Fehlerbehebung bei UCS Central-Backup-Fehlern aufgrund von SSH-Host-Schlüsselkonflikten

Inhalt

Einführung:

Voraussetzungen

- Anforderungen:
- Verwendete Komponenten

Problemaussage:

Lösung:

Einführung:

In diesem Dokument wird die Fehlerbehebung bei UCS Central-Backup-Fehlern beschrieben, die durch eine Nichtübereinstimmung des SSH-Hostschlüssels in UCS Central Version 2.0 und höher verursacht wurden.

Voraussetzungen

Anforderungen:

In diesem Dokument wird davon ausgegangen, dass Sie mit den folgenden Themen vertraut sind:

- Cisco UCS Central
- Grundlegendes Verständnis von Linux-Befehlen.

Verwendete Komponenten

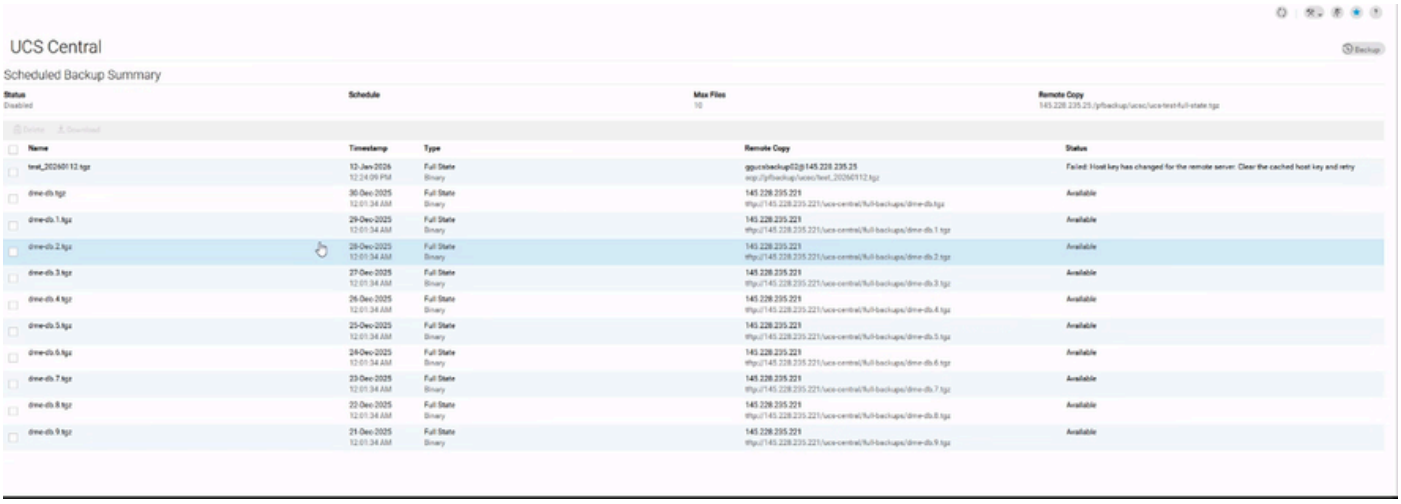
- UCS Central Version 2.1(1a)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Problemaussage:

Die UCS Central-Sicherungsvorgänge schlagen fehl, und auf der Registerkarte "Status" wird folgende Fehlermeldung angezeigt:

“Host key has changed for the remote server. Clear the cached host key and retry.”



Protokollnachweis:

```
# From svc_ops_dme.log:

Jan 6 11:36:47 degtlue2100 svc_ops_dme[1597]: [EVENT][E14194351][79965][transition][internal][] [FSM:STA
Jan 6 11:36:47 degtlue2100 svc_ops_dme[1597]: [EVENT][E14194351][79966][transition][internal][] [FSM:STA
Jan 6 11:36:47 degtlue2100 svc_ops_dme[1597]: [EVENT][E14194351][79968][transition][internal][] [FSM:STA
Jan 6 11:36:47 degtlue2100 svc_ops_dme[1597]: [EVENT][E14194351][79970][transition][internal][] [FSM:STA
```

Lösung:

1. Einrichten einer SSH-Sitzung mit dem UCS Central-System

2. Überprüfen Sie die installierte Version des UCS Central-Pakets.

```
Central-HTTS1# connect local-mgmt
Cisco UCS Central
TAC support: http://www.cisco.com/tac
Copyright (c) 2011-2025, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or later version. A copy of each
such license is available at
https://opensource.org/license/gpl-2-0 and
https://opensource.org/license/lgpl-2-1
```

```
Central-HTTS1(local-mgmt)# show version

Name                Package             Version        GUI
----                -------             -------        ----
core                Base System         2.1(1a)        2.1(1a)
central-mgr         Central Manager     2.1(1a)        2.1(1a)
service-reg         Service Registry    2.1(1a)        2.1(1a)
identifier-mgr      Identifier Manager  2.1(1a)        2.1(1a)
operation-mgr       Operations Manager  2.1(1a)        2.1(1a)
resource-mgr        Resource Manager    2.1(1a)        2.1(1a)
policy-mgr          Policy Manager      2.1(1a)        2.1(1a)
stats-mgr           Statistics Manager  2.1(1a)        2.1(1a)
server-mgr          Server Manager      2.1(1a)        2.1(1a)
gch                 Generic Call Home   2.1(1a)        none
rel-key             Release Key         2.1(1a)        none

Central-HTTS1(local-mgmt)#
```

3. Rufen Sie das Token vom zentralen Server ab.

Anmerkung: Dies ändert sich alle 10 Minuten.

```
Central-HTTS1(local-mgmt)# show token

OHPPCXXYGVR
```

* Verwenden Sie das Token im Antwortschlüsselgenerator: https://cspg-releng.cisco.com/UCSPassGen.php

Anmerkung: Wählen Sie zunächst Ihre UCSC-Version aus. (2.0 oder 2.1). Andernfalls funktioniert das Kennwort für den Benutzer root nicht. Stellen Sie sicher, dass Sie das Wort "Token" aus dem Feld "Debug-Token" auf der Website zur Kennworterstellung löschen, bevor Sie das von UCS Central erhaltene Token einfügen. Der Text bleibt anders und erzeugt ein ungültiges Passwort.

4. Initiieren Sie eine neue SSH-Sitzung mit UCS Central. Verwenden Sie dabei die Anmeldeinformationen als Root und den Antwortschlüssel als Kennwort.

```
login as: root
root@ <IP Address> password:
Last login: Tue Jan 13 17:57:20 2026 from <IP Address>
```

5. Navigieren Sie zu diesem Pfad, und überprüfen Sie die Datei "known_hosts" für die IP-Adresse des betroffenen Servers:

```
[root@Central-HTTS1 ~]# cd /root/.ssh
[root@Central-HTTS1 .ssh]# cat known_hosts

[root@Central-HTTS1 ~]# cd /root/
anaconda-ks.cfg  .bash_profile    .cshrc           ks-pre.log       .ssh/
.bash_history    .bashrc          ks-post1.log     opt/             .tcshrc
.bash_logout     .config/         ks-post.log      original-ks.cfg  .viminfo

[root@Central-HTTS1 ~]# cd /root/.ssh/
[root@Central-HTTS1 .ssh]# ls
id_rsa  id_rsa.pub  known_hosts

[root@Central-HTTS1 .ssh]# cat known_hosts
```

Wenn die IP-Adresse des betroffenen Servers in der Datei vorhanden ist, entfernen Sie den entsprechenden Eintrag manuell mithilfe des vim-Editors.

Navigieren Sie zur entsprechenden Zeile, und löschen Sie sie, indem Sie "dd" eingeben.

```
[root@Central-HTTS1 .ssh]# vi known_hosts
```

```
[root@Central-HTTS1 .ssh]# vi known_hosts
....
....
....
!wq     (Write and Quit  >> Saving changes and exiting)
```

Nachdem Sie die betroffene IP-Adresse entfernt haben, speichern Sie die Datei, und beenden Sie den Editor mit :wq.

Wenn die Datei known_hosts aktualisiert wurde, wiederholen Sie den Sicherungsvorgang von UCS Central aus.

Die Sicherung wird dieses Mal erfolgreich abgeschlossen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.