升級到UCSM 4.0韌體後SCP和SFTP備份失敗故障排除

目錄

簡介

本文檔介紹在韌體升級到4.0.2a後，如何對Unified Computing System Manager(UCSM)中與計畫或按需備份操作失敗相關的問題進行故障排除。

必要條件

需求

思科建議您瞭解以下主題：

- UCS管理器
- SCP（安全複製協定）或SFTP（安全檔案傳輸協定）

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

問題

韌體升級到4.0(2a)版或更高版本後，備份在UCSM上無法再工作。

可以看到類似的錯誤

```
[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.#
```

在Cisco UCS Manager 4.0(2a)版本及更高版本中，UCS交換矩陣互聯會阻止某些不安全密碼。為了通過安全協定登入到伺服器，必須使用至少支援以下三種類別中每種演算法的OpenSSH版本：

- 金鑰交換演算法

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

- 加密演算法

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

- MAC演算法

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

附註：請參閱發行說明UCSM 4.0

當傳輸協定為Secure Shell(SSH)、SFTP或SCP時，使用的備份實用程式或伺服器無法支援UCS的新OpenSSH要求。因此，連線被阻止，備份失敗。

升級到4.0.2a UCSM後，排除SFTP或SCP備份故障

步驟1. 升級Putty、SFTP伺服器、SCP伺服器或其他第三方工具的軟體版本。

步驟2.確認使用的安全工具支援所需的演算法，與Cisco UCS Manager版本4.0(2a)一樣，某些不安全密碼被UCS交換矩陣互聯阻止。要通過安全協定登入到伺服器，必須使用至少支援三種類別中每種演算法的OpenSSH版本：

- 金鑰交換演算法

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

- 加密演算法

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

- MAC演算法

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

步驟3.如果需要，請與Cisco TAC聯絡，以進行進一步故障排除。

相關資訊

- **錯誤CSCvr51157** - UCSM 4.0.4 - SFTP備份失敗，在libcrypto消息中顯**示錯**誤。
- **錯誤CSCvs62849** - UCSM備份操作失敗，**簽名不**正確， 目前的解決方法是通過debug外掛禁用聯邦資訊處理標準(FIPS)。
- 錯誤CSCvt27613 — 使用韌體4.1(1a)金鑰交換演算法的UCS-FI-6454-U diffie-hellman-group16-sha512。
- **發行說明UCSM 4.0**
- **技術支援與文件 - Cisco Systems**