Konfigurieren der kennwortlosen SSH-Dateikopie für AAA-authentifizierte Benutzerkonten auf Cisco Nexus 9000-Geräten

Inhalt

Einführung

Dieses Dokument beschreibt die Verwendung eines öffentlichen und privaten SSH-Schlüsselpaars zum Konfigurieren der SSH-Funktion für das Kopieren von Dateien ohne Kennworteingabe für Cisco Nexus 9000-Benutzerkonten, die mit AAA-Protokollen (Authentication, Authorization, and Accounting - Authentifizierung durch RADIUS und TACACS+) authentifiziert werden.

Voraussetzungen

Anforderungen

- Die Bash-Shell muss auf dem Cisco Nexus-Gerät aktiviert werden. Anweisungen zum Aktivieren der Bash-Shell finden Sie im Abschnitt "Accessing Bash" (Zugriff auf Bash) im Kapitel "Bash" im Cisco Nexus NX-OS-Programmierhandbuch der Serie 9000.
- Sie müssen dieses Verfahren von einem Benutzerkonto ausführen, das die Rolle "network-admin" besitzt.
- Sie müssen über ein vorhandenes öffentliches und privates SSH-Schlüsselpaar verfügen, um zu importieren.**Hinweis**: Die Vorgehensweise zum Generieren eines öffentlichen und privaten SSH-Schlüsselpaars ist plattformabhängig und nicht Bestandteil dieses Dokuments.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Nexus 9000-Plattform NX-OS 7.0(3)I7(6) oder höher

- Nexus 3000-Plattform NX-OS 7.0(3)I7(6) oder höher

Diese Software dient als SCP-/SFTP-Server:

- CentOS 7 Linux x86_64

Die Informationen in diesem Dokument wurden von Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen von Befehlen verstehen.

Hintergrundinformationen

Im Kapitel "Konfigurieren von SSH und Telnet" des Cisco Nexus NX-OS Security Configuration Guide der Serie 9000 wird beschrieben, wie die Funktion "SSH Passwordless File Copy" für Benutzerkonten konfiguriert wird, die mithilfe der NX-OS-Konfiguration auf Cisco Nexus-Geräten erstellt wurden. Mit dieser Funktion kann ein lokales Benutzerkonto SSH-basierte Protokolle wie Secure Copy Protocol (SCP) und Secure FTP (SFTP) verwenden, um Dateien von einem Remote-Server auf das Nexus-Gerät zu kopieren. Dieses Verfahren funktioniert jedoch nicht wie erwartet für Benutzerkonten, die über ein AAA-Protokoll wie RADIUS oder TACACS+ authentifiziert werden. Bei Ausführung auf AAA-authentifizierten Benutzerkonten besteht das öffentliche und private SSH-Schlüsselpaar nicht, wenn das Gerät aus irgendeinem Grund neu geladen wird. Dieses Dokument veranschaulicht ein Verfahren, mit dem ein öffentliches und privates SSH-Schlüsselpaar in ein AAA-authentifiziertes Benutzerkonto importiert werden kann, sodass das Schlüsselpaar beim erneuten Laden erhalten bleibt.

Konfigurieren

Konfigurieren der Funktion zum Kopieren von Dateien ohne SSH-Kennwort für AAA-authentifizierte Benutzerkonten

Bei diesem Verfahren wird "foo" verwendet, um den Namen eines AAA-authentifizierten Benutzerkontos darzustellen. Wenn Sie die Anweisungen in diesem Verfahren befolgen, ersetzen Sie "foo" durch den tatsächlichen Namen des AAA-authentifizierten Benutzerkontos, das Sie für die Verwendung mit der SSH Passwort less File Copy-Funktion konfigurieren möchten.

1. Aktivieren Sie die Bash-Shell, wenn sie nicht bereits aktiviert ist.
   ```
   N9K(config)# feature bash-shell
   ```
   Hinweis: Diese Aktion führt zu keiner Störung.
2. Geben Sie die Bash-Shell ein, und überprüfen Sie, ob das Benutzerkonto "foo" bereits vorhanden ist. Falls vorhanden, löschen Sie das "foo"-Benutzerkonto.
   ```
   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
```

Hinweis: In Bash wird das "foo"-Benutzerkonto nur erstellt, wenn sich das "foo"-Benutzerkonto seit dem letzten Neustart des Geräts per Fernzugriff beim Nexus-Gerät angemeldet hat. Wenn sich das "foo"-Benutzerkonto vor kurzem nicht beim Gerät angemeldet hat, ist es möglicherweise nicht in der Ausgabe der in diesem Schritt verwendeten Befehle vorhanden. Wenn das Benutzerkonto "foo" in der Ausgabe der Befehle nicht vorhanden ist, fahren Sie mit Schritt 3 fort.

3. Erstellen Sie das "foo"-Benutzerkonto in der Bash-Shell.

```
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. Fügen Sie das "foo"-Benutzerkonto zur Gruppe "network-admin" hinzu. **Hinweis**: Auf diese Weise kann das "foo"-Benutzerkonto Dateien in den Bootflash schreiben, was für die Verwendung von SSH-basierten Protokollen (wie SCP und SFTP) zum Durchführen einer Dateikopie erforderlich ist.
```
root@N9K# usermod -a -G network-admin foo
```

5. Beenden Sie die Bash-Shell, und überprüfen Sie, ob die Konfiguration für das "foo"-Benutzerkonto in der NX-OS-Konfiguration vorhanden ist.
```
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
```

   Vorsicht: Wenn Sie das "foo"-Benutzerkonto nicht wie in Schritt 4 beschrieben zur Gruppe "network-admin" hinzugefügt haben, wird in der NX-OS-Konfiguration weiterhin angezeigt, dass das "foo"-Benutzerkonto die Rolle "network-admin" übernimmt. Das "foo"-Benutzerkonto ist jedoch aus Linux-Sicht nicht tatsächlich Mitglied der "network-admin"-Gruppe und kann keine Dateien in den Bootflash des Nexus-Geräts schreiben. Um dieses Problem zu vermeiden, stellen Sie sicher, dass Sie das "foo"-Benutzerkonto zur Gruppe "network-admin" hinzugefügt haben, wie in Schritt 4 beschrieben, und vergewissern Sie sich, dass das "foo"-Benutzerkonto zur Gruppe "network-admin" in der Bash-Shell hinzugefügt wird.**Hinweis**: Obwohl die obige Konfiguration in NX-OS vorhanden ist, handelt es sich bei diesem Benutzerkonto *nicht* um ein lokales Benutzerkonto. Sie können sich bei diesem Benutzerkonto nicht als lokales Benutzerkonto anmelden, selbst wenn das Gerät von AAA-Servern (RADIUS/TACACS+) getrennt ist.
6. Kopieren Sie das öffentliche und das private SSH-Schlüsselpaar von einem Remote-Standort in den Bootflash des Nexus-Geräts. **Hinweis**: Bei diesem Schritt wird davon ausgegangen, dass das öffentliche und das private SSH-Schlüsselpaar bereits vorhanden sind. Die Vorgehensweise zum Generieren eines öffentlichen und privaten SSH-Schlüsselpaars ist plattformabhängig und nicht Bestandteil dieses Dokuments.**Hinweis**: In diesem Beispiel hat der öffentliche SSH-Schlüssel den Dateinamen "foo.pub" und der private SSH-Schlüssel den Dateinamen "foo". Der Remote-Standort ist ein SFTP-Server mit der Adresse 192.0.2.10, der über das Management Virtual Routing and Forwarding (VRF) erreichbar ist.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. Importieren Sie das gewünschte öffentliche und private SSH-Schlüsselpaar für dieses Konto.

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

Überprüfen

Befolgen Sie dieses Verfahren, um die Funktion "SSH Passwordless File Copy" (SSH-Kennwortloses Kopieren von Dateien für AAA-authentifizierte Benutzerkonten) zu überprüfen.

1. Überprüfen Sie, ob das SSH-Schlüsselpaar erfolgreich in das "foo"-Benutzerkonto importiert wurde.

```
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. Bestätigen Sie, dass Sie das SSH-Schlüsselpaar des "foo"-Benutzerkontos verwenden können, um Dateien von einem Remote-Server zu kopieren. **Hinweis**: In diesem Beispiel wird ein SFTP-Server verwendet, auf den im Verwaltungs-VRF unter 192.0.2.10 zugegriffen werden kann, wobei der öffentliche Schlüssel des Benutzerkontos "foo" als autorisierter Schlüssel hinzugefügt wird. Dieser SFTP-Server hat eine Datei "text.txt", die sich im absoluten Pfad **/home/foo/test.txt** befindet.

```
[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. Bestätigen Sie, dass Sie beim "foo"-Benutzerkonto angemeldet sind. anschließend versuchen Sie, die Datei "test.txt" vom zuvor erwähnten SFTP-Server zu kopieren. Beachten Sie, dass der Nexus nicht zur Eingabe eines Kennworts auffordert, um sich beim SFTP-Server anzumelden und die Datei in den Bootflash des Nexus zu übertragen.

```
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. (Optional) Überprüfen Sie die Persistenz des Schlüsselpaars. Speichern Sie auf Wunsch die Konfiguration des Nexus-Geräts, und laden Sie das Gerät neu. Wenn das Nexus-Gerät wieder online ist, stellen Sie sicher, dass das SSH-Schlüsselpaar weiterhin dem "foo"-Benutzerkonto zugeordnet ist.

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

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Kapitel "Konfigurieren von SSH und Telnet" des Cisco Nexus NX-OS Security Configuration Guide der Serie 9000:
  - Version 9.3(x)
  - Version 9.2(x)
  - Version 7.x
- Cisco Nexus NX-OS der Serie 9000 - Programmierhandbuch:
  - Version 9.x
  - Version 7.x
  - Version 6.x
- Cisco Nexus NX-OS der Serie 3600 - Programmierhandbuch:
  - Version 9.x
  - Version 7.x
- Cisco Nexus NX-OS der Serie 3500 - Programmierhandbuch:
  - Version 9.x
  - Version 7.x
  - Version 6.x
- Cisco Nexus NX-OS der Serie 3000 - Programmierhandbuch:
  - Version 9.x
  - Version 7.x
  - Version 6.x
- Programmierbarkeit und Automatisierung mit Cisco Open NX-OS
- Technischer Support und Dokumentation - Cisco Systems