

UCSM 4.0ファームウェアへのアップグレード後にSCPおよびSFTPバックアップが失敗するトラブルシューティング

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[問題](#)

[4.0.2a UCSMへのアップグレード後のSFTPまたはSCP障害のトラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、ファームウェアを4.0.2aにアップグレードした後、Unified Computing System Manager(UCSM)でスケジュールまたはオンデマンドのバックアップ操作が失敗した場合の問題をトラブルシューティングする方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- UCS マネージャ
- SCP(Secure Copy Protocol)またはSFTP(Secure File Transfer Protocol)

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

問題

ファームウェアをバージョン4.0(2a)以降にアップグレードすると、UCSMでバックアップを実行できなくなります。

同様のエラーが表示されます

```
[Critical] F999723 4154197 sys/backup-cop-swinds01.aaaaa.com Fsm Failed 1 2019-09-11T10:05:55.706 2019-09-11T10:05:55.706 [FSM:FAILED]: internal system backup(FSM:sam:dme:MgmtBackupBackup). Remote-Invocation-Error: End point timed out. Check for IP, password, space or access related issues.#
```

Cisco UCS Manager 4.0(2a)リリース以降では、セキュリティで保護されていない特定の暗号がUCSファブリックインターコネクトによってブロックされます。セキュアプロトコルを使用してサーバにログインするには、次の3つのカテゴリの少なくとも1つのアルゴリズムをサポートするバージョンのOpenSSHを使用する必要があります。

- キー交換アルゴリズム

```
diffie-hellman-group-exchange-sha256
diffie-hellman-group16-sha512
diffie-hellman-group18-sha512
```

- 暗号化アルゴリズム

```
aes128-ctr
aes192-ctr
aes256-ctr
```

- MACアルゴリズム

```
hmac-sha2-256
hmac-sha2-512
```

注： リリースノート[UCSM 4.0を参照してください](#)

転送プロトコルがセキュアシェル(SSH)、SFTP、またはSCPの場合、使用中のバックアップユーティリティまたはサーバはUCSの新しいOpenSSH要件をサポートできません。したがって、接続がブロックされ、バックアップが失敗します。

4.0.2a UCSMへのアップグレード後のSFTPまたはSCP障害のトラブルシューティング

ステップ 1： Putty、SFTPサーバ、SCPサーバ、またはその他のサードパーティツールのソフトウェアバージョンをアップグレードします。

ステップ2： 使用するセキュアツールが、Cisco UCS Managerリリース4.0(2a)と同様に必要なアルゴリズムをサポートしていることを確認します。特定の安全でない暗号がUCSファブリックインターコネクトによってブロックされます。セキュアなプロトコルを使用してサーバにログインするには、次の3つのカテゴリの少なくとも1つのアルゴリズムをサポートするバージョンのOpenSSHを使用する必要があります。

- キー交換アルゴリズム

```
diffie-hellman-group-exchange-sha256
diffie-hellman-group16-sha512
diffie-hellman-group18-sha512
```

- 暗号化アルゴリズム

aes128-ctr
aes192-ctr
aes256-ctr

- MACアルゴリズム

hmac-sha2-256
hmac-sha2-512

ステップ3：必要に応じてさらにトラブルシューティングを行うために、Cisco TACに契約します。

関連情報

- [バグCSCvr51157](#) - UCSM 4.0.4 - SFTPバックアップがlibcryptoメッセージのエラーで失敗します。
- [バグCSCvs62849](#) - UCSMのバックアップ操作が正しくない署名とおよび現在の回避策は、デバッグプラグインを使用して連邦情報処理標準(FIPS)を無効にすることです。
- [バグCSCvt27613](#):UCS-FI-6454-U with firmware 4.1(1a) key exchange algorithm error diffie-hellman-group16-sha512。
- [リリースノートUCSM 4.0](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)