

Risoluzione dei problemi di backup SCP e SFTP non riusciti dopo l'aggiornamento al firmware UCSM 4.0

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Problema](#)

[Risoluzione dei problemi di backup su SFTP o SCP dopo l'aggiornamento a UCSM 4.0.2a](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come risolvere un problema relativo a operazioni di backup pianificate o su richiesta non riuscite in Unified Computing System Manager (UCSM) dopo un aggiornamento del firmware alla versione 4.0.2a.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- UCS Manager
- SCP (Secure Copy Protocol) o SFTP (Secure File Transfer Protocol)

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

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.

Problema

Dopo un aggiornamento del firmware alla versione 4.0(2a) o successive, i backup non possono più funzionare su UCSM.

Errore simile

```
[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 Cisco UCS Manager 4.0(2a) e versioni successive, alcune cifrature non sicure vengono bloccate dalle interconnessioni fabric UCS. Per accedere ai server tramite il protocollo secure, è necessario utilizzare una versione di OpenSSH che supporti almeno un algoritmo in ciascuna delle tre categorie:

- Algoritmi di scambio chiave

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

- Algoritmi di crittografia

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

- Algoritmi MAC

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

Nota: Fare riferimento alle [note sulla versione UCSM 4.0](#)

L'utilità di backup o il server in uso non possono supportare i nuovi requisiti OpenSSH per UCS quando il protocollo di trasferimento è Secure Shell (SSH), SFTP o SCP. Pertanto, la connessione viene bloccata e il backup non riesce.

Risoluzione dei problemi di backup su SFTP o SCP dopo l'aggiornamento a UCSM 4.0.2a

Passaggio 1. Aggiornamento della versione software di Putty, SFTP Server, SCP Server o altro strumento di terze parti.

Passaggio 2. Confermare che lo strumento sicuro utilizzato supporti gli algoritmi richiesti come in Cisco UCS Manager versione 4.0(2a), in quanto alcune cifrature non sicure sono bloccate da UCS Fabric Interconnect. Per accedere ai server tramite un protocollo sicuro, è necessario utilizzare una versione di OpenSSH che supporti almeno un algoritmo in ciascuna delle tre categorie seguenti:

- Algoritmi di scambio chiave

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

- Algoritmi di crittografia

aes128-ctr
aes192-ctr
aes256-ctr

- Algoritmi MAC

hmac-sha2-256
hmac-sha2-512

Passaggio 3. Contrarre Cisco TAC per risolvere ulteriormente i problemi, se necessario.

Informazioni correlate

- [Bug CSCvr51157](#) - UCSM 4.0.4 - Il backup SFTP non riesce con un errore nel messaggio **libcrypto**.
- [Bug CSCvs62849](#) - Operazione di backup UCSM non riuscita con **firma non corretta** e Per ovviare al problema, è necessario disabilitare i Federal Information Processing Standards (FIPS) tramite il plug-in di debug.
- [Bug CSCvt27613](#) - UCS-FI-6454-U con firmware 4.1(1a) errore algoritmo scambio chiave diffie-hellman-group16-sha512.
- [Note sulla release UCSM 4.0](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)