



SSH サービスおよび Telnet の構成

この章では、Cisco MDS デバイス上でセキュア シェル プロトコル (SSH) サービスおよび Telnet を設定する手順について説明します。

この章は、次の項で構成されています。

- [SSH サービスに関する情報, on page 1](#)
- [Telnet サーバ, on page 3](#)
- [SSH の設定, on page 3](#)
- [SSH のデフォルト設定, on page 16](#)

SSH サービスに関する情報

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

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 サーバー キー ペアの生成, on page 5](#)を参照)。

サーバー キーを生成するには、`ssh key` コマンドを使用します。



Caution 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** を押すと、ログインは拒否されます。

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 サービスおよび Telnet の構成, on page 1](#)

SSH サーバー

SSH サーバを使用すると、SSH クライアントは Cisco MDS デバイスとの間で暗号化された安全な接続を確立できます。SSH は強化暗号化を使用して認証を行います。Cisco MDS NX-OS ソフトウェアの SSH サーバーは、市販の一般的な SSH クライアントと相互運用ができます。

SSH がサポートするユーザ認証メカニズムには、Remote Authentication Dial-In User Service (RADIUS)、TACACS+、LDAP、およびローカルに格納されたユーザ名とパスワードを使用した認証があります。

SSH クライアント

SSH クライアントは、SSH プロトコルで稼働しデバイス認証および暗号化を提供するアプリケーションです。Cisco MDS デバイスは、SSH クライアントを使用して、別の Cisco MDS デバイスまたは SSH サーバの稼働する他のデバイスとの間で暗号化された安全な接続を確立できます。この接続は、暗号化されたアウトバウンド接続を実現します。認証と暗号化により、SSH クライアントは、セキュリティ保護されていないネットワーク上でもセキュアな通信を実現できます。

Cisco NX-OS ソフトウェアの SSH クライアントは、市販の一般的な SSH クライアントと相互運用ができます。

SSH サーバキー

SSH では、Cisco MDS デバイスと安全な通信を行うためにサーバキーが必要です。SSH サーバキーは、次の SSH オプションに使用できます。

- Rivest, Shamir, and Adelman (RSA) 公開キー暗号化を使用した SSH バージョン 2
- Digital System Algorithm (DSA) を使用した SSH バージョン 2

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応じて、SSH サーバキーペアを生成します。SSH サービスは、SSH バージョン 2 で使用する次の 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。

デフォルトでは、Cisco NX-OS ソフトウェアは 1024 ビットの RSA キーを作成します。

SSH は、次の公開キー形式をサポートします。

- OpenSSH
- IETF SSH (SECSH)
- Privacy-Enhanced Mail (PEM) の公開キー証明書



Caution SSH キーをすべて削除すると、SSH サービスを開始できません。

デジタル証明書を使用した SSH 認証

Cisco MDS 9000 ファミリー 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处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。

Telnet サーバ

Telnet プロトコルは、ホストとの TCP/IP 接続を確立します。Telnet を使用すると、あるサイトのユーザが別のサイトのログインサーバと TCP 接続を確立し、キーストロークをデバイス間でやり取りできます。Telnet は、リモート デバイス アドレスとして IP アドレスまたはドメイン名のいずれかを受け入れます。

デフォルトでは、Telnet サーバは Cisco NX-OS デバイス上でディセーブルになっています。

SSH の設定

ここでは、SSH の設定方法について説明します。

SSH 名の構成

ユーザのプライマリ SSH 接続の名前を構成するには、次の手順に従います。

始める前に

機能 SSH を有効にします。

手順

	コマンドまたはアクション	目的
ステップ 1	<pre>switch#ssh name ssh-nameuser-nameip-address</pre> <p>例 :</p> <pre>switch# ssh name myhost user 192.168.1.1</pre>	プライマリ SSH 接続の SSH 名を構成します。
ステップ 2	<pre>switch# no ssh name</pre> <p>例 :</p> <pre>switch# no ssh name myhost user 192.168.1.1</pre>	(オプション) SSH 接続の名前を削除します。
ステップ 3	<pre>switch# show ssh names</pre> <p>例 :</p> <pre>switch# show ssh names</pre>	(オプション) SSH 接続の名前を表示します。

SSH 接続の構成

ユーザーの SSH 接続を構成するには、次の手順に従います。

始める前に

- 機能 SSH を有効にします。
- SSH 名を構成します。SSH 名の設定については、[SSH 名の構成 \(3 ページ\)](#) を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	<pre>switch#ssh connectdummy</pre> <p>例 :</p> <pre>switch# ssh connect myhost</pre>	SSH 名の SSH 接続を構成します。
ステップ 2	<pre>switch# no ssh connect</pre> <p>例 :</p> <pre>switch# no ssh connect myhost</pre>	(オプション) SSH 接続を削除します。
ステップ 3	<pre>switch# show ssh names</pre> <p>例 :</p> <pre>switch# show ssh names</pre>	(オプション) SSH 接続の名前を表示します。

SSH サーバー キー ペアの生成

セキュリティ要件に基づいて SSH サーバキーを生成できます。デフォルトの SSH サーバキーは、1024 ビットで生成される RSA キーです。SSH サービスを確立する前に、SSH サーバキーペアおよび適切なバージョンが存在することを確認します。使用中の SSH クライアントバージョンに従って、SSH サーバー 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。

RSA キー ペアの最大値とデフォルトの詳細については、[\[表 1 CA およびデジタル証明書の最大制限 \(Table 1 Maximum Limits for CA and Digital Certificate\)\]](#) および [\[表 2 デフォルトの CA およびデジタル証明書パラメータ \(Table 2 Default CA and Digital Certificate Parameters\)\]](#) を参照してください。

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。



Caution 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 サーバー キー ペアを生成する手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

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

Example:

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

DSA サーバー キー ペアを生成します。

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

Example:

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

RSA サーバー キー ペアを生成します。

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

Example:

```
cleared RSA keys
```


ステップ 2 switch# **configure terminal**

構成モードに入ります。

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

ユーザー 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) ユーザー 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

指定したユーザーの 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)#

構成モードに入ります。

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

ユーザー 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) ユーザー アカウント (usam) の SSH キーを削除します。

ログイングレイスタイムの SSH コネクションの構成

リモートデバイスから Cisco MDS デバイスへの SSH 接続のログイン猶予時間を設定できます。これにより、クライアントが自身を認証するための猶予時間が構成されます。SSH セッションへのログイン時間が指定された猶予時間を超えると、セッションが切断され、再度ログインする必要があります。



Note リモート デバイスの SSH サーバをイネーブルにします。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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	feature ssh Example: <pre>switch# feature ssh switch(config)#</pre>	SSH を有効にします。
ステップ 3	ssh login-gracetime number Example: <pre>switch(config)# ssh login-gracetime 120</pre>	<p>リモート デバイスから Cisco MDS デバイスへの SSH 接続のログイン猶予時間を秒単位で構成します。SSH がセッションを切断する前に、SSH サーバへの認証が成功するまでの時間を指定します。デフォルトログイン猶予時間は 120 秒です。範囲は 10 ~ 600 です。</p> <p>Note このコマンドの no 形式は、設定されたログイン猶予時間を削除し、デフォルト値の 120 秒にリセットします。</p>
ステップ 4	(Optional) exit Example: <pre>switch(config)# exit</pre>	グローバル コンフィギュレーション モードを終了します。
ステップ 5	(Optional) show running-config security Example: <pre>switch(config)# show running-config security</pre>	構成された SSH ログインの猶予時間を表示します。
ステップ 6	(Optional) show running-config security all Example: <pre>switch(config)# show running-config security all</pre>	構成されたまたはデフォルト SSH ログインの猶予時間を表示します。

	Command or Action	Purpose
ステップ 7	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	(任意) 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 アイドル タイムアウトの構成

ssh idle-timeout コマンドは、SSH セッションが終了するまでの非アクティブ時間を設定します。これにより、忘れられたセッションを閉じることでセッションセキュリティが強化され、スイッチリソースが保持されます。秒単位のタイムアウト期間。

ssh idle-timeout を構成するために、次の手順を使用します。の

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**

サービスを有効にします。

ステップ 3 switch(config)# **ssh idle-timeout 300**

SSH クライアントセッションのアイドルタイムアウトを 300 秒に設定し、キープアライブ試行回数をゼロに構成します（デフォルト：キープアライブは無効）。300 秒間 SSH クライアントからパケットを受信しなかった場合、セッションは即座に終了します。

ステップ 4 switch(config)# **ssh idle-timeout 300 keepalive-count 3**

SSH クライアントセッションのアイドルタイムアウトを 300 秒に、キープアライブカウントを 3 回の試行回数に構成します。これは、セッションが閉じられるまでに SSH クライアントからパケットを受信しなかった場合の $300 \times 3 = 900$ 秒になります。

ステップ 5 switch(config)# **no sshidle-timeout.**

(オプション) SSH クライアントセッションの非アクティブの監視を無効にします（デフォルト）。

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。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

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

Example:

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

サーバー キー ペアの設定を試みます。必要なサーバー 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、そのサーバー 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ー 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。

	コマンドまたはアクション	目的
ステップ 2	ssh login-attempts number 例： <pre>switch(config)# ssh login-attempts 5</pre>	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： <pre>switch(config)# show running-config security all</pre>	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： <pre>switch(config)# copy running-config startup-config</pre>	実行中の構成を、スタートアップ構成にコピーします。

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。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

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

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**

（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**

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**

（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
```

サーバー 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ー 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）。

```
switch# show ssh key
```

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

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQDQ7si46R6sYsWNBRFV+v662vbY6wmr9QMBU4N+BK8F
Iez+7U+2VRdylMykbb1HF/2zth3ZWuTkrTX+8cMnVdcwlfrvWY3g7CLmq5Wkxkq5PiSHsG9pnKM0ubw
Unqc4HYrjEiwJKAR2OBAylfHlajf7wYGQbOiTQMeMyo2nQK8yQ==
```

```
bitcount:1024
fingerprint:
SHA256:D4F+Tl7R3fVunGz9A4GKGLWMQ0r4YRbzf5GfNwylneg
*****
dsa Keys generated:Tue Feb 28 07:47:04 2017
```

```
ssh-dss AAAAB3NzaC1kc3MAAACBAJan5V/6YiKQZG2SCChmn9Mu5EbUQoTuCDyTCIYM35ofzh+dEALU
11XZrkG17V2Hfbgp57dcTyalgjeNOzwU32oOvbA8osJ3BWPiEpkZv+/t0feOz4LUhBz85ccmQeLJQ86R
UeJ6pAFsq+yk4XB/15qMv9SN/QY0/95gCIDt8Uq7AAAAFQDZUMiLvTZwIwajLdu8OtLfBlvmuwAAAIAE
7rIwqUlrDTqmvzRdrmayYM2cGfwL4x+8GpGe2kZoedFzv4vmmW2npD0E8qTws4nD0k7cioTjdgLXQoZ
yaQIpIEtd+qS8NHuCrtrGuVuDDCEOMTlhwNwL0iCHm08YgJIR3ho+V/nm5ko4kp7jA5e0h/9P/Rr4hCO
aZBNxPcSewAAAIbhcNhaVDYvEri7JCH8DbiZr30z2P3PpIQ8YWpHcOE7CBXkp++HjMFUKd9HJlIwd4bA
81tTkTfSxkPbc9ocHOv1vusVufj423HFjcbIODixY76gJzqlt3aNs54MDfiYxyJLh6yp6LZffDn4t2HF
x7tZSb4UJQKHdNR05d63Pybdbg==
```

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



Note 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。

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せん。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 SFTP 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 OPENSSSH 形式であることが必要です。

SSH サーバー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送り、サーバーの 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。同一のパスワードを入力するように求められます。パスワードを入力すると、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 ユーザー 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。

Procedure

ステップ 1 switch# **configure terminal**

構成モードに入ります。

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

Example:

```
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、指定されたユーザーのホームディレクトリにキーファイルを保存します。そのサーバー キーペアを上書きするには `force` オプションを使用します。

Note

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**Example:**

```
*****
rsa Keys generated: Thu Jul 9 11:10:29 2009
ssh-rsa
AAAAB3NzaC1yc2EAAAABIWAAAIEAxWmjJT+oQhIcvnrMbx2BmD
0P8boZE1TfJF9x9fexWp6rOiztlwODtehnjadWc6A+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**Example:**

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

ユーザー (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。ユーザー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。

ユーザー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 サーバーのホーム 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**Example:**

```
Enter Passphrase:
switch(config)# show username admin keypair
*****
rsa Keys generated: Thu Jul 9 11:10:29 2009
ssh-rsa
AAAAB3NzaC1yc2EAAAABIWAAAIEAxWmjJT+oQhIcvnrMbx2BmD
0P8boZE1TfJF9x9fexWp6rOiztlwODtehnjadWc6A+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。ユーザーはパスワードの入力が求められ、キーの暗号化に使用されたのと同じパスワードを入力する必要があります。

サーバーにパスワードレス 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、そのサーバーのホーム 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、ユーザーはスイッチからサーバー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。

Note

サーバーの `authorized_keys` ファイルに公開キーをコピーするのに、ユーザーは前述の `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 サーバーの `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ーへのパスワードレス `ssh` および `scp` が有効になりました。

SSH のデフォルト設定

次の表に、SSH パラメータのデフォルト設定を示します。

Table 1: デフォルトの SSH パラメータ

パラメータ	デフォルト
SSH サーバ	イネーブル
SSH サーバ キー	1024 ビットで生成された RSA キー
RSA キー生成ビット数	1024
SSH ログインの最大試行回数	3
SCP サーバ	ディセーブル
SFTP サーバ	無効化

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。