Índice

Introdução

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.

Pré-requisitos

Requisitos

Esta tabela mostra o estado do apoio SSH no Switches. Os usuários registrados podem alcançar estas imagens do software visitando o centro de software.

CatOS SSH	
Dispositivo	**Apoio SSH**
Gato 4000/4500/2948G/2980G (CatOS)	Imagens K9 até à data de 6.1
Gato 5000/5500 (CatOS)	Imagens K9 até à data de 6.1

Gato 6000/6500 (CatOS)	Imagens K9 até à data de 6.1
IO SSH	
Dispositivo	**Apoio SSH**
Gato 2950*	12.1(12c)EA1 e mais tarde
Gato 3550*	12.1(11)EA1 e mais tarde
Gato 4000/4500 (software do Cisco IOS integrado) *	12.1(13)EW e mais tarde **
Gato 6000/5500 (software do Cisco IOS integrado) *	12.1(11b)E e mais tarde
Gato 8540/8510	12.1(12c)EY e mais tarde, 12.1(14)E1 e mais tarde
Nenhum SSH	
Dispositivo	**Apoio SSH**
Gato 1900	não
Gato 2800	não
Gato 2948G-L3	não
Gato 2900XL	não
Gato 3500XL	não
Gato 4840G-L3	não
Gato 4908G-L3	não

* A configuração é coberta no Configuring Secure Shell no Roteadores e no Switches que executam o Cisco IOS.

** Não há nenhum apoio para o SSH no trem 12.1E para software running do Cisco IOS integrado do catalizador 4000.

Refira o formulário da autorização da distribuição da exportação do software de codificação a fim aplicar-se para o 3DES.

Este documento supõe que a autenticação trabalha antes da aplicação do SSH (com a senha telnet, TACACS+) ou do RAIO. O SSH com Kerberos não é apoiado antes da aplicação do SSH.

Componentes Utilizados

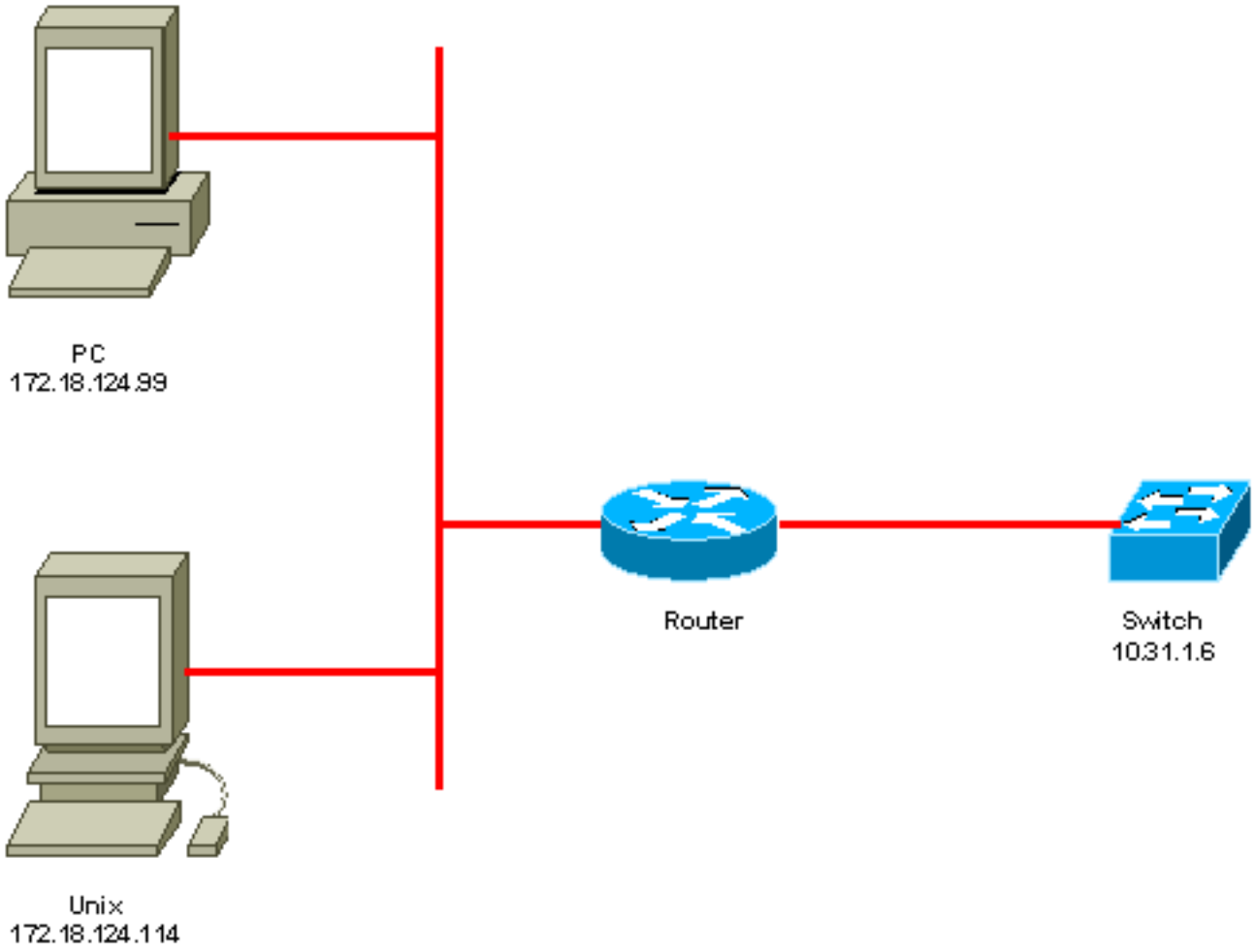
Este documento endereça o 4000/4500 Series somente do Catalyst 2948G, do Catalyst 2980G, do catalizador, a série do Catalyst 5000/5500, e a série do Catalyst 6000/6500 que executa a imagem de CatOS K9. Para mais detalhes, refira a seção das exigências deste documento.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

Convenções

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 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 de desabilitação

Em algumas situações pode ser necessário desabilitar o SSH no interruptor. Você deve verificar se o SSH está configurado no interruptor e em caso afirmativo, desabilita-o.

Para verificar se o SSH foi configurado no interruptor, emita o **comando show crypto key**. Se a saída indica a chave RSA, a seguir o SSH esteve configurado e permitido no interruptor. Um exemplo é mostrado aqui.

```
sec-cat6000> (enable) show crypto keyRSA keys were generated at: Mon Jul 23 2001, 15:03:30 1024
65537
151441469536057733285367170478570985060663476874686971696394035244062067857533870155088852569969
147833053784006695698761020781095949864817996533001801084478586347277306769718525641838624300188
100883056124113738169282007867437605827557313344852933219966820193013294709782680590633782154793
85405498193061651
```

Para remover a chave de criptografia, emita o **comando clear crypto key rsa** desabilitar o SSH no interruptor. 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 girar sobre debuga, emitem o **comando set trace ssh 4**.

Para desligar debuga, emitem o **comando set trace ssh 0**.

Exemplos de comando debug de uma boa conexão

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

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 para Catalyst, 3DES, senha Telnet

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>

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

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>

Exemplos do que pode dar errado com o comando debug

Depuração Catalyst com cliente tentando cifra Blowfish (não suportado)

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>

Depuração do Catalyst com Senha de Telnet Inválida

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>

Depuração do Catalyst com autenticação de AAA inválida

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>
```

Troubleshooting

Esta seção trata os scenarios de Troubleshooting diferentes relativos à configuração SSH em switch Cisco.

Não pode conectar para comutar com o SSH

Problema:

Não pode conectar ao interruptor usando o SSH.

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

```
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>
```

Solução:

Este problema ocorre devido a qualquer uma destas razões:

- As conexões de SSH novas falham após ter mudado o hostname.
- SSH configurado com chaves NON-etiquetadas (tendo o FQDN do roteador).

As ações alternativas para este problema são:

- Se o hostname foi mudado e o SSH já não está trabalhando, a seguir coloque a zero a chave nova e crie uma outra chave nova com a etiqueta apropriada.`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>`
- Não use as chaves anónimas RSA (nomeadas após o FQDN do interruptor). Use chaves

etiquetadas pelo contrário.
```
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>
```

A fim resolver para sempre este problema, promova o IOS Software a algumas das versões em que este problema é fixo.

Um erro foi arquivado sobre esta edição. Para mais informação, refira a identificação de bug Cisco CSCtc41114 (clientes registrados somente).

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