# Debug Secure Shell (SSH) على NCS1K

## المحتويات



## المقدمة

يصف هذا المستند ممارسات أستكشاف الأخطاء وإصلاحها الأساسية ل Secure Shell (SSH) على منصة NCS1K.

## المتطلبات الأساسية

يفترض هذا المستند الكفاءة مع أنظمة التشغيل المستندة إلى XR على أجهزة مثل نظام تقارب الشبكات (NCS) 1002.

### المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية لمتطلبات اتصال SSH:

- حزمة k9sec ذات الصلة لصورة XR
- تكوين SSH موجود على جهاز Cisco
- إنشاء مفتاح انجو تبادل مفتاح وتفاوض تشفير بين المضيف والخادم

### المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- NCS1002 مع XR 7.3.1
- NCS1004 مع XR 7.9.1

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

# التحقق من الحزم المثبتة

الأوامر show install active و show install committed التعرف على وجود حزمة k9sec. بدون تثبيت هذه الحزمة، لا يمكن إنشاء مفاتيح تشفير لبدء جلسة SSH.

```
<#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
```

## التكوين

يتطلب NCS1K على الأقل التكوين ssh server v2 للسماح باتصالات SSH. أدخل show run ssh لضمان وجود هذا التكوين:

```
<#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
```

## تحديد المفاتيح التي تم إنشاؤها

من أجل إنشاء جلسة SSH، يجب أن يكون لدى NCS1K مفتاح تشفير عام موجود. تعريف وجود المفاتيح التي تم إنشاؤها بواسطة show crypto key mypubkey { dsa | ecdsa | ed25519 | rsa }. نوع المفتاح الافتراضي هو rsa. يظهر المفتاح كسلسلة سداسية عشرية، مخزنة بأمان في الأغراض العامة.

<#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>
```

أدخل in order to خلق مفتاح من نوع خاص، الأمر crypto key generate { dsa | ecdsa | ed25519 | rsa } واختيار معامل أساسي. يختلف حجم المعامل حسب الخوارزمية.

| نوع المفتاح | أنواع المعامل/المنحنى المسموح بها | طول المعامل الافتراضي (بت) |
|---|---|---|
| DSA | 512، 768، 1024 م | 1024 |
| ECDSA | nistp256 و nistp384 و nistp521 | none |
| د.إ. 25519 | 256 | 256 |
| RSA | من 512 إلى 4096 | 2048 |

التحقق من صحة المفتاح الذي تم إنشاؤه بنجاح باستخدام show crypto key mypubkey.

دخلت in order to أزلت مفاتيح موجود، الأمر crypto key zeroize { authentication | dsa | ecdsa | ed25519 | rsa } [ label ]. تأكد من حصولك على الوصول إلى الجهاز من خلال وسائل أخرى مثل قطع الاتصال من جهاز ال توجد به مفاتيح تشفير تمنع الوصول إلى SSH.

## التعرف على إمكانيات خادم SSH

يجب أن يتفق الخادم والمضيف على تبادل مفاتيح ومفاتيح مضيف وشفرة قبل إنشاء جلسة SSH. دخلت in order to عينت القدرة من ال NCS1K منصة، الأمر show ssh server.

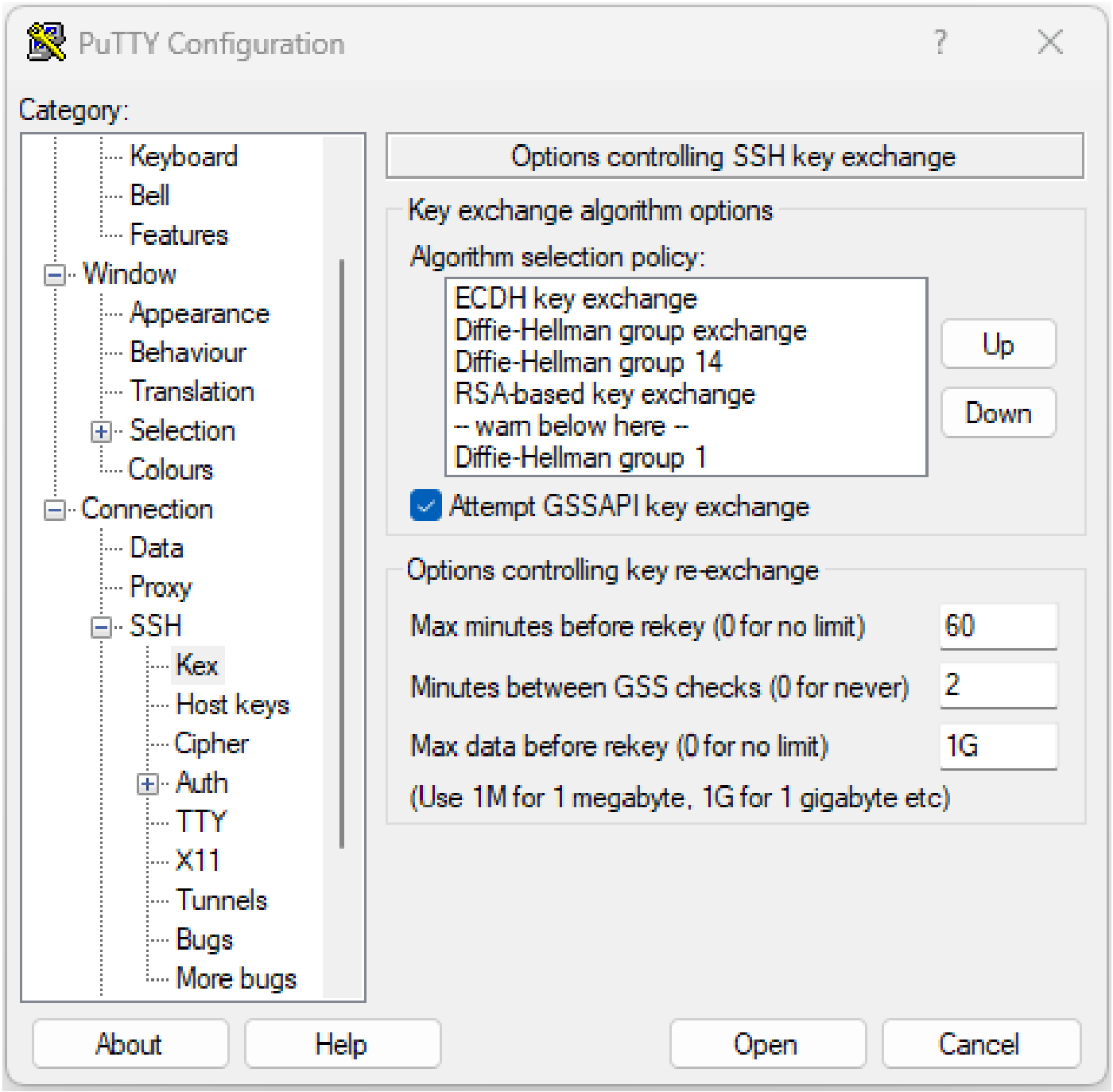
```
<#root>

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)
```

## التعرف على إمكانيات SSH الخاصة بالمضيف

يجب أن يطابق المضيف الذي يحاول الاتصال خوارزمية مضيف واحد على الأقل، وتبادل المفاتيح، وخوارزمية التشفير من الخادم لإنشاء جلسة SSH.

بوتي

يسرد PuTTY خوارزميات تبادل المفاتيح ومفاتيح المضيف والشفرة المدعومة أدناه Connections > SSH. يقوم المضيف بالتفاوض التلقائي على الخوارزميات استنادا إلى إمكانياته، مفضلا خوارزمية تبادل المفاتيح بالترتيب الذي يفضله المستخدم. الخيار Attempt GSSAPI key exchange غير مطلوب للاتصال بجهاز NCS1K.




لقطة شاشة لخيارات PuTTY SSH

ليكنس

تحافظ مداوخ Linux عادة على الخوارزميات المدعومة في /etc/ssh/ssh_config ملف. يمكنك أن تجد هذا المثال من مخدم Ubuntu 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
```

# أستكشاف أخطاء إتصالات SSH وإصلاحها

يمكن أن تساعد هذه الأوامر في عزل حالات الفشل باستخدام إتصالات SSH.

راجع جلسات SSH الواردة والصادرة الحالية مع 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
```

تتضمن جلسات عمل SSH السابقة محاولات اتصال فاشلة مع الأمر 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
```

توفر آثار برووتوكول طبقة الأمان (SSH) مستوى رائع من التفاصيل حول عملية الاتصال باستخدام 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
```

## تكوين قيم إعادة مفاتيح SSH

يحدد تكوين إعادة مفتاح SSH وقت وعدد وحدات البايت قبل حدوث تبادل مفاتيح جديد. راجع القيم الحالية باستخدام 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
```

in order to ثبتت ال rekey حجم، استعملت الأمر ssh server rekey-volume [ size ]. الحجم الافتراضي إلعادة المفتاح وه 1024 ميغابايت.

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

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

بالمثل، قم بتعيين قيمة مؤقت re-key مع ssh server rekey-time [ time ]. القيمة الافتراضية هي 60 دقيقة.

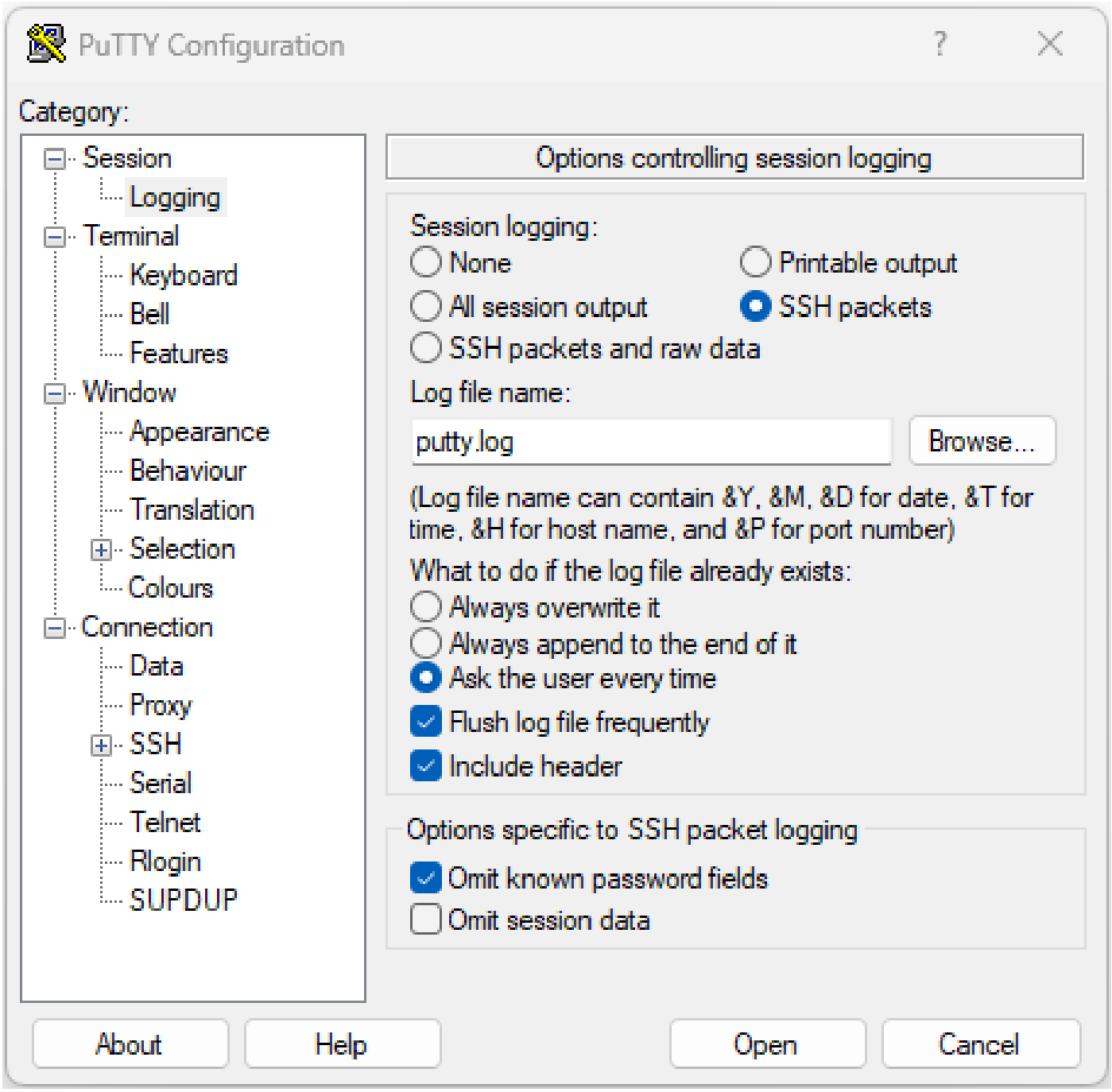
```
RP/0/RP0/CPU0:NCS1004_1(config)# ssh server rekey-time 120
RP/0/RP0/CPU0:NCS1004_1(config)# commit
```

## تصحيح أخطاء SSH

يعرض الأمر debug ssh server يعرض الأمر مخرجات الوقت الفعلي لجلسات SSH النشطة ومحاولات الاتصال. لاستكشاف أخطاء الاتصال الفاشل وإصلاحها، قم بتمكين تصحيح الأخطاء وحاول الاتصال، ثم قم بإيقاف تصحيح الأخطاء باستخدام undebug all. قم بتسجيل الجلسة باستخدام PuTTY أو تطبيق طرفي آخر للتحليل.

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

يتضمن PuTTY ميزة لتسجيل حزم SSH أسفل Session > Logging.




لقطة شاشة لتسجيل PuTTY SSH

في لينكس، ssh -vv (بشكل صريح للغاية) يوفر معلومات تفصيلية حول عملية اتصال SSH.

<#root>

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

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

## السجلات الإضافية

يقوم العديد من فنانين العرض بالتقاط معلومات مفيدة على SSH.

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

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).