تكوين SSH على الموجّهات والمُبدلات

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين Secure Shell (SSH) وتصحيح أخطائه على موجهات Cisco أو المُبدلات التي تقوم بتشغيل برنامج Cisco IOS®.

المتطلبات الأساسية

المتطلبات

يجب أن تكون صورة Cisco IOS المستخدمة صورة k9 (تشفير) لدعم SSH. على سبيل المثال، c3750e-universalk9-tar.122-35.SE5.tar هو صورة k9 (تشفير).

المكونات المستخدمة

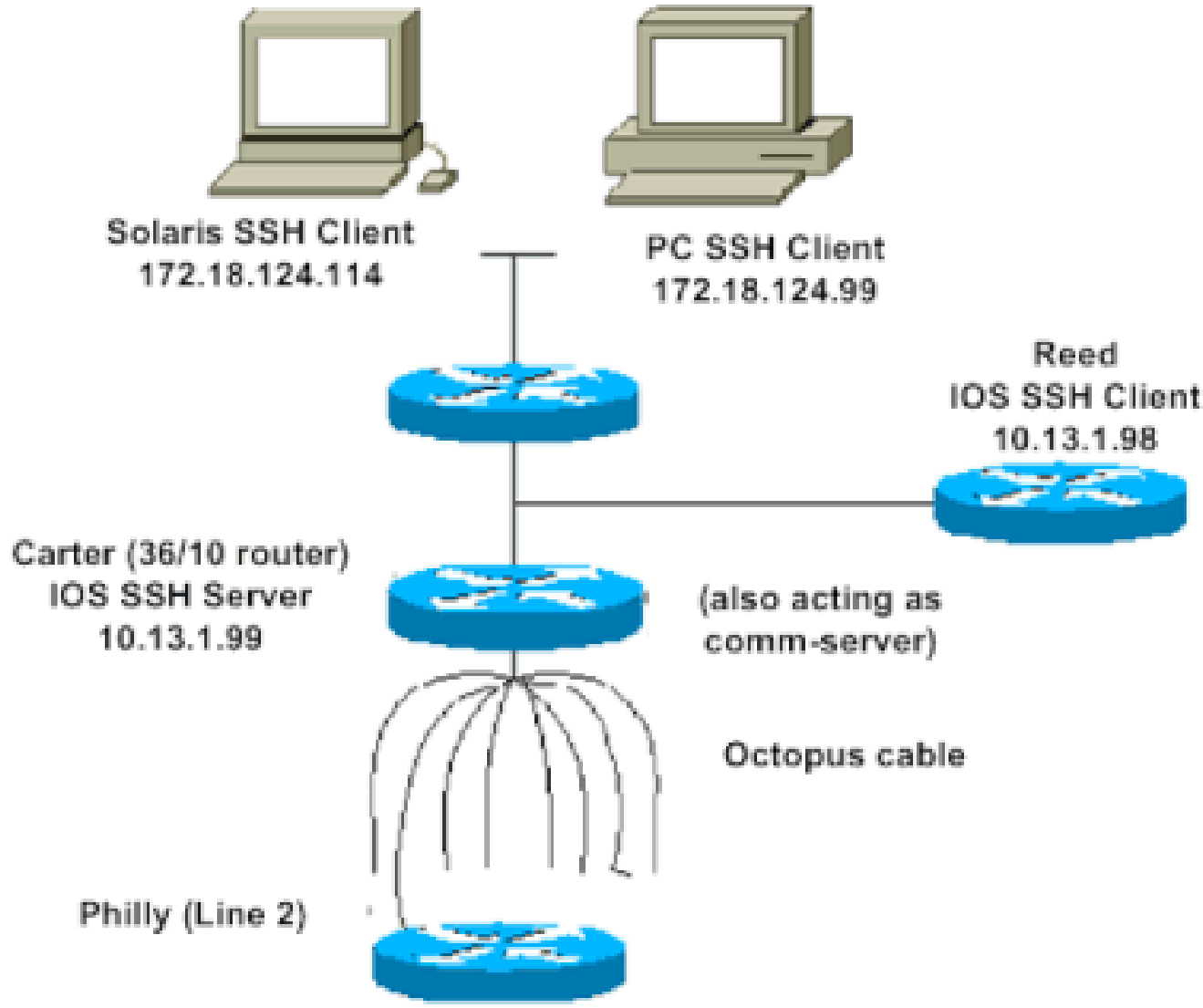
تستند المعلومات الواردة في هذا المستند إلى برنامج Cisco IOS 3600 (C3640-IK9S-M)، الإصدار 12.2(2)T1.

تم تقديم SSH في الصور والأنظمة الأساسية التالية من Cisco IOS:

- تم تقديم الوصول الآمن إلى خط SSH الطرفي (المعروف أيضا ب reverse-Telnet) في الصور والأنظمة الأساسية من Cisco IOS التي تبدأ في برنامج Cisco IOS الإصدار 12.2.2.T.
- تم تقديم SSH الإصدار 2.0 (SSH v2) في الصور والأنظمة الأساسية من Cisco IOS التي تبدأ في برنامج Cisco IOS الإصدار 12.1(19)E.

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.

الرسم التخطيطي لشبكة SSH الإصدار 2



اختبار المصادقة

اختبار المصادقة دون SSH

اختبر المصادقة دون SSH أولاً للتأكد من عمل المصادقة مع Carter للموجّه قبل إضافة SSH. يمكن أن تكون المصادقة باسم مستخدم وكلمة مرور محلي أو خادم المصادقة والتخويل والمحاسبة (AAA) الذي يشغّل TACACS+ أو RADIUS. (الذي يمكن أن تتم المصادقة من خلال كلمة مرور السطر مع SSH.) يوضح هذا المثال المصادقة المحلية، والتي تتيح لك إستخدام cisco وكلمة المرور cisco. اسم المستخدم cisco في الموجه Telnet

---

ملاحظة: خلال هذا المستند، يتم إستخدام vty للإشارة إلى نوع المحطة الطرفية الظاهرية.

```
!--- The aaa new-model command causes the local username and password on the router to be used in the al

aaa new-model
username cisco password 0 cisco
line vty 0 4
```

```
transport input telnet

!--- Instead of aaa new-model, you can use the login local command.
```

اختبار المصادقة مع SSH

لاختبار المصادقة مع SSH، يجب عليك الإضافة إلى العبارات السابقة لتمكين SSH على Carter، واختبار SSH من محطات PC و UNIX.

```
ip domain-name rtp.cisco.com

!--- Generate an SSH key to be used with SSH.

crypto key generate rsa
ip ssh time-out 60
ip ssh authentication-retries 2
```

عند هذه النقطة، يجب أن يعرض الأمر show crypto key mypubkey rsa المفاتيح الذي تم إنشاؤه. بعد إضافة تكوين SSH، اختبر قدرتك على الوصول إلى الموجّه من جهاز الكمبيوتر الشخصي ومحطة UNIX.

مجموعات التكوين الاختيارية

منع الاتصالات بخلاف SSH

إذا كنت ترغب في منع الاتصالات بخلاف SSH، قم بإضافة الأمر transport input ssh أسفل الأسطر لتحديد الموجّه إلى اتصالات SSH فقط. يتم رفض برامج Telnet (بخلاف SSH) المباشرة.

```
line vty 0 4

!--- Prevent non-SSH Telnets.

transport input ssh
```

قم بإجراء اختبار للتأكد من أنه لا يمكن لمستخدمي البرامج بخلاف SSH استخدام Telnet إلى الموجه Carter.

إعداد موجه Cisco IOS أو المحول كعميل SSH

هناك أربع خطوات مطلوبة لتمكين دعم SSH على موجّه Cisco IOS:

1. قم بتكوين الأمر hostname .

2. قم بتكوين مجال DNS.

3. أنشئ مفتاح SSH.

4. قم بتمكين دعم نقل SSH للوحدة الطرفية للنوع الافتراضي (vty).

إذا أردت أن يكون لديك جهاز واحد يعمل كعميل SSH إلى الآخر، فيمكنك إضافة SSH إلى جهاز العميل-الخادم، حيث يعمل Carter كخادم، ويضع ذلك هذه الأجهزة في ترتيب العميل-الخادم، حيث يعمل Carter كخادم، ويسمى Reed. تكوين عميل Cisco IOS SSH على Reed هو نفسه المطلوب لتكوين عميل Reed كخادم SSH على Carter.

```
!--- Step 1: Configure the hostname if you have not previously done so.

hostname carter

!--- The aaa new-model command causes the local username and password on the router to be used in the a

aaa new-model
username cisco password 0 cisco

!--- Step 2: Configure the DNS domain of the router.

ip domain-name rtp.cisco.com

!--- Step 3: Generate an SSH key to be used with SSH.

crypto key generate rsa
ip ssh time-out 60
ip ssh authentication-retries 2

!--- Step 4: By default the vty transport is Telnet. In this case, Telnet is disabled and only SSH is s

line vty 0 4
transport input ssh

!--- Instead of aaa new-model, you can use the login local command.
```

قم بإصدار هذا الأمر إلى SSH من عميل Cisco IOS SSH (Reed) إلى خادم Cisco IOS SSH (Carter) للاختبار هذا:

```
ssh -v 2 -c aes256-cbc -m hmac-sha1-160 -l cisco 10.31.1.99
```

إعداد موجه Cisco IOS كخادم SSH الذي يقوم بتنفيذ مصادقة المستخدم المستندة إلى RSA

أكمل هذه الخطوات لتكوين خادم SSH لتنفيذ المصادقة المستندة إلى RSA.

1. حدد اسم المضيف.

```
Router(config)#hostname
```

2. قم بتحديد اسم مجال افتراضي.

```
Router(config)#ip domain-name
```

3. قم بإنشاء أزواج مفاتيح RSA.

```
Router(config)#crypto key generate rsa
```

4. قم بتكوين مفاتيح SSH-RSA لمصادقة المستخدم والخادم.

```
Router(config)#ip ssh pubkey-chain
```

5. قم بتكوين اسم مستخدم SSH.

```
Router(conf-ssh-pubkey)#username
```

6. حدد مفتاح RSA العام للنظير البعيد.

```
Router(conf-ssh-pubkey-user)#key-string
```

7. حدد نوع مفتاح SSH وإصداره. (هذه الخطوة اختيارية.)

```
Router(conf-ssh-pubkey-data)#key-hash ssh-rsa
```

8. قم باالخروج من الوضع الحالي والرجوع إلى وضع EXEC في االمتيازات.

```
Router(conf-ssh-pubkey-data)#end
```

إضافة الوصول اآلمن إلى خط SSH الطرفي

إذا احتجت إلى مصادقة سطر خط SSH الطرفي الصادر، فيمكنك تكوين SSH واختباره لبرامج Telnet العكسية الصادرة من خالل Carter، والذي يعمل كخادم اتصاالت إلى فيالدلفيا.

```
ip ssh port 2001 rotary 1
line 1 16
   no exec
   rotary 1
   transport input ssh
   exec-timeout 0 0
   modem InOut
   stopbits 1
```

إذا كانت فيالدلفيا متصلة بالمنفذ 2 الخاص بـ Carter، فيمكنك تكوين SSH إلى فيالدلفيا من خالل Carter من Reed باستخدام هذا الأمر:

```
ssh -v 2 -c aes256-cbc -m hmac-shal-160 -p 2002 10.31.1.99
```

يمكنك استخدام هذا الأمر من Solaris:

```
ssh -c 3des -p 2002 -x -v 10.13.1.99
```

تقييد وصول SSH إلى شبكة فرعية

ستحتاج إلى تقييد اتصال SSH بشبكة فرعية معينة حيث يتم إسقاط جميع محاوالت SSH الأخرى من برتوكوالت IP خارج الشبكة الفرعية.

يمكنك استخدام هذه الخطوات للقيام باألمر نفسه:

1. تحديد قائمة وصول تسمح بحركة المرور من هذه الشبكة الفرعية المعينة.
2. تقييد الوصول إلى واجهة سطر VTY باستخدام قائمة الوصول.

هذا مثال على التكوين. في هذا المثال، مسموح بوصول SSH فقط إلى الشبكة الفرعية

10.10.10.0 255.255.255.0، ويتم رفض أي وصول آخر.

```
Router(config)#access-list 23 permit 10.10.10.0 0.0.0.255
Router(config)#line vty 5 15
Router(config-line)#transport input ssh
Router(config-line)#access-class 23 in
Router(config-line)#exit
```

ملاحظة: ويتم استخدام الإجراء نفسه أيضًا لتأمين وصول SSH على الأنظمة الأساسية للمبدّل.

تكوين SSH، الإصدار 2

```
carter(config)#ip ssh version 2
```

الاختلافات على إخراج أمر الشعار

يختلف إخراج أمر banner بين Telnet والإصدارات المختلفة من اتصالات SSH. يوضح هذا الجدول مدى اختلاف عمل خيارات أمر banner مع أنواع مختلفة من الاتصالات.

خيار أمر الشعار	Telnet	SSH v2
سجل الشعار	عرض قبل تسجيل الدخول إلى الجهاز.	عرض قبل تسجيل الدخول إلى الجهاز.
banner motd	عرض قبل تسجيل الدخول إلى الجهاز.	عرض بعد تسجيل الدخول إلى جهاز.
banner exec	عرض بعد تسجيل الدخول إلى جهاز.	عرض بعد تسجيل الدخول إلى جهاز.

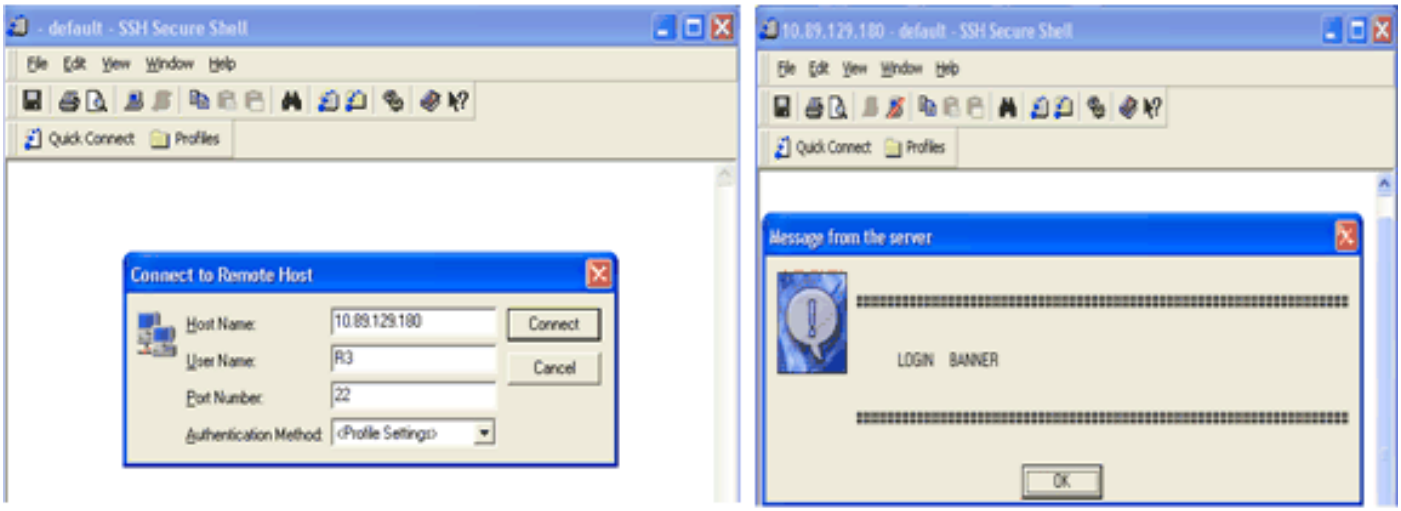
ملاحظة: لم يعد الإصدار 1 من SSH مُوصى به.

يتعذر عرض شعار تسجيل الدخول

يدعم SSH الإصدار 2 شعار تسجيل الدخول. عندما يبدأ جلسة SSH مع موجه Cisco، يتم عرض شعار تسجيل الدخول إذا أرسل عميل SSH اسم المستخدم. على سبيل المثال، عند إستخدام

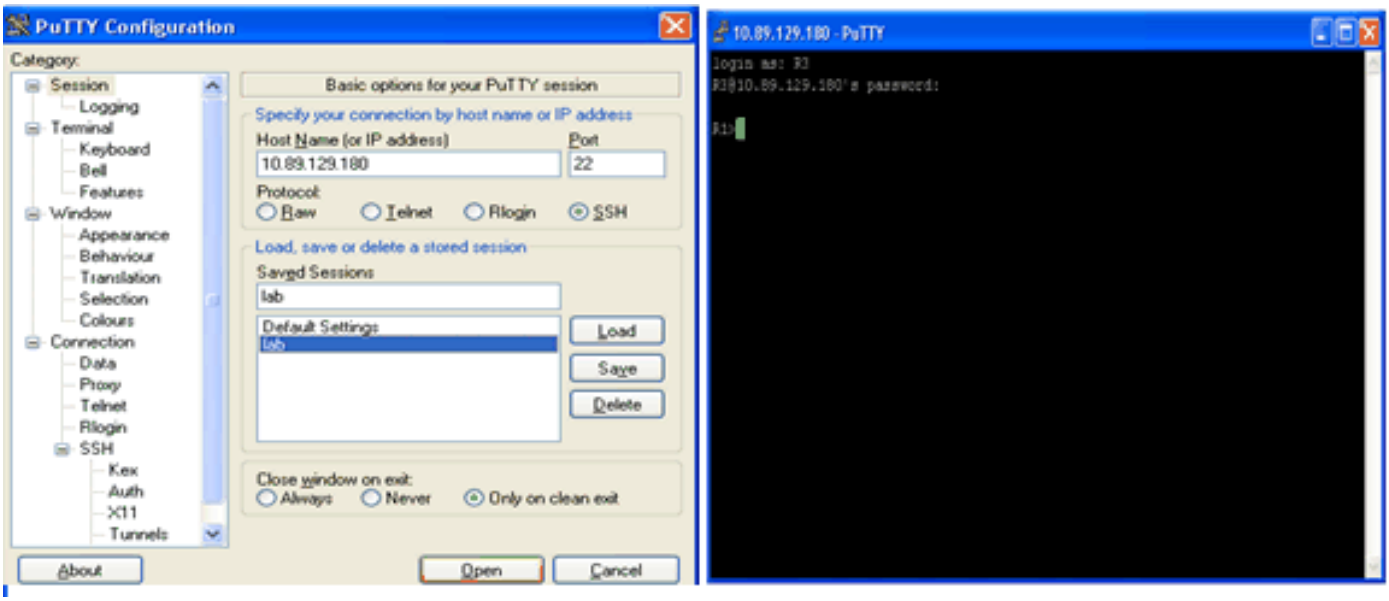
عميل Secure Shell ssh، يتم عرض شعار تسجيل الدخول. عند إستخدام عميل PuTTY ssh، ال يتم عرض شعار تسجيل الدخول. وذلك لأن SSH يرسل اسم المستخدم بشكل افتراضي و يقوم PuTTY بإرسال اسم المستخدم بشكل افتراضي.

يحتاج عميل SSH اسم المستخدم لبدء الاتصال بالجهاز الذي يدعم SSH. ال يتم تمكين زر الاتصال إذا لم تقم بإدخال اسم المضيف واسم المستخدم. يوضح التقاط الشاشة هذا أن يتم عرض شعار تسجيل الدخول عند اتصال SSH بالموجه. يُطالب الشعار بكلمة مرور.



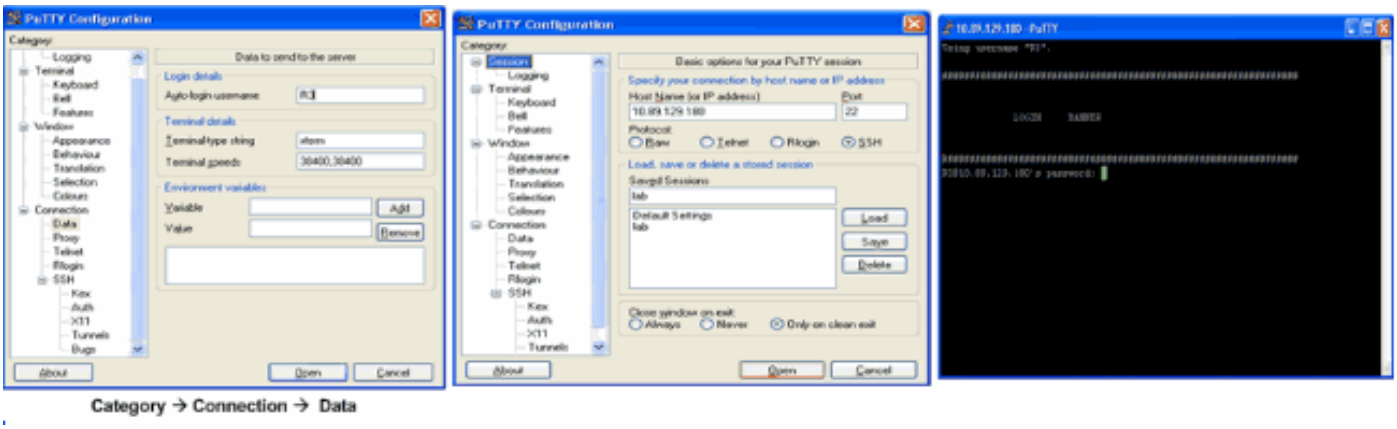
يطالب الشعار بكلمة مرور

ال يتطلب عميل PuTTY اسم المستخدم لبدء اتصال SSH بالموجّه. توضح صورة الشاشة هذه أن عميل PuTTY يتصل بالموجه ويطلب اسم المستخدم وكلمة المرور. والي يعرض شعار تسجيل الدخول.



اتصال SSH بالموجّه

يوضح التقاط الشاشة هذا أن شعار تسجيل الدخول يتم عرضه عند تكوين PuTTY لإرسال اسم المستخدم إلى الموجه.



إرسال اسم المستخدم إلى الموجّه

أوامر show وdebug

قبل إصدار أوامر debug الموضحة هنا، راجع المعلومات المهمة في أوامر تصحيح الأخطاء. يتم دعم بعض أوامر show بواسطة أداة متتبع الإخراج (المسجلة للعملاء فقط)، والتي تتيح لك عرض تحليل إخراج أمر show.

- debug ip ssh يعرض رسائل تصحيح الأخطاء لـ SSH.
- show ssh يعرض حالة اتصالات خادم SSH.

```
carter#show ssh
  Connection     Version Encryption     State               Username
   0             2.0     DES            Session started     cisco
```

- show ip ssh يعرض الإصدار وبيانات التكوين لـ SSH.

```
carter#show ip ssh
  SSH Enabled - version 2.0
  Authentication timeout: 120 secs; Authentication retries: 3
```

إخراج تصحيح الأخطاء للعينة

تصحيح أخطاء الموجّه

```
00:23:20: SSH0: starting SSH control process
00:23:20: SSH0: sent protocol version id SSH-2.0-Cisco-1.25
00:23:20: SSH0: protocol version id is - SSH-2.0-1.2.26
00:23:20: SSH0: SSH_SMSG_PUBLIC_KEY msg
00:23:21: SSH0: SSH_CMSG_SESSION_KEY msg - length 112, type 0x03
00:23:21: SSH: RSA decrypt started
```

```
00:23:21: SSH: RSA decrypt finished
00:23:21: SSH: RSA decrypt started
00:23:21: SSH: RSA decrypt finished
00:23:21: SSH0: sending encryption confirmation
00:23:21: SSH0: keys exchanged and encryption on
00:23:21: SSH0: SSH_CMSG_USER message received
00:23:21: SSH0: authentication request for userid cisco
00:23:21: SSH0: SSH_SMSG_FAILURE message sent
00:23:23: SSH0: SSH_CMSG_AUTH_PASSWORD message received
00:23:23: SSH0: authentication successful for cisco
00:23:23: SSH0: requesting TTY
00:23:23: SSH0: setting TTY - requested: length 24, width 80; set:
   length 24, width 80
00:23:23: SSH0: invalid request - 0x22
00:23:23: SSH0: SSH_CMSG_EXEC_SHELL message received
00:23:23: SSH0: starting shell for vty
```

تصحيح أخطاء الخادم

ملاحظة: هذه هو إخراج جهاز Solaris.

```
rtp-evergreen.rtp.cisco.com#ssh -c 3des -l cisco -v 10.31.1.99
rtp-evergreen#/opt/CISssh/bin/ssh -c 3des -l cisco -v 10.13.1.99
SSH Version 1.2.26 [sparc-sun-solaris2.5.1], protocol version 1.5.
Compiled with RSAREF.
rtp-evergreen: Reading configuration data /opt/CISssh/etc/ssh_config
rtp-evergreen: ssh_connect: getuid 0 geteuid 0 anon 0
rtp-evergreen: Allocated local port 1023.
rtp-evergreen: Connecting to 10.13.1.99 port 22.
rtp-evergreen: Connection established.
rtp-evergreen: Remote protocol version 2.0,
   remote software version Cisco-1.25
rtp-evergreen: Waiting for server public key.
rtp-evergreen: Received server public key (768 bits)
   and host key (512 bits).
rtp-evergreen: Host '10.13.1.99' is known and matches the host key.
rtp-evergreen: Initializing random; seed file //.ssh/random_seed
rtp-evergreen: Encryption type: 3des
rtp-evergreen: Sent encrypted session key.
rtp-evergreen: Installing crc compensation attack detector.
rtp-evergreen: Received encrypted confirmation.
rtp-evergreen: Doing password authentication.
cisco@10.13.1.99's password:
rtp-evergreen: Requesting pty.
rtp-evergreen: Failed to get local xauth data.
rtp-evergreen: Requesting X11 forwarding with authentication spoofing.
Warning: Remote host denied X11 forwarding, perhaps xauth program
   could not be run on the server side.
rtp-evergreen: Requesting shell.
rtp-evergreen: Entering interactive session.
```

التكوين غير الصحيح

تحتوي هذه الأقسام على إخراج تصحيح الأخطاء للعينة من العديد من التكوينات غير الصحيحة.

لم يتم تحويل SSH من عميل SSH باستخدام معيار تشفير البيانات (DES)

كلمة المرور غير صحيحة

تصحيح أخطاء المودّم

```
00:26:51: SSH0: starting SSH control process
00:26:51: SSH0: sent protocol version id SSH-2.0-Cisco-1.25
00:26:52: SSH0: protocol version id is - SSH-2.0-1.2.26
00:26:52: SSH0: SSH_SMSG_PUBLIC_KEY msg
00:26:52: SSH0: SSH_CMSG_SESSION_KEY msg - length 112, type 0x03
00:26:52: SSH: RSA decrypt started
00:26:52: SSH: RSA decrypt finished
00:26:52: SSH: RSA decrypt started
00:26:52: SSH: RSA decrypt finished
00:26:52: SSH0: sending encryption confirmation
00:26:52: SSH0: keys exchanged and encryption on
00:26:52: SSH0: SSH_CMSG_USER message received
00:26:52: SSH0: authentication request for userid cisco
00:26:52: SSH0: SSH_SMSG_FAILURE message sent
00:26:54: SSH0: SSH_CMSG_AUTH_PASSWORD message received
00:26:54: SSH0: password authentication failed for cisco
00:26:54: SSH0: SSH_SMSG_FAILURE message sent
00:26:54: SSH0: authentication failed for cisco (code=7)
00:26:54: SSH0: Session disconnected - error 0x07
```

يرسل عميل SSH شفرة (Blowfish) غير مدعومة

تصحيح أخطاء المودّم

```
00:39:26: SSH0: starting SSH control process
00:39:26: SSH0: sent protocol version id SSH-2.0-Cisco-1.25
00:39:26: SSH0: protocol version id is - SSH-2.0-W1.0
00:39:26: SSH0: SSH_SMSG_PUBLIC_KEY msg
00:39:26: SSH0: SSH_CMSG_SESSION_KEY msg - length 112, type 0x03
00:39:26: SSH0: Session disconnected - error 0x20
```

الحصول على "%SSH-3-PRIVATEKEY: تعذّر استرداد مفتاح RSA الخاص لـ" الخطأ

يمكن أن يؤدي التغيير في اسم المجال أو اسم المضيف إلى تشغيل رسالة الخطأ هذه. استخدم هذه الحلول البديلة:

- امل أ مفاتيح RSA باألصافر أو دِعأ إنشاء المفاتيح.

```
crypto key zeroize rsa label key_name
crypto key generate rsa label key_name modulus key_size
```

- إذا لم ينجح الحل السابق، فجرّب الخطوات التالية:
  1. امل أ جميع مفاتيح RSA باألصافر.
  2. أعِد تحميل الجهاز.
  3. قم بإنشاء مفاتيح جديدة مسماة لـ SSH.

النصائح

- إذا تم رفض أوامر تكوين SSH الخاصة بك كأوامر غير قانونية، فأنت لم تقم بإنشاء مفاتيح RSA بنجاح للموجّه الخاص بك. تأكد من تحديد اسم مضيف ومجال. ثم قم بتمكين خادم SSH واستخدم الأمر crypto key generate rsa لإنشاء أزواج من مفاتيح RSA.
- عند تكوين أزواج من مفاتيح RSA، يمكن الحصول على رسائل الخطأ هذه:
  1. "لم يتم تحديد اسم المضيف".

     يجب أن تستخدم أمر التكوين العام hostname لتكوين اسم مضيف للموجّه.
  2. "لم يتم تحديد مجال".

     يجب أن تستخدم أمر التكوين العام ip domain-name لتكوين مجال مضيف للموجّه.
- يقتصر عدد إتصالات SSH المسموح بها على الحد الأقصى لعدد الاتصالات التي vty تم تكوينها للموجه. يستخدم كل اتصال SSH vty موارد.
- يستخدم SSH إما أمان محلي أو بروتوكول الأمان الذي تم تكوينه من خلال AAA على الموجّه لمصادقة المستخدم. عند تكوين AAA، يجب التأكد من عدم تشغيل وحدة التحكم لـ AAA. قم بتطبيق كلمة أساسية في وضع التكوين العام لتعطيل AAA على وحدة التحكم.
- No SSH server connections running:

```
carter#show ssh

%No SSHv2 server connections running.
```

يقترح هذا الإخراج أن خادم SSH معطّل أو لم يتم تمكينه بشكل صحيح. إذا قمت بتكوين SSH

بالفعل، فيُوصى بإعادة تكوين خادم SSH في الجهاز. أكمل هذه الخطوات لإعادة تكوين خادم SSH على الجهاز.

1. احذف أزواج مفاتيح RSA. بعد حذف أزواج مفاتيح RSA، يتم تعطيل خادم SSH تلقائيًا.

```
carter(config)#crypto key zeroize rsa
```

ملاحظة: من المهم إنشاء أزواج مفاتيح بـ 768 على الأقل كحجم وحدات البت عند تمكين SSH v2.

تحذير: لا يمكن التراجع عن هذا الأمر بعد حفظ التكوين الخاص بك. وأيضًا، بعد حذف مفاتيح RSA، لا يمكنك استخدام الشهادات أو CA أو المشاركة في عمليات تبادل الشهادات باستخدام نظائر أمان IP (IPSec) الأخرى إلا إذا قمت بإعادة إنشاء مفاتيح RSA لإعادة تكوين إمكانية التشغيل البيني لـ CA، والحصول على شهادة CA، وطلب شهادتك الخاصة مجددًا.

2. أعِد تكوين اسم المضيف واسم المجال للجهاز.

```
carter(config)#hostname hostname

carter(config)#ip domain-name domainname
```

3. قم بإنشاء أزواج مفاتيح RSA للموجه الخاص بك. يؤدي هذا إلى تمكين SSH تلقائيًا.

```
carter(config)#crypto key generate rsa
```

ملاحظة: راجع [crypto key generate rsa - مرجع أمر أمان Cisco IOS، الإصدار 12.3 للحصول على مزيد من المعلومات حول استخدام هذا الأمر.]

ملاحظة: يمكنك تلقي SSH2 0: رسالة الخطأ تم إستلام نوع رسالة غير متوقع" بسبب وجود حزمة مستلمة لا يمكن فهمها بواسطة الموجه. قم بزيادة طول المفاتيح أثناء قيامك بإنشاء مفاتيح rsa لبروتوكول ssh لحل هذه المشكلة.

4. قم بتكوين خادم SSH.

5. لتمكين أحد مبدّلات/موجّهات Cisco وتكوين لخادم SSH، يجب عليك تكوين معلمات SSH. إذا لم تقم بتكوين معلمات SSH، سيتم استخدام القيم الافتراضية.

ip ssh {[timeout seconds] | [authentication-retries integer]}

```
carter(config)# ip ssh
```

معلومات ذات صلة

- صفحة دعم منتج SSH

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).