

Utilizzare l'opzione -O per garantire la riuscita dell'SCP dai client su dispositivi OpenSSH9.0 a IOS XE

Sommario

[Introduzione](#)

[Soluzione alternativa](#)

[Premesse](#)

[Configurazione di SSH e SCP](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come usare l'opzione -O per garantire la riuscita dell'SCP dai client su OpenSSH9.0 ai dispositivi Cisco IOS® XE.

Soluzione alternativa

L'opzione -O può essere usata sulle versioni più recenti di OpenSSH con il comando SCP per forzare l'uso di SCP per il trasferimento dei file invece di SFTP.

```
scp -O file.ext username@192.0.2.1:file.ext
```

Premesse

SCP può essere utilizzato per trasferire file tra un client SCP e un server SCP. SCP utilizza una sessione SSH per l'autenticazione. Una volta autenticato l'utente, si apre un altro canale per trasferire il file con SCP. In OpenSSH9.0 e versioni successive, per l'autenticazione viene ancora usato SSH, ma per il trasferimento dei file viene usato SFTP anziché SCP. Ciò crea un problema con le versioni correnti di Cisco IOS XE perché al momento SFTP non è supportato per trasferire i file tramite SSH. La sessione SSH ha esito positivo e nel buffer syslog è presente un log delle operazioni riuscite di accesso. Tuttavia, la connessione si chiude bruscamente quando il client SCP tenta di avviare il trasferimento SFTP.

Configurazione di SSH e SCP

Prerequisiti per l'utilizzo di un client SCP per trasferire un file a un dispositivo Cisco IOS XE.

- È necessario configurare SSH
- È necessario configurare l'accesso locale o AAA
- L'utente deve disporre del livello di privilegio 15 per eseguire SCP
- Il server SCP deve essere abilitato

Ecco un esempio di configurazione.

```
# configure SSH
hostname c8000v
ip domain name cisco.com
crypto key generate rsa
# optional - use ssh version 2
ip ssh version 2
# verify the SSH server is online
show ip ssh
# create a user with privilege level 15
username cisco privilege 15 password 0 cisco
# configure the vty line to use local login and allow ssh
line vty 0 4
login local
transport input ssh
# Enable the SCP server
ip scp server enable
```



Suggerimento: Per ulteriori informazioni sulla configurazione SSH, consultare [qui](#).



Nota: è possibile usare aaa anziché l'accesso locale.

Al termine della configurazione, è possibile configurare il protocollo SSH/SCP sul dispositivo con un indirizzo IP raggiungibile.

Da un dispositivo Linux, è possibile utilizzare questi comandi con l'indirizzo IP del dispositivo:

- ssh [cisco@192.0.2.1](#)
- scp file.ext cisco@192.0.2.1:file.ext



Nota: Per impostazione predefinita, il file viene copiato su bootflash.

Risoluzione dei problemi

In caso di problemi, verificare i seguenti sintomi:

1. La versione OpenSSH del client è 9.0 o successiva.

```
jeff@jeff-virtual-machine:~$ ssh -V  
OpenSSH_9.0p1 Ubuntu-1ubuntu7, OpenSSL 3.0.5 5 Jul 2022
```

2. Il client mostra che la connessione si chiude bruscamente senza alcun errore o trasferimento di file.

```
jeff@jeff-virtual-machine:~$ scp test.txt cisco@192.0.2.1:test.txt
(cisco@192.0.2.1) Password:
scp: Connection closed
```

3. Sul router, un syslog mostra la connessione SSH riuscita, ma il file non è stato trasferito.

```
*Mar 26 18:06:57.290: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: cisco] [Source: 192.0.2.2] [local]
```

4. I debug SCP sul router non mostrano alcuna informazione.

```
c8000v#debug ip scp
Incoming SCP debugging is on
```

5. L'opzione SCP con -v mostra i log di debug che inviano il sottosistema SFTP.

```
scp -v test.txt cisco@192.0.2.1:test.txt
Executing: program /usr/bin/ssh host 192.0.2.1, user cisco, command sftp
OpenSSH_9.0p1 Ubuntu-1ubuntu7, OpenSSL 3.0.5 5 Jul 2022
```

<snip>

```
debug1: Entering interactive session.
debug1: pledge: filesystem
debug1: Sending environment.
debug1: channel 0: setting env LANG = "en_US.UTF-8"
debug1: Sending subsystem: sftp
debug1: client_input_channel_req: channel 0 rtype exit-status reply 0
scp: Connection closed
```

6. I debug ssh sul router show SSH cercano un sottosistema SFTP e chiudono la connessione.

```
c8000v#debug ip ssh detail
```

```
ssh detail messages debugging is on
```

```
*Mar 24 14:25:05.074: SSH: MD5 compliance exception Registered
```

```
*Mar 24 14:25:05.074: SSH1: starting SSH control process
```

```
*Mar 24 14:25:05.074: SSH1: sent protocol version id SSH-2.0-Cisco-1.25
```

```
*Mar 24 14:25:05.075: SSH1: protocol version id is - SSH-2.0-OpenSSH_9.0p1 Ubuntu-1ubuntu7 <snip>
```

```
*Mar 24 14:25:07.370: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: cisco] [Source: 10.10.10.10] [local]
```

```
*Mar 24 14:25:07.379: SSH2 1: channel open request *Mar 24 14:25:07.389: SSH2 1: env request
*Mar 24 14:25:07.389: SSH2 1: subsystem request *Mar 24 14:25:07.389: SSH2 1: subsystem message received
*Mar 24 14:25:07.389: SSH2 1: searching for subsystem sftp for vty
*Mar 24 14:25:07.490: SSH1: Session terminated normally
```

7. Infine, l'opzione SCP con l'opzione -O ha esito positivo.

```
jeff@jeff-virtual-machine:~$ scp -O test.txt cisco@192.0.2.1:test.txt
(cisco@192.0.2.1) Password:
test.txt 100% 28 2.7KB/s 00:00
```

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).