Resolver problemas los problemas del registro UCSM con la central

Contenido

Introducción

Este documento describe cómo resolver problemas algunos de los problemas frecuentes con UCSM que se registra con la central UCS

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Unified Computing System (UCS)
- Central UCS

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Administrador del Cisco Unified Computing System (UCSM)
- Interconexión de la tela (FI)
- Funcionamiento central UCS en ESXi VM

Métodos de Troubleshooting

El troubleshooting se centra en el certificado autofirmado en UCSM y central y no los Certificados

de las de otras compañías

- Troubleshooting básico
- UCSM pegado registrando el estado con la central
- En curso pegada estatus central UCSM después de la actualización
- Perdido-visibilidad UCSM con la central
- Registros a marcar
- Comandos de Troubleshooting

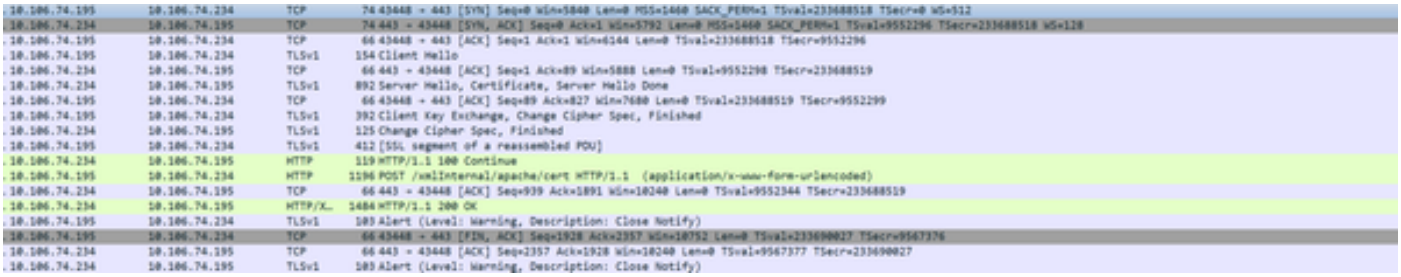
Resolución de problemas básicos

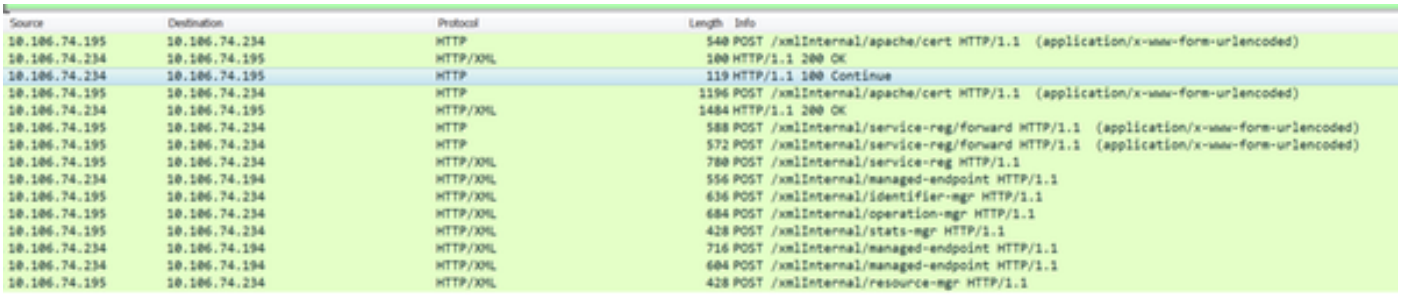
Asegúrese por favor que estos controles básicos estén completados:

- Discordancía del secreto compartido.
- El dispositivo central UCS no es accesible.
- El UCS GUID central es diferente del GUID de la central ya registradoa UCS.
- El tiempo no es adentro sincronizar entre la central UCSM y UCS.
- Certificado vencido en UCSM.
- El certificado predeterminado del llavero no está presente. Aunque el otro vendedor CA se puede utilizar para el HTTPS. El registro UCSM utiliza el certificado predeterminado del llavero y por lo tanto no debe ser borrado.
- Asegúrese que UCSM esté recibiendo la petición del apretón de manos del UCSC.

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

Captura de paquetes de UCSM que se registra con éxito con el proveedor central





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

No desregistre la central de UCSM. Cuando usted desregistra todos los servicio-perfiles globales llegarán a ser locales al dominio UCS. Es posible hacer un servicio-perfil local global otra vez. Sin embargo, es mismo un proceso complejo y tiene un impacto en el servicio.

UCSM pegado registrando el estado con la central

Si registran al administrador UCS a un UCS central y están actualizando a ese administrador UCS a 3.1.1, después el administrador UCS va a registrar el estado y se pega allí.

Demasiados errores del rizo observados en los registros centrales DME

```
  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.
```

De 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
certificate, status - 18
```

El problema podía ser debido al UCSM usando el hash viejo MDS en vez del SHA1 para los Certificados

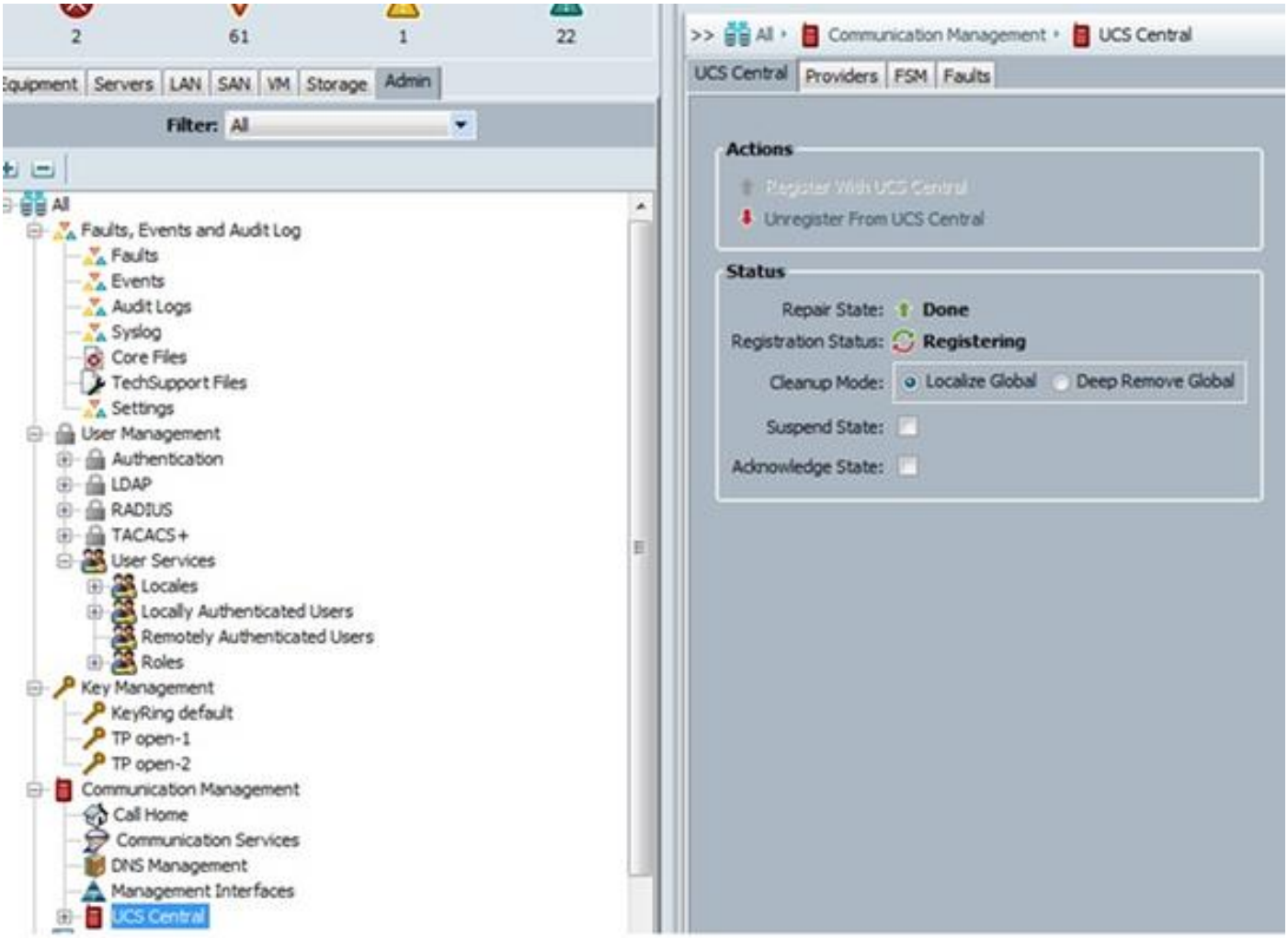
```
[WARN][0x674ffb90][Nov 22 19:11:49.227][net:write] write of 546 bytes using curl failed,
code=60, error: 'Peer certificate cannot be authenticated with given CA certificates(SSL
certificate problem: self signed certificate)', ep:
https://10.106.74.234:443/xmlInternal/service-reg
[INFO][0x674ffb90][Nov 22 19:11:49.227][net:certFailure] certificate is bad for connection to '
https://10.136.58.4:443/xmlInternal/service-reg';
```

Realice este la solución alternativa como hace al administrador UCS registrarse con éxito al UCS central y reparar el error del certificado

El llavero predeterminado se puede regenerar del UCS CLI central bajo sección del perfil del dispositivo.

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

Si la solución alternativa no resuelve por favor plantee un caso con el TAC de Cisco para validar más lejos



Si han registrado en cualquier momento al administrador UCS a la central UCS inicialmente en una versión de 2.1.3 o abajo. Entonces durante la actualización a 3.1.1 el Problema de inscripción mencionado anteriormente todavía se considera.

Para este TAC la implicación se necesita como UCS 2.1.3 y las versiones anteriores, UCSM no parten el certificado. Refundición de la necesidad de TAC el certificado de modo que cree los softlinks correctos al certificado.

En curso pegada estatus central UCSM después de la actualización

El problema es debido a la base de datos sale de sincroniza entre la central y el UCS

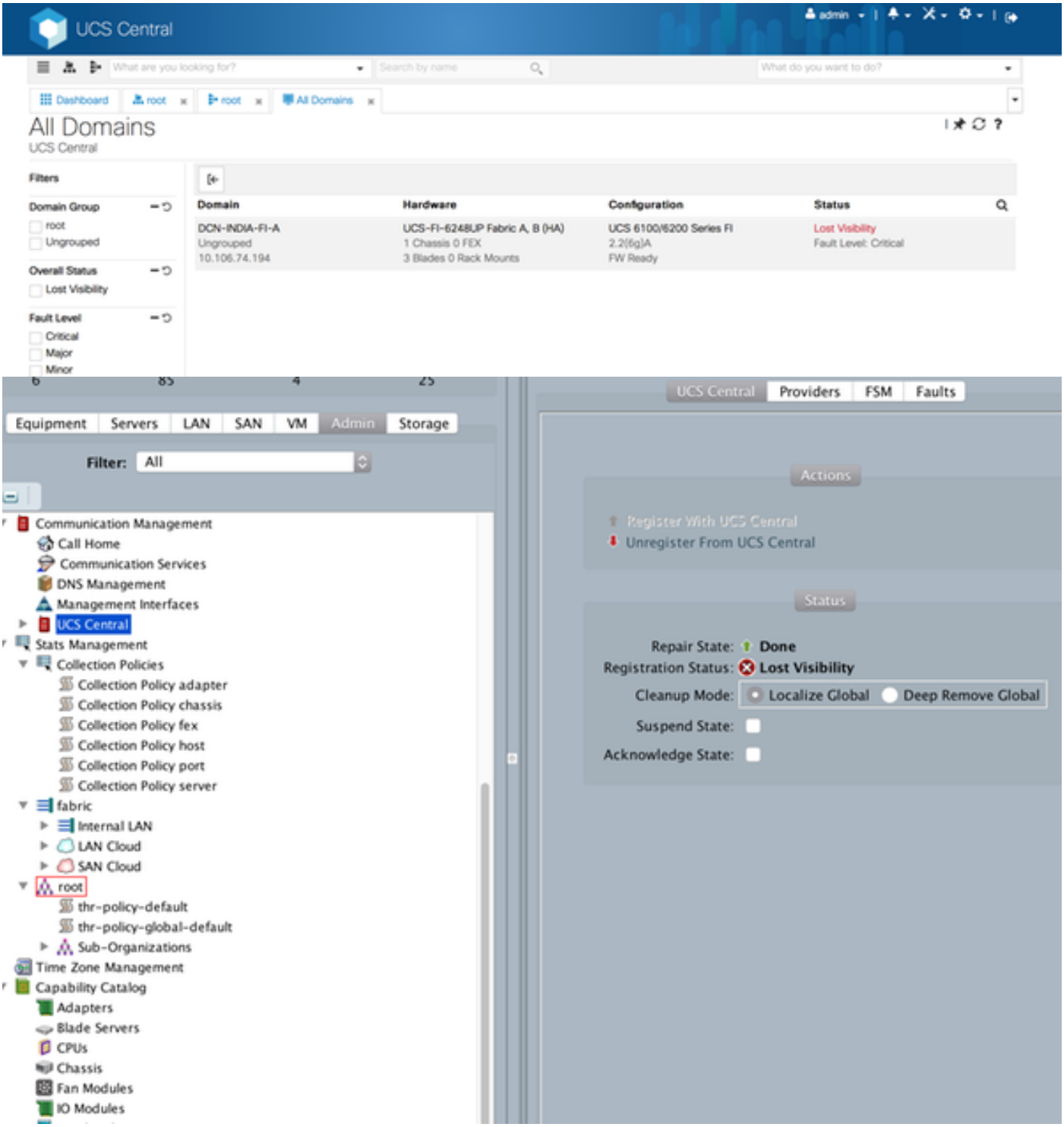
Estos errores observados en los registros del administrador de recursos

```
[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
```

Esto es un problema de la sincronización de la base de datos plantea por favor un caso con el TAC de Cisco para validar más lejos

Visibilidad perdida UCSM con la central



Marque el estado de registro

Si muestra la “perdido-visibilidad” la central UCS no se puede alcanzar en uno o más puertos requeridos. Si la central UCS está utilizando el flash GUI (flexión) los puertos siguientes necesitan estar abiertos a la central: 443, 80, 843. El HTML GUI requiere solamente el puerto 443.

Registros a marcar

UCSM

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

Central

Svc_dme_reg.log

Comandos de Troubleshooting

```
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
```

Defectos conocidos

- La dwngarde-actualización del **Id. de bug Cisco** CSCuy07652 de ECMR6 a Delmar-mr2 hace el dominio “que se registra”.
- Fall del re-registro del **Id. de bug Cisco** CSCuv07227 UCSM mientras que hace la actualización fw.
- Incapaz central del **Id. de bug Cisco** CSCuu91088 de restaurar el inventario.
- **El Id. de bug Cisco** CSCut72698 informe-FULL-inventario-falló en el ucs clásico en el entorno del ancho de banda baja.

Información Relacionada

Registro del dominio de Cisco UCSM con la 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