

Falha na solução de problemas de backups de SCP e SFTP após a atualização para o firmware UCSM 4.0

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Problema](#)

[Solução de problemas de backup em falhas de SFTP ou SCP após atualização para UCSM 4.0.2a](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve como solucionar um problema relacionado a operações de backup com falha programadas ou sob demanda no Unified Computing System Manager (UCSM) após uma atualização de firmware para 4.0.2a.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

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

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Problema

Após uma atualização do firmware para a versão 4.0(2a) ou posterior, os backups não podem mais funcionar no UCSM.

Um erro semelhante pode ser visto

```
[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.#
```

Com a versão 4.0(2a) do Cisco UCS Manager e posterior, algumas cifras inseguras são bloqueadas pelas interconexões em malha do UCS. Para fazer login nos servidores através do protocolo seguro, você deve usar uma versão do OpenSSH que suporte pelo menos um algoritmo em cada uma das três categorias:

- Algoritmos de troca de chaves

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

- Algoritmos de criptografia

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

- Algoritmos MAC

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

Note: Consulte as [Notas de Versão do UCSM 4.0](#)

O utilitário ou servidor de backup em uso não pode suportar os novos requisitos do OpenSSH para UCS quando o protocolo de transferência é Secure Shell (SSH), SFTP ou SCP. Portanto, a conexão é bloqueada e o backup falha.

Solução de problemas de backup em falhas de SFTP ou SCP após atualização para UCSM 4.0.2a

Etapa 1. Atualize a versão de software do Putty, SFTP Server, SCP Server ou outra ferramenta de terceiros.

Etapa 2. Confirme se a ferramenta segura usada oferece suporte aos algoritmos necessários, como no Cisco UCS Manager Release 4.0(2a), algumas cifras inseguras são bloqueadas pelas interconexões em malha do UCS. Para fazer login nos servidores por meio de um protocolo seguro, você deve usar uma versão do OpenSSH que suporte pelo menos um algoritmo em cada uma das três categorias:

- Algoritmos de troca de chaves

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

- Algoritmos de criptografia

aes128-ctr
aes192-ctr
aes256-ctr

- Algoritmos MAC

hmac-sha2-256
hmac-sha2-512

Etapa 3. Entre em contato com o TAC da Cisco para solucionar problemas ainda mais, se necessário.

Informações Relacionadas

- [Erro CSCvr51157](#) - UCSM 4.0.4 - O backup do SFTP falha com erro na mensagem `libcrypto`.
- [Erro CSCvs62849](#) - falha na operação de backup UCSM com **assinatura incorreta** e a solução atual é desabilitar o FIPS (Federal Information Processing Standards) por meio do plug-in de depuração.
- [Erro CSCvt27613](#) - UCS-FI-6454-U com firmware 4.1(1a) key exchange algorithm error diffie-hellman-group16-sha512.
- [Notas da versão UCSM 4.0](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)