

-Oオプションを使用して、OpenSSH9.0上のクライアントからIOS XEデバイスへのSCPを正常に実行します。

内容

[はじめに](#)

[回避策](#)

[背景説明](#)

[SSHおよびSCPの設定](#)

[トラブルシューティング](#)

はじめに

このドキュメントでは、-Oオプションを使用して、OpenSSH9.0上のクライアントからCisco IOS® XEデバイスへのSCPを正常に実行する方法について説明します。

回避策

-Oオプションは、SCPコマンドを使用してOpenSSHの新しいバージョンで使用し、ファイル転送にSFTPの代わりにSCPを使用できます。

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

背景説明

SCPを使用すると、SCPクライアントとSCPサーバの間でファイルを転送できます。SCPは認証にSSHセッションを使用します。ユーザが認証されると、別のチャンネルが開かれ、SCPを使用してファイルが転送されます。OpenSSH9.0以降のバージョンでは、認証にSSHが使用されていますが、ファイル転送にはSCPではなくSFTPが使用されます。現在のバージョンのCisco IOS XEでは、SSHによるファイル転送にSFTPが現在サポートされていないため、問題が発生します。SSHセッションは成功し、ログイン成功ログがsyslogバッファに記録されます。ただし、SCPクライアントがSFTP転送を開始しようとする、接続が突然終了します。

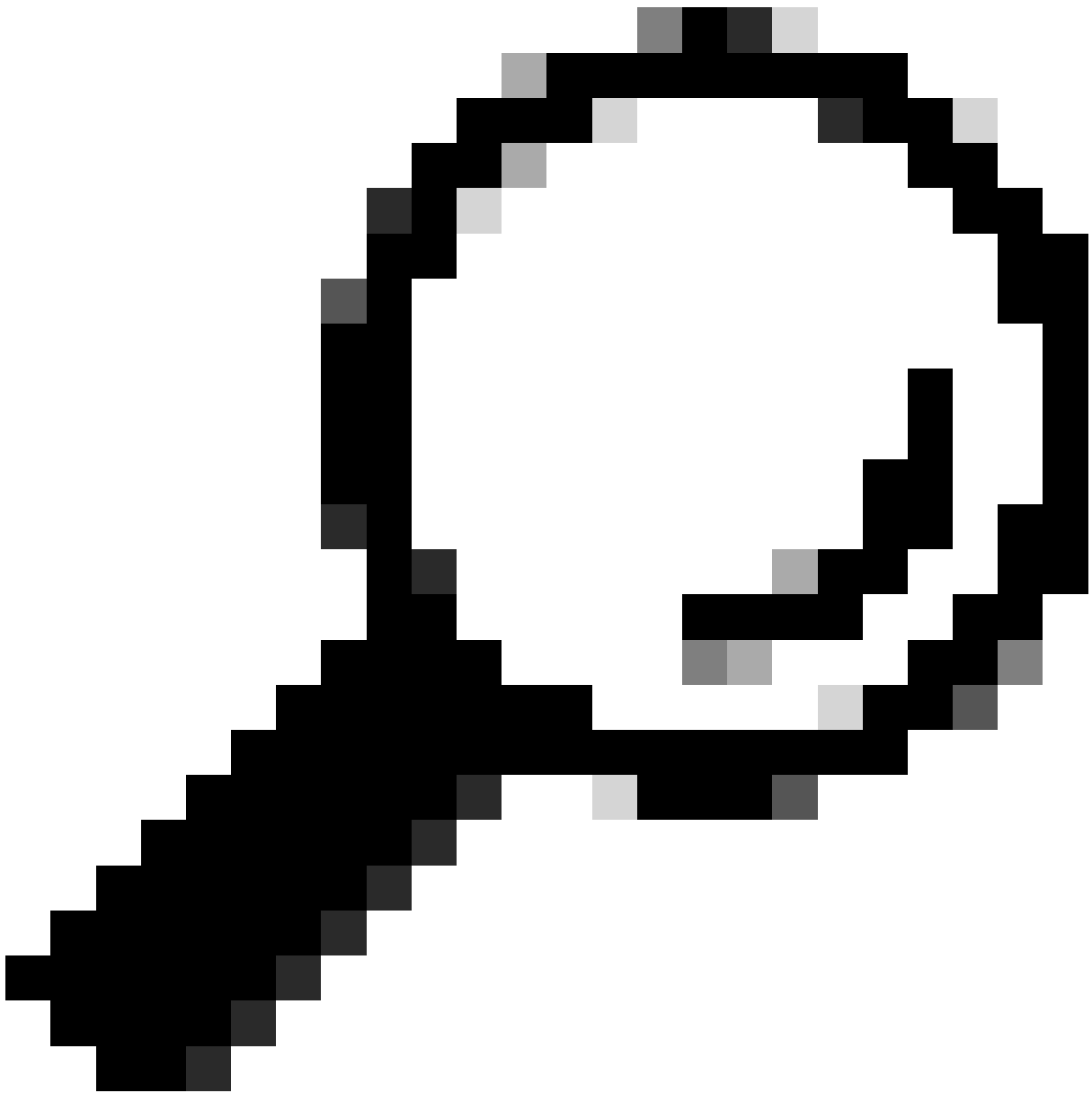
SSHおよびSCPの設定

SCPクライアントを使用してCisco IOS XEデバイスにファイルを転送するための前提条件。

- SSHを設定する必要がある
- ローカルログインまたはAAAを設定する必要がある
- ユーザがSCPにアクセスするには、特権レベル15が必要です
- SCPサーバを有効にする必要がある

次に設定例を示します

```
# 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
```



ヒント: SSHの設定に関する詳細は、[ここ](#)を参照してください。

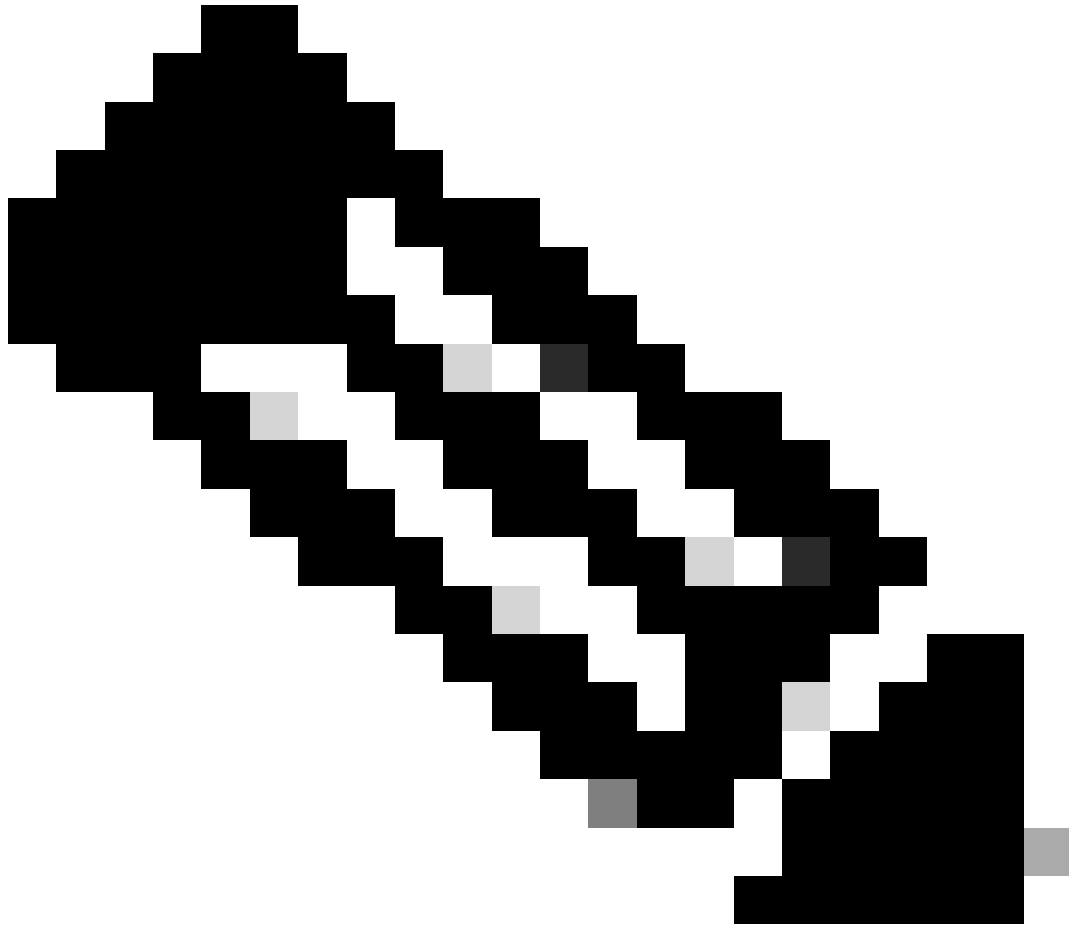


注：ローカルログインの代わりにaaaを使用できます。

設定が完了したら、デバイス上の到達可能なIPアドレスを持つデバイスにSSH/SCPを送信できます。

Linuxデバイスから、デバイスのIPアドレスに対して次のコマンドを使用できます。

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



注：デフォルトでは、ファイルはブートフラッシュにコピーされます。

トラブルシューティング

問題が発生した場合は、次の症状を確認してください。

1. OpenSSHバージョンのクライアントでは、9.0以降が表示されます。

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

2. クライアントは、エラーやファイル転送を行わずに接続が突然終了したことを示します。

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

3. ルータでsyslogにSSH接続の成功が表示されますが、ファイルは転送されませんでした。

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

4. ルータのSCPデバッグでは、情報が表示されません。

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

5. -vオプションを指定したSCPでは、SFTPサブシステムを送信しているデバッグログが表示されません。

```
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. ルータのsshデバッグでは、SSHはSFTPサブシステムを検索して接続を閉じます。

```
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] [10.10.10.10]
*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. 最後に、-Oオプションを指定したSCPは成功します。

```
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
```

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。