NCS1K에서 SSH(Secure Shell) 디버그

목차

소개

이 문서에서는 NCS1K 플랫폼의 SSH(Secure Shell)에 대한 기본적인 트러블슈팅 사례에 대해 설명합니다.

사전 요구 사항

이 문서에서는 NCS(Network Convergence System) 1002와 같은 디바이스에서 XR 기반 운영 체제에 대한 숙련된 기능을 전제로 합니다.

요구 사항

Cisco에서는 SSH 연결 요구 사항에 대한 다음 항목에 대해 알고 있는 것이 좋습니다.

- XR 이미지에 대한 관련 k9sec 패키지
- Cisco 디바이스에 있는 SSH 컨피그레이션
- 호스트와 서버 간의 성공적인 키 생성, 키 교환 및 암호 협상

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- NCS1002 및 XR 7.3.1
- NCS1004 및 XR 7.9.1

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

설치된 패키지 확인

명령 show install active 및 show install committed k9sec 패키지가 있는지 확인합니다. 이 패키지를 설치하지 않으면 SSH 세션을 시작하기 위한 암호화 키를 생성할 수 없습니다.

<#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

설정

최소한 NCS1K는 ssh server v2 SSH 연결을 허용합니다. 입력 사항 show run ssh 이 컨피그레이션을 사용하려면

<#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
```

생성된 키 식별

SSH 세션을 설정하려면 NCS1K에 공개 암호화 키가 있어야 합니다. 생성된 키의 존재 확인 show crypto key mypubkey { dsa | ecdsa | ed25519 | rsa }. 기본 키 유형은 rsa. 키는 16진수 문자열로 표시되며, 보안을 위해 여기에 생략됩니다.

<#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>
```

특정 유형의 키를 생성하려면 명령을 입력합니다 crypto key generate { dsa | ecdsa | ed25519 | rsa } 키 모듈러스를 선택합니다. 모듈러스 크기는 알고리즘에 따라 다릅니다.

키 유형	허용되는 모듈러스/커브 유형	기본 모듈러스 길이(비트)
DSA	512, 768, 1024	1024
ecdsa	nistp256, nistp384, nistp521	none
ed25519	256	256
rsa	512~4096	2048

키가 성공적으로 생성되었는지 확인합니다. show crypto key mypubkey.

기존 키를 제거하려면 명령을 입력합니다 crypto key zeroize { authentication | dsa | ecdsa | ed25519 | rsa } [label]. 암호

화 키가 없는 디바이스에서 연결을 해제하면 SSH로 액세스가 차단되므로 다른 방법을 통해 디바이스에 액세스할 수 있어야 합니다.

SSH 서버 기능 식별

SSH 세션을 설정하기 전에 서버와 호스트가 키 교환, 호스트 키 및 암호에 동의해야 합니다.
NCS1K 플랫폼의 기능을 식별하려면 명령을 입력합니다 show ssh server.

<#root>

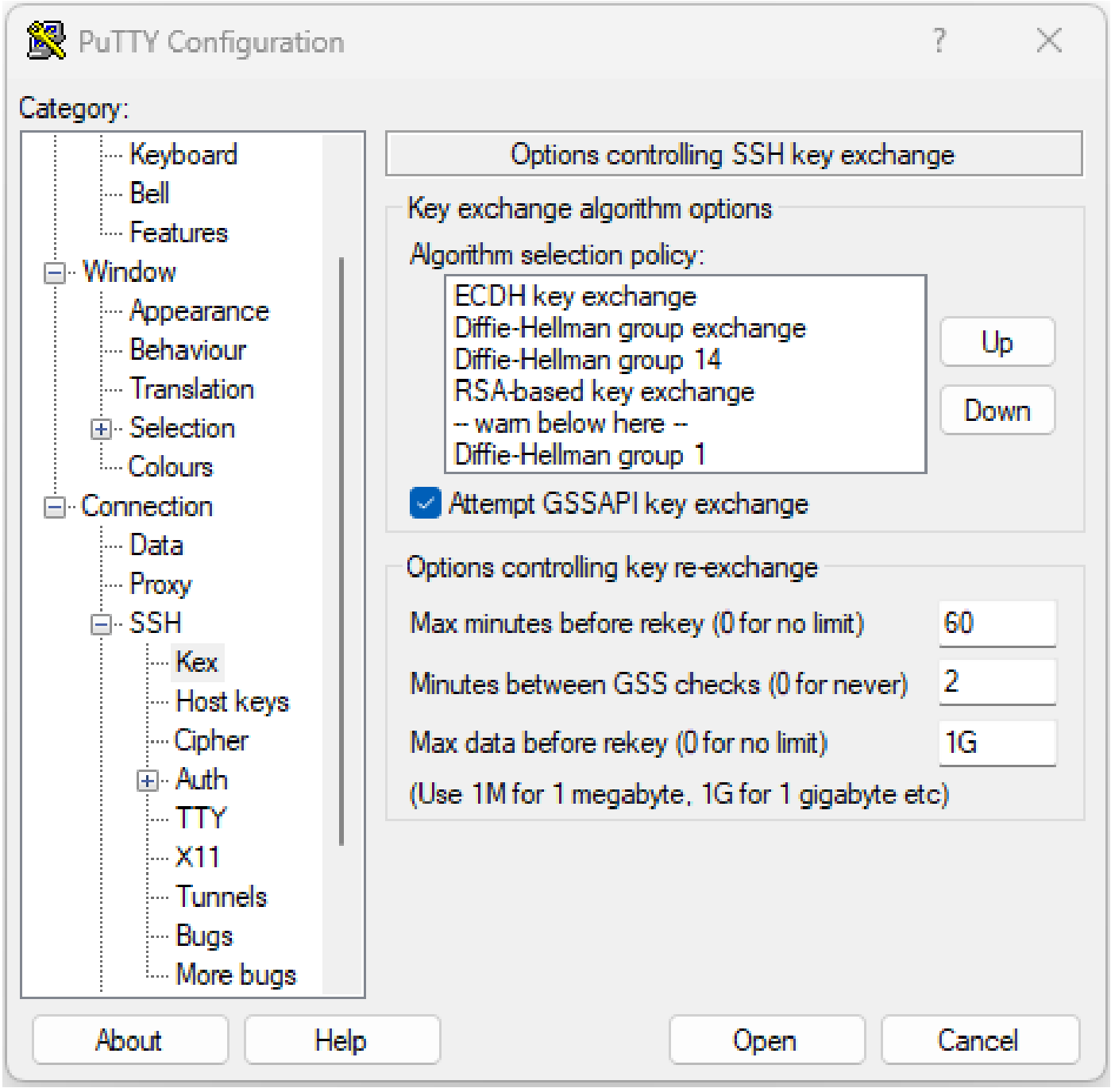
```
RP/0/RP0/CPU0:NCS1004_1#
show ssh server


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)
```

호스트 SSH 기능 식별

SSH 세션을 설정하려면 연결을 시도하는 호스트가 서버의 호스트 키, 키 교환 및 암호화 알고리즘을 하나 이상 일치해야 합니다.

PuTTY

PuTTY는에서 지원되는 키 교환, 호스트 키 및 암호 알고리즘을 나열합니다. Connections > SSH. 호스트는 기능을 기반으로 사용자 환경 설정 순서대로 키 교환 알고리즘을 선호하여 알고리즘을 자동으로 협상합니다. 옵션 Attempt GSSAPI key exchange 는 NCS1K 디바이스에 연결하는 데 필요하지 않습니다.



PuTTY SSH 옵션의 스크린샷

Linux

Linux 서버는 일반적으로 지원되는 알고리즘을 /etc/ssh/ssh_config 파일을 클릭합니다. 이 예는 Ubuntu Server 18.04.3에서 시작합니다.

```
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
```

SSH 연결 문제 해결

이러한 명령은 SSH 연결에서 오류를 격리하는 데 도움이 될 수 있습니다.

를 사용하여 현재 수신 및 발신 SSH 세션 보기 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
```

기록 SSH 세션에는 명령을 사용한 실패한 연결 시도가 포함됩니다 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 추적은 와의 연결 프로세스에 대한 세부 정보 레벨을 제공합니다. 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
```

SSH 키 재설정 값 구성

SSH 키 재지정 컨피그레이션은 새 키 교환이 발생하기 전의 시간 및 바이트 수를 결정합니다. 다음을 사용하여 현재 값을 확인합니다. 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
```

키 재설정 볼륨을 설정하려면 명령을 사용합니다 ssh server rekey-volume [size]. 기본 키 재설정 크기는 1024MB입니다.

```
<#root>

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

ssh server rekey-volume 4095


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

commit
```

마찬가지로 키 재설정 타이머 값을 ssh server rekey-time [time]. 기본값은 60분입니다.

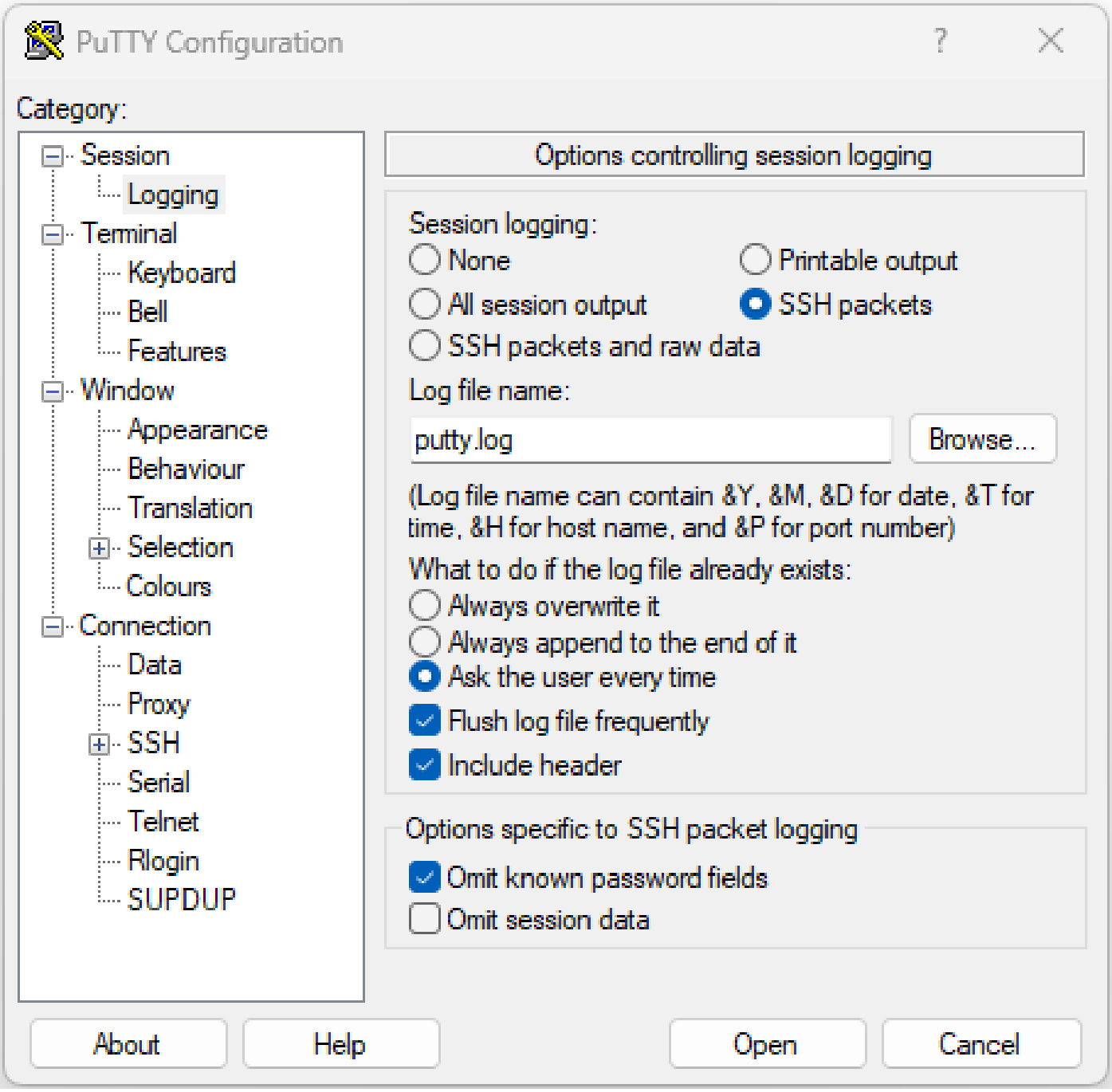
```
RP/0/RP0/CPU0:NCS1004_1(config)# ssh server rekey-time 120
RP/0/RP0/CPU0:NCS1004_1(config)# commit
```

SSH 디버그

이 debug ssh server 이 명령은 활성 SSH 세션 및 연결 시도에 대한 실시간 출력을 표시합니다. 오류가 발생한 연결을 트러블슈팅하려면 디버그를 활성화하고 연결을 시도한 다음 undebug all. 분석을 위해 PuTTY 또는 다른 터미널 애플리케이션을 사용하여 세션을 로깅합니다.

```
<#root>

RP/0/RP0/CPU0:NCS1002_1#

debug ssh server
```

PuTTY에는 SSH 패킷 로깅 기능이 포함되어 있습니다. Session > Logging.



PuTTY SSH 로깅 스크린샷

Linux에서는 ssh -vv (매우 자세한 정보) SSH 연결 프로세스에 대한 자세한 정보를 제공합니다.

<#root>

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

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

추가 로그

몇 가지 show techs는 SSH에서 유용한 정보를 캡처합니다.

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

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.