

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[网络图](#)

[交换机配置](#)

[禁用 SSH](#)

[Catalyst 中的调试](#)

[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](#)

[PC 到 Catalyst、3DES、Telnet 密码](#)

[Solaris 到 Catalyst、3DES、身份验证、授权和记账 \(AAA\) 认证](#)

[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](#)

[对错误的 Telnet 口令的 Catalyst 调试](#)

[对错误的 AAA 认证的 Catalyst 调试](#)

[故障排除](#)

[不能连接通过 SSH 交换](#)

[相关信息](#)

简介

本文档分步说明如何在运行 Catalyst OS (CatOS) 的 Catalyst 交换机上配置安全外壳 (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。注册用户能通过访问[软件中心](#)访问这些软件镜像。

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

*配置在[配置报道路由器和交换机上的安全Shell运行Cisco IOS](#)。

** 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](#) (加密软件导出分发授权表) 。

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

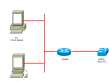
本文档仅讨论运行 CatOS K9 映像的 Catalyst 2948G、Catalyst 2980G、Catalyst 4000/4500 系列、Catalyst 5000/5500 系列和 Catalyst 6000/6500 系列。有关更详细信息 , 请参见本文档的[要求](#)部分。

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 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 -----
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 keyRSA keys were generated at: Mon Jul 23 2001, 15:03:30 1024
65537
151441469536057733285367170478570985060663476874686971696394035244062067857533870155088852569969
147833053784006695698761020781095949864817996533001801084478586347277306769718525641838624300188
100883056124113738169282007867437605827557313344852933219966820193013294709782680590633782154793
85405498193061651
```

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 10.31.1.6SSH 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 到 Catalyst、3DES、Telnet密码](#)

[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>
```

[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 10.31.1.6SSH 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.abcdel123@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 abcdel123 -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.abcdel123@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>
```

[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](#)

```
Solaris with aaa on:rtp-evergreen# ssh -c 3des -l abcdel123 -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.abcdel123@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>
```

[对错误的 Telnet 口令的 Catalyst 调试](#)

```
Solaris with aaa on:rtp-evergreen# ssh -c 3des -l abcdel123 -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.abcdel123@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>

对错误的 AAA 认证的 Catalyst 调试

```
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>
```

故障排除

此部分处理与在Cisco交换机的SSH配置涉及的不同的故障排除情况。

不能连接通过SSH交换

问题：

使用SSH，不能连接到交换机。

debug IP SSH命令显示此输出：

```
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>
```

解决方案：

此问题发生由于这些原因之一：

- 新的SSH连接在更改主机名以后失效。
- SSH配置与非被标记的密钥(有路由器FQDN)。

此问题的应急方案是：

- 如果主机名更改，并且SSH不再工作，则请调零新密钥并且创建另一新密钥用适当的标签。

```
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>
```

- **请勿使用匿名RSA密钥(被命名在交换机的FQDN以后)。请使用被标记的密钥。** 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>

为了解决此问题永久，请升级IOS软件对此问题修复的任何版本。

bug被归档了关于此问题。欲知更多信息，参考Cisco Bug ID [CSCtc41114](#) (仅限注册用户)。

[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](#)