SSH-passareloze bestandskopie configureren voor AAA-gewaarmerkte gebruikersaccounts op Cisco Nexus 9000-apparaten

Inhoud

Inleiding

Dit document beschrijft hoe u een openbaar en privé SSH-sleutelpaar kunt gebruiken om de optie Wachtwoord zonder wachtwoord te configureren voor Cisco Nexus 9000-gebruikersaccounts die zijn gecertificeerd met verificatie-, autorisatie- en accounting (AAA) protocollen (zoals RADIUS en TACACS+).

Voorwaarden

Vereisten

- De schaal van het Bash moet op het apparaat van Cisco Nexus worden geactiveerd. Raadpleeg het gedeelte "Toegang tot basis" van het Hoofdstuk in de Cisco Nexus 9000 Series NX-OS Programmakeuze voor de instructies om het veld Bash in te schakelen.
- U moet deze procedure uitvoeren vanuit een gebruikersaccount dat de "netwerk-beheerder" rol behoudt.
- U moet beschikken over een bestaand openbaar en privé SSH-toetsenbord om te importeren.Opmerking: De procedure voor het genereren van een openbaar en particulier SSH-sleutelpaar is van het platform afhankelijk en valt buiten het toepassingsgebied van dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Nexus 9000 platform NX-OS release 7.0(3)I7(6) of hoger

- Nexus 3000 platform NX-OS release 7.0(3)I7(6) of hoger

Deze software werd gebruikt om op te treden als een SCP/SFTP-server:

- CentOS 7 Linux x86_64

De informatie in dit document is gemaakt van apparatuur in een specifieke labomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdrachten begrijpt.

Achtergrondinformatie

Het hoofdstuk "SSH en telnet configureren" van de Cisco Nexus 9000 Series NX-OS security configuratiegids beschrijft hoe u de functie SSH Passive File Kopie kunt configureren voor gebruikersaccounts die worden gemaakt via NX-OS-configuratie op Cisco Nexus-apparaten. Deze optie stelt een lokale gebruikersaccount in staat om op SSH gebaseerde protocollen te gebruiken, zoals Secure Copy Protocol (SCP) en Secure FTP (SFTP), om bestanden van een externe server naar het Nexus-apparaat te kopiëren. Deze procedure werkt echter niet zoals verwacht voor gebruikersaccounts die via een AAA-protocol zijn geauthentiseerd, zoals RADIUS of TACACS+. Wanneer uitgevoerd op AAA-echt bevonden gebruikersrekeningen, zal het openbare en privé sleutelpaar van SSH niet blijven bestaan als het apparaat om wat voor reden dan ook opnieuw geladen is. Dit document toont een procedure aan die het mogelijk maakt om een publiek en privé zeer belangrijk paar van SSH in een AAA-geauthentiseerde gebruikersaccount te importeren zodat het belangrijkste paar bij herlading blijft.

Configureren

Functie voor SSH-passieve bestandskopie configureren voor AAA-verificatie

Deze procedure gebruikt "foo" om de naam van een AAA-echt bevonden gebruikersaccount weer te geven. Wanneer u de instructies in deze procedure opvolgt, vervangt u "foo" door de eigenlijke naam van de AAA-echt gewaarmerkte gebruikersaccount die u voor gebruik wilt configureren met de optie SSH Wachtwoordloze File Copy.

1. Schakel de shell in als deze niet reeds is ingeschakeld.
   ```
   N9K(config)# feature bash-shell
   ```
   Opmerking: Deze actie is niet-verstorend.
2. Voer de schaal van het Bash in en controleer of de gebruikersaccount voor "foo" al bestaat. Als het bestaat, verwijdert u de foo-gebruikersaccount.
   ```
   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
```

Opmerking: Binnen Bash wordt de gebruikersaccount voor "foo" alleen aangemaakt als de gebruikersaccount voor "foo" op afstand is aangemeld bij het Nexus-apparaat sinds het apparaat voor het laatst is herstart. Als de gebruikersaccount "foo" zich onlangs niet bij het apparaat heeft aangemeld, is de account mogelijk niet aanwezig in de uitvoer van de opdrachten die in deze stap zijn gebruikt. Als de gebruikersaccount "foo" niet aanwezig is in de uitvoer van de opdrachten, gaat u naar Stap 3.

3. Maak de foo-gebruikersaccount binnen het veld 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. Voeg de foo-gebruikersaccount toe aan het vak "netwerk-beheerder". Opmerking: Met deze actie kan de gebruikersaccount "foo" bestanden naar de flitser schrijven, die vereist is om op SSH gebaseerde protocollen (zoals SCP en SFTP) te kunnen gebruiken om een bestandskopie uit te voeren.
```
root@N9K# usermod -a -G network-admin foo
```

5. Afsluiten van de granaat Bash en bevestigen dat de configuratie voor de gebruikersaccount voor "foo" aanwezig is in de configuratie van het NX-OS-systeem.
```
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
```

   Voorzichtig: Als u de gebruikersaccount "foo" niet aan de groep "netwerk-admin" hebt toegevoegd zoals in Stap 4 is gericht, dan zal de actieve configuratie van NX-OS nog steeds laten zien dat de gebruikersaccount "foo" de rol "netwerk-admin" erft. De foo-gebruikersaccount is echter geen lid van de "netwerk-admin"-groep vanuit een Linux-perspectief, en kan geen bestanden naar de flitser van het Nexus-apparaat schrijven. Om dit probleem te voorkomen, zorg er dan voor dat u de foo-gebruikersaccount aan de groep "netwerk-beheerder" toevoegt zoals bedoeld in Stap 4 en bevestig dat de foo-gebruikersaccount is toegevoegd aan de groep "netwerk-beheerder" binnen het veld Bash.Opmerking: Hoewel de bovenstaande configuratie aanwezig is in NX-OS, is deze gebruikersaccount *geen* lokale gebruikersaccount. U kunt niet in deze gebruikersaccount loggen als lokale gebruikersaccount, zelfs niet als het apparaat is losgekoppeld van een AAA-server (RADIUS/TACACS+).
6. Kopieer het openbare en privé sleutelpaar van SSH van een externe locatie naar de Start van het Nexus-apparaat. Opmerking: Deze stap gaat ervan uit dat het openbare en particuliere SSH-sleutelpaar al bestaat. De procedure voor het genereren van een openbaar en particulier SSH-sleutelpaar is van het platform afhankelijk en valt buiten het toepassingsgebied van dit document.Opmerking: In dit voorbeeld heeft de SSH public key een bestandsnaam van "foo.pub" en de SSH private key heeft een bestandsnaam van "foo". De externe locatie is een SFTP-server op 192.0.2.10 die bereikbaar is via het Management Virtual Routing and Forwarding (VRF).
```
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. Importeer het gewenste openbare en particuliere SSH-toetsenbord voor deze account.

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

Verifiëren

Volg deze procedure om de optie SSH-bestandskopie voor AAA-gewaarmerkte gebruikersrekeningen te controleren.

1. Controleer dat het SSH-sleutelpaar met succes is geïmporteerd naar de foo-gebruikersaccount.

```
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. Bevestig dat u het SSH-sleutelpaar van de "foo"-gebruikersaccount kunt gebruiken om bestanden van een externe server te kopiëren. Opmerking: Dit voorbeeld gebruikt een SFTP-server die op 192.0.2.10 in het beheer VRF toegankelijk is, met de openbare sleutel van de "foo"-gebruikersaccount toegevoegd als geautoriseerde sleutel. Deze SFTP-server heeft een "text.txt"-bestand dat op het absolute pad **/home/foo/test.txt** aanwezig is.

```
[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. Bevestig dat u bent ingelogd op de foo-gebruikersaccount. Probeer vervolgens het bestand "test.txt" van de bovengenoemde SFTP-server te kopiëren. Let op dat de Nexus niet vraagt om een wachtwoord om in te loggen op de SFTP-server en het bestand over te brengen naar de Start of 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. (Optioneel) Controleer of er een paar toetsen aanwezig zijn. Bewaar desgewenst de configuratie van het Nexus-apparaat en herladen van het apparaat. Controleer, nadat het Nexus-apparaat weer online komt, of het SSH-sleutelpaar gekoppeld blijft aan de foo-gebruikersaccount.

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

Probleemoplossing

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- "Het configureren van SSH en telnet" hoofdstuk van Cisco Nexus 9000 Series NX-OS security configuratiegids:
  - release 9.3(x)
  - release 9.2(x)
  - release 7.x
- Cisco Nexus 9000 Series NX-OS programmeerbaarheidsgids:
  - release 9.x
  - release 7.x
  - release 6.x
- Cisco Nexus 3600 Series NX-OS programmeerbaarheidsgids:
  - release 9.x
  - release 7.x
- Cisco Nexus 3500 Series NX-OS programmeerbaarheidsgids:
  - release 9.x
  - release 7.x
  - release 6.x
- Cisco Nexus 3000 Series NX-OS programmeerbaarheidsgids:
  - release 9.x
  - release 7.x
  - release 6.x
- Programmeerbaarheid en automatisering met Cisco Open NX-OS
- Technische ondersteuning en documentatie – Cisco Systems