SCP和SFTP备份在升级到UCSM 4.0固件后失败故障排除

目录

简介

本文档介绍在固件升级到4.0.2a后如何对Unified Computing System Manager(UCSM)中计划备份或按需备份操作失败的问题进行故障排除。

先决条件

要求

Cisco 建议您了解以下主题：

- UCS 管理器
- SCP（安全复制协议）或SFTP（安全文件传输协议）

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

问题

固件升级到4.0(2a)或更高版本后，备份在UCSM上不再有效。

可以看到类似错误

```
[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.#
```

使用Cisco UCS Manager 4.0(2a)版及更高版本时，某些不安全的密码会被UCS交换矩阵互联阻止。要通过安全协议登录服务器，必须使用OpenSSH版本，该版本在以下三个类别中至少支持一种算法：

- 密钥交换算法

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

- 加密算法

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

- MAC算法

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

注意： *请参阅*版本说明UCSM 4.0

当传输协议为Secure Shell(SSH)、SFTP或SCP时，正在使用的备份实用程序或服务器无法支持UCS的新OpenSSH要求。因此，连接被阻止，备份失败。

升级到4.0.2a UCSM后，对备份到SFTP或SCP故障进行故障排除

步骤1：升级软件版本的Putty、SFTP服务器、SCP服务器或其他第三方工具。

步骤2.确认使用的安全工具支持所需的算法，如Cisco UCS Manager版本4.0(2a)一样，某些不安全的密码被UCS交换矩阵互联阻止。要通过安全协议登录到服务器，必须使用OpenSSH版本，该版本在以下三个类别中至少支持一种算法：

- 密钥交换算法

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

- 加密算法

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

- MAC算法

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

步骤3.根据需要，与Cisco TAC签订合同以进一步排除故障。

相关信息

- **错误CSCvr51157** - UCSM 4.0.4 - SFTP备份失败，libcrypto消息**中出**错。
- **漏洞CSCvs62849** - UCSM备份操作失败，**签名不正**确， 当前的解决方法是通过调试插件禁用联邦信息处理标准(FIPS)。
- 错误CSCvt27613 - UCS-FI-6454-U，带固件4.1(1a)密钥交换算法错误diffie-hellman-group16-sha512。
- **版本说明UCSM 4.0**
- **技术支持和文档 - Cisco Systems**