Problemen met UCS Central Backup oplossen vanwege een verkeerde SSH-hostsleutel

Inhoud

Inleiding:

In dit document wordt beschreven hoe u problemen met UCS Central-back-ups kunt oplossen die worden veroorzaakt door een fout in de SSH-hostsleutel in UCS Central versie 2.0 en hoger.

Voorwaarden

Vereisten:

In dit document wordt ervan uitgegaan dat u kennis heeft van deze onderwerpen:

- Cisco UCS Central
- Basiskennis van Linux-opdrachten.

Gebruikte componenten

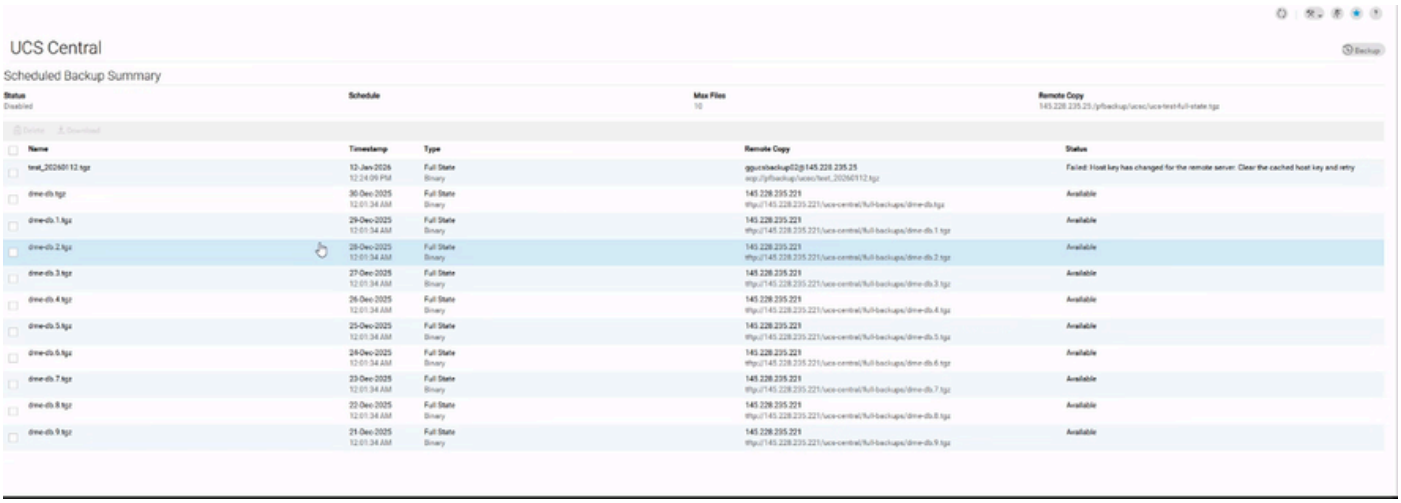
- UCS Central versie 2.1(1a)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Probleemverklaring:

De centrale back-upbewerkingen van UCS zijn mislukt en op het tabblad Status wordt dit foutbericht weergegeven:

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



Logboekbewijs:

```
# 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
```

Oplossing:

1. Stel een SSH-sessie in voor het centrale UCS-systeem.

2. Controleer de geïnstalleerde versie van het UCS Central-pakket.

```
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. Haal het token van de centrale server.

Let op: dit verandert elke 10 minuten.

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

0HPPCXXYGVR
```

* Gebruik de token op de antwoordsleutelgenerator: https://cspg-releng.cisco.com/UCSPassGen.php

Let op: Kies eerst uw UCSC-versie. (2,0 of 2,1). Anders werkt het wachtwoord niet voor root-gebruikers. Zorg ervoor dat u het woord "token" verwijdert uit het veld Debug-Token op de website voor het genereren van wachtwoorden voordat u het token plakt dat u van UCS Central hebt verkregen. De tekst blijft anders en genereert een ongeldig wachtwoord.

4. Start een nieuwe SSH-sessie naar UCS Central met rootreferenties en de reactiesleutel als wachtwoord.

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

5. Navigeer naar dit pad en controleer het bestand 'known_hosts' voor het IP-adres van de betreffende server:

```
[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
```

Als het IP-adres van de getroffen server in het bestand aanwezig is, verwijdert u handmatig de bijbehorende vermelding met behulp van de 'vim'-editor.

Navigeer naar de specifieke regel en verwijder deze door 'dd' te typen.

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

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

Nadat u het getroffen IP-adres hebt verwijderd, slaat u het bestand op en sluit u de editor af met :wq.

Zodra het bestand known_hosts is bijgewerkt, probeert u de back-upbewerking vanuit UCS Central opnieuw.

De back-up wordt deze keer met succes voltooid.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.