CatOS が稼働しているCatalyst スイッチ での SSH の設定方法

内容

概要

このドキュメントでは、Catalyst OS（CatOS）が稼働している Catalyst スイッチで Secure Shell（SSH）バージョン 1 を設定する手順について説明しています。 テストされたバージョンは cat6000-supk9.6-1-1c.bin です。

前提条件

要件

次の表に、各スイッチでの SSH のサポート状況を示します。登録済みユーザは、Software Center でこれらのソフトウェア イメージにアクセスできます。

CatOS SSH	
デバイス	SSH サポート

Cat 4000/4500/2948G/2980G（CatOS）	6.1 時点の K9 イメージ
Cat 5000/5500（CatOS）	6.1 時点の K9 イメージ
Cat 6000/6500（CatOS）	6.1 時点の K9 イメージ
IOS SSH	
デバイス	**SSH サポート**
Cat 2950*	12.1(12c)EA1 以降
Cat 3550*	12.1(11)EA1 以降
Cat 4000/4500（統合 Cisco IOS ソフトウェア）*	12.1(13)EW 以降 **
Cat 6000/5500（統合 Cisco IOS ソフトウェア）*	12.1(11b)E 以降
Cat 8540/8510	12.1(12c)EY 以降、12.1(14)E1 以降
SSH なし	
デバイス	**SSH サポート**
Cat 1900	no
Cat 2800	no
Cat 2948G-L3	no
Cat 2900XL	no
Cat 3500XL	no
Cat 4840G-L3	no
Cat 4908G-L3	no

* 設定については「Cisco IOS を実行するルータおよびスイッチのセキュア シェルの設定」で説明しています。

** 統合 Cisco IOS ソフトウェアが稼働する Catalyst 4000 の 12.1E トレインでは SSH はサポートされません。

3DES の申し込みについては、「Encryption Software Export Distribution Authorization Form」を参照してください。

このドキュメントでは、（Telnet パスワード TACACS+ を介して）SSH または RADIUS を実装する前に、認証が機能していることを前提としています。SSH を実装するまでは、SSH with Kerberos はサポートされません。

使用するコンポーネント

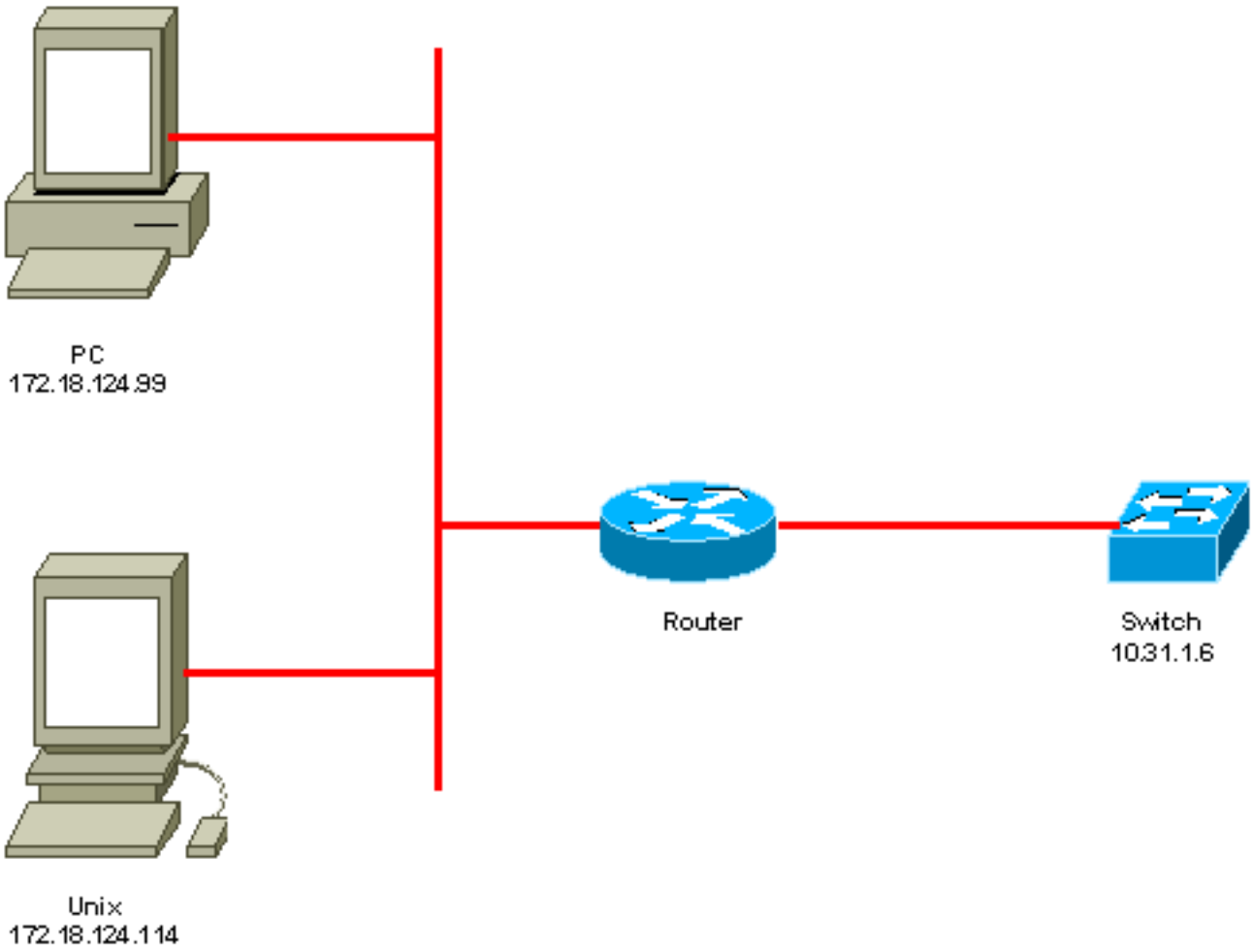
このドキュメントでは、CatOS K9 イメージが稼働する Catalyst 2948G、Catalyst 2980G、Catalyst 4000/4500 シリーズ、Catalyst 5000/5500 シリーズ、および Catalyst 6000/6500 シリーズのみを対象としています。詳細については、このドキュメントの「要件」のセクションを参照してください。

このマニュアルの情報は、特定のラボ環境に置かれた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。実稼動中のネットワークで作業をしている場合、実際にコマンドを使用する前に、その潜在的な影響について理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

ネットワーク図



スイッチの設定

```
!--- Generate and verify RSA key. sec-cat6000> (enable) set crypto key rsa 1024
Generating RSA keys..... [OK]
sec-cat6000> (enable) ssh_key_process: host/server key size: 1024/768
 !--- Display the RSA key. sec-cat6000> (enable) show crypto key
RSA keys were generated at: Mon Jul 23 2001, 15:03:30 1024 65537 1514414695360
577332853671704785709850606634768746869716963940352440620678575338701550888525
699691478330537840066956987610207810959498648179965330018010844785863472773067
697185256418386243001881008830561241137381692820078674376058275573133448529332
199668201930132947097826805906337821547938540549819306165l
```

```
!--- Restrict which host/subnets are allowed to use SSH to the switch. !--- Note: If you do not
do this, the switch will display the message !--- "WARNING!! IP permit list has no entries!"
sec-cat6000> set ip permit 172.18.124.0 255.255.255.0
172.18.124.0 with mask 255.255.255.0 added to IP permit list.
!--- Turn on SSH. sec-cat6000> (enable) set ip permit enable ssh
SSH permit list enabled.
!--- Verity SSH permit list. sec-cat6000> (enable) show ip permit
Telnet permit list disabled.
Ssh permit list enabled.
Snmp permit list disabled.
Permit List Mask Access-Type
---------------- ---------------- -------------
172.18.124.0 255.255.255.0 telnet ssh snmp

Denied IP Address Last Accessed Time Type
---------------- ----------------- ------
```

SSH の無効化

状況によっては、スイッチで SSH を無効にすることが必要になる場合があります。スイッチで SSH が設定されているかどうかを確認し、設定されている場合は無効にします。

スイッチで SSH が設定されているかどうかを確認するには、**show crypto key コマンドを発行します。**出力に RSA キーが表示される場合は、スイッチで SSH が設定され、有効になっています。次に例を示します。

```
sec-cat6000> (enable) show crypto key
RSA keys were generated at: Mon Jul 23 2001, 15:03:30 1024 65537 1514414695360
57733285367170478570985060663476874686971696394035244062067857533870155088852 5
69969147833053784006695698761020781095949864817996533001801084478586347277306 7
69718525641838624300188100883056124113738169282007867437605827557313344852933 2
19966820193013294709782680590633782154793854054981930616 51
```

暗号キーを削除するには、clear crypto key rsa コマンドを発行して、スイッチで SSH を無効にします。次に例を示します。

```
sec-cat6000> (enable) clear crypto key rsa
Do you really want to clear RSA keys (y/n) [n]? y
RSA keys has been cleared.
sec-cat6000> (enable)
```

Catalyst でのデバッグ

デバッグをオンにするには、**set trace ssh 4 コマンドを発行します。**

デバッグをオフにするには、**set trace ssh 0 コマンドを発行します。**

接続が良好な場合の debug コマンドの例

Solaris から Catalyst への Triple Data Encryption Standard (3DES) Telnet パスワード

Solaris

```
rtp-evergreen# ssh -c 3des -v 10.31.1.6
SSH Version 1.2.26 [sparc-sun-solaris2.5.1], protocol version 1.5.
Compiled with RSAREF.
rtp-evergreen: Reading configuration data /opt/CISssh/etc/ssh_config
rtp-evergreen: ssh_connect: getuid 0 geteuid 0 anon 0
rtp-evergreen: Allocated local port 1023.
rtp-evergreen: Connecting to 10.31.1.6 port 22.
rtp-evergreen: Connection established.
rtp-evergreen: Remote protocol version 1.5, remote software version 1.2.26
rtp-evergreen: Waiting for server public key.
rtp-evergreen: Received server public key (768 bits) and host key (1024 bits).
Host key not found from the list of known hosts.
Are you sure you want to continue connecting (yes/no)? yes
Host '10.31.1.6' added to the list of known hosts.
rtp-evergreen: Initializing random; seed file //.ssh/random_seed
rtp-evergreen: Encryption type: 3des
rtp-evergreen: Sent encrypted session key.
rtp-evergreen: Installing crc compensation attack detector.
rtp-evergreen: Received encrypted confirmation.
rtp-evergreen: Doing password authentication.
root@10.31.1.6's password:
rtp-evergreen: Requesting pty.
rtp-evergreen: Failed to get local xauth data.
rtp-evergreen: Requesting X11 forwarding with authentication spoofing.
Warning: Remote host denied X11 forwarding, perhaps xauth program
   could not be run on the server side.
rtp-evergreen: Requesting shell.
rtp-evergreen: Entering interactive session.

Cisco Systems Console

sec-cat6000>
```

Catalyst

```
sec-cat6000> (enable) debug: _proc->tty = 0x8298a494, socket_index = 3
debug: version: SSH-1.5-1.2.26

debug: Client protocol version 1.5; client software version 1.2.26
debug: Sent 768 bit public key and 1024 bit host key.
debug: Encryption type: 3des
debug: Received session key; encryption turned on.
debug: ssh login by user: root
debug: Trying Local Login
Password authentication for root accepted.
debug: ssh received packet type: 10
debug: ssh received packet type: 34
Unknown packet type received after authentication: 34
debug: ssh received packet type: 12
debug: ssh88: starting exec shell
debug: Entering interactive session.
```

PC から Catalyst への 3DES Telnet パスワード

Catalyst

```
debug: Client protocol version 1.5; client software version W1.0
debug: Sent 768 bit public key and 1024 bit host key.
debug: Encryption type: des
```

```
debug: Received session key; encryption turned on.
debug: ssh login by user:
debug: Trying Local Login
Password authentication for accepted.
debug: ssh received packet type: 10
debug: ssh received packet type: 37
Unknown packet type received after authentication: 37
debug: ssh received packet type: 12
debug: ssh89: starting exec shell
debug: Entering interactive session.
```

Solaris から Catalyst への 3DES 認証、認可、およびアカウンティング（AAA）認証

Solaris

```
Solaris with aaa on:
rtp-evergreen# ssh -c 3des -l abcde123 -v 10.31.1.6
SSH Version 1.2.26 [sparc-sun-solaris2.5.1], protocol version 1.5.
Compiled with RSAREF.
rtp-evergreen: Reading configuration data /opt/CISssh/etc/ssh_config
rtp-evergreen: ssh_connect: getuid 0 geteuid 0 anon 0
rtp-evergreen: Allocated local port 1023.
rtp-evergreen: Connecting to 10.31.1.6 port 22.
rtp-evergreen: Connection established.
rtp-evergreen: Remote protocol version 1.5, remote software version 1.2.26
rtp-evergreen: Waiting for server public key.
rtp-evergreen: Received server public key (768 bits) and host key (1024 bits).
rtp-evergreen: Host '10.31.1.6' is known and matches the host key.
rtp-evergreen: Initializing random; seed file //.ssh/random_seed
rtp-evergreen: Encryption type: 3des
rtp-evergreen: Sent encrypted session key.
rtp-evergreen: Installing crc compensation attack detector.
rtp-evergreen: Received encrypted confirmation.
rtp-evergreen: Doing password authentication.
abcde123@10.31.1.6's password:
rtp-evergreen: Requesting pty.
rtp-evergreen: Failed to get local xauth data.
rtp-evergreen: Requesting X11 forwarding with authentication spoofing.
Warning: Remote host denied X11 forwarding, perhaps xauth program
   could not be run on the server side.
rtp-evergreen: Requesting shell.
rtp-evergreen: Entering interactive session.

Cisco Systems Console

sec-cat6000>
```

Catalyst

```
sec-cat6000> (enable) debug: _proc->tty = 0x82a07714, socket_index = 3
debug: version: SSH-1.5-1.2.26

debug: Client protocol version 1.5; client software version 1.2.26
debug: Sent 768 bit public key and 1024 bit host key.
debug: Encryption type: 3des
debug: Received session key; encryption turned on.
debug: ssh login by user: abcde123
debug: Trying TACACS+ Login
Password authentication for abcde123 accepted.
```

```
debug: ssh received packet type: 10
debug: ssh received packet type: 34
Unknown packet type received after authentication: 34
debug: ssh received packet type: 12
debug: ssh88: starting exec shell
debug: Entering interactive session.
```

問題が発生した場合の debug コマンドの例

クライアントが Blowfish 暗号（未サポート）を試みる場合の Catalyst でのデバッグ

```
debug: Client protocol version 1.5; client software version W1.0
debug: Sent 768 bit public key and 1024 bit host key.
debug: Encryption type: blowfish
cipher_set_key: unknown cipher: 6
debug: Calling cleanup
```

Telnet パスワードが不正な場合の Catalyst でのデバッグ

```
debug: _proc->tty = 0x82897414, socket_index = 4
debug: version: SSH-1.5-1.2.26
debug: Client protocol version 1.5; client software version W1.0
debug: Sent 768 bit public key and 1024 bit host key.
debug: Encryption type: 3des
debug: Received session key; encryption turned on.
debug: ssh login by user:
debug: Trying Local Login
debug: Password authentication for failed.
```

AAA 認証が正常に行われない場合の Catalyst でのデバッグ

```
cat6000> (enable) debug: _proc->tty = 0x829abd94, socket_index = 3
debug: version: SSH-1.5-1.2.26

debug: Client protocol version 1.5; client software version 1.2.26
debug: Sent 768 bit public key and 1024 bit host key.
debug: Encryption type: 3des
debug: Received session key; encryption turned on.
debug: ssh login by user: junkuser
debug: Trying TACACS+ Login
debug: Password authentication for junkuser failed.
SSH connection closed by remote host.
debug: Calling cleanup
```

トラブルシュート

ここでは、Cisco スイッチでの SSH 設定に関連する各種トラブルシューティング シナリオについて説明します。

SSH を使用してスイッチに接続できない

問題：

SSH を使用してスイッチに接続できません。

debug ip ssh コマンドが次の出力を表示します。

```
Jun 15 20:29:26.207: SSH2 1: RSA_sign: private key not found
Jun 15 20:29:26.207: SSH2 1: signature creation failed, status -1
```

ソリューション：

この問題は次のいずれかが原因で発生します。

- ホスト名の変更後に新しい SSH 接続が失敗するようになった。
- SSH がラベルの付いていないキー（ルータの FQDN が使用されることになる）を使用して設定されている。

この問題の回避策を次に示します。

- ホスト名を変更した後に SSH が機能しなくなった場合は、新しいキーを抹消し、適切なラベルを使用して別の新しいキーを作成します。
  ```
  crypto key zeroize rsa
  crypto key generate rsa general-keys label (label) mod (modulus) [exportable]
  ```
- 匿名 RSA キー（スイッチの FQDN に基づく名前が付けられる）は使用しないでください。代わりにラベル付きキーを使用してください。
  ```
  crypto key generate rsa general-keys label (label) mod (modulus) [exportable]
  ```

この問題を完全に解決するには、IOS ソフトウェアをこの問題が修正されているバージョンにアップグレードします。

この問題に関するバグが報告されています。詳細については、Cisco Bug ID CSCtc41114（登録ユーザ専用）を参照してください。

関連情報

- SSH サポート ページ
- Cisco IOS を実行するルータとスイッチでのセキュア シェルの設定
- バグ ツールキット
- テクニカルサポート - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。