

排除Hyperflex許可證註冊問題

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[什麼是智慧許可證](#)

[許可證如何在Hyperflex上工作](#)

[嚴格執行策略](#)

[設定](#)

[驗證](#)

[疑難排解](#)

[場景1:HTTP/HTTPS連線](#)

[案例2：代理問題](#)

[案例3：雲環境](#)

[案例4：線上憑證狀態通訊協定\(OCSP\)](#)

[案例5：憑證已變更](#)

[附加程式](#)

[相關資訊](#)

簡介

本文說明如何解決最常見的Hyperflex註冊許可證問題。

必要條件

需求

思科建議您瞭解以下主題的基本知識：

- Hyperflex Connect
- 授權註冊
- HTTP/HTTPS

採用元件

本檔案中的資訊是根據：

- Hyperflex資料程式(HXDP)5.0.(2a)及更高版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

什麼是智慧許可證


思科智慧許可 (智慧許可) 是一種基於雲的智慧軟體許可管理解決方案，可簡化整個組織的三個核心許可功能 (購買、管理和報告)。

您可以在此處訪問您的智慧許可證[帳戶](#)。

許可證如何在Hyperflex上工作

Cisco Hyperflex與智慧許可整合，在您建立Hyperflex儲存集群時，預設情況下會自動啟用該功能。但是，要使用Hyperflex儲存群集和報告許可證，您必須通過思科智慧帳戶向思科智慧軟體管理器 (SSM)註冊該群集。

智慧帳戶是一個基於雲的儲存庫，可讓您全面瞭解和控制所購買的所有思科軟體許可證和整個公司的產品例項。

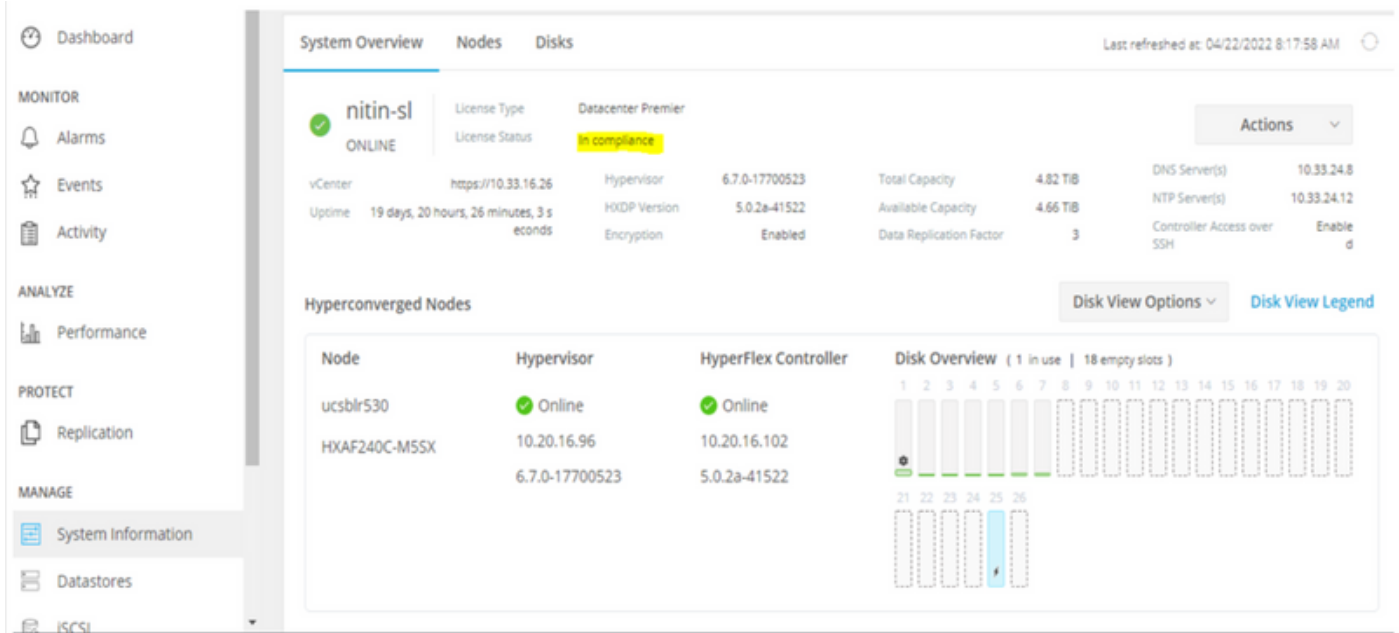
 註：在Hyperflex集群中，註冊有效期為一年。之後，Hyperflex會自動嘗試重新註冊，因此無需人工干預。

嚴格執行策略

從HXDP 5.0(2a)版本開始，如果群集不符合許可證，Hyperflex Connect GUI會阻止某些功能。

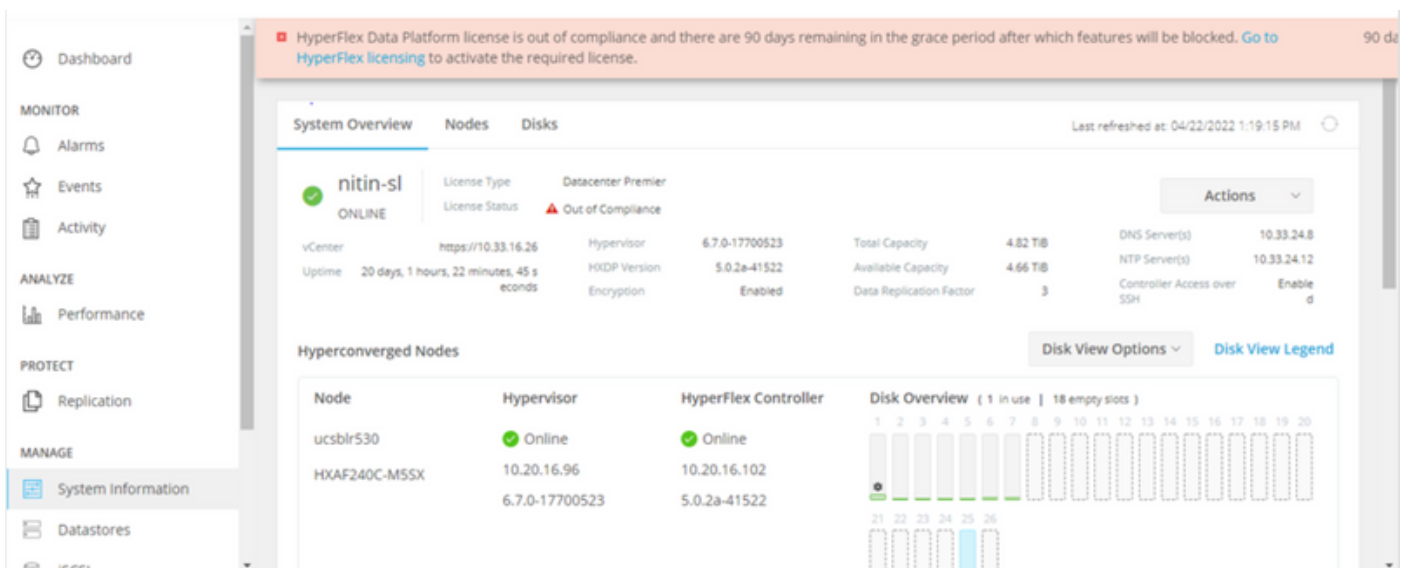
許可證狀態示例場景：

在此場景中，集群符合許可證狀態。

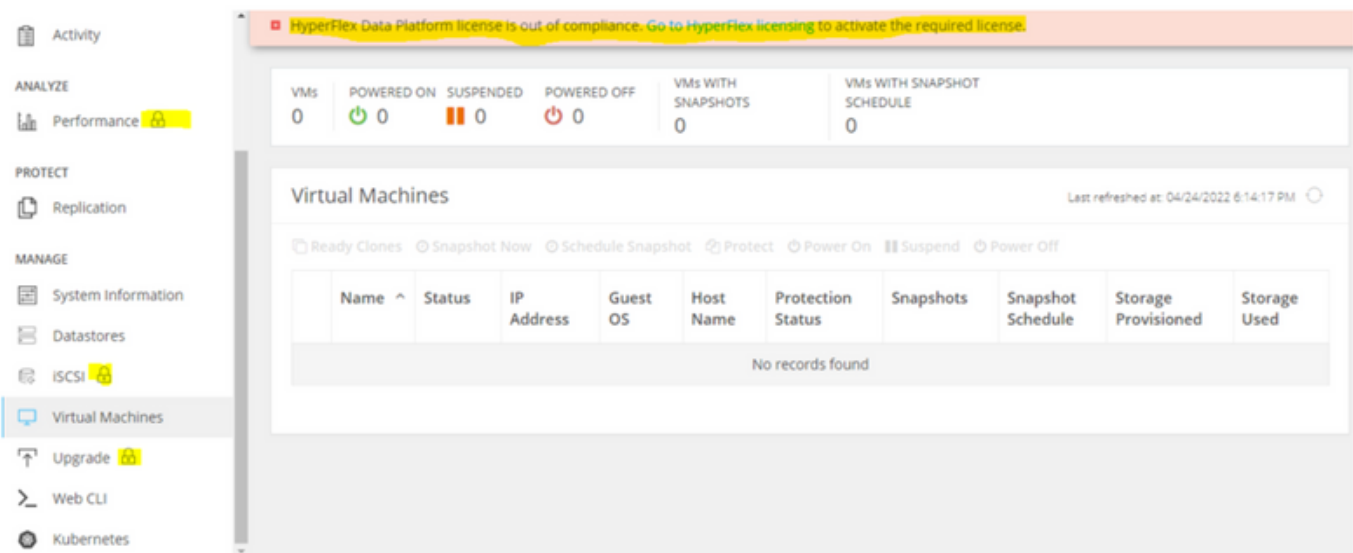


在下一個場景中，群集已註冊，但許可證狀態為不合規，寬限期為一(1)天至九十(90)天之間。

在這種情況下，不會阻止任何功能，但選單頂部會出現一個橫幅，提示您啟用所需的許可證，以防寬限期過期。



在此場景中，群集已註冊，許可證狀態為不合規，寬限期為零(0)。



設定

有關如何在您的智慧許可證帳戶中註冊Hyperflex的指導，請檢查[此影片](#)。

驗證

確認您的組態是否正常運作。

通過CLI驗證許可證狀態。檢視註冊狀態和授權狀態。

```
admin:~$ stcli license show all
```

Registration:

```
Status: REGISTERED
Smart Account: TAC Cisco Systems, Inc.
Virtual Account: DC TAC
Export-Controlled Functionality: Allowed
Initial Registration: SUCCEEDED on Apr 12 15:59:46 2022 EDT
Last Renewal Attempt: SUCCEEDED on Apr 12 15:59:46 2022 EDT
Next Renewal Attempt: Oct 9 15:59:46 2022 EDT
Registration Expires: Apr 12 15:54:43 2023 EDT
```

Registration Status:
Registered
Registered – Specific License Reservation
Unregistered
Unregistered – Registration Pending

License Authorization:

```
Status: AUTHORIZED on Jul 14 08:55:08 2022 EDT
Last Communication Attempt: SUCCEEDED on Jul 14 08:55:08 2022 EDT
Next Communication Attempt: Aug 13 08:55:08 2022 EDT
Communication Deadline: Oct 12 08:50:08 2022 EDT
```

Authorization Status:
Authorized
Eval Mode
Evaluation Period Expired
Authorized – Reserved
Authorized Expired
No licenses in use

Evaluation Period:

```
Evaluation Mode: Not In Use
EVALUATION PERIOD EXPIRED on Apr 11 10:09:30 2022 EDT
```

疑難排解

在某些常見情況下，這兩種狀態都可能失敗，但原因都是相同的。

場景1:HTTP/HTTPS連線

許可證註冊通過TCP進行，尤其是通過HTTP和HTTPS，因此允許此通訊至關重要。

測試來自每個儲存控制器VM(SCVM)(但主要來自群集管理IP(CMIP)SCVM的連線。

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

您必須取得範例中所示的輸出，否則就表示流量遭封鎖。

```
<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>
```

如果收到的輸出與先前的輸出不同，請確認連線並使用以下命令驗證埠是否已開啟：

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

案例2：代理問題

有時，當所有Web客戶端和公共Web伺服器對流量執行安全檢查時，會在它們之間配置Proxy。

在這種情況下，在具有CMIP的SCVM和cisco.com之間，驗證已在群集中配置代理（如示例所示）。

```
<#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
```

如果proxy顯示已設定，請使用代理URL或IP位址以及已設定的連線埠測試連線。

```
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
```

此外，測試與Proxy的連線。

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

案例3：雲環境

在某些情況下，雲環境設定為devtest，從而導致註冊失敗。在此示例中，將其設定為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:
```

從日誌中，當環境錯誤地設定為devtest時，您可以看到特定錯誤。

```
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
```

 提示：從5.0(2a)版本起，diag使用者可用於允許使用者擁有更多許可權進行故障排除，從而訪問無法通過priv command line (在Hyperflex 4.5.x版本中引入) 訪問的受限資料夾和命令。


您可以將環境型別更改為生產並重試註冊。

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

案例4：線上憑證狀態通訊協定(OCSP)

Hyperflex利用OCSP和憑證撤銷清單(CRL)伺服器來在授權註冊過程中驗證HTTPS憑證。

這些協定用於通過HTTP分發撤銷狀態。CRL和OCSP消息是公共文檔，指示X.509證書在OCSP驗證失敗後許可證註冊失敗時的吊銷狀態。

 提示：如果OCSP失敗，則表示介於二者之間的安全裝置會斷開HTTP連線。

為了確認OCSP驗證是否正常，您可以嘗試將檔案下載到CMIP SCVM/tmp分割槽，如示例所示。

```
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
```

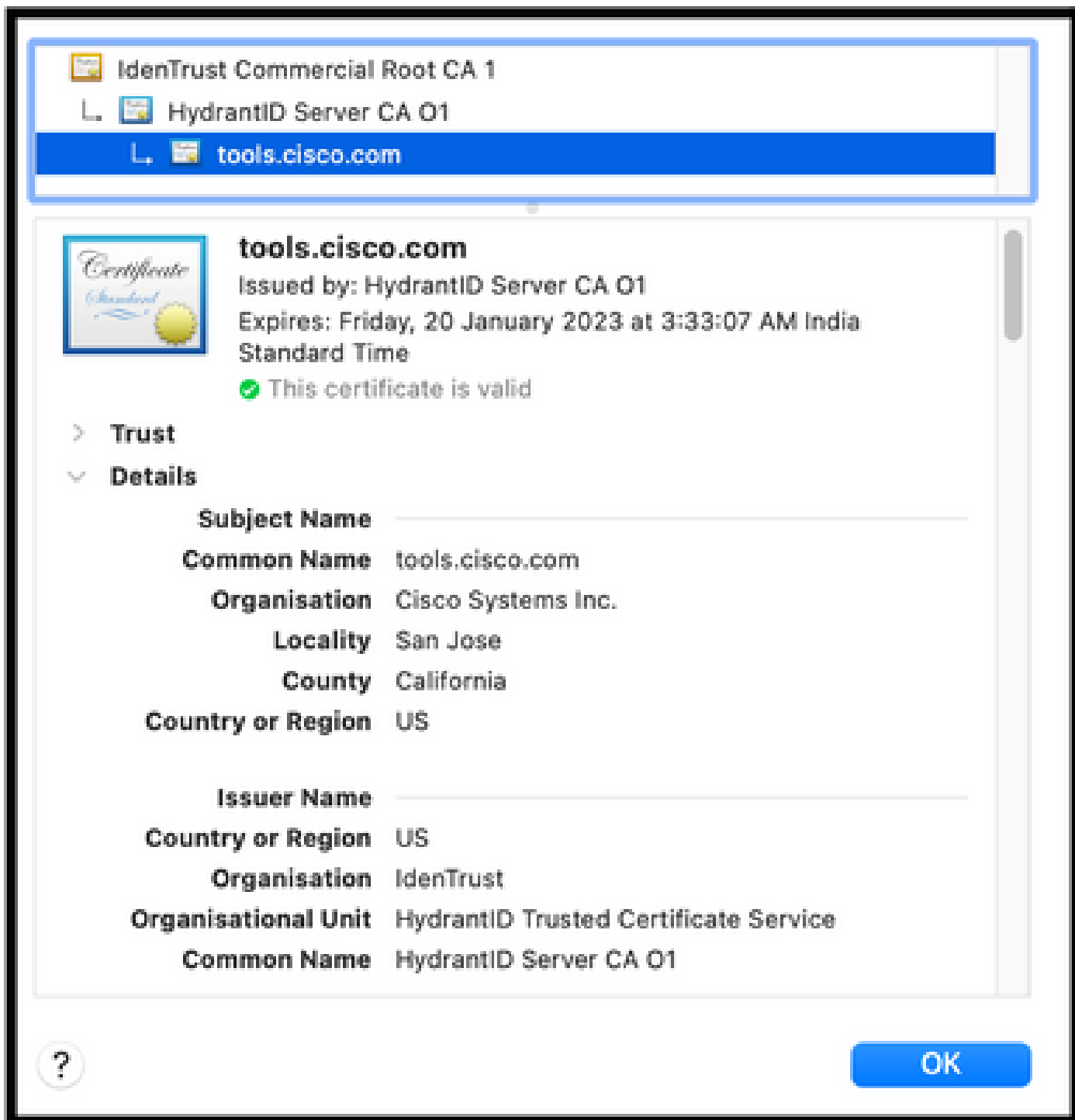
案例5：憑證已變更

在某些網路中，代理和防火牆安全裝置運行安全套接字層(SSL)檢查，並且可能會損壞Hyperflex預期會接收from tools.cisco.com:443的證書。

若要檢查代理或防火牆未更改證書，請在持有CMIP的SCVM中運行命令：

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

必須注意，「使用者名稱」和「頒發者名稱」資訊必須與本示例中所示的證書相匹配。



警告：如果主題或頒發者中的至少一個欄位不同，則註冊將失敗。適用於Hyperflex集群管理IP和tools.cisco.com:443的安全SSL檢查中的旁路規則可以解決此問題。

在此範例中，您可以看到如何在Hyperflex CMIP SCVM中驗證從憑證接收的相同資訊。

```
<#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 01

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 01

...

<TRUNCATED>

...

1 s:/

C=US

```
/
O=IdenTrust
/
OU=HydrantID Trusted Certificate Service
/
CN=HydrantID Server CA 01
```

```
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 01

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

附加程式

如果所涵蓋的場景成功或得到解決，但許可證註冊仍失敗，則可以使用此過程。

註銷許可證。

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

從智慧許可獲取新令牌，重新啟動許可過程，然後重試許可證註冊。

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

相關資訊

- [Cisco HyperFlex HX資料平台 — 最終使用手冊](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。