account utente "foo".

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

## Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

## Informazioni correlate

- Capitolo "Configuring SSH and Telnet" della guida alla configurazione della sicurezza di Cisco Nexus serie 9000 NX-OS:
  - Release 9.3(x)
  - Release 9.2(x)
  - Release 7.x
- Guida alla programmabilità di Cisco Nexus serie 9000 NX-OS:
  - Release 9.x
  - Release 7.x
  - Release 6.x
- Cisco Nexus serie 3600 NX-OS Guida alla programmabilità:
  - Release 9.x
  - Release 7.x
- Guida alla programmabilità di Cisco Nexus serie 3500 NX-OS:
  - Release 9.x
  - Release 7.x
  - Release 6.x
- Cisco Nexus serie 3000 NX-OS Guida alla programmabilità:
  - Release 9.x
  - Release 7.x
  - Release 6.x
- Programmabilità e automazione con Cisco Open NX-OS
- Documentazione e supporto tecnico – Cisco Systems