

SSH into NX-OS Switches Using Key-Based Authentication

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Verify](#)

Introduction

This document describes how to ssh into Cisco Multilayer Data Switch (MDS) 9000 or Nexus Series switches without being prompted for a Secure Shell (SSH) user password.

You can use ssh with key-based authentication and run commands so that there are no password prompts.

```
switch# ssh username@switch command
```

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Server with ssh application that is current

Components Used

The information in this document is based on a Linux server with ssh version:

```
$ ssh -v  
OpenSSH_5.0p1-hpn13v1, OpenSSL 0.9.8d 28 Sep 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.

Configure

To enable this feature please perform these steps:

Step 1. SSH needs to be enabled on the MDS/Nexus switch.

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

Step 2. You need to get the public key off the host and configure it on the MDS/Nexus switch.

Options:

-v : Verbose Enabled

-b: Number of Bits for the key

-t: Type of Algorithm either DSA or 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: In this example, RSA is used, you can also choose the Digital Signature Algorithm (DSA) key.

Verify generated key using cat with id_rsa.pub file (file can also be id_dsa.pub)

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

Step 3. Transfer the id_rsa.pub (or id_dsa.pub) file to bootflash directory of the MDS/Nexus switch and configure the ssh public key.

In this example SFTP is used to transfer id_rsa.pub in MDS switch

```
#copy sftp: bootflash
```

To transfer file in Nexus switches include **vrf** in the command.

Step 4. Generate SSH key on the switch using the **id_rsa.pub** or **id_dsa.pub**.

for reference *teoh* username used.

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

Step 5. You can check command completed successfully.

```
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#
```

Verify

You can now ssh to switch and issue any command without password prompt now:

```
$ 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
```