Cisco Nexus 9000 디바이스에서 AAA 인증 사용자 계정에 대한 SSH 비밀번호 없는 파일 복사 구성

목차

소개

이 문서에서는 SSH 공개 및 개인 키 쌍을 사용하여 AAA(Authentication, Authorization, and Accounting) 프로토콜(예: RADIUS 및 TACACS+)로 인증된 Cisco Nexus 9000 사용자 계정에 대한 SSH PasswordLess File Copy 기능을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

- Cisco Nexus 디바이스에서 Bash 셸을 활성화해야 합니다.Bash 셸을 활성화하는 지침은 Cisco Nexus 9000 Series NX-OS 프로그래밍 기능 가이드의 Bash 장에서 "Accesing Bash" 섹션을 참조하십시오.
- "network-admin" 역할이 있는 사용자 계정에서 이 절차를 수행해야 합니다.
- 가져오려면 기존 SSH 공개 및 개인 키 쌍이 있어야 합니다.**참고:**SSH 공개 및 개인 키 쌍을 생성하는 절차는 플랫폼에 따라 달라지며 이 문서의 범위를 벗어납니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Nexus 9000 플랫폼 NX-OS 릴리스 7.0(3)I7(6) 이상
- Nexus 3000 플랫폼 NX-OS 릴리스 7.0(3)I7(6) 이상

이 소프트웨어는 SCP/SFTP 서버 역할을 하는 데 사용되었습니다.

- CentOS 7 Linux x86_64

이 문서의 정보는 특정 랩 환경의 디바이스에서 생성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

배경 정보

Cisco Nexus 9000 Series NX-OS 보안 컨피그레이션 가이드의 "SSH 및 텔넷 구성" 장에서는 Cisco Nexus 디바이스에서 NX-OS 컨피그레이션을 통해 생성된 사용자 계정에 대해 SSH PasswordLess File Copy 기능을 구성하는 방법에 대해 설명합니다.이 기능을 사용하면 로컬 사용자 계정이 SCP(Secure Copy Protocol) 및 SFTP(Secure FTP)와 같은 SSH 기반 프로토콜을 사용하여 원격 서버에서 Nexus 디바이스로 파일을 복사할 수 있습니다.그러나 이 절차는 RADIUS 또는 TACACS+와 같은 AAA 프로토콜을 통해 인증되는 사용자 어카운트에 대해 예상대로 작동하지 않습니다.AAA 인증 사용자 계정에서 수행할 경우 어떤 이유로든 디바이스가 다시 로드되면 SSH 공개 및 개인 키 쌍이 지속되지 않습니다.이 문서에서는 키 쌍이 다시 로드될 때 유지되도록 AAA 인증 사용자 계정으로 SSH 공개 및 개인 키 쌍을 가져올 수 있는 절차를 보여 줍니다.

구성

AAA-Authenticated User Accounts용 SSH PasswordLess File Copy 기능 구성

이 절차에서는 "foo"를 사용하여 AAA 인증 사용자 계정의 이름을 나타냅니다.이 절차의 지침에 따라 "foo"를 SSH PasswordLess File Copy 기능과 함께 사용하도록 구성할 AAA 인증 사용자 계정의 실제 이름으로 대체합니다.

1. Bash 셸이 이미 활성화되어 있지 않은 경우 활성화합니다.
   ```
   N9K(config)# feature bash-shell
   ```
   참고:이 작업은 중단 없이 수행됩니다.
2. Bash 셸을 입력하고 "foo" 사용자 계정이 이미 있는지 확인합니다.있는 경우 "foo" 사용자 계정을 삭제합니다.
   ```
   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
```

참고: Bash 내에서 "foo" 사용자 계정은 디바이스를 마지막으로 재부팅한 후 Nexus 디바이스에 원격으로 로그인한 경우에만 생성됩니다."foo" 사용자 계정이 최근에 디바이스에 로그인하지 않은 경우 이 단계에서 사용된 명령의 출력에 표시되지 않을 수 있습니다.명령 출력에 "foo" 사용자 계정이 없는 경우 3단계로 진행합니다.

3. Bash 셸 내에 "foo" 사용자 계정을 생성합니다.

```
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. "network-admin" 그룹에 "foo" 사용자 계정을 추가합니다. **참고:**이 작업을 수행하면 "foo" 사용자 계정에서 bootflash에 파일을 쓸 수 있습니다. 이는 SCP 및 SFTP와 같은 SSH 기반 프로토콜을 사용하여 파일 복사를 수행하는 데 필요합니다.

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

5. Bash 셸을 종료하고 "foo" 사용자 계정에 대한 컨피그레이션이 NX-OS 실행 컨피그레이션에 있는지 확인합니다.

```
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
```

주의:4단계의 지침에 따라 "network-admin" 그룹에 "foo" 사용자 계정을 추가하지 않은 경우 NX-OS 실행 컨피그레이션은 "foo" 사용자 계정이 "network-admin" 역할을 상속함을 보여줍니다.그러나 "foo" 사용자 계정은 실제로 Linux 관점에서 "network-admin" 그룹의 구성원이 아니며 Nexus 디바이스의 부트플래시에 파일을 쓸 수 없습니다.이 문제를 방지하려면 4단계의 지침에 따라 "network-admin" 그룹에 "foo" 사용자 계정을 추가하고 "foo" 사용자 계정이 Bash 셸 내의 "network-admin" 그룹에 추가되었는지 확인합니다.**참고:**위의 컨피그레이션이 NX-OS에 있더라도 이 사용자 어카운트는 로컬 사용자 어카운트가 *아닙니다*.디바이스가 AAA(RADIUS/TACACS+) 서버와 연결이 끊어진 경우에도 이 사용자 계정에 로컬 사용자 계정으로 로그인할 수 없습니다.

6. SSH 공개 및 개인 키 쌍을 원격 위치에서 Nexus 디바이스의 부트플래시로 복사합니다. **참고:**이 단계에서는 SSH 공개 및 개인 키 쌍이 이미 있다고 가정합니다.SSH 공개 및 개인 키 쌍을 생성하는 절차는 플랫폼에 따라 달라지며 이 문서의 범위를 벗어납니다.**참고:**이 예에서는 SSH 공개 키의 파일 이름은 "foo.pub"이고 SSH 개인 키의 파일 이름은 "foo"입니다. 원격 위치는 관리 VRF(Virtual Routing and Forwarding)를 통해 192.0.2.10에 연결할 수 있는 SFTP 서버입니다.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. 이 계정에 대해 원하는 SSH 공개 및 개인 키 쌍을 가져옵니다.

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

다음을 확인합니다.

AAA 인증 사용자 계정에 대한 SSH PasswordLess File Copy 기능을 확인하려면 다음 절차를 수행합니다.

1. SSH 키 쌍을 "foo" 사용자 계정으로 성공적으로 가져왔는지 확인합니다.

```
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. "foo" 사용자 계정의 SSH 키 쌍을 사용하여 원격 서버에서 파일을 복사할 수 있는지 확인합니다. **참고:**이 예에서는 관리 VRF에서 192.0.2.10에서 액세스할 수 있는 SFTP 서버를 사용하며, "foo" 사용자 계정의 공개 키가 권한 있는 키로 추가되었습니다.이 SFTP 서버에는 절대 경로 /home/foo/test.txt에 "text.txt" 파일이 **있습니다**.

```
[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. "foo" 사용자 계정에 로그인했는지 확인합니다.그런 다음 앞서 언급한 SFTP 서버에서 "test.txt" 파일을 복사해 보십시오.Nexus에서 SFTP 서버에 로그인하고 파일을 Nexus의 부트 플래시에 전송할 비밀번호를 묻는 메시지를 표시하지 않습니다.

```
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. (선택 사항) 키 쌍 지속성을 확인합니다. 필요한 경우 Nexus 디바이스의 컨피그레이션을 저장

하고 디바이스를 다시 로드합니다.Nexus 디바이스가 다시 온라인 상태가 된 후 SSH 키 쌍이 "foo" 사용자 계정과 계속 연결되어 있는지 확인합니다.

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

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- Cisco Nexus 9000 Series NX-OS 보안 컨피그레이션 설명서의 "SSH 및 텔넷 구성" 장:
  - 릴리스 9.3(x)
  - 릴리스 9.2(x)

    - 릴리스 7.x
- Cisco Nexus 9000 Series NX-OS 프로그래밍 기능 가이드:
    - 릴리스 9.x
    - 릴리스 7.x
    - 릴리스 6.x
- Cisco Nexus 3600 Series NX-OS 프로그래밍 기능 가이드:
    - 릴리스 9.x
    - 릴리스 7.x
- Cisco Nexus 3500 Series NX-OS 프로그래밍 기능 가이드:
    - 릴리스 9.x
    - 릴리스 7.x
    - 릴리스 6.x
- Cisco Nexus 3000 Series NX-OS 프로그래밍 기능 가이드:
    - 릴리스 9.x
    - 릴리스 7.x
    - 릴리스 6.x
- Cisco Open NX-OS를 통한 프로그래밍 기능 및 자동화
- 기술 지원 및 문서 – Cisco Systems