SSH dans les commutateurs NX-OS à l'aide de l'authentification par clé

Contenu

Introduction

Ce document décrit comment effectuer une ssh dans les commutateurs Cisco MDS (Multilayer Data Switch) 9000 ou Nexus sans qu'un mot de passe utilisateur Secure Shell (SSH) soit demandé.

Vous pouvez utiliser ssh avec une authentification basée sur des clés et exécuter des commandes pour qu'il n'y ait pas d'invite de mot de passe.

switch# ssh username@switch, commande

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Serveur avec application ssh actuelle

Components Used

Les informations de ce document sont basées sur un serveur Linux avec une version ssh :

$ **ssh -v**
OpenSSH_5.0p1-hpn13v1, OpenSSL 0.9.8d 28 sept. 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.

Configuration

Pour activer cette fonctionnalité, procédez comme suit :

Étape 1. SSH doit être activé sur le commutateur MDS/Nexus.

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

Étape 2. Vous devez retirer la clé publique de l'hôte et la configurer sur le commutateur MDS/Nexus.

Options:

-v : Verbose activé

-b : Nombre de bits pour la clé

-t : Type d'algorithme 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**: Dans cet exemple, RSA est utilisé, vous pouvez également choisir la clé DSA (Digital Signature Algorithm).

Vérifier la clé générée à l'aide de cat avec le fichier id_rsa.pub (le fichier peut également être id_dsa.pub)

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

Étape 3. Transférez le fichier id_rsa.pub (ou id_dsa.pub) dans le répertoire bootflash du commutateur MDS/Nexus et configurez la clé publique ssh.

Dans cet exemple, SFTP est utilisé pour transférer id_rsa.pub dans le commutateur MDS

```
#copy sftp:  bootflash
```

Pour transférer un fichier dans les commutateurs Nexus, incluez **vrf** dans la commande.

Étape 4.Générez la clé SSH sur le commutateur à l'aide de **id_rsa.pub** ou **id_dsa.pub**.

pour référence *teoh* nom d'utilisateur utilisé.

```
#conf
```

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

Étape 5. Vous pouvez vérifier que la commande est terminée.

```
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#
```

Vérification

Vous pouvez maintenant envoyer une requête ssh pour basculer et émettre n'importe quelle commande sans invite de mot de passe maintenant :

```
$ 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
```