Como configurar o SSH nos Catalyst Switches que executam CatOS

Contents

Introduction

Este documento oferece instruções passo a passo para configurar o Secure Shell (SSH) Version 1 nos switches Catalyst que executam o Catalyst OS (CatOS). A versão testada é cat6000-supk9.6-1-1c.bin.

Prerequisites

Requirements

Esta tabela mostra o status do suporte SSH nos switches. Os usuários registrados podem acessar essas imagens de software visitando o Centro de Software.

SSH CatOS	
Dispositivo	**Suporte SSH**

Cat 4000/4500/2948G/2980G (CatOS)	Imagens K9 a partir do 6.1
Cat 5000/5500 (CatOS)	Imagens K9 a partir do 6.1
Cat 6000/6500 (CatOS)	Imagens K9 a partir do 6.1
SSH IOS	
Dispositivo	**Suporte SSH**
Cat 2950*	12.1(12c)EA1 e posterior
Cat 3550*	12.1(11)EA1 e posterior
Cat 4000/4500 (Cisco IOS Software integrado)*	12.1(13)EW e ** posteriores
Cat 6000/5500 (Cisco IOS Software integrado)*	12.1(11b)E e posterior
Cat 8540/8510	12.1(12c)EY e posterior, 12.1(14)E1 e posterior
Sem SSH	
Dispositivo	**Suporte SSH**
CAT 1900	não
CAT 2800	não
Cat 2948G-L3	não
Cat 2900XL	não
Cat 3500XL	não
Cat 4840G-L3	não
Cat 4908G-L3	não

* A configuração é abordada em Configuração de Secure Shell em Roteadores e Switches com Cisco IOS.

** Não há suporte para SSH no trem 12.1E para o Catalyst 4000 que executa o software Cisco IOS integrado.

Consulte Formulário de autorização de distribuição de exportação de software de criptografia para solicitar 3DES.

Este documento supõe que a autenticação funciona antes da implementação do SSH (através da senha Telnet, TACACS+) ou RADIUS. SSH com Kerberos não é suportado antes da implementação de SSH.

Componentes Utilizados

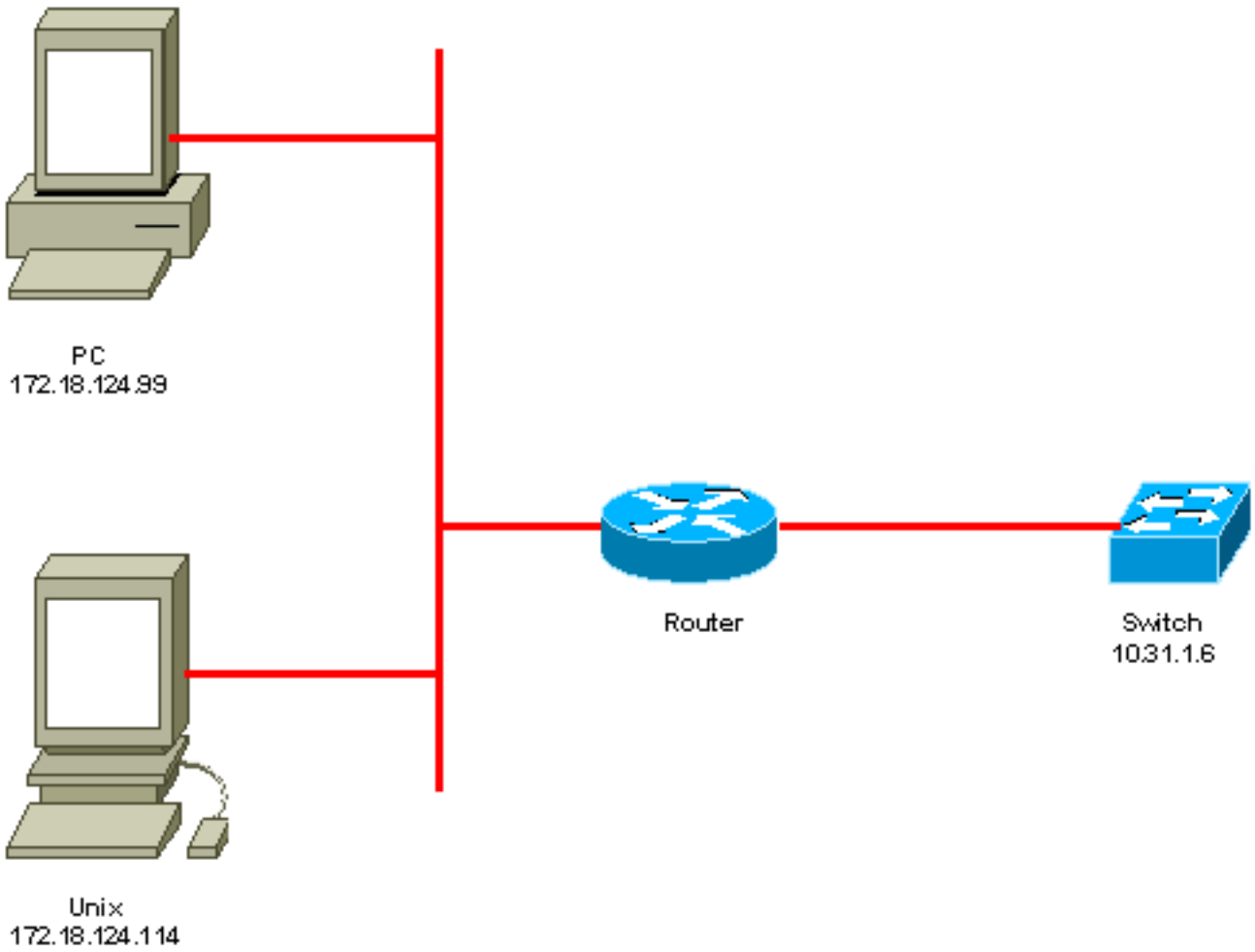
Este documento aborda somente as séries Catalyst 2948G, Catalyst 2980G, Catalyst 4000/4500, Catalyst 5000/5500 e Catalyst 6000/6500 que executam a imagem CatOS K9. Para obter mais detalhes, consulte a seção Requisitos deste documento.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. All of the devices used in this document started with a cleared (default) configuration. Se você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

Conventions

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Diagrama de Rede



Configuração do Switch

```
!--- 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
---------------- ----------------- ------
```

Desabilitando o SSH

Em algumas situações, pode ser necessário desativar o SSH no switch. Você deve verificar se o SSH está configurado no switch e, se estiver, desabilitá-lo.

Para verificar se o SSH foi configurado no switch, emita o comando **show crypto key**. Se a saída exibir a chave RSA, o SSH foi configurado e ativado no switch. Um exemplo é mostrado aqui.

```
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
```

Para remover a chave de criptografia, emita o comando **clear crypto key rsa** para desativar o SSH no switch. Um exemplo é mostrado aqui.

```
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)
```

debug no Catalyst

Para ativar depurações, emita o comando **set trace ssh 4**.

Para desativar depurações, emita o comando **set trace ssh 0**.

Exemplos de comando debug de uma boa conexão

Senha do Solaris para Catalyst, Triple Data Encryption Standard (3DES) e Telnet

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 para Catalyst, 3DES, senha Telnet

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.
```

Autenticação Solaris para Catalyst, 3DES e AAA (autenticação, autorização e auditoria)

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.
```

Exemplos do que pode dar errado com o comando debug

Depuração Catalyst com cliente tentando cifra Blowfish (não suportado)

```
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
```

Depuração do Catalyst com Senha de Telnet Inválida

```
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.
```

Depuração do Catalyst com autenticação de AAA inválida

```
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
```

Troubleshoot

Esta seção trata de diferentes cenários de solução de problemas relacionados à configuração SSH em switches Cisco.

Não é possível conectar-se ao switch através de SSH

Problema:

Não é possível conectar ao switch usando SSH.

O comando **debug ip ssh** mostra esta saída:

```
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
```

Solução:

Esse problema ocorre por uma destas razões:

- Novas conexões SSH falham após alterar o nome do host.
- SSH configurado com chaves não rotuladas (com o FQDN do roteador).

As soluções para esse problema são:

- Se o nome do host foi alterado e o SSH não estiver mais funcionando, anule a nova chave e crie outra nova chave com o rótulo apropriado.
  ```
  crypto key zeroize rsa
  crypto key generate rsa general-keys label (label) mod (modulus) [exportable]
  ```
- Não use chaves RSA anônimas (nomeadas após o FQDN do switch). Em vez disso, use teclas rotuladas.
  ```
  crypto key generate rsa general-keys label (label) mod (modulus) [exportable]
  ```

Para resolver esse problema para sempre, atualize o software IOS para qualquer uma das versões nas quais esse problema foi corrigido.

Um bug foi registrado sobre esse problema. Para obter mais informações, consulte o bug da Cisco ID CSCtc4114 (somente clientes registrados).

Informações Relacionadas

- Página de suporte SSH
- Configuring Secure Shell on Routers and Switches Running Cisco IOS
- Conjunto de ferramentas do bug
- Suporte Técnico - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.