# SSH sugli switch NX-OS con autenticazione basata su chiavi

## Sommario



## Introduzione

In questo documento viene descritto come eseguire il protocollo ssh sugli switch Cisco Multilayer Data Switch (MDS) 9000 o Nexus Series senza che venga richiesta una password utente Secure Shell (SSH).

È possibile usare ssh con l'autenticazione basata su chiavi e eseguire i comandi in modo che non vengano richieste password.

**switch# ssh username@switch, comando**

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Server con l'applicazione SSH corrente

### Componenti usati

Le informazioni di questo documento si basano su un server Linux con versione ssh:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Configurazione

Per abilitare questa funzione, effettuare le seguenti operazioni:

Passaggio 1. È necessario abilitare SSH sullo switch MDS/Nexus.

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

Passaggio 2. È necessario rimuovere la chiave pubblica dall'host e configurarla sullo switch MDS/Nexus.

Opzioni:

-v : Modalità dettagliata abilitata

-b: Numero di bit per la chiave

-t: Tipo di 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:** Nell'esempio riportato, viene utilizzato RSA. È inoltre possibile scegliere la chiave DSA (Digital Signature Algorithm).

Verificare la chiave generata utilizzando cat con il file id_rsa.pub (il file può anche essere id_dsa.pub)

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

Passaggio 3. Trasferire il file id_rsa.pub (o id_dsa.pub) nella directory bootflash dello switch MDS/Nexus e configurare la chiave pubblica ssh.

In questo esempio, SFTP viene usato per trasferire id_rsa.pub nello switch MDS

```
#copy sftp:  bootflash
```

Per trasferire il file negli switch Nexus, includere **vrf** nel comando.

Passaggio 4. Generare la chiave SSH sullo switch usando **id_rsa.pub** o **id_dsa.pub**.

per riferimento *teoh* username.

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

Passaggio 5. È possibile verificare se il comando è stato completato correttamente.

```
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#
```

# Verifica

Èquindi possibile eseguire il comando ssh per switch ed eseguire qualsiasi comando senza visualizzare una richiesta della password:

```
$ 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
```