

由于SSH主机密钥不匹配而导致UCS中心备份失败故障排除

目录

[简介：](#)

[先决条件](#)

[要求:](#)

[使用的组件](#)

[问题陈述：](#)

[解决方案：](#)

简介：

本文档介绍如何排除UCS中心2.0版及更高版本中由SSH主机密钥不匹配导致的UCS中心备份故障。

先决条件

要求:

本文档假定您了解以下主题：

- Cisco UCS中心
- 基本的Linux命令了解。

使用的组件

- UCS中心2.1(1a)版

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

问题陈述：

UCS中心备份操作失败，并且Status选项卡显示以下错误消息：

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

UCS Central

Scheduled Backup Summary

Status	Schedule	Max Files	Remote Copy	
Disabled		10	145.228.235.221:/pfsbackups/ucs/ucs-test-full-state.tgz	
DetailsDownload				
Name	Timestamp	Type	Remote Copy	Status
test_20240112.tgz	12-Jan-2026 12:24:09 PM	Full State Binary	ggpfsbackups@145.228.235.221 scp:/pfsbackups/ucs/ucs-test_20240112.tgz	Failed: Host key has changed for the remote server. Clear the cached host key and retry
dme-ds.tgz	30-Dec-2025 12:01:34 AM	Full State Binary	145.228.235.221 http://145.228.235.221/ucs-central/full-backups/dme-ds.tgz	Available
dme-ds.1.tgz	29-Dec-2025 12:01:34 AM	Full State Binary	145.228.235.221 http://145.228.235.221/ucs-central/full-backups/dme-ds.1.tgz	Available
dme-ds.2.tgz	28-Dec-2025 12:01:34 AM	Full State Binary	145.228.235.221 http://145.228.235.221/ucs-central/full-backups/dme-ds.2.tgz	Available
dme-ds.3.tgz	27-Dec-2025 12:01:34 AM	Full State Binary	145.228.235.221 http://145.228.235.221/ucs-central/full-backups/dme-ds.3.tgz	Available
dme-ds.4.tgz	26-Dec-2025 12:01:34 AM	Full State Binary	145.228.235.221 http://145.228.235.221/ucs-central/full-backups/dme-ds.4.tgz	Available
dme-ds.5.tgz	25-Dec-2025 12:01:34 AM	Full State Binary	145.228.235.221 http://145.228.235.221/ucs-central/full-backups/dme-ds.5.tgz	Available
dme-ds.6.tgz	24-Dec-2025 12:01:34 AM	Full State Binary	145.228.235.221 http://145.228.235.221/ucs-central/full-backups/dme-ds.6.tgz	Available
dme-ds.7.tgz	23-Dec-2025 12:01:34 AM	Full State Binary	145.228.235.221 http://145.228.235.221/ucs-central/full-backups/dme-ds.7.tgz	Available
dme-ds.8.tgz	22-Dec-2025 12:01:34 AM	Full State Binary	145.228.235.221 http://145.228.235.221/ucs-central/full-backups/dme-ds.8.tgz	Available
dme-ds.9.tgz	21-Dec-2025 12:01:34 AM	Full State Binary	145.228.235.221 http://145.228.235.221/ucs-central/full-backups/dme-ds.9.tgz	Available

日志证据：

```
# 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
```

解决方案：

- 1. 建立到UCS中心系统的SSH会话。
- 2.验证已安装的UCS中心软件包版本。

```
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-HTTPS1(local-mgmt)#
```

3.从中央服务器获取令牌。



注意：每10分钟更改一次。

```
Central-HTTPS1(local-mgmt)# show token
```

```
0HPPCXYGVR
```

*使用响应密钥生成器上的令牌：<https://cspg-releng.cisco.com/UCSPassGen.php>



注意：首先选择您的UCSC版本。(2.0或2.1)。否则，根用户将无法使用密码。在粘贴从UCS中心获取的令牌之前，请确保从密码生成网站上的Debug-Token字段中删除“token”一词。文本将保持其他状态，并生成无效密码。

4.使用根凭证和响应密钥作为密码，启动到UCS中心的新SSH会话。

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

5.导航到此路径，并检查“known_hosts”文件以查找受影响服务器的IP地址：

```
[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
```

如果文件中存在受影响服务器的IP地址，请使用“vim”编辑器手动删除相应的条目。

导航到特定行，然后键入“dd”将其删除。

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

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

删除受影响的IP地址后，使用：wq保存文件并退出编辑器。

更新known_hosts文件后，请再次从UCS中心重试备份操作。

然后，这次备份成功完成。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。