

使用FMC 7.2.4集成对ISE 3.2进行配置和故障排除

目录

[简介](#)

[先决条件](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[准备ISE以进行集成。](#)

[准备FMC进行集成。](#)

[设置ISE和FMC之间的pxGrid连接。](#)

[验证](#)

[在FMC上验证。](#)

[在ISE上验证。](#)

[故障排除](#)

[排除FMC故障。](#)

[ISE故障排除。](#)

[常见问题](#)

[PxGrid用户客户端未在ISE上获得批准。](#)

[PxGrid ISE证书链不完整。](#)

[参考](#)

简介

本文档介绍使用Platform Exchange Grid连接将身份服务引擎与防火墙管理中心集成的过程。

先决条件

思科建议了解以下主题：

- 身份服务引擎 (ISE)
- 平台交换网格
- 防火墙管理(FMC)
- TLS/SSL证书。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 身份服务引擎(ISE)版本3.2补丁3

- 防火墙管理中心版本7.2.4

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.

本文档提供使用pxGrid版本2集成FMC和ISE的解决方案。

Cisco Firepower管理中心(FMC)是下一代防火墙和入侵防御系统的集中式平台，提供策略管理、威胁检测和事件响应。

思科身份服务引擎是一个全面的解决方案，通过提供身份验证、授权和责任(AAA)以及策略实施服务提供对终端的安全访问。

Platform Exchange Grid(pxGrid)允许您在多供应商跨平台网络之间交换信息。

通过这种集成，您可以获得安全监控、威胁检测和基于共享信息设置网络策略。

PxGrid框架有2个版本。要使用的版本取决于您需要查看的ISE版本和修补程序。

从ISE 3.1版本开始，所有pxG来自ISE的RID连接基于pxgrid版本 2.

PxGrid第1版。

T此框架的第一个版本 (pxGrid v1) 特征在于通过命令show application status ise看到的适用性 在随后的输出中显示。

在节点中启用pxGrid功能时，您会看到pxGrid 功能 处于运行状态.

```
ise/admin# show application status ise
```

ISE PROCESS NAME	STATE	PROCESS ID
-----	-----	-----
Database Listener	running	3688
Database Server	running	41 PROCESSES
Application Server	running	6041
Profiler Database	running	4533
AD Connector	running	6447
M&T Session Database	running	2363
M&T Log Collector	running	6297
M&T Log Processor	running	6324
Certificate Authority Service	running	6263
pxGrid Infrastructure Service	disabled	
pxGrid Publisher Subscriber Service	disabled	
pxGrid Connection Manager	disabled	
pxGrid Controller	disabled	
Identity Mapping Service	disabled	

PxGrid版本1可维护性。

在此平台版本中，已知只有一个pxGrid节点的pxGrid进程处于运行状态，而其他pxGrid节点处于备用状态。

这些节点持续监控pxGrid节点的状态，同时运行相关服务。

其中，主要pxGrid节点存在升级，另一个pxGrid节点启用其pxGrid服务。

但是，这表示发生此故障转移时的停机时间。

第一个版本的pxgrid基于可扩展消息传送和在线状态协议(XMPP)中的通信，后者是一组用于协作和语音基础设施的技术。

pxGrid v1连接中共享的主题如下：

- 会话目录
- 终端配置文件元数据
- Trustsec元数据
- 终端保护功能
- 自适应网络控制
- MDM_Offline主题
- 身份
- SXP

PxGrid第2版。

本文档介绍如何使用PxGrid版本2。此平台在ISE和WebSocket协议上使用REST操作，从而在数据模型中带来增强功能、提高的可扩展性、性能和灵活性。

在此版本中，您不会看到使用命令show application status ise运行的pxgrid功能与先前版本中的功能相同。

请参阅本文档中ISE的验证部分，了解要检查哪些机制以查看pxGrid功能。

在此版本中，您拥有配置为活动pxGrid节点的所有pxGrid节点。随时可以参加交流信息。

在版本1中，只有一个节点将pxGrid的可维护性保持为正在运行。

pxGrid v2连接中共享的主题如下：

- 会话目录
- Radius故障
- 分析器配置
- 系统运行状况
- MDM
- ANC状态
- Trustsec
- TrustSec配置
- TrustSec SXP
- 终端资产。

作为平台的pxGrid组件。

PxGrid控制器(ISE):必须信任使用pxGrid的每个参与者。

客户端：可以成为不同主题的订阅服务器和发布服务器。

发布者：与控制器共享信息的客户端。

用户：使用主题信息的客户端。

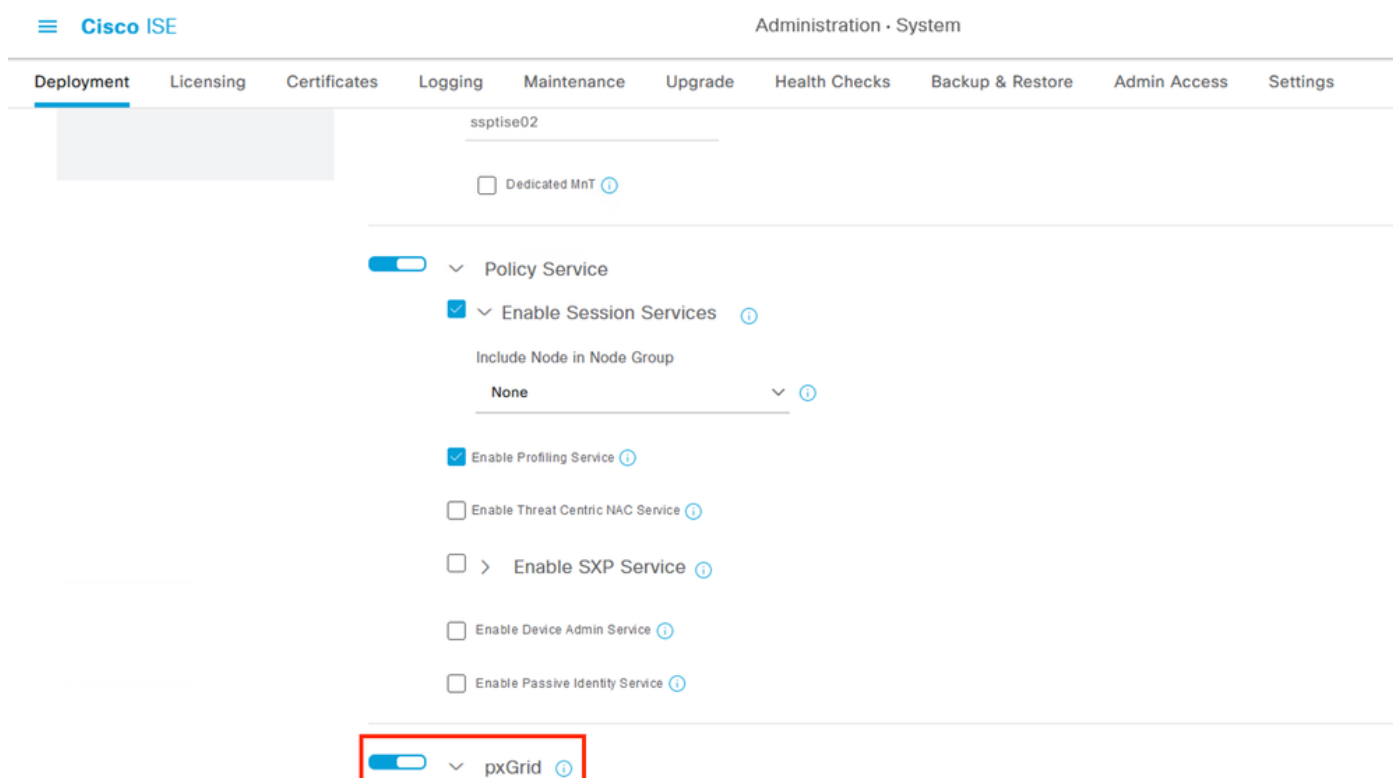
此集成允许您根据ISE共享的信息及其发布的主题（与终端活动相关），在FMC上创建内容策略。

配置

准备ISE以进行集成。

第1步：在Administration > System > Deployment菜单中，配置ISE节点以在其上运行pxGrid角色。

选择节点并启用功能pxGrid。



在节点中启用ISE pxGrid服务。

步骤2.启用具有pxGrid功能的节点后，查看与连接的内部客户端相关的Websockets的状态。

导航到管理> pxGrid服务> Websocket。注意通过IP地址127.0.0.1直接指向ISE服务的客户端。

Cisco ISE

Administration - pxGrid Services

Q

?

Summary

Client Management

Diagnostics

Settings

WebSocket

Log

Tests

WebSocket

Clients

Topics

Clients

Rows/Page

8

<<

<

1

>

>>

Go

8 Total Rows

Filter

Client Name	Connect To	Session Id	Certificate	Subscriptions	Publications	IP Address	Status
-ise-fanout-spsptise01	sspsptise01	sspsptise01:0	CN=sspsptise01.ss...	/topic/wildcard	/topic/com.cisco.ise.pxgrid...	127.0.0.1	Connected
-ise-fanout-spsptise02	sspsptise01	sspsptise01:1	CN=sspsptise02.ss...	/topic/distributed	/topic/distributed	10.4.49.42	Connected
-ise-fanout-spsptise01	sspsptise01	sspsptise01:2	CN=sspsptise01.ss...	/topic/distributed		10.4.49.41	Connected
-ise-fanout-spsptise02	sspsptise02	sspsptise02:9	CN=sspsptise02.ss...	/topic/wildcard	/topic/com.cisco.ise.pxgrid...	127.0.0.1	Connected
-ise-mnt-spsptise02	sspsptise02	sspsptise02:11	CN=sspsptise02.ss...	/topic/com.cisco.ise.sessio...	/topic/com.cisco.ise.sessio...	10.4.49.42	Connected
-ise-admin-spsptise02	sspsptise02	sspsptise02:12	CN=sspsptise02.ss...		/topic/com.cisco.ise.pxgrid...	10.4.49.42	Connected
-ise-mnt-spsptise01	sspsptise02	sspsptise02:13	CN=sspsptise01.ss...	/topic/com.cisco.ise.sessio...	/topic/com.cisco.ise.sessio...	10.4.49.41	Connected
-ise-admin-spsptise01	sspsptise02	sspsptise02:14	CN=sspsptise01.ss...	/topic/com.cisco.ise.pxgrid...	/topic/com.cisco.ise.pxgrid...	10.4.49.41	Connected

来自ISE的内部WebSocket。

第 3 步： 浏览菜单Administration > pxGrid Services > Settings，然后选择自动批准新的基于证书的帐户选项

此时此步骤是可选的，但是，对于pxGrid连接，建议启用此复选框。

之后，您可以手动接受FMC作为用户。

Cisco ISE

Administration - pxGrid Services

Summary

Client Management

Diagnostics

Settings

Settings

Automatically approve new certificate-based accounts

?

Allow password based account creation

?

Use Default

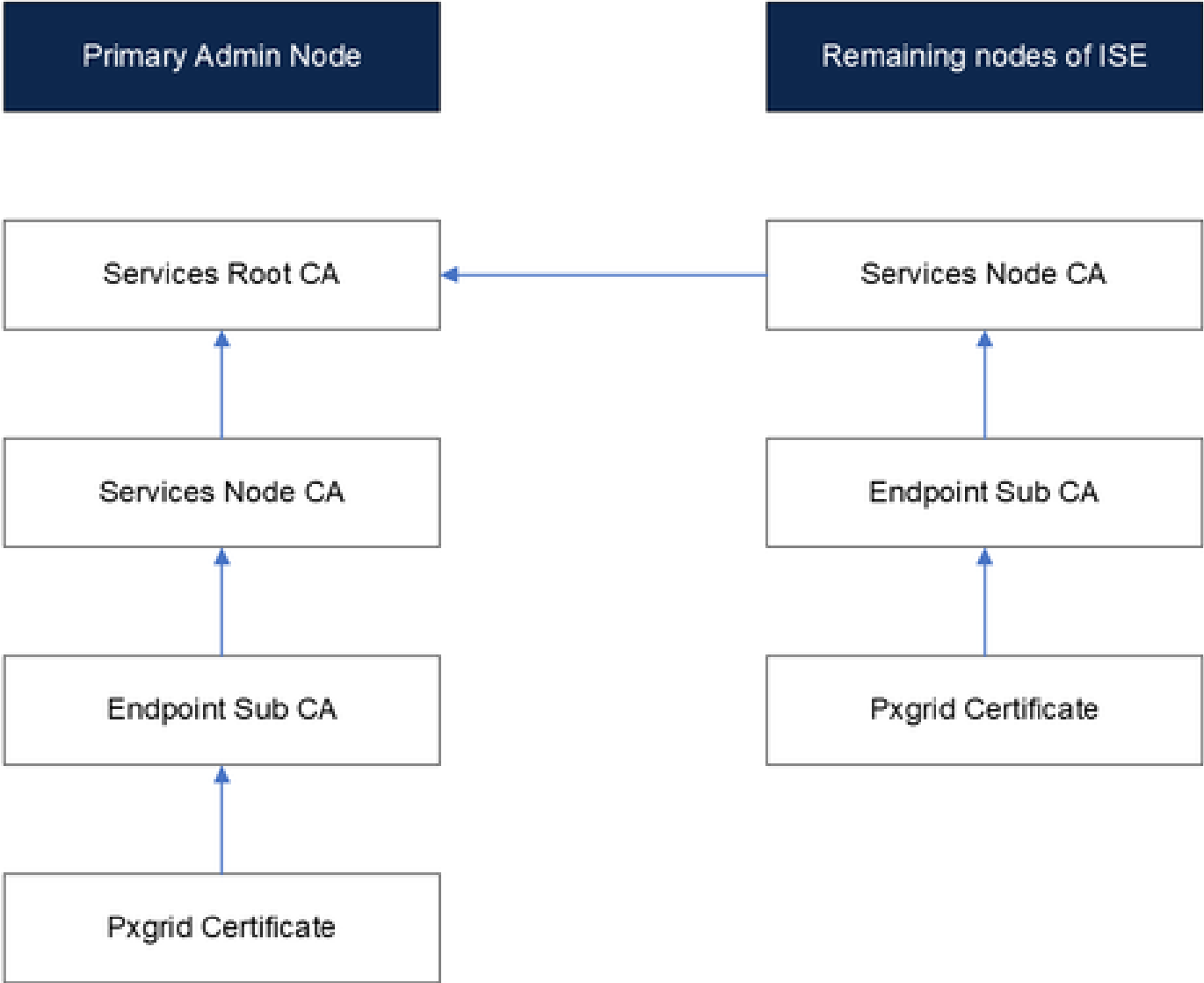
Save

为基于pxGrid证书的帐户启用自动审批。

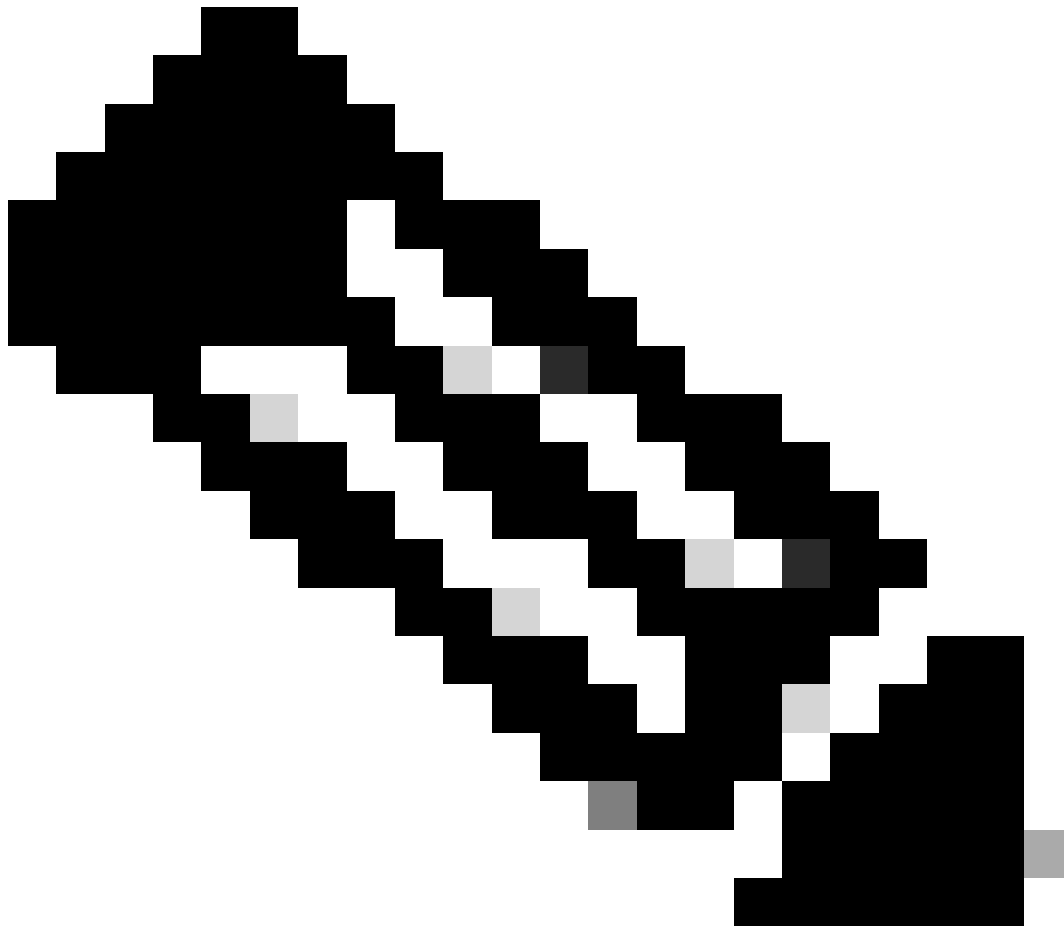
第 4 步： 在Administration > System > System Certificates中查看与您的环境的pxGrid功能相关的证书

建议在部署的所有节点中具有同一pxGrid证书，这些证书由同一根证书颁发机构(CA)签名

在此场景中，我们使用生成的内部ISE证书。对于此版本的ISE，在本示例中，根CA对应于PAN节点。



绘制ISE上的内部证书图。



注意：有关ISE上生成的证书的内部结构的详细信息，请参阅[了解ISE内部证书授权服务](#)。

Cisco ISE

Administration - System

DeploymentLicensingCertificatesLoggingMaintenanceUpgradeHealth ChecksBackup & RestoreAdmin AccessSettings

Certificate Management

System Certificates

Trusted Certificates

OCSP Client Profile

Certificate Signing Requests

Certificate Periodic Check Se...

Certificate Authority

System Certificates

For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

EditGenerate Self Signed CertificateImportExportDeleteView

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
CA - sspisecv1m00001							
☐ CN=ssptise01.sspisec.mex, O=U-Certificate Services System Certificate/Certificate Services Endpoint Sub CA - sspisec01#00002	pxGrid		ssptise01.sspisec.mex	Certificate Services Endpoint Sub CA - sspisec01	Fri, 30 Jun 2023	Sat, 1 Jul 2028	Active
☐ ise01_External_CA	Admin, EAP Authentication, RADIUS DTLS, Portal	Default Portal Certificate Group	ssptise01.sspisec.mex	ssptise01.sspisec.mex	Mon, 3 Jul 2023	Wed, 2 Jul 2025	Active
ssptise02							
☐ Default self-signed saml server certificate - CN=SAML_sspisec01.sspisec.mex	SAML		SAML_sspisec01.sspisec.mex	SAML_sspisec01.sspisec.mex	Sat, 1 Jul 2023	Thu, 29 Jun 2028	Active
☐ ise02_External_CA	Admin, EAP Authentication, RADIUS DTLS, Portal	Default Portal Certificate Group	ssptise01.sspisec.mex	ssptise01.sspisec.mex	Mon, 3 Jul 2023	Wed, 2 Jul 2025	Active
☐ CN=ssptise02.sspisec.mex, O=U-ISE Messaging Services/Certificate Services Endpoint Sub CA - sspisec02#00004	ISE Messaging Service		ssptise02.sspisec.mex	Certificate Services Endpoint Sub CA - sspisec02	Sat, 1 Jul 2023	Sun, 2 Jul 2028	Active
☐ CN=ssptise02.sspisec.mex, O=U-Certificate Services System Certificate/Certificate Services Endpoint Sub CA - sspisec02#00003	pxGrid		ssptise02.sspisec.mex	Certificate Services Endpoint Sub CA - sspisec02	Sat, 1 Jul 2023	Sun, 2 Jul 2028	Active

分布式部署中的PxGrid证书。

步骤5.验证pxGrid证书的状态。

从上一个菜单中，选中节点pxGrid证书中的复选框，然后选择选项View。

输出看起来与pxGrid证书中显示的输出类似。

Cisco ISE

Administration - System

DeploymentLicensingCertificatesLoggingMaintenanceUpgradeHealth Checks

Certificate Management

System Certificates

Trusted Certificates

OCSP Client Profile

Certificate Signing Requests

Certificate Periodic Check Se...

Certificate Authority

System Certificates

For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

EditGenerate Self Signed CertificateImportExportDeleteView

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
CA - sspisecv1m00001							
☐ CN=ssptise01.sspisec.mex, O=U-Certificate Services System Certificate/Certificate Services Endpoint Sub CA - sspisec01#00002	pxGrid		ssptise01.sspisec.mex	Certificate Services Endpoint Sub CA - sspisec01	Fri, 30 Jun 2023	Sat, 1 Jul 2028	Active
☐ ise01_External_CA	Admin, EAP Authentication, RADIUS DTLS, Portal	Default Portal Certificate Group	ssptise01.sspisec.mex	ssptise01.sspisec.mex	Mon, 3 Jul 2023	Wed, 2 Jul 2025	Active
ssptise02							
☐ Default self-signed saml server certificate - CN=SAML_sspisec01.sspisec.mex	SAML		SAML_sspisec01.sspisec.mex	SAML_sspisec01.sspisec.mex	Sat, 1 Jul 2023	Thu, 29 Jun 2028	Active
☐ ise02_External_CA	Admin, EAP Authentication, RADIUS DTLS, Portal	Default Portal Certificate Group	ssptise01.sspisec.mex	ssptise01.sspisec.mex	Mon, 3 Jul 2023	Wed, 2 Jul 2025	Active
☐ CN=ssptise02.sspisec.mex, O=U-ISE Messaging Services/Certificate Services Endpoint Sub CA - sspisec02#00004	ISE Messaging Service		ssptise02.sspisec.mex	Certificate Services Endpoint Sub CA - sspisec02	Sat, 1 Jul 2023	Sun, 2 Jul 2028	Active
☐ CN=ssptise02.sspisec.mex, O=U-Certificate Services System Certificate/Certificate Services Endpoint Sub CA - sspisec02#00003	pxGrid		ssptise02.sspisec.mex	Certificate Services Endpoint Sub CA - sspisec02	Sat, 1 Jul 2023	Sun, 2 Jul 2028	Active

Certificate Hierarchy

Certificate Services Root CA - sspisec01
Certificate Services Node CA - sspisec02
Certificate Services Endpoint Sub CA - sspisec02
ssptise02.sspisec.mex

ssptise02.sspisec.mex

Issued By: Certificate Services Endpoint Sub CA - sspisec02

Expires: Sun, 2 Jul 2028 11:45:44 MDT

Certificate status is good

Details

Issued To

Common Name (CN)ssptise02.sspisec.mex

Organization Unit (OU)Certificate Services System Certificate

Organization (O)

City (L)

State (ST)

Country (C)

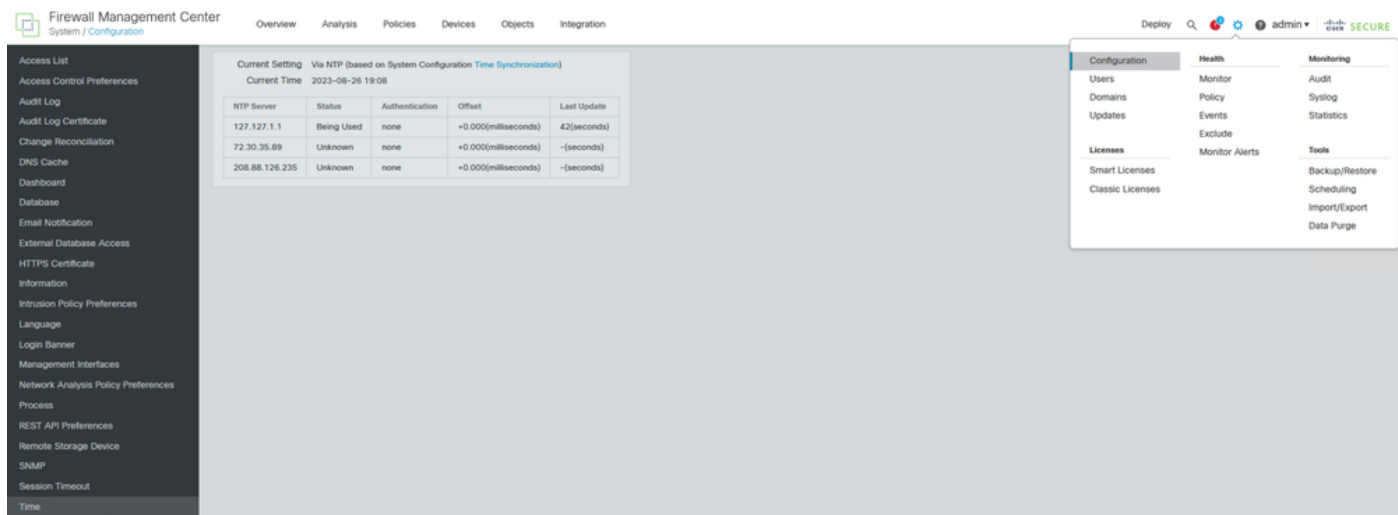
Expiration Date	Status
1 Jul 2028	Active
2 Jul 2025	Active
29 Jun 2028	Active
2 Jul 2025	Active

pxGrid证书验证。

准备FMC进行集成。

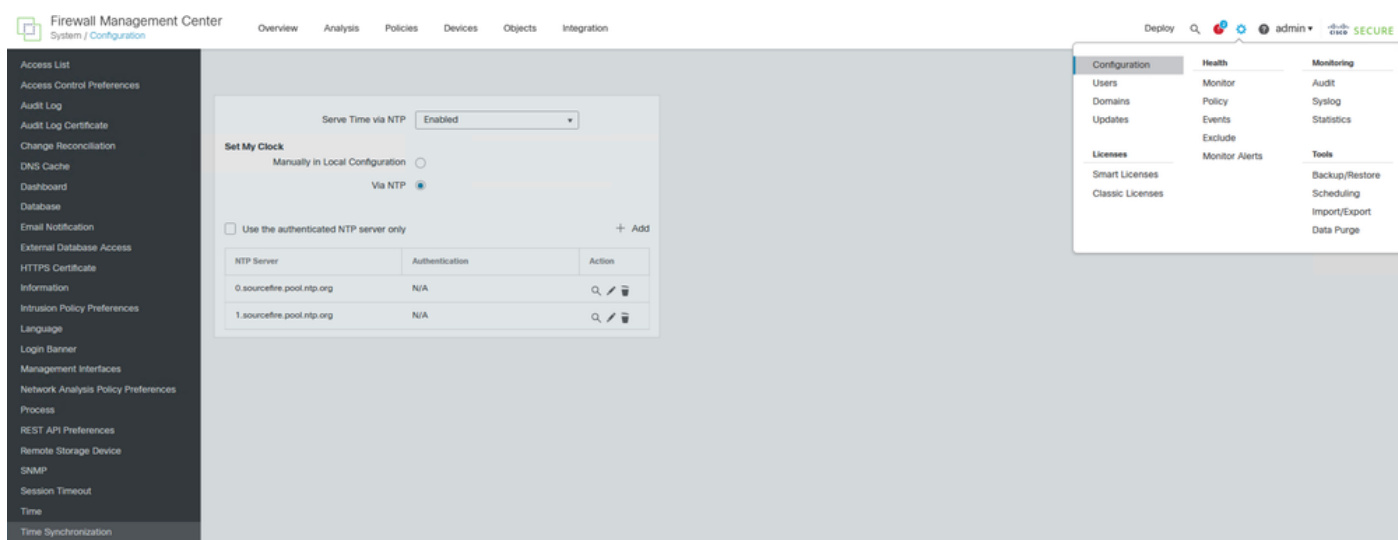
步骤1:确认FMC内部时间是 最新.

导航至 System > Configuration > 时间 并确保在FMC上配置的时间为 最新.



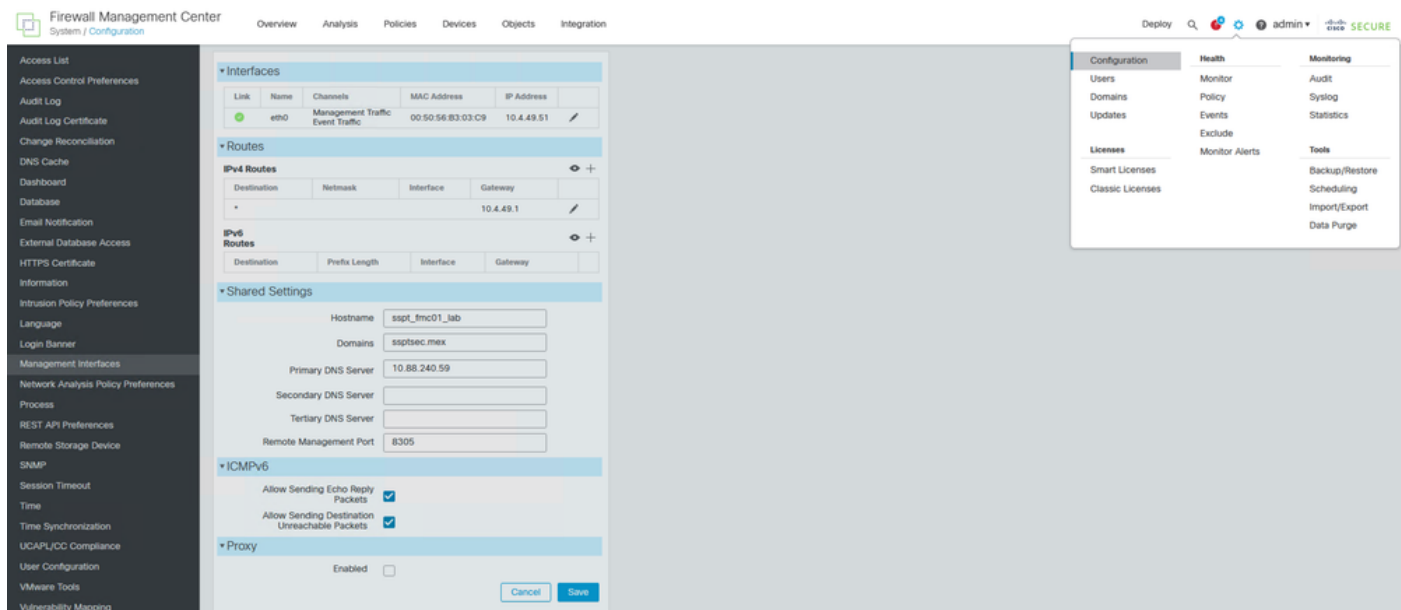
验证FMC是否处于最新状态。

如果未更新FMC时间，请确保正确配置NTP 和 在 同步.NTP可在 系统>配置>时间> +添加.



FMC上的时间同步。

Step 2. 导航至 System > Configuration > 管理接口 > 共享设置 并验证至少 主 DNS 服务器 字段 包含有效的 DNS服务器IP。



FMC上的DNS配置。

步骤3.确认配置了FMC主机名。

导航至 System > Configuration > Management Interface > Shared Settings 并确认 主机名 字段包含FMC主机名。

您可以在查看本部分中上一步时验证此步骤。

设置ISE和FMC之间的pxGrid连接。

步骤1.导航到菜单Administration > pxGrid Services > Client Management > Certificates。

在第一个选项中，选择I want to Generate a single certificate(without a certificate signing request)。

在Common Name(CN)部分，输入ISE要颁发证书的FMC的FQDN。

提供说明。

在Subject Alternative Name(SAN)部分，输入要连接的FMC的FQDN和IP地址。

在Certificate Download Format的底部，从下拉菜单中选择选项Certificate in Privacy Enhanced Electronic Mail(PEM)格式。

输入PKCSS PEM格式（包括证书链）。

稍后在FMC中使用此密码时，在证书密码中输入并存储密码。

确认密码，然后选择Create。

Cisco ISE

Administration · pxGrid Services

SummaryClient ManagementDiagnosticsSettings

ClientsPolicyGroupsCertificatespxGrid Cloud ConnectionpxGrid Cloud Policy

Certificates

Generate pxGrid Certificates

I want to*

Generate a single certificate (without...▼

Common Name (CN)*
sspt_fmc01_lab.sstsec.mex

Description
testing lab

Certificate Template
pxGrid_Certificate_Template ⓘ

Subject Alternative Name (SAN)
FQDN
sspt_fmc01_lab.sstsec.mex -- +

Subject Alternative Name (SAN)
IP address
10.4.49.51 -- +

Certificate Download Format*
Certificate in Privacy Enhanced Elect...▼ ⓘ

Certificate Password*
***** ⓘ

Confirm Password*

Reset Create

pxGrid证书生成示例。

步骤2.将zip文件下载到您的计算机。解压缩文件，并确认您的环境中存在以下文件：

Name	Date modified	Type	Size
CertificateServicesEndpointSubCA-ssptise01_	21/08/2023 04:55	Security Certificate	3 KB
CertificateServicesNodeCA-ssptise01_	21/08/2023 04:55	Security Certificate	2 KB
CertificateServicesRootCA-ssptise01_	21/08/2023 04:55	Security Certificate	2 KB
sspt_fmc01_lab.sstsec.mex_sspt_fmc01_lab.sstsec.mex	21/08/2023 04:55	Security Certificate	2 KB
sspt_fmc01_lab.sstsec.mex_sspt_fmc01_lab.sstsec.mex.key	21/08/2023 04:55	KEY File	2 KB

ISE生成的PxGrid证书。

第3步：在FMC中，导航到菜单Objects > Objects Management > PKI > Internal Certs。

选择Add Internal Cert选项。

Firewall Management Center

OverviewAnalysisPoliciesDevicesObjectsIntegration

Deploy 🔍 ⚙️ 👤 admin | **SECURE**

AAA ServerAccess ListAddress PoolsApplication FiltersAS PathCipher Suite ListCommunity ListDistinguished NameDNS Server GroupExternal AttributesFile ListFlexConfigGeolocationInterfaceKey ChainNetworkPKICert EnrollmentExternal Cert GroupsExternal CertsInternal CA GroupsInternal CAsInternal Cert GroupsInternal CertsTrusted CA GroupsTrusted CAs

Internal Certs

Internal certificate object represents a server public key certificate belonging to your organization. You can use internal certificate objects and groups in SSL rules, ISE/ISE-PIC connection and captive portal configuration.

Name	Value
No records to display	

Add Internal Cert 🔍 Filter

将FMC证书添加为内部证书。

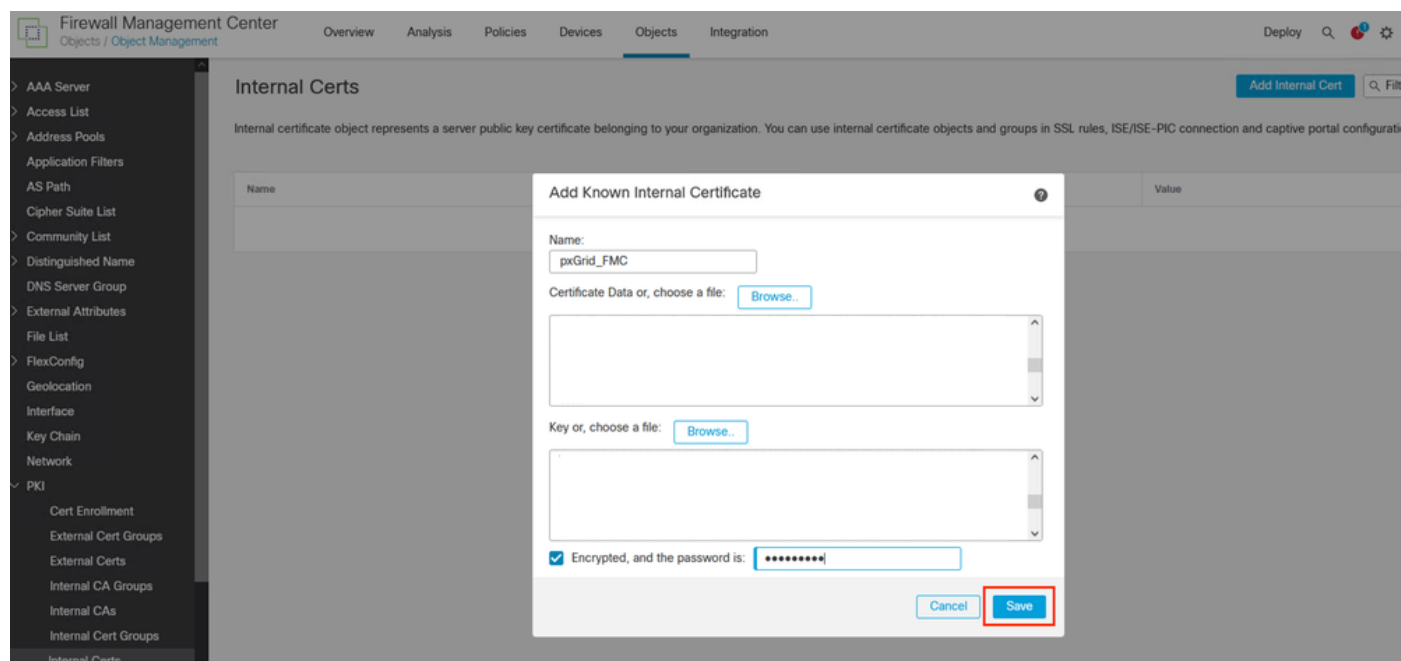
步骤4.为在FMC上分配的证书命名。

在Certificate Data部分浏览您从ISE为FMC创建的证书。

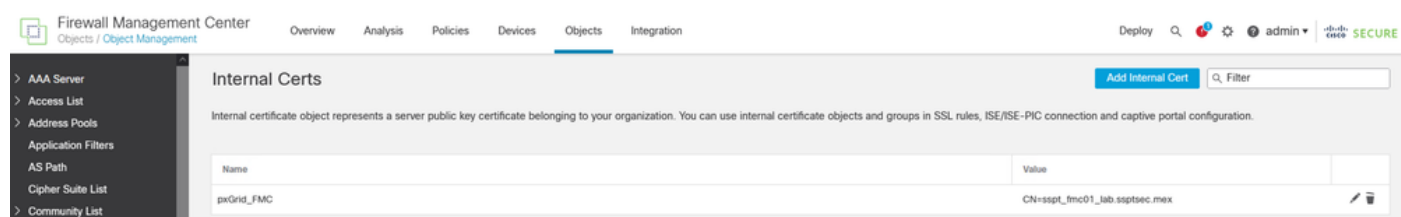
浏览扩展名为。key的文件以填写下一个字段。

选择Encrypted选项，并输入您在ISE上创建证书时使用的密码。

保存配置。



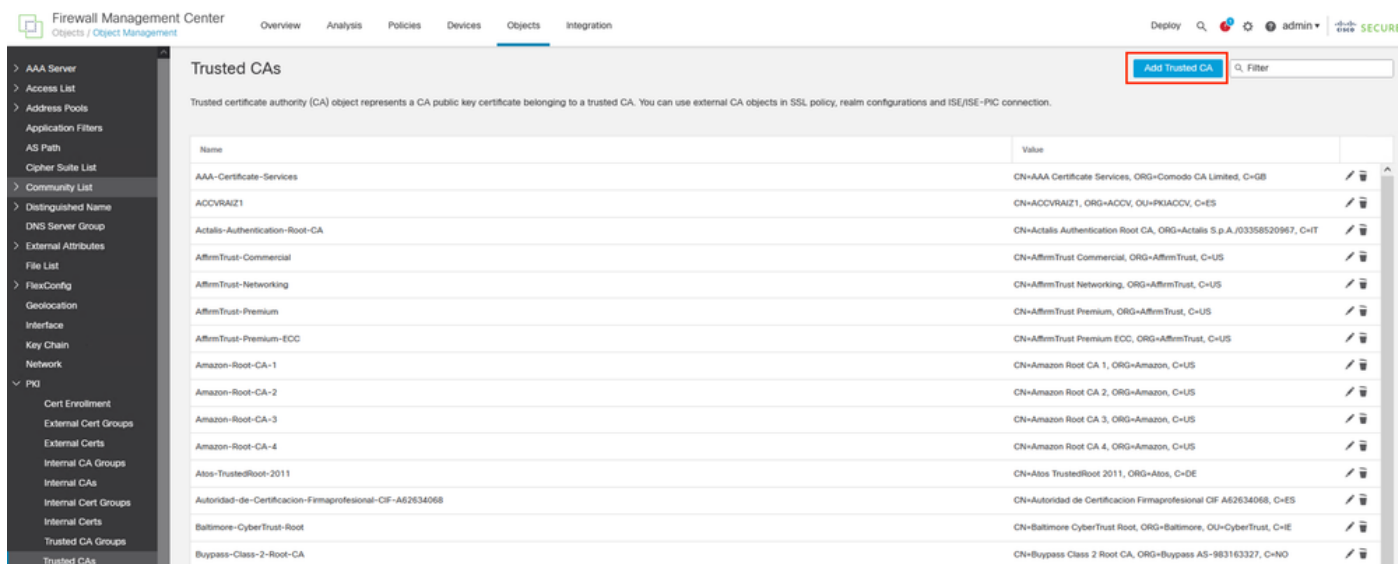
导出ISE生成的FMC证书。



FMC证书。

步骤5.导航到菜单Objects > Objects Management > PKI > Trusted CAs,

选择Add Trusted CAs。

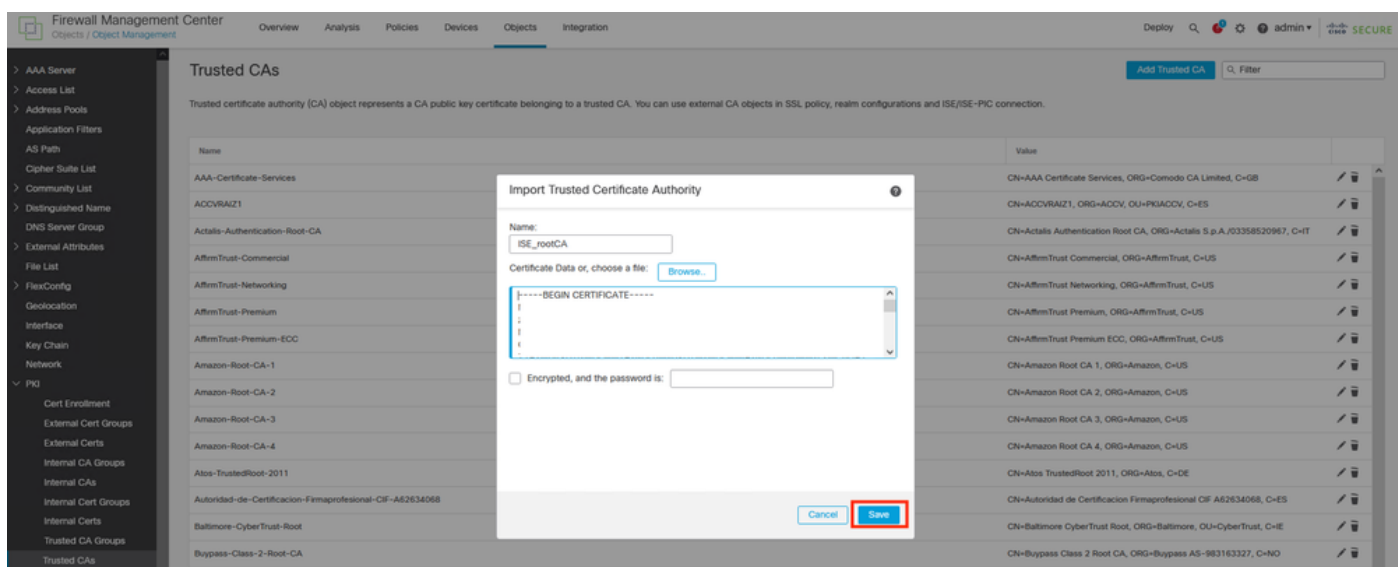


将ISE rootCA添加为受信任证书。

步骤6.命名证书颁发机构。

浏览并选择从ISE文件下载的ISE rootCA。

保存配置。



导出ISE rootCA。

步骤7.导航至菜单Integration > Other Integrations > Identity Sources。

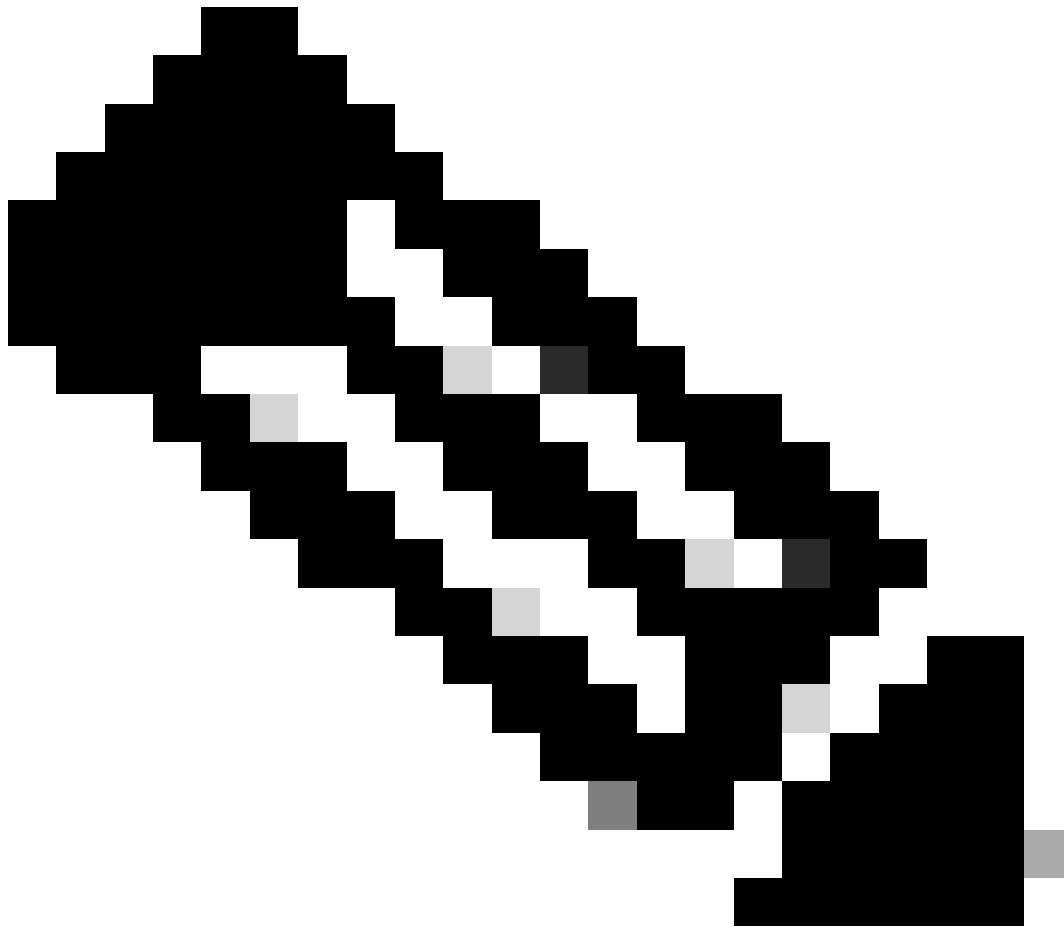
在Service Type中选择：身份服务引擎、

输入成为主节点的pxGrid节点的IP地址或FQDN。

对辅助pxGrid节点重复此过程。

从下拉菜单中选择ISE为pxGrid Client Certificate部分生成的pxGrid证书，

在MNT Server CA和pxGrid Server CA部分，选择您在上一步导出的ISE rootCA。



注意：pxGrid服务器CA对应于pxGrid节点上pxGrid正在使用的证书的根证书颁发机构。

MNT服务器CA对应于MNT节点上pxGrid正在使用的证书的证书颁发机构。

(可选) 您可以从ISE订用会话目录和SXP主题。

保存配置。

Firewall Management Center
Integration / Other Integrations / Identity Sources

Overview Analysis Policies Devices Objects Integration

Cloud Services Realms Identity Sources High Availability eStreamer Host Input Client Smart Software Manager On-Prem

You have unsaved changes Cancel Save

Service Type:
☐ None ☒ Identity Services Engine

Primary Host Name/IP Address*
10.4.49.41

Secondary Host Name/IP Address
10.4.19.42

pxGrid Client Certificate*
pxGrid_FMC

MNT Server CA*
ISE_rootCA

pxGrid Server CA*
ISE_rootCA

ISE Network Filter
ex. 10.89.31.0/24

Subscribe To:
☒ Session Directory Topic
☒ SXP Topic

Test

在FMC中将ISE设置为身份源。

验证.

在FMC上验证。

在菜单中，导航到集成>其他集成>身份源>身份服务引擎，然后保存配置。您可以测试pxGrid链接的设置。

Firewall Management Center
Integration / Other Integrations / Identity Sources

Overview Analysis Policies Devices Objects Integration

Cloud Services Realms Identity Sources High Availability eStreamer Host Input Client Smart Software Manager On-Prem

Service Type:
☐ None ☒ Identity Services Engine

Primary Host Name/IP Address*
10.4.49.41

Secondary Host Name/IP Address
10.4.49.42

pxGrid Client Certificate*
pxGrid_FMC

MNT Server CA*
ISE_rootCA

pxGrid Server CA*
ISE_rootCA

ISE Network Filter
ex. 10.89.31.0/24

Subscribe To:
☒ Session Directory Topic
☒ SXP Topic

Test

Status

ISE connection status:
Primary host: Success
Secondary host: Success

Additional Logs

Primary host:
[INFO]: PXGrid v2 is enabled
[INFO]: pxgrid 2.0: account activate succeeded
[INFO]: Successful connection to
ssptise02.ssptsec.mex:8910

OK

PxGrid通信成功。

Primary host:

[INFO]: PXGrid v2 is enabled

[INFO]: pxgrid 2.0: account activate succeeded

[INFO]: Successful connection to ssptise02.ssptsec.mex:8910

[INFO]: Successful connection to ssptise01.ssptsec.mex:8910

[INFO]: These ISE Services are up: SessionDirectory, SXP, EndpointProfile, SecurityGroups, AdaptiveNetwork

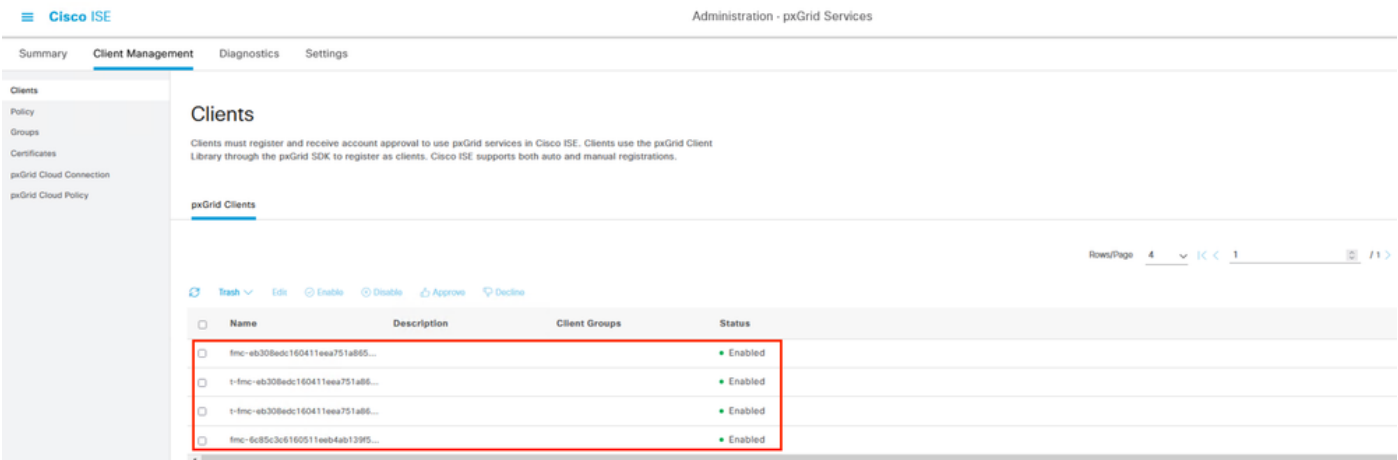
[INFO]: All requested ISE Services are online.

Secondary host:

```
[INFO]: PXGrid v2 is enabled
[INFO]: pxgrid 2.0: account activate succeeded
[INFO]: Successful connection to ssptise02.ssptsec.mex:8910
[INFO]: Successful connection to ssptise01.ssptsec.mex:8910
[INFO]: These ISE Services are up: SessionDirectory, SXP, EndpointProfile, SecurityGroups, AdaptiveNetwork
[INFO]: All requested ISE Services are online.
```

在ISE上验证。

当FMC pxGrid客户端成功集成到ISE时，您 然后请参阅(如果 Administration > pxGrid Services > Client Management > Clients菜单) 包含名为fmc的客户端，且 启用。



PxGrid客户端可用并启用。

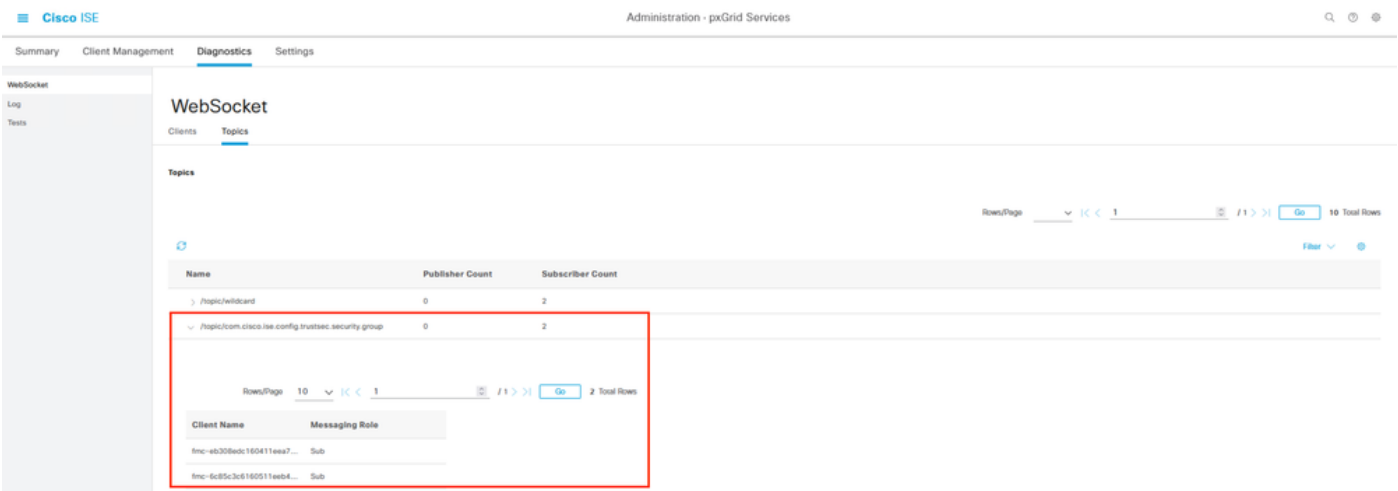


在您使用FMC的情况下，高可用性，然后，您会看到主要和辅助设备，如下例所示：

WebSocket在ISE上可用。

在下一个选项卡中 从此菜单 已命名 Topics, 也可以 验证FMC用户已添加到ISE发布的pxGrid主题。

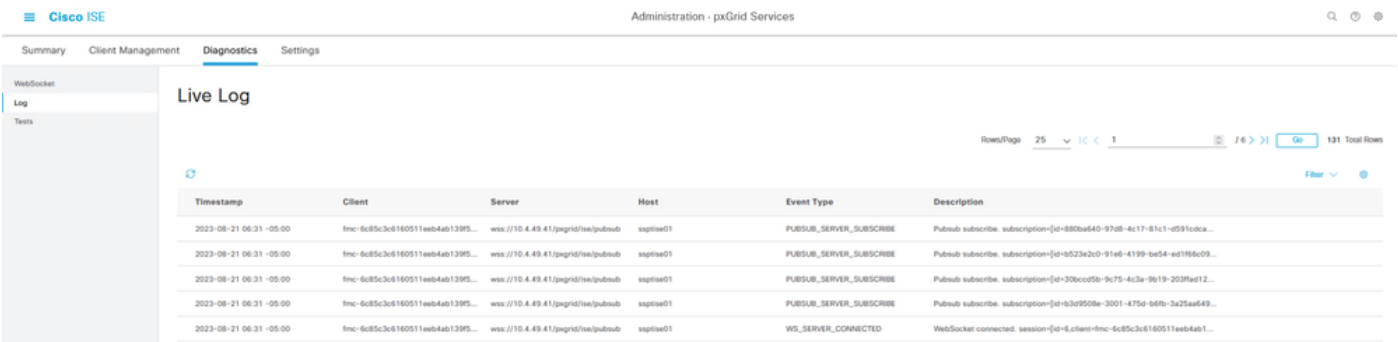
例如，有一个主题与中的安全组相关 其中 您 可以看到两个FMC 订阅和接收相关的信息 到 SGT 由 ISE发布。



每个pxGrid用户的主题。

I在菜单Administration > pxGrid Services > Diagnostics > Log, 重要事件 显示pxGrid通信中的“相关” (对于已启用功能的节点) 。

这些描述的是与集成相关的信息。



PxGrid实时日志。

故障排除

排除FMC故障。

确认FMC能够按主机名解析自己的主机名和ISE节点。

例如：

<#root>

> expert

admin@sspt_fmc01_lab:~\$ ping sspt_fmc01_lab

PING sspt_fmc01_lab (10.4.49.51) 56(84) bytes of data.

```

64 bytes from sspt_fmc01_lab (10.4.49.51): icmp_seq=1 ttl=64 time=0.029 ms
64 bytes from sspt_fmc01_lab (10.4.49.51): icmp_seq=2 ttl=64 time=0.071 ms
64 bytes from sspt_fmc01_lab (10.4.49.51): icmp_seq=3 ttl=64 time=0.055 ms
^C
--- sspt_fmc01_lab ping statistics ---
3 packets transmitted, 3 received,
0% packet loss, time 27ms

admin@sspt_fmc01_lab:~$ ping ssptise01
PING ssptise01.ssptsec.mex (10.4.49.41) 56(84) bytes of data.
64 bytes from ssptise01.ssptsec.mex (10.4.49.41): icmp_seq=1 ttl=64 time=0.586 ms
64 bytes from ssptise01.ssptsec.mex (10.4.49.41): icmp_seq=2 ttl=64 time=0.646 ms
64 bytes from ssptise01.ssptsec.mex (10.4.49.41): icmp_seq=3 ttl=64 time=0.743 ms
^C
--- ssptise01.ssptsec.mex ping statistics ---
3 packets transmitted, 3 received,
0% packet loss, time 82ms
rtt min/avg/max/mdev = 0.586/0.658/0.743/0.068 ms
admin@sspt_fmc01_lab:~$
admin@sspt_fmc01_lab:~$ ping ssptise02

PING ssptise02.ssptsec.mex (10.4.49.42) 56(84) bytes of data.
64 bytes from ssptise02.ssptsec.mex (10.4.49.42): icmp_seq=1 ttl=64 time=0.588 ms
64 bytes from ssptise02.ssptsec.mex (10.4.49.42): icmp_seq=2 ttl=64 time=0.609 ms
64 bytes from ssptise02.ssptsec.mex (10.4.49.42): icmp_seq=3 ttl=64 time=0.628 ms
^C
--- ssptise02.ssptsec.mex ping statistics ---
3 packets transmitted, 3 received
, 0% packet loss, time 45ms
rtt min/avg/max/mdev = 0.588/0.608/0.628/0.025 ms

```

确保 ADI进程已启动并正在运行：

```
<#root>
```

```
>
```

```
expert
```

```
sudo suadmin@sspt_fmc01_lab:~$
```

```
sudo su
```

```
root@sspt_fmc01_lab:/Volume/home/admin#
```

```
pmtool status | grep adi
```

```
adi (normal) - Running 7911
```

E确保从FMC到ISE的通信 port TCP 8910允许。来自FMC CLI 我们可以 配置 a tcpdump 数据包捕获，用于确认双向通信。

```
<#root>
```

```
>
```

```
expert
```

```
sudo suadmin@sspt_fmc01_lab:~$
```

```
sudo su
```

```
root@sspt_fmc01_lab:/Volume/home/admin#
```

```
tcpdump -i any tcp and port 8910
```

```
22:34:08.415370 IP
```

```
sspt_fmc01_lab.46248 > ssptise01.ssptsec.mex.8910
```

```
: Flags [S], seq 3033526171, win 29200, options [mss 1460,sackOK,TS val 2701166399 ecr 0,nop,wscale 7],  
22:34:08.415840 IP
```

```
ssptise01.ssptsec.mex.8910 > sspt_fmc01_lab.46248
```

```
: Flags [S.], seq 3024877968, ack 3033526172, win 28960, options [mss 1460,sackOK,TS val 2268665064 ecr  
22:34:08.415894 IP
```

```
sspt_fmc01_lab.46248 > ssptise01.ssptsec.mex.8910
```

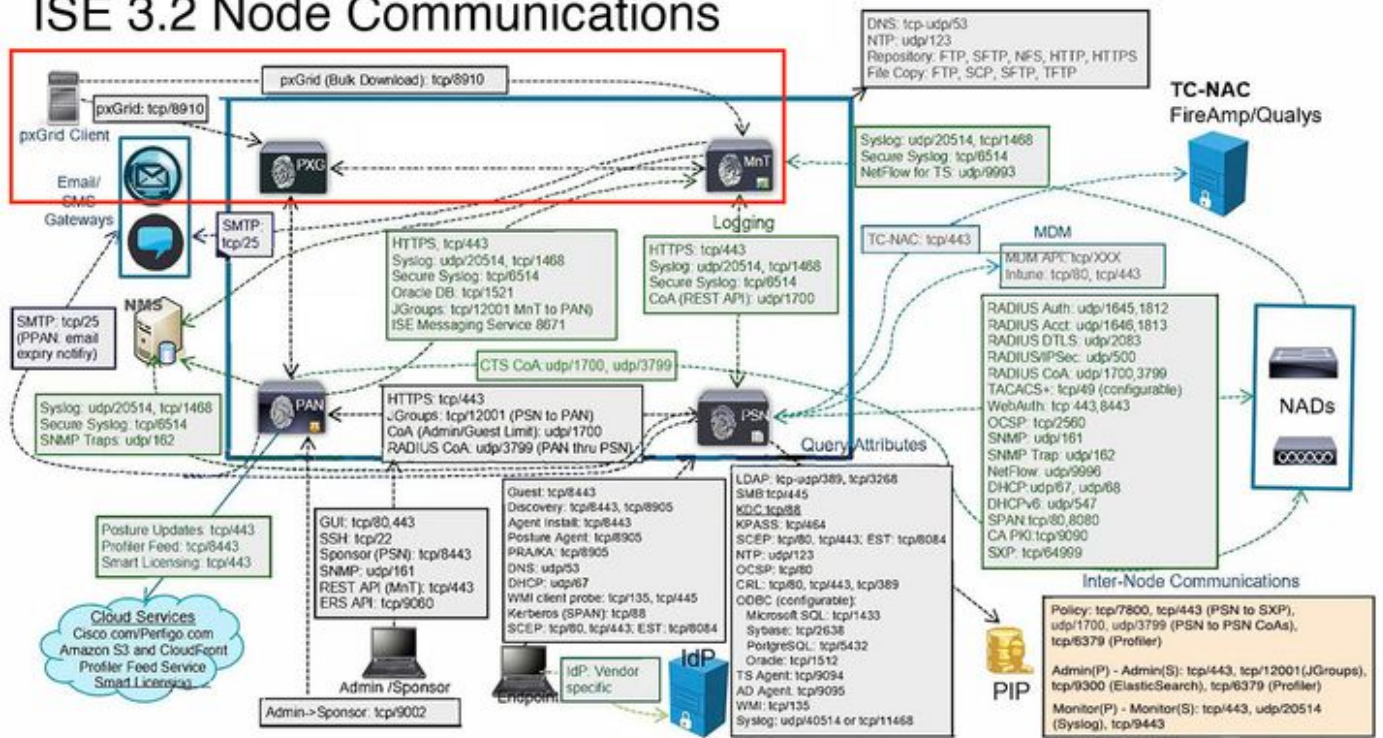
```
: Flags [.], ack 1, win 229, options [nop,nop,TS val 2701166400 ecr 2268665064], length 0  
[...]
```

ISE故障排除。

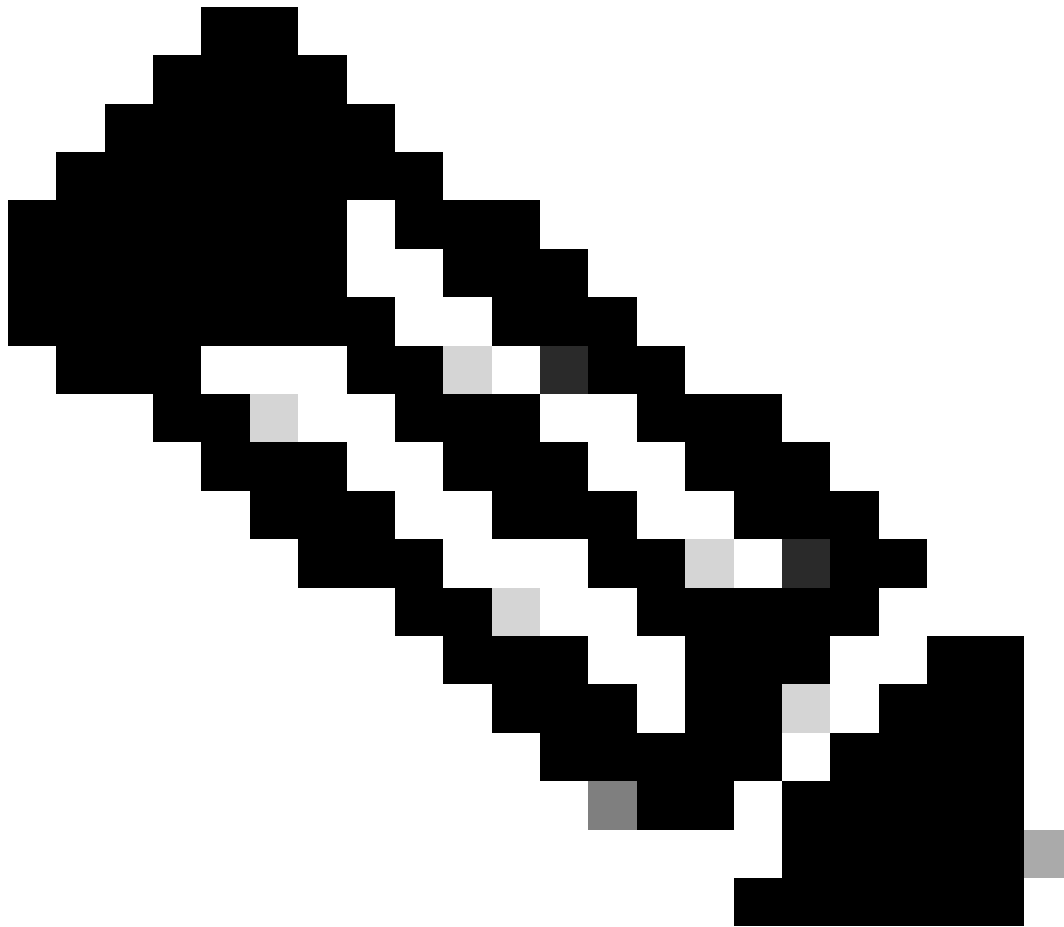
验证端口8910上的通信 运行正常。

这是pxGrid客户端使用的端口用于与pxGrid节点和MnT节点通信以批量下载信息。

ISE 3.2 Node Communications



ISE环境中的PxGrid交互。



注意：pxGrid客户端(在本例中，FMC与pxGrid节点和辅助MNT(SMNT)节点通信以获取 (批量下载) 信息，如果SMNT发生故障，则通过主要MNT查找信息。

I在与pxGrid客户端进行通信的ISE节点上，您可以查看 如果 端口是 打开或 如果有套接字连接到 那个端口。

```
#show ports | include 8910  
tcp: (output omitted), :::8910,
```

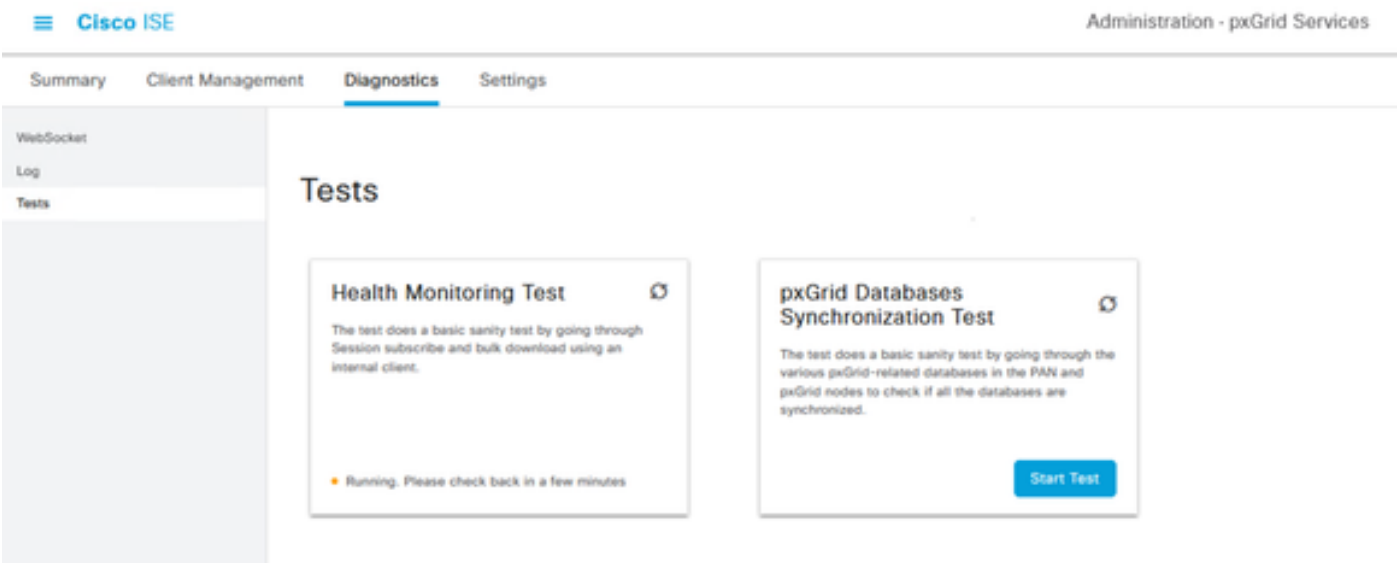
在ISE上有2项测试可用于诊断pxGrid实施的总体状态。

这些可在菜单中找到 Administration > pxGrid Services > Diagnostics > Test。

此部分显示的测试在ISE内部执行。

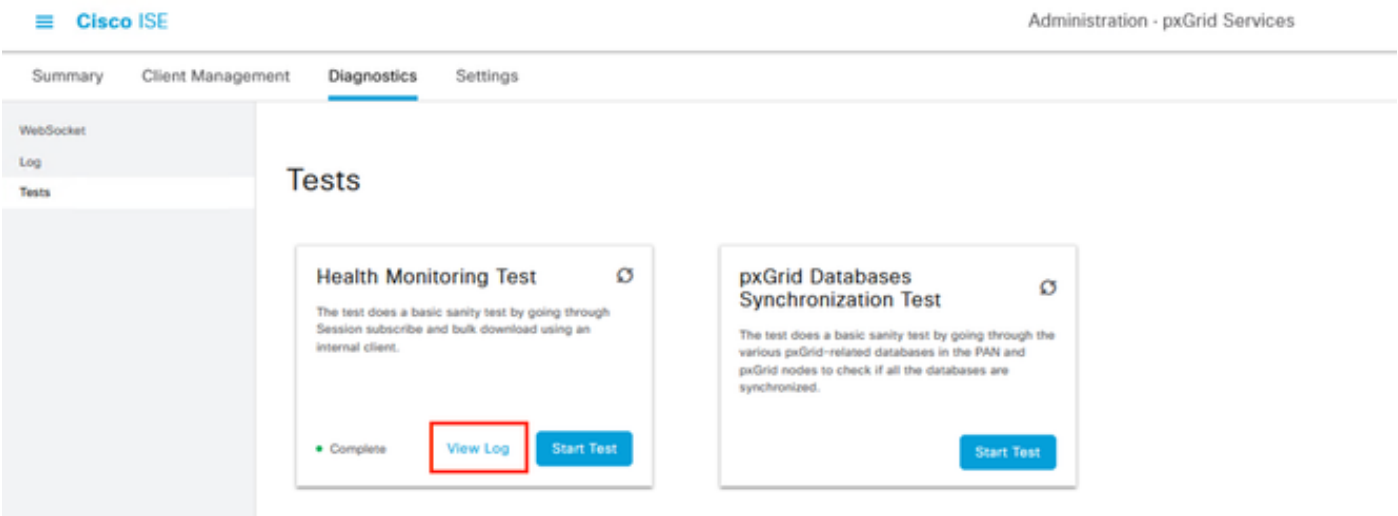
运行状况监控测试 查看pxGrid服务外观 up，评估客户端是否可以访问pxGrid控制器发布的会话目录、服务和主题。

选择 选项 开始 测试 并等待日志的收集。



PxGrid运行状况监控测试。

测试完成后，选择 选项 查看日志。 在本例中，日志的内容 is：



检查运行状况监控测试。

```
22-Aug-2023 17:03:13 [INFO] ***** pxGrid Session Directory Test *****
22-Aug-2023 17:03:13 [INFO] ----- Starting Connection Test -----
22-Aug-2023 17:03:14 [INFO] pxGrid Node: ssptise01.ssptsec.mex
22-Aug-2023 17:03:14 [INFO] wsPubsubServiceName=com.cisco.ise.pubsub
22-Aug-2023 17:03:14 [INFO] sessionTopic=/topic/com.cisco.ise.session
22-Aug-2023 17:03:14 [INFO] sessionRestBaseUrl=https://ssptise01.ssptsec.mex:8910/pxgrid/mnt/sd
22-Aug-2023 17:03:14 [INFO] wsUrl=wss://ssptise02.ssptsec.mex:8910/pxgrid/ise/pubsub
22-Aug-2023 17:03:15 [INFO] ----- Connection Test Completed -----
22-Aug-2023 17:03:15 [INFO] ----- Starting Download Test -----
22-Aug-2023 17:03:15 [INFO] Downloading sessions since 2023-08-21T17:03:15.273-06:00
22-Aug-2023 17:03:15 [INFO] Response status=200
22-Aug-2023 17:03:15 [INFO] Number of sessions read: 0
```

```

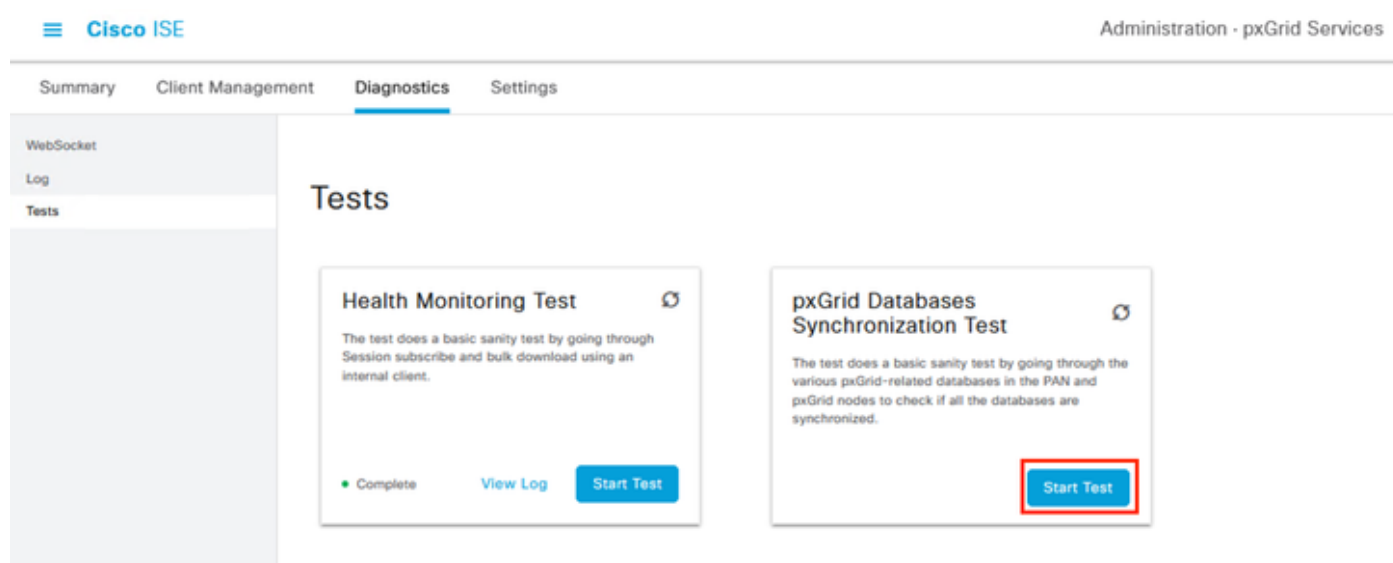
22-Aug-2023 17:03:15 [INFO] ----- Download Test Completed -----
22-Aug-2023 17:03:15 [INFO] ----- Starting Subscribe Test -----
22-Aug-2023 17:03:16 [INFO] STOMP CONNECT host=ssptise02.ssptsec.mex
22-Aug-2023 17:03:16 [INFO] STOMP SUBSCRIBE topic=/topic/com.cisco.ise.session
22-Aug-2023 17:03:16 [INFO] STOMP CONNECTED version=1.2
22-Aug-2023 17:07:16 [INFO] A total of 0 notifications were received.
22-Aug-2023 17:07:16 [INFO] STOMP RECEIPT id=77
22-Aug-2023 17:07:19 [INFO] ----- Subscribe Test Completed -----
22-Aug-2023 17:07:19 [INFO] ***** pxGrid Session Directory Test Complete *****

```

PxGrid数据库同步测试检查是否 信息 数据库中的PAN和pxGrid节点之间正确且已同步。

因此，发送到pxGrid用户的信息是 准确。

选择 选项 开始测试 等待评估结果。



PxGrid数据库同步测试。

从生成的日志中获得此输出。

```

ssptise01.ssptsec.mex : In Sync
ssptise02.ssptsec.mex : In Sync

```

```

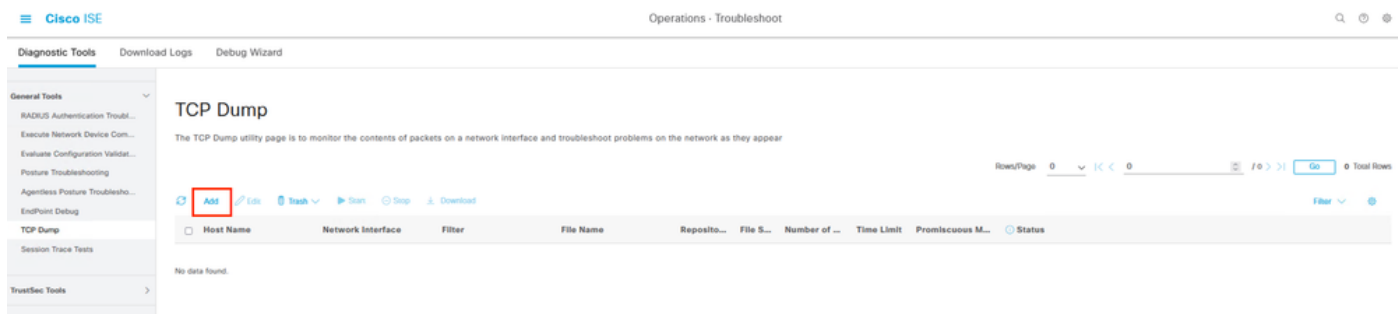
Primary PAN : ssptise01.ssptsec.mex
pxGrid Nodes : ssptise01.ssptsec.mex ssptise02.ssptsec.mex

```

收集捕获时间 从指向主FMC节点的pxGrid节点。

导航至菜单 Operations > Troubleshoot > Diagnostic Tools > TCP Dump,

选择 选项 到 Add (添加) 新的捕获。



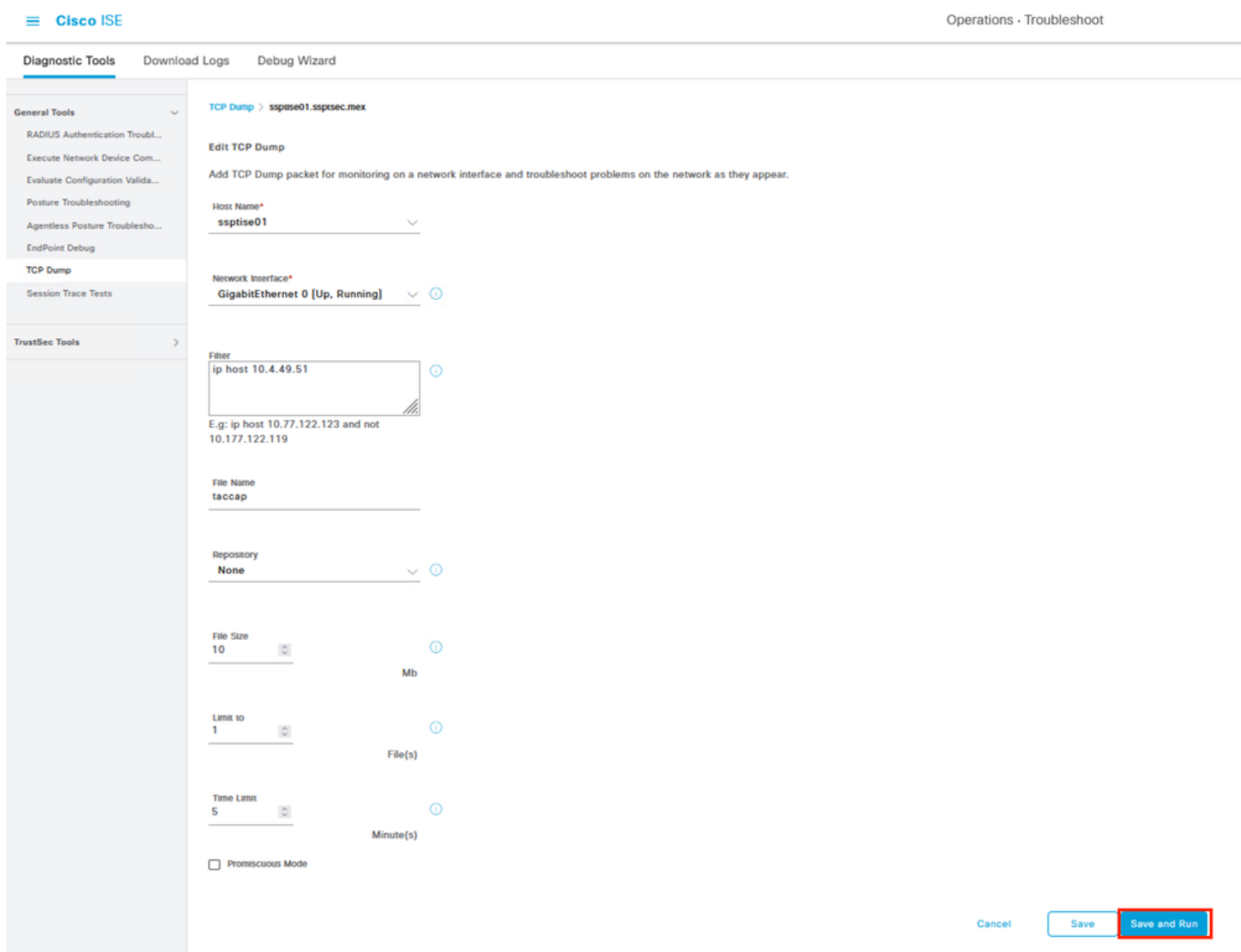
在ISE上生成数据包捕获。

配置捕获参数。

在 主机名，选择在FMC中选择的主pxGrid节点。

过滤器 此流量 语法 ip host <FMC IP>

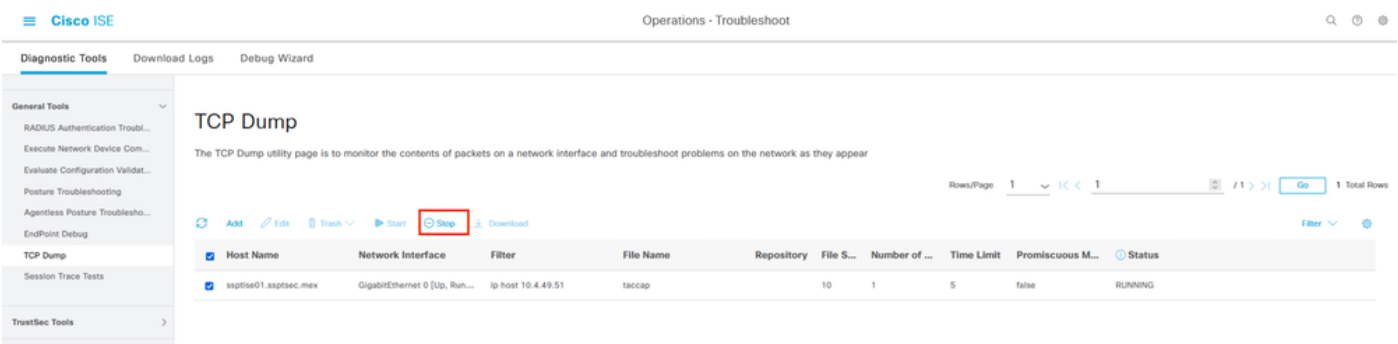
为捕获命名 然后 继续 到 保存 并运行。



数据包捕获配置示例。

在另一窗口中，在FMC菜单中 集成>其他集成>身份 来源，测试通过pxGrid通道与ISE的连接。

W当你得到测试的结果时，继续到S顶部在ISE上捕获。



停止ISE上的数据包捕获。

下载 捕获并开始分析。此方案显示可用作参考的工作连接的捕获。

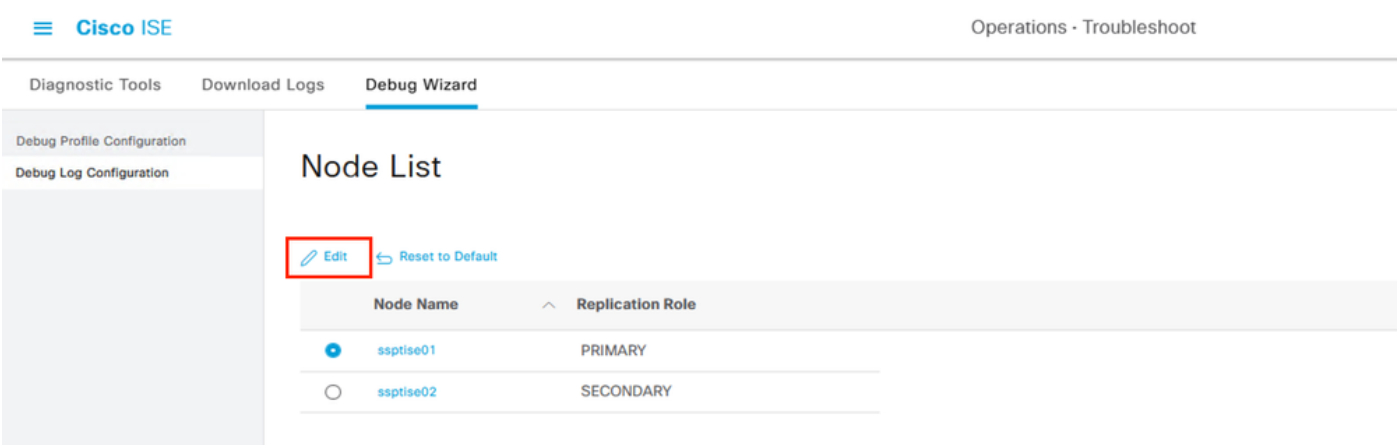
10.4.49.51	10.4.49.41	TCP	74	47508 → 8910 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=2738457626 TSecr=0 WS=128
10.4.49.41	10.4.49.51	TCP	74	8910 → 47508 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=2305956319 TSecr=2738457626 WS=128
10.4.49.51	10.4.49.41	TCP	66	47508 → 8910 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=2738457627 TSecr=2305956319
10.4.49.51	10.4.49.41	TLV1.2	389	Client Hello
10.4.49.41	10.4.49.51	TCP	66	8910 → 47508 [ACK] Seq=1 Ack=324 Win=30080 Len=0 TSval=2305956319 TSecr=2738457627
10.4.49.41	10.4.49.51	TCP	7306	8910 → 47508 [ACK] Seq=1 Ack=324 Win=30080 Len=7240 TSval=2305956341 TSecr=2738457627 [TCP segment of a reassembled PDU]
10.4.49.41	10.4.49.51	TLV1.2	462	Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
10.4.49.51	10.4.49.41	TCP	66	47508 → 8910 [ACK] Seq=324 Ack=7637 Win=44544 Len=0 TSval=2738457650 TSecr=2305956341
10.4.49.51	10.4.49.41	TLV1.2	1783	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
10.4.49.41	10.4.49.51	TCP	66	8910 → 47508 [ACK] Seq=7637 Ack=2041 Win=33536 Len=0 TSval=2305956345 TSecr=2738457653
10.4.49.41	10.4.49.51	TLV1.2	72	Change Cipher Spec
10.4.49.41	10.4.49.51	TLV1.2	111	Encrypted Handshake Message
10.4.49.51	10.4.49.41	TCP	66	47508 → 8910 [ACK] Seq=2041 Ack=7688 Win=44544 Len=0 TSval=2738457658 TSecr=2305956349
10.4.49.51	10.4.49.41	TLV1.2	99	Application Data
10.4.49.41	10.4.49.51	TCP	66	8910 → 47508 [ACK] Seq=7688 Ack=2074 Win=33536 Len=0 TSval=2305956391 TSecr=2738457658
10.4.49.51	10.4.49.41	TLV1.2	615	Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application Data
10.4.49.41	10.4.49.51	TCP	66	8910 → 47508 [ACK] Seq=7688 Ack=2623 Win=36480 Len=0 TSval=2305956391 TSecr=2738457699
10.4.49.51	10.4.49.41	TLV1.2	515	Application Data
10.4.49.41	10.4.49.51	TLV1.2	100	Application Data
10.4.49.51	10.4.49.41	TCP	66	47508 → 8910 [ACK] Seq=2623 Ack=8171 Win=47488 Len=0 TSval=2738457708 TSecr=2305956400
10.4.49.51	10.4.49.41	TCP	66	47508 → 8910 [FIN, ACK] Seq=2623 Ack=8171 Win=47488 Len=0 TSval=2738457708 TSecr=2305956400
10.4.49.41	10.4.49.51	TLV1.2	97	Encrypted Alert
10.4.49.41	10.4.49.51	TCP	66	8910 → 47508 [FIN, ACK] Seq=8202 Ack=2624 Win=36480 Len=0 TSval=2305956401 TSecr=2738457708

ISE和FMC之间的PxGrid通信。

此外，在ISE上，您可以收集与px相关的调试网格处理。

浏览菜单 Operations > Troubleshoot > Debug Wizard > Debug 日志配置，

选择要分析的对应ISE节点，然后 编辑。



选择要在ISE上调试的节点。

过滤显示的组件并更改 日志级别到 DEBUG the pxgrid 组件 到 继续 分析。

保存 配置。

Diagnostic Tools Download Logs **Debug Wizard**

Debug Profile Configuration
Debug Log Configuration

Node List > ssptise01.sspitsec.mex

Debug Level Configuration

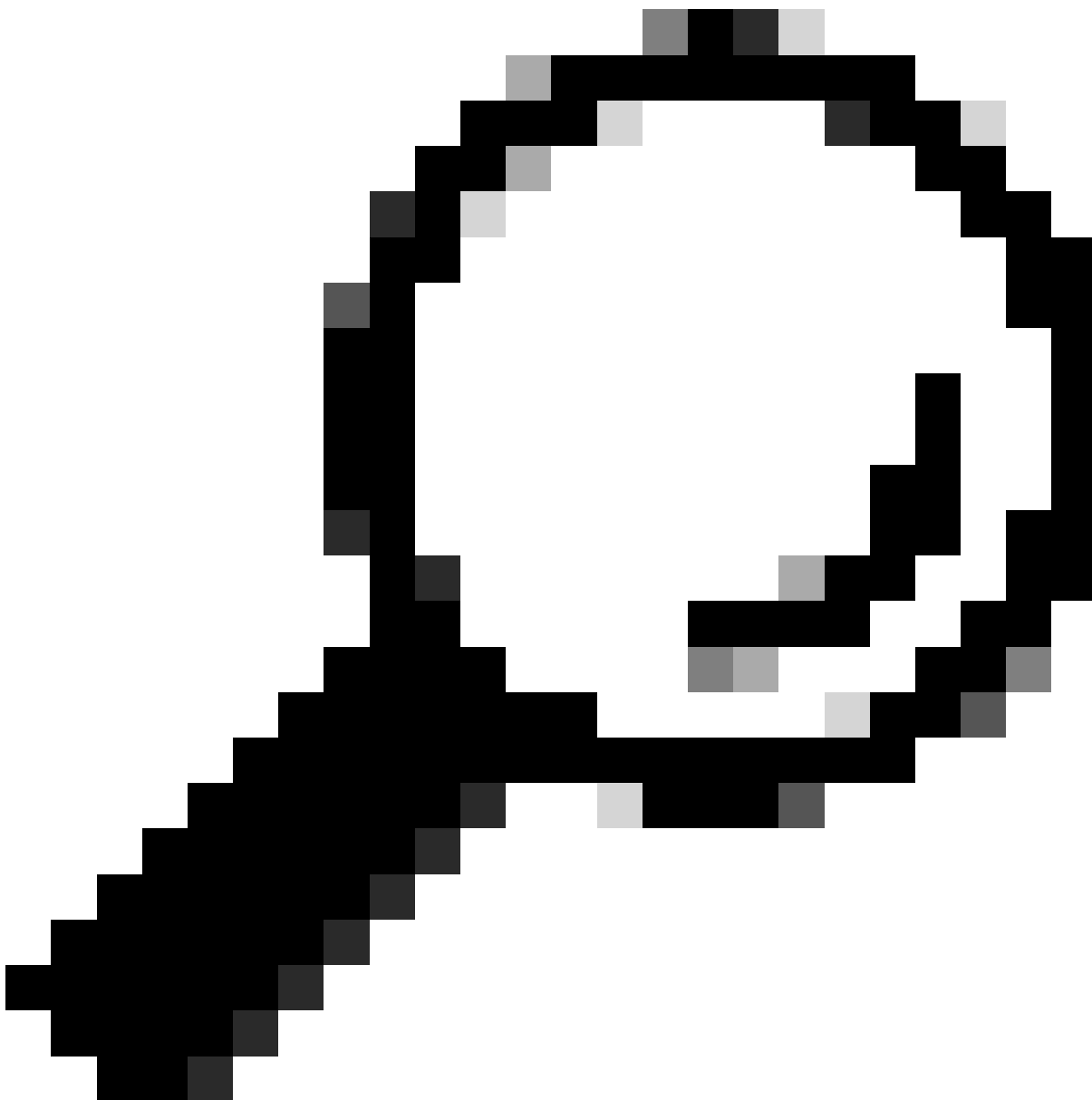
[Edit](#) [Reset to Default](#)

	Component Name	Log Level	Description	Log file Name
	pxgrid			
☐	pxgrid	DEBUG	pxGrid messages	pxgrid-server.log
☐	pxGrid Cloud	INFO	pxGrid Cloud messages	pxcloud.log Save Cancel
☐	pxGrid Direct	INFO	pxGrid Direct backend and UI log messages	ise-pxgriddirect.log, pxgriddirect.log

将pxGrid组件更改为调试级别。

重现要分析的行为，然后继续分析在pxgrid-server.log文件中收集的日志。其他日志您可以在ISE节点上查看以下内容进行故障排除：

```
#show logging application | include pxgrid  
ise-pxgriddirect.log  
pxgrid/pxgrid-server.log  
pxgrid/pxgrid-test.log  
pxgrid/pxgrid_dbsync_summary.log  
pxgrid/pxgrid_internal_dbsync_summary.log  
pxgriddirect.log
```

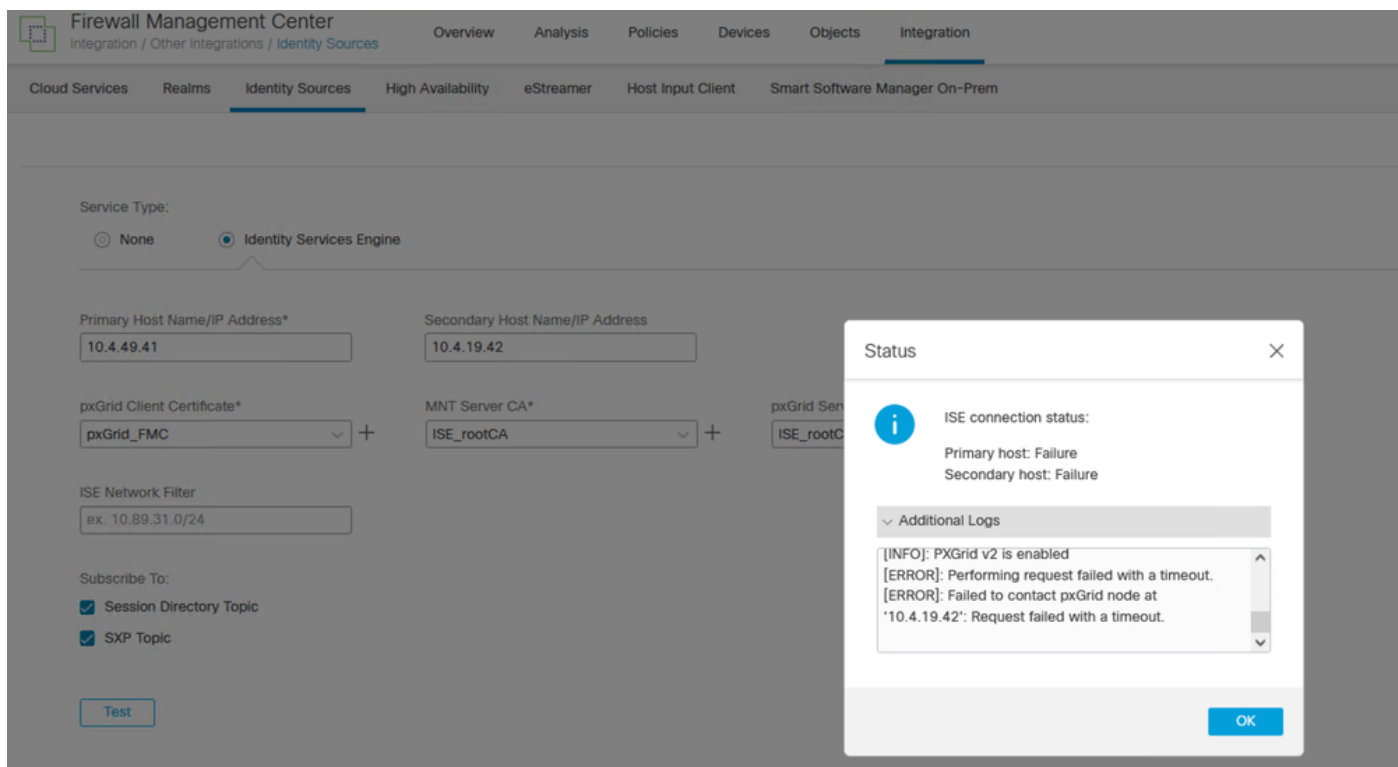


提示：有关更多日志收集建议，请查看[如何在ISE 3.x版本上启用调试](#)视频。

常见问题.

PxGrid用户客户端未在ISE上获得批准。

对于此使用案例，FMC测试pxGrid按钮的相关输出显示以下行为：



FMC pxGrid连接失败。

Primary host:

```
[INFO]: PXGrid v2 is enabled
[ERROR]: pxgrid 2.0: failed account activation. accountState=PENDING
[ERROR]: Failed to contact pxGrid node at '10.4.49.41': pxgrid2.0: Could not activate account
```

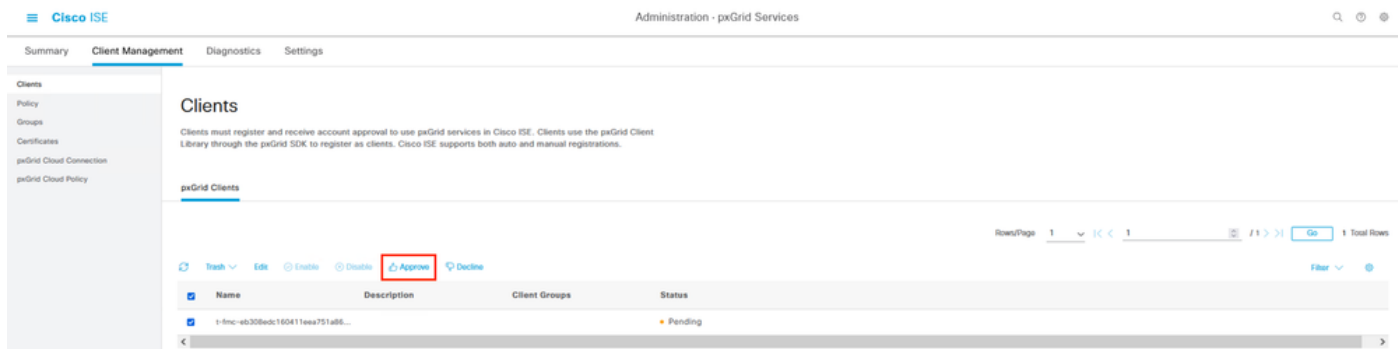
Secondary host:

```
[INFO]: PXGrid v2 is enabled
[ERROR]: Performing request failed with a timeout.
[ERROR]: Failed to contact pxGrid node at '10.4.19.42': Request failed with a timeout.
```

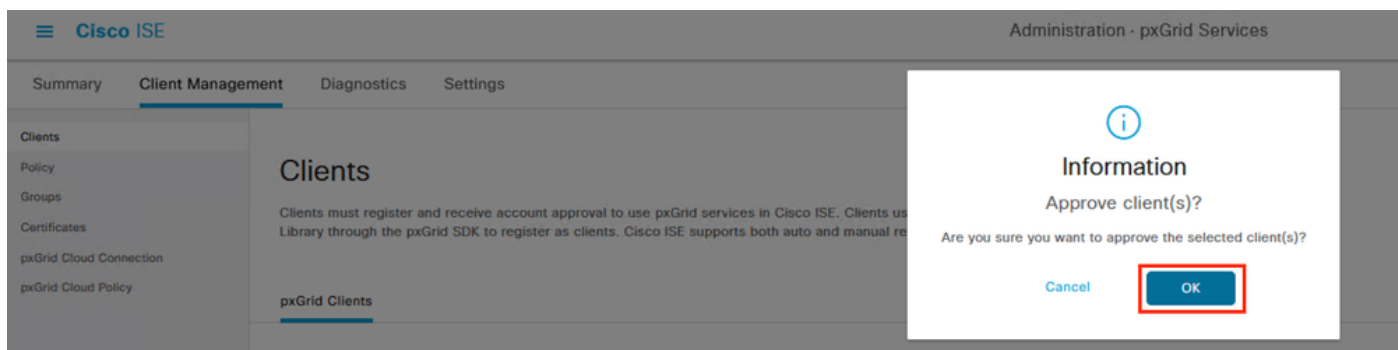
在ISE上，请注意菜单Administration > PxGrid Services > Client Management > Clients中的行为，该行为表示pxGrid客户端(FMC)正在等待审批。

选择Approve按钮，确认下一个窗口中的选择，然后再次尝试集成。

这次集成成功。



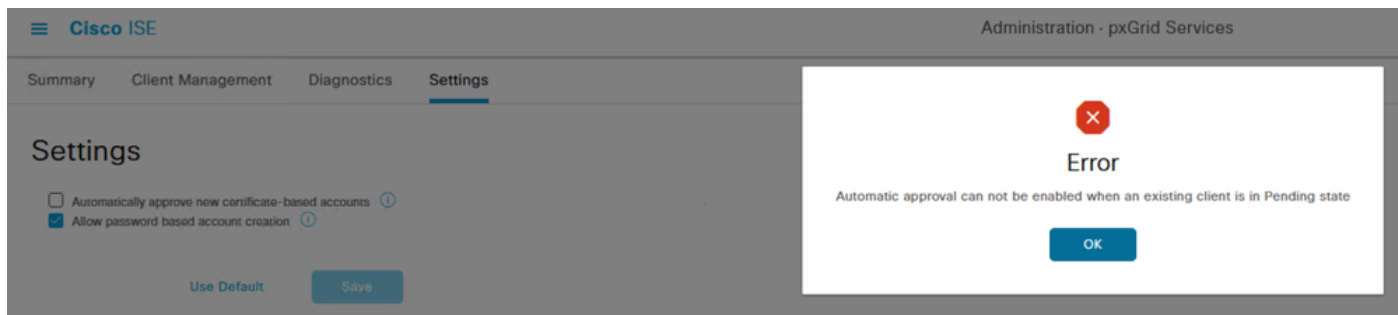
FMC客户端处于待处理状态。



确认pxGrid客户端的批准。

请注意，如果要启用基于证书的pxGrid客户端的自动审批。

批准/拒绝上一页中的客户端，因为可能会出现此警报。



与审批pxGrid客户端相关的错误。

PxGrid ISE证书 链 incomplete.

在此场景中，如果导航到菜单Administration > System > Certificate，请选择pxgrid证书并选择View选项，

如果证书有问题，可能会出现这些相关错误。

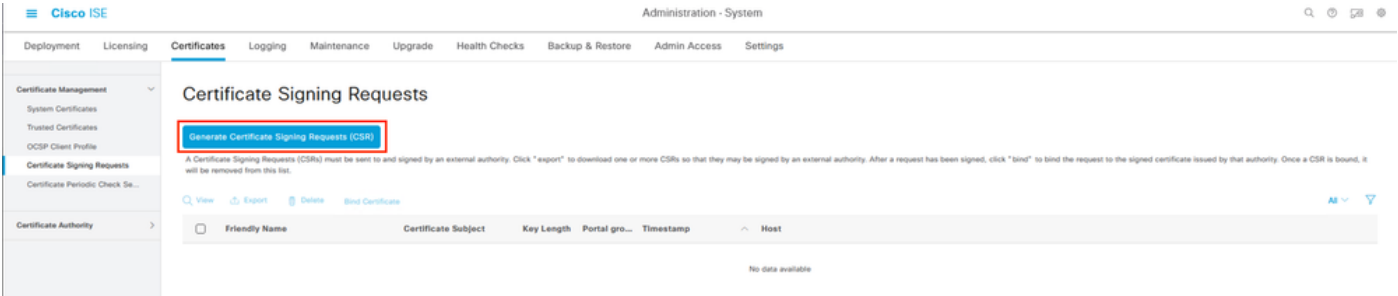
 Certificate trust chain is incomplete

与证书链不完整相关的错误。

T检查的第一步是是否已完成ISE根CA在View选项中编辑。

如果层次结构中缺少证书，您可以颁发整个ISE部署根CA。

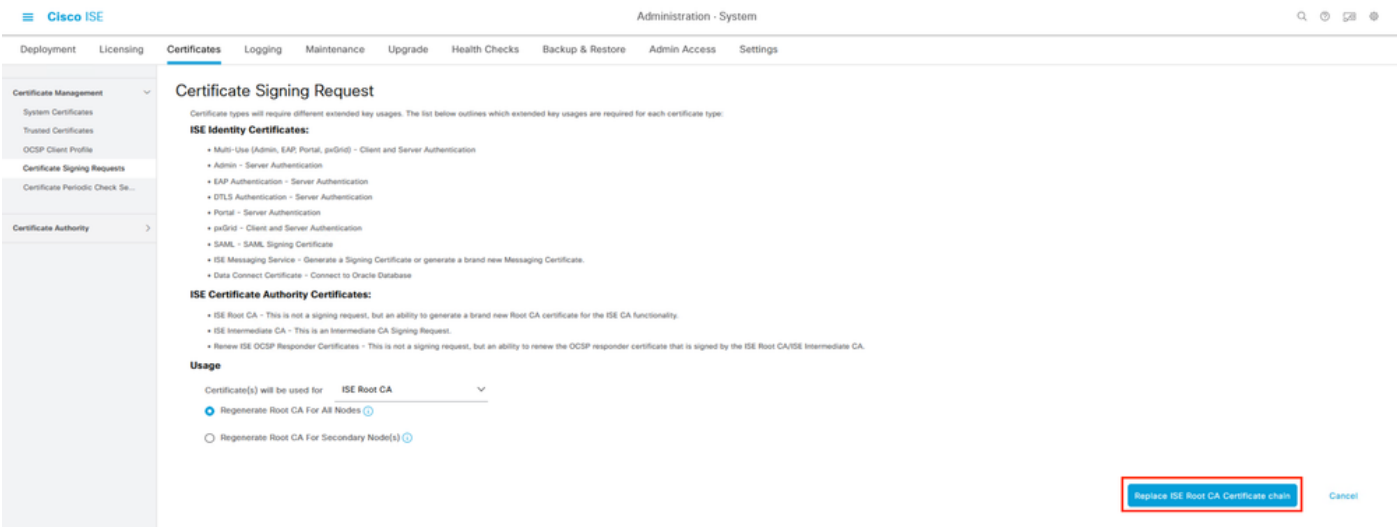
B浏览到菜单Administration > System > Certificates > Certificate Management > Certificate Signing Request(CSR)和 选择该按钮。



在ISE上生成CSR。

在此菜单中，选择 使用ISE根CA 和为所有节点重新生成ISE根CA。

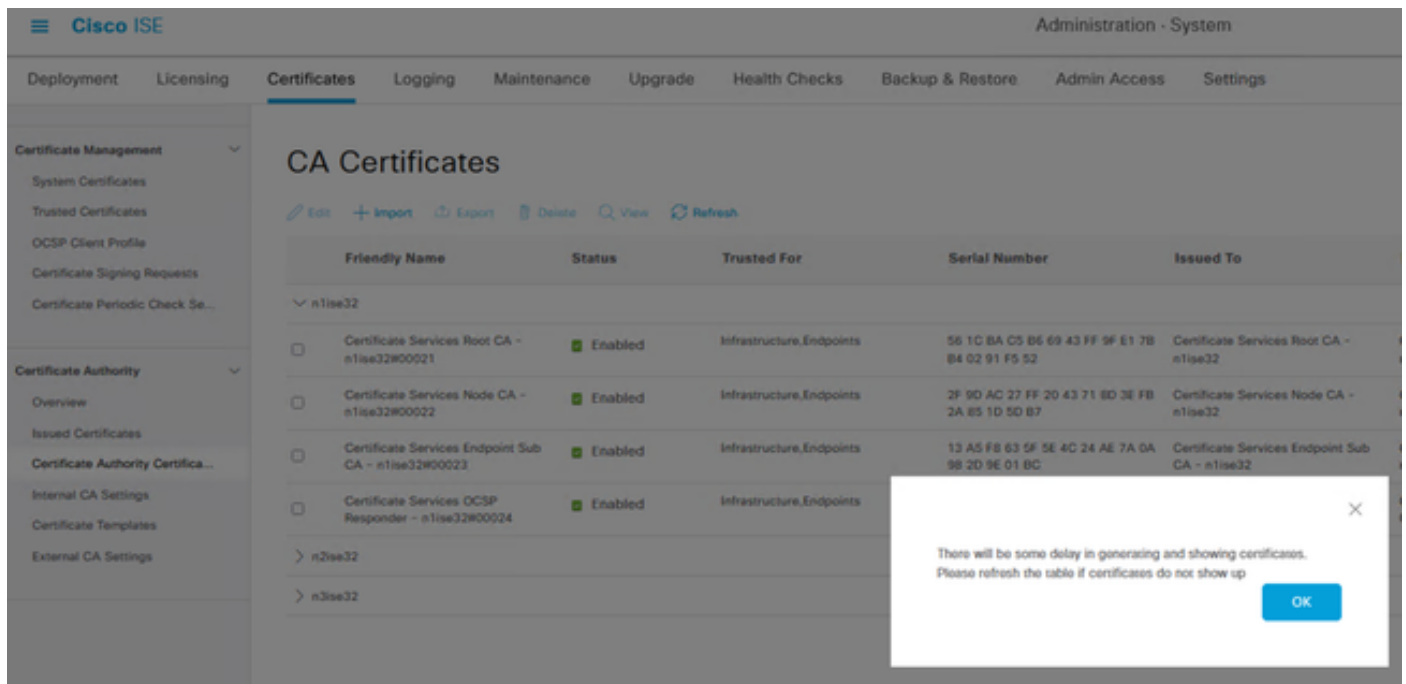
继续按钮操作 替换ISE根CA证书链。



配置证书签名请求。

等待在IMP的所有节点中生成证书病理。

完成后，ISE显示下一个通知。



确认证书的生成。

确认pxGRID证书信任链已完成 通过选择选项 查看 在系统证书中。

参考.

[PxGrid思科开发人员页面。](#)

[思科身份服务引擎管理员指南，版本3.2，章节：思科pxGrid。](#)

[思科身份服务引擎安装指南，版本3.2，章节：Cisco ISE端口参考](#)

[思科身份服务引擎CLI参考指南，版本2.4](#)

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）。