Troubleshoot SCP and SFTP Backups Fail After Upgrade to UCSM 4.0 Firmware

Contents

Introduction

This document describes how to troubleshoot an issue related to failed scheduled or on-demand backup operations in Unified Computing System Manager (UCSM) after a firmware upgrade to 4.0.2a.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

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

Components Used

This document is not restricted to specific software and hardware versions.

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. If your network is live, ensure that you understand the potential impact of any command.

Problem

After a firmware upgrade to version 4.0(2a) or later, backups can no longer work on UCSM.

A similar error can be seen

```
[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.#
```

With Cisco UCS Manager 4.0(2a) release and later, certain insecure ciphers are blocked by UCS Fabric Interconnects. In order to log in to servers through the secure protocol, you must use a version of OpenSSH that supports at least one algorithm in each of the three categories:

- Key exchange algorithms

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

- Encryption algorithms

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

- MAC algorithms

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

Note: *Refer to* Release Notes UCSM 4.0

The backup utility or server in use can not support the new OpenSSH requirements for UCS when the transfer protocol is Secure Shell (SSH), SFTP or SCP. Therefore, the connection is blocked, and the backup fails.

Troubleshoot Backup to SFTP or SCP Failure After Upgrade to 4.0.2a UCSM

Step 1. Upgrade software version of Putty, SFTP Server, SCP Server or other third party tool.

Step 2. Confirm that the secure tool used supports the required algorithms as with Cisco UCS Manager Release 4.0(2a), certain insecure ciphers are blocked by UCS Fabric Interconnects. To log in to servers through a secure protocol, you must use a version of OpenSSH that supports at least one algorithm in each of the three categories:

- Key exchange algorithms

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

- Encryption algorithms

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

- MAC algorithms

```
hmac-sha2-256
```

`hmac-sha2-512`

Step 3. Contract Cisco TAC to troubleshoot further if needed.

Related Information

- **Bug CSCvr51157** - UCSM 4.0.4 - SFTP back up fails with error in **libcrypto** message.
- **Bug CSCvs62849** - UCSM backup operation fails with **incorrect signature** and the current workaround is to disable Federal Information Processing Standards (FIPS) via the debug plugin.
- Bug CSCvt27613 - UCS-FI-6454-U with firmware 4.1(1a) key exchange algorithm error diffie-hellman-group16-sha512.
- **Release Notes UCSM 4.0**
- **Technical Support & Documentation - Cisco Systems**