Échec du dépannage des sauvegardes SCP et SFTP après la mise à niveau vers le microprogramme UCSM 4.0

Contenu

Introduction

Ce document décrit comment dépanner un problème lié aux opérations de sauvegarde planifiées ou à la demande ayant échoué dans Unified Computing System Manager (UCSM) après une mise à niveau du micrologiciel vers la version 4.0.2a.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Problème

Après une mise à niveau du micrologiciel vers la version 4.0(2a) ou ultérieure, les sauvegardes ne peuvent plus fonctionner sur UCSM.

Une erreur similaire s'affiche

```
[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.#
```

Avec la version 4.0(2a) de Cisco UCS Manager et les versions ultérieures, certains chiffrement non sécurisés sont bloqués par les interconnexions de fabric UCS. Pour vous connecter aux serveurs via le protocole sécurisé, vous devez utiliser une version d'OpenSSH qui prend en charge au moins un algorithme dans chacune des trois catégories :

- Algorithmes d'échange de clés

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

- Algorithmes de chiffrement

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

- Algorithmes MAC

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

Note: *Reportez-vous aux* notes de version UCSM 4.0

L'utilitaire de sauvegarde ou le serveur utilisé ne peut pas prendre en charge les nouvelles exigences OpenSSH pour UCS lorsque le protocole de transfert est Secure Shell (SSH), SFTP ou SCP. Par conséquent, la connexion est bloquée et la sauvegarde échoue.

Dépannage de la sauvegarde sur SFTP ou SCP après la mise à niveau vers UCSM 4.0.2a

Étape 1. Mise à niveau de la version logicielle de Putty, SFTP Server, SCP Server ou d'un autre outil tiers.

Étape 2. Vérifiez que l'outil sécurisé utilisé prend en charge les algorithmes requis, comme avec Cisco UCS Manager version 4.0(2a), certains chiffrement non sécurisés sont bloqués par les interconnexions de fabric UCS. Pour vous connecter aux serveurs via un protocole sécurisé, vous devez utiliser une version d'OpenSSH qui prend en charge au moins un algorithme dans chacune des trois catégories :

- Algorithmes d'échange de clés

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

- Algorithmes de chiffrement

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

- Algorithmes MAC

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

Étape 3. Adressez un contrat au centre d'assistance technique de Cisco pour résoudre les problèmes supplémentaires si nécessaire.

Informations connexes

- Bogue CSCvr51157 - UCSM 4.0.4 - La sauvegarde SFTP échoue avec une erreur dans le message **libcrypto**.
- Bogue CSCvs62849 - L'opération de sauvegarde UCSM échoue avec une **signature incorrecte** et la solution de contournement actuelle consiste à désactiver les normes de traitement de l'information fédérale (FIPS) via le plug-in de débogage.
- Bogue CSCvt27613 - UCS-FI-6454-U avec microprogramme 4.1(1a), algorithme d'échange de clés erreur diffie-hellman-group16-sha512.
- Notes de version UCSM 4.0
- Support et documentation techniques - Cisco Systems