

Dépannage des questions d'enregistrement UCSM avec le central

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Dépannage des méthodes](#)

[Dépannage de base](#)

[UCSM coincé enregistrant l'état avec le central](#)

[En cours coincé par état central UCSM après mise à jour](#)

[Visibilité perdue UCSM avec le central](#)

[Logs à vérifier](#)

[Défauts connus](#)

[Informations connexes](#)

Introduction

Ce document décrit comment dépanner certains des problèmes courants avec UCSM s'inscrivant au central UCS

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Système d'informatique unifiée Cisco (UCS)
- Central UCS

[Composants utilisés](#)

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Gestionnaire de Système d'informatique unifiée Cisco (UCSM)
- Fabric Interconnect (fi)
- Exécution centrale UCS sur la VM d'ESXi

Dépannage des méthodes

Le dépannage n'est concentré sur le certificat auto-signé sur UCSM et central et pas Certificats de

tiers

- Dépannage de base
- UCSM coincé enregistrant l'état avec le central
- En cours coincé par état central UCSM après mise à jour
- Perdre-visibilité UCSM avec le central
- Logs à vérifier
- Commandes de dépannage

Dépannage de base

Assurez s'il vous plaît que ces contrôles de base sont terminés :

- Non-concordance secrète partagée.
- Le périphérique central UCS n'est pas accessible.
- UCS GUID central est différent du GUID du central déjà enregistré UCS.
- Le temps n'est pas dans le sync entre le central UCSM et UCS.
- Certificat expiré sur UCSM.
- Le certificat par défaut de keyring n'est pas présent. Bien que le tiers CAs puisse être utilisé pour HTTPS. L'enregistrement UCSM utilise le certificat par défaut de keyring et par conséquent ne devrait pas être supprimé.
- Assurez qu'UCSM reçoit la demande de prise de contact de l'UCSC.

```
Central# connect local-mgmt
```

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

Capture de paquet d'UCSM s'inscrivant avec succès au fournisseur central

10.106.74.195	10.106.74.234	TCP	74 43448 → 443 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=233688518 TSecr=0 WS=128
10.106.74.234	10.106.74.195	TCP	74 443 → 43448 [SYN, ACK] Seq=8 Acc=1 Win=0 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 Acc=1 Win=0 Len=0 MSS=1460 SACK_PERM=1 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 Acc=89 Win=8888 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 Acc=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
10.106.74.234	10.106.74.195	TLSv1	125 Change Cipher Spec, Finished
10.106.74.195	10.106.74.234	TLSv1	412 [5G 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 Acc=1891 Win=10240 Len=0 TSval=9552344 TSecr=233688519
10.106.74.234	10.106.74.195	HTTP/XML	1484 HTTP/1.1 200 OK
10.106.74.195	10.106.74.234	TLSv1	183 Alert (Level: Warning, Description: Close Notify)
10.106.74.195	10.106.74.234	TCP	66 43448 → 443 [FIN, ACK] Seq=1928 Acc=2357 Win=10752 Len=0 TSval=233690027 TSecr=9567374
10.106.74.234	10.106.74.195	TCP	66 443 → 43448 [ACK] Seq=2357 Acc=1928 Win=10240 Len=0 TSval=9567377 TSecr=233690027
10.106.74.234	10.106.74.195	TLSv1	183 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	684	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

NE FONT PAS l'unregister le central d'UCSM. Quand vous unregister tous les services profils globaux deviendrez local au domaine UCS. Il est possible de rendre un service profile local global de nouveau. Cependant, c'est un processus très complexe et a une incidence sur le service.

UCSM coincé enregistrant l'état avec le central

Si des UCS Manager sont enregistrées à un UCS central et ces UCS Manager sont mises à jour à 3.1.1, alors les UCS Manager vont à enregistrer l'état et sont coincées là.

Trop d'erreurs de boucle observées dans le télémètre radar central se connecte

```
9603: [WARN][0x27699940][Apr 5 18:00:54.714][write:net] write of 3752 bytes using curl failed, code=7, error: 'Couldn't connect to server', ep:
```

```
https://10.106.74.195:443/xmlInternal/managed-endpoint
```

```
9604: [WARN][0x27699940][Apr 5 18:00:54.714][write:net] non-critical curl write error.
```

Du télémètre radar 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] ErrorMessage:ok ErrorNo:0
```

```
[INFO][0x682ffb90][Nov 1 16:05:24.886][app_sam_dme:processKey] something wrong with KR-default certificate, status - 18
```

Le problème a pu être dû à l'UCSM utilisant de vieilles informations parasites MDS au lieu de SHA1 pour les Certificats

```
[WARN][0x674ffb90][Nov 22 19:11:49.227][net:write] write of 546 bytes using curl failed, code=60, error: 'Peer certificate cannot be authenticated with given CA certificates(SSL certificate problem: self signed certificate)', ep:
```

```
https://10.106.74.234:443/xmlInternal/service-req
```

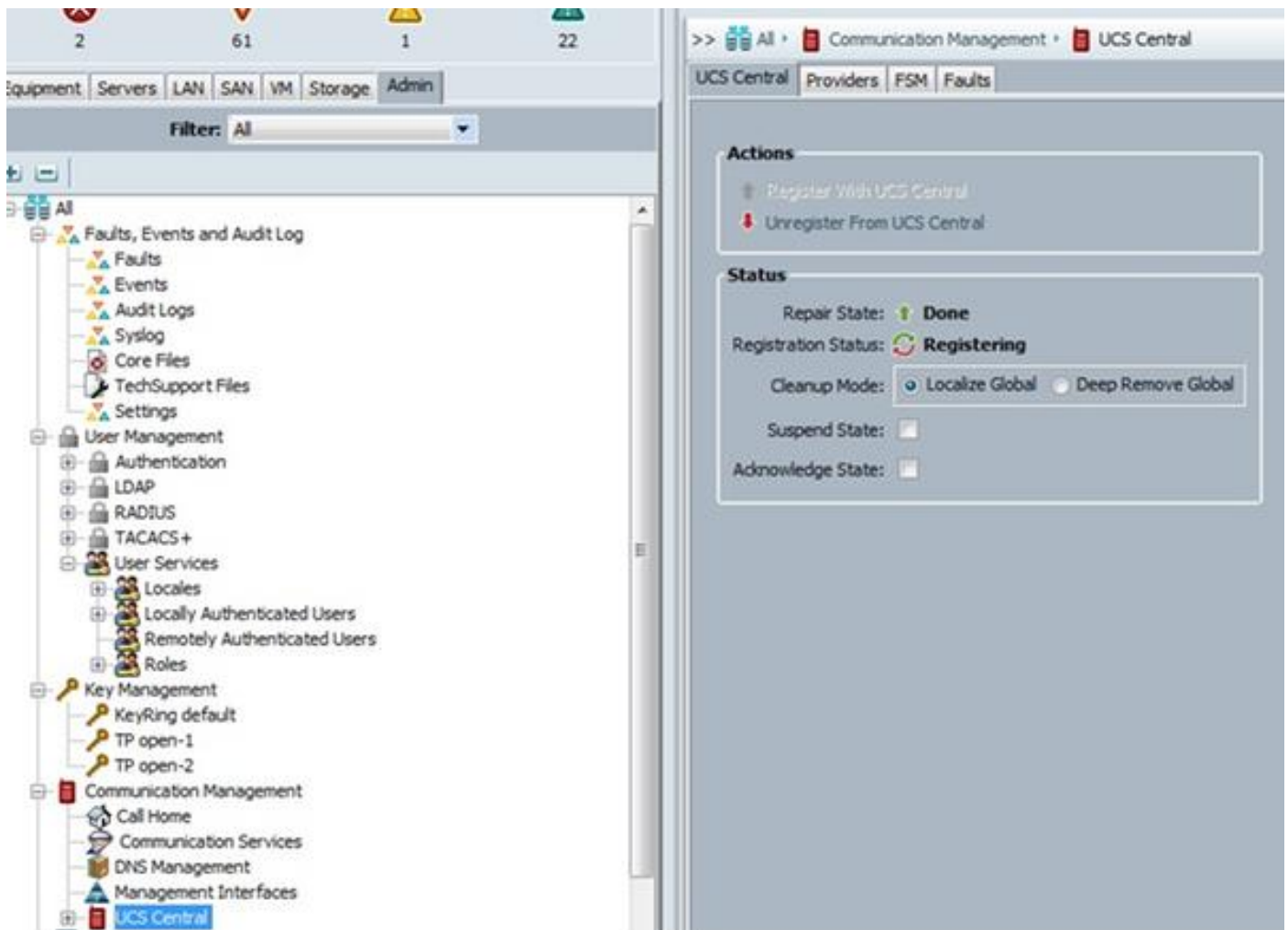
```
[INFO][0x674ffb90][Nov 22 19:11:49.227][net:certFailure] certificate is bad for connection to 'https://10.136.58.4:443/xmlInternal/service-req';
```

Exécutez ces le contournement comme il fait enregistrer avec succès à l'UCS central et corriger les UCS Manager l'erreur de certificat

Le keyring par défaut peut être régénéré de l'UCS CLI central sous la section de profil de périphérique.

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

Si le contournement ne le résout pas s'il vous plaît soulevez un cas avec Cisco TAC pour valider plus loin



Si à tout moment les UCS Manager ont été enregistrées au central UCS au commencement à une version de 2.1.3 ou ci-dessous. Alors pendant la mise à jour à 3.1.1 le problème d'enregistrement mentionné ci-dessus est encore vu.

Pour ce TAC l'implication est nécessaire comme UCS 2.1.3 et les versions antérieures, UCSM ne sépare pas le certificat. Réchauffé du besoin TAC le certificat de sorte que crée les bons softlinks au certificat.

En cours coincé par état central UCSM après mise à jour

La question est due à la base de données sort du sync entre le central et l'UCS

Ces erreurs observées dans les logs de gestionnaire de ressources

```
[WARN][0xbbce9940][Aug 11 10:23:18.194][storeMo:mit_init] SQL error [SQLParamData failure: Error while executing the query (non-fatal);
ERROR: duplicate key value violates unique constraint "InstanceId2DN_dn_key"] stmt [INSERT INTO "InstanceId2DN" ("instanceId", "dn", "className", "parent") VALUES (?, ?, ?, ?)]
[INFO][0xbbce9940][Aug 11 10:23:18.194][report:exception_handl] FATAL[3|150]
/ramfs/buildsa/150407-104741-rev219791-
FCSa/resMgr/sam/src/lib/framework/core/sql/MitDbImpl.cc(1167):storeMo: Failed to connect to database. Transaction aborted.
[INFO][0xbbce9940][Aug 11 10:23:18.201][report:exception_handl] ERROR[3|150]
/ramfs/buildsa/150407-104741-rev219791-
FCSa/resMgr/sam/src/lib/framework/core/proc/Doer.cc(795):exceptionCB: exception encountered during processing: "Failed to connect to database. Transaction aborted." [150] Failed to connect
```

to database. Transaction aborted.

[INFO][0xbbce9940][Aug 11 10:23:18.201][failedCb:tx] TX FAILED

C'est une question de sync de base de données soulèvent s'il vous plaît un cas avec Cisco TAC pour valider plus loin

Visibilité perdue UCSM avec le central

The image shows two screenshots from the UCS Central web interface. The top screenshot displays the 'All Domains' page with a table listing domains. The bottom screenshot shows the detailed configuration page for a domain, highlighting the registration status.

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(f)gA FW Ready	Lost Visibility Fault Level: Critical

The bottom screenshot shows the 'Providers' tab with the following registration status:

- Repair State: Done
- Registration Status: Lost Visibility
- Cleanup Mode: Localize Global (selected), Deep Remove Global
- Suspend State: []
- Acknowledge State: []

Vérifiez l'état d'enregistrement

S'il affiche la « perdre-visibilité » le central UCS ne peut pas être atteint sur un ou plusieurs ports exigés. Si le central UCS utilise le GUI d'instantané (flexible) les ports suivants doivent être ouverts de central : 443, 80, 843. Le GUI HTML exige seulement le port 443.

Logs à vérifier

UCSM

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

Central

Svc_dme_reg.log

Commandes de dépannage

```
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
```

Défauts connus

- La dwngarde-mise à jour de l'**ID de bogue Cisco [CSCuy07652](#)** d'ECMR6 à Delmar-mr2 fait le domaine « s'enregistrant ».
- Re-enregistrement de l'**ID de bogue Cisco [CSCuv07227](#)** UCSM manquant tout en faisant la mise à jour FW.
- Incapable central de l'**ID de bogue Cisco [CSCuu91088](#)** de régénérer l'inventaire.
- L'**ID de bogue Cisco [CSCut72698](#)** **état-plein-inventaire**-a échoué sur l'UCS classique dans l'environnement de faible bande passante.

Informations connexes

Enregistrement du domaine de Cisco UCSM avec le central UCS

http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/gui/config/guide/2-2/b_UCSM_GUI_Configuration_Guide_2_2/registering_cisco_ucs_domains_with_cisco_ucs_central.html