Configurar a cópia do arquivo sem senha SSH para contas de usuário autenticadas por AAA em dispositivos Cisco Nexus 9000

Contents

Introduction

Este documento descreve como usar um par de chaves públicas e privadas SSH para configurar o recurso de Cópia de Arquivo Sem Senhas SSH para contas de usuário do Cisco Nexus 9000 autenticadas com protocolos de Autenticação, Autorização e Contabilidade (AAA - Authentication, Authorization, and Accounting) (como RADIUS e TACACS+).

Prerequisites

Requirements

- O shell Bash deve estar ativado no dispositivo Cisco Nexus. Consulte a seção "Access Bash" do capítulo Bash no Cisco Nexus 9000 Series NX-OS Programmability Guide para obter instruções sobre como ativar o shell Bash.
- Você deve executar este procedimento a partir de uma conta de usuário que tenha a função "network-admin".
- Você deve ter um par de chaves públicas e privadas SSH existente para importar.**Note**: O procedimento para gerar um par de chaves públicas e privadas do SSH depende da plataforma e está fora do escopo deste documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Plataforma NX-OS Nexus 9000 versão 7.0(3)I7(6) ou posterior

- Plataforma NX-OS Nexus 3000 versão 7.0(3)I7(6) ou posterior

Este software foi usado para atuar como um servidor SCP/SFTP:

- CentOS 7 Linux x86_64

As informações apresentadas neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. All of the devices used in this document started with a cleared (default) configuration. Se a sua rede estiver ativa, certifique-se de que você entende o impacto potencial de qualquer comando.

Informações de Apoio

O capítulo "Configurando SSH e Telnet" do Guia de Configuração de Segurança do Cisco Nexus 9000 Series NX-OS descreve como configurar o recurso de Cópia de Arquivo Sem Senhas SSH para contas de usuário criadas através da configuração do NX-OS em dispositivos Cisco Nexus. Esse recurso permite que uma conta de usuário local use protocolos baseados em SSH, como o protocolo de cópia segura (SCP) e o FTP seguro (SFTP) para copiar arquivos de um servidor remoto para o dispositivo Nexus. No entanto, esse procedimento não funciona como esperado para contas de usuário autenticadas através de um protocolo AAA, como RADIUS ou TACACS+. Quando executado em contas de usuário autenticadas por AAA, o par de chaves públicas e privadas do SSH não persistirá se o dispositivo for recarregado por qualquer motivo. Este documento demonstra um procedimento que permite que um par de chaves públicas e privadas SSH seja importado em uma conta de usuário autenticada por AAA para que o par de chaves persista durante o recarregamento.

Configurar

Configurar o recurso de cópia de arquivo sem senha SSH para contas de usuário autenticadas por AAA

Este procedimento usa "foo" para representar o nome de uma conta de usuário autenticada por AAA. Ao seguir as instruções neste procedimento, substitua "foo" pelo nome real da conta de usuário autenticada AAA que você deseja configurar para uso com o recurso de Cópia de arquivo sem senha SSH.

1. Ative o shell Bash se ele ainda não estiver ativado.
   ```
   N9K(config)# feature bash-shell
   ```
   Note: Esta ação não causa interrupções.
2. Insira o shell Bash e verifique se a conta de usuário "foo" já existe. Se existir, exclua a conta de usuário "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: Em Bash, a conta de usuário "foo" é criada somente se a conta de usuário "foo" tiver feito logon remotamente no dispositivo Nexus desde a última reinicialização do dispositivo. Se a conta de usuário "foo" não tiver feito login no dispositivo recentemente, ela pode não estar presente na saída dos comandos usados nesta etapa. Se a conta de usuário "foo" não estiver presente na saída dos comandos, vá para a Etapa 3.

3. Crie a conta de usuário "foo" no shell 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. Adicione a conta de usuário "foo" ao grupo "network-admin". **Note**: Esta ação permite que a conta de usuário "foo" grave arquivos no flash de inicialização, o que é necessário para usar protocolos baseados em SSH (como SCP e SFTP) para executar uma cópia de arquivos.
```
root@N9K# usermod -a -G network-admin foo
```

5. Saia do shell Bash e confirme se a configuração para a conta de usuário "foo" está presente na configuração atual do 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
```

   Caution: Se você não adicionou a conta de usuário "foo" ao grupo "network-admin", como instruído na Etapa 4, a configuração atual do NX-OS ainda mostrará que a conta de usuário "foo" herda a função "network-admin". No entanto, a conta de usuário "foo" não é, na verdade, um membro do grupo "network-admin" sob a perspectiva do Linux e não poderá gravar arquivos no flash de inicialização do dispositivo Nexus. Para evitar esse problema, certifique-se de ter adicionado a conta de usuário "foo" ao grupo "network-admin", conforme instruído na Etapa 4, e confirme se a conta de usuário "foo" foi adicionada ao grupo "network-admin" no shell Bash.**Note**: Embora a configuração acima esteja presente no NX-OS, essa conta de usuário *não* é uma conta de usuário local. Não é possível iniciar sessão nesta conta de utilizador como uma conta de utilizador local, mesmo que o dispositivo esteja desligado de qualquer servidor AAA (RADIUS/TACACS+).
6. Copie o par de chaves públicas e privadas SSH de um local remoto para o flash de inicialização do dispositivo Nexus. **Note**: Esta etapa supõe que o par de chaves públicas e privadas do SSH já existe. O procedimento para gerar um par de chaves públicas e privadas do SSH depende da plataforma e está fora do escopo deste documento.**Note**: Neste exemplo, a chave pública SSH tem um nome de arquivo "foo.pub" e a chave privada SSH tem um nome de arquivo "foo". O local remoto é um servidor SFTP em 192.0.2.10 acessível através do Virtual Routing and Forwarding (VRF) de gerenciamento.
```
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. Importar o par de chaves públicas e privadas SSH desejado para esta conta.

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

Verificar

Siga este procedimento para verificar o recurso Cópia de arquivo sem senha SSH para contas de usuário autenticadas por AAA.

1. Verifique se o par de chaves SSH foi importado para a conta de usuário "foo" com êxito.

```
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 se você pode usar o par de chaves SSH da conta de usuário "foo" para copiar arquivos de um servidor remoto. **Note**: Este exemplo usa um servidor SFTP acessível em 192.0.2.10 no VRF de gerenciamento com a chave pública da conta de usuário "foo" adicionada como uma chave autorizada. Este servidor SFTP tem um arquivo "text.txt" presente no caminho absoluto **/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 se você está conectado à conta de usuário "foo"; em seguida, tente copiar o arquivo "test.txt" do servidor SFTP acima. Observe que o Nexus não solicita uma senha para

fazer login no servidor SFTP e transferir o arquivo para o flash de inicialização do 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 a persistência do par de chaves. Se desejar, salve a configuração do dispositivo Nexus e recarregue o dispositivo. Depois que o dispositivo Nexus voltar a ficar on-line, verifique se o par de chaves SSH continua associado à conta de usuário "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
************************************
```

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Capítulo "Configurando SSH e Telnet" do Guia de Configuração de Segurança do Cisco Nexus 9000 Series NX-OS:
  - Versão 9.3(x)
  - Versão 9.2(x)
  - Versão 7.x
- Guia de programabilidade do Cisco Nexus 9000 Series NX-OS:
  - Versão 9.x
  - Versão 7.x
  - Versão 6.x
- Guia de programabilidade do Cisco Nexus 3600 Series NX-OS:
  - Versão 9.x
  - Versão 7.x
- Guia de programabilidade do Cisco Nexus 3500 Series NX-OS:
  - Versão 9.x
  - Versão 7.x
  - Versão 6.x
- Guia de programabilidade do Cisco Nexus 3000 Series NX-OS:
  - Versão 9.x
  - Versão 7.x
  - Versão 6.x
- Programabilidade e automação com o Cisco Open NX-OS
- Suporte Técnico e Documentação - Cisco Systems