

Solucionar falhas de backup do UCS Central devido à incompatibilidade da chave do host SSH

Contents

[Introdução:](#)

[Pré-requisitos](#)

[Requisitos:](#)

[Componentes Utilizados](#)

[Instrução do problema:](#)

[Solução:](#)

Introdução:

Este documento descreve como solucionar problemas de falhas de backup do UCS Central causadas por uma incompatibilidade de chave de host SSH no UCS Central versão 2.0 e posterior.

Pré-requisitos

Requisitos:

Este documento pressupõe que você tenha conhecimento destes tópicos:

- Cisco UCS Central
- Compreensão básica dos comandos do Linux.

Componentes Utilizados

- UCS Central versão 2.1(1a)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Instrução do problema:

As operações de backup do UCS Central falham, e a guia Status exibe esta mensagem de erro:

“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:/backups/ucsc/ucsc-test/full-state.tgz	
<div>Download</div>				
Name	Timestamp	Type	Remote Copy	Status
test_20260112.tgz	12-Jan-2026 12:24:09 PM	Full State Binary	gpus-backup02@145.228.235.221 wp:/backups/ucsc/test_20260112.tgz	Failed: Host key has changed for the remote server. Clear the cached host key and retry
dme-ds.tgz	26-Dec-2025 12:01:34 AM	Full State Binary	145.228.235.221 wp:/145.228.235.221/ucsc-central/full-backups/dme-ds.tgz	Available
dme-ds.1.tgz	26-Dec-2025 12:01:34 AM	Full State Binary	145.228.235.221 wp:/145.228.235.221/ucsc-central/full-backups/dme-ds.1.tgz	Available
dme-ds.2.tgz	26-Dec-2025 12:01:34 AM	Full State Binary	145.228.235.221 wp:/145.228.235.221/ucsc-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 wp:/145.228.235.221/ucsc-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 wp:/145.228.235.221/ucsc-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 wp:/145.228.235.221/ucsc-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 wp:/145.228.235.221/ucsc-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 wp:/145.228.235.221/ucsc-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 wp:/145.228.235.221/ucsc-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 wp:/145.228.235.221/ucsc-central/full-backups/dme-ds.9.tgz	Available

Log de Evidência:

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

Solução:

- 1. Estabeleça uma sessão SSH para o sistema UCS Central.
- 2. Verifique a versão instalada do pacote do 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. Obtenha o token do servidor Central.



Note: Isso muda a cada 10 minutos.

Central-HTTPS1(local-mgmt)# show token

0HPPCXYGVR

* Use o token no gerador de chave de resposta: <https://cspg-releng.cisco.com/UCSPassGen.php>



Note: Escolha a versão do UCSC primeiro. (2.0 ou 2.1). Caso contrário, a senha não funcionará para o usuário root. Certifique-se de excluir a palavra "token" do campo Debug-Token no site de geração de senha antes de colar o token obtido no UCS Central. O texto permanece de outra forma e gera uma senha inválida.

4. Inicie uma nova sessão SSH para o UCS Central usando as credenciais raiz e a chave de resposta como a senha.

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

5. Navegue até esse caminho e verifique o arquivo 'known_hosts' para obter o endereço IP do servidor afetado:

```
[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
```

Se o endereço IP do servidor afetado estiver presente no arquivo, remova manualmente a entrada correspondente usando o editor 'vim'.

Navegue até a linha específica e exclua-a digitando 'dd'.

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

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

Após remover o endereço IP afetado, salve o arquivo e saia do editor usando :wq.

Depois que o arquivo known_hosts for atualizado, repita a operação de backup do UCS Central novamente.

O backup é concluído com êxito desta vez.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.