SSH サービスの設定

RSA キーによるセキュア SSH 接続は、Cisco MDS 9000 シリーズのすべてのスイッチでデフォルトで使用できます。DSA キーによるセキュア SSH 接続が必要な場合は、デフォルトの SSH 接続をディセーブルにし、DSA キーを生成して、SSH 接続をイネーブルにする必要があります（SSH サーバ キー ペアの生成 （2 ページ）を参照）。

サーバ キーを生成するには、**ssh key** コマンドを使用します。

⚠

注意 SSH でスイッチにログインし、**aaa authentication login default none** コマンドを発行した場合、ログインするために 1 つ以上のキーストロークを入力する必要があります。少なくとも 1 つのキーストロークを入力せずに **Enter** キーを押すと、ログインは拒否されます。

この項では、次のトピックについて取り上げます。

- SSH サービス （1 ページ）
- SSH サーバ キー ペアの生成 （2 ページ）
- SSH キーの指定 （3 ページ）
- 生成したキー ペアの上書き （5 ページ）
- SSH ログイン試行の最大回数の設定 （5 ページ）
- SSH ホストのクリア （6 ページ）
- SSH または Telnet サービスのイネーブル化 （7 ページ）
- SSH プロトコル ステータスの表示 （8 ページ）
- デジタル証明書を使用した SSH 認証 （9 ページ）
- パスワードのないファイル コピーおよび SSH （9 ページ）

SSH サービス

セキュア シェル（SSH）は、Cisco NX-OS CLI に対する安全なリモート接続を可能にするプロトコルです。SSH は、デバイスの認証時に強力な暗号化を行うことで、リモート接続について Telnet 以上のセキュリティを実現します。SSH キーは、次の SSH オプションに使用できます。

- Rivest, Shamir, Adelman（RSA）を使用する SSH2

- DSA を使用する SSH2

Cisco MDS NX-OS リリース 8.2(1) 以降、SHA2 フィンガー プリント ハッシュはすべての Cisco MDS デバイスでデフォルトでサポートされています。

SSH サービスの設定の詳細については、次を参照してください。 SSH サービスの設定 （1 ページ）

SSH サーバ キー ペアの生成

SSH サービスをイネーブルにする前に、適切なバージョンの SSH サーバ キー ペアを取得してください。使用中の SSH クライアント バージョンに従って、SSH サーバ キー ペアを生成します。各キー ペアに指定するビット数は、768 ～ 2048 です。

Cisco MDS NX-OS リリース 8.2(1) 以降、FIPS モードの最小 RSA キー サイズは 2048 ビットである必要があります。

SSH サービスは、SSH バージョン 2 で使用する 2 種類のキー ペアを受け入れます。

- **dsa** オプションでは、SSH バージョン 2 プロトコル用の DSA キー ペアを作成します。
- **rsa** オプションでは、SSH バージョン 2 プロトコル用の RSA キー ペアを作成します。

⚠

注意 SSH キーをすべて削除した場合、新しい SSH セッションを開始できません。

SSH サーバ キー ペアを生成する手順は、次のとおりです。

手順

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **ssh key dsa 1024**

例：

```
generating dsa key.....
generated dsa key
```

DSA サーバ キー ペアを生成します。

ステップ 3 switch(config)# **ssh key rsa 1024**

例：

```
generating rsa key.....
generated rsa key
```

RSA サーバ キー ペアを生成します。

ステップ 4 switch(config)# **no ssh key rsa 1024**

例：

```
cleared RSA keys
```

RSA サーバ キーペアの設定をクリアします。

SSH キーの指定

SSH キーを指定すると、パスワードを要求されることなく、SSH クライアントを使用してログインできます。SSH キーは次の 3 種類の形式で指定できます。

- Open SSH 形式
- Internet Engineering Task Force（IETF）SECSH 形式
- Privacy Enhanced Mail（PEM）形式の公開キー証明書

OpenSSH による SSH キーの指定

指定したユーザの OpenSSH 形式の SSH キーを指定または削除するには、次の手順を実行します。

手順

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **username admin sshkey ssh-rsa**
[illegible]

ユーザ アカウント（admin）の SSH キーを指定します。

ステップ 3 switch(config)# **no username admin sshkey ssh-rsa**
[illegible]

（オプション）ユーザ アカウント（admin）の SSH キーを削除します。

IETF SECSH による SSH キーの指定

指定したユーザの IETF SECSH 形式の SSH キーを指定または削除するには、次の手順を実行します。

手順

ステップ 1 switch# **copy tftp://10.10.1.1/secsh_file.pub bootflash:secsh_file.pub**

IETF SECSH 形式の SSH キーを含むファイルをダウンロードします。

ステップ 2 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 3 switch(config)# **username admin sshkey file bootflash:secsh_file.pub**

ユーザ アカウント（admin）の SSH キーを指定します。

ステップ 4 switch(config)# **no username admin sshkey file bootflash:secsh_file.pub**

（オプション）ユーザ アカウント（admin）の SSH キーを削除します。

PEM の公開キー証明書による SSH キーの指定

指定したユーザの PEM フォーマット化された公開キー証明書形式の SSH キーを指定または削除するには、次の手順を実行します。

手順

ステップ 1 switch# **copy tftp://10.10.1.1/cert.pem bootflash:cert.pem**

PEM フォーマット化された公開キー証明書形式の SSH キーを含むファイルをダウンロードします。

ステップ 2 switch# **configure terminal**

switch(config)#

コンフィギュレーション モードに入ります。

ステップ 3 switch(config)# **username admin sshkey file bootflash:cert.pem**

ユーザ アカウント（usam）の SSH キーを指定します。

ステップ 4 switch(config)# **no username admin sshkey file bootflash:cert.pem**

（オプション）ユーザ アカウント（usam）の SSH キーを削除します。

生成したキー ペアの上書き

必要なバージョンの SSH キー ペア オプションがすでに生成されている場合は、前回生成されたキー ペアをスイッチに上書きさせることができます。

前回生成されたキー ペアを上書きする手順は、次のとおりです。

手順

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **ssh key dsa 768**

例：

```
ssh key dsa 512
dsa keys already present, use force option to overwrite them

switch(config)# ssh key dsa 512 force
deleting old dsa key.....
generating dsa key.....
generated dsa key
```

サーバ キー ペアの設定を試みます。必要なサーバ キー ペアがすでに設定されている場合は、**force** オプションを使用して、そのサーバ キーペアを上書きします。古いDSA キーを削除し、新しく指定されたビットを使用してサーバ キー ペアを設定します。

SSH ログイン試行の最大回数の設定

SSH ログイン試行の最大回数を設定できます。許可される試行の最大回数を超えると、セッションが切断されます。

（注） ログイン試行の合計回数には、公開キー認証、証明書ベースの認証、およびパスワードベースの認証を使用した試行が含まれます。イネーブルにされている場合は、公開キー認証が優先されます。証明書ベースとパスワードベースの認証だけがイネーブルにされている場合は、証明書ベースの認証が優先されます。これらすべての方法で、ログイン試行の設定された数を超えると、認証失敗回数を超過したことを示すメッセージが表示されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ssh login-attempts** *number* 例： `switch(config)# ssh login-attempts 5`	ユーザが SSH セッションへのログインを試行できる最大回数を設定します。ログイン試行のデフォルトの最大回数は3です。値の範囲は 1 ～ 10 です。 （注） このコマンドの **no** 形式を使用すると、以前のログイン試行の値が削除され、ログイン試行の最大回数がデフォルト値の 3 に設定されます。 SSH ログイン試行の値を 2 以上に設定することをお勧めします。
ステップ 3	（任意） **show running-config security all** 例： `switch(config)# show running-config security all`	SSH ログイン試行の設定された最大回数を表示します。
ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

SSH ホストのクリア

clear ssh hosts コマンドは、信頼できる SSH ホストの既存のリストをクリアし、SCP/SFTP を特定のホストの **copy** コマンドとともに使用することを再許可します。

SCP/SFTP を **copy** コマンドとともに使用する場合は、信頼できる SSH ホストのリストが作成され、スイッチ内に保存されます（次の例を参照）。

SCP/SFTP を使用したファイルのコピー

```
switch# copy scp://abcd@10.10.1.1/users/abcd/abc

bootflash:abc The authenticity of host '10.10.1.1 (10.10.1.1)'
```

```
can't be established.
RSA1 key fingerprint is 01:29:62:16:33:ff:f7:dc:cc:af:aa:20:f8:20:a2:db.
Are you sure you want to continue connecting (yes/no)? yes
Added the host to the list of known hosts
(/var/home/admin/.ssh/known_hosts). [SSH key information about the host is
stored on the switch]
abcd@10.10.1.1's password:
switch#
```

SCP/SFTP を使用したファイルのコピー（SSH キーの変更によるエラーの発生）

copy コマンドとともに SCP/SFTP を使用する前にホストの SSH キーが変更された場合は、エラーが表示されます（次の例を参照）。

```
switch# copy scp://apn@10.10.1.1/isan-104

bootflash:isan-ram-1.0.4
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA1 host key has just been changed.
The fingerprint for the RSA1 key sent by the remote host is
36:96:ca:d7:29:99:79:74:aa:4d:97:49:81:fb:23:2f.
Please contact your system administrator.
Add correct host key in /mnt/pss/.ssh/known_hosts to get rid of this
message.
Offending key in /mnt/pss/.ssh/known_hosts:2
RSA1 host key for 10.10.1.1 has changed and you have requested strict
checking.
```

SSH または Telnet サービスのイネーブル化

デフォルトでは、SSH サービスは、RSA キーによってイネーブルになっています。

SSH または Telnet サービスをイネーブルまたはディセーブルにするには、次の手順を実行します。

手順

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **feature ssh**

Updated

SSH サービスの使用を有効にします。

ステップ 3 switch(config)# **no feature ssh**

Updated

（オプション）SSH サービスの使用をディセーブル（デフォルト）にします。

ステップ 4 switch(config)# **feature telnet**

Updated

Telnet サービスの使用をイネーブルにします。

ステップ 5 switch(config)# **no feature telnet**

Updated

（オプション）Telnet サービスの使用をディセーブル（デフォルト）にします。

SSH プロトコル ステータスの表示

SSH プロトコルのステータスの表示

SSH プロトコルのステータス（イネーブルまたはディセーブル）、およびそのスイッチでイネーブルになっているバージョンを表示するには、**show ssh server** コマンドを使用します（次の例を参照）。

```
switch# show ssh server

ssh is enabled
version 1 enabled
version 2 enabled
```

サーバ キーペアの詳細の表示

指定されたキーまたはすべてのキーのサーバ キーペアの詳細を表示するには、**show ssh key** コマンドを使用します（次の例を参照）。

（注） SHA-2 値は安全だと考えられるため、Cisco MDS NX-OS リリース 8.2(1) 以降、show ssh key [rsa | dsa] コマンドの出力に表示されるフィンガープリント値は SHA-2 値になります

```
switch# show ssh key

rsa Keys generated:Thu Feb 16 14:12:21 2017

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQDQ7si46R6sYsWNBRFV+v662vbY6wmr9QMBU4N+BK8F
Iez+7U+2VRdyz1Mykbb1HF/2zth3ZWuTkrTX+8cMnVdcwlfrvWY3g7CLmq5Wkxkq5PiSHsG9pnKM0ubw
Unqc4HYrjEiwJKAR2OBAylfH1ajf7wYGQbOiTQMeMyo2nQK8yQ==

bitcount:1024
fingerprint:
SHA256:D4F+Tl7R3fVunGz9A4GKGLWMQ0r4YRbzf5GfNwy1neg
*************************************
dsa Keys generated:Tue Feb 28 07:47:04 2017
```

```
ssh-dss AAAAB3NzaC1kc3MAAACBAJan5V/6YiKQZG2SCChmn9Mu5EbUQoTuCDyTCIYM35ofzh+dEALU
11XZrkGl7V2Hfbgp57dcTya1gjeNOzwU32oOvbA8osJ3BWpIePkZv+/t0feOz4LUhBz85ccmQeLJQ86R
UeJ6pAFsq+yk4XB/l5qMv9SN/QY0/95gCIDt8Uq7AAAAFQDZUMiLvTZwIwajLdu8OtLfB1vmuwAAAIAE
7rIwgUlrDTqmzvRdrmayYM2cGfwL4x+8gGpGe2kZoedFzv4vmmW2npD0E8qTWs4nD0k7cioTjdgLXQoZ
yaQIpIEtd+qS8NHuCrtRguVuDDCEOMTlhwNwL0iCHm08YgJIR3ho+V/nm5ko4kp7jA5eOh/9P/Rr4hCO
aZBNxPcSewAAAIBhcNhaVDYvEri7JCH8DbiZr30z2P3PpIQ8YWpHcOE7CBXkp++HjMFUKd9HJlIwd4bA
81tTkTfSxkPBc9ocHOv1vusVufj423HFjcBIODixY76gJzqlt3aNs54MDfiYxyJLh6yp6LZffDn4t2HF
x7tZSb4UJQKHdNR05d63Pybdbg==

bitcount:1024
fingerprint:
SHA256:kbHB73ZEhZaqJp/J68f1nfN9pJaQUkdHt0iKJc0c+Ao
```

（注） SSH でスイッチにログインし、**aaa authentication login default none CLI** コマンドを発行した場合、ログインするために 1 つ以上のキーストロークを入力する必要があります。少なくとも 1 つのキーストロークを入力せずに **Enter** キーを押すと、ログインは拒否されます。

デジタル証明書を使用した SSH 認証

Cisco MDS 9000 ファミリ スイッチ製品の SSH 認証はホスト認証に X.509 デジタル証明書のサポートを提供します。X.509 デジタル証明書は出処と完全性を保証する 1 つのデータ項目です。これには安全な通信のための暗号化されたキーが含まれています。また、発信者のアイデンティティを証明するために信頼できる認証局（CA）によって署名されています。X.509 デジタル証明書のサポートにより、認証に DSA と RSA のいずれかのアルゴリズムを使用します。

証明書インフラストラクチャは Secure Socket Layer（SSL）をサポートする最初の証明書を使用し、セキュリティインフラストラクチャにより照会または通知の形で返信を受け取ります。証明書が信頼できる CA のいずれかから発行されたものであれば、証明書の検証は成功です。

スイッチは、X.509 証明書を使用する SSH 認証、または公開キー証明書を使用する SSH 認証のいずれかに設定できますが、両方に設定することはできません。いずれかに設定されている場合は、その認証が失敗すると、パスワードの入力を求められます。

パスワードのないファイル コピーおよび SSH

セキュア シェル（SSH）公開キー認証は、パスワードのないログインを行うために使用できます。SCP および SFTP は SSH をバックグラウンドで使用するため、これらのコピー プロトコルを使用することにより、公開キー認証によるパスワードのないコピーが可能になります。この NX-OS バージョンは、SCP および STFP クライアント機能だけをサポートしています。

SSH による認証に使用できる RSA および DSA ID を作成できます。この ID は、公開キーと秘密キーという 2 つの部分から構成されています。公開キーおよび秘密キーはスイッチによって生成されますが、外部で生成してスイッチにインポートすることもできます。インポートするためには、キーが OPENSSH 形式であることが必要です。

SSH サーバをホストしているホスト マシン上でキーを使用するには、そのマシンに公開キーファイルを転送し、サーバの SSH ディレクトリ（たとえば、$HOME/.ssh）にあるファイル authorized_keys に内容を追加します。秘密キーをインポートおよびエクスポートする場合、キーは暗号化によって保護されます。同一のパスフレーズを入力するように求められます。パスフレーズを入力すると、秘密キーは暗号化によって保護されます。パスワードフィールドを空白のままにしておくと、キーは暗号化されません。

キーを別のスイッチにコピーする必要がある場合は、スイッチからホストマシンにキーをエクスポートし、そのマシンから他のスイッチに同じキーをインポートします。

- キー ファイルは、リブート後も維持されます。

キー ペアをインポートおよびエクスポートするために、次の CLI が提供されます。スイッチで SSH ユーザ キー ペアを生成する CLI コマンドは次のように定義されます。

手順

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **username admin keypair generate rsa**

例：

```
generating rsa key(1024 bits).....
generated rsa key
```

アカウント（admin）の公開および秘密 RSA キーを生成します。その後、指定されたユーザのホーム ディレクトリにキー ファイルを保存します。そのサーバ キー ペアを上書きするには force オプションを使用します。

（注） この例は RSA キーの場合です。DSA キーの場合、rsa を dsa に置き換えます。

ステップ 3 switch(config)# **no username admin keypair generate rsa**

（オプション）アカウント（admin）の公開および秘密 RSA キーを削除します。

ステップ 4 switch# **show username admin keypair**

例：

```
**************************************
rsa Keys generated: Thu Jul 9 11:10:29 2009
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAxWmjJT+oQhIcvnrMbx2BmD
0P8boZElTfJFx9fexWp6rOiztlwODtehnjadWc6A+DE2DvYNvq
srU9TBypYDPQkR/+Y6cKubyFWVxSBG/NHztQc3+QC1zdkIxGNJ
bEHyFoajzNEO8LLOVFIMCZ2Td7gxUGRZc+fbqS33GZsCAX6v0=
bitcount:262144
fingerprint:
8d:44:ee:6c:ca:0b:44:95:36:d0:7d:f2:b5:78:74:7d
**************************************
could not retrieve dsa key information
**************************************
```

アカウント（admin）の公開キーを示します。

ステップ 5 switch(config)# **username admin keypair export bootflash:key_rsa rsa**

例：

```
Enter Passphrase:
switch(config)# dir
 951 Jul 09 11:13:59 2009 key_rsa
 221 Jul 09 11:14:00 2009 key_rsa.pub
```

ユーザ（admin）のホームディレクトリからブートフラッシュ メモリにキー ペアをエクスポートします。

キーペア（公開キーと秘密キー）が指定の場所にエクスポートされます。ユーザは秘密キーを暗号化するパスフレーズを入力するように求められます。秘密キーは uri で指定したファイル名としてエクスポートされ、公開キーは「.pub」拡張子が後に付く同じファイル名でエクスポートされます。

ユーザは任意のスイッチにこのキー ペアをコピーして、さらに SCP サーバのホーム ディレクトリに公開ファイルをコピーできるようになります。

ステップ 6 switch(config)# **username admin keypair import bootflash:key_rsa rsa**

例：

```
Enter Passphrase:
switch(config)# show username admin keypair
**************************************
rsa Keys generated: Thu Jul 9 11:10:29 2009
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAxWmjJT+oQhIcvnrMbx2BmD
0P8boZElTfJFx9fexWp6rOiztlwODtehnjadWc6A+DE2DvYNvq
srU9TBypYDPQkR/+Y6cKubyFWVxSBG/NHztQc3+QC1zdkIxGNJ
bEHyFoajzNEO8LLOVFIMCZ2Td7gxUGRZc+fbqS33GZsCAX6v0=
bitcount:262144
fingerprint:
8d:44:ee:6c:ca:0b:44:95:36:d0:7d:f2:b5:78:74:7d
**************************************
could not retrieve dsa key information
**************************************
```

スイッチのホーム ディレクトリにキー ペアをインポートします。

ここで示す uri は秘密キーの uri であり、公開キーは「.pub」拡張子が付いて同じ場所に存在する必要があります。ユーザはパスフレーズの入力が求められ、キーの暗号化に使用されたのと同じパスフレーズを入力する必要があります。

サーバにパスワードレス コピーをする必要があるスイッチに秘密キーがコピーされ、そのサーバのホーム ディレクトリの authorized_keys ファイルにコピーされた公開キーがある場合、ユーザはスイッチからサーバへのパスワードレス ファイル コピーおよび ssh を実行できます。

（注） サーバの authorized_keys ファイルに公開キーをコピーするのに、ユーザは前述の show コマンドからキーをコピーすることもできます。

ステップ 7 server# **cat key_rsa.pub >> $HOME/.ssh/ authorized_keys**

SCP サーバの authorized_keys ファイルに key_rsa.pub に保存されている公開キーを追加します。標準 ssh と scp コマンドを使用して、スイッチからこのサーバへのパスワードレス ssh および scp が有効になりました。