Configurazione di SSH su router e switch

Sommario

Introduzione

In questo documento viene descritto come configurare Secure Shell (SSH) ed eseguirne il debug

sui router o sugli switch Cisco con software Cisco IOS®.

Prerequisiti

Requisiti

Per il supporto del protocollo SSH, l'immagine Cisco IOS in uso deve essere un'immagine k9(crypto). Ad esempio, c3750e-universalk9-tar.122-35.SE5.tar è un'immagine k9(crypto).

Componenti usati

Il riferimento delle informazioni contenute in questo documento è il software Cisco IOS 3600 (C3640-IK9S-M), versione 12.2(2)T1.

Il protocollo SSH è stato introdotto nelle seguenti piattaforme e immagini Cisco IOS:

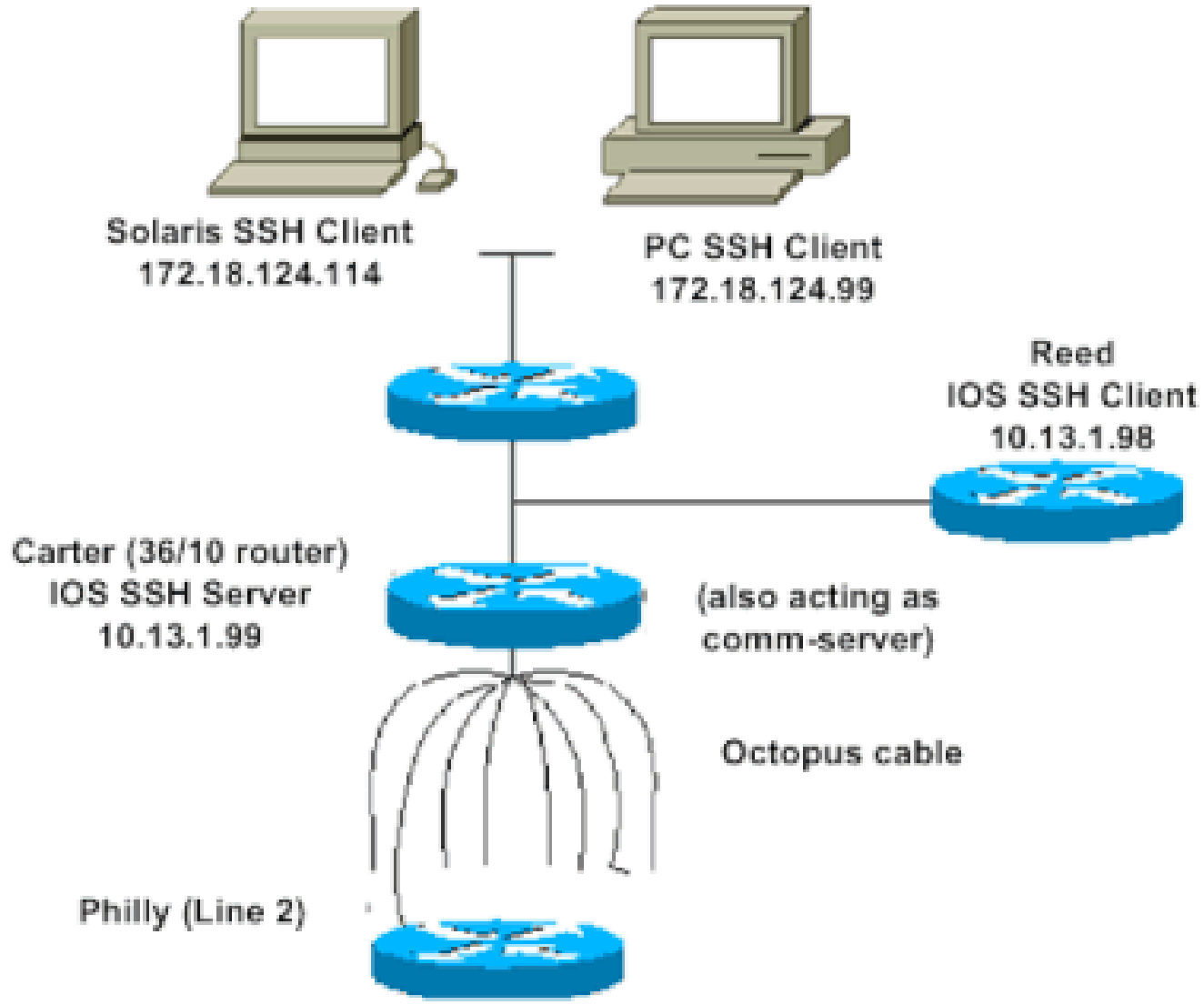
- L'accesso alla linea terminale SSH (nota anche come reverse Telnet) è stato introdotto in alcune piattaforme e immagini Cisco IOS a partire da Cisco IOS Software Release 12.2.2.T.
- Il supporto SSH versione 2.0 (SSH v2) è stato introdotto in alcune piattaforme e immagini Cisco IOS a partire da Cisco IOS Software Release 12.1(19)E.

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, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Diagramma di rete SSH v2



Test di autenticazione

Test di autenticazione senza SSH

Provare anzitutto l'autenticazione senza SSH per essere certi che funzioni sul router Carter prima di aggiungere il supporto SSH. Ai fini dell'autenticazione, è possibile usare un nome utente e una password locali o un server di autenticazione, autorizzazione e accounting (AAA) con TACACS+ o RADIUS. (L'autenticazione tramite password della linea non è consentita con SSH.) In questo esempio l'autenticazione viene effettuata con i dati di accesso locali, per accedere al router in modalità Telnet con il nome utente cisco e la password cisco.

Nota: in questo documento, viene usato l'acronimo vty per indicare il tipo di terminale virtuale (Virtual Terminal Type).

```
!--- 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.
```

Test di autenticazione con SSH

Per effettuare il test di autenticazione con SSH, aggiungere le istruzioni precedenti per abilitare SSH sul server Carter e testare il protocollo SSH tra le postazioni PC e 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
```

A questo punto, il comando show crypto key mypubkey rsa deve restituire la chiave generata. Dopo aver aggiunto la configurazione SSH, verificare la possibilità di accedere al router dalle postazioni PC e UNIX.

Impostazioni di configurazione facoltative

Prevenzione di connessioni non SSH

Per fare in modo che il router stabilisca esclusivamente connessioni SSH, aggiungere il comando transport input ssh dopo le istruzioni con cui si negano le connessioni non SSH. Le connessioni Telnet dirette (non SSH) vengono rifiutate.

```
line vty 0 4

!--- Prevent non-SSH Telnets.

transport input ssh
```

Verificare che gli utenti non SSH non possano connettersi al router Carter in modalità Telnet.

Configurazione di un router o di uno switch IOS come client SSH

Per abilitare il supporto SSH su un router Cisco IOS, è necessario eseguire quattro passaggi:

1. Configurare il comando hostname.

2. Configurare il dominio DNS.

3. Generare la chiave SSH.

4. Abilitare il supporto del trasporto SSH per vty.

Affinché un dispositivo agisca come client SSH, è necessario aggiungere il supporto SSH su un secondo dispositivo chiamato Reed. Si realizzerà quindi una relazione client-server tra i dispositivi, in cui il dispositivo Carter agirà come server e il dispositivo Reed come client. La configurazione del client SSH Cisco IOS sul dispositivo Reed è la stessa di quella richiesta per il server SSH sul dispositivo 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 al

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 su

line vty 0 4
transport input ssh

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

Per verificarlo, inviare questo comando dal client SSH Cisco IOS (Reed) al server SSH Cisco IOS (Carter):

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

Configurazione di un router IOS come server SSH per eseguire l'autenticazione RSA

Completare questa procedura per configurare il server SSH in modo che esegua l'autenticazione RSA.

1. Specificare il nome dell'host.

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

2. Assegnare un nome al dominio predefinito.

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

3. Generare una coppia di chiavi RSA.

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

4. Configurare le chiavi SSH-RSA per l'autenticazione di server e utente.

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

5. Configurare il nome utente SSH.

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

6. Specificare la chiave pubblica RSA del dispositivo peer remoto.

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

7. Specificare il tipo di chiave SSH e la versione. (Questo passaggio è facoltativo.)

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

8. Uscire dalla modalità corrente e tornare alla modalità di esecuzione privilegiata.

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

Aggiunta dell'accesso SSH alla linea terminale

Per autenticare la linea terminale SSH in uscita, è possibile configurare e provare il protocollo SSH sul collegamento in modalità reverse Telnet in uscita tramite il dispositivo Carter, che agisce da server di comunicazione per Philly.

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

Se Philly è collegato alla porta 2 di Carter, è possibile configurare il supporto SSH su Philly dal dispositivo Reed tramite Carter usando questo comando:

```
ssh -v 2 -c aes256-cbc -m hmac-sha1-160 -p 2002 10.31.1.99
```

In Solaris, è possibile usare questo comando:

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

Limitazione dell'accesso SSH a una subnet

La connettività SSH deve essere limitata a una sottorete in cui far rientrare tutti gli altri tentativi SSH provenienti da indirizzi IP esterni alla sottorete.

A tal fine, attenersi alla seguente procedura:

1. Definire un elenco degli accessi che autorizzi il traffico proveniente dalla sottorete specificata.
2. Limitare l'accesso all'interfaccia della linea VTY con `access-class`.

Di seguito viene riportata una configurazione di esempio. Nell'esempio, solo l'accesso SSH alla subnet 10.10.10.0 255.255.255.0 è consentito, ogni altro tipo di accesso è negato.

```
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
```

Nota: la stessa procedura di blocco dell'accesso SSH è applicabile anche alle piattaforme dello switch.

Configurazione di SSH versione 2

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

Differenze nell'output del comando banner

L'output del comando banner è diverso nelle connessioni Telnet e nelle diverse versioni SSH. Nella tabella viene mostrata la logica di funzionamento del comando banner a seconda del tipo di connessione.

Opzioni del comando banner	Telnet	SSH v2
banner log	Viene visualizzato prima dell'accesso al dispositivo.	Viene visualizzato prima dell'accesso al dispositivo.
banner motd	Viene visualizzato prima	Viene visualizzato dopo

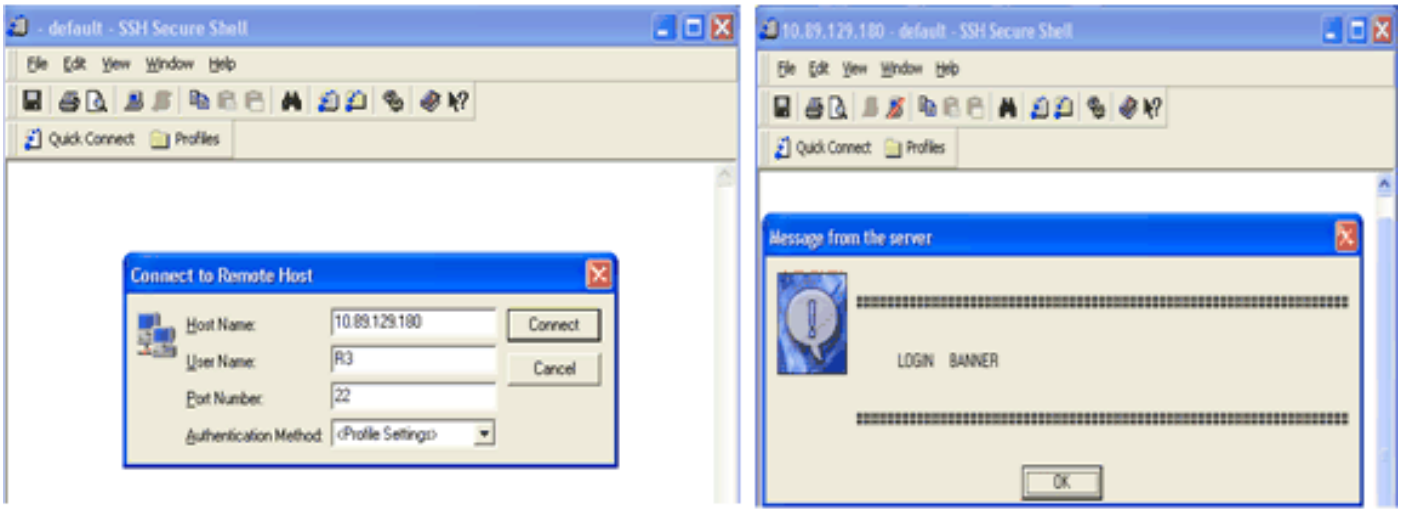
	dell'accesso al dispositivo.	l'accesso al dispositivo.
banner exec	Viene visualizzato dopo l'accesso al dispositivo.	Viene visualizzato dopo l'accesso al dispositivo.

Nota: l'uso di SSH versione 1 non è più consigliato.

Impossibile visualizzare il banner di accesso

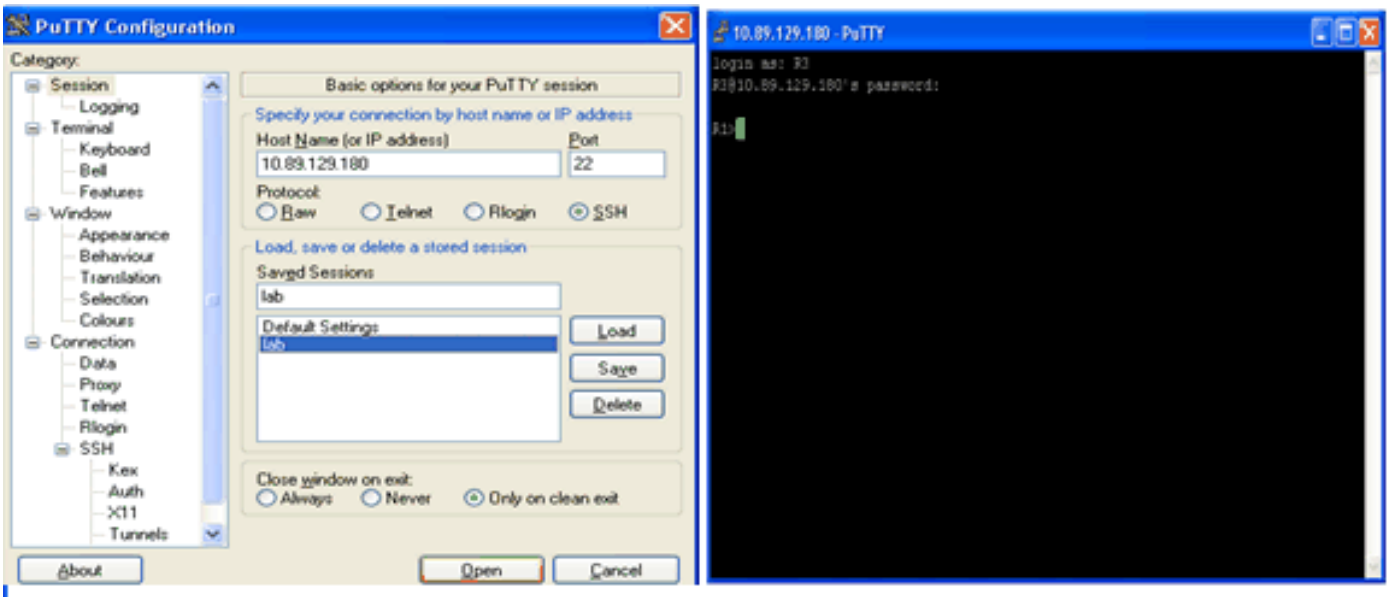
L'uso di SSH versione 2 supporta il banner di accesso. Quando si avvia la sessione SSH con il router Cisco, il banner di accesso viene visualizzato se il client SSH invia il nome utente. Ad esempio, quando si usa il client Secure Shell ssh, il banner di accesso viene visualizzato. Quando si usa il client PuTTY ssh, il banner di accesso non viene visualizzato. Infatti, a differenza del client PuTTY, il client SSH invia il nome utente per impostazione predefinita.

Il client SSH ha bisogno del nome utente per avviare la connessione con il dispositivo SSH. Se il nome dell'host e il nome dell'utente non sono stati specificati, il pulsante Connect (Connetti) non risulterà abilitato. In questa schermata viene mostrata la visualizzazione del banner di accesso quando il client SSH si connette al router. Il banner richiede quindi una password.



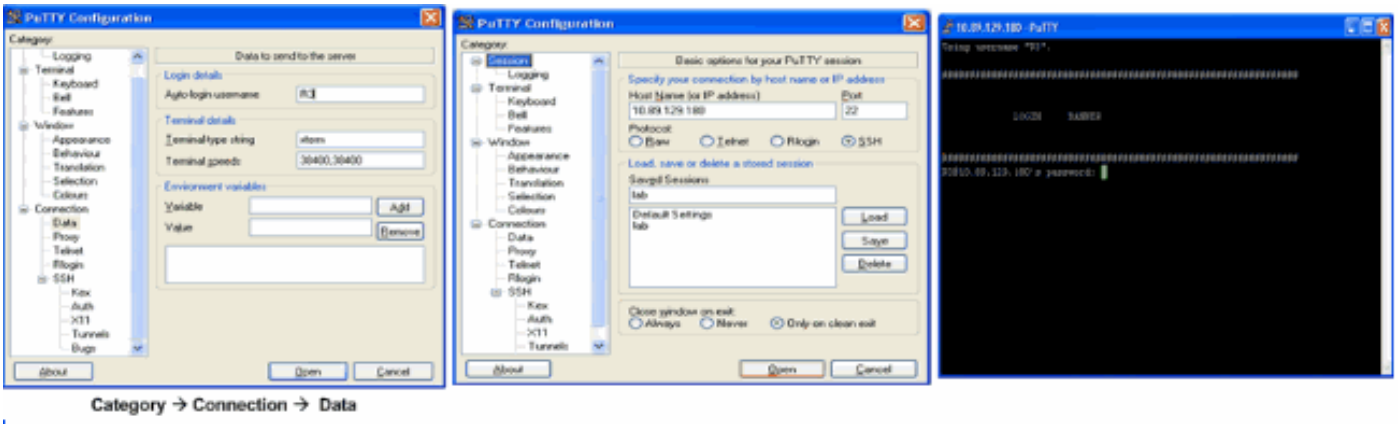
Il banner richiede una password

Il client PuTTy non ha bisogno del nome utente per avviare la connessione SSH al router. In questa schermata viene mostrato come il client PuTTy si connetta al router e richieda il nome utente e la password. Il banner di accesso non viene visualizzato.



Connessione SSH al router

In questa schermata viene mostrata la visualizzazione del banner di accesso quando il client PuTTY è configurato in modo da inviare al router il nome utente.



Invio del nome utente al router

Comandi debug e show

Prima di usare i comandi debug qui descritti, consultare il documento Informazioni importanti sui comandi di debug. Alcuni comandi show sono supportati dallo strumento Output Interpreter (solo utenti registrati); lo strumento permette di visualizzare un'analisi dell'output del comando show.

- debug ip ssh: visualizza i messaggi di debug per SSH.
- show ssh: visualizza lo stato delle connessioni del server SSH.

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

- show IP ssh: visualizza la versione e i dati di configurazione del protocollo SSH.

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

Output di esempio del comando debug

Debug del router

```
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
```

Debug del server

Nota: questo è l'output sulle macchine 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.
```

Configurazioni errate

Nelle sezioni seguenti vengono riportati alcuni output di esempio del comando debug per diverse configurazioni errate.

SSH da un client SSH senza Data Encryption Standard (DES)

Password non valida

Debug del router

```
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
```

Il client SSH usa una crittografia non supportata (Blowfish)

Debug del router

```
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
```

Errore "%SSH-3-PRIVATEKEY: Unable to Retrieve RSA Private Key for"

Questo messaggio di errore, che segnala l'impossibilità di richiamare la chiave privata RSA, può essere generato in caso di modifica del nome di dominio o del nome host. Provare a risolvere il problema con queste soluzioni temporanee:

- Azzerare le chiavi RSA e rigenerarle.

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

- Se la soluzione precedente non funziona, provare la seguente procedura:
    1. Azzerare tutte le chiavi RSA.
    2. Riavviare il dispositivo.
    3. Creare nuove chiavi contrassegnate per SSH.

Suggerimenti

- Se i comandi della configurazione SSH sono rifiutati come non validi, la coppia di chiavi RSA per il router non è stata generata correttamente. Verificare di aver specificato un nome host e un dominio. Quindi, usare il comando crypto key generate rsa per generare una coppia di chiavi RSA e abilitare il server SSH.
- Quando si configura la coppia di chiavi RSA, potrebbero essere visualizzati questi messaggi di errore:
    1. `Nessun nome host specificato.`

       Configurare un nome host per il router utilizzando il comando hostname in modalità di

configurazione globale.

2. `Nessun dominio specificato.`

   Configurare un dominio host per il router usando il comando ip domain-name in modalità di configurazione globale.

- Il numero di connessioni SSH ammesse è limitato al numero massimo di connessioni vty configurate per il router. Ogni connessione SSH utilizza una vty risorsa.
- SSH utilizza la sicurezza locale o il protocollo di sicurezza configurato sul server AAA sul router utilizzato per autenticare l'utente. Quando si configura la modalità AAA, verificare che tale modalità non venga utilizzata per la console. Per disabilitare la funzionalità AAA sulla console, usare la parola chiave appropriata in modalità di configurazione globale.
- No SSH server connections running:

```
carter#show ssh

%No SSHv2 server connections running.
```

Questo output suggerisce che il server SSH è disabilitato o non abilitato correttamente. Se il server SSH è già stato configurato, si consiglia di riconfigurarlo nel dispositivo. Completare questa procedura per riconfigurare il server SSH sul dispositivo.

1. Eliminare la coppia di chiavi RSA. Dopo aver eliminato la coppia di chiavi RSA, il server SSH viene disabilitato automaticamente.

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

Nota: quando si abilita SSH v2, è importante generare una coppia di chiavi di almeno 768 bit.

Attenzione: dopo aver salvato la configurazione, questo comando non può più essere annullato. Inoltre, dopo aver eliminato le chiavi RSA, non è più possibile usare i certificati o l'autorità di certificazione o scambiare i certificati con altri dispositivi peer IP Security (IPSec) a meno che non si rigenerino le chiavi RSA per riconfigurare l'interoperabilità con l'autorità di certificazione, ottenere il certificato dall'autorità di certificazione e richiedere nuovamente il certificato.

---

2. Riconfigurare il nome dell'host e il nome di dominio del dispositivo.

```
carter(config)#hostname hostname

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

3. Generare la coppia di chiavi RSA per il router. Questa operazione abilita automaticamente l'accesso SSH.

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

Nota: per ulteriori informazioni sull'uso del comando crypto key generate rsa, consultare la Guida di riferimento ai comandi di Cisco IOS Security, release 12.3.

Nota: in caso il router non riesca a leggere un pacchetto, potrebbe essere generato il messaggio `SSH2 0: Unexpected mesg type received` (SSH2 0: ricevuto messaggio di tipo imprevisto). Per risolvere il problema, aumentare la lunghezza della chiave durante la generazione delle chiavi RSA per SSH.

4. Configurare il server SSH.

5. Per abilitare e configurare un router/uno switch Cisco per il server SSH, utilizzare i parametri SSH. In assenza di parametri SSH configurati dall'utente, vengono utilizzati i valori predefiniti.

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

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

Informazioni correlate

- Pagina di supporto dei prodotti SSH

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).