Probleemoplossing voor SCP en SFTP-back-ups na upgrade op UCSM 4.0 firmware

Inhoud

Inleiding

Dit document beschrijft hoe u een probleem met betrekking tot mislukte geplande of on-demand back-upbewerkingen op Unified Computing System Manager (UCSM) kunt oplossen na een upgrade naar 4.0.2a.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- UCS Manager
- SCP (Secure Kopie Protocol) of SFTP (Secure File Transfer Protocol)

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Probleem

Na een upgrade op versie 4.0(2a) of later kunnen back-ups niet langer aan UCSM werken.

Een soortgelijke fout is zichtbaar

```
[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.#
```

Met de release van Cisco UCS Manager 4.0(2a) en later worden bepaalde onveilige telefoons geblokkeerd door UCS Fabric Interconnect. Om in te loggen op servers via het beveiligde protocol, moet u een versie van OpenSSH gebruiken die minimaal één algoritme ondersteunt in elk van de drie categorieën:

- Toetsuitwisselingsalgoritmen

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

- Encryptiealgoritmen

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

- MAC-algoritmen

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

Opmerking: *Raadpleeg* release Notes UCSM 4.0

Het back-uphulpprogramma of de server in gebruik kan de nieuwe OpenSSH-vereisten voor UCS niet ondersteunen wanneer het overdrachtprotocol Secure Shell (SSH), SFTP of SCP is. Daarom is de verbinding geblokkeerd, en de back-up mislukt.

Probleemoplossing voor back-up naar SFTP of SCP-fout na upgrade naar 4.0.2a UCSM

Stap 1. Software voor upgrade-versie van Poetin, SFTP-server, SCP-server of een ander derdengereedschap.

Stap 2. Controleer dat het gebruikte beveiligde gereedschap de vereiste algoritmen ondersteunt zoals met Cisco UCS Manager release 4.0(2a), dat bepaalde onveilige tekens worden geblokkeerd door UCS Fabric Interconnect. Om in te loggen op servers via een beveiligd protocol, moet u een versie van OpenSSH gebruiken die minimaal één algoritme in elk van de drie categorieën ondersteunt:

- Toetsuitwisselingsalgoritmen

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

- Encryptiealgoritmen

```
 aes128-ctr
```

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

- MAC-algoritmen

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

Stap 3. Neem indien nodig contact op met Cisco TAC om de oplossing verder te ondersteunen.

Gerelateerde informatie

- CSCvr5157 - UCSM 4.0.4 - SFTP-back-up faalt bij fout in het bericht **libcrypto**.
- CSCvs62849 voor bugs - De UCS back-up-operatie heeft geen **onjuiste handtekening** en de de huidige tijdelijke oplossing is om Federal Information Processing Standards (FIPS) uit te schakelen via de debug plug-in.
- CSCvt27613 - UCS-FI-6454-U met firmware 4.1(1a) algoritme voor uitwisseling van algoritme diffie-hellman-group16-sha512.
- Release Notes UCSM 4.0
- Technische ondersteuning en documentatie – Cisco Systems