Solucionar problemas de registro de licença do Hyperflex

Contents

Introdução

Este documento descreve como solucionar os problemas mais comuns da licença de registro Hyperflex.

Pré-requisitos

A Cisco recomenda que você tenha conhecimento básico destes tópicos:

- Conexão Hyperflex
- Registro de licença
- HTTP/HTTPS

Componentes Utilizados

As informações neste documento são baseadas em:

Hyperflex Data Platform (HXDP) 5.0.(2a) e posterior

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O que é Smart License?

Cisco Smart Software Licensing (Smart Licensing) é uma solução inteligente de gerenciamento de licenças de software baseada em nuvem que simplifica as três principais funções de licença (compra, gerenciamento e relatório) em toda a sua organização.

Você pode acessar sua conta da Smart License aqui.

Como funcionam as licenças do Hyperflex?

Cisco Hyperflex integra-se com **Smart Licensing** e é automaticamente habilitado por padrão quando você cria um cluster de armazenamento Hyperflex.

No entanto, para que o cluster de armazenamento Hyperflex consuma e relate licenças, você deve registrá-lo no **Cisco Smart Software Manager** (SSM) através do seu **Cisco Smart Account.**

R **Smart Account** é um repositório baseado em nuvem que fornece visibilidade total e controle de acesso a todas as licenças de software da Cisco adquiridas e instâncias de produtos em sua empresa.

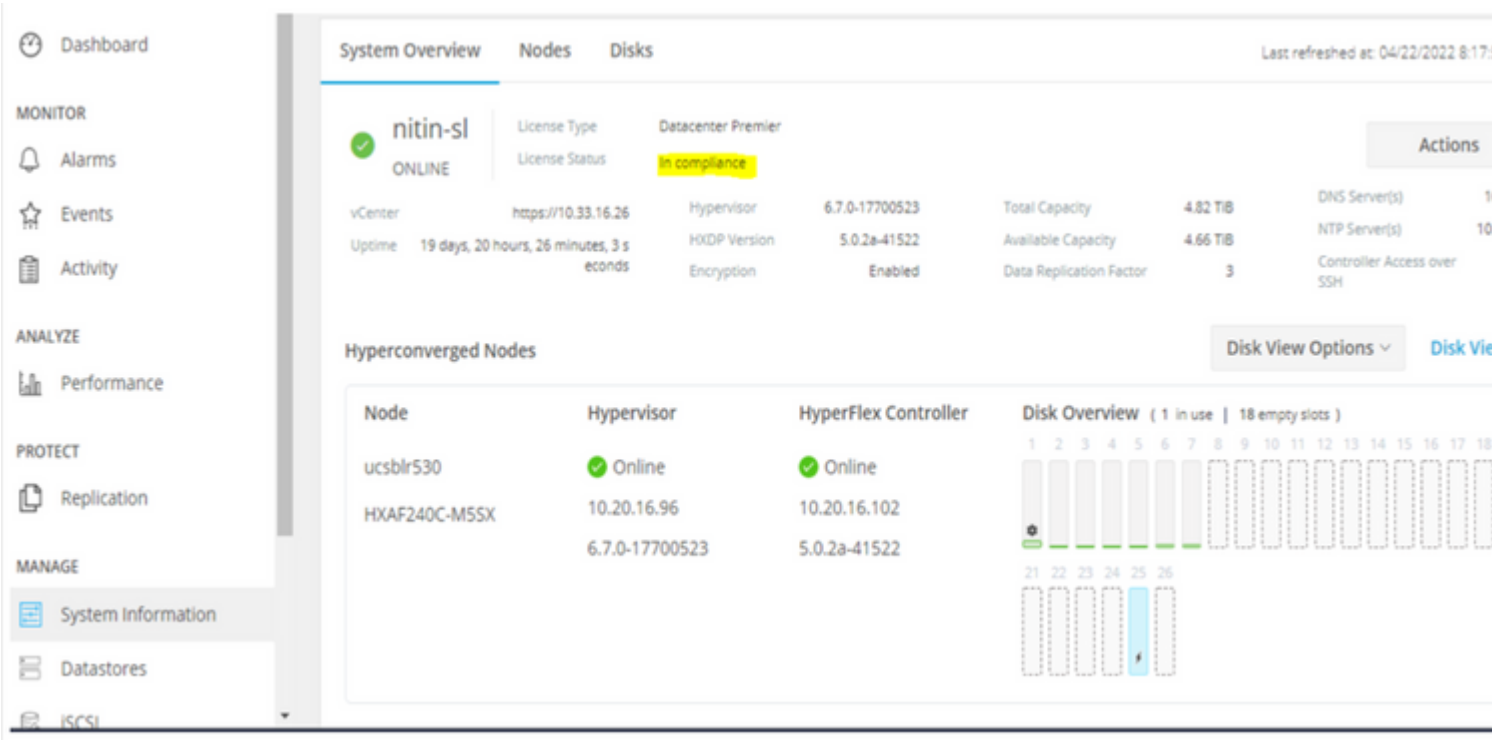
> **Observação**: nos clusters Hyperflex, o registro é válido por um ano, após o qual o Hyperflex tenta registrar-se novamente de forma que nenhuma interação humana seja necessária.

Política de aplicação rígida

Da versão HXDP 5.0(2a) em diante, alguns recursos são bloqueados da GUI do Hyperflex Connect se o cluster não estiver em conformidade com a licença.

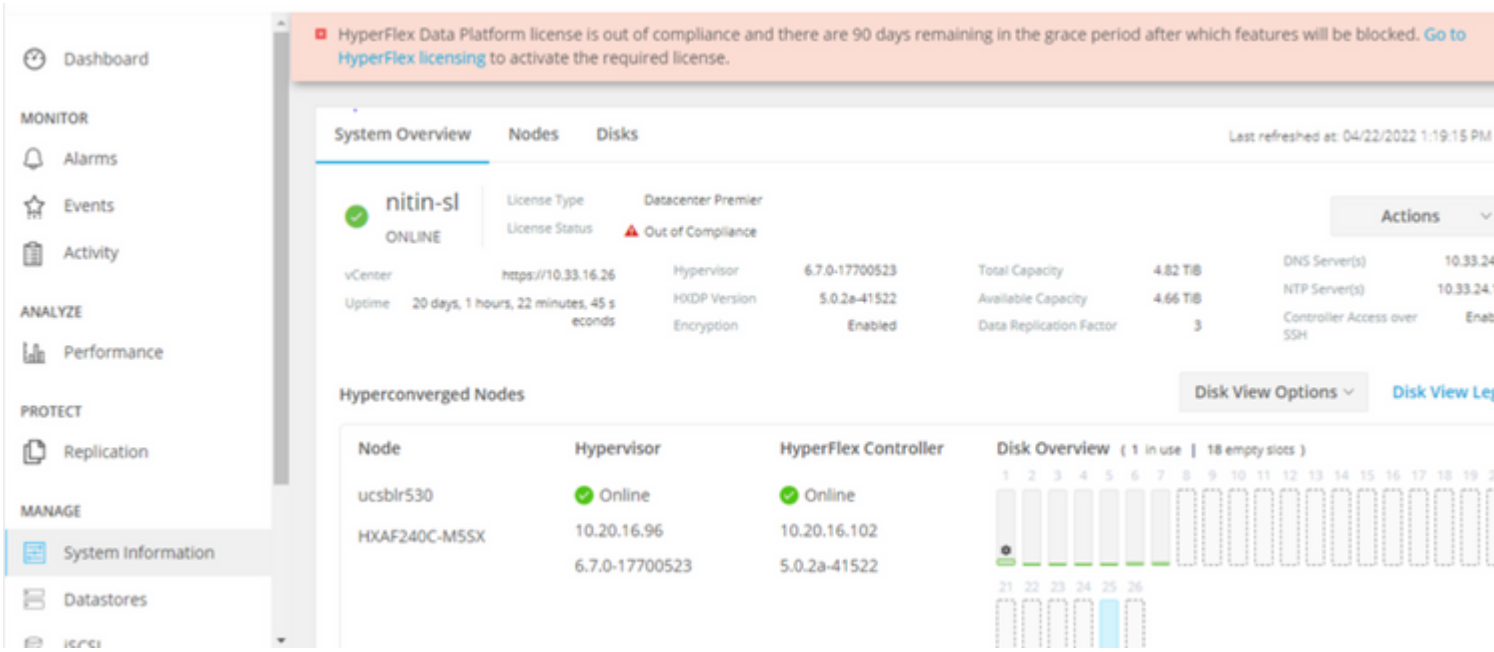
Cenários de exemplo de status de licença:

Neste cenário, o cluster é **In compliance** com o **License Status**

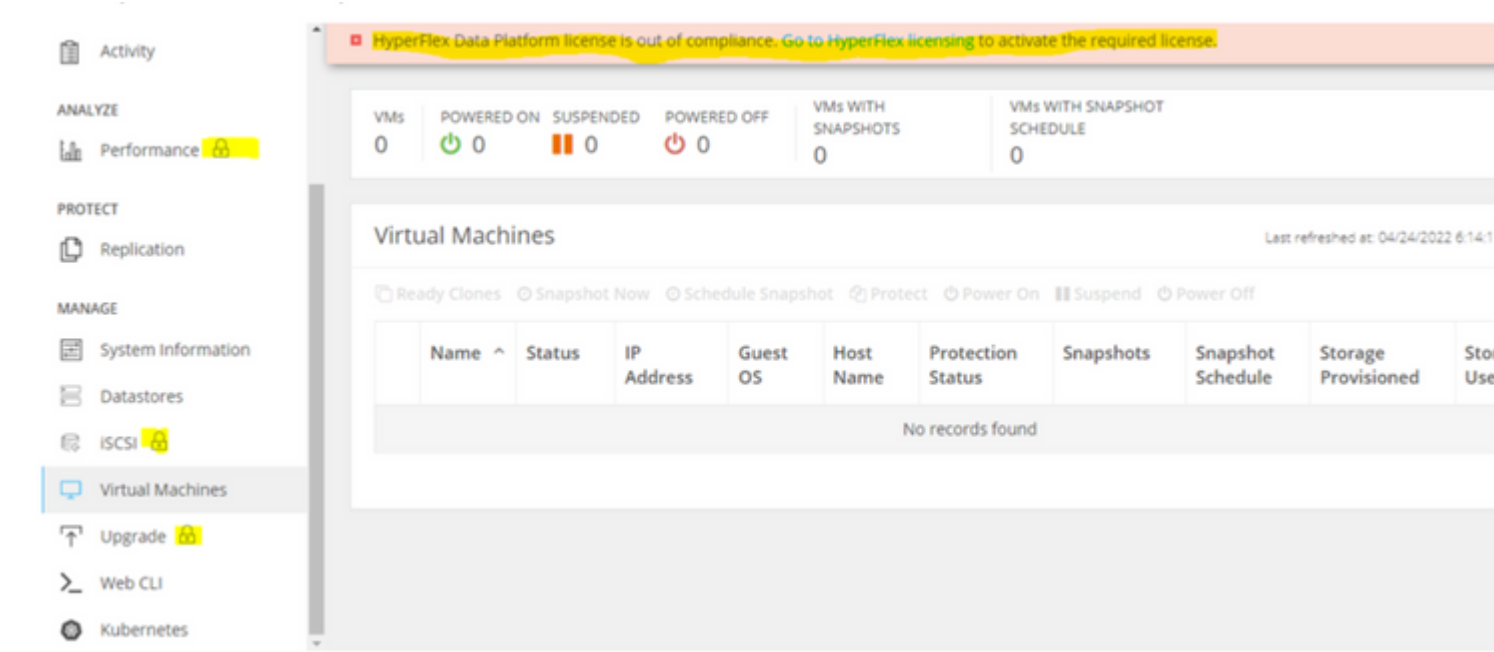


No próximo cenário, o cluster é registrado, mas o **License Status** é **Out of Compliance** e o período de carência está entre um (1) a noventa (90) dias.

Nesse caso, nenhum recurso é bloqueado, mas um banner é exibido na parte superior do menu solicitando que você ative a licença necessária antes que o período de cortesia expire.



Neste cenário, o cluster é registrado, o **License Status** é **Out of Compliance** e o período de carência é zero (0).



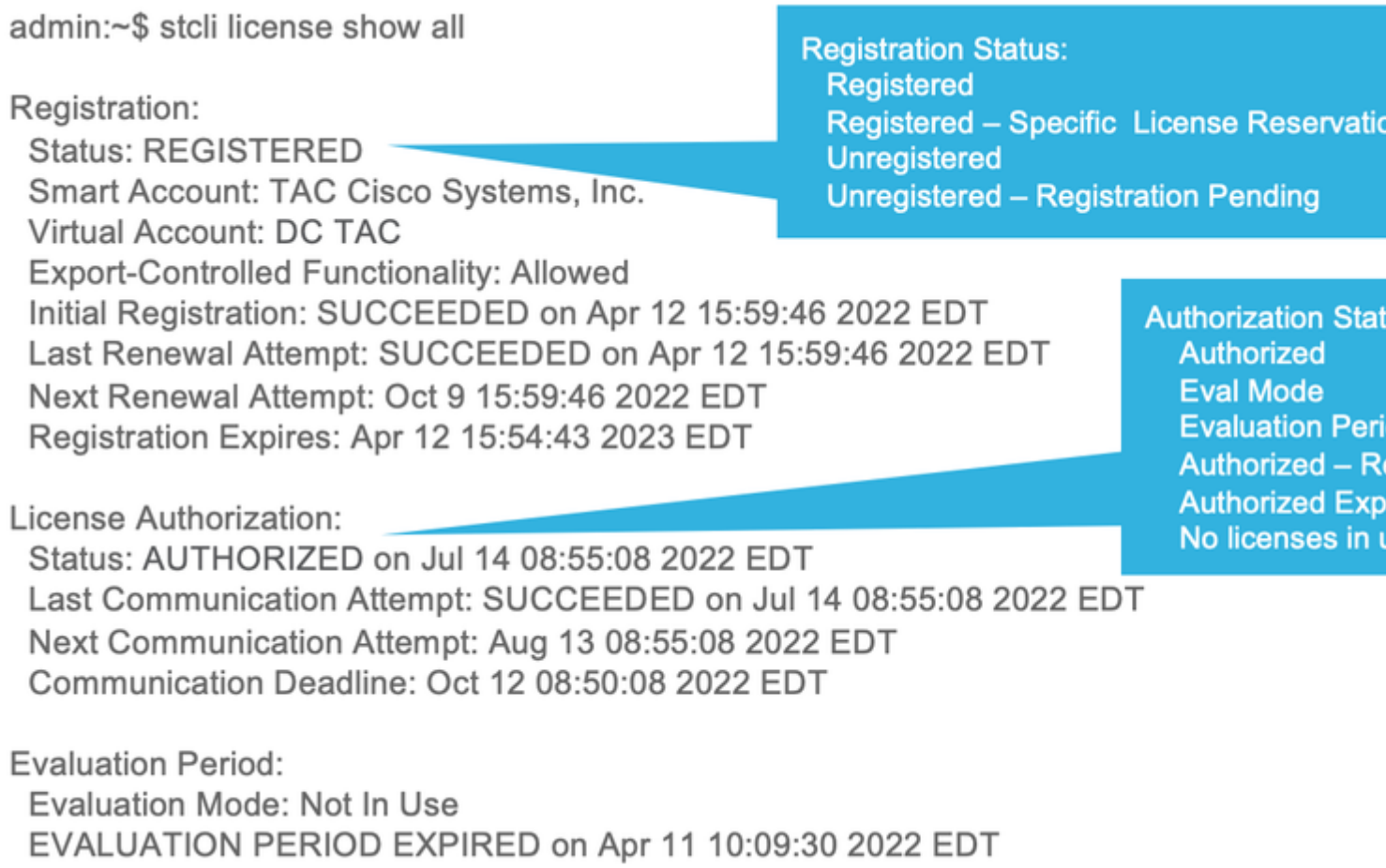
Configurar

Para orientação sobre como registrar o Hyperflex no seu **Smart License** verifique [este vídeo.]

Verificar

Confirme se a configuração está funcionando corretamente.

Verifique o status da licença via CLI. Exibir o status do registro e o status da autorização.



Troubleshooting

Há alguns cenários comuns em que esses dois status podem falhar, ambos causados pela mesma causa raiz.

Cenário 1: Conectividade HTTP/HTTPs

O registro de licença passa por TCP e, mais especificamente, por HTTP e HTTPS, portanto, é essencial permitir essa comunicação.

Teste a conectividade de cada um **Storage Controller VM** (SCVM), mas principalmente de **Cluster Management IP** (CMIP) SCVM.

```
curl https://tools.cisco.com/its/service/oddce/services/DDCEService
```

Você deve obter a saída mostrada no exemplo, caso contrário, isso significa que o tráfego está bloqueado.

```
<h1>DDCEService</h1>
```

```
 <p>Hi there, this is an AXIS service!</p>
 <i>Perhaps there will be a form for invoking the service here...</i>
```

Se a saída recebida for diferente da saída anterior, confirme a conectividade e verifique se as portas estão abertas com estes comandos:

```
ping tools.cisco.com -c 5
nc -zv tools.cisco.com 80
nc -zv tools.cisco.com 443
```

Cenário 2: Problemas de proxy

Às vezes, um proxy é configurado entre todos os clientes Web e servidores Web públicos quando eles realizam inspeções de segurança do tráfego.

Nesse caso, entre o SCVM com o CMIP e cisco.com, confirme se o proxy já está configurado no cluster (como mostrado no exemplo).

<#root>

```
hxshell:/var/log/springpath$ stcli services sch show
cloudEnvironment: production
enabled: True
emailAddress: johndoe@example.com
portalUrl:
```

enableProxy: True

```
proxyPassword:
encEnabled: True
proxyUser:
cloudAsupEndpoint: https://diag.hyperflex.io/
proxyUrl:
proxyPort: 0
```

se o proxy mostrar já configurado, teste a conectividade com o URL do proxy ou o endereço IP junto com a porta configurada.

```
curl -v --proxy https://url:
```

https://tools.cisco.com/its/service/oddce/services/DDCEService

```
curl -v --proxy <Proxy IP>:<Proxy Port> https://tools.cisco.com/its/service/oddce/services/DDCEService
```

Além disso, teste a conectividade com o proxy.

```
nc -vzw2 x.x.x.x 8080
```

Cenário 3: ambiente de nuvem

Em determinadas situações, o ambiente de nuvem é definido como **devtest**, o que causa falha no registro. Neste exemplo, ele está definido como **production.**

<#root>

```
hxshell:/var/log/springpath$ stcli services sch show
```

```
cloudEnvironment: production
```

```
cloudAsupEndpoint: https://diag.hyperflex.io/
portalUrl:
proxyPort: 0
enabled: True
encEnabled: True
proxyUser:
proxyPassword:
enableProxy: True
emailAddress: johndoe@example.com
proxyUrl:
```

A partir dos registros, você pode ver erros específicos quando o ambiente é definido incorretamente como **devtest**.

```
cat hxLicenseSvc.log | grep -ia "Name or service not known"
2021-09-01-18:27:11.557 [] [Thread-40] ERROR event_msg_sender_log - sch-alpha.cisco.com: Name or service
```

Dica: da versão 5.0(2a), o **usuário diag** está disponível para permitir que os usuários tenham mais privilégios para solucionar problemas com acesso a pastas restritas e comandos que não são acessíveis através da linha de comando **priv**, que foi introduzida na versão 4.5.x do Hyperflex.

Você pode alterar o tipo de ambiente para **production** e repita o registro.

```
diag# stcli services sch set --email johndoe@example.com --environment production --e
```

Cenário 4: protocolo de status de certificados online (OCSP)

A Hyperflex utiliza OCSP e **Certificate Revocation Lists** (CRL) para validar certificados HTTPS durante o processo de registro de licença.

Esses protocolos são projetados para distribuir o status de revogação por HTTP. As mensagens CRLs e OCSP são documentos públicos que indicam o status de revogação de certificados X.509 quando a validação OCSP falha e o registro de licença também falha.

> **Dica**: se o OCSP falhar, significa que um dispositivo de segurança no meio interrompe a conexão HTTP

Para confirmar se a validação do OCSP é boa, você pode tentar fazer o download do arquivo para sua partição CMIP SCVM/**tmp**, como mostrado no exemplo.

```
hxshell:~$cd /tmp
hxshell:/tmp$ wget http://www.cisco.com/security/pki/trs/ios_core.p7b
--2022-08-18 00:13:37-- http://www.cisco.com/security/pki/trs/ios_core.p7b
Resolving www.cisco.com (www.cisco.com)... x.x.x.x aaaa:aaaa:aaaa:aaaa::aaaa
Connecting to www.cisco.com (www.cisco.com)|x.x.x.x|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 25799 (25K)
Saving to: 'ios_core.p7b'

ios_core.p7b 100%[=========================================================================================

2022-08-18 00:13:37 (719 KB/s) - 'ios_core.p7b' saved [25799/25799]

hxshell:/tmp$ ls -lath ios*
-rw-rw-r-- 1 diag diag 26K Jun 30 18:00 ios_core.p7b
-rw-rw-r-- 1 diag diag 26K Jun 30 18:00 ios_core.p7b.1
-rw-rw-r-- 1 diag diag 26K Jun 30 18:00 ios_core.p7b.2
-rw-rw-r-- 1 diag diag 26K Jun 30 18:00 ios_core.p7b.3
-rw-r--r-- 1 admin springpath 26K Jun 30 18:00 ios_core.p7b.4
```

Cenário 5: Certificado Alterado

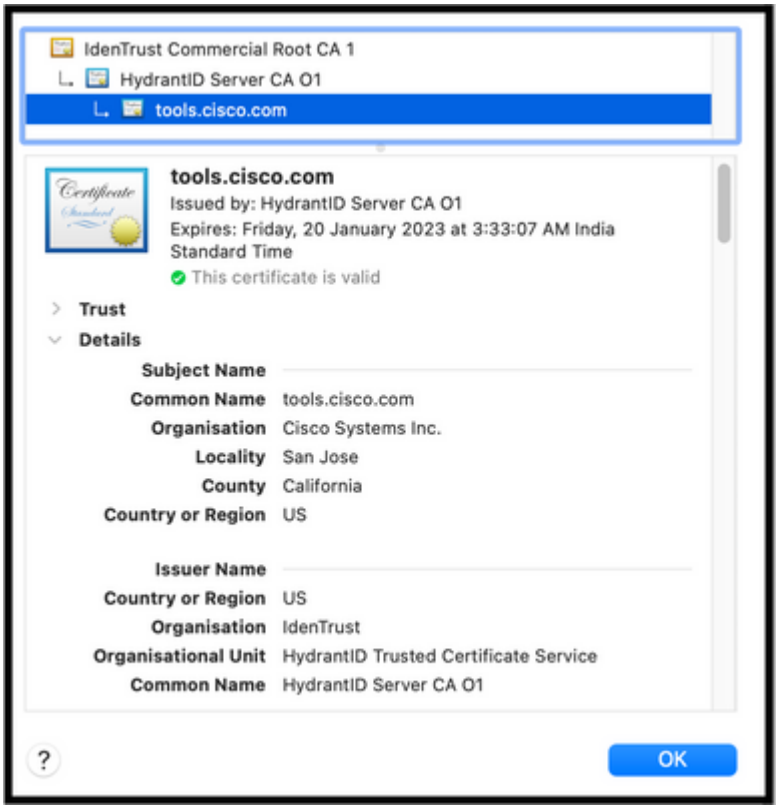
Em algumas redes, os dispositivos de segurança de proxy e firewall são executados **Secure Sockets Layer** (SSL)

e podem corromper o certificado que a Hyperflex espera receber de **tools.cisco.com:443**.

Para verificar se o certificado não foi alterado por um proxy ou firewall, no SCVM que contém o CMIP, execute o comando:

```
diag# openssl s_client -connect tools.cisco.com:443 -showcerts < /dev/null
```

é importante observar que a **Subject Name** e **Issuer Name** as informações devem corresponder ao certificado mostrado neste exemplo.



> **Aviso**: se pelo menos um campo no assunto ou no emissor for diferente, o registro falhará. Uma regra de desvio na Inspeção SSL de segurança para IPs de gerenciamento de Cluster Hyperflex e **tools.cisco.com:443** pode corrigir isso.

Neste exemplo, você pode ver como validar as mesmas informações recebidas do certificado no Hyperflex CMIP SCVM.

<#root>

```
hxshell:~$ su diag
diag# openssl s_client -connect tools.cisco.com:443 -showcerts < /dev/null
CONNECTED(00000003)
depth=2
```

C = US, O = IdenTrust, CN = IdenTrust Commercial Root CA 1

verify return:1
depth=1

C = US, O = IdenTrust, OU = HydrantID Trusted Certificate Service,

CN = HydrantID Server CA O1

verify return:1
depth=0

CN = tools.cisco.com, O = Cisco Systems Inc., L = San Jose, ST = California, C = US

verify return:1

Certificate chain
0 s:/

CN=tools.cisco.com

/

O=Cisco Systems Inc.

/

L=San Jose

/

ST=California

/

C=US

i:/

C=US

/

O=IdenTrust

/

OU=HydrantID Trusted Certificate Service

/C

N=HydrantID Server CA O1

...
<TRUNCATED>
...
1 s:/

C=US

/

O=IdenTrust

/

OU=HydrantID Trusted Certificate Service

/

CN=HydrantID Server CA O1

i:/

C=US

/

O=IdenTrust

/

CN=IdenTrust Commercial Root CA 1

...
<TRUNCATED>
...
2 s:/

C=US

/

O=IdenTrust

/

CN=IdenTrust Commercial Root CA 1

i:/

C=US

/

O=IdenTrust

/

CN=IdenTrust Commercial Root CA 1

...
<TRUNCATED>
...

Server certificate
subject=/

CN=tools.cisco.com

/

O=Cisco Systems Inc.

/

L=San Jose

/

```
ST=California

/

C=US


issuer=/

C=US

/

O=IdenTrust

/

OU=HydrantID Trusted Certificate Service

/

CN=HydrantID Server CA O1


---
...
<TRUNCATED>
...
---
DONE
```

Procedimento adicional

Esse procedimento pode ser aproveitado se os cenários cobertos forem bem-sucedidos ou resolvidos, mas o registro de licença ainda falhar.

Cancelar o registro da licença

```
hxshell:~$stcli license disable
hxshell:~$stcli license enable
hxshell:~$stcli license deregister
```

Adquira um novo token do licenciamento inteligente, reinicie o processo de licenciamento e repita o registro da licença.

```
hxshell:~$priv service hxLicenseSvc stop
hxshell:~$priv service hxLicenseSvc start
hxshell:~$stcli license register --idtoken IDTOKEN --force
```

Informações Relacionadas

- **Plataforma de dados Cisco HyperFlex HX - Guias do usuário final**

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.