Debug Secure Shell (SSH) op NCS1K

Inhoud

Inleiding

Dit document beschrijft basisprocedures voor probleemoplossing voor Secure Shell (SSH) op het NCS1K-platform.

Voorwaarden

Dit document veronderstelt competentie met op XR gebaseerde besturingssystemen op apparaten zoals het Network Convergence System (NCS) 1002.

Vereisten

Cisco raadt u aan deze onderwerpen te kennen voor de vereisten van de SSH-verbinding:

- Het relevante k9sec-pakket voor de XR-afbeelding
- SSH-configuratie aanwezig op het Cisco-apparaat
- Een succesvolle sleutelgeneratie, toetsuitwisseling en algoritmeonderhandeling tussen de host en de server

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- NCS 1002 met XR 7.3.1

- NCS 1004 met XR 7.9.1

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Controleer de geïnstalleerde pakketten

De opdrachten show install active en show install committed de aanwezigheid van het k9sec-pakket te identificeren. Zonder dit pakket geïnstalleerd, kunt u geen crypto sleutels genereren om een SSH-sessie te starten.

<#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
```

Configuratie

Minstens vereist de NCS1K de configuratie ssh server v2 om SSH-verbindingen mogelijk te maken. Voer in show run ssh om ervoor te zorgen dat deze configuratie aanwezig is:

<#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
```

Geproduceerde toetsen identificeren

Om een SSH-sessie op te zetten, moet de NCS1K een openbare cryptografische sleutel hebben. Identificeer de aanwezigheid van gegenereerde sleutels met show crypto key mypubkey { dsa | ecdsa | ed25519 | rsa }. Het standaard sleuteltype is rsa. De toets verschijnt als een hexadecimale tekenreeks, die hier wordt weggelaten voor beveiligingsdoeleinden.

<#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>
```

Om een sleutel van een bepaald type te genereren, voert u de opdracht in crypto key generate { dsa | ecdsa | ed25519 | rsa } en kies een belangrijke modulus. De modulusgrootte varieert per algoritme.

Type sleutel	Toegestane modulus/curvetypen	Standaard moduluslengte (bits)
DSA	512, 768, 1024	1024
ecdsa	nistp256, nistp384, nistp521	none
d25519	256	256
RSA	512 t/m 4096	2048

Controleer de sleutel die met succes is gegenereerd met show crypto key mypubkey.

Om een bestaande toets te verwijderen voert u de opdracht in crypto key zeroize { authentication | dsa | ecdsa | ed25519 | rsa } [label]. Zorg ervoor dat u toegang tot het apparaat op een andere manier als ontkoppeling van een apparaat zonder crypto toetsen blokkeert toegang met SSH.

Mogelijkheden voor SSH-servers identificeren

De server en de host moeten het eens worden over een key exchange, host key en algoritme voordat een SSH sessie kan worden ingesteld. Om de mogelijkheden van het NCS1K-platform te identificeren, voert u de opdracht in show ssh server.

<#root>

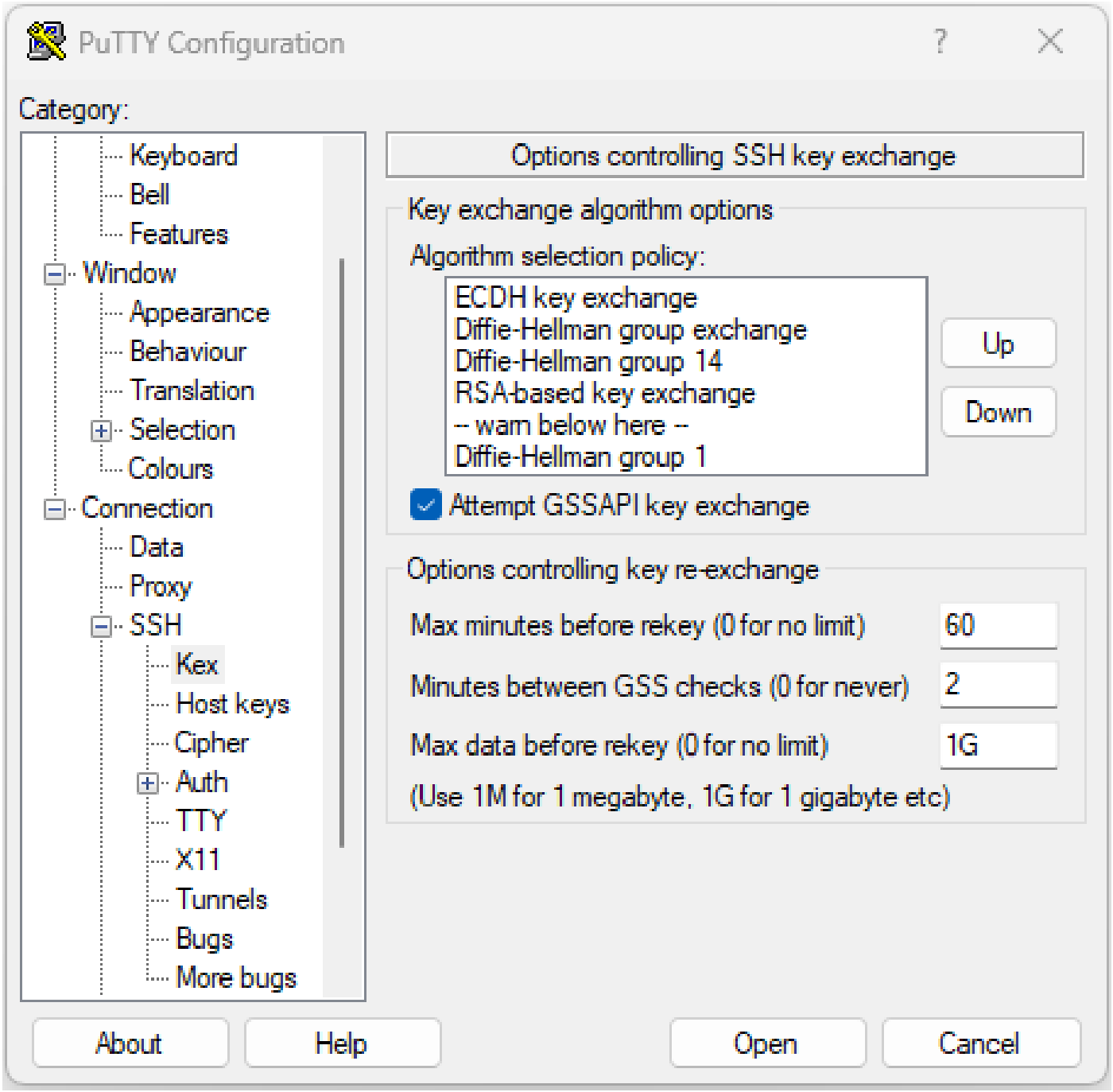
```
RP/0/RP0/CPU0:NCS1004_1#
show ssh server


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)
```

Mogelijkheden voor SSH-host identificeren

De host die probeert verbinding te maken moet minimaal één hostkey, key exchange en encryptie algoritme van de server aan om een SSH sessie te kunnen maken.

PuTTY

PuTTY geeft de ondersteunde sleuteluitwisseling, hostsleutel en algoritmen weer onder Connections > SSH. De host onderhandelt automatisch over de algoritmen op basis van zijn mogelijkheden, waarbij hij de voorkeur geeft aan het sleuteluitwisselingsalgoritme in volgorde van voorkeur van de gebruiker. De optie Attempt GSSAPI key exchange is niet vereist om verbinding te maken met een NCS1K-apparaat.



Screenshot van de PuTTY SSH-opties

Linux

Linux-servers houden de ondersteunde algoritmen meestal in de /etc/ssh/ssh_config bestand. Dit voorbeeld is afkomstig van 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
```

Probleemoplossing voor SSH-verbindingen

Deze opdrachten kunnen helpen storingen met SSH-verbindingen te isoleren.

Zie huidige inkomende en uitgaande SSH-sessies met 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
```

Historische SSH-sessies omvatten mislukte verbindingspogingen met de opdracht 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-sporen geven een fijn detailniveau van het aansluitingsproces met 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
```

Waarden voor SSH-re-toetsen configureren

De configuratie van de SSH-re-toets bepaalt de tijd en het aantal bytes voordat een nieuwe sleuteluitwisseling plaatsvindt. Zie de huidige waarden met 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
```

Gebruik de opdracht om het volume opnieuw in te stellen ssh server rekey-volume [size]. De standaardgrootte voor het opnieuw instellen van de toets is 1024 MB.

<#root>

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

ssh server rekey-volume 4095

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

commit

Stel ook de waarde van de timer voor opnieuw instellen in op ssh server rekey-time [time]. De standaardwaarde is 60 minuten.

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

SSH-debug

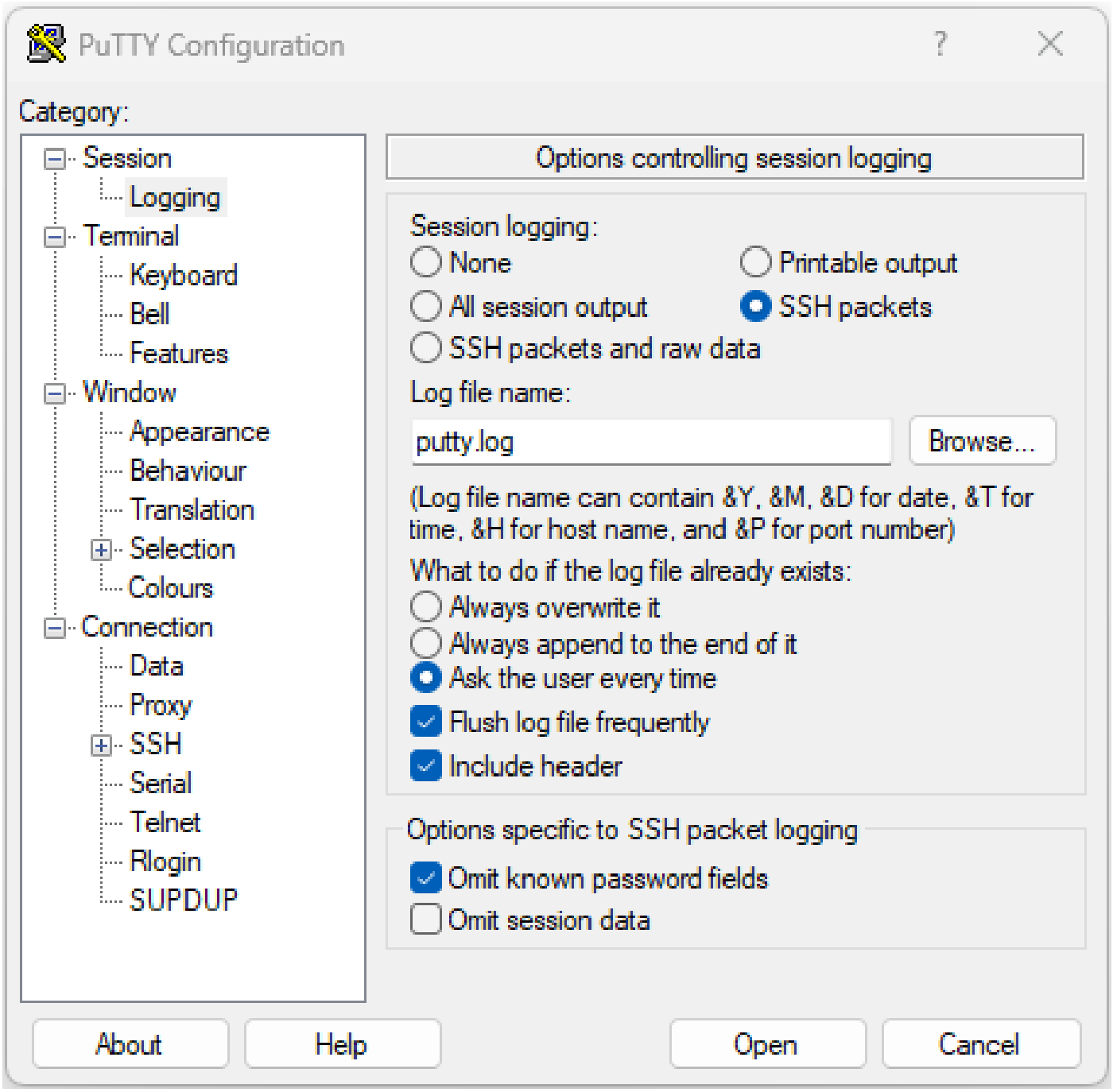
Het debug ssh server Het bevel toont real-time output voor actieve zittingen van SSH en verbindingspogingen. Als u een mislukte verbinding wilt oplossen, schakelt u de debug in, probeert u de verbinding en stopt u de debug met undebug all. Log de sessie in met PuTTY of een andere terminaltoepassing voor analyse.

<#root>

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

debug ssh server

PuTTY bevat een functie voor het vastleggen van SSH-pakketten onder Session > Logging.



Screenshot van PuTTY SSH-logboekregistratie

In Linux, ssh -vv (zeer uitgebreid) geeft gedetailleerde informatie over het SSH-verbindingsproces.

<#root>

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

ssh -vv admin@192.168.190.2

Aanvullende logbestanden

Verschillende show techs vangen nuttige informatie over SSH.

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.