在NCS1K上调试安全外壳(SSH)

目录

简介

本文档介绍NCS1K平台上安全外壳(SSH)的基本故障排除实践。

先决条件

本文档假定读者能够熟练使用网络融合系统(NCS)1002等设备上基于XR的操作系统。

要求

Cisco建议您了解下列有关SSH连接要求的知识：

- XR映像的相关k9sec包
- 思科设备上存在SSH配置
- 成功的密钥生成、密钥交换以及主机和服务器之间的密码协商

使用的组件

本文档中的信息基于以下软件和硬件版本：

- NCS1002，带XR 7.3.1
- NCS1004，带XR 7.9.1

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

验证已安装的软件包

命令 show install active 和 show install committed 确定k9sec数据包是否存在。如果没有安装此软件包，您将无法生成加密密钥以启动SSH会话。

<#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
```

配置

NCS1K至少需要配置 ssh server v2 以便允许SSH连接。输入 show run ssh 要确保存在此配置：

<#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
```

识别生成的密钥

为了建立SSH会话，NCS1K必须存在公共加密密钥。通过识别生成的密钥是否存在 show crypto key mypubkey { dsa | ecdsa | ed25519 | rsa }.默认密钥类型为 rsa.密钥以十六进制字符串形式显示，出于安全考虑，此处省略了此项。

```
<#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>
```

要生成特定类型的密钥，请输入命令 crypto key generate { dsa | ecdsa | ed25519 | rsa } 并选择一个密钥模数。模数大小因算法而异。

密钥类型	允许的模数/曲线类型	默认模数长度（位）
dsa	512、768、1024	1024
ecdsa	nistp256、nistp384、nistp521	none
ed25519	256	256
rsa	512 到 4096	2048

验证使用成功生成的密钥 show crypto key mypubkey.

要删除现有密钥，请输入命令 crypto key zeroize { authentication | dsa | ecdsa | ed25519 | rsa } [label].确保您能够通过其他方法访问设备，因为与无加密密钥的设备断开连接会阻止通过SSH进行访问。

确定SSH服务器功能

服务器和主机在建立SSH会话之前必须同意密钥交换、主机密钥和密码。要确定NCS1K平台的功能，请输入命令 show ssh server.

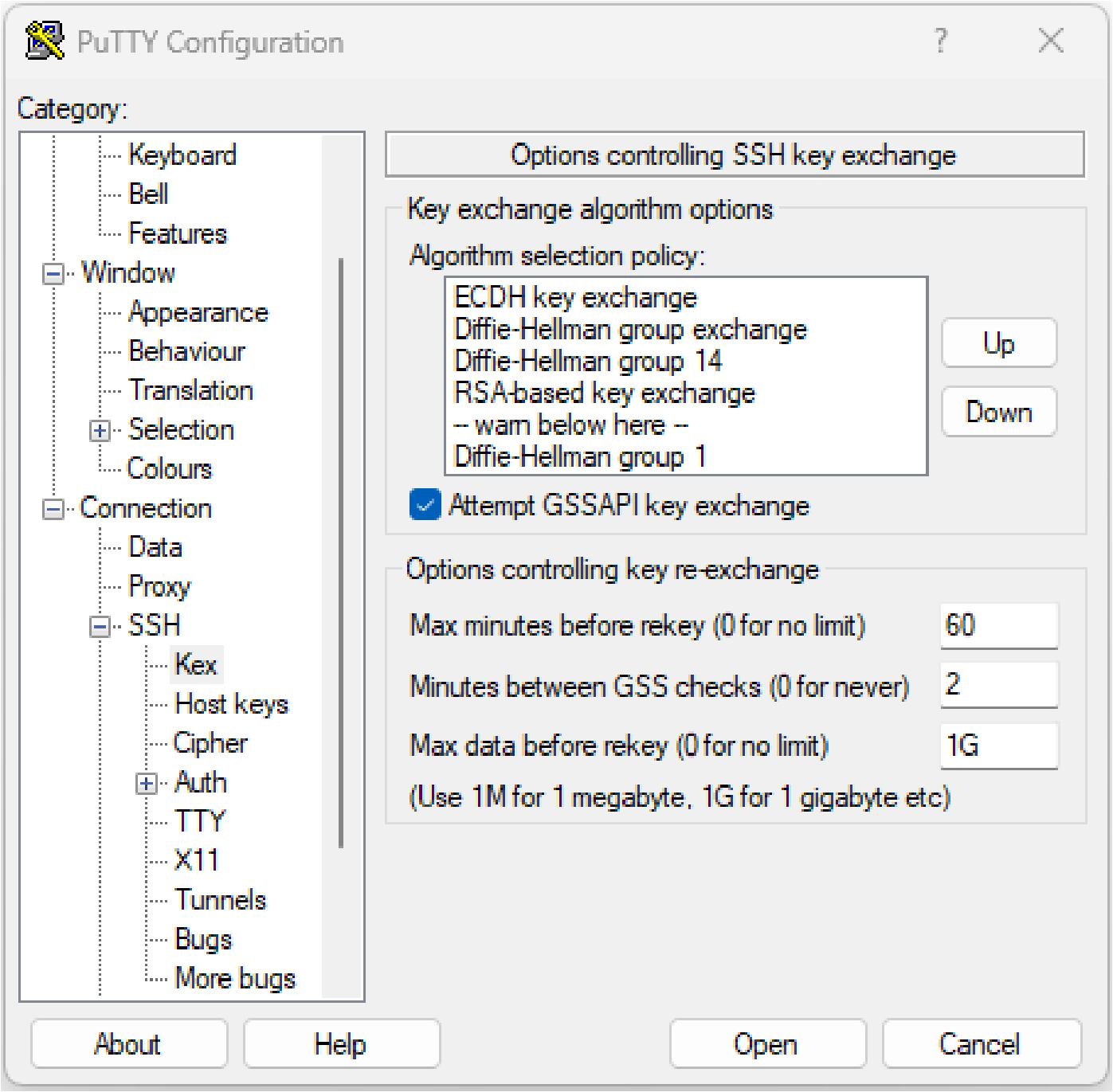
```
<#root>

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)
```

识别主机SSH功能

尝试连接的主机必须与来自服务器的至少一个主机密钥、密钥交换和加密算法匹配，才能建立SSH会话。

PuTTY

PuTTY列出支持的密钥交换、主机密钥和加密算法 Connections > SSH.主机根据自身能力自动协商算法，按照用户偏好的顺序优先选择密钥交换算法。选项 Attempt GSSAPI key exchange 不需要连接到NCS1K设备。



PuTTY SSH选项的截图

Linux

Linux服务器通常将支持的算法保留在 /etc/ssh/ssh_config 文件.此示例源自Ubuntu服务器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
```

排除SSH连接故障

这些命令有助于隔离SSH连接故障。

查看当前传入和传出SSH会话 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
```

历史SSH会话使用命令包括失败的连接尝试 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
```

SSH踪迹可提供有关连接过程的详细程度 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
```

配置SSH重新生成密钥值

SSH重新生成密钥配置确定发生新的密钥交换之前的时间和字节数。使用查看当前值 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
```

要设置重新生成密钥的卷，请使用命令 ssh server rekey-volume [size].默认的重新生成密钥大小为1024 MB。

<#root>

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

ssh server rekey-volume 4095

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

commit

同样，使用 ssh server rekey-time [time].默认值为60分钟。

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

SSH 调试

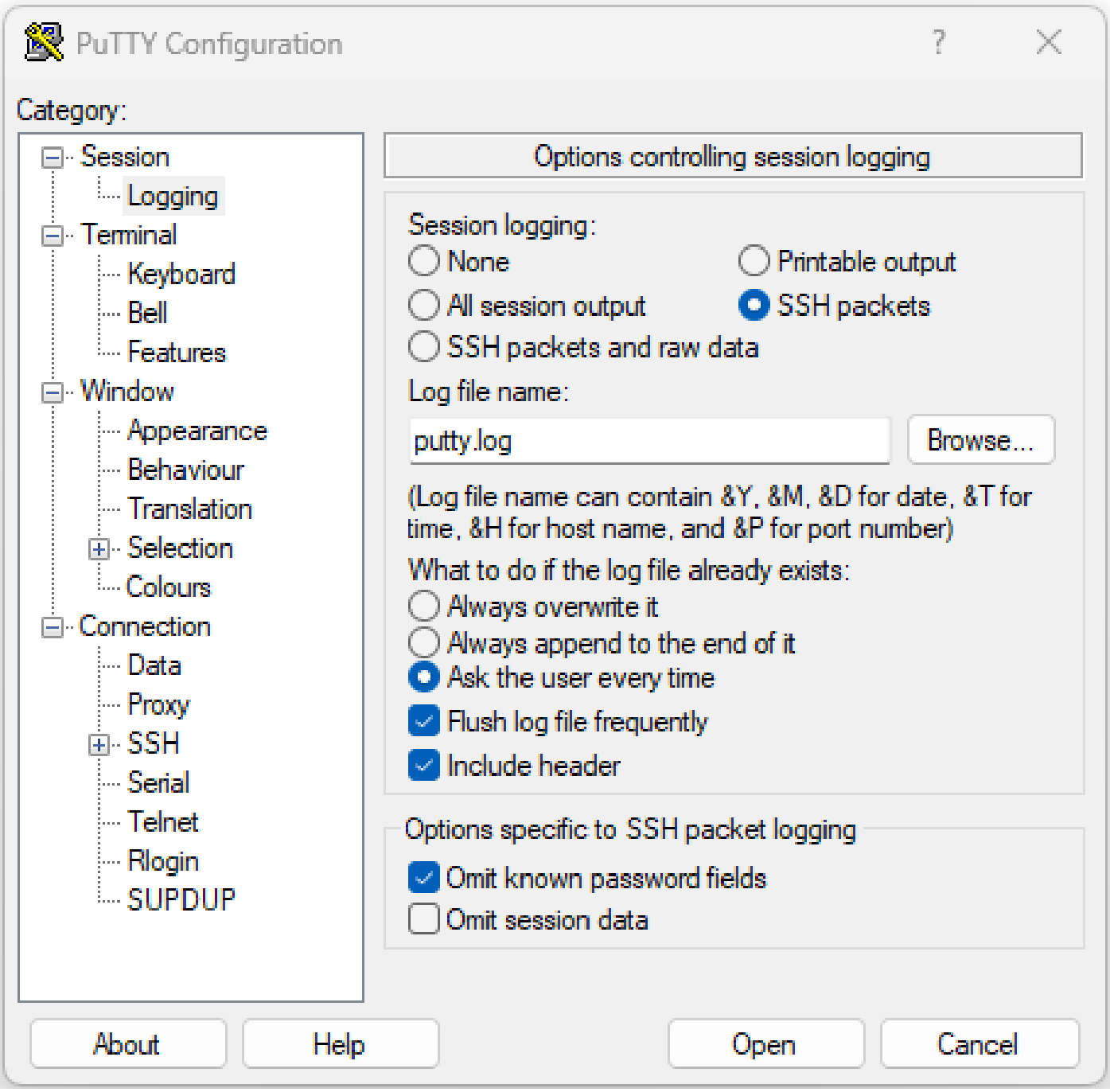
此 debug ssh server 命令显示活动SSH会话和连接尝试的实时输出。要对连接失败进行故障排除，请启用调试，尝试连接，然后使用以下命令停止调试 undebug all.使用PuTTY或其他终端应用程序记录会话进行分析。

<#root>

RP/0/RP0/CPU0:NCS1002_1#

debug ssh server

PuTTY包括一项功能，用于记录SSH数据包 Session > Logging.



PuTTY SSH日志记录的截图

在Linux中， ssh -vv （非常详细）提供有关SSH连接过程的详细信息。

<#root>

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

```
ssh -vv admin@192.168.190.2
```

其他日志

有几个show techs命令可捕获有关SSH的有用信息。

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

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）。