如何在執行CatOS的Catalyst交換器上設定SSH

目錄

簡介

本文分步介紹如何在執行Catalyst OS(CatOS)的Catalyst交換器上設定安全殼層(SSH)版本1。 測試的版本是cat6000-**supk9**.6-1-1c.bin。

必要條件

需求

下表顯示了交換機中的SSH支援狀態。註冊使用者可以通過訪問軟體中心來訪問這些軟體映像。

CatOS SSH	
裝置	**SSH支援**
Cat 4000/4500/2948G/2980G(CatOS)	K9映像（截至6.1）

Cat 5000/5500(CatOS)	K9映像（截至6.1）
Cat 6000/6500(CatOS)	K9映像（截至6.1）
IOS SSH	
裝置	**SSH支援**
Cat 2950*	12.1(12c)EA1及更高版本
Cat 3550*	12.1(11)EA1及更高版本
Cat 4000/4500（整合式Cisco IOS軟體）*	12.1(13)EW及更高版**
Cat 6000/5500（整合式Cisco IOS軟體）*	12.1(11b)E及更高版本
Cat 8540/8510	12.1(12c)EY及更高版本、 12.1(14)E1及更高版本
無SSH	
裝置	**SSH支援**
Cat 1900	否
Cat 2800	否
Cat 2948G-L3	否
Cat 2900XL	否
Cat 3500XL	否
Cat 4840G-L3	否
Cat 4908G-L3	否

*配置在運行Cisco IOS的路由器和交換機上配置Secure Shell中。

**運行整合Cisco IOS軟體的Catalyst 4000的12.1E系列不支援SSH。

要申請3DES，請參閱加密軟體匯出分發授權表。

本檔案假設驗證在SSH（透過Telnet密碼、TACACS+）或RADIUS實作之前有效。在實施SSH之前，不支援使用Kerberos的SSH。

採用元件

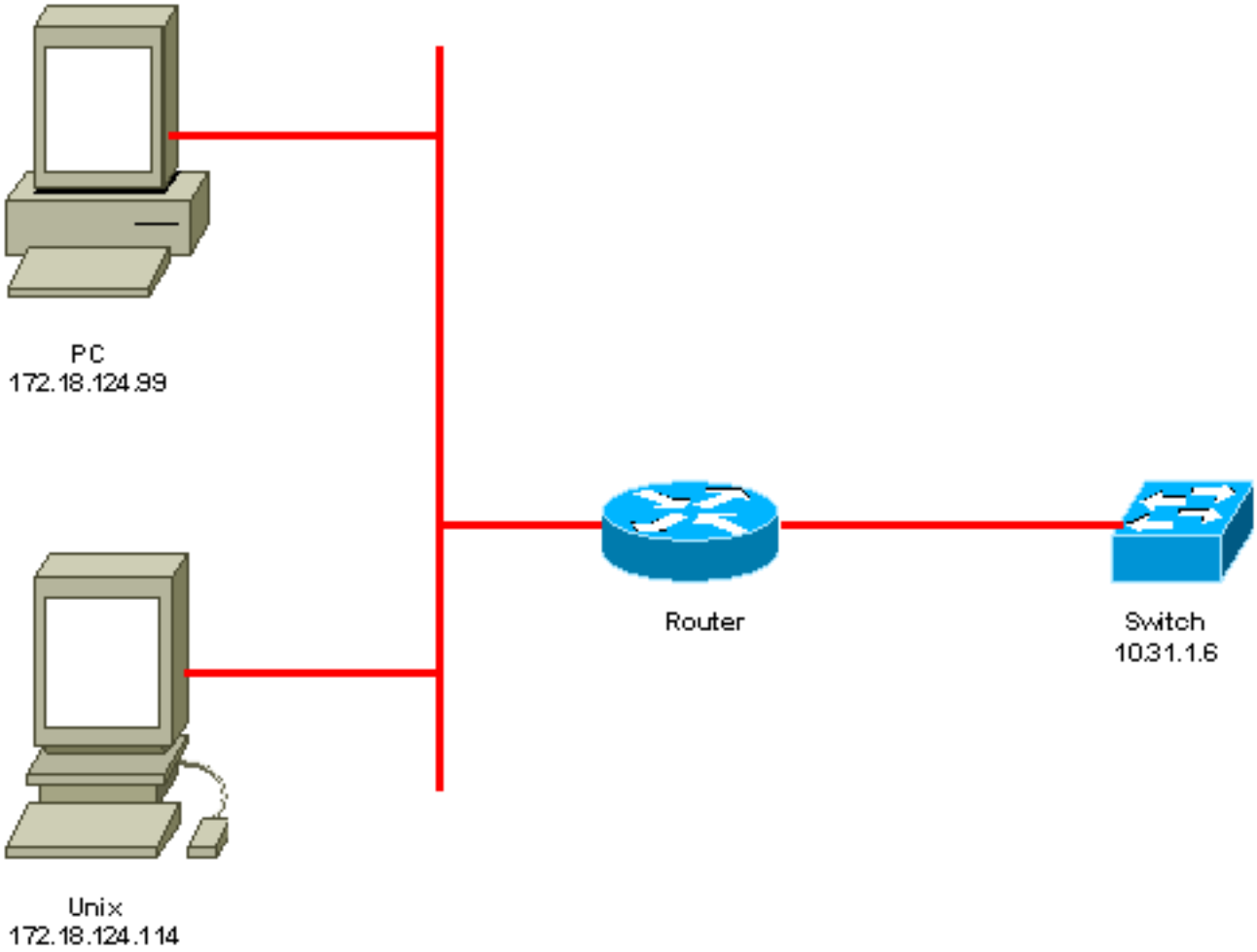
本文僅討論執行CatOS K9映像的Catalyst 2948G、Catalyst 2980G、Catalyst 4000/4500系列、Catalyst 500/5500系列和Catalyst 6000/6500系列。有關詳細資訊，請參閱本文檔的要求部分。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您在即時網路中工作，請確保在使用任何命令之前瞭解其潛在影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

網路圖表



交換器組態

```
!--- 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
57733285367170478570985060663476874686971696394035244062067857533870155088852 5
69969147833053784006695698761020781095949864817996533001801084478586347277306 7
69718525641838624300188100883056124113738169282007867437605827557313344852933 2
19966820193013294709782680590633782154793854054981930616 51
!--- 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
```

---------------- ----------------- ------

禁用SSH

在某些情況下，可能需要禁用交換機上的SSH。必須驗證交換機上是否配置了SSH，如果配置了，請將其禁用。

要驗證交換機上是否配置了SSH，請發出**show crypto key**命令。如果輸出顯示RSA金鑰，則交換機上已配置並啟用了SSH。此處顯示範例。

```
sec-cat6000> (enable) show crypto key
RSA keys were generated at: Mon Jul 23 2001, 15:03:30 1024 65537 1514414695360
577332853671704785709850606634768746869716963940352440620678575338701550888525
699691478330537840066956987610207810959498648179965330018010844785863472773067
697185256418386243001881008830561241137381692820078674376058275573133448529332
199668201930132947097826805906337821547938540549819306165 1
```

要刪除加密金鑰，請發出**clear crypto key rsa**命令以禁用交換機上的SSH。此處顯示範例。

```
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)
```

在Catalyst中調試

要啟用調試，請發出**set trace ssh 4**命令。

要關閉調試，請發出**set trace ssh 0**命令。

debug命令良好連線的示例

Solaris到Catalyst、三重資料加密標準(3DES)、Telnet密碼

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到Catalyst、3DES、Telnet密碼

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到Catalyst、3DES、身份驗證、授權和記帳(AAA)身份驗證

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.
```

debug指令錯誤範例

Catalyst調試，客戶端嘗試[不受支援] Blowfish密碼

```
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
```

使用錯誤的Telnet密碼進行Catalyst調試

```
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.
```

使用錯誤的AAA驗證的Catalyst調試

```
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
```

疑難排解

本節介紹與思科交換機上的SSH配置相關的不同故障排除場景。

無法通過SSH連線到交換機

問題：

無法使用SSH連線到交換機。

debug ip ssh命令會顯示以下輸出：

```
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
```

解決方案：

出現此問題的原因如下：

- 更改主機名後，新的SSH連線失敗。
- 使用未標籤的金鑰（具有路由器FQDN）配置SSH。

此問題的解決方法為：

- 如果主機名已更改且SSH不再工作，則清空新金鑰並用正確的標籤建立另一個新金鑰。
  ```
  crypto key zeroize rsa
  crypto key generate rsa general-keys label (label) mod (modulus) [exportable]
  ```
- 請勿使用匿名RSA金鑰（以交換機的FQDN命名）。 改用帶標籤的金鑰。
  ```
  crypto key generate rsa general-keys label (label) mod (modulus) [exportable]
  ```

若要永久解決此問題，請將IOS軟體升級至解決此問題的任何版本。

已針對此問題提出錯誤。如需更多資訊，請參閱Cisco錯誤ID CSCtc4114(僅限註冊客戶)。

相關資訊

- SSH支援頁面
- 在執行Cisco IOS的路由器和交換器上設定Secure Shell
- 錯誤工具包
- 技術支援 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。