Configuración de SSH Passwordless File Copy for AAA-Authenticated User Accounts on Cisco Nexus 9000 Devices

Contenido

Introducción

Este documento describe cómo utilizar un par de claves públicas y privadas SSH para configurar la función SSH Passwordless File Copy para cuentas de usuario Cisco Nexus 9000 autenticadas con protocolos de autenticación, autorización y contabilidad (AAA) (como RADIUS y TACACS+).

Prerequisites

Requirements

- El shell Bash debe estar habilitado en el dispositivo Cisco Nexus. Consulte la sección "Acceso a la memoria flash" del capítulo Bash de la Guía de programabilidad de Cisco Nexus serie 9000 NX-OS para obtener las instrucciones para habilitar el shell Bash.
- Debe realizar este procedimiento desde una cuenta de usuario que tenga la función "administrador de red".
- Debe tener un par de claves SSH público y privado existente para importar.**Nota:** El procedimiento para generar un par de claves públicas y privadas de SSH depende de la plataforma y está fuera del alcance de este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Plataforma Nexus 9000 NX-OS versión 7.0(3)I7(6) o posterior

- Plataforma Nexus 3000 NX-OS versión 7.0(3)I7(6) o posterior

Este software se utilizó para actuar como servidor SCP/SFTP:

- CentOS 7 Linux x86_64

La información de este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. All of the devices used in this document started with a cleared (default) configuration. Si su red está activa, asegúrese de comprender el impacto potencial de cualquier comando.

Antecedentes

El "capítulo "Configuración de SSH y Telnet" de la Guía de Configuración de Seguridad de Cisco Nexus serie 9000 NX-OS describe cómo configurar la función SSH Passwordless File Copy para cuentas de usuario que se crean a través de la configuración de NX-OS en dispositivos Cisco Nexus. Esta función permite que una cuenta de usuario local utilice protocolos basados en SSH, como el protocolo de copia segura (SCP) y el FTP seguro (SFTP), para copiar archivos desde un servidor remoto al dispositivo Nexus. Sin embargo, este procedimiento no funciona como se espera para las cuentas de usuario que se autentican a través de un protocolo AAA, como RADIUS o TACACS+. Cuando se realiza en cuentas de usuario autenticadas AAA, el par de claves públicas y privadas SSH no persistirá si el dispositivo se recarga por cualquier motivo. Este documento muestra un procedimiento que permite importar un par de claves públicas y privadas SSH a una cuenta de usuario autenticada AAA para que el par de claves continúe en la recarga.

Configurar

Configuración de la Función SSH Passwordless File Copy para Cuentas de Usuario Autenticadas AAA

Este procedimiento utiliza "foo" para representar el nombre de una cuenta de usuario autenticada AAA. Cuando siga las instrucciones de este procedimiento, reemplace "foo" por el nombre real de la cuenta de usuario autenticada AAA que desea configurar para su uso con la función SSH Passwordless File Copy .

1. Habilite el shell Bash si aún no está habilitado.
   ```
   N9K(config)# feature bash-shell
   ```
   Nota: Esta acción no es disruptiva.
2. Introduzca el shell de Bash y verifique si la cuenta de usuario "foo" ya existe. Si existe, elimine la cuenta de usuario "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: Dentro de Bash, la cuenta de usuario "foo" se crea sólo si la cuenta de usuario "foo" ha iniciado sesión de forma remota en el dispositivo Nexus desde la última vez que se reinició el dispositivo. Si la cuenta de usuario "foo" no ha iniciado sesión en el dispositivo recientemente, es posible que no esté presente en el resultado de los comandos utilizados en este paso. Si la cuenta de usuario "foo" no está presente en el resultado de los comandos, vaya al Paso 3.

3. Cree la cuenta de usuario "foo" dentro del shell de 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. Agregue la cuenta de usuario "foo" al grupo "network-admin". **Nota:** Esta acción permite que la cuenta de usuario "foo" escriba archivos en la memoria flash de inicialización, que es necesaria para utilizar protocolos basados en SSH (como SCP y SFTP) para realizar una copia del archivo.

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

5. Salga del shell de Bash y confirme que la configuración de la cuenta de usuario "foo" está presente en la configuración de NX-OS en ejecución.

```
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
```

Precaución: Si no ha agregado la cuenta de usuario "foo" al grupo "network-admin" como se indica en el paso 4, la configuración en ejecución de NX-OS seguirá mostrando que la cuenta de usuario "foo" hereda la función "network-admin". Sin embargo, la cuenta de usuario "foo" no es en realidad miembro del grupo "network-admin" desde una perspectiva de Linux, y no podrá escribir archivos en la memoria flash de inicialización del dispositivo Nexus. Para evitar este problema, asegúrese de agregar la cuenta de usuario "foo" al grupo "network-admin" como se indica en el Paso 4 y confirme que la cuenta de usuario "foo" se agrega al grupo "network-admin" dentro del shell de Bash.**Nota:** Aunque la configuración anterior está presente en NX-OS, esta cuenta de usuario *no* es una cuenta de usuario local. No puede iniciar sesión en esta cuenta de usuario como cuenta de usuario local, incluso si el dispositivo está desconectado de cualquier servidor AAA (RADIUS/TACACS+).

6. Copie el par de claves pública y privada de SSH desde una ubicación remota a la memoria flash de inicialización del dispositivo Nexus. **Nota:** Este paso asume que el par de claves pública y privada SSH ya existe. El procedimiento para generar un par de claves públicas y privadas de SSH depende de la plataforma y está fuera del alcance de este documento.**Nota:** En este ejemplo, la clave pública SSH tiene un nombre de archivo de "foo.pub" y la clave privada SSH tiene un nombre de archivo de "foo". La ubicación remota es un servidor SFTP en 192.0.2.10 al que se puede acceder a través de la administración de 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. Importe el par de claves pública y privada SSH deseado para esta cuenta.

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

Verificación

Siga este procedimiento para verificar la función SSH Passwordless File Copy para cuentas de usuario autenticadas por AAA.

1. Verifique que el par de claves SSH se haya importado correctamente a la cuenta de usuario "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
**************************************
```

2. Confirme que puede utilizar el par de claves SSH de la cuenta de usuario "foo" para copiar archivos desde un servidor remoto. **Nota:** Este ejemplo utiliza un servidor SFTP accesible en 192.0.2.10 en el VRF de administración con la clave pública de la cuenta de usuario "foo" agregada como clave autorizada. Este servidor SFTP tiene un archivo "text.txt" presente en la ruta absoluta **/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. Confirme que ha iniciado sesión en la cuenta de usuario "foo"; a continuación, intente copiar el archivo "test.txt" del servidor SFTP mencionado. Observe que Nexus no solicita una contraseña para iniciar sesión en el servidor SFTP y transferir el archivo a la memoria flash de inicialización del 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. (Opcional) Verifique la persistencia del par de claves. Si lo desea, guarde la configuración del dispositivo Nexus y recargue el dispositivo. Después de que el dispositivo Nexus vuelva a estar en línea, verifique que el par de claves SSH siga estando asociado a la cuenta de usuario "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
************************************
```

Resolución de problemas

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Capítulo "Configuración de SSH y Telnet" de la Guía de Configuración de Seguridad de Cisco Nexus serie 9000 NX-OS:
  - Versión 9.3(x)
  - Versión 9.2(x)
  - Versión 7.x
- Guía de programabilidad de Cisco Nexus serie 9000 NX-OS:
  - Versión 9.x
  - Versión 7.x
  - Versión 6.x
- Guía de programabilidad de Cisco Nexus serie 3600 NX-OS:
  - Versión 9.x
  - Versión 7.x
- Guía de programabilidad de Cisco Nexus serie 3500 NX-OS:
  - Versión 9.x
  - Versión 7.x
  - Versión 6.x
- Guía de programabilidad de Cisco Nexus serie 3000 NX-OS:
  - Versión 9.x
  - Versión 7.x
  - Versión 6.x
- Capacidad de programación y automatización con Cisco Open NX-OS
- Soporte Técnico y Documentación - Cisco Systems