Configurer la copie de fichier sans mot de passe SSH pour les comptes d'utilisateurs authentifiés AAA sur les périphériques Cisco Nexus 9000

Contenu

Introduction

Ce document décrit comment utiliser une paire de clés publiques et privées SSH pour configurer la fonctionnalité de copie de fichier sans mot de passe SSH pour les comptes d'utilisateurs Cisco Nexus 9000 authentifiés avec les protocoles AAA (Authentication, Authorization, and Accounting) (tels que RADIUS et TACACS+).

Conditions préalables

Conditions requises

- Le shell Bash doit être activé sur le périphérique Cisco Nexus. Reportez-vous à la section « Accéder à Bash » du chapitre Bash du Guide de programmabilité NX-OS de la gamme Cisco Nexus 9000 pour obtenir les instructions d'activation du shell Bash.
- Vous devez effectuer cette procédure à partir d'un compte d'utilisateur qui détient le rôle « network-admin ».
- Vous devez avoir une paire de clés publiques et privées SSH existante à importer.**Note**: La procédure de génération d'une paire de clés publiques et privées SSH dépend de la plate-forme et n'entre pas dans le cadre de ce document.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Plate-forme NX-OS version 7.0(3)I7(6) ou ultérieure du Nexus 9000

- Plate-forme NX-OS version 7.0(3)I7(6) ou ultérieure de la plate-forme Nexus 3000

Ce logiciel a été utilisé comme serveur SCP/SFTP :

- CentOS 7 Linux x86_64

Les informations contenues dans ce document ont été créées à partir des périphériques dans un environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est actif, assurez-vous de bien comprendre l'impact potentiel de toutes les commandes.

Informations générales

Le chapitre Configuration de SSH et de Telnet du Guide de configuration de la sécurité NX-OS de la gamme Cisco Nexus 9000 décrit comment configurer la fonctionnalité de copie de fichier sans mot de passe SSH pour les comptes d'utilisateurs créés par le biais de la configuration NX-OS sur les périphériques Cisco Nexus. Cette fonctionnalité permet à un compte d'utilisateur local d'utiliser des protocoles basés sur SSH tels que Secure Copy Protocol (SCP) et Secure FTP (SFTP) pour copier des fichiers d'un serveur distant vers le périphérique Nexus. Cependant, cette procédure ne fonctionne pas comme prévu pour les comptes d'utilisateurs authentifiés via un protocole AAA, tel que RADIUS ou TACACS+. Lorsqu'elle est exécutée sur des comptes d'utilisateurs authentifiés AAA, la paire de clés publiques et privées SSH ne persistera pas si le périphérique est rechargé pour une raison quelconque. Ce document montre une procédure qui permet d'importer une paire de clés publiques et privées SSH dans un compte d'utilisateur authentifié AAA de sorte que la paire de clés persiste lors du rechargement.

Configuration

Configurer la fonction de copie de fichier sans mot de passe SSH pour les comptes d'utilisateurs authentifiés AAA

Cette procédure utilise « foo » pour représenter le nom d'un compte utilisateur authentifié AAA. Lorsque vous suivez les instructions de cette procédure, remplacez « foo » par le nom réel du compte d'utilisateur authentifié AAA que vous souhaitez configurer pour une utilisation avec la fonction de copie de fichier sans mot de passe SSH.

1. Activez le shell Bash s'il n'est pas déjà activé.
   ```
   N9K(config)# feature bash-shell
   ```
   Note: Cette action est sans interruption.
2. Entrez le shell Bash et vérifiez si le compte utilisateur « foo » existe déjà. S'il existe, supprimez le compte utilisateur « 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
```

Note: Dans Bash, le compte utilisateur « foo » est créé uniquement si le compte utilisateur « foo » s'est connecté à distance au périphérique Nexus depuis le dernier redémarrage du périphérique. Si le compte utilisateur “ foo ” n'est pas connecté au périphérique récemment, il se peut qu'il ne figure pas dans le résultat des commandes utilisées dans cette étape. Si le compte utilisateur foo n'est pas présent dans le résultat des commandes, passez à l'étape 3.

3. Créez le compte utilisateur « foo » dans l'interpréteur de commandes 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. Ajoutez le compte utilisateur « foo » au groupe « network-admin ». **Note**: Cette action permet au compte d'utilisateur « foo » d'écrire des fichiers dans le bootflash, qui est nécessaire pour utiliser des protocoles basés sur SSH (tels que SCP et SFTP) pour effectuer une copie de fichier.
```
root@N9K# usermod -a -G network-admin foo
```

5. Quittez le shell Bash et vérifiez que la configuration du compte utilisateur « foo » est présente dans la configuration en cours de NX-OS.
```
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
```

Attention : Si vous n'avez pas ajouté le compte d'utilisateur « foo » au groupe « network-admin » comme indiqué à l'étape 4, alors la configuration en cours de NX-OS montrera toujours que le compte d'utilisateur « foo » hérite du rôle « network-admin ». Cependant, le compte d'utilisateur « foo » n'est pas en fait membre du groupe « network-admin » du point de vue de Linux, et il ne sera pas en mesure d'écrire des fichiers sur le bootflash du périphérique Nexus. Pour éviter ce problème, assurez-vous d'avoir ajouté le compte d'utilisateur « foo » au groupe « network-admin » comme indiqué à l'étape 4 et confirmez que le compte d'utilisateur « foo » est ajouté au groupe « network-admin » dans l'interpréteur de commandes Bash.**Note**: Même si la configuration ci-dessus est présente dans NX-OS, ce compte d'utilisateur *n*'est *pas* un compte d'utilisateur local. Vous ne pouvez pas vous connecter à ce compte d'utilisateur en tant que compte d'utilisateur local, même si le périphérique est déconnecté d'un serveur AAA (RADIUS/TACACS+).

6. Copiez la paire de clés publiques et privées SSH d'un emplacement distant vers le bootflash du périphérique Nexus. **Note**: Cette étape suppose que la paire de clés publiques et privées SSH existe déjà. La procédure de génération d'une paire de clés publiques et privées SSH dépend de la plate-forme et n'entre pas dans le cadre de ce document.**Note**: Dans cet exemple, la clé publique SSH a un nom de fichier « foo.pub » et la clé privée SSH a un nom de fichier « foo ». L'emplacement distant est un serveur SFTP à l'adresse 192.0.2.10 accessible via le VRF (Virtual Routing and Forwarding) de gestion.
```
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. Importez la paire de clés publique et privée SSH souhaitée pour ce compte.

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

Vérification

Suivez cette procédure pour vérifier la fonctionnalité de copie de fichier sans mot de passe SSH pour les comptes d'utilisateurs authentifiés AAA.

1. Vérifiez que la paire de clés SSH a bien été importée dans le compte utilisateur « 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. Confirmez que vous pouvez utiliser la paire de clés SSH du compte d'utilisateur « foo » pour copier des fichiers à partir d'un serveur distant. **Note**: Cet exemple utilise un serveur SFTP accessible à l'adresse 192.0.2.10 dans le VRF de gestion avec la clé publique du compte d'utilisateur « foo » ajoutée en tant que clé autorisée. Ce serveur SFTP a un fichier « text.txt » présent sur le chemin absolu **/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. Confirmez que vous êtes connecté au compte utilisateur « foo » ; puis essayez de copier le fichier « test.txt » à partir du serveur SFTP mentionné ci-dessus. Observez que le Nexus n'invite pas un mot de passe à se connecter au serveur SFTP et à transférer le fichier vers le bootflash du 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. (Facultatif) Vérifiez la persistance de la paire de clés. Si vous le souhaitez, enregistrez la configuration du périphérique Nexus et rechargez-le. Une fois le périphérique Nexus remis en ligne, vérifiez que la paire de clés SSH continue d'être associée au compte utilisateur « 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
**********************************
```

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Chapitre « Configuring SSH and Telnet » du Guide de configuration de la sécurité NX-OS de la gamme Cisco Nexus 9000 :
  - Version 9.3(x)
  - Version 9.2(x)
  - Version 7.x
- Guide de programmabilité NX-OS de la gamme Cisco Nexus 9000 :
  - Version 9.x
  - Version 7.x
  - Version 6.x
- Guide de programmabilité NX-OS de la gamme Cisco Nexus 3600 :
  - Version 9.x
  - Version 7.x
- Guide de programmabilité NX-OS de la gamme Cisco Nexus 3500 :
  - Version 9.x
  - Version 7.x
  - Version 6.x
- Guide de programmabilité NX-OS de la gamme Cisco Nexus 3000 :
  - Version 9.x
  - Version 7.x
  - Version 6.x
- Programmabilité et automatisation avec Cisco Open NX-OS
- Support et documentation techniques - Cisco Systems