

排除Hyperflex许可证注册问题

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[什么是智能许可证](#)

[许可证如何在Hyperflex上工作](#)

[严格实施策略](#)

[配置](#)

[验证](#)

[故障排除](#)

[场景1:HTTP/HTTPS连接](#)

[场景2：代理问题](#)

[场景3：云环境](#)

[场景4：在线证书状态协议\(OCSP\)](#)

[场景5：证书已更改](#)

[附加程序](#)

[相关信息](#)

简介

本文档介绍如何解决最常见的Hyperflex注册许可证问题。

先决条件

要求

Cisco 建议您具有以下主题的基础知识：

- Hyperflex Connect
- 许可证注册
- HTTP/HTTPS

使用的组件

本文档中的信息基于：

- Hyperflex数据程序(HXDP)5.0.(2a)及更高版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

什么是智能许可证


思科智能许可（智能许可）是一种基于云的智能软件许可管理解决方案，可简化整个组织的三个核心许可功能（购买、管理和报告）。

您可以在此处访问智能许可证[帐户](#)。

许可证如何在Hyperflex上工作

Cisco Hyperflex与智能许可集成，在您创建Hyperflex存储集群时，默认情况下会自动启用该功能。但是，要使用Hyperflex存储群集和报告许可证，您必须通过思科智能帐户向思科智能软件管理器 (SSM)注册该群集。

智能帐户是一个基于云的存储库，提供对您公司内购买的所有思科软件许可证和产品实例的完全可视性和访问控制。

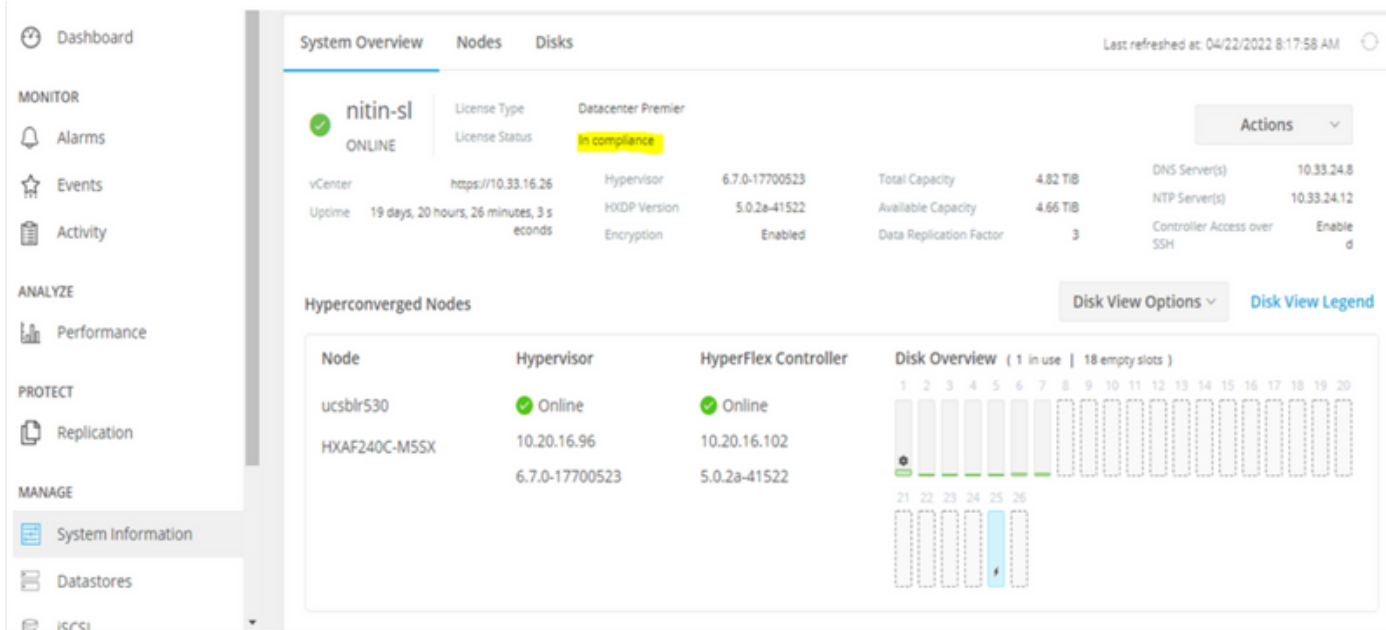
 注：在Hyperflex集群中，注册有效期为一年。之后，Hyperflex会自动尝试重新注册，因此无需人工交互。

严格实施策略

从HXDP 5.0(2a)版本开始，如果集群不符合许可证，则Hyperflex Connect GUI会阻止某些功能。

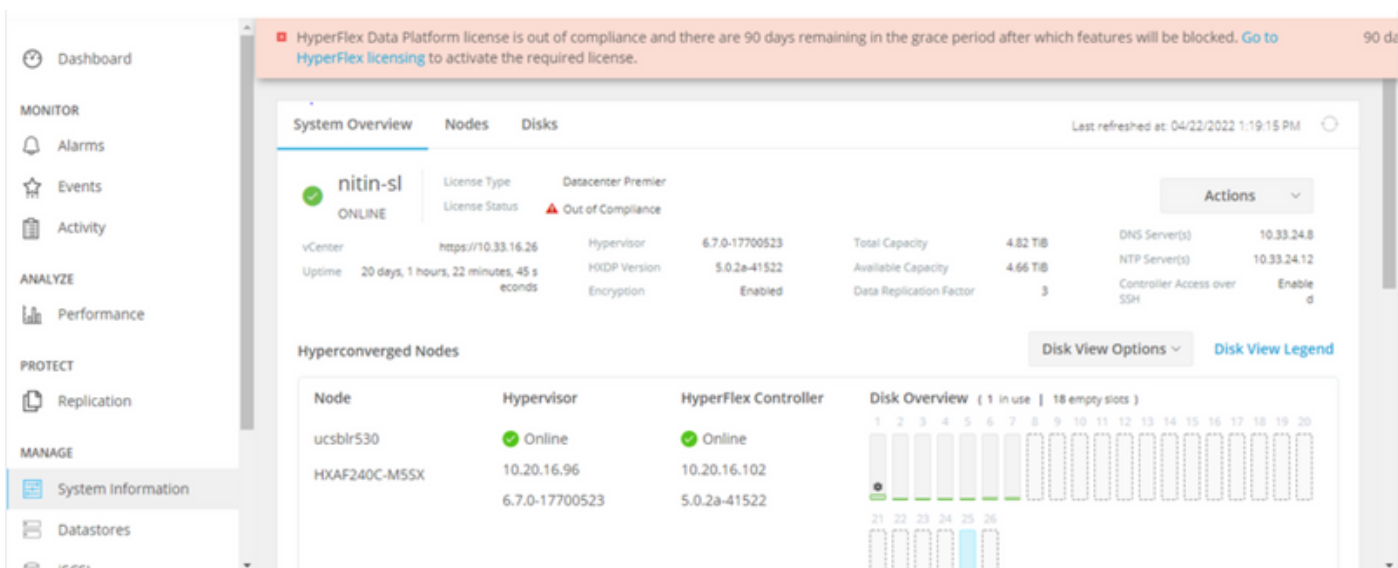
许可证状态示例场景：

在此方案中，集群符合许可证状态。

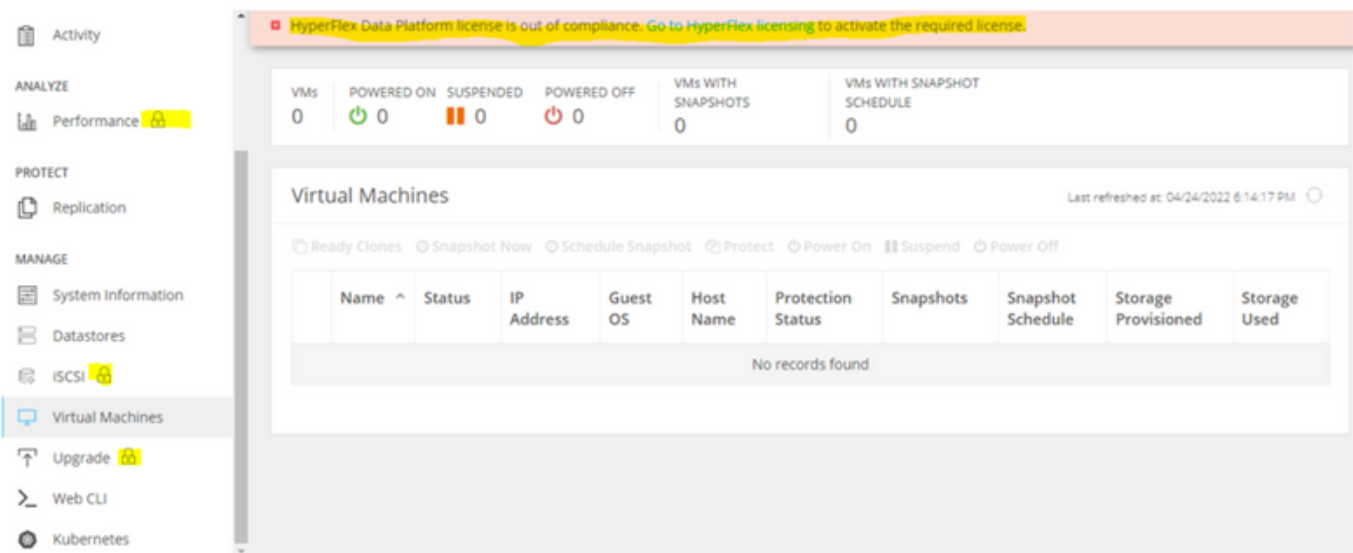


在下一个场景中，集群已注册，但许可证状态为不合规，且宽限期为一(1)天至九十(90)天。

在这种情况下，不会阻止任何功能，但菜单顶部会显示一条横幅，提示您激活所需的许可证，以防宽限期过期。



在这种情况下，集群已注册，许可证状态不合规，宽限期为零(0)。



配置

有关如何在智能许可证帐户中注册Hyperflex的指导，请查看[此视频](#)。

验证

确认您的配置工作正常。

通过CLI验证许可证状态。查看注册状态和授权状态。

```
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

故障排除

在一些常见情况下，这两种状态都可能失败，但原因都是相同的。

场景1:HTTP/HTTPS连接

许可证注册通过TCP进行，尤其是通过HTTP和HTTPS，因此允许此通信至关重要。

测试来自每个存储控制器VM(SCVM)(但主要来自群集管理IP(CMIP)SCVM的连接。

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

您必须获取示例中所示的输出，否则，这意味着流量被阻止。

```
<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>
```

如果收到的输出与之前的输出不同，请确认连通性并使用以下命令检验端口是否已打开：

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

场景2：代理问题

有时，当所有Web客户端和公共Web服务器对流量执行安全检查时，会在它们之间配置代理。

在这种情况下，在具有CMIP的SCVM和cisco.com之间，验证已在集群中配置代理（如示例所示）。

```
<#root>
```

```
hxsshell:/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
```

如果代理显示已配置，请使用代理URL或IP地址以及配置的端口测试连接。

```
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，测试与代理的连接。

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

场景3：云环境

在某些情况下，云环境设置为devtest，这会导致注册失败。在本例中，它被设置为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:
```

从日志中，当环境错误地设置为devtest时，您会看到特定的错误。

```
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：从5.0(2a)版本开始，diag用户可用于允许用户拥有更多权限进行故障排除，以访问受限文件夹和无法通过priv command line (Hyperflex版本4.5.x中引入) 访问的命令。


您可以将环境类型更改为“生产”，然后重试注册。

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

场景4：在线证书状态协议(OCSP)

Hyperflex在许可证注册过程中利用OCSP和证书撤销列表(CRL)服务器来验证HTTPS证书。

这些协议旨在通过HTTP分发撤销状态。CRL和OCSP消息是公共文档，指示OCSP验证失败时以及许可证注册失败时X.509证书的撤销状态。

 提示：如果OCSP发生故障，则意味着中间的安全设备会断开HTTP连接。

为了确认OCSP验证是否正常，您可以尝试将文件下载到CMIP SCVM/tmp分区，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
```

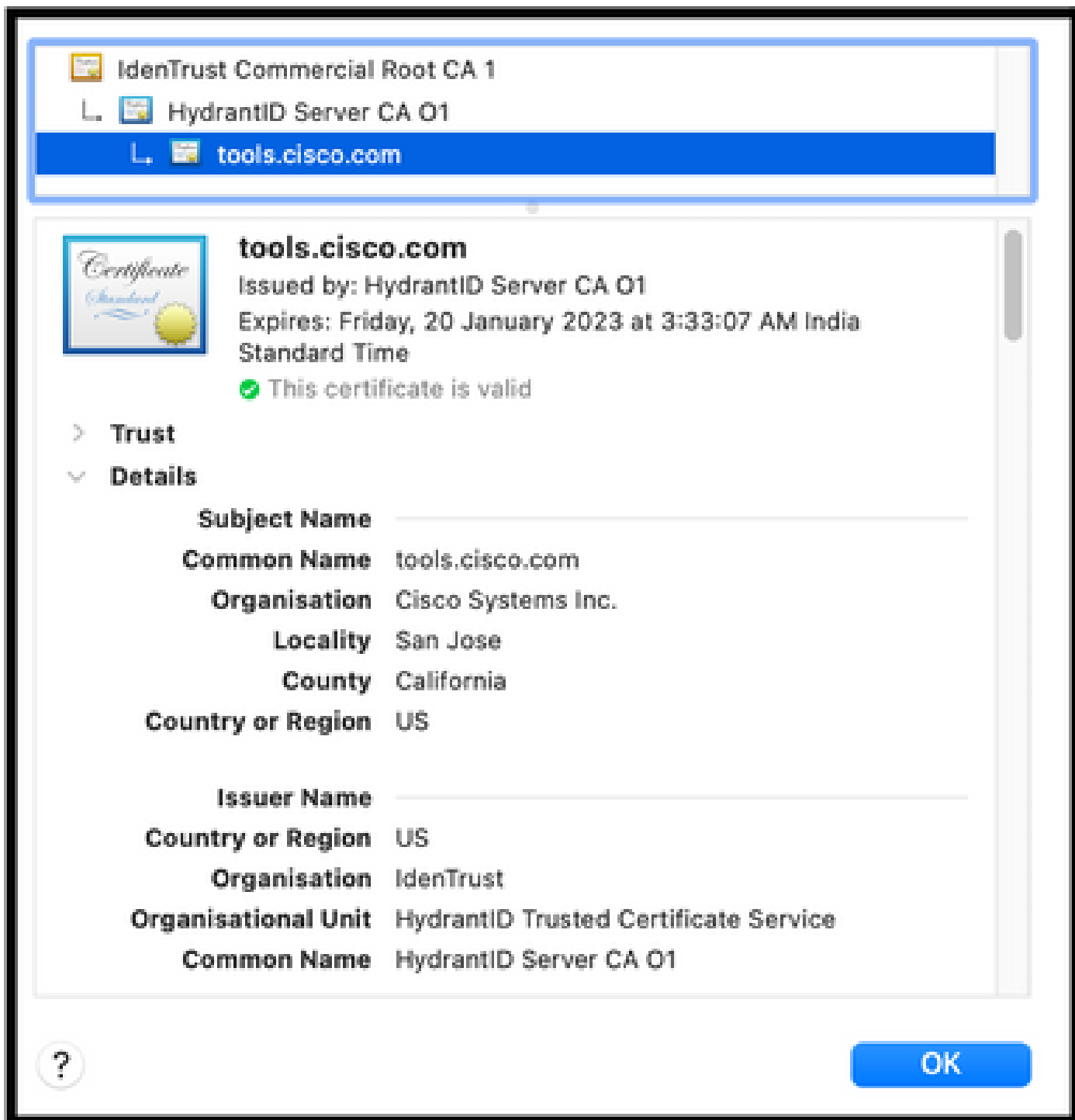
场景5：证书已更改

在某些网络中，代理和防火墙安全设备运行安全套接字层(SSL)检查，并且它们可能会损坏 Hyperflex预期会接收from tools.cisco.com:443的证书。

要检查代理或防火墙未更改证书，请在保存CMIP的SCVM中运行命令：

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

请注意，主题名称和颁发者名称信息必须与本示例中显示的证书匹配。



警告：如果主题或颁发者中的至少一个字段不同，则注册失败。Hyperflex集群管理IP和tools.cisco.com:443的安全SSL检查中的旁路规则可以解决此问题。

在本示例中，您可以看到如何验证从Hyperflex CMIP SCVM中的证书收到的相同信息。

```
<#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
```

附加程序

如果涵盖的场景成功或解决，但许可证注册仍然失败，则可以使用此程序。

注销许可证。

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

从智能许可获取新令牌，重新启动许可过程，然后重试许可证注册。

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

相关信息

- [Cisco HyperFlex HX数据平台 — 最终用户指南](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。