如何在运行 CatOS 的 Catalyst 交换机上配置 SSH

目录

简介

本文档分步说明如何在运行 Catalyst OS (CatOS) 的 Catalyst 交换机上配置Secure Shell (SSH) 版本 1。 测试的版本是 cat6000-supk9.6-1-1c.bin。

先决条件

要求

此表显示交换机中的 SSH 支持状态。注册用户可以通过访问软件中心来访问这些软件映像。

CatOS SSH	
设备	**SSH 支持**
Cat 4000/4500/2948G/2980G	自 6.1 起的 K9 映像

(CatOS)	
Cat 5000/5500 (CatOS)	自 6.1 起的 K9 映像
Cat 6000/6500 (CatOS)	自 6.1 起的 K9 映像
IOS SSH	
设备	**SSH 支持**
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（集成了 Cisco IOS 软件）*	12.1(13)EW 及更高版本**
Cat 6000/5500（集成了 Cisco IOS 软件）*	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
无 SSH	
设备	**SSH 支持**
Cat 1900	否
Cat 2800	否
Cat 2948G-L3	否
Cat 2900XL	否
Cat 3500XL	否
Cat 4840G-L3	否
Cat 4908G-L3	否

*在运行Cisco IOS的路由器和交换机上配置Secure Shell中介绍了配置。

** 对于运行集成的 Cisco IOS 软件的 Catalyst 4000，在 12.1E 系列中不支持 SSH。

若要申请 3DES，请参见 Encryption Software Export Distribution Authorization Form（加密软件导出分发权表）。

本文档假设在实施 SSH（通过 Telnet 口令 TACACS+）或 RADIUS 之前进行了认证工作。在实施 SSH 之前，不支持带有 Kerberos 的 SSH。

使用的组件

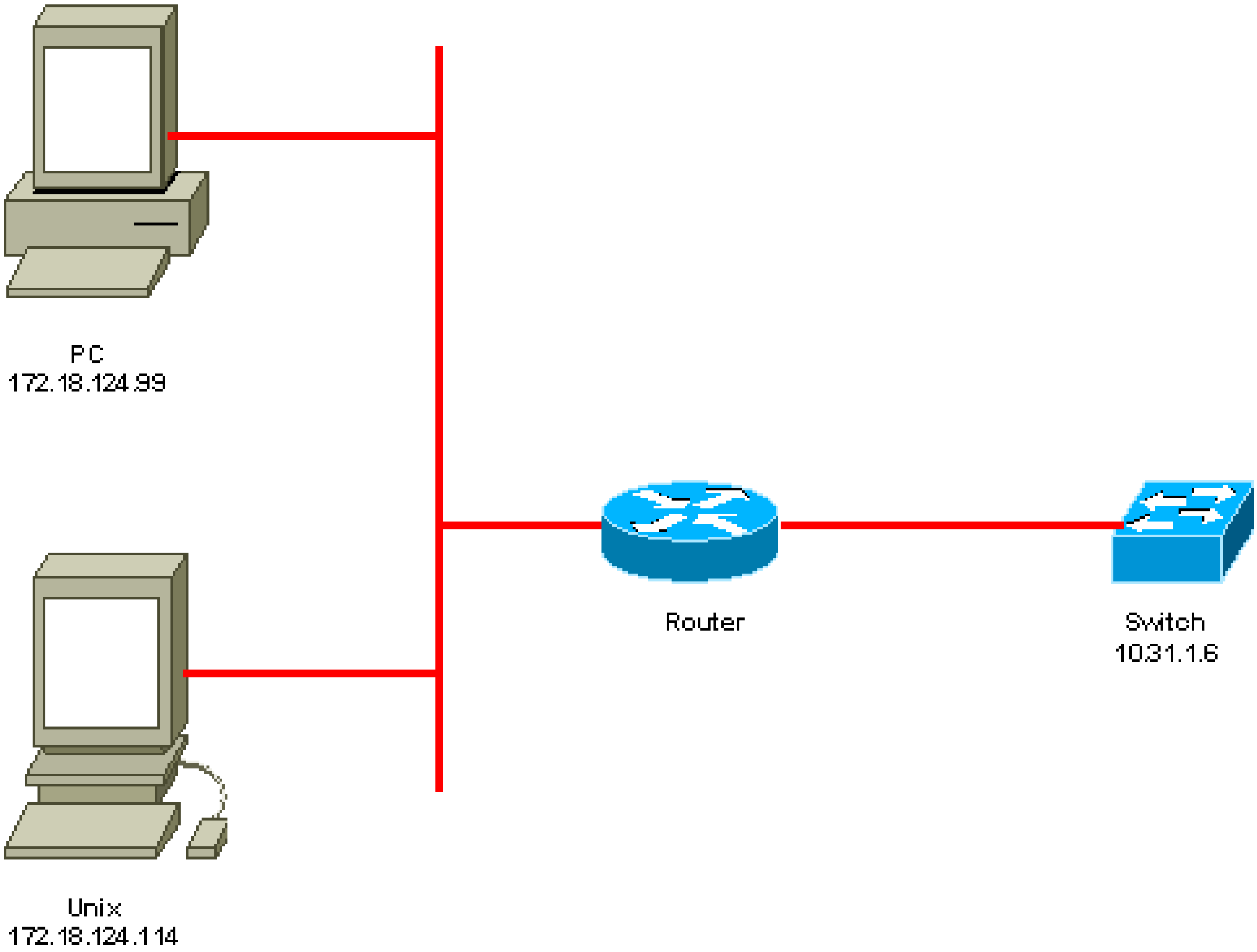
本文档仅讨论运行 CatOS K9 映像的 Catalyst 2948G、Catalyst 2980G、Catalyst 4000/4500 系列、Catalyst 5000/5500 系列和 Catalyst 6000/6500 系列。有关更详细信息，请参见本文档的要求部分。

本文档中的信息都是基于特定实验室环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您是在真实网络上操作，请确保您在使用任何命令前已经了解其潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

网络图



交换机配置

```
!--- 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
1996682019301329470978268059063378215479385405498193061651
!--- 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

在某些情况下，可能有必要在交换机上禁用 SSH。您必须验证是否在交换机上配置了 SSH，如果已配置，则禁用它。

若要验证是否在交换机上配置了 SSH，请发出 **show crypto key 命令。**如果输出显示 RSA 密钥，则已在交换机上配置并启用 SSH。此处给出了一个示例。

```
sec-cat6000> (enable) show crypto key
RSA keys were generated at: Mon Jul 23 2001, 15:03:30 1024 65537 1514414695360
577332853671704785709850606634768746869716963940352440620678575338701550888525
699691478330537840066956987610207810959498648179965330018010844785863472773067
697185256418386243001881008830561241137381692820078674376058275573133448529332
1996682019301329470978268059063378215479385405498193061651
```

若要删除加密密钥，请发出 **clear crypto key rsa 命令以在交换机上禁用 SSH。**此处给出了一个示例。

```
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)
```

Catalyst 中的调试

若要打开调试，请发出 **set trace ssh 4 命令。**

若要关闭调试，请发出 **set trace ssh 0 命令。**

针对正常连接执行 debug 命令的示例

Solaris 到 Catalyst、三重数据加密标准 (3DES)、Telnet 密码

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>
```

催化剂

```
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密码

催化剂

```
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、身份验证、授权和记账 (AAA) 认证

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>
```

催化剂

```
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.
```

针对可能出现的错误执行 debug 命令的示例

对尝试 [不支持的] Blowfish 口令的客户端的 Catalyst 调试

```
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
```

对错误的 Telnet 口令的 Catalyst 调试

```
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.
```

对错误的 AAA 认证的 Catalyst 调试

```
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
```

故障排除

本节介绍与Cisco交换机上的SSH配置相关的不同故障排除场景。

无法通过SSH连接到交换机

问题：

无法使用SSH连接到交换机。

debug ip ssh命令显示以下输出：

```
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
```

解决方案：

出现此问题的原因如下：

- 更改主机名后，新的SSH连接失败。
- 使用非标记密钥（具有路由器FQDN）配置SSH。

此问题的解决方法如下：

- 如果主机名已更改且SSH不再工作，则清空新密钥并使用正确的标签创建另一个新密钥。
  ```
  crypto key zeroize rsa
  crypto key generate rsa general-keys label (label) mod (modulus) [exportable]
  ```
- 请勿使用匿名RSA密钥（以交换机的FQDN命名）。 改用标记密钥。

```
    crypto key generate rsa general-keys label (label) mod (modulus) [exportable]
```

为了永久解决此问题，请将IOS软件升级到解决此问题的任何版本。

已针对此问题提交了错误。有关详细信息，请参阅Cisco Bug ID CSCtc41114（仅限注册客户）。

相关信息

- SSH Support Page（SSH 技术支持页面）
- 在运行 Cisco IOS 的路由器与交换机上配置Secure Shell
- Bug Toolkit
- 技术支持 - Cisco Systems

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。