

Risoluzione dei problemi di registrazione UCSM con Central

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Metodi di risoluzione dei problemi](#)

[Risoluzione dei problemi di base](#)

[Stato di registrazione bloccato UCSM con Central](#)

[Stato centrale UCSM bloccato in corso dopo l'aggiornamento](#)

[UCSM - Perdita di visibilità con Central](#)

[Registri da controllare](#)

[Difetti noti](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive come risolvere alcuni dei problemi comuni relativi alla registrazione UCSM con UCS Central

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Unified Computing System (UCS)
- UCS Central

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e

hardware:

- Cisco Unified Computing System Manager (UCSM)
- Fabric Interconnect (FI)
- UCS central in esecuzione su VM ESXi

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.

Metodi di risoluzione dei problemi

La risoluzione dei problemi è incentrata sul certificato autofirmato su UCSM e sui certificati centrali e non di terze parti

- Risoluzione problemi di base
- UCSM bloccato durante la registrazione dello stato con il
- Stato centrale UCSM bloccato in corso dopo l'aggiornamento
- UCSM perso-visibilità con centralizzazione
- Registri da controllare
- Comandi per la risoluzione dei problemi

Risoluzione dei problemi di base

Accertarsi che i controlli di base siano stati completati:

- Mancata corrispondenza del segreto condiviso.
- Dispositivo UCS Central non raggiungibile.
- Il GUID di UCS Central è diverso dal GUID di UCS Central già registrato.
- L'ora non è sincronizzata tra UCSM e UCS Central.
- Certificato scaduto in UCSM.
- Il certificato keyring predefinito non è presente. Anche se è possibile utilizzare CA di terze parti per HTTPS. La registrazione UCSM utilizza il certificato keyring predefinito e pertanto non deve essere eliminata.
- Verificare che UCSM riceva la richiesta di handshake da UCSC.

```
Central# connect local-mgmt  
Central(local-mgmt)# test ucsm-connectivity <ucsm_ip>
```

Acquisizione pacchetto da UCSM con registrazione completata con il provider centrale

10.106.74.195	10.106.74.234	TCP	74 43448 → 443 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=233688518 TSecr=0 WS=512
10.106.74.234	10.106.74.195	TCP	74 443 → 43448 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=9552296 TSecr=233688518 WS=128
10.106.74.195	10.106.74.234	TCP	66 43448 → 443 [ACK] Seq=1 Ack=1 Win=6144 Len=0 TSval=233688518 TSecr=9552296
10.106.74.195	10.106.74.234	TLSv1	154 Client Hello
10.106.74.234	10.106.74.195	TCP	66 443 → 43448 [ACK] Seq=1 Ack=89 Win=5888 Len=0 TSval=9552298 TSecr=233688519
10.106.74.234	10.106.74.195	TLSv1	892 Server Hello, Certificate, Server Hello Done
10.106.74.195	10.106.74.234	TCP	66 43448 → 443 [ACK] Seq=89 Ack=827 Win=7680 Len=0 TSval=233688519 TSecr=9552299
10.106.74.195	10.106.74.234	TLSv1	392 Client Key Exchange, Change Cipher Spec, Finished
10.106.74.195	10.106.74.234	TLSv1	125 Change Cipher Spec, Finished
10.106.74.195	10.106.74.234	TLSv1	412 [SSL segment of a reassembled PDU]
10.106.74.234	10.106.74.195	HTTP	119 HTTP/1.1 100 Continue
10.106.74.195	10.106.74.234	HTTP	1196 POST /xmlInternal/apache/cert HTTP/1.1 (application/x-www-form-urlencoded)
10.106.74.234	10.106.74.195	TCP	66 443 → 43448 [ACK] Seq=939 Ack=1891 Win=10240 Len=0 TSval=9552344 TSecr=233688519
10.106.74.195	10.106.74.234	HTTP/X.	1484 HTTP/1.1 200 OK
10.106.74.195	10.106.74.234	TLSv1	103 Alert (Level: Warning, Description: Close Notify)
10.106.74.195	10.106.74.234	TCP	66 43448 → 443 [FIN, ACK] Seq=1928 Ack=2357 Win=10752 Len=0 TSval=233690027 TSecr=9567376
10.106.74.234	10.106.74.195	TCP	66 443 → 43448 [ACK] Seq=2357 Ack=1928 Win=10240 Len=0 TSval=9567377 TSecr=233690027
10.106.74.234	10.106.74.195	TLSv1	103 Alert (Level: Warning, Description: Close Notify)

Source	Destination	Protocol	Length	Info
10.106.74.195	10.106.74.234	HTTP	540	POST /xmlInternal/apache/cert HTTP/1.1 (application/x-www-form-urlencoded)
10.106.74.234	10.106.74.195	HTTP/XML	100	HTTP/1.1 200 OK
10.106.74.234	10.106.74.195	HTTP	119	HTTP/1.1 100 Continue
10.106.74.195	10.106.74.234	HTTP	1196	POST /xmlInternal/apache/cert HTTP/1.1 (application/x-www-form-urlencoded)
10.106.74.234	10.106.74.195	HTTP/XML	1484	HTTP/1.1 200 OK
10.106.74.195	10.106.74.234	HTTP	588	POST /xmlInternal/service-reg/forward HTTP/1.1 (application/x-www-form-urlencoded)
10.106.74.195	10.106.74.234	HTTP	572	POST /xmlInternal/service-reg/forward HTTP/1.1 (application/x-www-form-urlencoded)
10.106.74.195	10.106.74.234	HTTP/XML	780	POST /xmlInternal/service-reg HTTP/1.1
10.106.74.234	10.106.74.194	HTTP/XML	556	POST /xmlInternal/managed-endpoint HTTP/1.1
10.106.74.195	10.106.74.234	HTTP/XML	636	POST /xmlInternal/identifier-mgr HTTP/1.1
10.106.74.195	10.106.74.234	HTTP/XML	684	POST /xmlInternal/operation-mgr HTTP/1.1
10.106.74.195	10.106.74.234	HTTP/XML	428	POST /xmlInternal/stats-mgr HTTP/1.1
10.106.74.234	10.106.74.194	HTTP/XML	716	POST /xmlInternal/managed-endpoint HTTP/1.1
10.106.74.234	10.106.74.194	HTTP/XML	604	POST /xmlInternal/managed-endpoint HTTP/1.1
10.106.74.195	10.106.74.234	HTTP/XML	428	POST /xmlInternal/resource-mgr HTTP/1.1

NON annullare la registrazione della centrale da UCSM. Quando si annulla la registrazione, tutti i profili di servizio globali diventano locali per il dominio UCS. È possibile rendere nuovamente globale un profilo di servizio locale. Si tratta tuttavia di un processo molto complesso che ha un impatto sul servizio.

Stato di registrazione bloccato UCSM con Central

Se UCS Manager è registrato in UCS Central e UCS Manager è in fase di aggiornamento alla versione 3.1.1, UCS Manager passa allo stato di registrazione e rimane bloccato in tale stato.

Troppi errori di curl nei log DME centrali

```
9603: [WARN][0x27699940][Apr  5 18:00:54.714][write:net] write of 3752 bytes using curl failed, code=
9604: [WARN][0x27699940][Apr  5 18:00:54.714][write:net] non-critical curl write error.
```

Da DME UCSM

```
[INFO][0x682ffb90][Nov  1 16:05:24.886][sam_sec:check_cert_val] X509_verify_cert_error_string - ok
[INFO][0x682ffb90][Nov  1 16:05:24.886][sam_sec:X509VerifyCert] ErrorMsg:ok ErrorNo:0
[INFO][0x682ffb90][Nov  1 16:05:24.886][app_sam_dme:processKey] something wrong with KR-default certifi
```

Il problema potrebbe essere dovuto al fatto che UCSM utilizza per i certificati il vecchio hash MD5 anziché SHA1

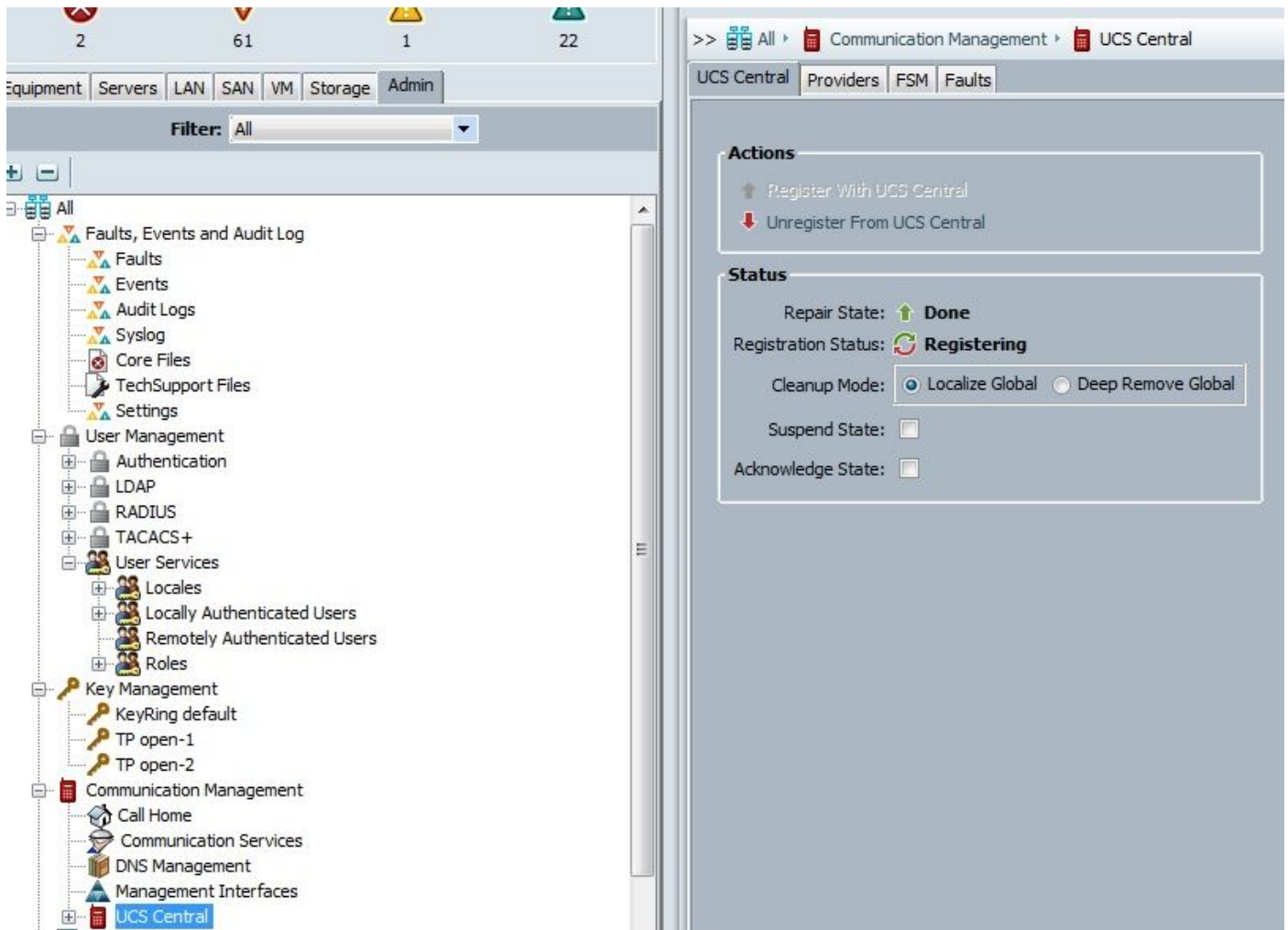
```
[WARN][0x674ffb90][Nov 22 19:11:49.227][net:write] write of 546 bytes using curl failed, code=60, error  
[INFO][0x674ffb90][Nov 22 19:11:49.227][net:certFailure] certificate is bad for connection to ' https://
```

Per risolvere il problema, eseguire le soluzioni indicate di seguito in quanto la registrazione di UCS Manager in UCS Central è riuscita e correggere l'errore del certificato

Il keyring predefinito può essere rigenerato dalla CLI di UCS Central nella sezione del profilo del dispositivo.

```
connect policy-mgr  
  scope org  
  scope device-profile  
  scope security  
  scope keyring default  
  set regenerate yes  
  commit-buffer
```

Se la soluzione non viene risolta, sollevare una richiesta in Cisco TAC per convalidare ulteriormente



Se in qualsiasi momento UCS Manager è stato registrato su UCS Central inizialmente nella versione 2.1.3 o successiva. Durante l'aggiornamento alla versione 3.1.1, il problema di registrazione menzionato è ancora visibile.

Per questo coinvolgimento TAC è necessario come UCS 2.1.3 e versioni precedenti, UCSM non suddivide il certificato. TAC deve rieseguire il reset del certificato in modo da creare i collegamenti software corretti al certificato.

Stato centrale UCSM bloccato in corso dopo l'aggiornamento

Il problema è dovuto a un errore di sincronizzazione del database tra UCS e Central

Questi errori osservati nei registri di gestione risorse

```
[WARN][0xbbce9940][Aug 11 10:23:18.194][storeMo:mit_init] SQL error [SQLParamData failure: Error while  
ERROR: duplicate key value violates unique constraint "InstanceId2DN_dn_key"] stmt [INSERT INTO "Insta
```

```
[INFO][0xbbce9940][Aug 11 10:23:18.194][report:exception_handl] FATAL[3|150] /ramfs/buildsa/150407-1047
[INFO][0xbbce9940][Aug 11 10:23:18.201][report:exception_handl] ERROR[3|150] /ramfs/buildsa/150407-1047
[INFO][0xbbce9940][Aug 11 10:23:18.201][failedCb:tx] TX FAILED
```

Si tratta di un problema di sincronizzazione del database. Sollevare una richiesta in Cisco TAC per convalidare ulteriormente

UCSM - Perdita di visibilità con Central

UCS Central

admin

What are you looking for? Search by name What do you want to do?

Dashboard root root All Domains

All Domains

UCS Central

Filters

Domain Group

- ☐ root
- ☐ Ungrouped

Overall Status

- ☐ Lost Visibility

Fault Level

- ☐ Critical
- ☐ Major
- ☐ Minor

Domain	Hardware	Configuration	Status
DCN-INDIA-FI-A Ungrouped 10.106.74.194	UCS-FI-6248UP Fabric A, B (HA) 1 Chassis 0 FEX 3 Blades 0 Rack Mounts	UCS 6100/6200 Series FI 2.2(6g)A FW Ready	Lost Visibility Fault Level: Critical

Controllare lo stato della registrazione

Se viene visualizzato "lost-visibility", UCS Central non può essere raggiunto su una o più porte richieste. Se UCS Central utilizza la GUI flash (Flex), queste porte devono essere aperte a Central: 443, 80, 843. L'interfaccia grafica HTML richiede solo la porta 443.

Registri da controllare

UCSM

```
/var/sysmgr/sam_logs/pa_setup.log
svc_sam_dme.log files on FI
```

Centrale

Svc_dme_reg.log

Comandi per la risoluzione dei problemi

```
Central# connect policy-mgr
Central# scope org
Central# scope device-profile
Central# scope security
Central# Show keyring detail
```

```
UCSM# scope system
UCSM# scope security
UCSM# show keyring detail
connect local-mgmt
telnet <Central IP> <port>
^ (Shift+6) ] with no spaces to exit
```

```
FSM status
  scope system
  scope control-ep policy
  show fsm status
```

```
Central# connect service-reg
Central(service-reg)# show fault
Central(service-reg)# show clients detail
Registered Clients:
  ID: 1008
  Registered Client IP: 10.106.74.194
  Registered Client IPV6: ::
  Registered Client Connection Protocol: Ipv4
  Registered Client Name: DCN-INDIA-FI-A
  Registered Client GUID: e832cfc2-548b-11e4-b8f2-002a6a6f6dc1
  Registered Client Version: 2.2(6g)
  Registered Client Type: Managed Endpoint
  Registered Client Capability: Policy Client Module
  Registered Client Last Poll Timestamp: 2016-12-08T12:33:36.417
  Registered Client Operational State: Registered
  Registered Client Suspend State: Off
  Registered Client License State: License Graceperiod
  Registered Client grace period used: 33
  Registered Client Network Connection State: Connected
```

Difetti noti

- L'ID bug Cisco [CSCuy07652](#) per l'aggiornamento dall'ECMR6 a Delmar-mr2 rende il dominio "in registrazione".
- Errore durante l'aggiornamento di Cisco Bug ID [CSCuv07227](#) UCSM dopo la nuova registrazione.
- Impossibile aggiornare l'inventario. ID bug Cisco [CSCuu91088](#) Central.
- Cisco Bug ID [CSCut72698](#) report-full-inventory-failed su ucs classico in ambiente a larghezza di banda ridotta.

Informazioni correlate

[Registrazione dei domini Cisco UCS con Cisco UCS Central](#)

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).