O SSH em NX-OS comuta usando a autenticação Chave-baseada

Índice

Introdução

Este documento descreve como ao ssh no switch de dados Multilayer de Cisco (MDS) 9000 ou Series Switch do nexo sem ser alertado para uma senha do usuário do Shell Seguro (ssh).

Você pode usar o ssh com autenticação chave-baseada e executar comandos de modo que não haja nenhuma solicitação da senha.

comando de **username@switch do ssh do switch#**

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Server com aplicativo do ssh que é atual

Componentes Utilizados

A informação neste documento é baseada em um servidor Linux com versão do ssh:

$ do **ssh - v**
OpenSSH_5.0p1-hpn13v1, OpenSSL 0.9.8d 28 de setembro de 2006

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

Para permitir esta característica execute por favor estas etapas:

Etapa 1. O SSH precisa de ser permitido no interruptor MDS/Nexus.

```
#conf
(config)#feature ssh
```

Etapa 2. Você precisa de obter a chave pública fora do host e de configurar-la no interruptor MDS/Nexus.

Opções:

- v: Verboso permitido

- b: Número de bit para a chave

- t: Tipo do algoritmo DSA ou RSA

```
$ ssh-keygen -v -b 1024 -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/users/thteoh/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /users/thteoh/.ssh/id_rsa.
Your public key has been saved in /users/thteoh/.ssh/id_rsa.pub.
The key fingerprint is:
61:18:ad:14:cd:a7:bf:44:89:73:4a:2e:09:96:bb:51 thteoh@people
```

> Nota: Neste exemplo, o RSA é usado, você pode igualmente escolher a chave do Digital Signature Algorithm (DSA).

Verify gerou o gato de utilização chave com arquivo id_rsa.pub (o arquivo pode igualmente ser id_dsa.pub)

```
$ cat id_rsa.pub
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAzDWrMuGDkDXFRnuCqdJRM9Yd+oi0ff2K6HxRsyqh82GmQJ3IX6OG7obiQTKnT9+eH7h2
WCArEiMsOz3GYtakEkpYx6zR3cKwrsrgKv4TwRgSv8yUyH8GwPZOvZP97szJDu/3WP/ni4wJBb+yDqoI6+G1Rq/F2aYx45fh
6SwlPv0= thteoh@people
```

Etapa 3. Transfira o arquivo id_rsa.pub (ou id_dsa.pub) ao diretório do bootflash do interruptor MDS/Nexus e configurar a chave pública do ssh.

Neste SFTP examble é usado para transferir id_rsa.pub no interruptor MDS

```
#copy sftp:  bootflash
```

Para transferir o arquivo no Switches do nexo inclua o **vrf no** comando.

Chave da etapa 4.Generate SSH no interruptor usando o **id_rsa.pub ou o** id_dsa.pub**.**

para o username do *teoh da* referência usado.

```
#conf
(config)#username teoh sshkey file bootflash:id_rsa.pub
```

Etapa 5. Você pode comando de verificação terminado com sucesso.

```
switch# show user-account teoh
user:teoh
this user account has no expiry date
```

```
roles:network-admin
ssh public key: ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAzDWrMuGDkDXFRnuCqdJRM9Yd+oi0ff2K6HxRsyqh82GmQJ3IX6OG7o
biQTKnT9+eH7h2WCArEiMsOz3GYtakEkpYx6zR3cKwrsrgKv4TwRgSv8yUyH8GwPZOvZP97szJDu/3WP/ni4wJBb+yDqoI6+
G1Rq/F2aYx45fh6Swl
Pv0= thteoh@people
switch#
```

Verificar

Você pode ssh comutar e emitir agora agora o comando any sem solicitação da senha:

```
$ ssh teoh@10.66.78.53 "sh system uptime"
Warning: the output may not have all the roles
System start time: Tue May 29 17:51:30 2012
System uptime: 7 days, 19 hours, 42 minutes, 15 seconds
Kernel uptime: 7 days, 19 hours, 45 minutes, 17 seconds
```