كيفية تكوين SSH على محولات Catalyst التي تقوم بتشغيل CatOS

المحتويات

المقدمة

يقدم هذا المستند إرشادات خطوة بخطوة لتكوين الإصدار 1 من بروتوكول طبقة الأمان (SSH) على محولات Catalyst التي تعمل بنظام التشغيل Catalyst OS (CatOS). الإصدار الذي تم إختباره هو 6-1-1. cat6000-**supk9**.1c.bin.

المتطلبات الأساسية

المتطلبات

يوضح هذا الجدول حالة دعم SSH في المحولات. يمكن للمستخدمين المسجلين الوصول إلى صور البرامج هذه من خلال زيارة مركز البرامج.

CatOS SSH	
في المثال التالي	دعم SSH

Cat 4000/4500/2948G/2980G ((CatOS	صور K9 اعتبارا من 6.1
(Cat 5000/5500 (CatOS	صور K9 اعتبارا من 6.1
(Cat 6000/6500 (CatOS	صور K9 اعتبارا من 6.1
IOS SSH	
في المثال التالي	**دعم SSH**
الفئة Cat 2950*	12.1(12c)EA1 والإصدارات الأحدث
Cat 3550*	12.1(11)EA1 والإصدارات الأحدث
CAT 4000/4500 (برنامج Cisco IOS المتكامل)*	12.1(13)ew وفيما بعد **
CAT 6000/5500 (برنامج Cisco IOS المتكامل)*	الإصدار 12.1(11b)E والإصدارات الأحدث
Cat 8540/8510	12.1(12c)EY وفيما بعد، الإصدار 12.1(14)E1 والإصدارات الأحدث
لا يوجد SSH	
في المثال التالي	**دعم SSH**
كات 1900	لا
كات 2800	لا
cat 2948g-l3	لا
Cat 2900XL	لا
Cat 3500XL	لا
Cat 4840G-L3	لا
Cat 4908G-L3	لا

* تتم تغطية التكوين في تكوين "طبقة الأمان" على الموجهات والمحولات التي تشغل نظام Cisco IOS.

** لا يوجد دعم ل SSH في قطار 12.1E لمادة حفازة 4000 التي تشغل برنامج Cisco IOS المتكامل.

ارجع إلى نموذج تفويض توزيع تصدير برنامج التشفير لتطبيق 3DES.

يفترض هذا المستند أن المصادقة تعمل قبل تنفيذ بروتوكول SSH (من خلال كلمة مرور برنامج Telnet أو TACACS+) أو RADIUS. لا يتم دعم SSH مع Kerberos قبل تنفيذ SSH.

المكونات المستخدمة

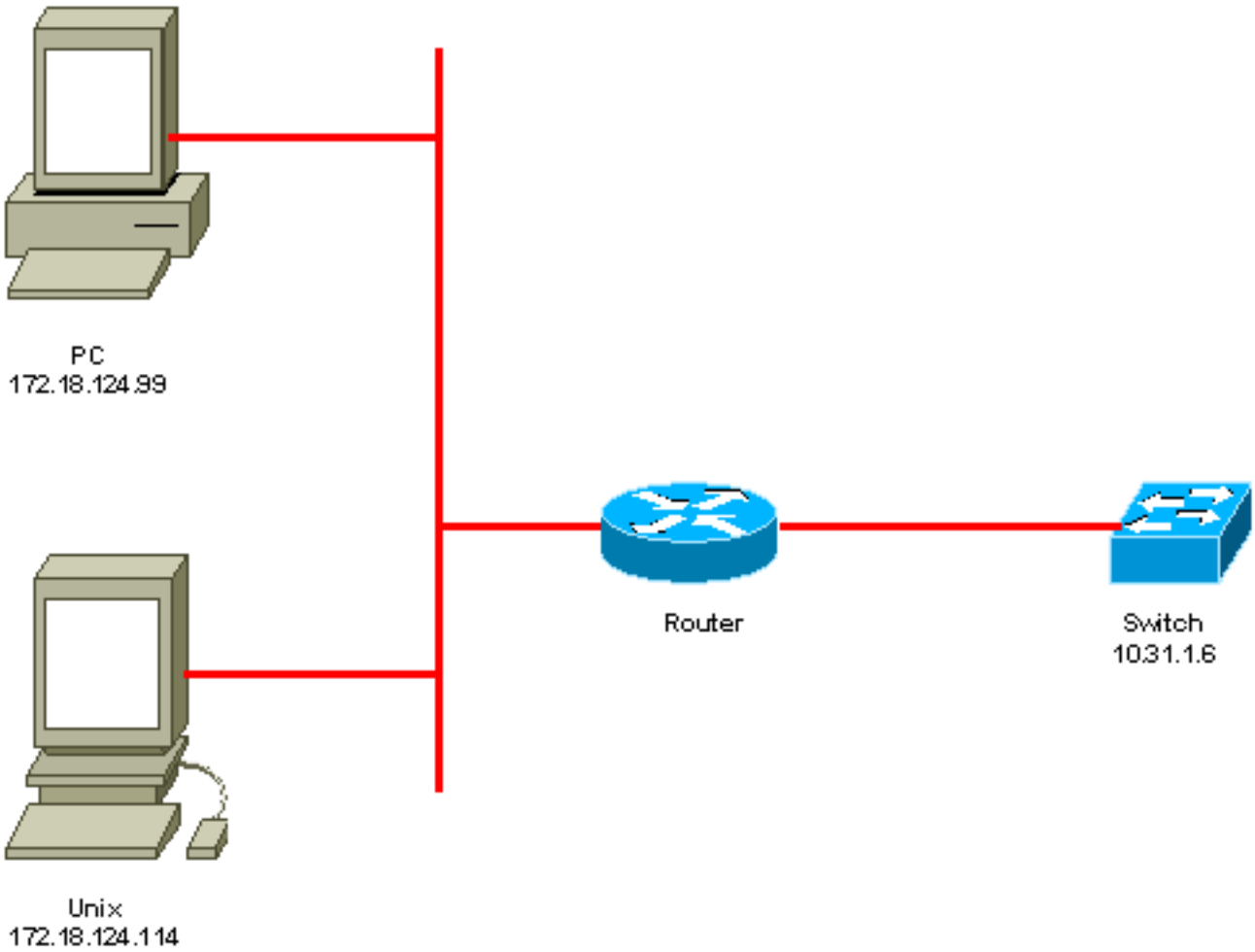
يخاطب هذا وثيقة فقط المادة حفازة 2948g، مادة حفازة 2980g، مادة حفازة 4500/4000 sery، مادة حفازة 5500/5000 sery، ومادة حفازة 6500/6000 sery يركض ال CatOS k9 صورة. لمزيد من التفاصيل، ارجع إلى قسم المتطلبات في هذا المستند.

تم إنشاء المعلومات المُقدمة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كنت تعمل في شبكة مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر قبل استخدامه.

الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، راجع اصطلاحات تلميحات Cisco التقنية.

الرسم التخطيطي للشبكة



تكوين المبدّل

```
Generate and verify RSA key. sec-cat6000> (enable) set crypto key rsa 1024 ---!
                                                    [Generating RSA keys..... [OK
          sec-cat6000> (enable) ssh_key_process: host/server key size: 1024/768
              Display the RSA key. sec-cat6000> (enable) show crypto key ---!
 RSA keys were generated at: Mon Jul 23 2001, 15:03:30 1024 65537 1514414695360
 57733285367170478570985060663476874686971696394035244062067857533870155088852 5
 69969147833053784006695698761020781095949864817996533001801084478586347277306 7
 69718525641838624300188100883056124113738169282007867437605827557313344852933 2
                  19966820193013294709782680590633782154793854054981930616 51
Restrict which host/subnets are allowed to use SSH to the switch. !--- Note: If you do not ---!
   do this, the switch will display the message !--- "WARNING!! IP permit list has no entries!"
                                  sec-cat6000> set ip permit 172.18.124.0 255.255.255.0
                .with mask 255.255.255.0 added to IP permit list 172.18.124.0
                Turn on SSH. sec-cat6000> (enable) set ip permit enable ssh ---!
                                                                .SSH permit list enabled
              Verity SSH permit list. sec-cat6000> (enable) show ip permit ---!
                                                               .Telnet permit list disabled
                                                                .Ssh permit list enabled
```

```
.Snmp permit list disabled
Permit List Mask Access-Type
------------ --------------- ---------------
telnet ssh snmp 255.255.255.0 172.18.124.0

Denied IP Address Last Accessed Time Type
------ ----------------- ----------------
```

تعطيل SSH

في بعض الحالات، قد يكون من الضروري تعطيل SSH على المحول. يجب عليك التحقق من تكوين SSH على المحول وإذا كان الأمر كذلك، فعليك تعطيله.

للتحقق من تكوين SSH على المحول، قم بإصدار الأمر **show crypto key**. إذا عرض الإخراج مفتاح RSA، فسيتم تكوين SSH وتمكينه على المحول. وهناك مثال على ذلك.

```
sec-cat6000> (enable) show crypto key
RSA keys were generated at: Mon Jul 23 2001, 15:03:30 1024 65537 1514414695360
577332853671704785709850606634768746869716963940352440620678575338701550888525
699691478330537840066956987610207810959498648179965330018010844785863472773067
697185256418386243001881008830561241137381692820078674376058275573133448529332
199668201930132947097826805906337821547938540549819306165 1
```

لإزالة مفتاح التشفير، قم بإصدار الأمر **clear crypto key rsa** لتعطيل SSH على المحول. وهناك مثال على ذلك.

```
sec-cat6000> (enable) clear crypto key rsa
Do you really want to clear RSA keys (y/n) [n]? y
.RSA keys has been cleared
(sec-cat6000> (enable
```

تصحيح الأخطاء في المادة حفازة

لتشغيل تصحيح الأخطاء، قم بإصدار الأمر **set trace ssh 4**.

لإيقاف تشغيل تصحيح الأخطاء، قم بإصدار الأمر **set trace ssh 0**.

أمثلة أوامر debug للاتصال الجيد

Solaris إلى Catalyst، المعيار الثلاثي لتشفير البيانات (3DES)، كلمة مرور Telnet

سولاريس

```
rtp-evergreen# ssh -c 3des -v 10.31.1.6
.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 10.31.1.6 port 22
.rtp-evergreen: Connection established
rtp-evergreen: Remote protocol version 1.5, remote software version 1.2.26
.rtp-evergreen: Waiting for server public key
.(rtp-evergreen: Received server public key (768 bits) and host key (1024 bits
.Host key not found from the list of known hosts
```

```
Are you sure you want to continue connecting (yes/no)? yes
.Host '10.31.1.6' added to the list of known hosts
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
:root@10.31.1.6'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

Cisco Systems Console

<sec-cat6000
```

مادة حفازة

```
sec-cat6000> (enable) debug: _proc->tty = 0x8298a494, socket_index = 3
debug: version: SSH-1.5-1.2.26

debug: Client protocol version 1.5; client software version 1.2.26
.debug: Sent 768 bit public key and 1024 bit host key
debug: Encryption type: 3des
.debug: Received session key; encryption turned on
debug: ssh login by user: root
debug: Trying Local Login
.Password authentication for root accepted
debug: ssh received packet type: 10
debug: ssh received packet type: 34
Unknown packet type received after authentication: 34
debug: ssh received packet type: 12
debug: ssh88: starting exec shell
.debug: Entering interactive session
```

كلمة مرور PC إلى Catalyst و 3DES و Telnet

مادة حفازة

```
debug: Client protocol version 1.5; client software version W1.0
.debug: Sent 768 bit public key and 1024 bit host key
debug: Encryption type: des
.debug: Received session key; encryption turned on
:debug: ssh login by user
debug: Trying Local Login
.Password authentication for accepted
debug: ssh received packet type: 10
debug: ssh received packet type: 37
Unknown packet type received after authentication: 37
debug: ssh received packet type: 12
debug: ssh89: starting exec shell
.debug: Entering interactive session
```

Solaris إلى مصادقة Catalyst و 3DES والمصادقة والتفويض والمحاسبة (AAA)

سولاريس

```
:Solaris with aaa on
rtp-evergreen# ssh -c 3des -l abcde123 -v 10.31.1.6
.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 10.31.1.6 port 22
.rtp-evergreen: Connection established
rtp-evergreen: Remote protocol version 1.5, remote software version 1.2.26
.rtp-evergreen: Waiting for server public key
.(rtp-evergreen: Received server public key (768 bits) and host key (1024 bits
.rtp-evergreen: Host '10.31.1.6' 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
:abcde123@10.31.1.6'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

Cisco Systems Console

<sec-cat6000
```

مادة حفازة

```
sec-cat6000> (enable) debug: _proc->tty = 0x82a07714, socket_index = 3
debug: version: SSH-1.5-1.2.26

debug: Client protocol version 1.5; client software version 1.2.26
.debug: Sent 768 bit public key and 1024 bit host key
debug: Encryption type: 3des
.debug: Received session key; encryption turned on
debug: ssh login by user: abcde123
debug: Trying TACACS+ Login
.Password authentication for abcde123 accepted
debug: ssh received packet type: 10
debug: ssh received packet type: 34
Unknown packet type received after authentication: 34
debug: ssh received packet type: 12
debug: ssh88: starting exec shell
.debug: Entering interactive session
```

أمثلة أوامر debug لما يمكن أن يحدث بشكل خاطئ

تصحيح أخطاء Catalyst مع محاولة العميل [غير مدعوم] تشفير Blowfish

```
debug: Client protocol version 1.5; client software version W1.0
```

```
.debug: Sent 768 bit public key and 1024 bit host key
debug: Encryption type: blowfish
cipher_set_key: unknown cipher: 6
debug: Calling cleanup
```

تصحيح أخطاء Catalyst باستخدام كلمة مرور برنامج Telnet غير صحيحة

```
debug: _proc->tty = 0x82897414, socket_index = 4
debug: version: SSH-1.5-1.2.26
debug: Client protocol version 1.5; client software version W1.0
.debug: Sent 768 bit public key and 1024 bit host key
debug: Encryption type: 3des
.debug: Received session key; encryption turned on
:debug: ssh login by user
debug: Trying Local Login
.debug: Password authentication for failed
```

تصحيح أخطاء Catalyst باستخدام مصادقة AAA غير صحيحة

```
cat6000> (enable) debug: _proc->tty = 0x829abd94, socket_index = 3
debug: version: SSH-1.5-1.2.26

debug: Client protocol version 1.5; client software version 1.2.26
.debug: Sent 768 bit public key and 1024 bit host key
debug: Encryption type: 3des
.debug: Received session key; encryption turned on
debug: ssh login by user: junkuser
debug: Trying TACACS+ Login
.debug: Password authentication for junkuser failed
.SSH connection closed by remote host
debug: Calling cleanup
```

استكشاف الأخطاء وإصلاحها

يتعامل هذا القسم مع سيناريوهات أستكشاف الأخطاء وإصلاحها المختلفة المتعلقة بتكوين SSH على محولات Cisco.

لا يمكن الاتصال بالمحول من خلال SSH

المشكلة:

لا يمكن الاتصال بالمحول باستخدام SSH.

يعرض الأمر **debug ip ssh** هذا الإخراج:

```
Jun 15 20:29:26.207: SSH2 1: RSA_sign: private key not found
Jun 15 20:29:26.207: SSH2 1: signature creation failed, status -1
```

الحل:

يقع هذا مشكلة بسبب أحد من هذا سبب:

- تفشل إتصالات SSH الجديدة بعد تغيير اسم المضيف.
- تم تكوين SSH باستخدام مفاتيح غير مسماة (تتضمن FQDN للموجه).

الحلول البديلة لهذه المشكلة هي:

- إذا تم تغيير اسم المضيف ولم يعد SSH يعمل، فعليك بالأصفار إنشاء مفتاح جديد آخر باستخدام التسمية المناسبة.

```
crypto key zeroize rsa
[crypto key generate rsa general-keys label (label) mod (modulus) [exportable
```

- لا تستخدم مفاتيح RSA مجهولة (المسماة بعد FQDN الخاصة بالمحول). أستخدم بدلا من ذلك المفاتيح المسماة.

```
[crypto key generate rsa general-keys label (label) mod (modulus) [exportable
```

لحل هذه المشكلة إلى الأبد، قم بترقية برنامج IOS إلى أي من الإصدارات التي تم فيها إصلاح هذه المشكلة.

تم تسجيل خطأ حول هذه المسألة. أحلت ل كثير معلومة، cisco بق CSCtc4114 id (يسجل زبون فقط) .

معلومات ذات صلة

- صفحة دعم SSH
- تكوين بروتوكول Secure Shell على الموجهات والمحولات التي تعمل بنظام التشغيل Cisco IOS
- مجموعة أدوات الأخطاء
- الدعم الفني - Cisco Systems

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).