SSH en el Switches NX-OS usando la autenticación Clave-basada

Contenido

Introducción

Este documento describe cómo al ssh en el switch de datos de múltiples capas de Cisco (MDS) 9000 o los switches de la serie del nexo sin ser indicado para una contraseña del usuario del Secure Shell (SSH).

Usted puede utilizar el ssh con la autenticación clave-basada y funcionar con los comandos de modo que no haya prompts de contraseña.

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

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Servidor con la aplicación del ssh que es actual

Componentes Utilizados

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

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

Para habilitar esta característica realice por favor estos pasos:

Paso 1. SSH necesita ser habilitado en el Switch MDS/Nexus.

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

Paso 2. Usted necesita conseguir la clave pública del host y configurarla en el Switch MDS/Nexus.

Opciones:

- v: Habilitado prolijo

- b: Número de bits para la clave

- t: Tipo del algoritmo 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 el RSA, usted puede también elegir la clave del Digital Signature Algorithm (DSA).

Verify generó la clave usando el gato con el archivo id_rsa.pub (el archivo puede también ser id_dsa.pub)

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

Paso 3. La transferencia el archivo id_rsa.pub (o id_dsa.pub) al directorio del bootflash del Switch MDS/Nexus y configura la clave pública del ssh.

En este SFTP examble se utiliza para transferir id_rsa.pub en el Switch MDS

```
#copy sftp:  bootflash
```

Para transferir el archivo en el Switches del nexo incluya el **vrf** en el comando.

Clave del paso 4.Generate SSH en el Switch usando el **id_rsa.pub o el** id_dsa.pub**.**

para el nombre de usuario del *teoh de la* referencia usado.

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

Paso 5. Usted puede comando de control completado con éxito.

```
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

Usted puede ahora ssh conmutar y ahora para publicar el comando any sin el prompt 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
```