Depurar Secure Shell (SSH) no NCS1K

Contents

Introdução

Este documento descreve práticas básicas de Troubleshooting para Secure Shell (SSH) na plataforma NCS1K.

Pré-requisitos

Este documento assume proficiência com sistemas operacionais baseados em XR em dispositivos como o Network Convergence System (NCS) 1002.

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos para os requisitos de conexão SSH:

- O pacote k9sec relevante para a imagem XR
- Configuração SSH presente no dispositivo Cisco
- Uma geração de chave bem-sucedida, troca de chave e negociação de codificação entre o host e o servidor

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- NCS1002 com XR 7.3.1
- NCS1004 com XR 7.9.1

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 a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Verificar pacotes instalados

Os comandos show install active e show install committed identifique a presença do pacote k9sec. Sem este pacote instalado, você não pode gerar chaves de criptografia para iniciar uma sessão SSH.

<#root>

```
RP/0/RP0/CPU0:NCS1002_1#
show install active


Wed Jul 19 09:31:18.977 UTC
Label : 7.3.1

Node 0/RP0/CPU0 [RP]
Boot Partition: xr_lv58
Active Packages: 4
ncs1k-xr-7.3.1 version=7.3.1 [Boot image]
ncs1k-mpls-te-rsvp-3.1.0.0-r731
ncs1k-mpls-2.1.0.0-r731
ncs1k-k9sec-3.1.0.0-r731

RP/0/RP0/CPU0:NCS1002_1#
show install committed


Wed Jul 19 09:31:37.359 UTC
Label : 7.3.1

Node 0/RP0/CPU0 [RP]
Boot Partition: xr_lv58
Committed Packages: 4
ncs1k-xr-7.3.1 version=7.3.1 [Boot image]
ncs1k-mpls-te-rsvp-3.1.0.0-r731
ncs1k-mpls-2.1.0.0-r731
ncs1k-k9sec-3.1.0.0-r731
```

Configuração

No mínimo, o NCS1K requer a configuração ssh server v2 para permitir conexões SSH. Enter show run ssh para garantir que essa configuração esteja presente:

<#root>

```
RP/0/RP0/CPU0:NCS1004_1#
show run ssh

Wed Jul 19 13:06:57.207 CDT
ssh server rate-limit 600
ssh server v2
ssh server netconf vrf default
```

Identificar chaves geradas

Para estabelecer uma sessão SSH, o NCS1K deve ter uma chave criptográfica pública presente. Identificar a presença de chaves geradas com show crypto key mypubkey { dsa | ecdsa | ed25519 | rsa }. O tipo de chave padrão é rsa. A chave aparece como uma string hexadecimal, omitida aqui para fins de segurança.

<#root>

```
RP/0/RP0/CPU0:NCS1002_1#
show crypto key mypubkey rsa

Wed Jul 19 10:30:09.333 UTC
Key label: the_default
Type : RSA General purpose
Size : 2048
Created : 11:59:56 UTC Tue Aug 23 2022
Data : <key>
```

Para gerar uma chave de um tipo específico, insira o comando crypto key generate { dsa | ecdsa | ed25519 | rsa } e escolha um módulo de chave. O tamanho do módulo varia de acordo com o algoritmo.

Tipo de chave	Tipos de módulo/curva permitidos	Comprimento padrão do módulo (bits)
dsa	512, 768, 1024	1024
ecdsa	nistp256, nistp384, nistp521	nenhum
ad25519	256	256
rsa	512 a 4096	2048

Verifique se a chave foi gerada com êxito com show crypto key mypubkey.

Para remover uma chave existente, insira o comando crypto key zeroize { authentication | dsa | ecdsa | ed25519 | rsa } [label]. Certifique-se de que você tenha acesso ao dispositivo por outros meios como a desconexão de um dispositivo sem chaves de criptografia bloqueia o acesso com SSH.

Identificar recursos do servidor SSH

O servidor e o host devem concordar com uma troca de chave, chave de host e codificação antes de estabelecer uma sessão SSH. Para identificar os recursos da plataforma NCS1K, insira o comando show ssh server.

<#root>

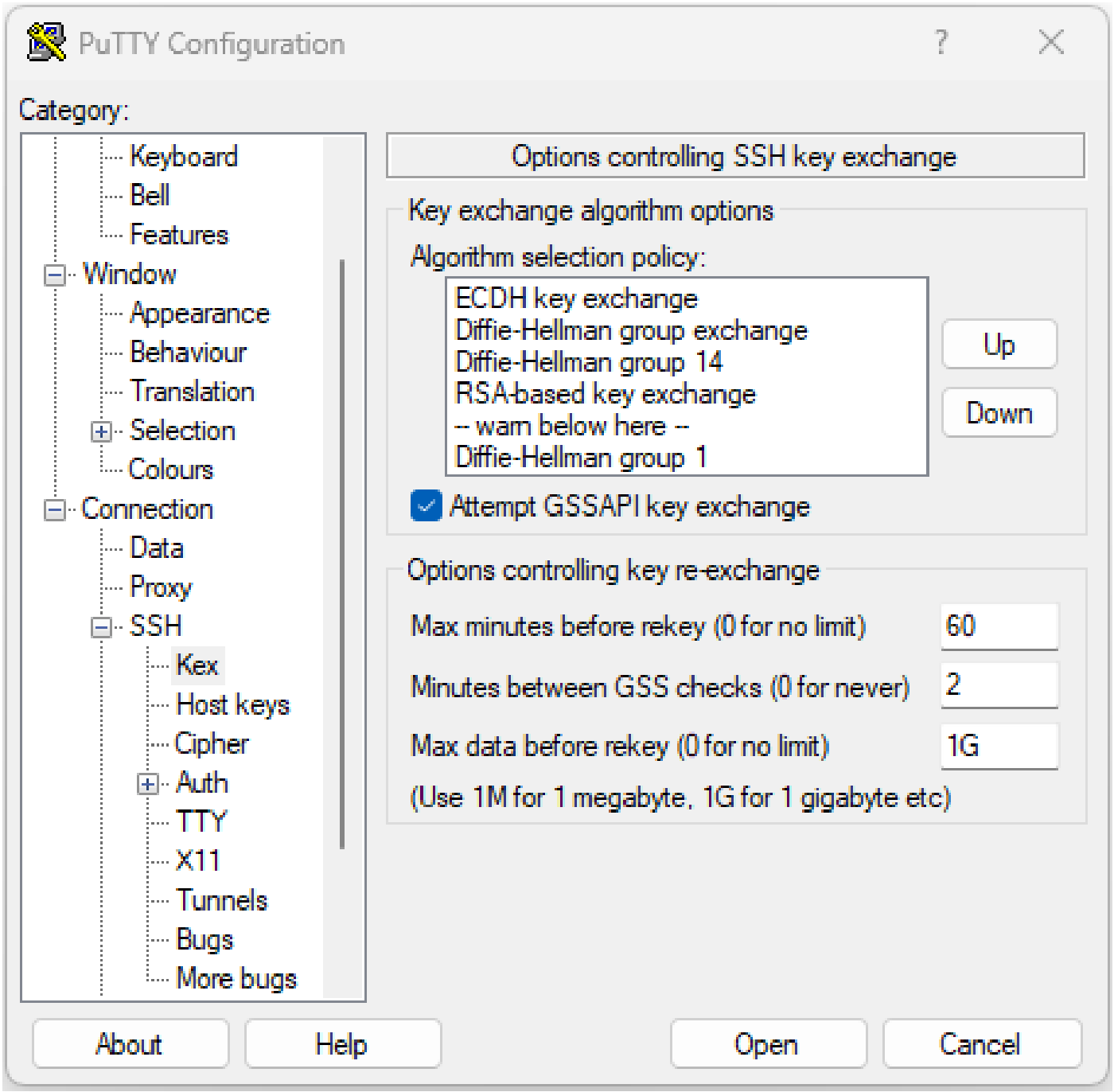
```
RP/0/RP0/CPU0:NCS1004_1#
show ssh server


Wed Jul 19 13:28:04.820 CDT
---------------------
SSH Server Parameters
---------------------

Current supported versions := v2
SSH port := 22
SSH vrfs := vrfname:=default(v4-acl:=, v6-acl:=)
Netconf Port := 830
Netconf Vrfs := vrfname:=default(v4-acl:=, v6-acl:=)

Algorithms
---------------
Hostkey Algorithms := x509v3-ssh-rsa,ecdsa-sha2-nistp521,ecdsa-sha2-nistp384,ecdsa-sha2-nistp256,rsa-sh
Key-Exchange Algorithms := ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-grou
Encryption Algorithms := aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com
Mac Algorithms := hmac-sha2-512,hmac-sha2-256,hmac-sha1

Authentication Method Supported
-----------------------------------
PublicKey := Yes
Password := Yes
Keyboard-Interactive := Yes
Certificate Based := Yes

Others
------------
DSCP := 16
Ratelimit := 600
Sessionlimit := 64
Rekeytime := 60
Server rekeyvolume := 1024
TCP window scale factor := 1
Backup Server := Disabled
Host Trustpoint :=
User Trustpoint :=
Port Forwarding := Disabled
Max Authentication Limit := 20
Certificate username := Common name(CN)
```

Identificar os recursos do SSH do host

O host que está tentando se conectar deve corresponder a pelo menos uma chave de host, troca de chave e algoritmo de criptografia do servidor para estabelecer uma sessão SSH.

PuTTY

O PuTTY lista a troca de chaves suportada, a chave de host e os algoritmos de cifra sob Connections > SSH. O host negocia automaticamente os algoritmos com base em suas capacidades, preferindo o algoritmo de troca de chave na ordem de preferência do usuário. A opção Attempt GSSAPI key exchange não é necessário para se conectar a um dispositivo NCS1K.



Captura de tela das opções PuTTY SSH

Linux

Os servidores Linux normalmente mantêm os algoritmos suportados no /etc/ssh/ssh_config arquivo. Este exemplo se origina do servidor Ubuntu 18.04.3.

```
Host *
# ForwardAgent no
# ForwardX11 no
# ForwardX11Trusted yes
# PasswordAuthentication yes
# HostbasedAuthentication no
# GSSAPIAuthentication no
# GSSAPIDelegateCredentials no
# GSSAPIKeyExchange no
# GSSAPITrustDNS no
# BatchMode no
# CheckHostIP yes
# AddressFamily any
# ConnectTimeout 0
# StrictHostKeyChecking ask
# IdentityFile ~/.ssh/id_rsa
# IdentityFile ~/.ssh/id_dsa
# IdentityFile ~/.ssh/id_ecdsa
# IdentityFile ~/.ssh/id_ed25519
# Port 22
# Protocol 2
# Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc
# MACs hmac-md5,hmac-sha1,umac-64@openssh.com
# EscapeChar ~
# Tunnel no
# TunnelDevice any:any
# PermitLocalCommand no
# VisualHostKey no
# ProxyCommand ssh -q -W %h:%p gateway.example.com
# RekeyLimit 1G 1h
SendEnv LANG LC_*
HashKnownHosts yes
GSSAPIAuthentication yes
```

Solucionar problemas de conexões SSH

Esses comandos podem ajudar a isolar falhas com conexões SSH.

Consulte as sessões SSH atuais de entrada e saída com show ssh session details.

```
<#root>

RP/0/RP0/CPU0:NCS1002_1#

show ssh session details
```

```
Wed Jul 19 13:08:46.147 UTC
SSH version : Cisco-2.0

id key-exchange pubkey incipher outcipher inmac outmac
-----------------------------------------------------------------------------------------------
Incoming Sessions
128733 ecdh-sha2-nistp256 ssh-rsa aes256-ctr aes256-ctr hmac-sha2-256 hmac-sha2-256
128986 diffie-hellman-group14 ssh-rsa aes128-ctr aes128-ctr hmac-sha1 hmac-sha1
128988 diffie-hellman-group14 ssh-rsa aes128-ctr aes128-ctr hmac-sha1 hmac-sha1

Outgoing sessions
```

As sessões SSH históricas incluem tentativas de conexão com o comando show ssh history detail.

<#root>

```
RP/0/RP0/CPU0:NCS1002_1#
```

show ssh history details

```
Wed Jul 19 13:13:26.821 UTC
SSH version : Cisco-2.0

id key-exchange pubkey incipher outcipher inmac outmac start_time end_time
-----------------------------------------------------------------------------------------------------------
Incoming Session
128869diffie-hellman-group14-sha1ssh-rsa aes128-ctr aes128-ctr hmac-sha1 hmac-sha1 19-07-23 11:28:55 19
```

Os rastreamentos SSH fornecem um nível fino de detalhes sobre o processo de conexão com show ssh trace all.

<#root>

```
RP/0/RP0/CPU0:NCS1002_1#
```

show ssh trace all

```
Wed Jul 19 13:15:53.701 UTC
3986 wrapping entries (57920 possible, 40896 allocated, 0 filtered, 392083 total)
Apr 29 19:13:19.438 ssh/backup-server/event 0/RP0/CPU0 t6478 [SId:=0] Respawn-count:=1, Starting SSH Se
Apr 29 19:13:19.438 ssh/backup-server/shmem 0/RP0/CPU0 t6478 [SId:=0] Shared memory does not exist duri
```

Configurar os valores da nova chave do SSH

A configuração de rechaveamento SSH determina o tempo e o número de bytes antes que ocorra uma nova troca de chave. Ver os valores atuais usando show ssh rekey.

<#root>

```
RP/0/RP0/CPU0:NCS1004_1#
```

show ssh rekey

```
Wed Jul 19 15:23:06.379 CDT
SSH version : Cisco-2.0

id RekeyCount TimeToRekey(min) VolumeToRekey(MB)
------------------------------------------------------------
Incoming Session
1015      6      6.4              1024.0
1016      0      58.8             1024.0

Outgoing sessions
```

Para definir o volume de rechaveamento, use o comando ssh server rekey-volume [size]. O tamanho padrão da nova chave é 1024 MB.

<#root>

```
RP/0/RP0/CPU0:NCS1004_1(config)#
```

ssh server rekey-volume 4095

```
RP/0/RP0/CPU0:NCS1004_1(config)#
```

commit

Da mesma forma, defina o valor do temporizador de rechaveamento com ssh server rekey-time [time]. O valor padrão é 60 minutos.

```
RP/0/RP0/CPU0:NCS1004_1(config)# ssh server rekey-time 120
RP/0/RP0/CPU0:NCS1004_1(config)# commit
```

Depuração SSH

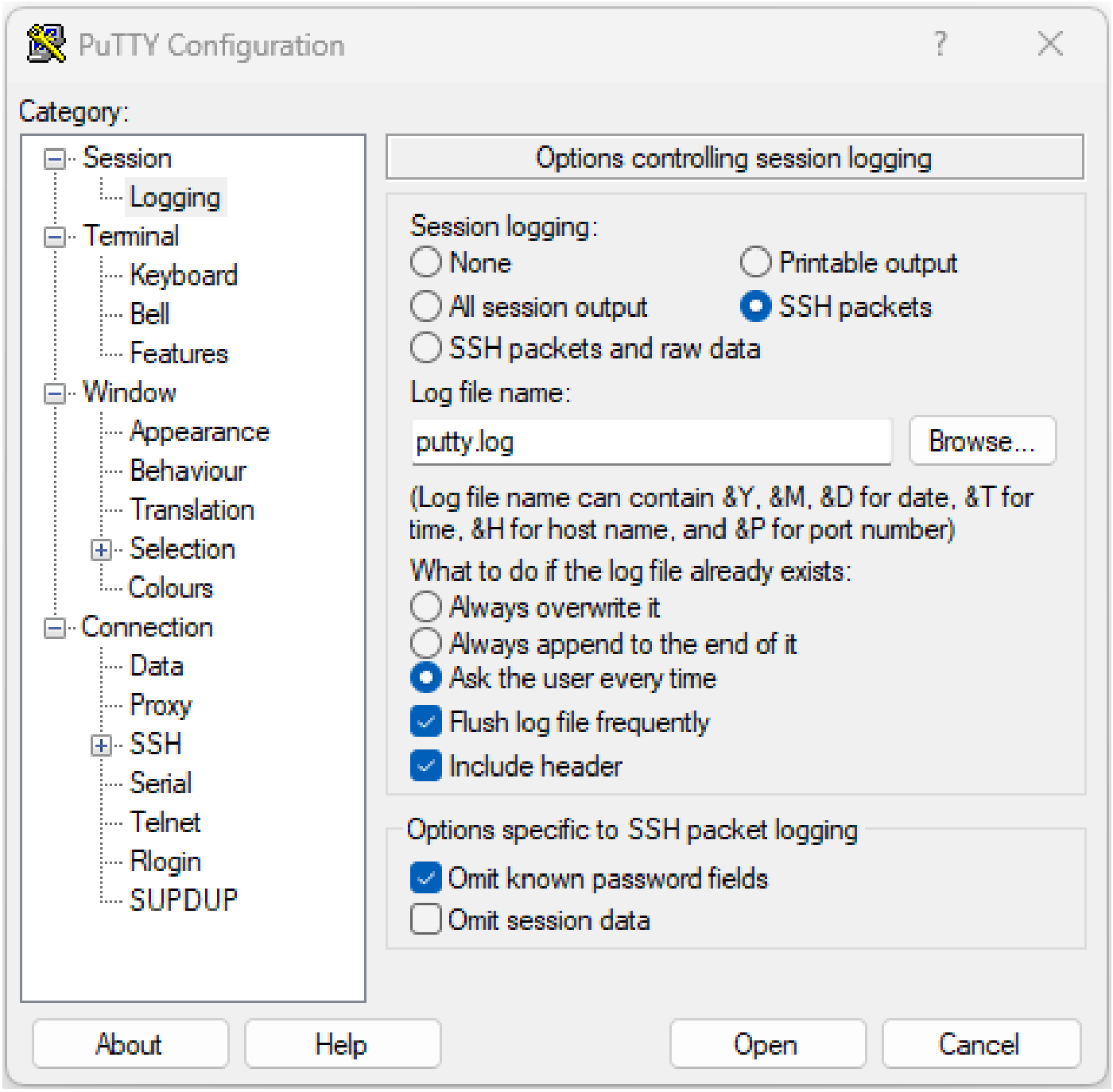
O debug ssh server exibe saídas em tempo real para sessões SSH ativas e tentativas de conexão. Para solucionar problemas de uma conexão com falha, habilite a depuração, tente a conexão e interrompa a depuração com undebug all. Registre a sessão usando PuTTY ou outro aplicativo de terminal para análise.

<#root>

```
RP/0/RP0/CPU0:NCS1002_1#
```

debug ssh server

O PuTTY inclui um recurso para registrar pacotes SSH em Session > Logging.



Captura de tela do registro PuTTY SSH

No Linux, ssh -vv (muito detalhado) fornece informações detalhadas sobre o processo de conexão SSH.

<#root>

```
ubuntu-18@admin:/$
```

ssh -vv admin@192.168.190.2

Logs adicionais

Vários técnicos de exibição capturam informações úteis no SSH.

- **show tech { ncs1k | ncs1001 | ncs1004 } detail**
- **show tech crypto session**
- **show tech ssh**
- **admin show tech { ncs1k | ncs1001 | ncs1004 }-admin**

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.