Troubleshoot Hyperflex License Registration Issues

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

- What is Smart License
- How Do Licenses Work on Hyperflex
- Strict Enforcement Policy

Configure

Verify

Troubleshoot

- Scenario 1: HTTP/HTTPs Connectivity
- Scenario 2: Proxy Issues
- Scenario 3: Cloud Environment
- Scenario 4: Online Certificate Status Protocol (OCSP)
- Scenario 5: Certificate Changed
- Additional Procedure

Related Information

Introduction

This document describes how to troubleshoot the most common issues of Hyperflex registration license issues.

Prerequisites

Requirements

Cisco recommends that you have basic knowledge of these topics:

- Hyperflex Connect
- License Registration
- HTTP/HTTPS

Components Used

The information in this document is based on:

- Hyperflex Data Program (HXDP) 5.0.(2a) and higher

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

What is Smart License

Cisco Smart Licensing (Smart Licensing) is an intelligent cloud-based software license management solution that simplifies the three core license functions (Purchase, Management, and Report) across your entire organization.

You can access your smart license account here.

How Do Licenses Work on Hyperflex

Cisco Hyperflex integrates with Smart Licensing and it is automatically enabled by default as you create a Hyperflex storage cluster. However, for your Hyperflex storage cluster to consume and report licenses, you must register it with Cisco Smart Software Manager (SSM) through your Cisco Smart Account.

A Smart Account is a cloud-based repository that provides full visibility and access control to all the Cisco software licenses purchased and product instances across your company.

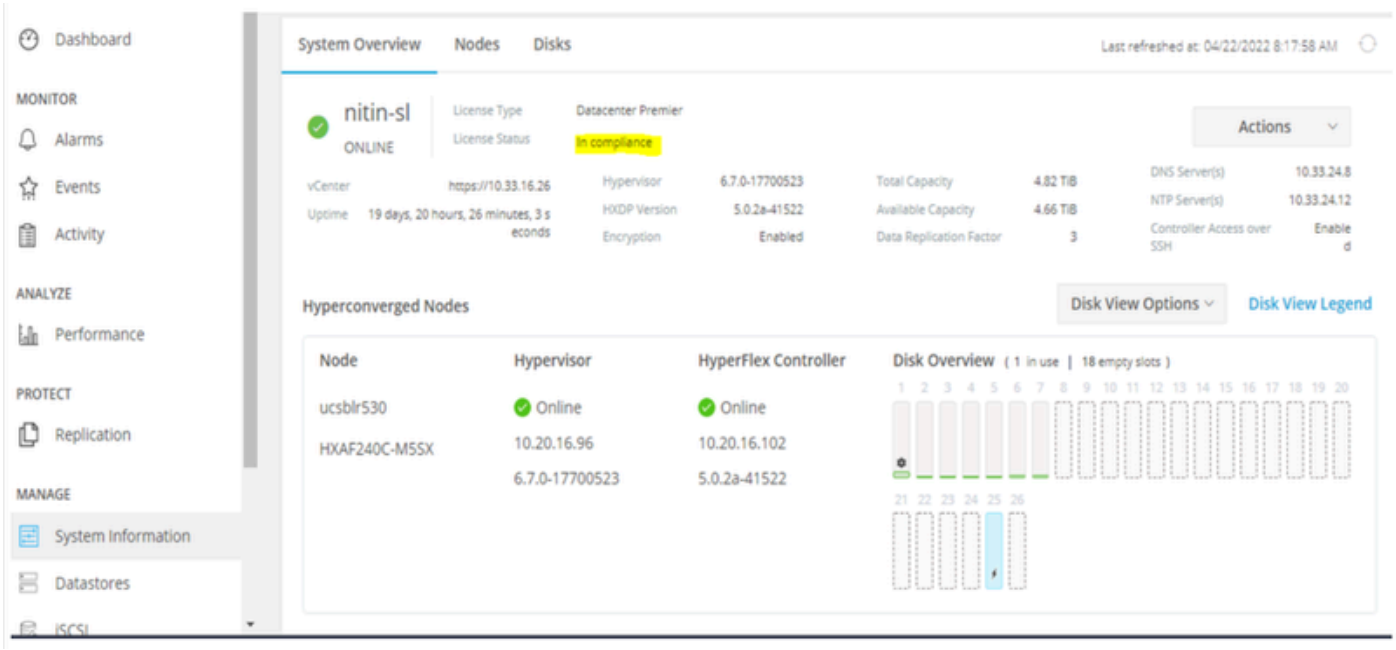
Note: In Hyperflex clusters, registration is valid for one year. After that, Hyperflex automatically attempts to re-register so no human interaction is required.

Strict Enforcement Policy

From version HXDP 5.0(2a) onward, some features are blocked from Hyperflex Connect GUI if the cluster is not in compliance with the license.

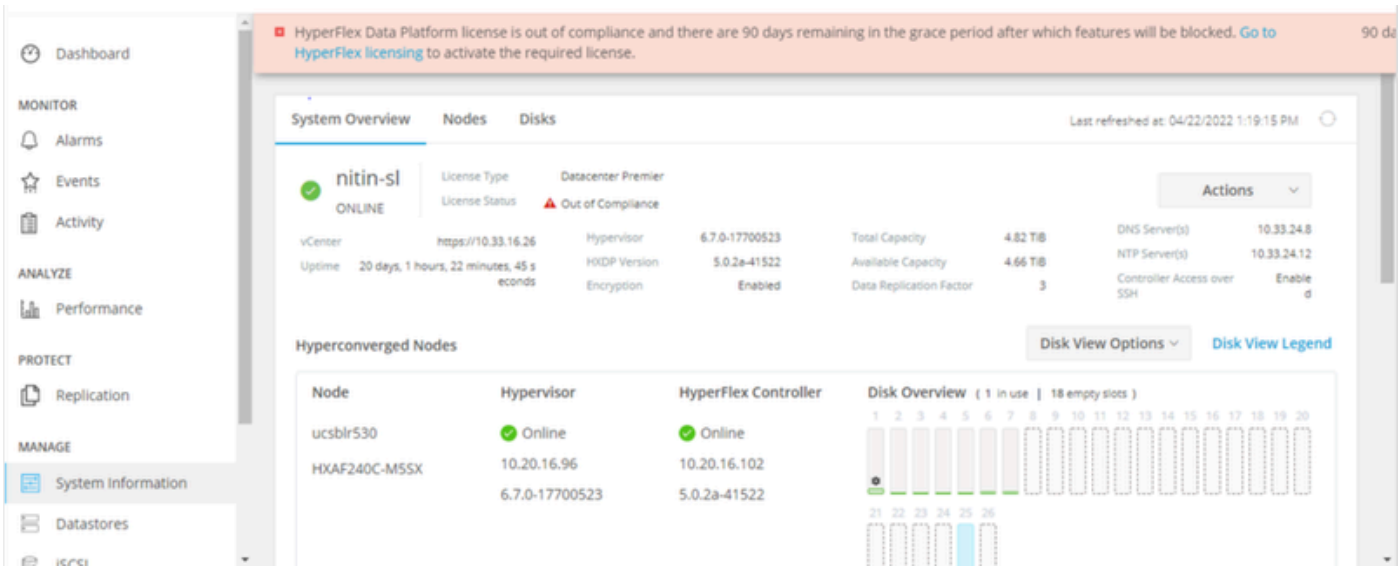
License status example scenarios:

In this scenario, the cluster is In compliance with the License status.

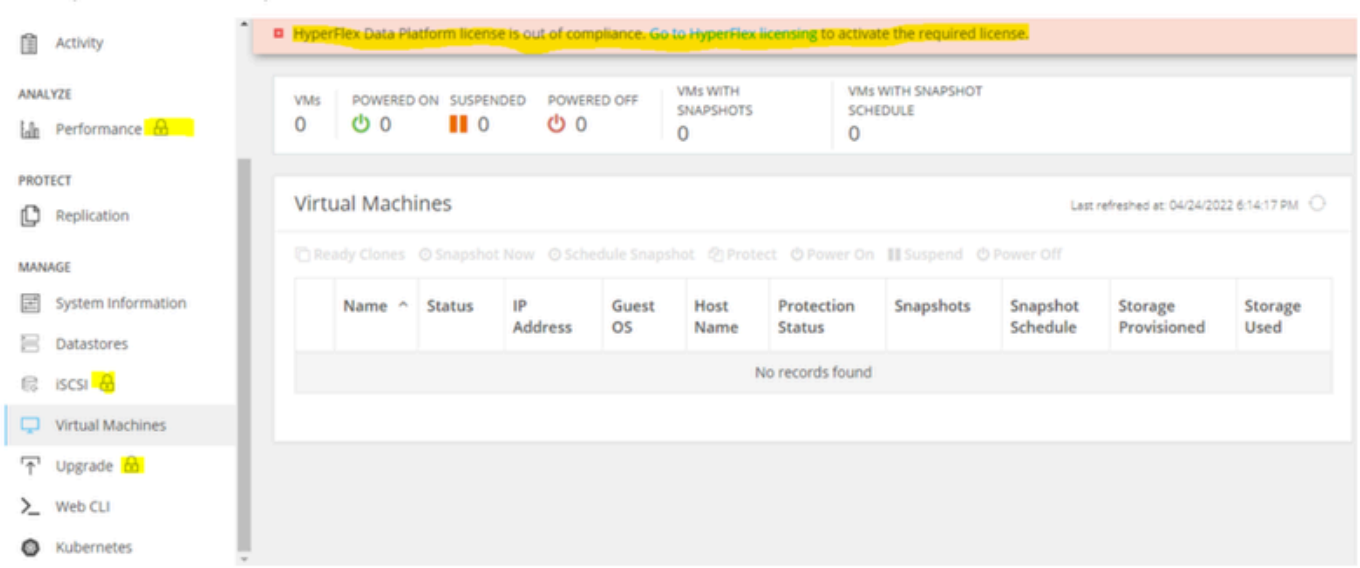


In the next scenario, the Cluster is registered, but the License State is Out of Compliance, and the grace period is between one (1) to ninety (90) days.

In this case, no features are blocked, but a banner appears on the top of the menu which prompts you to activate the required license before the grace period expires.



In this scenario, the cluster is registered, the License State is Out of Compliance, and the grace period is zero (0).



Configure

For guidance on how to register Hyperflex with your Smart License account, check this video.

Verify

Confirm that your configuration works properly.

Verify the license status via CLI. View the registration status and the authorization status.

```
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

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

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

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

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

Troubleshoot

There are some common scenarios where these two statuses can fail, both of them caused by the same root cause.

Scenario 1: HTTP/HTTPs Connectivity

License registration goes over TCP, and more specifically over HTTP and HTTPS, therefore it is critical to allow this communication.

Test connectivity from each Storage Controller VM (SCVM), but mainly from Cluster Management IP (CMIP) SCVM.

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

You must obtain the output shown in the example, otherwise, it means the traffic is blocked.

```
<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>
```

If the output received is different than the previous output, confirm connectivity and verify that ports are opened with these commands:

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

Scenario 2: Proxy Issues

Sometimes, a proxy is configured between all web clients and public web servers when they perform security inspections of the traffic.

In this case, between the SCVM with the CMIP and cisco.com, validate that the proxy is already configured in the cluster (as shown in the example).

<#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
```

if the proxy shows already configured, test connectivity either with proxy URL or IP address along with the port configured.

```
curl -v --proxy https://url:<Proxy Port> 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
```

Additionally, test connectivity to the proxy.

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

Scenario 3: Cloud Environment

In certain situations, the cloud environment is set to devtest which causes registration to fail. In this example, it is set to 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:
```

From logs, you can see specific errors when the environment is set incorrectly as 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 servic
```

Tip: From the 5.0(2a) version, diag user is available to allow users to have more privileges to troubleshoot with access to restricted folders and commands that are not accessible via **priv** command line which was introduced in Hyperflex version 4.5.x.

You can change the environment type to production and retry the registration.

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

Scenario 4: Online Certificate Status Protocol (OCSP)

Hyperflex leverages OCSP and Certificate Revocation Lists (CRL) servers to validate HTTPS certificates during the license registration process.

These protocols are designed to distribute the revocation status over HTTP. CRLs and OCSP messages are public documents that indicate the revocation status of X.509 certificates when OCSP validation fails then license registration fails as well.

Tip: If OCSP fails, it means that a security device in between breaks the HTTP connection.

In order to confirm if OCSP validation is good, you can try to download the file to your CMIP SCVM / tmp partition, as shown in the example.

```
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
```

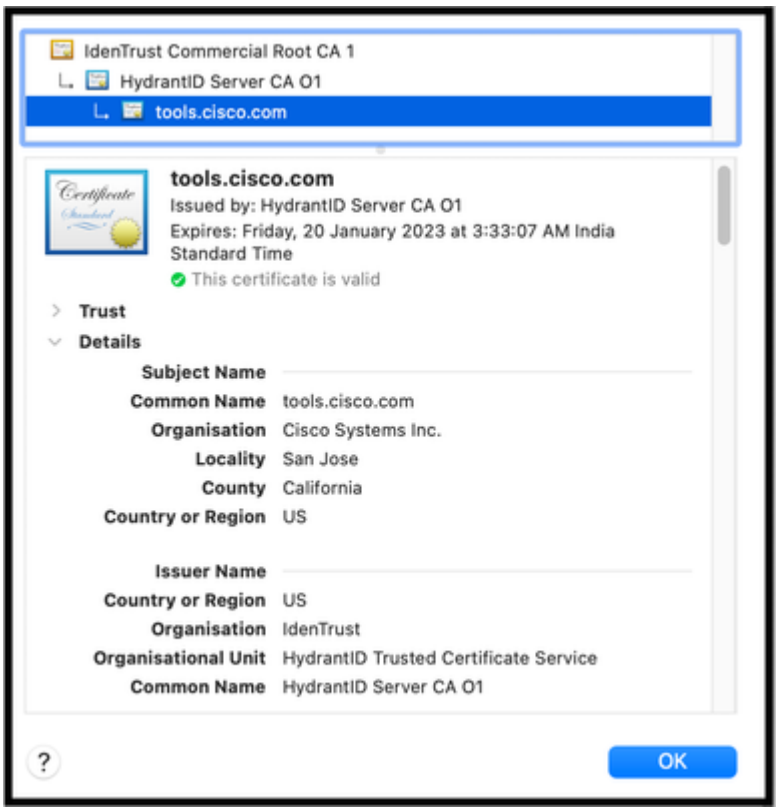
Scenario 5: Certificate Changed

In some networks, proxy and firewall security devices run Secure Sockets Layer (SSL) inspection and they can corrupt the certificate that Hyperflex expects to receive from tools.cisco.com:443.

In order to check the certificate is not changed by a proxy or firewall, in the SCVM that holds the CMIP, run the command:

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

It is important to remark that the Subject Name and Issuer Name information must match the certificate shown in this example.



Warning: If at least one field in the subject or issuer is different, the registration fails. A bypass rule in the security SSL Inspection for Hyperflex Cluster management IPs and tools.cisco.com:443 can fix this.

In this example, you can see how to validate the same information received from the certificate in 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
```

Additional Procedure

This procedure can be leveraged if the covered scenarios are successful or resolved, yet license registration still fails.

Deregister the license.

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

Acquire a new token from Smart licensing, restart the licensing process, and retry the license registration.

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

Related Information

- Cisco HyperFlex HX Data Platform - End-User Guides