

Risoluzione dei problemi di backup di UCS Central a causa di una mancata corrispondenza della chiave host SSH

Sommario

[Introduzione:](#)

[Prerequisiti](#)

[Requisiti:](#)

[Componenti usati](#)

[Problema:](#)

[Soluzione:](#)

Introduzione:

In questo documento viene descritto come risolvere gli errori di backup di UCS Central causati da una mancata corrispondenza della chiave host SSH in UCS Central versione 2.0 e successive.

Prerequisiti

Requisiti:

In questo documento si presume che l'utente abbia conoscenza dei seguenti argomenti:

- Cisco UCS Central
- Comandi Linux di base.

Componenti usati

- UCS Central versione 2.1(1a)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Problema:

Le operazioni di backup di UCS Central non riescono e nella scheda Stato viene visualizzato questo messaggio di errore:

“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:/backup/ucsc/ucsc-test/full-state.tgz	
<div>📁 Select 📄 Download</div>				
<input type="checkbox"/> Name	Timestamp	Type	Remote Copy	Status
<input type="checkbox"/> test_20260112.tgz	12-Jan-2026 12:24:09 PM	Full State Binary	gpus-backup10@145.228.235.221 wp:/backup/ucsc/test_20260112.tgz	Failed: Host key has changed for the remote server. Clear the cached host key and retry
<input type="checkbox"/> dme-ds.tgz	20-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
<input type="checkbox"/> dme-ds.1.tgz	20-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
<input type="checkbox"/> dme-ds.2.tgz	20-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
<input type="checkbox"/> 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
<input type="checkbox"/> 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
<input type="checkbox"/> 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
<input type="checkbox"/> 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
<input type="checkbox"/> 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
<input type="checkbox"/> 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
<input type="checkbox"/> 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

Registra evidenza:

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

Soluzione:

1. Stabilire una sessione SSH con il sistema UCS Central.
2. Verificare la versione installata del pacchetto 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. Ottenere il token dal server centrale.



Nota: Questo cambia ogni 10 minuti.

Central-HTTPS1(local-mgmt)# show token

0HPPCXYGVR

* Utilizzare il token sul generatore di tasti di risposta: <https://cspg-releng.cisco.com/UCSPassGen.php>



Nota: Scegliere prima la versione UCS. (2.0 o 2.1). In caso contrario, la password non funziona per l'utente root. Prima di incollare il token ottenuto da UCS Central, accertarsi di eliminare la parola "token" dal campo Debug-Token sul sito Web di generazione della password. In caso contrario il testo rimane e viene generata una password non valida.

4. Avviare una nuova sessione SSH su UCS Central usando le credenziali della radice e la chiave di risposta come password.

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

5. Passare a questo percorso e controllare il file 'known_hosts' per l'indirizzo IP del server

interessato:

```
[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 l'indirizzo IP del server interessato è presente nel file, rimuovere manualmente la voce corrispondente utilizzando l'editor 'vim'.

Passare alla riga specifica ed eliminarla digitando 'aggiungi'.

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

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

Dopo aver rimosso l'indirizzo IP interessato, salvare il file e uscire dall'editor utilizzando :wq.

Una volta aggiornato il file known_hosts, riprovare l'operazione di backup da UCS Central.

Questa volta il backup viene completato correttamente.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).