NCS1Kでのセキュアシェル(SSH)のデバッグ

内容

概要

前提条件

- 要件
- 使用するコンポーネント

インストール済みパッケージの確認

- コンフィギュレーション
- 生成されたキーの識別
- SSHサーバ機能の特定
- ホストのSSH機能の特定
  - PuTTY
  - Linux

SSH接続のトラブルシューティング

- SSHキー再生成の値の設定
- SSH のデバッグ
- その他のログ

概要

このドキュメントでは、NCS1Kプラットフォームでのセキュアシェル(SSH)の基本的なトラブルシューティング方法について説明します。

前提条件

このドキュメントは、Network Convergence System(NCS)1002などのデバイス上のXRベースのオペレーティングシステムに習熟していることを前提としています。

要件

SSH接続の要件に関する次の項目に関する知識があることが推奨されます。

- XRイメージに関連するk9secパッケージ
- Ciscoデバイスに存在するSSH設定
- ホストとサーバ間のキー生成、キー交換、および暗号ネゴシエーションの成功

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- XR 7.3.1を搭載したNCS1002
- NCS1004（XR7.9.1を搭載）

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

インストール済みパッケージの確認

コマンド show install active と show install committed k9secパッケージの存在を確認します。このパッケージがインストールされていないと、SSHセッションを開始するための暗号キーを生成できません。

```
<#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
```

コンフィギュレーション

少なくとも、NCS1Kには次の設定が必要です ssh server v2 SSH接続を許可します。 show run ssh この設定が存在することを確認するには、次の手順を実行します。

```
<#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
```

生成されたキーの識別

SSHセッションを確立するには、NCS1Kに公開暗号キーが存在する必要があります。生成されたキーの存在の特定 show crypto key mypubkey { dsa | ecdsa | ed25519 | rsa }を参照。デフォルトのキータイプは次のとおりです rsaを参照。キーは16進数の文字列として表示され、ここではセキュリティ上の理由から省略します。

```
<#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>
```

特定のタイプのキーを生成するには、コマンドを入力します crypto key generate { dsa | ecdsa | ed25519 | rsa } キーモジュラスを選択します。モジュラスサイズはアルゴリズムによって異なります。

キーの種類	許容モジュラス/曲線タイプ	デフォルトのモジュラス長（ビット）
DSA	512、768、1024	1024
ecdsa	nips256、nips384、nips521	none
ed25519	256	256
rsa	512 ~ 4096	2048

次のコマンドでキーが正常に生成されたことを確認します。 show crypto key mypubkeyを参照。

既存のキーを削除するには、コマンドを入力します crypto key zeroize { authentication | dsa | ecdsa | ed25519 | rsa } [label]を参照。暗号キーを使用せずにデバイスから切断すると、SSHを使用したアクセスがブロックされるため、他の手段でデバイスにアクセスできることを確認します。

SSHサーバ機能の特定

サーバとホストは、SSHセッションを確立する前に、鍵交換、ホスト鍵、および暗号について合意する必要があります。NCS1Kプラットフォームの機能を確認するには、次のコマンドを入力します show ssh serverを参照。

<#root>

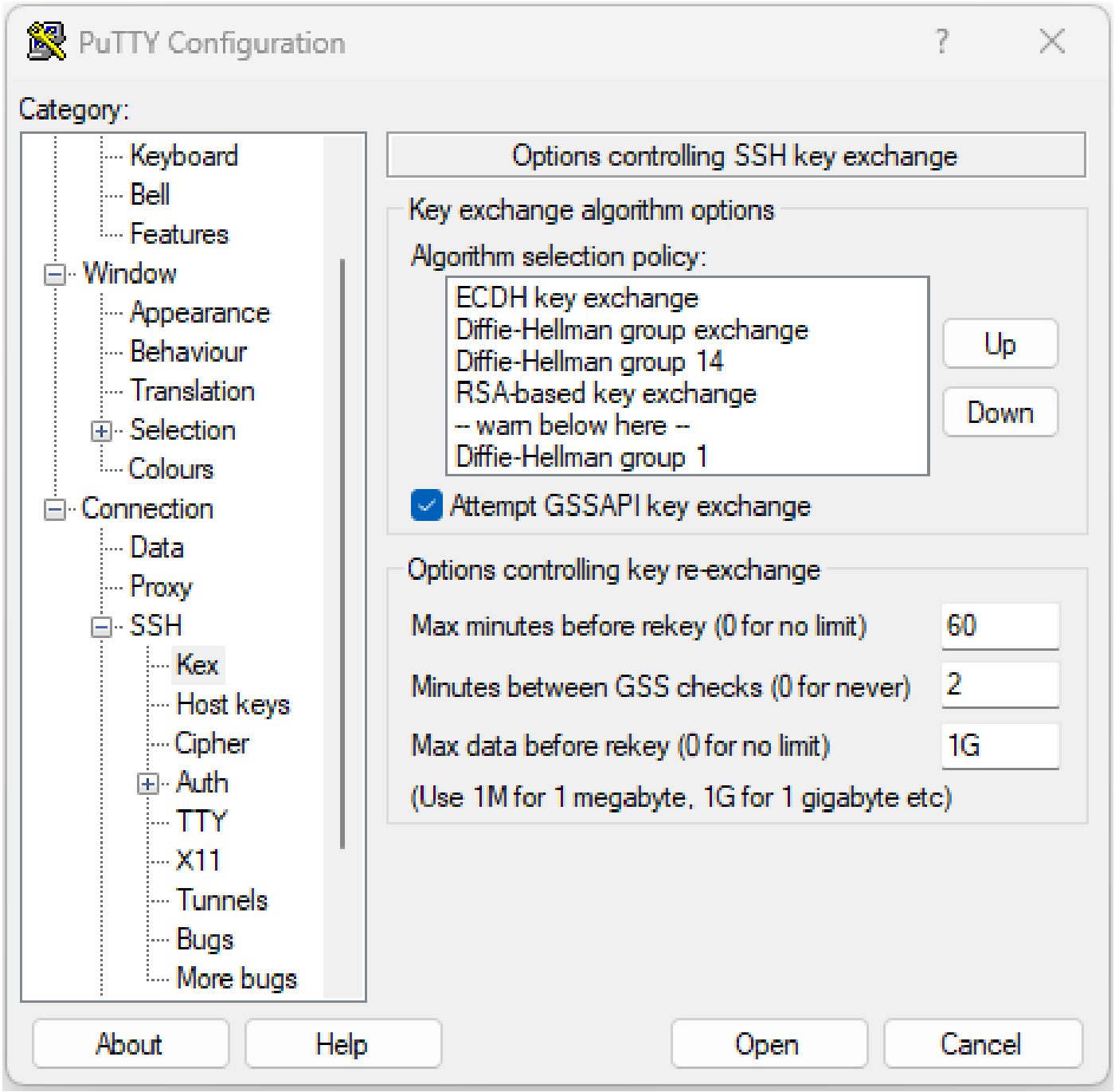
```
RP/0/RP0/CPU0:NCS1004_1#
show ssh server


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)
```

ホストのSSH機能の特定

SSHセッションを確立するには、接続を試行するホストが、サーバからの少なくとも1つのホストキー、キー交換、および暗号化アルゴリズムと一致している必要があります。

PuTTY

PuTTYは、サポートされるキー交換、ホストキー、および暗号アルゴリズムを Connections > SSH を参照。ホストは、自身の機能に基づいてアルゴリズムを自動的にネゴシエートし、ユーザの好みに応じてキー交換アルゴリズムを優先します。オプション Attempt GSSAPI key exchange NCS1Kデバイスに接続するために必要ではありません。



PuTTY SSHオプションのスクリーンショット

Linux

Linuxサーバは通常、サポートされているアルゴリズムを /etc/ssh/ssh_config 出力を提供してください。この例は、Ubuntu Server 18.04.3に基づいています。

```
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接続のトラブルシューティング

これらのコマンドは、SSH接続の障害を切り分けるのに役立ちます。

現在の着信および発信SSHセッションを show ssh session detailsを参照。

```
<#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
```

過去のSSHセッションには、コマンドによる接続試行の失敗が含まれます。 show ssh history detailを参照。

```
<#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トレースは、接続プロセスに関する詳細なレベルの情報を提供します。 show ssh trace allを参照。

```
<#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キー再生成の値の設定

SSHキー再生成の設定により、新しいキー交換が発生するまでの時間とバイト数が決まります。次の方法で現在の値を表示します show ssh rekeyを参照。

<#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
```

キー再生成ボリュームを設定するには、次のコマンドを使用します ssh server rekey-volume [size]を参照。デフォルトのキー再生成サイズは1024 MBです。

<#root>

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

ssh server rekey-volume 4095

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

commit

同様に、キー再生成タイマー値を ssh server rekey-time [time]を参照。デフォルト値は 60 分です。

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

SSH のデバッグ

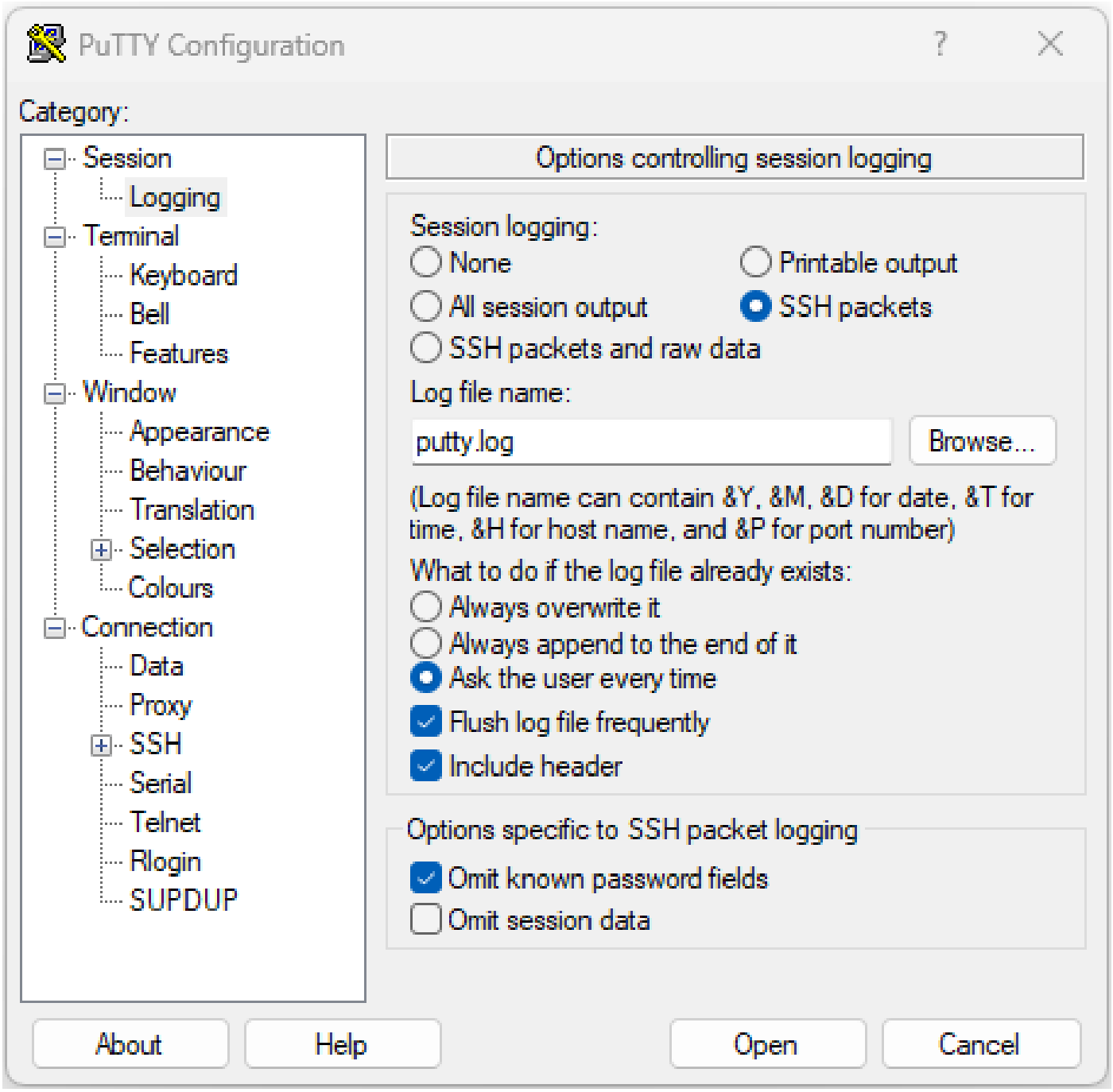
「 debug ssh server コマンドは、アクティブなSSHセッションおよび接続試行に関するリアルタイム出力を表示します。障害が発生した接続をトラブルシューティングするには、デバッグを有効にし、接続を試行してから、次のコマンドでデバッグを停止します。 undebug allを参照。PuTTYまたは別のターミナルアプリケーションを使用してセッションを口グに記録し、分析します。

<#root>

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

debug ssh server

PuTTYには、SSHパケットをロギングする機能があります。 Session > Loggingを参照。



PuTTY SSHロギングのスクリーンショット

Linuxでは – ssh -vv （非常に冗長）は、SSH接続プロセスに関する詳細情報を提供します。

<#root>

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

ssh -vv admin@192.168.190.2

その他の口グ

いくつかのshow techsは、SSHに関する有用な情報をキャプチャします。

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

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。