

# Resolución de problemas de errores de UCS Central Backup debido a discordancia de clave de host SSH

## Contenido

---

[Introducción:](#)

[Prerequisites](#)

[Requerimientos:](#)

[Componentes Utilizados](#)

[Declaración de problema:](#)

[Solución:](#)

---

## Introducción:

Este documento describe cómo resolver problemas de fallas de respaldo de UCS Central causadas por una discordancia de clave de host SSH en UCS Central versión 2.0 y posteriores.

## Prerequisites

### Requerimientos:

Este documento supone que usted tiene conocimiento de estos temas:

- Cisco UCS Central
- Comprensión básica del comando Linux.

### Componentes Utilizados

- UCS Central versión 2.1(1a)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Declaración de problema:

Las operaciones de copia de seguridad de UCS Central fallan y la ficha Estado muestra este mensaje de error:

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

UCS Central

Scheduled Backup Summary

| Status              | Schedule                   | Miss Files           | Remote Copy                                                                     |                                                                                         |
|---------------------|----------------------------|----------------------|---------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| Disabled            |                            | 10                   | 145.228.235.221:/backup/ucsc/ucsc-test/full-state.tgz                           |                                                                                         |
| <div>Download</div> |                            |                      |                                                                                 |                                                                                         |
| Name                | Timestamp                  | Type                 | Remote Copy                                                                     | Status                                                                                  |
| test_2020112.tgz    | 12-Jan-2026<br>12:24:09 PM | Full State<br>Binary | gpus-backup02@145.228.235.25<br>wp:/backup/ucsc/test_2020112.tgz                | Failed: Host key has changed for the remote server. Clear the cached host key and retry |
| dme-ds.tgz          | 30-Dec-2025<br>12:01:34 AM | Full State<br>Binary | 145.228.235.221<br>ftp://145.228.235.221/ucsc-central/full-backups/dme-ds.tgz   | Available                                                                               |
| dme-ds.1.tgz        | 29-Dec-2025<br>12:01:34 AM | Full State<br>Binary | 145.228.235.221<br>ftp://145.228.235.221/ucsc-central/full-backups/dme-ds.1.tgz | Available                                                                               |
| dme-ds.2.tgz        | 28-Dec-2025<br>12:01:34 AM | Full State<br>Binary | 145.228.235.221<br>ftp://145.228.235.221/ucsc-central/full-backups/dme-ds.2.tgz | Available                                                                               |
| dme-ds.3.tgz        | 27-Dec-2025<br>12:01:34 AM | Full State<br>Binary | 145.228.235.221<br>ftp://145.228.235.221/ucsc-central/full-backups/dme-ds.3.tgz | Available                                                                               |
| dme-ds.4.tgz        | 26-Dec-2025<br>12:01:34 AM | Full State<br>Binary | 145.228.235.221<br>ftp://145.228.235.221/ucsc-central/full-backups/dme-ds.4.tgz | Available                                                                               |
| dme-ds.5.tgz        | 25-Dec-2025<br>12:01:34 AM | Full State<br>Binary | 145.228.235.221<br>ftp://145.228.235.221/ucsc-central/full-backups/dme-ds.5.tgz | Available                                                                               |
| dme-ds.6.tgz        | 24-Dec-2025<br>12:01:34 AM | Full State<br>Binary | 145.228.235.221<br>ftp://145.228.235.221/ucsc-central/full-backups/dme-ds.6.tgz | Available                                                                               |
| dme-ds.7.tgz        | 23-Dec-2025<br>12:01:34 AM | Full State<br>Binary | 145.228.235.221<br>ftp://145.228.235.221/ucsc-central/full-backups/dme-ds.7.tgz | Available                                                                               |
| dme-ds.8.tgz        | 22-Dec-2025<br>12:01:34 AM | Full State<br>Binary | 145.228.235.221<br>ftp://145.228.235.221/ucsc-central/full-backups/dme-ds.8.tgz | Available                                                                               |
| dme-ds.9.tgz        | 21-Dec-2025<br>12:01:34 AM | Full State<br>Binary | 145.228.235.221<br>ftp://145.228.235.221/ucsc-central/full-backups/dme-ds.9.tgz | Available                                                                               |

Prueba de registro:

# From svc\_ops\_dme.log:

Jan 6 11:36:47 degtlue2100 svc\_ops\_dme[1597]: [EVENT][E14194351][79965][transition][internal][] [FSM:ST  
Jan 6 11:36:47 degtlue2100 svc\_ops\_dme[1597]: [EVENT][E14194351][79966][transition][internal][] [FSM:ST  
Jan 6 11:36:47 degtlue2100 svc\_ops\_dme[1597]: [EVENT][E14194351][79968][transition][internal][] [FSM:ST  
Jan 6 11:36:47 degtlue2100 svc\_ops\_dme[1597]: [EVENT][E14194351][79970][transition][internal][] [FSM:ST

## Solución:

1. Establezca una sesión SSH para el sistema UCS Central.
2. Compruebe la versión instalada del paquete de UCS Central.

Central-HTTPS1# 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-HTTPS1(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-HTTPS1(local-mgmt)#

### 3. Obtenga el token del servidor central.



Nota: Esto cambia cada 10 minutos.

Central-HTTPS1(local-mgmt)# show token

0HPPCXYGVR

\* Utilice el token en el generador de claves de respuesta: <https://cspg-releng.cisco.com/UCSPassGen.php>



Nota: Elija primero su versión de UCSC. (2.0 o 2.1). De lo contrario, la contraseña no funcionará para el usuario raíz. Asegúrese de eliminar la palabra "token" del campo Debug-Token del sitio web de generación de contraseñas antes de pegar el token obtenido de UCS Central. El texto permanece en otro lugar y genera una contraseña no válida.

### 4. Inicie una nueva sesión SSH en UCS Central con las credenciales raíz y la clave de respuesta como contraseña.

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

### 5. Navegue hasta esta ruta y verifique el archivo 'known\_hosts' para la dirección IP del servidor

afectado:

```
[root@Central-HTTPS1 ~]# cd /root/.ssh
[root@Central-HTTPS1 .ssh]# cat known_hosts

[root@Central-HTTPS1 ~]# 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-HTTPS1 ~]# cd /root/.ssh/
[root@Central-HTTPS1 .ssh]# ls
id_rsa  id_rsa.pub  known_hosts

[root@Central-HTTPS1 .ssh]# cat known_hosts
```

Si la dirección IP del servidor afectado está presente en el archivo, elimine manualmente la entrada correspondiente mediante el editor 'vim'.

Desplácese hasta la línea específica y elimínela escribiendo 'dd'.

```
[root@Central-HTTPS1 .ssh]# vi known_hosts

[root@Central-HTTPS1 .ssh]# vi known_hosts
....
....
....
!wq      (Write and Quit >> Saving changes and exiting)
```

Después de quitar la dirección IP afectada, guarde el archivo y salga del editor mediante :wq.

Una vez actualizado el archivo known\_hosts, vuelva a intentar la operación de copia de seguridad desde UCS Central.

Esta vez, la copia de seguridad se completará correctamente.

#### Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).