

# 使用基于密钥的身份验证通过SSH连接到NX-OS交换机

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[验证](#)

## 简介

本文档介绍如何在不提示输入安全外壳(SSH)用户密码的情况下通过SSH连接到思科多层数据交换机(MDS)9000或Nexus系列交换机。

您可以将ssh与基于密钥的身份验证和运行命令配合使用，以便不出现密码提示。

```
switch# ssh username@switch命令
```

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- 具有当前SSH应用的服务器

### 使用的组件

本文档中的信息基于具有ssh版本的Linux服务器：

```
$ ssh -v  
OpenSSH_5.0p1-hpn13v1,OpenSSL 0.9.8d 2006年9月28日
```

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

## 配置

要启用此功能，请执行以下步骤：

步骤1.需要在MDS/Nexus交换机上启用SSH。

```
#conf
```

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

步骤2.您需要从主机获取公钥，并在MDS/Nexus交换机上进行配置。

选项:

-v :启用详细

-b:密钥的位数

-t:算法类型DSA或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
```

**注意：**在本例中，使用RSA，您还可以选择数字签名算法(DSA)密钥。

使用带id\_rsa.pub文件的cat验证生成的密钥（文件也可以是id\_dsa.pub）

```
$ cat id_rsa.pub
```

```
ssh-rsa
```

```
AAAAB3NzaC1yc2EAAAABIWAAAIEAzDWrMuGDkDXFRnuCqdJRM9Yd+oi0ff2K6HxRsyqh82GmQJ3IX6OG7obiQTKnT9+eH7h2  
WCAReiMsOz3GYtakEkpYx6zR3cKwrsrgKv4TwRgSv8yUyH8GwPZOvZP97szJDdu/3WP/ni4wJBb+yDqoI6+G1Rq/F2aYx45fh  
6SwlPv0= thteoh@people
```

步骤3.将id\_rsa.pub（或id\_dsa.pub）文件传输到MDS/Nexus交换机的bootflash目录并配置ssh公钥

。

在本示例中，SFTP用于在MDS交换机中传输id\_rsa.pub

```
#copy sftp: bootflash
```

要在Nexus交换机中传输文件，请在命令中包含vrf。

步骤4.使用id\_rsa.pub或id\_dsa.pub在交换机上生成SSH密钥。

供参考使用的用户名。

```
#conf
```

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

步骤5.您可以检查命令是否成功完成。

```
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#
```

## 验证

现在，您可以ssh到交换机并发出任何命令，而无需口令提示：

```
$ 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
```