

キーベース認証を使用したNX-OSスイッチへのSSH

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[確認](#)

概要

このドキュメントでは、セキュアシェル(SSH)ユーザパスワードを要求されずに、Cisco Multilayer Data Switch(MDS)9000またはNexusシリーズスイッチにSSH接続する方法について説明します。

キーベースの認証でsshを使用し、パスワードプロンプトが表示されないようにコマンドを実行できます。

```
switch# ssh username@switchコマンド
```

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 現在のsshアプリケーションを持つサーバ

使用するコンポーネント

このドキュメントの情報は、sshバージョンのLinuxサーバに基づいています。

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

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

設定

この機能を有効にするには、次の手順を実行します。

ステップ1:MDS/NexusスイッチでSSHを有効にする必要があります。

```
#conf
```

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

ステップ2 : ホストから公開キーを取得し、MDS/Nexusスイッチで設定する必要があります。

Options:

-v:詳細が有効

-b:キーのビット数

-t:DSAまたはRSAのいずれかのアルゴリズムのタイプ

```
$ 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 : この例では、RSAを使用して、デジタル署名アルゴリズム(DSA)キーを選択することもできます。

id_rsa.pubファイルを持つcatを使用して、生成されたキーを確認します (ファイルはid_dsa.pubにすることもできます)

```
$ cat id_rsa.pub
```

```
ssh-rsa
```

```
AAAAB3NzaC1yc2EAAAABIwAAAIEAzDWrMuGDkDXFRnuCqdJRM9Yd+oi0ff2K6HxRsyqh82GmQJ3IX6OG7obiQTKnT9+eH7h2  
WCArEiMsOz3GYtakEkpYx6zR3cKwrsrgKv4TwRgSv8yUyH8GwPZOvZP97szJDdu/3WP/ni4wJBb+yDqoI6+G1Rq/F2aYx45fh  
6SwlPv0= thteoh@people
```

ステップ3:id_rsa.pub (またはid_dsa.pub) ファイルをMDS/Nexusスイッチのブートフラッシュディレクトリに転送し、ssh公開キーを設定します。

この例では、MDSスイッチでid_rsa.pubを転送するためにSFTPが使用されています

```
#copy sftp: bootflash
```

Nexusスイッチでファイルを転送するには、コマンドにvrfを含めます。

ステップ4:id_rsa.pubまたはid_dsa.pubを使用してスイッチ上でSSHキーを生成します。

を参照してください。

```
#conf
```

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

ステップ5 : コマンドが正常に完了したことを確認できます。

```
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#
```

確認

これで、スイッチにsshで接続し、パスワードプロンプトなしでコマンドを発行できるようになりました。

```
$ 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
```