

SSH in NX-OS-switches met Key-Based Verificatie

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Verifiëren](#)

Inleiding

Dit document beschrijft hoe u de Cisco Multilayer Data Switch (MDS) 9000- of Nexus Series-switches kunt insturen zonder dat dit wordt gevraagd voor een Secure Shell (SSH)-gebruikerswachtwoord.

U kunt ssh gebruiken met op toetsen gebaseerde verificatie en run opdrachten zodat er geen wachtwoordaanwijzingen zijn.

```
schakelaar# ssh username@switch opdracht
```

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Server met SSH-toepassing die momenteel bestaat

Gebruikte componenten

De informatie in dit document is gebaseerd op een Linux-server met ssh versie:

```
$ ssh -v  
OpenSSL_5.0p1-pn13v1, OpenSSL 0.9.8d 28 sep. 2006
```

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

Voer de volgende stappen uit om deze functie te activeren:

Stap 1. SSH moet worden ingeschakeld op de MDS/Nexus-schakelaar.

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

Stap 2. U moet de openbare toets van de host verwijderen en hem op de MDS/Nexus-schakelaar configureren.

Opties:

-v : Ingeschakeld

-b: Aantal bits voor de toets

-t: Type algoritme of DSA of 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
```

Opmerking: In dit voorbeeld, wordt RSA gebruikt, kunt u ook de Digitaal Algorithm (DSA) sleutel kiezen.

Controleer de gegenereerde toets met cat met id_rsa.pub bestand (bestand kan ook id_dsa.pub zijn)

```
$ cat id_rsa.pub
ssh-rsa
AAAAB3NzaC1yc2EAAAABIWAAAIEAzDWrMuGDkDXFRnuCqdJRM9Yd+oi0ff2K6HxRsyqh82GmQJ3IX6OG7obiQTKnT9+eH7h2
WCArEiMsOz3GYtakEkpYx6zR3cKwrsrgKv4TwRgSv8yUyH8GwPZOvZP97szJDu/3WP/ni4wJBb+yDqoI6+G1Rq/F2aYx45fh
6SwlPv0= thteoh@people
```

Stap 3. Breng het bestand id_rsa.pub (of id_dsa.pub) over naar de folder van de MDS/Nexus-schakelaar en stel de ssh openbare toets in.

In dit voorbeeld wordt SFTP gebruikt om id_rsa.pub over te dragen in MDS-switch

```
#copy sftp: bootflash
```

Om bestand in Nexus-switches over te dragen, neemt u vrf in de opdracht op.

Stap 4. Generate SSH op de schakelaar met behulp van de id_rsa.pub of id_dsa.pub.

voor de gebruikte referentietersnaam.

```
#conf
```

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

Stap 5. U kunt de opdracht voltooid controleren.

```
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+eH7h2WCAReiMsOz3GYtakEkpYx6zR3cKwrsrgKv4TwRgSv8yUyH8GwPZOvZP97szJDdu/3WP/ni4wJBb+yDqoI6+
```

```
G1Rq/F2aYx45fh6Swl
```

```
Pv0= thteoh@people
```

```
switch#
```

Verifiëren

U kunt nu overschakelen naar een andere opdracht en elke opdracht uitvoeren zonder wachtwoord te vragen:

```
$ 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
```