SSH および Telnet の設定

この章は、次の項で構成されています。

SSH および Telnet の設定

SSH および Telnet の概要

SSH サーバー

セキュア シェル（SSH）プロトコル サーバー機能を使用すると、SSH クライアントは Cisco Nexus デバイスとの間で、セキュアな暗号化された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 Nexus デバイス スイッチの SSH サーバーは、無償あるいは商用の SSH クライアントと連係して動作します。

SSH がサポートするユーザー認証メカニズムには、RADIUS、TACACS+、およびローカルに格納されたユーザー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 クライアント機能は、SSH プロトコルを介して実行されるアプリケーションで、認証と暗号化を行います。SSH クライアントを使用すると、スイッチは、別の Cisco Nexus デバイス スイッチとの間、または SSH サーバーを稼働している他の任意のデバイスとの間でセキュアな暗号化された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 Nexus デバイスの SSH クライアントは、無償あるいは商用の SSH サーバーと連係して動作します。

SSH サーバ キー

SSH では、Cisco Nexus デバイスとのセキュアな通信を行うためにサーバー キーが必要です。SSH 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 Algrorithm（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 サービスでは、SSH バージョン 2 に対応する 2 とおりのキー ペアを使用できます。

- dsa オプションを使用すると、SSH バージョン 2 プロトコルに対応する DSA キーペアが生成されます。
- rsa オプションを使用すると、SSH バージョン 2 プロトコルに対応する RSA キーペアが生成されます。

デフォルトでは、Cisco Nexus デバイスは 1024 ビットの RSA キーを生成します。

SSH は、次の公開キー形式をサポートします。

- OpenSSH
- IETF SSH（SECSH）

⚠

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。

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ーが別サイトのログイン サーバーとの TCP 接続を確立して、システム間でキーストロークをやり取りできます。Telnet は、リモート システムのアドレスとして、IP アドレスまたはドメイン名を受け取ります。

Cisco Nexus デバイスでは、デフォルトで Telnet サーバーがイネーブルになっています。

SSH の注意事項および制約事項

SSH には、次の注意事項および制限事項があります。

- Cisco Nexus デバイスは、SSH バージョン 2（SSHv2）だけをサポートしています。
- SSH パスワードレス ファイル コピーを目的として AAA プロトコル（RADIUS や TACACS+ など）を介してリモート認証されたユーザ アカウントにインポートされた SSH 公開キーと秘密キーは、同じ名前のローカル ユーザ アカウントでない限り、Nexus デバイスがリロードされると保持されません。リモート ユーザ アカウントは、SSH キーがインポートされる前にデバイスで設定されます。

SSH の設定

SSH サーバ キーの生成

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。

Procedure

	Command or Action	Purpose
ステップ 1	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	switch(config)# **ssh key** {**dsa** [**force**] | **rsa** [*bits* [**force**]]}	SSH サーバー キーを生成します。 *bits* 引数には、キーの生成に使用するビット数を指定します。有効な範囲は 768 ～ 2048 です。デフォルト値は 1024 です。 既存のキーを置き換える場合は、キーワード **force** を使用します。
ステップ 3	switch(config)# **exit**	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 4	(Optional) switch# **show ssh key**	SSH サーバー キーを表示します。
ステップ 5	(Optional) switch# **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。

Example

次に、SSH サーバー キーを生成する例を示します。

```
switch# configure terminal
switch(config)# ssh key rsa 2048
switch(config)# exit
switch# show ssh key
switch# copy running-config startup-config
```

ユーザ アカウント用 SSH 公開キーの指定

SSH 公開キーを設定すると、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 公開キーは、次の 3 種類のいずれか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

Open SSH 形式による SSH 公開キーの指定

ユーザー アカウント用に SSH 形式で SSH 公開キーを指定できます。

Procedure

	Command or Action	Purpose
ステップ 1	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	switch(config)# **username** *username* **sshkey** *ssh-key*	SSH形式でSSH公開キーを設定します。
ステップ 3	switch(config)# **exit**	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 4	(Optional) switch# **show user-account**	ユーザー アカウントの設定を表示します。
ステップ 5	(Optional) switch# **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。

Example

次に、Open SSH 形式で SSH 公開キーを指定する例を示します。

```
switch# configure terminal
switch(config)# username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAri3mQy4W1AV9Y2t2hrEWgbUEYz
CfTPO5B8LRkedn56BEy2N9ZcdpqE6aqJLZwfZcTFEzaAAZp9AS86dgBAjsKGs7UxnhGySr8ZELv+DQBsDQH6rZt0KR+2Da8hJD4Z
XIeccWk0gS1DQUNZ300xstQsYZUtqnx1bvm5Ninn0McNinn0Mc=
switch(config)# exit
switch# show user-account
switch# copy running-config startup-config
```

Note 上記の例の **username** コマンドは、読みやすくするために改行されていますが、単一行です。

IETF SECSH 形式による SSH 公開キーの指定

ユーザー アカウント用に IETF SECSH 形式で SSH 公開キーを指定できます。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **copy** *server-file* **bootflash:** *filename*	サーバーから 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。File Transfer Protocol（FTP）、SCP、SSH File Transfer Protocol（SFTP）、または Trivial File Transfer Protocol（TFTP）サーバーを利用できます。
ステップ 2	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 3	switch(config)# **username** *username* **sshkey file** *filename*	SSH形式でSSH公開キーを設定します。
ステップ 4	switch(config)# **exit**	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) switch# **show user-account**	ユーザー アカウントの設定を表示します。
ステップ 6	(Optional) switch# **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。

Example

次に、IETF SECSH 形式で SSH 公開キーを指定する例を示します。

```
switch#copy tftp://10.10.1.1/secsh_file.pub bootflash:secsh_file.pub
switch# configure terminal
switch(config)# username User1 sshkey file bootflash:secsh_file.pub
switch(config)# exit
switch# show user-account
switch# copy running-config startup-config
```

PEM フォーマット化された公開キー証明書形式による SSH 公開キーの指定

ユーザー アカウント用に PEM フォーマット化された公開キー証明書形式で SSH 公開キーを指定できます。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **copy** *server-file* **bootflash:** *filename*	サーバーから 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。

	Command or Action	Purpose
		FTP、SCP、SFTP、または TFTP サーバーを利用できます。
ステップ 2	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 3	(Optional) switch# **show user-account**	ユーザー アカウントの設定を表示します。
ステップ 4	(Optional) switch# **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。

Example

次に、PEM フォーマット化された公開キー証明書形式で SSH 公開キーを指定する例を示します。

```
switch# copy tftp://10.10.1.1/cert.pem bootflash:cert.pem
switch# configure terminal
switch# show user-account
switch# copy running-config startup-config
```

リモート デバイスとの SSH セッションの開始

Cisco Nexus デバイスからリモート デバイスに接続する SSH セッションを開始できます。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **ssh** {*hostname* | *username@hostname*} [**vrf** *vrf-name*]	リモート デバイスとの SSH セッションを作成します。引数 *hostname* には、IPv4 アドレスまたはホスト名を指定します。

SSH ホストのクリア

SCP または SFTP を使用してサーバーからファイルをダウンロードする場合は、サーバーと信頼性のある SSH 関係を確立します。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **clear ssh hosts**	SSH ホストセッションをクリアします。

SSH サーバのディセーブル化

SSH サーバーは、デフォルトでCisco Nexus デバイスでイネーブルになっています。

Procedure

	Command or Action	Purpose
ステップ 1	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	switch(config)# **[no] feature ssh**	SSH サーバーをイネーブル/ディセーブルにします。デフォルトではイネーブルになっています。
ステップ 3	switch(config)# **exit**	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 4	(Optional) switch# **show ssh server**	SSH サーバーの設定を表示します。
ステップ 5	(Optional) switch# **copy running-config startup-config**	実行設定を、スタートアップ設定にコピーします。

SSH サーバ キーの削除

SSH サーバーをディセーブルにした後、SSH サーバー キーを削除できます。

Note SSHを再度イネーブルにするには、まず、SSHサーバー キーを生成する必要があります。

Procedure

	Command or Action	Purpose
ステップ 1	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	switch(config)# **no feature ssh**	SSHサーバーをディセーブルにします。
ステップ 3	switch(config)# **no ssh key** [**dsa** | **rsa**]	SSH サーバ キーを削除します。 デフォルトでは、すべての SSH キーが削除されます。
ステップ 4	switch(config)# **exit**	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) switch# **show ssh key**	SSH サーバーの設定を表示します。

	Command or Action	Purpose
ステップ 6	(Optional) switch# **copy running-config startup-config**	実行設定を、スタートアップ設定にコピーします。

SSH セッションのクリア

Cisco Nexus デバイスから SSH セッションをクリアできます。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **show users**	ユーザーセッション情報を表示します。
ステップ 2	switch# **clear line** *vty-line*	ユーザSSHセッションをクリアします。

SSH の設定例

次に、SSH を設定する例を示します。

Procedure

ステップ 1 SSH サーバ キーを生成します。

```
switch(config)# ssh key rsa
generating rsa key(1024 bits).....
.
generated rsa key
```

ステップ 2 SSH サーバをイネーブルにします。

```
switch# configure terminal
switch(config)# feature ssh
```

Note SSHサーバーはデフォルトでイネーブルになっているため、この手順は必要ありません。

ステップ 3 SSH サーバー キーを表示します。

```
switch(config)# show ssh key
rsa Keys generated:Fri May  8 22:09:47 2009

ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAri3mQy4W1AV9Y2t2hrEWgbUEYzCfTPO5B8LRkedn56BEy2N9ZcdpqE6aqJLZwfZ/
cTFEzaAAZp9AS86dgBAjsKGs7UxnhGySr8ZELv+DQBsDQH6rZt0KR+2Da8hJD4ZXIeccWk0gS1DQUNZ300xstQsYZUtqnx1bvm5/
```

```
Ninn0Mc=

bitcount:1024
fingerprint:
4b:4d:f6:b9:42:e9:d9:71:3c:bd:09:94:4a:93:ac:ca
*************************************
could not retrieve dsa key information
*************************************
```

ステップ 4 Open SSH 形式による SSH 公開キーを指定します。

```
switch(config)# username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAri3mQy4W1AV9Y2t2hrEWgbUEYz
CfTPO5B8LRkedn56BEy2N9ZcdpqE6aqJLZwfZcTFEzaAAZp9AS86dgBAjsKGs7UxnhGySr8ZELv+DQBsDQH6rZt0KR+2Da8hJD4Z
XIeccWk0gS1DQUNZ300xstQsYZUtqnx1bvm5Ninn0McNinn0Mc=
```

ステップ 5 設定を保存します。

```
switch(config)# copy running-config startup-config
```

Telnet の設定

Telnet サーバのイネーブル化

デフォルトでは、Telnet サーバーはイネーブルに設定されています。Cisco Nexus デバイスの Telnet サーバーをディセーブルにできます。

Procedure

	Command or Action	Purpose
ステップ 1	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	switch(config)# **[no] feature telnet**	Telnet サーバーをイネーブル/ディセーブルにします。デフォルトではイネーブルになっています。

Telnet サーバーの再イネーブル化

Cisco Nexus デバイスの Telnet サーバーがディセーブルにされた場合は、再度イネーブルにできます。

Procedure

	Command or Action	Purpose
ステップ 1	switch(config)# **[no] feature telnet**	Telnet サーバーを再度イネーブルにします。

リモート デバイスとの Telnet セッションの開始

Telnetセッションを開始してリモートデバイスに接続する前に、次の作業を行う必要があります。

- リモートデバイスのホスト名を取得します。必要に応じて、リモートデバイスのユーザー名も取得します。
- Cisco Nexus デバイス上で Telnet サーバーをイネーブルにします。
- リモート デバイス上で Telnet サーバーをイネーブルにします。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **telnet** *hostname*	リモート デバイスとの Telnet セッションを作成します。引数 *hostname* には、IPv4 アドレスまたはデバイス名を指定します。

Example

次に、Telnet セッションを開始してリモート デバイスに接続する例を示します。

```
switch# telnet 10.10.1.1
Trying 10.10.1.1...
Connected to 10.10.1.1.
Escape character is '^]'.
switch login:
```

Telnet セッションのクリア

Cisco Nexus デバイスから Telnet セッションをクリアできます。

Procedure

	Command or Action	Purpose
ステップ 1	switch# **show users**	ユーザーセッション情報を表示します。
ステップ 2	switch# **clear line** *vty-line*	ユーザ Telnet セッションをクリアします。

SSH および Telnet の設定の確認

SSH の設定情報を表示するには、次のいずれかの作業を行います。

Procedure

- switch# **show ssh key** [**dsa** | **rsa**]

コマンドまたはアクション	目的
switch# **show running-config security**[**all**]	実行コンフィギュレーション内の SSH とユーザ アカウントの設定を表示します。**all** キーワードを指定すると、SSH およびユーザー アカウントのデフォルト値が表示されます。
switch# **show ssh server**	SSH サーバーの設定を表示します。
switch# **show user-account**	ユーザー アカウント情報を表示します。

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
Telnet サーバ	有効（Enabled）

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。