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

Contents

Introduction

This document describes how to use an SSH public and private key pair to configure the SSH Passwordless File Copy feature for Cisco Nexus 9000 user accounts that are authenticated with Authentication, Authorization, and Accounting (AAA) protocols (such as RADIUS and TACACS+).

Prerequisites

Requirements

- The Bash shell must be enabled on the Cisco Nexus device. Refer to the "Accessing Bash" section of the Bash chapter in the Cisco Nexus 9000 Series NX-OS Programmability Guide for the instructions to enable the Bash shell.
- You must perform this procedure from a user account that holds the "network-admin" role.
- You must have an existing SSH public and private key pair to import.**Note**: The procedure to generate an SSH public and private key pair is platform-dependent and is outside the scope of this document.

Components Used

The information in this document is based on these software and hardware versions:

- Nexus 9000 platform NX-OS Release 7.0(3)I7(6) or later
- Nexus 3000 platform NX-OS Release 7.0(3)I7(6) or later

This software was used to act as an SCP/SFTP server:

- CentOS 7 Linux x86_64

The information in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any commands.

Background Information

The "Configuring SSH and Telnet" chapter of the Cisco Nexus 9000 Series NX-OS Security Configuration Guide describes how to configure the SSH Passwordless File Copy feature for user accounts that are created through NX-OS configuration on Cisco Nexus devices. This feature enables a local user account to use SSH-based protocols such as Secure Copy Protocol (SCP) and Secure FTP (SFTP) to copy files from a remote server to the Nexus device. However, this procedure does not work as expected for user accounts that are authenticated via an AAA protocol, such as RADIUS or TACACS+. When performed on AAA-authenticated user accounts, the SSH public and private key pair will not persist if the device is reloaded for any reason. This document demonstrates a procedure that allows an SSH public and private key pair to be imported into an AAA-authenticated user account so that the key pair persists on reload.

Configure

Configure SSH Passwordless File Copy Feature for AAA-Authenticated User Accounts

This procedure uses "foo" to represent the name of an AAA-authenticated user account. When you follow the instructions in this procedure, replace "foo" with the actual name of the AAA-authenticated user account that you want to configure for use with the SSH Passwordless File Copy feature.

1. Enable the Bash shell if it is not enabled already.
   ```
   N9K(config)# feature bash-shell
   ```
   Note: This action is non-disruptive.
2. Enter the Bash shell and verify whether the "foo" user account already exists. If it does exist, delete the "foo" user account.
   ```
   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: Within Bash, the "foo" user account is created only if the "foo" user account has remotely logged in to the Nexus device since the device was last rebooted. If the “foo” user account has not logged in to the device recently, it might not be present in the output of the commands used in this step. If the "foo" user account is not present in the output of the commands, proceed to Step 3.

3. Create the "foo" user account within the 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. Add the "foo" user account to the "network-admin" group. **Note**: This action allows the "foo" user account to write files to the bootflash, which is required in order to use SSH-based protocols (such as SCP and SFTP) to perform a file copy.

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

5. Exit the Bash shell and confirm that the configuration for the "foo" user account is present in the NX-OS running configuration.

```
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
```

   Caution: If you did not add the "foo" user account to the "network-admin" group as directed in Step 4, then the NX-OS running configuration will still show that the "foo" user account inherits the "network-admin" role. However, the "foo" user account is not actually a member of the "network-admin" group from a Linux perspective, and it will not be able to write files to the bootflash of the Nexus device. To avoid this problem, make sure that you added the "foo" user account to the "network-admin" group as directed in Step 4 and confirm that the "foo" user account is added to the "network-admin" group within the Bash shell.**Note**: Even though the above configuration is present in NX-OS, this user account is *not* a local user account. You cannot log in to this user account as a local user account, even if the device is disconnected from any AAA (RADIUS/TACACS+) servers.

6. Copy the SSH public and private key pair from a remote location to the bootflash of the Nexus device. **Note**: This step assumes that the SSH public and private key pair already exists. The procedure to generate an SSH public and private key pair is platform-dependent and is outside the scope of this document.**Note**: In this example, the SSH public key has a filename of "foo.pub" and the SSH private key has a filename of "foo". The remote location is an SFTP server at 192.0.2.10 reachable via the 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. Import the desired SSH public and private key pair for this account.

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

Verify

Follow this procedure to verify the SSH Passwordless File Copy feature for AAA-authenticated user accounts.

1. Verify that the SSH key pair was imported to the "foo" user account successfully.

```
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. Confirm that you can use the "foo" user account's SSH key pair to copy files from a remote server. **Note**: This example uses an SFTP server accessible at 192.0.2.10 in the management VRF with the "foo" user account's public key added as an authorized key. This SFTP server has a "text.txt" file present at the absolute path **/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. Confirm that you are logged in to the "foo" user account; then try to copy the "test.txt" file from the aforementioned SFTP server. Observe that the Nexus does not prompt for a password to log in to the SFTP server and transfer the file to the bootflash of the 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. (Optional) Verify key-pair persistence. If desired, save the configuration of the Nexus device and reload the device. After the Nexus device comes back online, verify that the SSH key pair continues to be associated with the "foo" user account.

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

Troubleshooting

There is currently no specific troubleshooting information available for this configuration.

Related Information

- **"Configuring SSH and Telnet" chapter of Cisco Nexus 9000 Series NX-OS Security Configuration Guide:**
  - **Release 9.3(x)**
  - **Release 9.2(x)**
  - **Release 7.x**
- **Cisco Nexus 9000 Series NX-OS Programmability Guide:**
  - **Release 9.x**
  - **Release 7.x**
  - **Release 6.x**
- **Cisco Nexus 3600 Series NX-OS Programmability Guide:**
  - **Release 9.x**
  - **Release 7.x**
- **Cisco Nexus 3500 Series NX-OS Programmability Guide:**
  - **Release 9.x**
  - **Release 7.x**
  - **Release 6.x**
- **Cisco Nexus 3000 Series NX-OS Programmability Guide:**
  - **Release 9.x**
  - **Release 7.x**
  - **Release 6.x**
- **Programmability and Automation with Cisco Open NX-OS**
- **Technical Support & Documentation - Cisco Systems**