

Resolución de problemas de copias de seguridad SCP y SFTP que fallan después de actualizar al firmware UCSM 4.0

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Problema](#)

[Solución de problemas de respaldo a SFTP o falla SCP después de actualizar a UCSM 4.0.2a](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo resolver un problema relacionado con operaciones de copia de seguridad fallidas programadas o a petición en Unified Computing System Manager (UCSM) después de una actualización del firmware a 4.0.2a.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- UCS Manager
- SCP (protocolo de copia segura) o SFTP (protocolo de transferencia segura de archivos)

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Problema

Después de actualizar el firmware a la versión 4.0(2a) o posterior, las copias de seguridad ya no pueden funcionar en UCSM.

Se puede ver un error similar

```
[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.#
```

Con la versión 4.0(2a) de Cisco UCS Manager y las versiones posteriores, Fabric Interconnects UCS bloquean determinados elementos inseguros. Para iniciar sesión en los servidores a través del protocolo seguro, debe utilizar una versión de OpenSSH que admita al menos un algoritmo en cada una de las tres categorías:

- Algoritmos de intercambio de claves

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

- Algoritmos de cifrado

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

- Algoritmos MAC

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

Nota: Consulte [Release Notes UCSM 4.0](#)

La utilidad de respaldo o el servidor en uso no pueden soportar los nuevos requisitos de OpenSSH para UCS cuando el protocolo de transferencia es Secure Shell (SSH), SFTP o SCP. Por lo tanto, la conexión se bloquea y la copia de seguridad falla.

Solución de problemas de respaldo a SFTP o falla SCP después de actualizar a UCSM 4.0.2a

Paso 1. Actualización de la versión de software de Putty, SFTP Server, SCP Server u otra herramienta de terceros.

Paso 2. Confirme que la herramienta segura utilizada es compatible con los algoritmos requeridos, como con Cisco UCS Manager versión 4.0(2a), algunos cifrados inseguros están bloqueados por Fabric Interconnects UCS. Para iniciar sesión en los servidores a través de un protocolo seguro, debe utilizar una versión de OpenSSH que admita al menos un algoritmo en cada una de las tres categorías:

- Algoritmos de intercambio de claves

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

- Algoritmos de cifrado

aes128-ctr
aes192-ctr
aes256-ctr

- Algoritmos MAC

hmac-sha2-256
hmac-sha2-512

Paso 3. Contrate el TAC de Cisco para resolver problemas adicionales si es necesario.

Información Relacionada

- [Error CSCvr51157](#) - UCSM 4.0.4 - La copia de seguridad de SFTP falla con error en el mensaje **libcrypto**.
- [Error CSCvs62849](#) - La operación de respaldo de UCSM falla con la **firma incorrecta** y la solución alternativa actual es deshabilitar los estándares federales de procesamiento de información (FIPS) a través del complemento de depuración.
- [Error CSCvt27613](#) - UCS-FI-6454-U con el algoritmo de intercambio de claves firmware 4.1(1a) error diffie-hellman-group16-sha512.
- [Notas de la versión UCSM 4.0](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)