Configurazione del protocollo SSH sugli switch Catalyst con CatOS

Sommario

Introduzione

In questo documento vengono fornite istruzioni dettagliate per configurare Secure Shell (SSH) versione 1 sugli switch Catalyst con Catalyst OS (CatOS). La versione testata è cat6000-**supk9**.6-1-1c.bin.

Prerequisiti

Requisiti

Nella tabella viene mostrato lo stato del supporto SSH sugli switch. Gli utenti registrati possono accedere a queste immagini software visitando il Software Center.

CatOS SSH	
Sul dispositivo	**Supporto SSH**

bootflash o slot0:	
Cat 4000/4500/2948G/2980G (CatOS)	Immagini K9 della versione 6.1
Cat 5000/5500 (CatOS)	Immagini K9 della versione 6.1
Cat 6000/6500 (CatOS)	Immagini K9 della versione 6.1
IOS SSH	
Sul dispositivo bootflash o slot0:	**Supporto SSH**
Cat 2950*	12.1(12c)EA1 e versioni successive
Cat 3550*	12.1(11)EA1 e versioni successive
Cat 4000/4500 (software Cisco IOS integrato)*	12.1(13)EW e successive **
Cat 6000/5500 (software Cisco IOS integrato)*	12.1(11b)E e successive
Cat 8540/8510	12.1(12c)EY e versioni successive, 12.1(14)E1 e versioni successive
No SSH	
Sul dispositivo bootflash o slot0:	**Supporto SSH**
Cat 1900	no
Cat 2800	no
Cat 2948G-L3	no
Cat 2900XL	no
Cat 3500XL	no
Cat 4840G-L3	no
Cat 4908G-L3	no

* La configurazione è illustrata in Configurazione di Secure Shell sui router e gli switch con Cisco IOS.

** Il supporto SSH nella versione 12.1E non è disponibile per gli switch Catalyst 4000 con software Cisco IOS integrato.

Per la richiesta di 3DES, consultare il modulo di autorizzazione della distribuzione dell'esportazione del software di crittografia.

in questo documento si presume che l'autenticazione venga eseguita prima dell'implementazione di SSH (tramite la password Telnet, TACACS+) o RADIUS. Il protocollo SSH con Kerberos non è supportato prima dell'implementazione del protocollo SSH.

Componenti usati

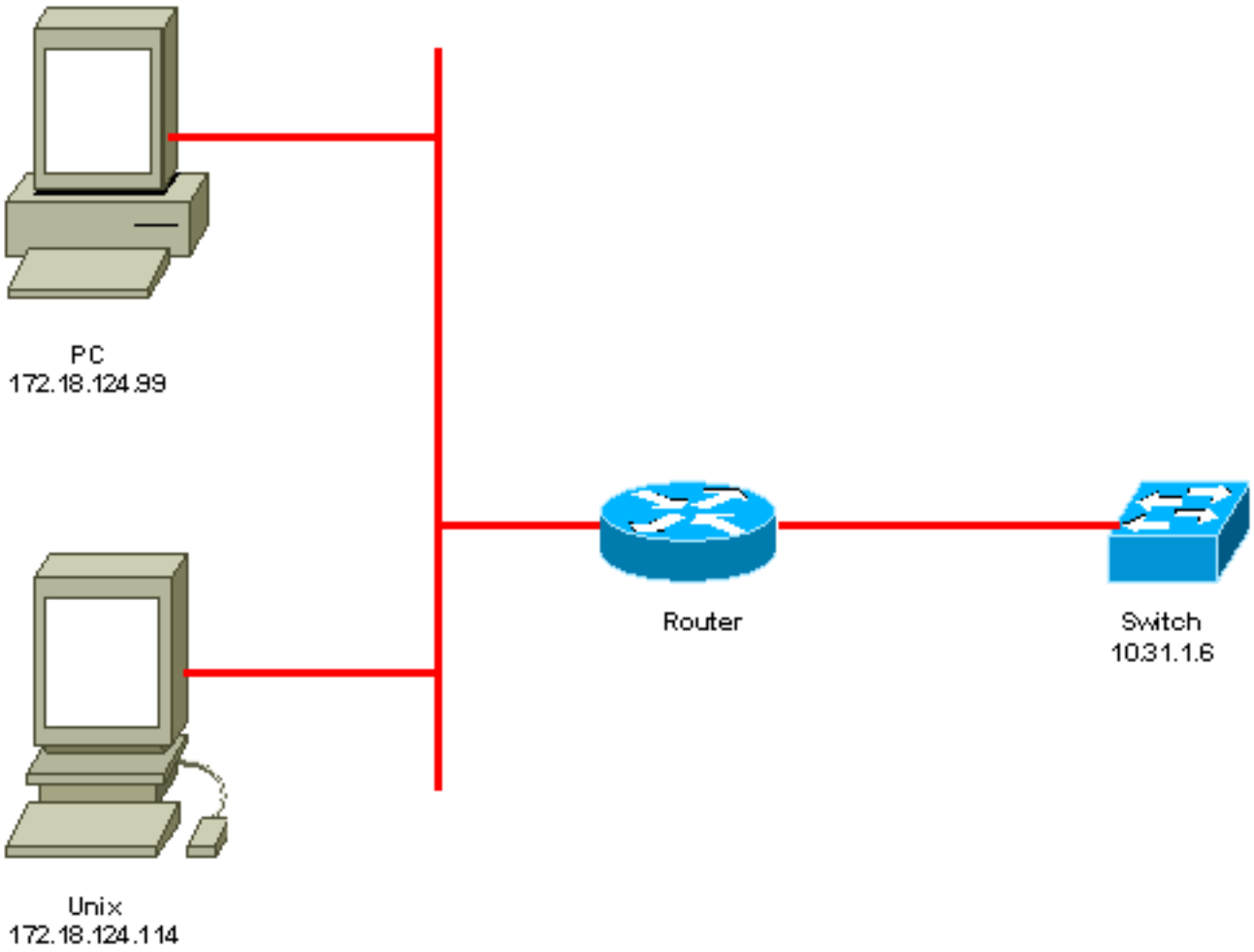
Questo documento riguarda solo Catalyst serie 2948G, Catalyst 2980G, Catalyst serie 4000/4500, Catalyst serie 5000/5500 e Catalyst serie 6000/6500 con immagine CatOS K9. Per ulteriori informazioni, fare riferimento alla sezione Requisiti di questo documento.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Esempio di rete



Configurazione degli switch

```
!--- 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
577332853671704785709850606634768746869716963940352440620678575338701550888525
699691478330537840066956987610207810959498648179965330018010844785863472773067
697185256418386243001881008830561241137381692820078674376058275573133448529332
199668201930132947097826805906337821547938540549819306165 1
!--- 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
172.18.124.0 with mask 255.255.255.0 added to IP permit list.
!--- 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
---------------- ---------------- -------------
172.18.124.0 255.255.255.0 telnet ssh snmp

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

Disabilitazione di SSH

In alcune situazioni, potrebbe essere necessario disabilitare il protocollo SSH sullo switch. È necessario verificare se il protocollo SSH è configurato sullo switch e, in caso affermativo, disabilitarlo.

Per verificare se SSH è stato configurato sullo switch, usare il comando **show crypto key**. Se nell'output viene visualizzata la chiave RSA, il protocollo SSH è stato configurato e abilitato sullo switch. Di seguito è riportato un esempio.

```
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
```

Per rimuovere la chiave crittografica, usare il comando **clear crypto key rsa** per disabilitare il protocollo SSH sullo switch. Di seguito è riportato un esempio.

```
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)
```

debug in Catalyst

Per attivare i debug, usare il comando **set trace ssh 4**.

Per disattivare i debug, usare il comando **set trace ssh 0**.

Esempi di comandi debug per una connessione corretta

Da Solaris a Catalyst, 3DES (Triple Data Encryption Standard), password Telnet

Solaris

```
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>
```

Catalyst

```
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.
```

Da PC a Catalyst, 3DES, password Telnet

Catalyst

```
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.
```

Da Solaris a Catalyst, 3DES, autenticazione, autorizzazione e autenticazione (AAA)

Solaris

```
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>
```

Catalyst

```
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.
```

Esempi di comandi debug per problemi che possono verificarsi

Debug Catalyst con il client che tenta di eseguire [non supportato] la crittografia 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
```

Debug Catalyst con password Telnet non valida

```
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.
```

Debug Catalyst con autenticazione AAA non valida

```
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
```

Risoluzione dei problemi

In questa sezione vengono illustrati diversi scenari di risoluzione dei problemi relativi alla configurazione SSH sugli switch Cisco.

Impossibile connettersi allo switch tramite SSH

Problema:

Impossibile connettersi allo switch con SSH.

Il comando **debug ip ssh** visualizza questo output:

```
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
```

Soluzione:

Il problema si verifica per uno dei motivi seguenti:

- Le nuove connessioni SSH hanno esito negativo dopo la modifica del nome host.
- SSH configurato con chiavi senza etichetta (con FQDN del router).

Le soluzioni per questo problema sono:

- Se il nome host è stato modificato e SSH non funziona più, azzerare la nuova chiave e creare un'altra chiave con l'etichetta appropriata.
  ```
  crypto key zeroize rsa
  crypto key generate rsa general-keys label (label) mod (modulus) [exportable]
  ```
- Non utilizzare chiavi RSA anonime (denominate in base all'FQDN dello switch). Utilizzare chiavi contrassegnate.
  ```
  crypto key generate rsa general-keys label (label) mod (modulus) [exportable]
  ```

Per risolvere il problema per sempre, aggiornare il software IOS a una delle versioni in cui il problema è stato risolto.

Èstato segnalato un bug relativo a questo problema. Per ulteriori informazioni, fare riferimento all'ID bug Cisco CSCtc41114 (solo utenti registrati).

Informazioni correlate

- Pagina di supporto SSH
- Configurazione di Secure Shell sui router e gli switch con Cisco IOS
- Bug Toolkit
- Supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).