在NCS1K上調試安全外殼(SSH)

目錄

簡介

本文檔介紹NCS1K平台上安全外殼(SSH)的基本故障排除實踐。

必要條件

本文檔假設在諸如網路融合系統(NCS)1002等裝置上熟練使用基於XR的作業系統。

需求

Cisco建議您瞭解以下有關SSH連線要求的主題：

- XR映像的相關k9sec包
- 思科裝置上存在SSH配置
- 主機與伺服器之間成功的金鑰生成、金鑰交換和密碼協商

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 採用XR 7.3.1的NCS1002
- NCS1004，帶XR 7.9.1

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設

）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

驗證已安裝的軟體包

指令 show install active 和 show install committed 確定k9sec資料包是否存在。如果不安裝此軟體包，您將無法生成加密金鑰以啟動SSH會話。

<#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
```

組態

NCS1K至少需要配置 ssh server v2 以便允許SSH連線。輸入 show run ssh 若要確儲存在此設定：

<#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
```

標識生成的金鑰

為了建立SSH會話，NCS1K必須具有公共加密金鑰。確定生成的金鑰是否存在 show crypto key mypubkey { dsa | ecdsa | ed25519 | rsa }.預設金鑰型別為 rsa.金鑰以十六進位制字串形式顯示，出於安全考慮，此處省略。

<#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>
```

要生成特定型別的金鑰，請輸入命令 crypto key generate { dsa | ecdsa | ed25519 | rsa } 並選擇一個金鑰模數。模數大小因演算法而異。

金鑰型別	允許的模數/曲線型別	預設模數長度（位）
dsa	512、768、1024	1024
ecdsa	nistp256、nistp384、nistp521	none
ed25519	256	256
rsa	512 - 4096	2048

驗證使用成功生成的金鑰 show crypto key mypubkey.

若要移除現有金鑰，請輸入命令 crypto key zeroize { authentication | dsa | ecdsa | ed25519 | rsa } [label].確保您能夠通過其他方法訪問裝置，如與無加密金鑰的裝置斷開連線，會阻止通過SSH進行訪問。

確定SSH伺服器功能

在建立SSH會話之前，伺服器和主機必須就金鑰交換、主機金鑰和密碼達成一致。要確定NCS1K平台的功能，請輸入命令 show ssh server.

<#root>

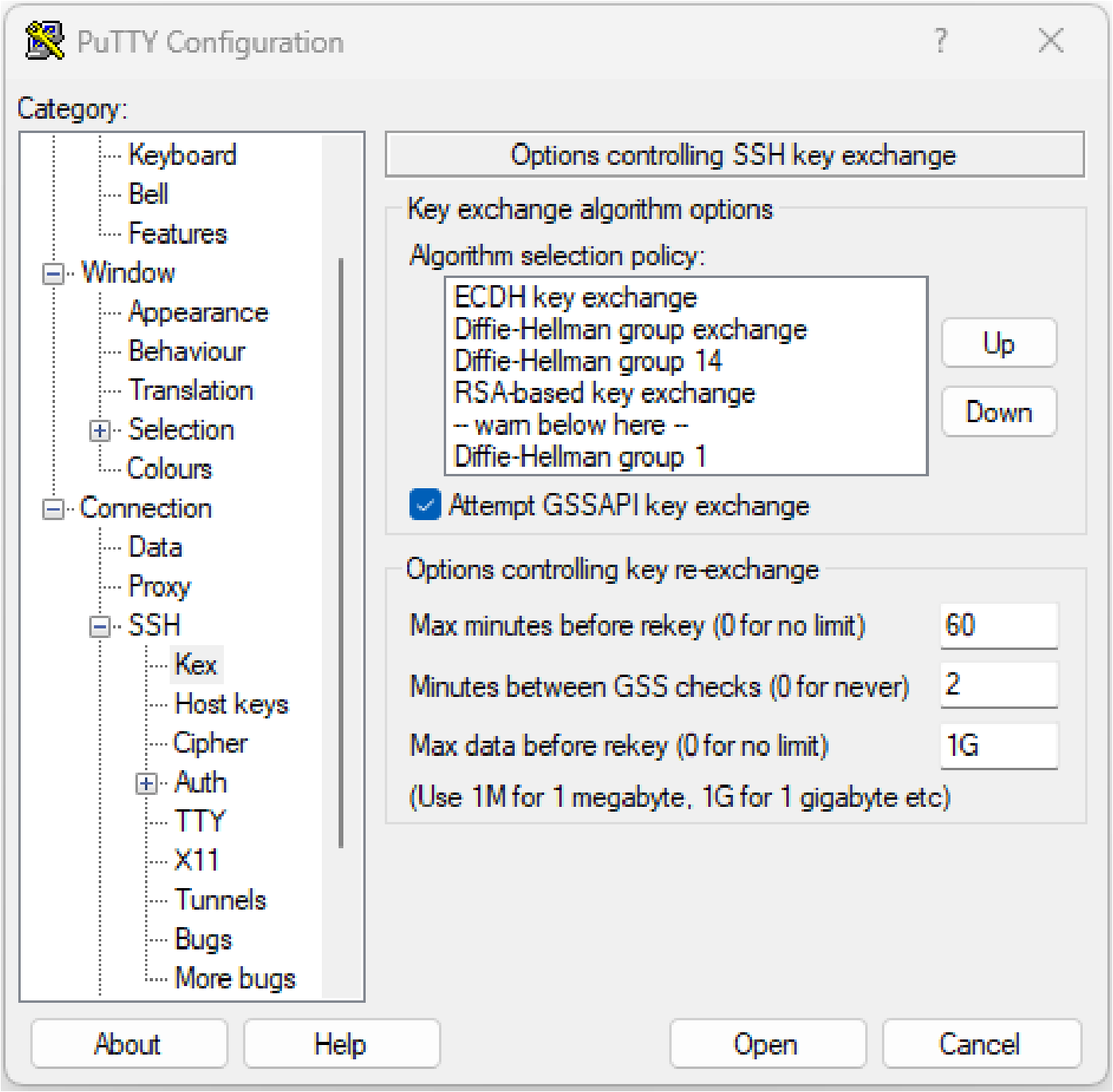
```
RP/0/RP0/CPU0:NCS1004_1#
show ssh server


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)
```

確定主機SSH功能

嘗試連線的主機必須至少匹配伺服器的一個主機金鑰、金鑰交換和加密演算法，才能建立SSH會話。

PuTTY

PuTTY列出以下項中支援的金鑰交換、主機金鑰和密碼演算法 Connections > SSH.主機根據其能力自動協商演算法，按照使用者偏好的順序優先使用金鑰交換演算法。選項 Attempt GSSAPI key exchange 不需要連線到NCS1K裝置。



PuTTY SSH選項的螢幕截圖

Linux

Linux伺服器通常將受支援的演算法保留在 /etc/ssh/ssh_config 檔案。此範例源自Ubuntu Server 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連線故障

這些命令有助於隔離使用SSH連線的故障。

檢視當前傳入和傳出SSH會話 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
```

使用命令時，歷史SSH會話包含失敗的連線嘗試 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跟蹤提供有關連線的詳細程度 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重新生成金鑰值

SSH重新生成金鑰配置確定進行新金鑰交換之前的時間和位元組數。使用檢視當前值 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
```

要設定重新生成金鑰的卷，請使用命令 ssh server rekey-volume [size].預設的重新生成金鑰大小為1024 MB。

<#root>

```
RP/0/RP0/CPU0:NCS1004_1(config)#
ssh server rekey-volume 4095

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

同樣，使用 ssh server rekey-time [time].預設值為60分鐘。

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

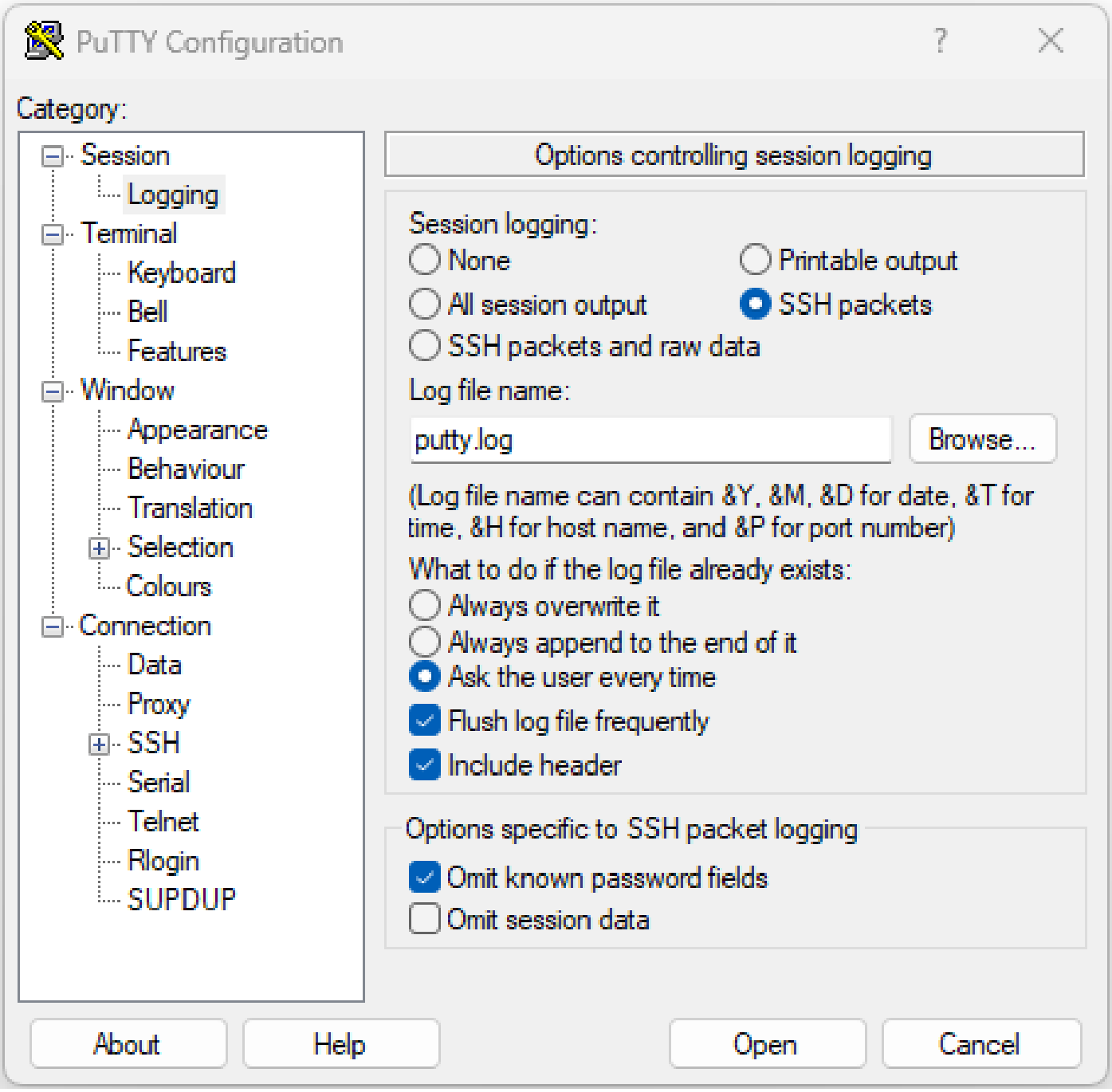
SSH調試

其 debug ssh server 命令顯示活動SSH會話和連線嘗試的即時輸出。若要對失敗的連線進行故障排除，請啟用調試，嘗試連線，然後停止調試 undebug all.使用PuTTY或其他終端應用程式記錄會話進行分析。

<#root>

```
RP/0/RP0/CPU0:NCS1002_1#
debug ssh server
```

PuTTY包括一項功能，用於記錄SSH資料包 Session > Logging.



PuTTY SSH日誌記錄的截圖

在Linux中， ssh -vv （非常詳細）提供了有關SSH連線過程的詳細資訊。

<#root>

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

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

其他日誌

有幾個show techs捕獲有關SSH的有用資訊。

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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。