Fehlerbehebung bei Problemen mit der Hyperflex-Lizenzregistrierung

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie die häufigsten Probleme mit der Hyperflex-Registrierungslizenz beheben.

Voraussetzungen

Cisco empfiehlt, dass Sie über Grundkenntnisse in diesen Themen verfügen:

- HyperFlex Connect
- Lizenzregistrierung
- HTTP/HTTPS

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf:

Hyperflex Data Platform (HXDP) 5.0.(2a) und höher

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Was ist Smart License?

Cisco Smart Software Licensing (Smart Licensing) ist eine intelligente Cloud-basierte Lösung für das Lizenzmanagement, die die drei Kernfunktionen (Kauf, Management und Reporting) Ihres gesamten Unternehmens vereinfacht.

Sie können hier auf Ihr Smart-Lizenzkonto zugreifen.

Wie funktionieren Lizenzen auf Hyperflex?

Cisco Hyperflex integriert mit **Smart Licensing** und wird beim Erstellen eines Hyperflex-Storage-Clusters standardmäßig automatisch aktiviert.

Damit Ihr Hyperflex-Storage-Cluster Lizenzen nutzen und melden kann, müssen Sie es jedoch bei registrieren. **Cisco Smart Software Manager** (SSM) über Ihre **Cisco Smart Account.**

A **Smart Account** ist ein Cloud-basiertes Repository, das umfassende Transparenz und Zugriffskontrolle für alle erworbenen Cisco Softwarelizenzen und Produktinstanzen in Ihrem Unternehmen bietet.

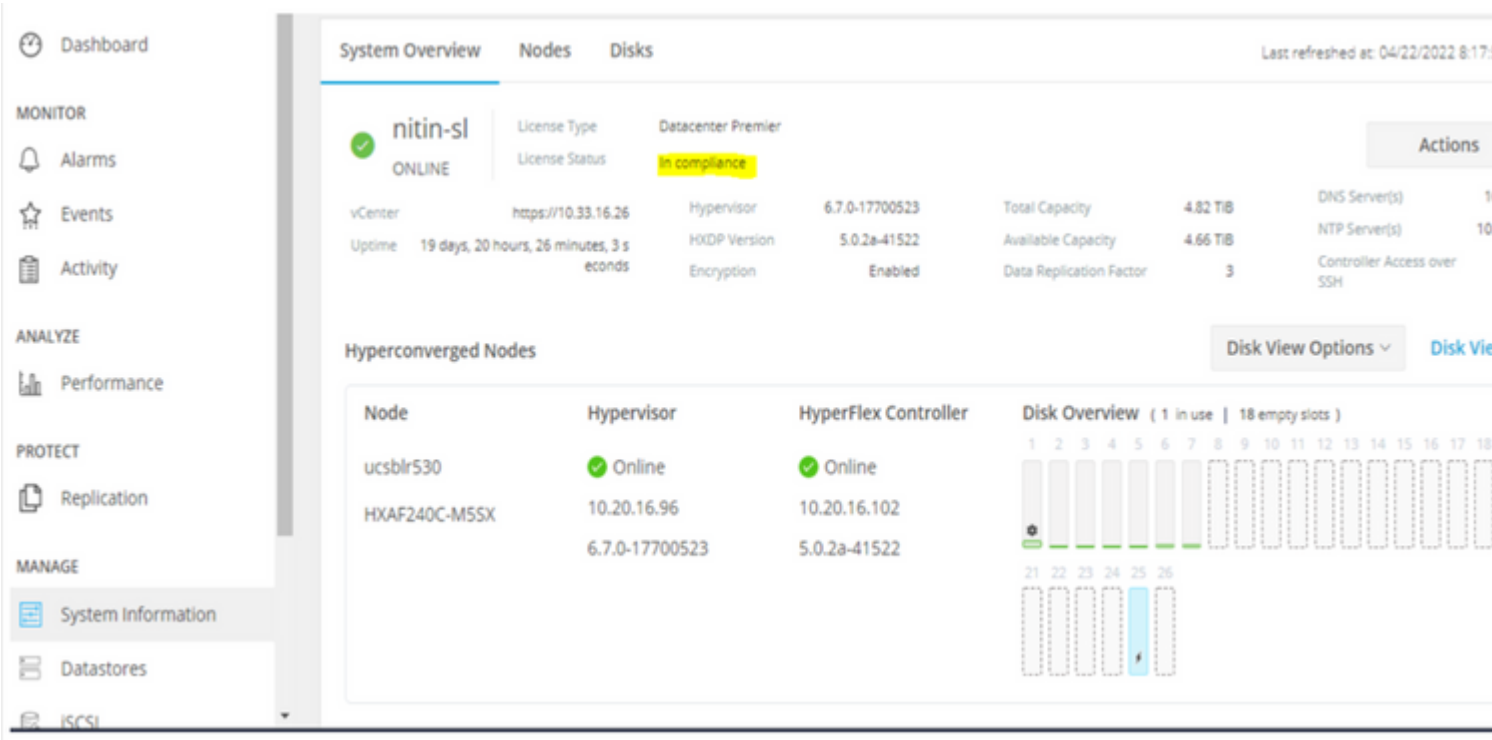
> **Hinweis**: Bei Hyperflex-Clustern ist die Registrierung ein Jahr lang gültig. Danach versucht Hyperflex automatisch, sich neu zu registrieren, sodass keine menschliche Interaktion erforderlich ist.

Strikte Durchsetzungsrichtlinie

Ab Version HXDP 5.0(2a) werden einige Funktionen von der Hyperflex Connect-GUI blockiert, wenn der Cluster nicht mit der Lizenz konform ist.

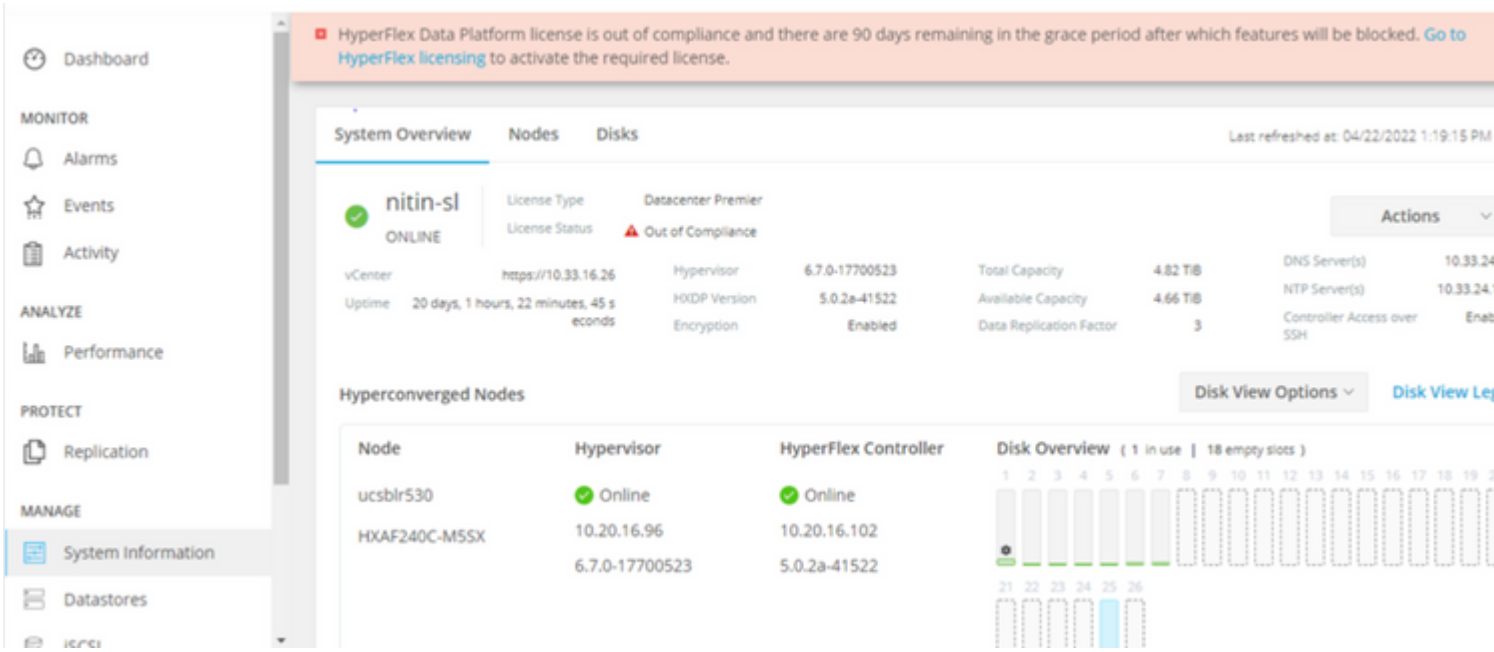
Lizenzstatus-Beispielszenarien:

In diesem Szenario ist der Cluster **In compliance** mit dem **License Status**

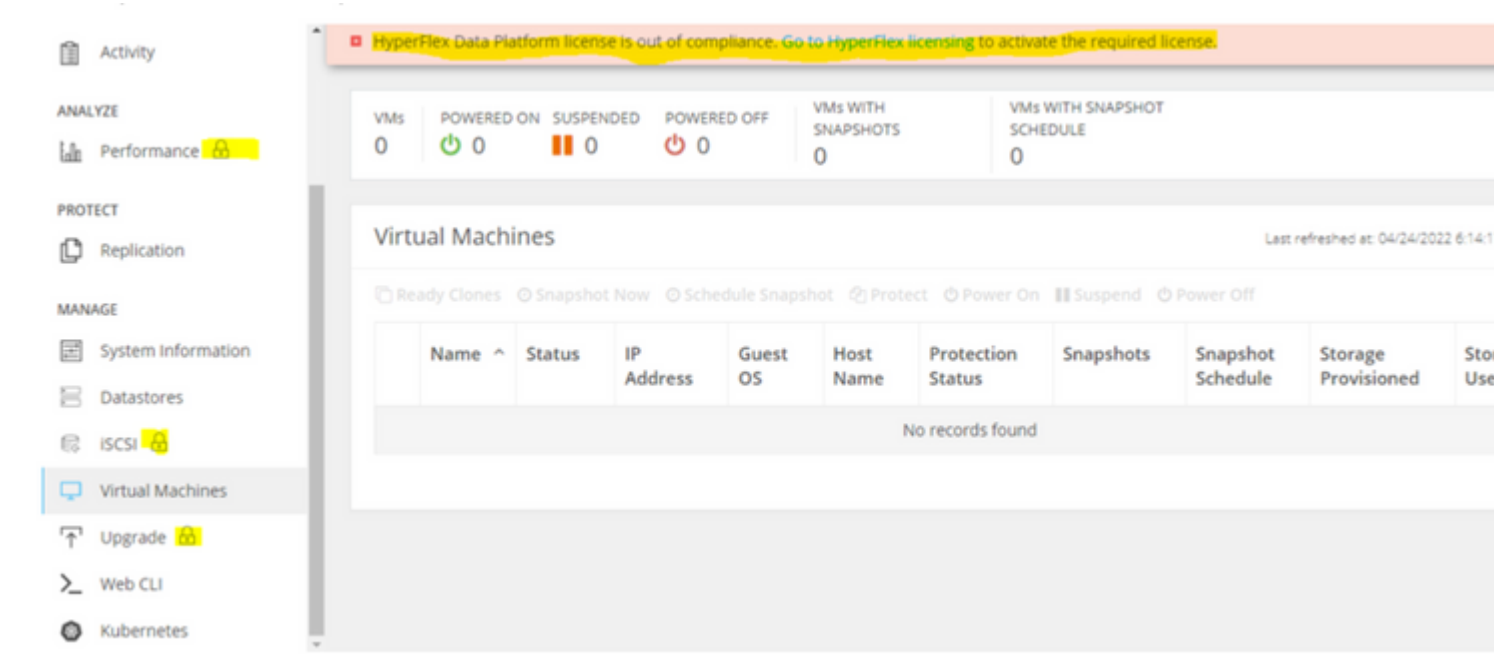


Im nächsten Szenario wird der Cluster registriert, aber die **License Status** ist **Out of Compliance** und die Nachfrist zwischen einem (1) und neunzig (90) Tagen beträgt.

In diesem Fall werden keine Funktionen blockiert, aber oben im Menü wird ein Banner angezeigt, das Sie auffordert, die erforderliche Lizenz zu aktivieren, bevor die Kulanzfrist abläuft.



In diesem Szenario wird der Cluster registriert, der **License Status** ist **Out of Compliance** und die Kulanzfrist ist Null (0).



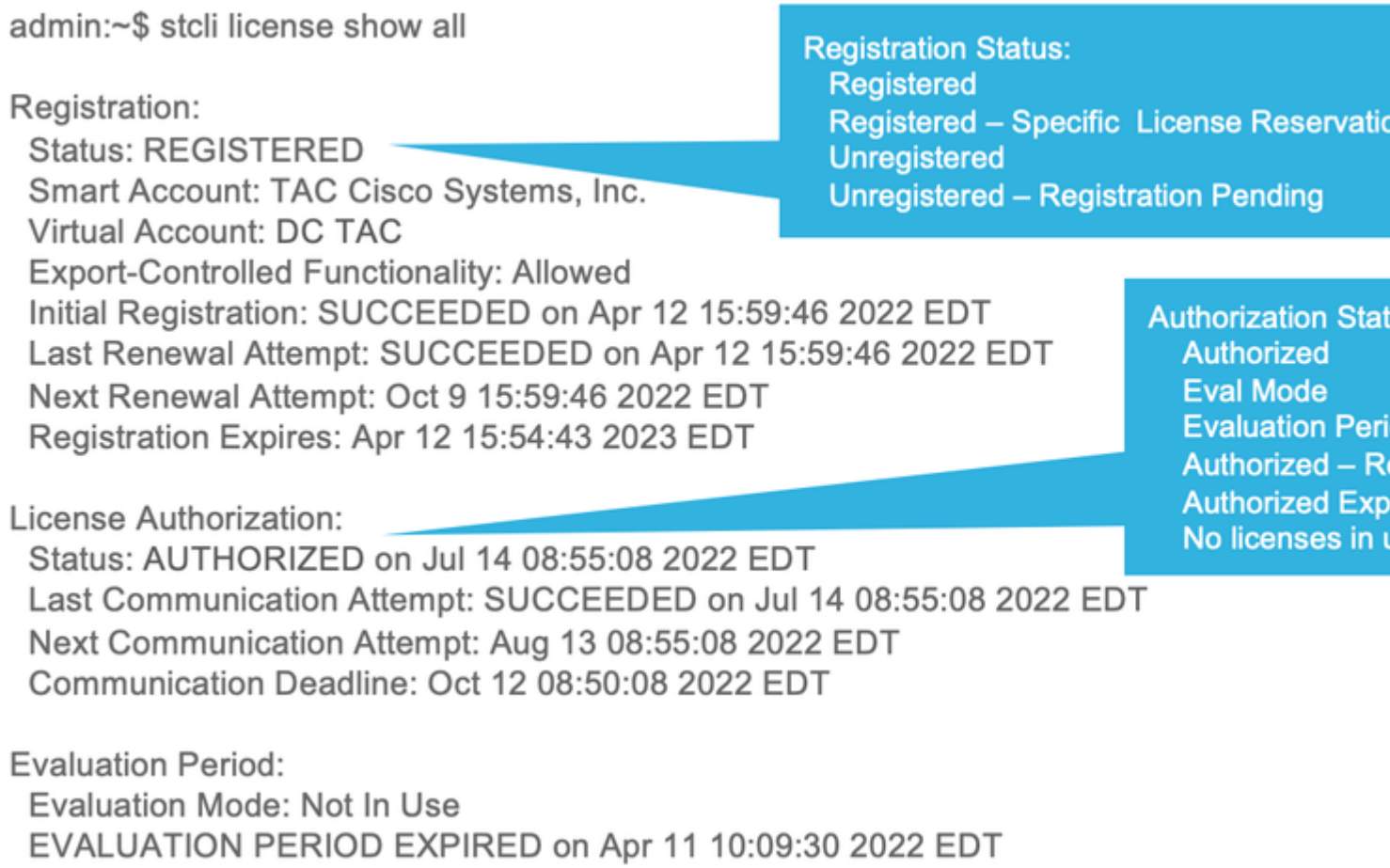
Konfigurieren

Für Hinweise zur Registrierung von Hyperflex bei Ihrem **Smart License** Account, sehen Sie sich dieses Video.

Überprüfung

Bestätigen Sie, dass Ihre Konfiguration ordnungsgemäß funktioniert.

Überprüfen des Lizenzstatus über die CLI Anzeigen des Registrierungsstatus und des Autorisierungsstatus



Fehlerbehebung

Es gibt einige gängige Szenarien, in denen diese beiden Status fehlschlagen können, die beide von derselben Ursache verursacht werden.

Szenario 1: HTTP-/HTTP-Verbindungen

Die Lizenzregistrierung erfolgt über TCP und insbesondere über HTTP und HTTPS. Daher muss diese Kommunikation unbedingt zugelassen werden.

Testen der Verbindungen von jedem **Storage Controller VM** (SCVM), aber hauptsächlich von **Cluster Management IP** (CMIP)-SCVM

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

Sie müssen die im Beispiel gezeigte Ausgabe abrufen, andernfalls bedeutet dies, dass der Datenverkehr blockiert wird.

```
 <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>
```

Wenn sich die empfangenen Daten von der vorherigen Ausgabe unterscheiden, überprüfen Sie die Verbindung, und stellen Sie mithilfe der folgenden Befehle sicher, dass die Ports geöffnet sind:

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

Szenario 2: Proxy-Probleme

Manchmal wird ein Proxy zwischen allen Web-Clients und öffentlichen Web-Servern konfiguriert, wenn diese Sicherheitsinspektionen des Datenverkehrs durchführen.

Überprüfen Sie in diesem Fall zwischen der SCVM mit dem CMIP und cisco.com, ob der Proxy bereits im Cluster konfiguriert ist (wie im Beispiel gezeigt).

<#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
```

Wenn der Proxy bereits konfiguriert ist, testen Sie die Verbindung entweder mit der Proxy-URL oder der IP-Adresse zusammen mit dem konfigurierten Port.

```
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
```

Testen Sie außerdem die Verbindung zum Proxy.

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

Szenario 3: Cloud-Umgebung

In bestimmten Situationen wird die Cloud-Umgebung auf "**entschlüsseln"** gesetzt, was zu einem Registrierungsfehler führt. In diesem Beispiel ist festgelegt auf **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:
```

Aus Protokollen können Sie bestimmte Fehler anzeigen, wenn die Umgebung fälschlicherweise als **devtest** festgelegt ist.

```
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
```

> **Tipp:** In der Version 5.0(2a) **steht** Ihnen diag user zur Verfügung, um Benutzern mehr Rechte für die Fehlerbehebung mit Zugriff auf beschränkte Ordner und Befehle zu gewähren, auf die über die **priv-**Befehlszeile, die in Hyperflex 4.5.x eingeführt wurde, nicht zugegriffen werden kann.

Sie können den Umgebungstyp in **production** und versuchen Sie es erneut.

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

Szenario 4: Online Certificate Status Protocol (OCSP)

Hyperflex nutzt OCSP und **Certificate Revocation Lists** (CRL)-Server, um HTTPS-Zertifikate während des Registrierungsprozesses für Lizenzen zu validieren.

Diese Protokolle sind darauf ausgelegt, den Sperrstatus über HTTP zu verteilen. CRLs und OCSP-Nachrichten sind öffentliche Dokumente, die den Sperrstatus von X.509-Zertifikaten angeben, wenn die OCSP-Validierung fehlschlägt und die Lizenzregistrierung ebenfalls fehlschlägt.

> **Tipp:** Wenn OCSP ausfällt, bedeutet dies, dass ein zwischengeschaltetes Sicherheitsgerät die HTTP-Verbindung unterbricht.

Um zu überprüfen, ob die OCSP-Validierung ordnungsgemäß ist, können Sie versuchen, die Datei auf Ihre CMIP SCVM-/**tmp-**Partition herunterzuladen, wie im Beispiel gezeigt.

```
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
```

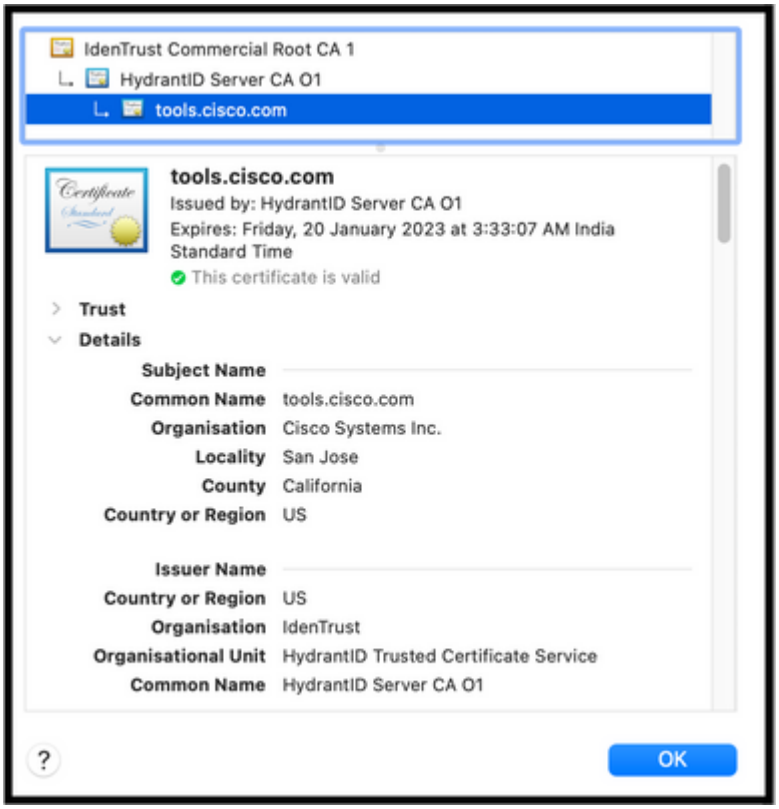
Szenario 5: Zertifikat geändert

In einigen Netzwerken werden Proxy- und Firewall-Sicherheitsgeräte ausgeführt **Secure Sockets Layer** (SSL)-Überprüfung und sie können das Zertifikat beschädigen, das Hyperflex von **tools.cisco.com:443** erwartet.

Um zu überprüfen, ob das Zertifikat nicht von einem Proxy oder einer Firewall geändert wird, führen Sie in der SCVM, die die CMIP enthält, den folgenden Befehl aus:

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

es ist wichtig zu bemerken, dass die **Subject Name** und **Issuer Name** Die Informationen müssen mit dem in diesem Beispiel gezeigten Zertifikat übereinstimmen.



> **Warnung:** Wenn mindestens ein Feld in der Betreffzeile oder im Aussteller anders ist, schlägt die Registrierung fehl. Eine Umgehungsregel in der SSL-Sicherheitsüberprüfung für Hyperflex-Cluster-Management-IPs und **tools.cisco.com:443** kann dies beheben.

In diesem Beispiel sehen Sie, wie Sie die gleichen Informationen, die Sie vom Zertifikat erhalten haben, in Hyperflex CMIP SCVM validieren können.

<#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
```

Zusätzliches Verfahren

Dieses Verfahren kann verwendet werden, wenn die Szenarien erfolgreich sind oder behoben wurden, die Lizenzregistrierung jedoch weiterhin fehlschlägt.

Lizenz abmelden

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

Erwerben Sie ein neues Token von Smart Licensing, starten Sie den Lizenzierungsprozess neu, und wiederholen Sie die Lizenzregistrierung.

```
hxshell:~$priv service hxLicenseSvc stop
hxshell:~$priv service hxLicenseSvc start
```

```
hxshell:~$stcli license register --idtoken IDTOKEN --force
```

Zugehörige Informationen

- **Cisco HyperFlex HX Data Platform - Benutzerhandbücher**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.