

SSH em switches NX-OS usando autenticação baseada em chave

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Verificar](#)

Introduction

Este documento descreve como entrar em switches Cisco Multilayer Data Switch (MDS) 9000 ou Nexus Series sem ser solicitado a fornecer uma senha de usuário Secure Shell (SSH).

Você pode usar ssh com autenticação baseada em chave e executar comandos para que não haja prompts de senha.

comando `switch# ssh username@switch`

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Servidor com aplicativo ssh atual

Componentes Utilizados

As informações neste documento são baseadas em um servidor Linux com a versão ssh:

```
$ ssh -v
```

```
OpenSSH_5.0p1-hpn13v1, OpenSSL 0.9.8d 28 de setembro 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 habilitar esse recurso, execute estas etapas:

Etapa 1. O SSH precisa ser ativado no switch MDS/Nexus.

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

Etapa 2. Você precisa obter a chave pública do host e configurá-la no switch MDS/Nexus.

Opções:

-v : Verbose ativado

-b: Número de bits da chave

-t: Tipo de 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
```

Note: Neste exemplo, RSA é usado, você também pode escolher a chave DSA (Digital Signature Algorithm).

Verifique a chave gerada usando o arquivo cat com id_rsa.pub (o arquivo também pode ser id_dsa.pub)

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

Etapa 3. Transfira o arquivo id_rsa.pub (ou id_dsa.pub) para o diretório bootflash do switch MDS/Nexus e configure a chave pública ssh.

Neste exemplo, o SFTP é usado para transferir id_rsa.pub no switch MDS

```
#copy sftp: bootflash
```

Para transferir arquivos em switches Nexus, inclua vrf no comando.

Etapa 4. Gere a chave SSH no switch usando o id_rsa.pub ou id_dsa.pub.

para referência *teoh* username usado.

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

Etapa 5. Você pode verificar se o comando foi concluído com êxito.

```
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

Agora você pode trocar de ssh para switch e emitir qualquer comando sem o prompt de senha agora:

```
$ 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
```