Dépannage des problèmes d'enregistrement UCSM avec Central

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Méthodes de dépannage

- Dépannage de base
- État d'enregistrement bloqué UCSM avec Central
- État central UCSM bloqué après la mise à niveau
- UCSM a perdu sa visibilité avec Central
- Journaux à vérifier

Défauts connus

Informations connexes

Introduction

Ce document décrit comment résoudre certains des problèmes courants liés à l'enregistrement UCSM avec UCS Central

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Unified Computing System (UCS)
- UCS Central

Composants utilisés

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

logiciel suivantes :

- Cisco Unified Computing System Manager (UCSM)
- Interconnexion de fabric (FI)
- UCS central exécuté sur VM ESXi

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Méthodes de dépannage

Le dépannage est axé sur le certificat auto-signé sur UCSM et les certificats centraux et non sur les certificats tiers

- Dépannage de base
- État d'enregistrement UCSM bloqué avec central
- État central UCSM bloqué après la mise à niveau
- Visibilité perdue UCSM avec
- Journaux à vérifier
- Commandes de dépannage

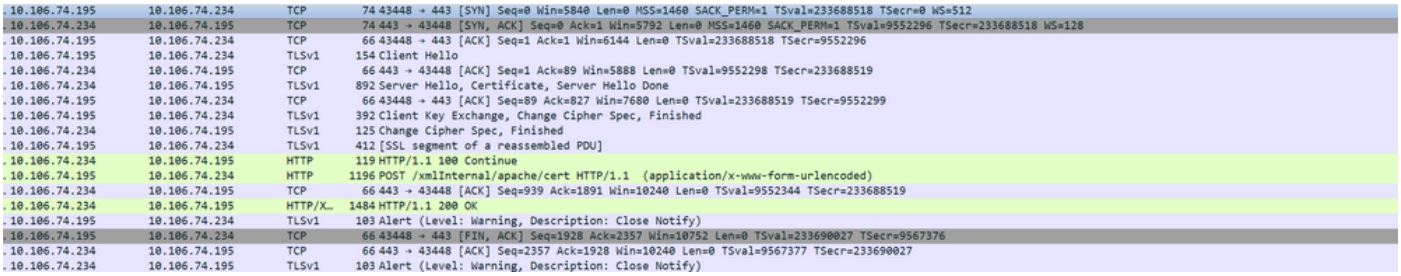
Dépannage de base

Assurez-vous que les vérifications de base suivantes sont effectuées :

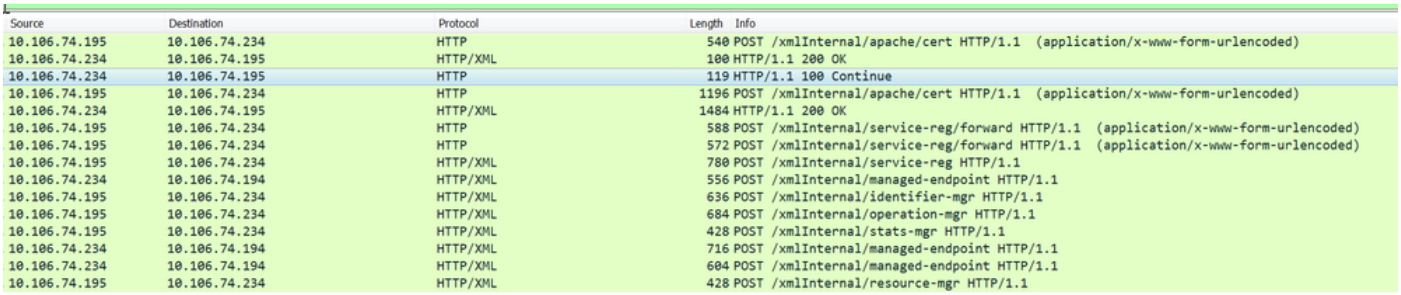
- Non-concordance du secret partagé.
- Le périphérique UCS Central n'est pas accessible.
- Le GUID d'UCS Central est différent du GUID d'UCS Central déjà enregistré.
- L'heure n'est pas synchronisée entre UCSM et UCS Central.
- Certificat expiré sur UCSM.
- Le certificat de porte-clés par défaut n'est pas présent. Bien que les autorités de certification tierces puissent être utilisées pour HTTPS. L'enregistrement UCSM utilise le certificat de trousseau par défaut et ne doit donc pas être supprimé.
- Assurez-vous qu'UCSM reçoit la demande de connexion de l'UCSC.

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

Capture de paquets à partir de l'enregistrement UCSM avec succès auprès du fournisseur central



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
10.106.74.234	10.106.74.195	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
10.106.74.234	10.106.74.195	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

NE DÉSINSCRIVEZ PAS le central de UCSM. Lorsque vous annulez l'inscription, tous les profils de service globaux deviennent locaux dans le domaine UCS. Il est possible de redéfinir un profil de service local global. Cependant, il s'agit d'un processus très complexe qui a un impact sur le service.

État d'enregistrement bloqué UCSM avec Central

Si UCS Manager est enregistré auprès d'UCS Central et qu'UCS Manager est mis à niveau vers la version 3.1.1, UCS Manager passe à l'état d'enregistrement et est bloqué.

Trop d'erreurs de boucle observées dans les journaux DME centraux

```
  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.
```

Depuis UCSM DME

```
[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
```

Le problème peut être dû à l'utilisation de l'ancien hachage MDS par UCSM au lieu de SHA1 pour les certificats

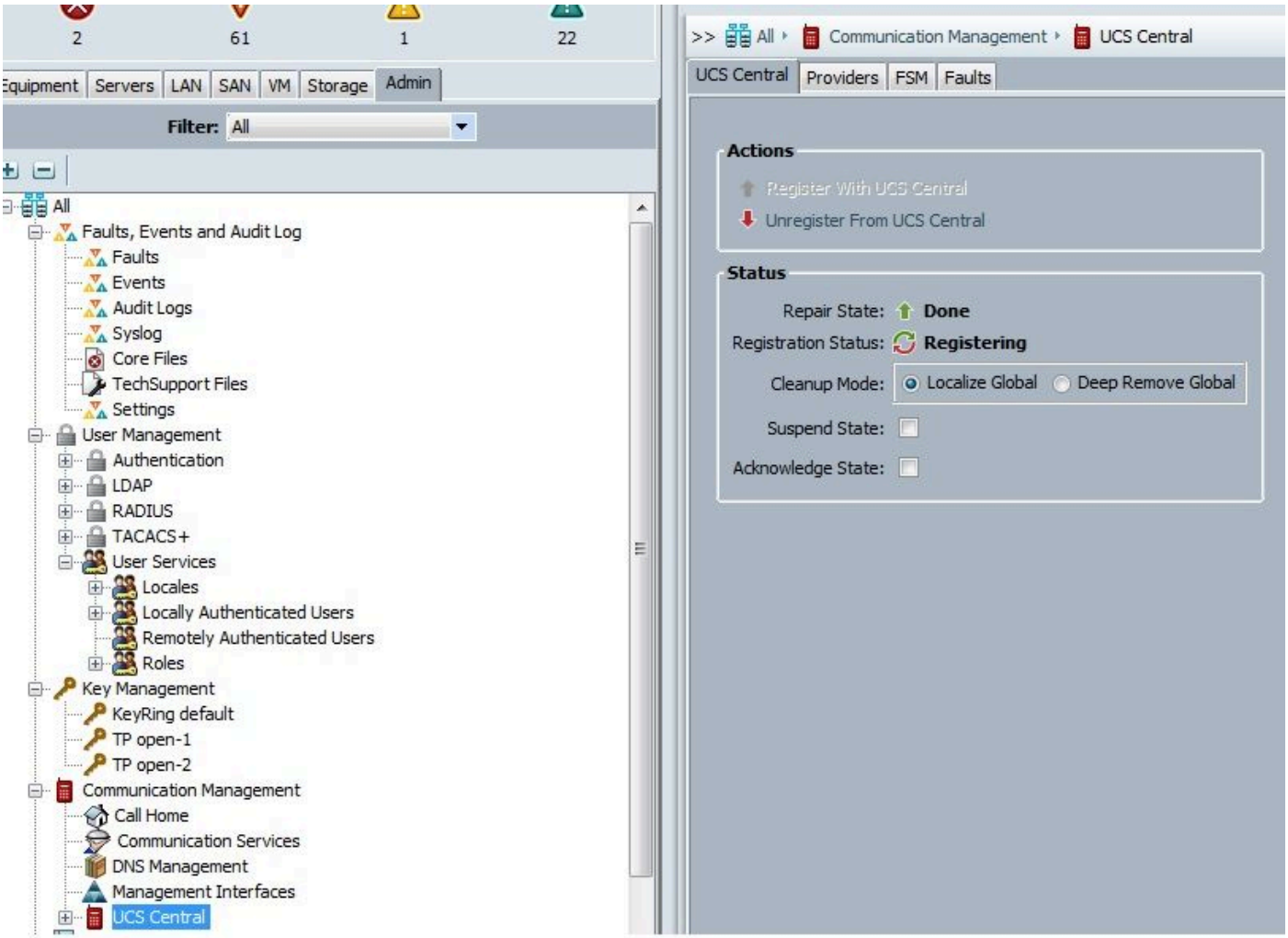
```
[WARN][0x674ffb90][Nov 22 19:11:49.227][net:write] write of 546 bytes using curl failed, code=60, error
[INFO][0x674ffb90][Nov 22 19:11:49.227][net:certFailure] certificate is bad for connection to ' https:/
```

Effectuez ces solutions de contournement car cela permet à UCS Manager de s'enregistrer correctement auprès d'UCS Central et de corriger l'erreur de certificat

Le trousseau de clés par défaut peut être régénéré à partir de l'interface de ligne de commande UCS Central sous la section du profil de périphérique.

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

Si la solution de contournement ne résout pas le problème, soumettez un dossier au TAC Cisco pour valider



Si, à un moment quelconque, UCS Manager a été enregistré auprès d'UCS Central à partir de la version 2.1.3 ou d'une version antérieure. Ensuite, lors de la mise à niveau vers la version 3.1.1, le problème d'enregistrement mentionné est toujours visible.

Pour cette participation du TAC, UCS 2.1.3 et les versions antérieures sont nécessaires. UCSM ne divise pas le certificat. Le TAC doit hacher à nouveau le certificat afin de créer les liens logiciels appropriés au certificat.

État central UCSM bloqué après la mise à niveau

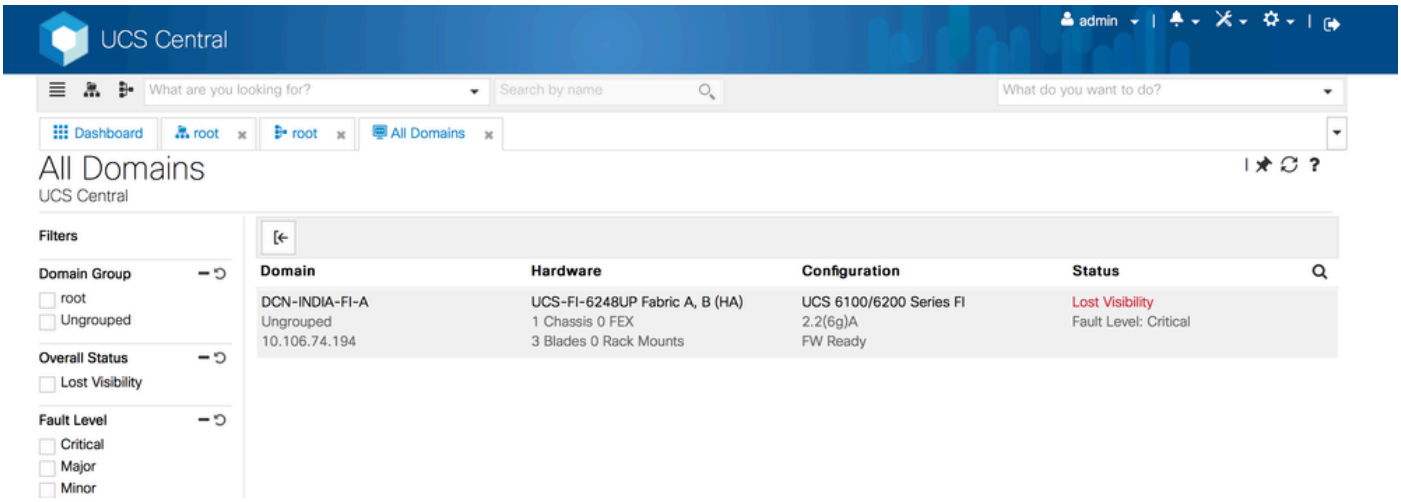
Le problème est dû à une désynchronisation de la base de données entre le serveur central et UCS

Ces erreurs ont été observées dans les journaux du gestionnaire de ressources

```
[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
```

Il s'agit d'un problème de synchronisation de base de données. Veuillez contacter le TAC Cisco pour valider

UCSM a perdu sa visibilité avec Central



Vérifier l'état d'enregistrement

S'il indique une perte de visibilité, UCS Central n'est pas accessible sur un ou plusieurs ports requis. Si UCS Central utilise l'interface utilisateur graphique flash (Flex), ces ports doivent être ouverts sur Central : 443, 80, 843. L'interface utilisateur graphique HTML requiert uniquement le port 443.

Journaux 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

- L'ID de bogue Cisco CSCuy07652 downgrade-upgrade de ECMR6 à Delmar-mr2 rend le domaine « enregistrement ».
- Échec de la réinscription de l'ID de bogue Cisco CSCuv07227 UCSM lors de la mise à niveau.
    - Le bogue Cisco CSCuu91088 Central n'a pas pu actualiser l'inventaire.
    - Le rapport d'ID de bogue Cisco CSCut72698-full-inventory-failed on classic ucs in low bandwidth environment.

Informations connexes

Enregistrement des domaines Cisco UCS auprès de Cisco UCS Central

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.