Pesquisando defeitos edições do registro UCSM com central

Índice

Introdução

Este documento descreve como pesquisar defeitos alguns dos problemas comuns com o UCSM que registra-se com central UCS

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Unified Computing System (UCS)
- Central UCS

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Gerente do Cisco Unified Computing System (UCSM)
- Interconexão da tela (FI)
- Corredor central UCS em ESXi VM

Métodos de Troubleshooting

O Troubleshooting é focalizado no certificado auto-assinado em UCSM e central e não Certificados da 3ª parte

- Troubleshooting básico
- UCSM colado registrando o estado com central
- Em andamento colado UCSM estado central após a elevação
- Perdido-visibilidade UCSM com central
- Logs a verificar
- Comandos de Troubleshooting

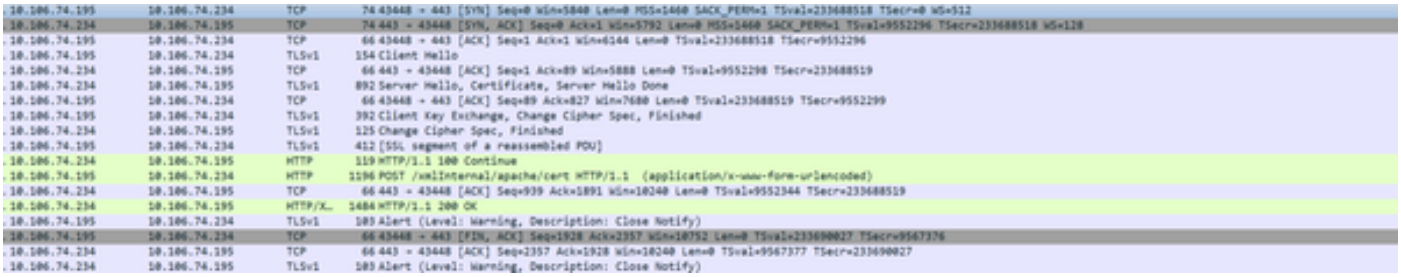
Troubleshooting Básico

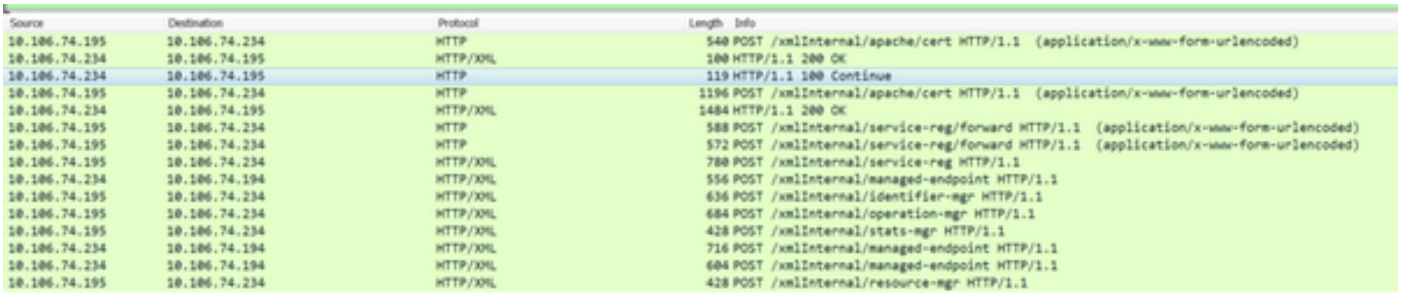
Assegure-se de por favor que estas verificações básicas estejam terminadas:

- Má combinação secreta compartilhada.
- O dispositivo central UCS não é alcançável.
- O UCS GUID central é diferente do GUID da central já registrada UCS.
- O tempo não está na sincronização entre a central UCSM e UCS.
- Certificado expirado em UCSM.
- O certificado do keyring do padrão não está atual. Embora a terceira parte CA pode ser usada para o HTTPS. O registro UCSM usa o certificado do keyring do padrão e daqui não deve ser suprimido.
- Assegure-se de que UCSM esteja recebendo o pedido do aperto de mão do UCSC.

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

Captura de pacote de informação de UCSM que registra-se com sucesso com fornecedor 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

Não remover registro a central de UCSM. Quando você remove registro todos os serviço-perfis globais se tornarão locais ao domínio UCS. É possível fazer outra vez um serviço-perfil local global. Contudo, é muito um processo complexo e tem um impacto no serviço.

UCSM colado registrando o estado com central

Se o gerente UCS é registrado a um UCS central e esse gerente UCS está sendo promovido a 3.1.1, a seguir o gerente UCS vai a registrar o estado e é colado lá.

Erros demais da onda observados nos logs centrais 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
```

O problema podia ser devido ao UCSM usando a mistura velha MDS em vez do SHA1 para os Certificados

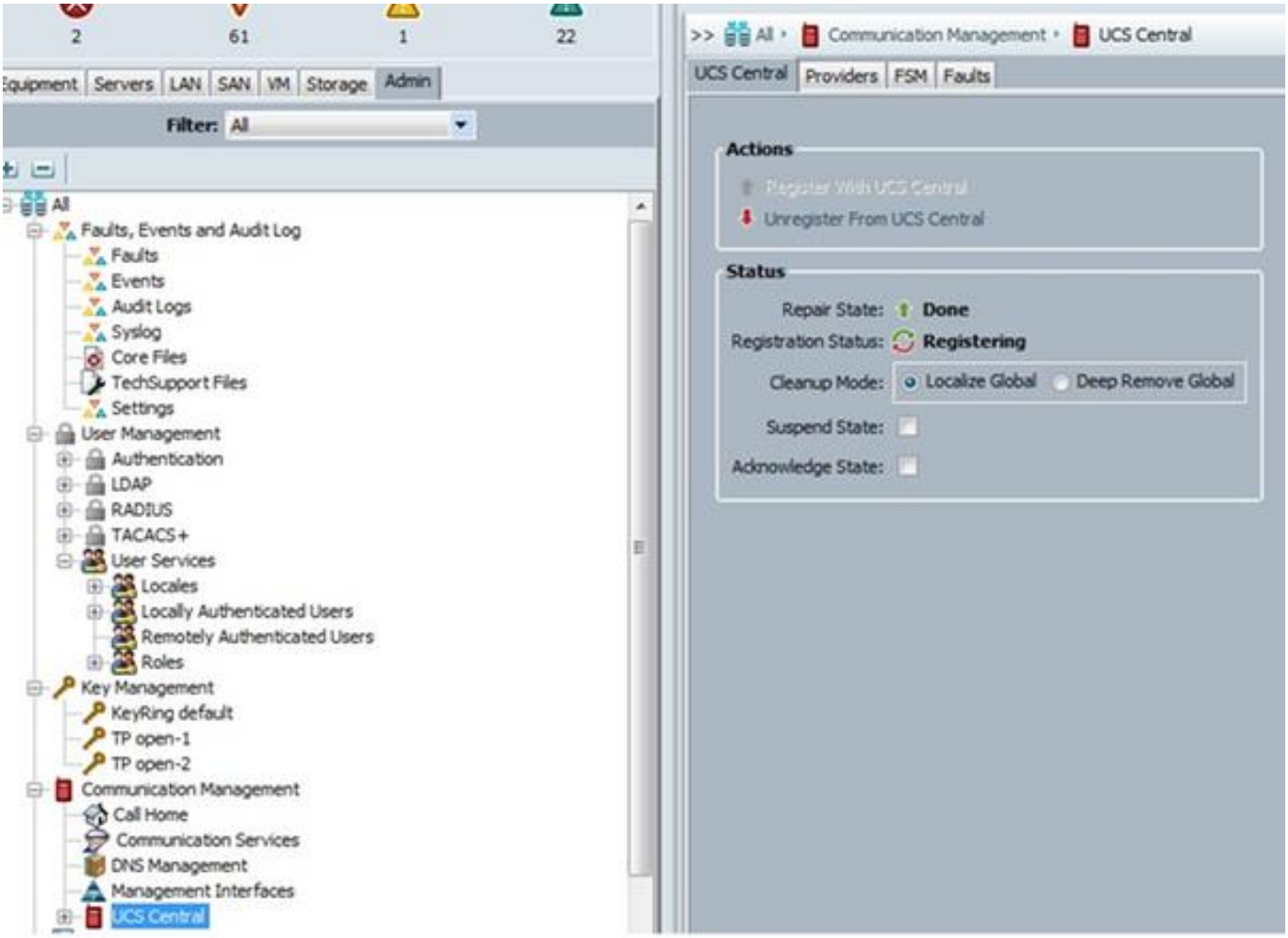
```
[WARN][0x674ffb90][Nov 22 19:11:49.227][net:write] write of 546 bytes using curl failed,
code=60, error: 'Peer certificate cannot be authenticated with given CA certificates(SSL
certificate problem: self signed certificate)', ep:
https://10.106.74.234:443/xmlInternal/service-reg
[INFO][0x674ffb90][Nov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

Execute este a ação alternativa como faz com que o gerente UCS se registre com sucesso ao UCS central e se fixe o erro do certificado

O keyring do padrão pode ser regenerado do UCS CLI central sob a seção do perfil de dispositivo.

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

Se a ação alternativa não resolve por favor aumente um caso com tac Cisco para validar mais



Se o gerente UCS tem sido registrado a qualquer hora à central UCS inicialmente em uma versão de 2.1.3 ou abaixo. Então durante a elevação a 3.1.1 o problema de registro mencionado acima é considerado ainda.

Para este TAC a participação é precisada como UCS 2.1.3 e as versões anterior, UCSM não racham o certificado. Necessidade TAC de repetir o certificado de modo que crie os softlinks direitos ao certificado.

Em andamento colado UCSM estado central após a elevação

A edição é devido ao base de dados sai da sincronização entre a central e o UCS

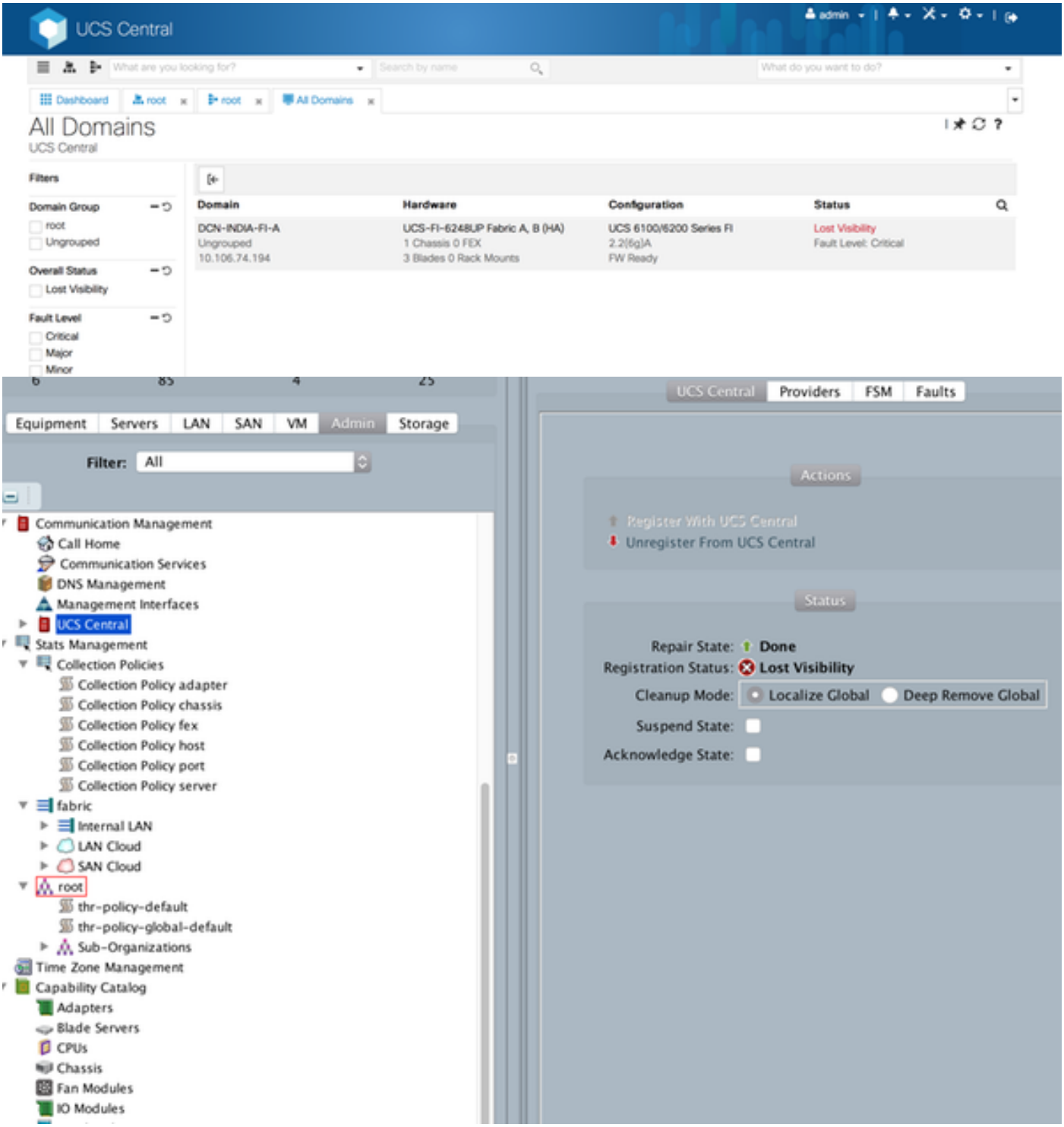
Estes erros observados nos logs do gerenciador de recurso

```
[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
```

Esta é uma edição da sincronização de base de dados aumenta por favor um caso com tac Cisco para validar mais

Visibilidade perdida UCSM com central



Verifique o status de registro

Se mostra a “perdido-visibilidade” a central UCS não pode ser alcançada em umas ou várias portas exigidas. Se a central UCS está usando o flash GUI (cabo flexível) as seguintes portas precisam de estar abertas à central: 443, 80, 843. O HTML GUI exige somente a porta 443.

Logs a verificar

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
```

Defeitos conhecidos

- A dwngarde-elevação da **identificação de bug Cisco** CSCuy07652 de ECMR6 a Delmar-mr2 faz o domínio “que registra-se”.
- Failing do re-registro da **identificação de bug Cisco** CSCuv07227 UCSM ao fazer a elevação fw.
- Incapaz central da **identificação de bug Cisco** CSCuu91088 de refrescar o inventário.
- **A identificação de bug Cisco** CSCut72698 relatório-FULL-inventário-falhou no ucs clássico no ambiente da largura de banda baixa.

Informações Relacionadas

Registrando o domínio de Cisco UCSM com 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