

SSH en switches NX-OS mediante autenticación basada en clave

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Verificación](#)

Introducción

Este documento describe cómo enviar a los switches Cisco Multilayer Data Switch (MDS) 9000 o Nexus Series sin que se le pida una contraseña de usuario de Secure Shell (SSH).

Puede utilizar ssh con autenticación basada en clave y ejecutar comandos para que no haya avisos de contraseña.

comando `switch# ssh username@switch`

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Servidor con la aplicación ssh actual

Componentes Utilizados

La información en este documento se basa en un servidor Linux con versión ssh:

```
$ ssh -v
```

```
OpenSSH_5.0p1-hpn13v1, OpenSSL 0.9.8d 28 de septiembre de 2006
```

The information in this document was created from the 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 command.

Configurar

Para activar esta función, siga estos pasos:

Paso 1. SSH debe estar habilitado en el switch MDS/Nexus.

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

Paso 2. Debe sacar la clave pública del host y configurarla en el switch MDS/Nexus.

Opciones:

-v: Verbose habilitado

-b: Número de bits para la clave

-t: Tipo de algoritmo ya sea DSA o 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: En este ejemplo, se utiliza RSA, también puede elegir la clave Digital Signature Algorithm (DSA).

Verifique la clave generada utilizando cat con el archivo id_rsa.pub (el archivo también puede ser id_dsa.pub)

```
$ cat id_rsa.pub
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAzDWrMuGDkDXFRnuCqdJRM9Yd+oi0ff2K6HxRsyqh82GmQJ3IX6OG7obiQTKnT9+eH7h2
WCArEiMsOz3GYtakEkpYx6zR3cKwrsrgKv4TwRgSv8yUyH8GwPZOvZP97szJDdu/3WP/ni4wJBb+yDqoI6+G1Rq/F2aYx45fh
6SwlPv0= thteoh@people
```

Paso 3. Transfiera el archivo id_rsa.pub (o id_dsa.pub) al directorio bootflash del switch MDS/Nexus y configure la clave pública ssh.

En este ejemplo, SFTP se utiliza para transferir id_rsa.pub en el switch MDS

```
#copy sftp: bootflash
```

Para transferir el archivo en los switches Nexus, incluya vrf en el comando.

Paso 4. Genere la clave SSH en el switch usando id_rsa.pub o id_dsa.pub.

para referencia *teoh* nombre de usuario utilizado.

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

Paso 5. Puede comprobar que el comando se ha completado correctamente.

```
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#
```

Verificación

Ahora puede enviar a switch y ejecutar cualquier comando sin mensaje de contraseña:

```
$ 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
```