目次

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	いいえ
Cat 2800	いいえ
Cat 2948G-L3	いいえ
Cat 2900XL	いいえ
Cat 3500XL	いいえ
Cat 4840G-L3	いいえ
Cat 4908G-L3	いいえ

* 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

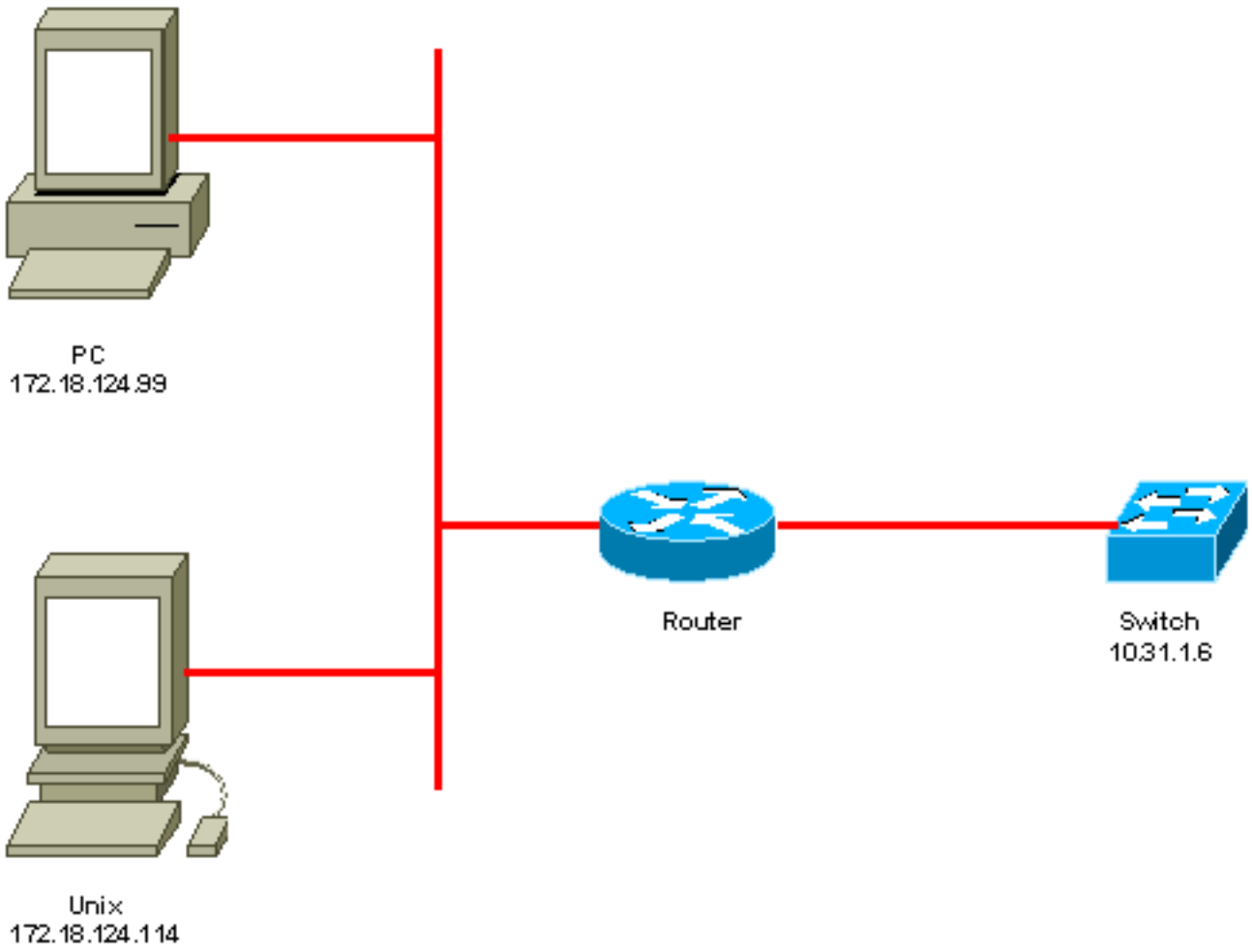
このドキュメントでは、CatOS K9 イメージが稼働する Catalyst 2948G、Catalyst 2980G、Catalyst 4000/4500 シリーズ、Catalyst 5000/5500 シリーズ、および Catalyst 6000/6500 シリーズのみを対象としています。 詳細については、このドキュメントの「要件」のセクションを参照してください。

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たものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 対象のネットワークが実稼働中である場合には、どのような作業についても、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。

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 1024Generating RSA
keys..... [OK]sec-cat6000> (enable) ssh_key_process: host/server key size: 1024/768 !--- Display
the RSA key.sec-cat6000> (enable) show crypto keyRSA keys were generated at: Mon Jul 23 2001,
15:03:30 1024 65537
151441469536057733285367170478570985060663476874686971696394035244062067857533870155088852569969
147833053784006695698761020781095949864817996533001801084478586347277306769718525641838624300188
100883056124113738169282007867437605827557313344852933219966820193013294709782680590633782154793
85405498193061651 !--- 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 172.18.124.0 255.255.255.0172.18.124.0 with mask
255.255.255.0 added to IP permit list. !--- Turn on SSH.sec-cat6000> (enable) set ip permit
enable sshSSH permit list enabled. !--- Verity SSH permit list.sec-cat6000> (enable) show ip
permitTelnet 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 keyRSA keys were generated at: Mon Jul 23 2001, 15:03:30 1024
65537
151441469536057733285367170478570985060663476874686971696394035244062067857533870155088852569969
147833053784006695698761020781095949864817996533001801084478586347277306769718525641838624300188
100883056124113738169282007867437605827557313344852933219966820193013294709782680590633782154793
85405498193061651
```

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 10.31.1.6SSH 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_configrtp-evergreen: ssh_connect: getuid 0 geteuid 0 anon 0rtp-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
1.2.26rtp-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)? yesHost '10.31.1.6' added to the list of known
hosts.rtp-evergreen: Initializing random; seed file //.ssh/random_seedrtp-evergreen: Encryption
type: 3desrtp-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 Consolesec-cat6000>
```

「Catalyst

```
rtp-evergreen# ssh -c 3des -v 10.31.1.6SSH 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_configrtp-evergreen: ssh_connect: getuid 0 geteuid 0 anon 0rtp-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 1.2.26rtp-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)? yesHost '10.31.1.6' added to the list of known hosts.rtp-evergreen: Initializing random; seed file //.ssh/random_seedrtp-evergreen: Encryption type: 3desrtp-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 Consolesec-cat6000>

PC から Catalyst への 3DES Telnet パスワード

「Catalyst

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_configrtp-evergreen: ssh_connect: getuid 0 geteuid 0 anon 0rtp-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 1.2.26rtp-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)? yesHost '10.31.1.6' added to the list of known hosts.rtp-evergreen: Initializing random; seed file //.ssh/random_seedrtp-evergreen: Encryption type: 3desrtp-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 Consolesec-cat6000>

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_configrtp-evergreen: ssh_connect: getuid 0 geteuid 0 anon 0rtp-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 1.2.26rtp-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_seedrtp-evergreen: Encryption type: 3desrtp-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 Consolesec-cat6000>

「Catalyst

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_configrtp-evergreen: ssh_connect: getuid 0 geteuid 0 anon

```
0rtp-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 1.2.26rtp-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_seedrtp-evergreen:
Encryption type: 3desrtp-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 Consolesec-cat6000>
```

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

```
Solaris with aaa on:rtp-evergreen# ssh -c 3des -l abcde123 -v 10.31.1.6SSH 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_configrtp-evergreen: ssh_connect: getuid 0 geteuid 0 anon
0rtp-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 1.2.26rtp-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_seedrtp-evergreen:
Encryption type: 3desrtp-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 Consolesec-cat6000>
```

Telnet パスワードが不正な場合の Catalyst でのデバッグ

```
Solaris with aaa on:rtp-evergreen# ssh -c 3des -l abcde123 -v 10.31.1.6SSH 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_configrtp-evergreen: ssh_connect: getuid 0 geteuid 0 anon
0rtp-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 1.2.26rtp-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_seedrtp-evergreen:
Encryption type: 3desrtp-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 Consolesec-cat6000>
```

AAA 認証が正常に行われない場合の Catalyst でのデバッグ

```
Solaris with aaa on:rtp-evergreen# ssh -c 3des -l abcde123 -v 10.31.1.6SSH 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_configrtp-evergreen: ssh_connect: getuid 0 geteuid 0 anon
0rtp-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 1.2.26rtp-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_seedrtp-evergreen:
```

```
Encryption type: 3desrtp-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 Consolesec-cat6000>
```

トラブルシューティング

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。

```
Solaris with aaa on:rtp-evergreen# ssh -c 3des -l abcde123 -v 10.31.1.6SSH 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_configrtp-evergreen: ssh_connect: getuid 0 geteuid 0 anon
0rtp-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 1.2.26rtp-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_seedrtp-evergreen:
Encryption type: 3desrtp-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 Consolesec-cat6000>
```

解決策：

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。`Solaris with aaa on:rtp-evergreen# ssh -c 3des -l abcde123 -v 10.31.1.6SSH 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_configrtp-evergreen: ssh_connect: getuid 0 geteuid 0 anon 0rtp-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 1.2.26rtp-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_seedrtp-evergreen: Encryption type: 3desrtp-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
Consolesec-cat6000>
```

- 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。`Solaris with aaa on:rtp-evergreen# ssh -c 3des -l abcde123 -v 10.31.1.6SSH 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_configrtp-evergreen: ssh_connect: getuid 0 geteuid 0 anon 0rtp-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 1.2.26rtp-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_seedrtp-evergreen: Encryption type: 3desrtp-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 Consolesec-cat6000>`

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 を実行するルータおよびスイッチのセキュア 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