

Problemen met UCSM-registratie oplossen met Central

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Methoden voor probleemoplossing](#)

[Basisproblemen oplossen](#)

[UCSM vastgelopen Registrerende Staat met Centrale](#)

[Centrale status van UCSM vastgelopen na upgrade](#)

[UCSM verloor zichtbaarheid met Central](#)

[Te controleren logs](#)

[Bekende gebreken](#)

[Gerelateerde informatie](#)

Inleiding

In dit document wordt beschreven hoe u een aantal veelvoorkomende problemen met UCSM-registratie bij UCS Central kunt oplossen

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Unified Computing System (UCS)
- UCS Central

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Unified Computing System Manager (UCSM)
- Fabric Interconnect (FI)
- Centrale UCS die op ESXi VM wordt uitgevoerd

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Methoden voor probleemoplossing

De probleemoplossing is gericht op zelfondertekende certificaten op UCSM en centrale en niet op certificaten van derden

- Basisprobleemoplossing
- UCSM blijft staat registreren bij centrale
- Centrale status van UCSM vastgelopen na upgrade
- Verloren zichtbaarheid van UCSM met centrale
- Logboeken om te controleren
- Opdrachten voor troubleshooting

Basisproblemen oplossen

Controleer of deze basiscontroles zijn voltooid:

- Gedeelde geheime mismatch.
- UCS Central is niet bereikbaar.
- UCS Central GUID verschilt van de reeds geregistreerde UCS Central GUID.
- De tijd is niet synchroon tussen UCSM en UCS Central.
- Verlopen certificaat op UCSM.
- Het standaardcertificaat voor de sleutelhanger is niet aanwezig. CA's van derden kunnen worden gebruikt voor HTTPS. De UCSM-registratie maakt gebruik van het standaard sleutelhangercertificaat en mag daarom niet worden verwijderd.
- Zorg ervoor dat UCSM het handdruk verzoek van de UCSC ontvangt.

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

Packet capture van UCSM met succes registreren bij Central Provider

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	183 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	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	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

DEREGISTREER de centrale niet van UCSM. Wanneer u alle wereldwijde serviceprofielen verwijdert, wordt deze lokaal voor het UCS-domein. Het is mogelijk om een lokaal serviceprofiel weer globaal te maken. Het is echter een zeer complex proces en heeft een impact op de service.

UCSM vastgelopen Registrerende Staat met Centrale

Als UCS Manager is geregistreerd bij een UCS Central en die UCS Manager wordt geüpgraded naar 3.1.1, gaat de UCS Manager naar de registratiestatus en zit daar vast.

Te veel curlfouten waargenomen in de centrale DME-logboeken

```
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.
```

Van 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
```

Het probleem kan te wijten zijn aan het UCSM met behulp van oude MDS hash in plaats van

SHA1 voor de certificaten

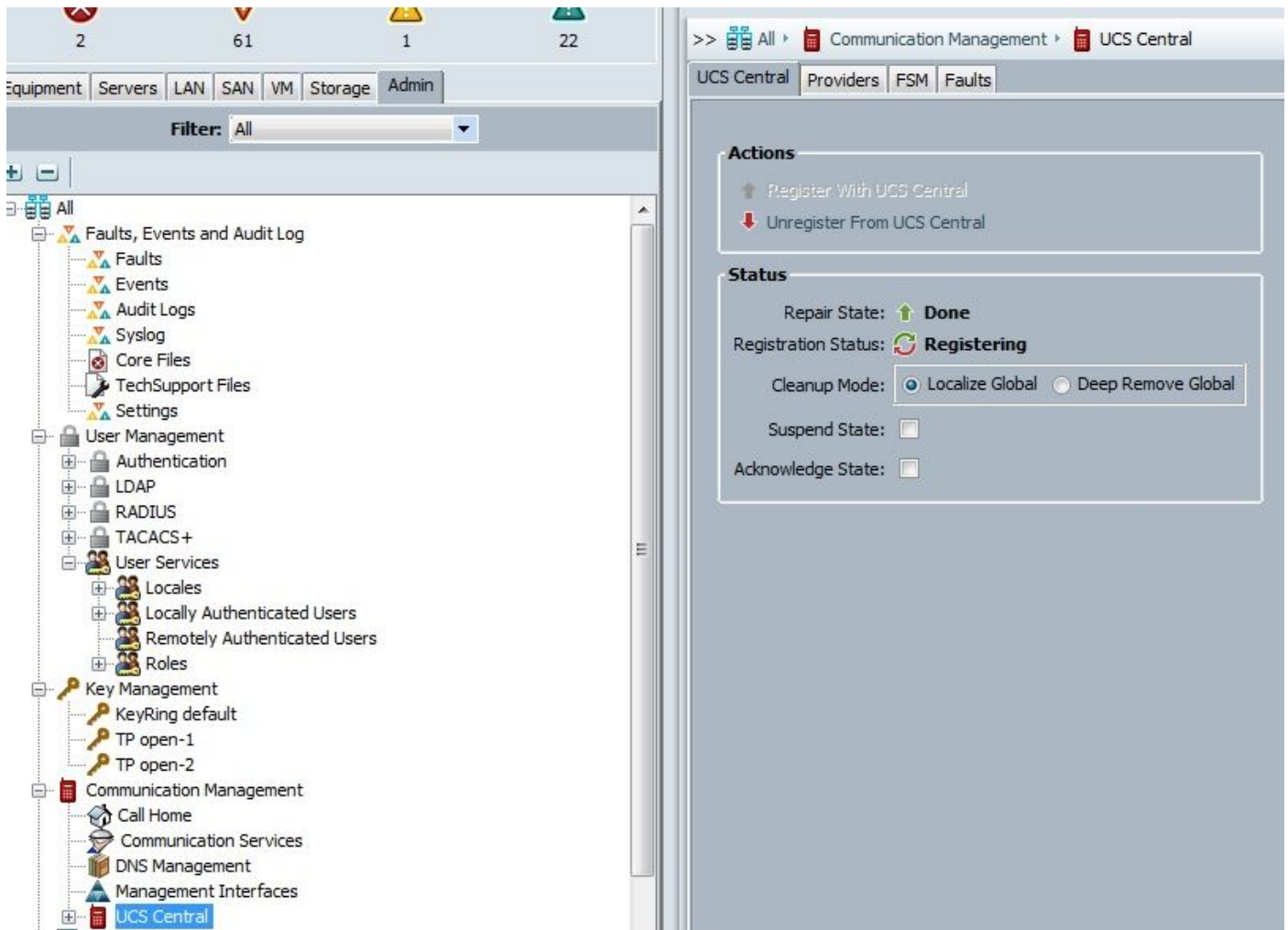
```
[WARN][0x674ffb90][Nov 22 19:11:49.227][net:write] write of 546 bytes using curl failed, code=60, error  
[INFO][0x674ffb90][Nov 22 19:11:49.227][net:certFailure] certificate is bad for connection to ' https://
```

Voer deze tijdelijke oplossing uit omdat de UCS Manager zich succesvol registreert bij UCS Central en de certificaatfout verhelpt

De standaardsleutelhanger kan worden geregenereerd vanuit de UCS Central CLI onder het gedeelte Apparaatprofiel.

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

Als de oplossing van de workaround niet wordt opgelost, dient u een zaak aan te kaarten bij Cisco TAC om deze verder te valideren



Als de UCS Manager op enig moment in eerste instantie bij UCS Central is geregistreerd in een versie van 2.1.3 of lager. Dan wordt tijdens de upgrade naar 3.1.1 het genoemde registratieprobleem nog steeds gezien.

Voor deze TAC-betrokkenheid is nodig als UCS 2.1.3 en eerdere releases, UCSM niet splitsen certificaat. TAC's moeten het certificaat opnieuw hashen, zodat de juiste softlinks naar het certificaat worden gemaakt.

Centrale status van UCSM vastgelopen na upgrade

Het probleem is te wijten aan database gaat uit van sync tussen centrale en UCS

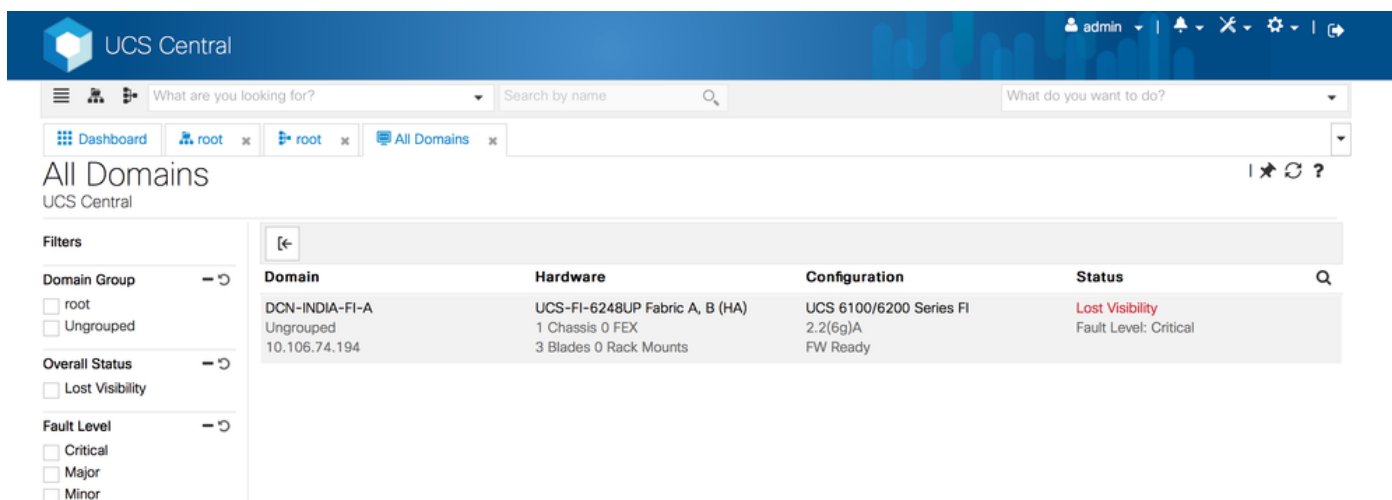
Deze fouten zijn waargenomen in de logboeken van de resource manager

```
[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
```

Dit is een probleem met de database-synchronisatie. Breng een zaak aan bij Cisco TAC om deze verder te valideren

UCSM verloor zichtbaarheid met Central



The screenshot shows the UCS Central web interface. The top navigation bar includes the UCS Central logo, a user profile (admin), and various icons. Below the navigation bar, there are tabs for 'Dashboard', 'root', and 'All Domains'. The main content area is titled 'All Domains' and displays a table of domains. The table has columns for 'Domain', 'Hardware', 'Configuration', and 'Status'. One domain is listed: 'DCN-INDIA-FI-A', which is 'Ungrouped' with IP '10.106.74.194'. Its hardware is 'UCS-FI-6248UP Fabric A, B (HA)' with '1 Chassis 0 FEX' and '3 Blades 0 Rack Mounts'. The configuration is 'UCS 6100/6200 Series FI 2.2(6g)A' and 'FW Ready'. The status is 'Lost Visibility' with a 'Fault Level: Critical'.

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

Controleer de registratiestatus

Als het "verloren-zichtbaarheid" laat zien, kan UCS Central niet worden bereikt op een of meer vereiste poorten. Als UCS Central de flash GUI (Flex) gebruikt, moeten deze poorten open zijn voor Central: 443, 80, 843. Voor HTML GUI is poort 443 vereist.

Te controleren logs

UCSM

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

centraal

Svc_dme_reg.log

Opdrachten voor 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
```

Bekende gebreken

- Cisco Bug ID [CSCuy07652](#) downgarde-upgrade van ECMR6 naar Delmar-mr2 maakt domein "registreren".
- Cisco Bug ID [CSCuv07227](#) UCSM-herregistratie mislukt tijdens fw-upgrade.
- Cisco Bug ID [CSCuu91088](#) Central kan voorraad niet vernieuwen.
- Cisco Bug ID [CSCut72698](#) rapporteert een volledige inventarisatie van klassieke ucs in een omgeving met lage bandbreedte.

Gerelateerde informatie

[Cisco UCS-domeinen registreren bij Cisco UCS Central](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.