Fehlerbehebung bei SCP- und SFTP-Backups nach dem Upgrade auf die UCSM 4.0-Firmware fehlgeschlagen

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie nach einem Firmware-Upgrade auf 4.0.2a ein Problem im Zusammenhang mit fehlgeschlagenen geplanten oder On-Demand-Backups in Unified Computing System Manager (UCSM) beheben können.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

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

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Problem

Nach einem Firmware-Upgrade auf Version 4.0(2a) oder höher können Backups auf UCSM nicht mehr funktionieren.

Ein ähnlicher Fehler ist zu erkennen.

```
[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.#
```

Ab der Version Cisco UCS Manager 4.0(2a) werden bestimmte unsichere Chiffren von UCS Fabric Interconnects blockiert. Um sich über das sichere Protokoll bei Servern anzumelden, müssen Sie eine Version von OpenSSH verwenden, die mindestens einen Algorithmus in jeder der drei folgenden Kategorien unterstützt:

- Schlüsselaustauschalgorithmen

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

- Verschlüsselungsalgorithmen

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

- MAC-Algorithmen

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

Hinweis: *Weitere Informationen finden Sie in den* Versionshinweisen zu UCSM 4.0.

Das verwendete Backup-Dienstprogramm oder der verwendete Server kann die neuen OpenSSH-Anforderungen für UCS nicht unterstützen, wenn das Übertragungsprotokoll Secure Shell (SSH), SFTP oder SCP ist. Daher wird die Verbindung blockiert, und die Sicherung schlägt fehl.

Fehlerbehebung für Backup auf SFTP- oder SCP-Fehler nach dem Upgrade auf 4.0.2a UCSM

Schritt 1: Aktualisieren Sie die Softwareversion von Putty, SFTP Server, SCP Server oder einem anderen Drittanbieter-Tool.

Schritt 2: Vergewissern Sie sich, dass das verwendete sichere Tool die erforderlichen Algorithmen unterstützt, wie bei Cisco UCS Manager Version 4.0(2a), bestimmte unsichere Chiffren von UCS Fabric Interconnects blockiert werden. Um sich über ein sicheres Protokoll bei Servern anzumelden, müssen Sie eine Version von OpenSSH verwenden, die mindestens einen Algorithmus in jeder der drei Kategorien unterstützt:

- Schlüsselaustauschalgorithmen

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

- Verschlüsselungsalgorithmen

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

- MAC-Algorithmen

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

Schritt 3: Wenden Sie sich an das Cisco TAC, um bei Bedarf weitere Fehlerbehebungen durchzuführen.

Zugehörige Informationen

- **Bug CSCvr51157** - UCSM 4.0.4 - SFTP-Sicherung fehlschlägt mit Fehler in der **libcrypto-**Nachricht.
- **Bug CSCvs62849** - Der UCSM-Sicherungsvorgang schlägt mit **falscher Signatur** und Die aktuelle Problemumgehung besteht darin, die Federal Information Processing Standards (FIPS) über das Debug-Plugin zu deaktivieren.
- Bug CSCvt27613 - UCS-FI-6454-U mit Firmware 4.1(1a) Schlüsselaustauschalgorithmus diffie-hellman-group16-sha512.
- **Versionshinweise für UCSM 4.0**
- **Technischer Support und Dokumentation - Cisco Systems**