

通過FMC 7.2.4整合配置ISE 3.2並對其進行故障排除

目錄

[簡介](#)

[必要條件](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[準備ISE以進行整合。](#)

[準備FMC進行整合。](#)

[設定ISE和FMC之間的pxGrid連線。](#)

[驗證](#)

[驗證FMC。](#)

[在ISE上驗證。](#)

[疑難排解](#)

[FMC故障排除。](#)

[ISE故障排除。](#)

[常見問題。](#)

[PxGrid使用者客戶端未在ISE上獲得批准。](#)

[PxGrid ISE證書鏈不完整。](#)

[參考。](#)

簡介

本文檔介紹使用Platform Exchange Grid連線將Identity Services Engine與防火牆管理中心整合的過程。

必要條件

思科建議瞭解以下主題：

- 身分識別服務引擎 (ISE)
- Platform Exchange Grid
- 防火牆管理中心(FMC)
- TLS/SSL證書。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 身分識別服務引擎(ISE)版本3.2補丁3
- 防火牆管理中心版本7.2.4

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.

本文檔提供使用pxGrid版本2整合FMC和ISE的解決方案。

Cisco Firepower Management Center(FMC)是下一代防火牆和入侵防禦系統的集中平台，提供策略管理、威脅檢測和事件響應。

思科身份服務引擎是一個全面的解決方案，通過提供身份驗證、授權和責任(AAA)以及策略實施服務來提供對終端的安全訪問。

Platform Exchange Grid(pxGrid)允許您在多供應商跨平台網路之間交換資訊。

通過這種整合，您可以獲得安全監控、威脅檢測和基於共用資訊設定的網路策略。

PxGrid框架有2個版本。要使用的版本取決於您需要檢視的ISE版本和修補程式。

從ISE 3.1版開始，所有pxG來自ISE的RID連線基於pxgrid版本 2.

PxGrid版本1.

T此框架的第一個版本 (pxGrid v1) 特徵在於通過命令show application status ise看到的可維護性 在隨後的輸出中顯示。

在節點中啟用pxGrid功能時，您會看到pxGrid 功能 處於運行狀態.

```
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的可維護性。

在此平台版本中，已知只有一個pxGrid節點的pxGrid進程處於運行狀態，而其他pxGrid節點處於備用狀態。

這些節點持續監控pxGrid節點的狀態，同時運行相關服務。

其中主pxGrid節點進行了升級，另一個pxGrid節點啟用了其pxGrid服務。

但是，當發生此故障轉移時，這意味著停機時間。

第一個版本的pxgrid是基於可擴充訊息和存在通訊協定(XMPP)中的通訊，該通訊協定是合作和語音基礎架構中使用的一組技術。

pxGrid v1連線中共用的主題包括：

- 會話目錄
- 終端配置檔案後設資料
- Trustsec後設資料
- 端點保護功能
- 自適應網路控制
- MDM_Offline主題
- 身份
- SXP

PxGrid版本2.

本文檔介紹如何使用PxGrid版本2。此平台在ISE和WebSocket協定上使用REST操作運行，從而在資料模型中帶來增強功能、改進的可擴充性、效能和靈活性。

在此版本中，您不會看到使用命令show application status ise運行的pxgrid功能與先前版本相同。

請參閱本文檔中ISE的驗證部分，瞭解要檢查哪些機制以檢視pxGrid功能。

在此版本中，您擁有配置為活動pxGrid節點的所有pxGrid節點。隨時可以交換情報。

在版本1中，只有一個節點將pxGrid的可維護性保持在運行狀態。

pxGrid v2連線中共用的主題包括：

- 會話目錄
- Radius故障
- 探查器配置
- 系統運行狀況
- MDM
- ANC狀態
- TrustSec
- TrustSec配置
- TrustSec SXP
- 終端資產。

作為平台的pxGrid元件。

PxGrid控制器(ISE):必須信任使用pxGrid的每個參與者。

用戶端:可以是不同主題的訂閱者和發佈者。

發佈者：與控制器共用資訊的客戶端。

訂閱者：使用主題資訊的客戶端。

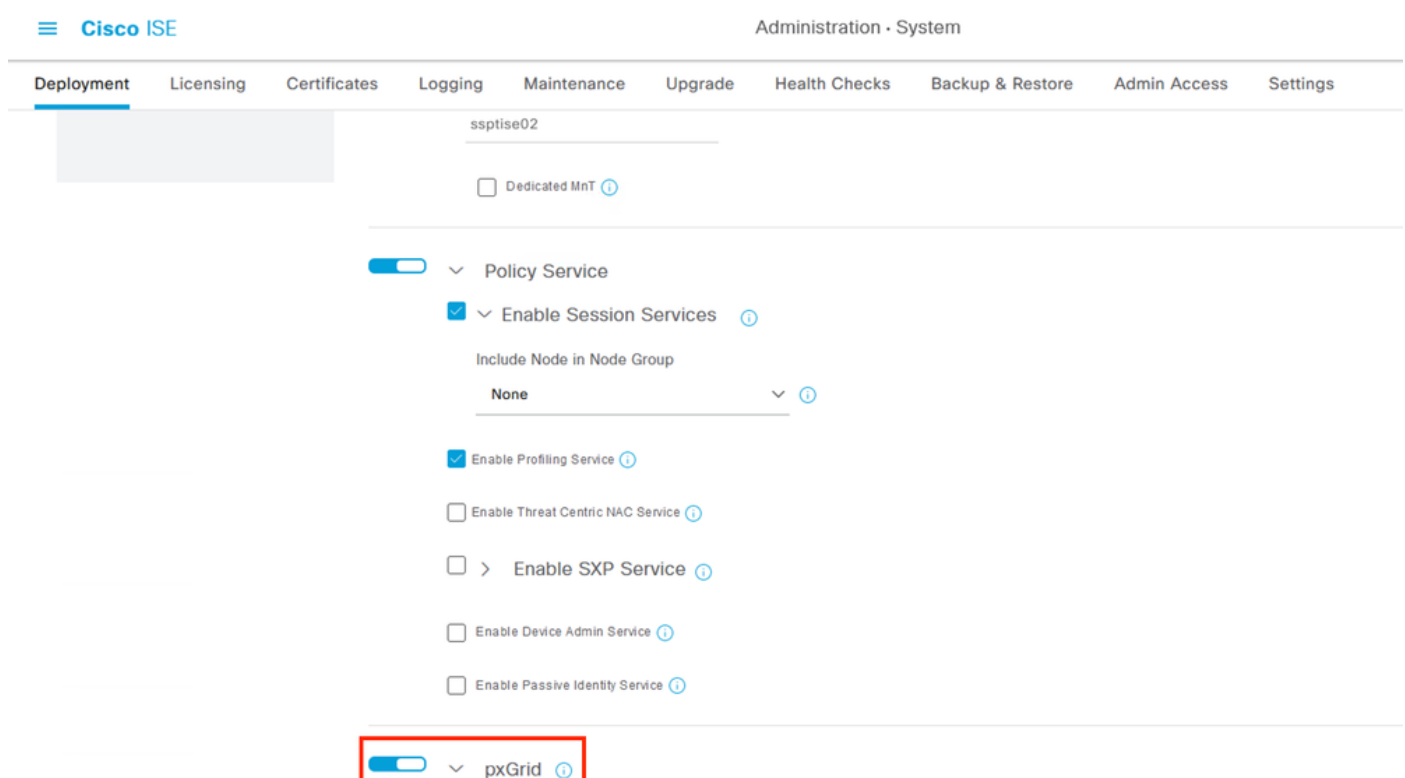
通過此整合，您可以根據ISE共用的資訊及其發佈的主題（與終端活動相關）在FMC上建立內容策略。

設定

準備ISE以進行整合。

步驟1.在Administration > System > Deployment選單中配置ISE節點以在其上運行pxGrid角色。

選擇節點並啟用功能pxGrid。



在節點中啟用ISE pxGrid服務。

步驟2.啟用具有pxGrid功能的節點後，檢視與連線的內部客戶端相關的Websockets的狀態。

導航到Administration > pxGrid Services > Websocket。注意通過IP地址127.0.0.1直接指向ISE服務的客戶端。

Cisco ISE

Administration - pxGrid Services

Q

ⓘ

⚙

SummaryClient ManagementDiagnosticsSettings

WebSocket

Log

Tests

WebSocket

ClientsTopics

Clients

Rows/Page8<<1Go8 Total Rows

Filter

ⓘ

Client Name	Connect To	Session Id	Certificate	Subscriptions	Publications	IP Address	Status
-ise-fanout-ssptise01	ssptise01	ssptise01:0	CN=ssptise01.ss...	/topic/wildcard	/topic/com.cisco.ise.pxgrid...	127.0.0.1	Connected
-ise-fanout-ssptise02	ssptise01	ssptise01:1	CN=ssptise02.ss...	/topic/distributed	/topic/distributed	10.4.49.42	Connected
-ise-fanout-ssptise01	ssptise01	ssptise01:2	CN=ssptise01.ss...	/topic/distributed		10.4.49.41	Connected
-ise-fanout-ssptise02	ssptise02	ssptise02:9	CN=ssptise02.ss...	/topic/wildcard	/topic/com.cisco.ise.pxgrid...	127.0.0.1	Connected
-ise-mnt-ssptise02	ssptise02	ssptise02:11	CN=ssptise02.ss...	/topic/com.cisco.ise.sessio...	/topic/com.cisco.ise.sessio...	10.4.49.42	Connected
-ise-admin-ssptise02	ssptise02	ssptise02:12	CN=ssptise02.ss...		/topic/com.cisco.ise.pxgrid...	10.4.49.42	Connected
-ise-mnt-ssptise01	ssptise02	ssptise02:13	CN=ssptise01.ss...	/topic/com.cisco.ise.sessio...	/topic/com.cisco.ise.sessio...	10.4.49.41	Connected
-ise-admin-ssptise01	ssptise02	ssptise02:14	CN=ssptise01.ss...	/topic/com.cisco.ise.pxgrid...	/topic/com.cisco.ise.pxgrid...	10.4.49.41	Connected

來自ISE的內部WebSocket。

步驟 3. 在選單Administration > pxGrid Services > Settings中導航，然後選擇Automatically approve new certificate-base accounts選項

此時此步驟是可選的，但是對於pxGrid連線，建議啟用此覈取方塊。

您之後可以手動接受FMC作為訂戶。

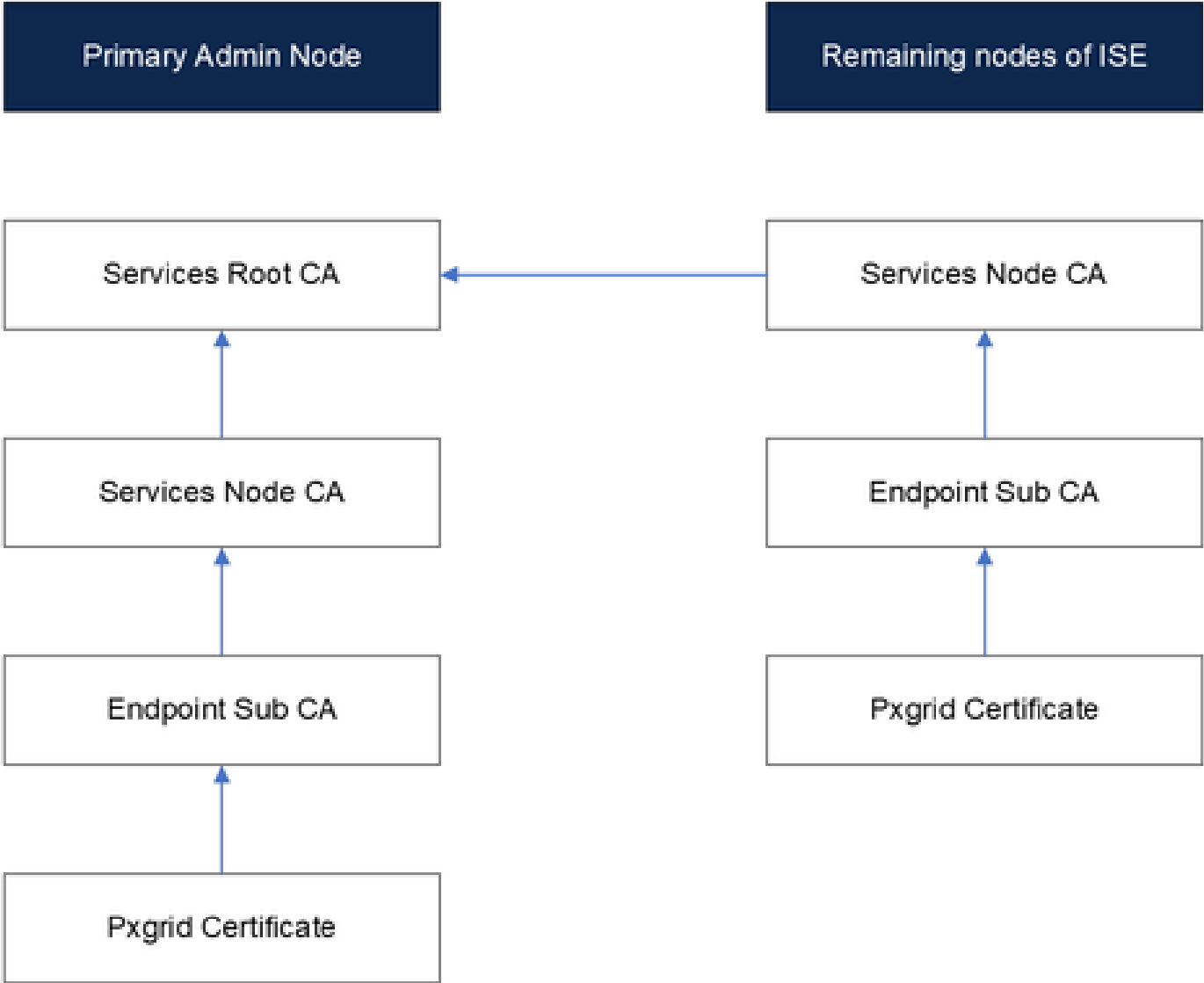
Cisco ISE		Administration - pxGrid Services			
Summary Client Management Diagnostics Settings					
Settings					
☒ Automatically approve new certificate-based accounts ⓘ ☒ Allow password based account creation ⓘ					
Use Default		Save			

為基於pxGrid證書的帳戶啟用自動批准。

步驟 4. 在Administration > System > System Certificates中檢視與您的環境的pxGrid功能相關的證書，

建議在部署的所有節點中具有同一pxGrid證書，這些證書由同一個根證書頒發機構(CA)簽名

在此場景中，我們使用生成的內部ISE證書。對於此版本的ISE，在本示例中，根CA對應於PAN節點。



ISE上的內部證書圖表。



附註：有關ISE上生成的證書的內部結構的詳細資訊，請參閱[瞭解ISE內部證書授權服務。](#)

Administration · System

DeploymentLicensingCertificatesLoggingMaintenanceUpgradeHealth ChecksBackup & RestoreAdmin AccessSettings

Certificate ManagementSystem CertificatesTrusted CertificatesOCSP Client ProfileCertificate Signing RequestsCertificate 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 - ssp01seu1m00001							
CA-sps01se01.ssp01sec.mex, O Un-Certificate Services System CertificateCertificate Services Endpoint Sub CA - ssp01se01#00002	pxGrid		ssp01se01.ssp01sec.mex	Certificate Services Endpoint Sub CA - ssp01se01	Fri, 30 Jun 2023	Sat, 1 Jul 2028	Active
ise01_External_CA	Admin, EAP Authentication, RADIUS DTLS, Portal	Default Portal Certificate Group	ssp01se01.ssp01sec.mex	ssp01se01.ssp01sec.mex	Mon, 3 Jul 2023	Wed, 2 Jul 2025	Active
ssp01se02							
Default self-signed saml server certificate - CN=SAML_ssp01se01.ssp01sec.mex	SAML		SAML_ssp01se01.ssp01sec.mex	SAML_ssp01se01.ssp01sec.mex	Sat, 1 Jul 2023	Thu, 29 Jun 2028	Active
ise02_External_CA	Admin, EAP Authentication, RADIUS DTLS, Portal	Default Portal Certificate Group	ssp02se01.ssp02sec.mex	ssp02se01.ssp02sec.mex	Mon, 3 Jul 2023	Wed, 2 Jul 2025	Active
CN=ssp02se02.ssp02sec.mex, O Un-Certificate Services System CertificateCertificate Services Endpoint Sub CA - ssp02se02#00004	ISE Messaging Service		ssp02se02.ssp02sec.mex	Certificate Services Endpoint Sub CA - ssp02se02	Sat, 1 Jul 2023	Sun, 2 Jul 2028	Active
CN=ssp02se02.ssp02sec.mex, O Un-Certificate Services System CertificateCertificate Services Endpoint Sub CA - ssp02se02#00003	pxGrid		ssp02se02.ssp02sec.mex	Certificate Services Endpoint Sub CA - ssp02se02	Sat, 1 Jul 2023	Sun, 2 Jul 2028	Active

分散式部署中的PxGrid證書。

步驟5.驗證pxGrid證書的狀態。

從上一個選單中，從節點pxGrid證書中選擇一個覈取方塊，然後選擇選項「檢視」。

輸出看起來與pxGrid證書中顯示的輸出類似。

Certificate ManagementSystem CertificatesTrusted CertificatesOCSP Client ProfileCertificate Signing RequestsCertificate 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 - ssp01seu1m00001							
CA-sps01se01.ssp01sec.mex, O Un-Certificate Services System CertificateCertificate Services Endpoint Sub CA - ssp01se01#00002	pxGrid		ssp01se01.ssp01sec.mex	Certificate Services Endpoint Sub CA - ssp01se01	Fri, 30 Jun 2023	Sat, 1 Jul 2028	Active
ise01_External_CA	Admin, EAP Authentication, RADIUS DTLS, Portal	Default Portal Certificate Group	ssp01se01.ssp01sec.mex	ssp01se01.ssp01sec.mex	Mon, 3 Jul 2023	Wed, 2 Jul 2025	Active
ssp01se02							
Default self-signed saml server certificate - CN=SAML_ssp01se01.ssp01sec.mex	SAML		SAML_ssp01se01.ssp01sec.mex	SAML_ssp01se01.ssp01sec.mex	Sat, 1 Jul 2023	Thu, 29 Jun 2028	Active
ise02_External_CA	Admin, EAP Authentication, RADIUS DTLS, Portal	Default Portal Certificate Group	ssp02se01.ssp02sec.mex	ssp02se01.ssp02sec.mex	Mon, 3 Jul 2023	Wed, 2 Jul 2025	Active
CN=ssp02se02.ssp02sec.mex, O Un-Certificate Services System CertificateCertificate Services Endpoint Sub CA - ssp02se02#00004	ISE Messaging Service		ssp02se02.ssp02sec.mex	Certificate Services Endpoint Sub CA - ssp02se02	Sat, 1 Jul 2023	Sun, 2 Jul 2028	Active
CN=ssp02se02.ssp02sec.mex, O Un-Certificate Services System CertificateCertificate Services Endpoint Sub CA - ssp02se02#00003	pxGrid		ssp02se02.ssp02sec.mex	Certificate Services Endpoint Sub CA - ssp02se02	Sat, 1 Jul 2023	Sun, 2 Jul 2028	Active

Certificate Hierarchy

Certificate Services Root CA - ssp01se01
Certificate Services Node CA - ssp01se02
Certificate Services Endpoint Sub CA - ssp01se02
ssp01se02.ssp01sec.mex

ssp01se02.ssp01sec.mex

Issued By: Certificate Services Endpoint Sub CA - ssp01se02
Expires: Sun, 2 Jul 2028 11:45:44 MDT

Certificate status is good

Details

Issued To

Common Name (CN) ssp01se02.ssp01sec.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

驗證pxGrid證書。

準備FMC進行整合。

步驟 1.確認FMC內部時間是 最新.

導航至 System > Configuration > 時間 並確保在FMC上配置的時間為 最新.

Firewall Management Center
System / Configuration

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

Configuration Health Monitoring

Users Monitor Audit
Domains Policy Syslog
Updates Events Statistics
Licenses Exclude
Smart Licenses Monitor Alerts
Classic Licenses

Tools
Backup/Restore
Scheduling
Import/Export
Data Purge

Current Setting Via NTP (based on System Configuration [Time Synchronization](#))
Current Time 2023-08-26 19:08

NTP Server	Status	Authentication	Offset	Last Update
127.127.1.1	Being Used	none	+0.000(milliseconds)	42(seconds)
72.30.35.89	Unknown	none	+0.000(milliseconds)	~(seconds)
208.88.126.235	Unknown	none	+0.000(milliseconds)	~(seconds)

驗證FMC是否處於最新狀態。

如果未更新FMC時間，請確保正確配置NTP 和 在 同步.NTP可在 系統>配置>時間> +新增.

Firewall Management Center
System / Configuration

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

Configuration Health Monitoring

Users Monitor Audit
Domains Policy Syslog
Updates Events Statistics
Licenses Exclude
Smart Licenses Monitor Alerts
Classic Licenses

Tools
Backup/Restore
Scheduling
Import/Export
Data Purge

Serve Time via NTP Enabled

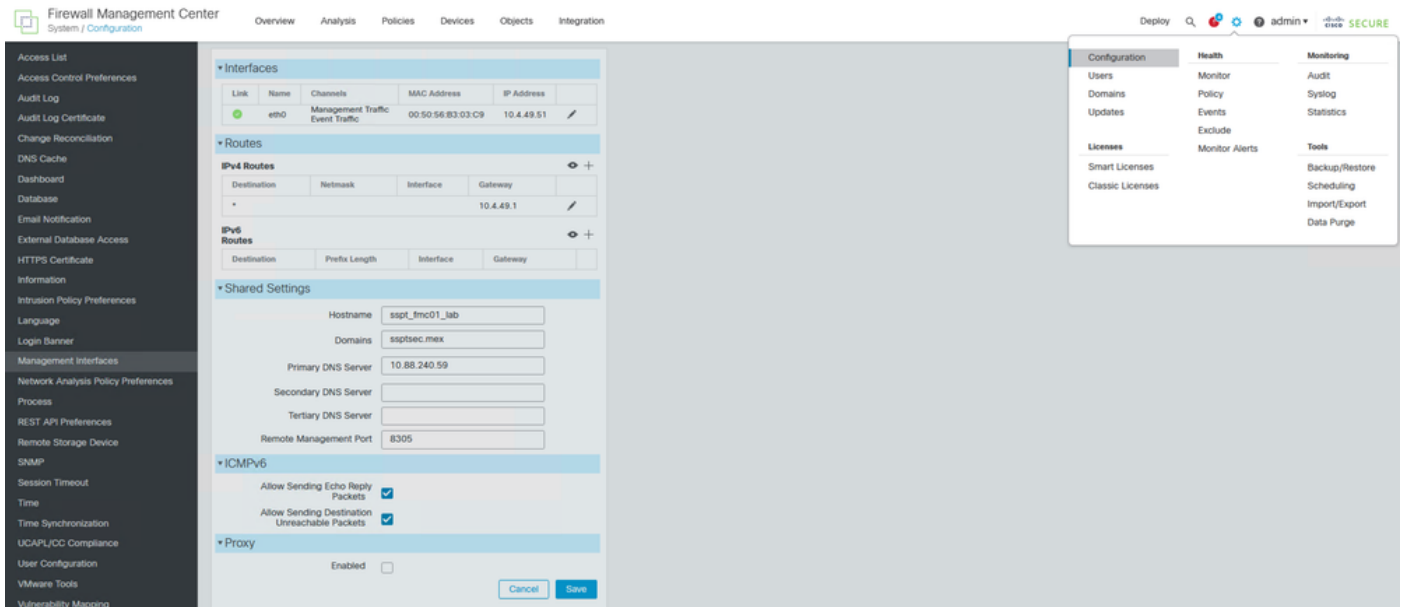
Set My Clock
Manually in Local Configuration ☐
Via NTP ☒

☐ Use the authenticated NTP server only + Add

NTP Server	Authentication	Action
0.sourcefire.pool.ntp.org	N/A	🔍 ✎️ 🗑️
1.sourcefire.pool.ntp.org	N/A	🔍 ✎️ 🗑️

FMC上的時間同步。

步驟 2. 導航至 System > Configuration > 管理介面 > 共用設定 並驗證至少 主DNS伺服器 欄位 包含有效的 DNS伺服器IP。



FMC上的DNS配置。

步驟3.確認已配置FMC主機名。

導航至 系統>配置>管理介面>共用設定 並驗證 主機名 欄位包含FMC主機名。

您可以在檢視本節中上一步時驗證此步驟。

設定ISE和FMC之間的pxGrid連線。

步驟1.導航到選單Administration > pxGrid Services > Client Management > Certificates。

在第一個選項中，選擇I want to Generate a single certificate(without a certificate signing request)。

在Common Name(CN)部分，輸入ISE要頒發證書的FMC的FQDN。

提供說明。

在Subject Alternative Name(SAN)部分，輸入要連線的FMC的FQDN和IP地址。

在Certificate Download Format的底部，從下拉選單中選擇選項Certificate in Privacy Enhanced Email(PEM) format。

輸入PKCSS PEM格式 (包括證書鏈)。

稍後在FMC中使用此密碼時，在Certificate Password中輸入並儲存密碼。

確認密碼，然後選擇Create。

Cisco ISE Administration - pxGrid Services

Summary Client Management Diagnostics Settings

Clients
Policy
Groups
Certificates
pxGrid Cloud Connection
pxGrid Cloud Policy

Certificates

Generate pxGrid Certificates

I want to*
Generate a single certificate (without...

Common Name (CN)*
sspt_fmc01_lab.ssptsec.mex

Description
testing lab

Certificate Template pxGrid_Certificate_Template ⓘ

Subject Alternative Name (SAN)
FQDN sspt_fmc01_lab.ssptsec.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證書生成示例。

步驟2.將zip檔案下載到您的電腦。解壓縮檔案，並確認環境中存在以下檔案：

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.ssptsec.mex_sspt_fmc01_lab.ssptsec.mex	21/08/2023 04:55	Security Certificate	2 KB
 sspt_fmc01_lab.ssptsec.mex_sspt_fmc01_lab.ssptsec.mex.key	21/08/2023 04:55	KEY File	2 KB

由ISE生成的PxGrid證書。

步驟3.在FMC中，導覽至功能表Objects > Objects Management > PKI > Internal Certs。

選擇新增內部證書選項。

Firewall Management Center Objects / Object Management Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ admin 🔒 SECURE

Internal Certs

Add Internal Cert 🔍 Filter

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	

- AAA Server
- Access List
- Address Pools
- Application Filters
- AS Path
- Cipher Suite List
- Community List
- Distinguished Name
- DNS Server Group
- External Attributes
- File List
- FlexConfig
- Geolocation
- Interface
- Key Chain
- Network
- PKI
 - Cert Enrollment
 - External Cert Groups
 - External Certs
 - Internal CA Groups
 - Internal CAs
 - Internal Cert Groups
 - Internal Certs
 - Trusted CA Groups
 - Trusted CAs

將FMC證書新增為內部證書。

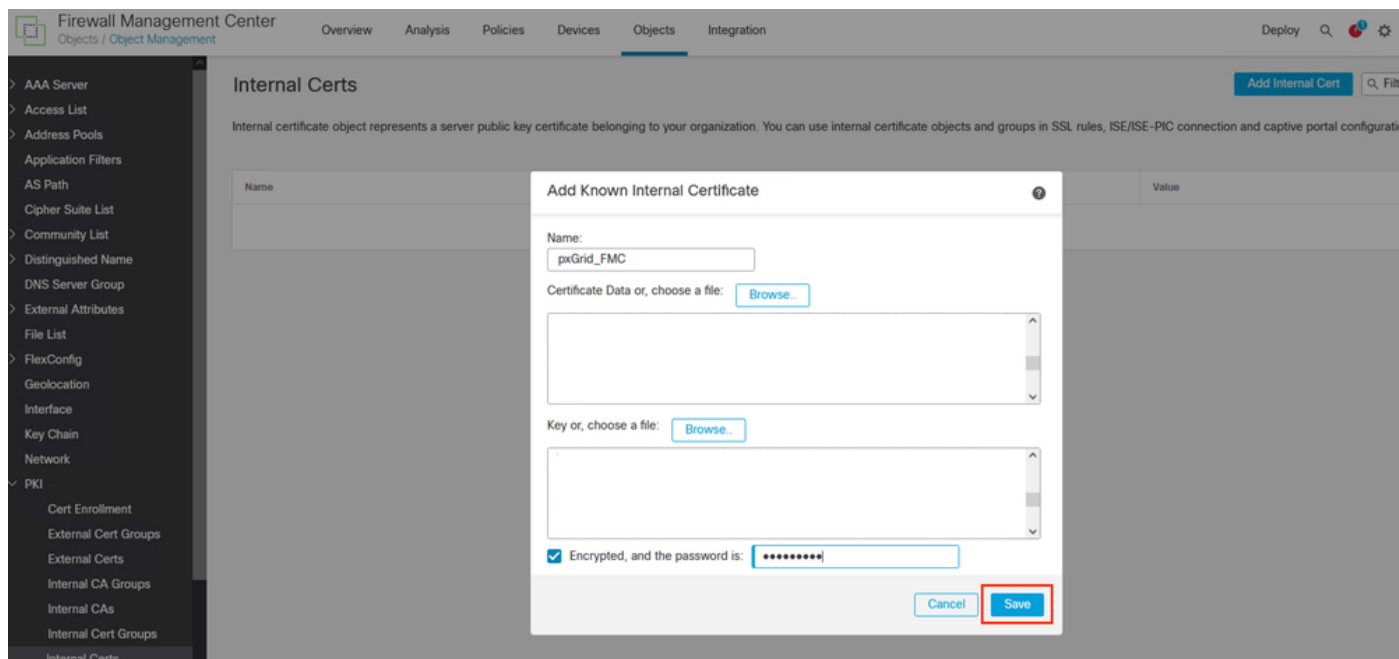
步驟4.將在FMC上分配的證書命名。

在Certificate Data一節中瀏覽您從ISE為FMC建立的證書。

瀏覽副檔名為.key的檔案，以填寫下一個欄位。

選擇Encrypted選項，並輸入您在ISE上建立證書時使用的密碼。

儲存組態。



Firewall Management Center
Objects / Object Management

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️

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.

Add Internal Cert 🔍 Filter

Name

pxGrid_FMC

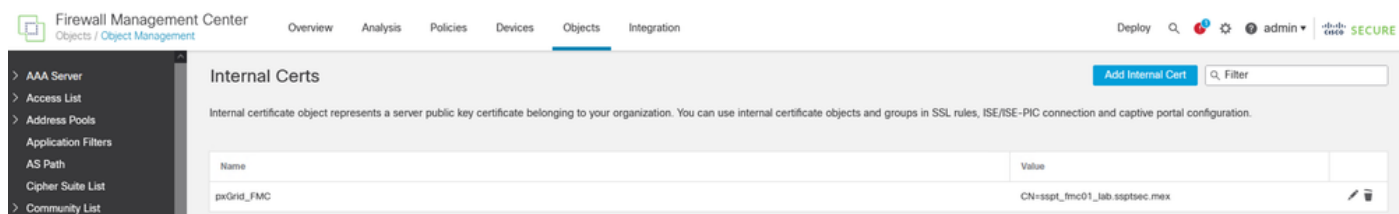
Certificate Data or, choose a file: Browse..

Key or, choose a file: Browse..

☒ Encrypted, and the password is: *****

Cancel Save

匯出ISE生成的FMC證書。



Firewall Management Center
Objects / Object Management

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ admin 🔒 SECURE

Internal Certs

Add Internal Cert 🔍 Filter

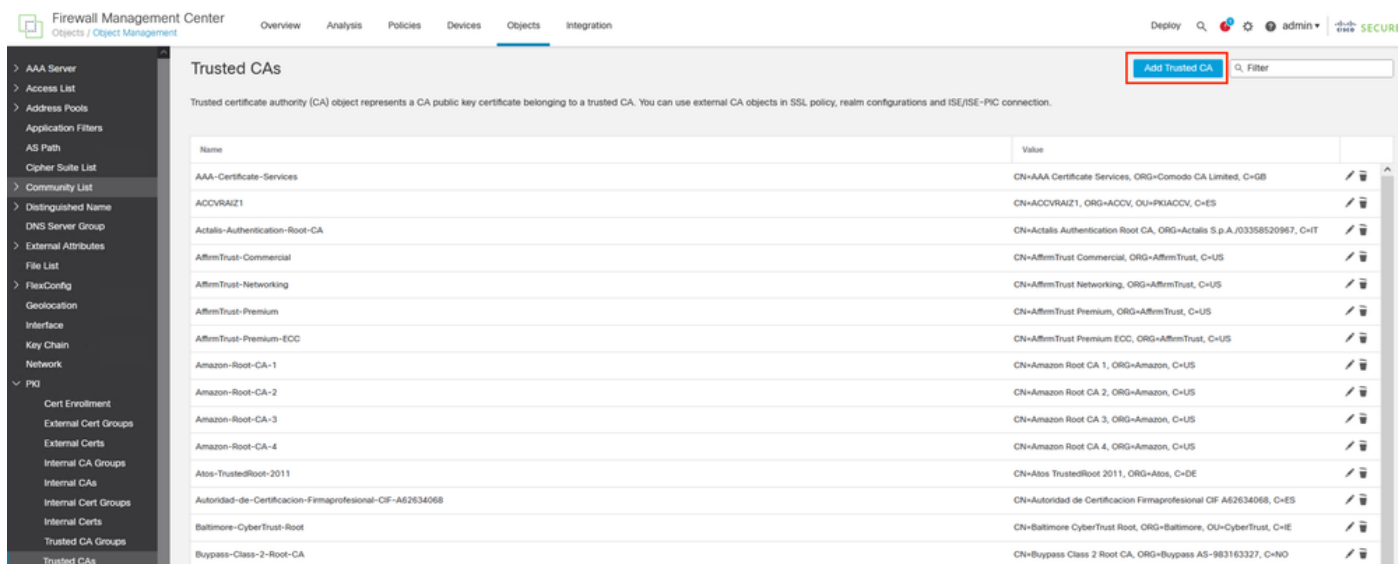
Internal certificate object represents a server public key certificate belonging to your organization. You can use internal certificate objects and groups in SSL rules, ISE/ISE-PIC connection and captive portal configuration.

Name	Value
pxGrid_FMC	CN=sspt_fmc01_lab.sspsec.mex

FMC證書。

步驟5.導航至功能表Objects > Objects Management > PKI > Trusted CAs,

選擇Add Trusted CAs。

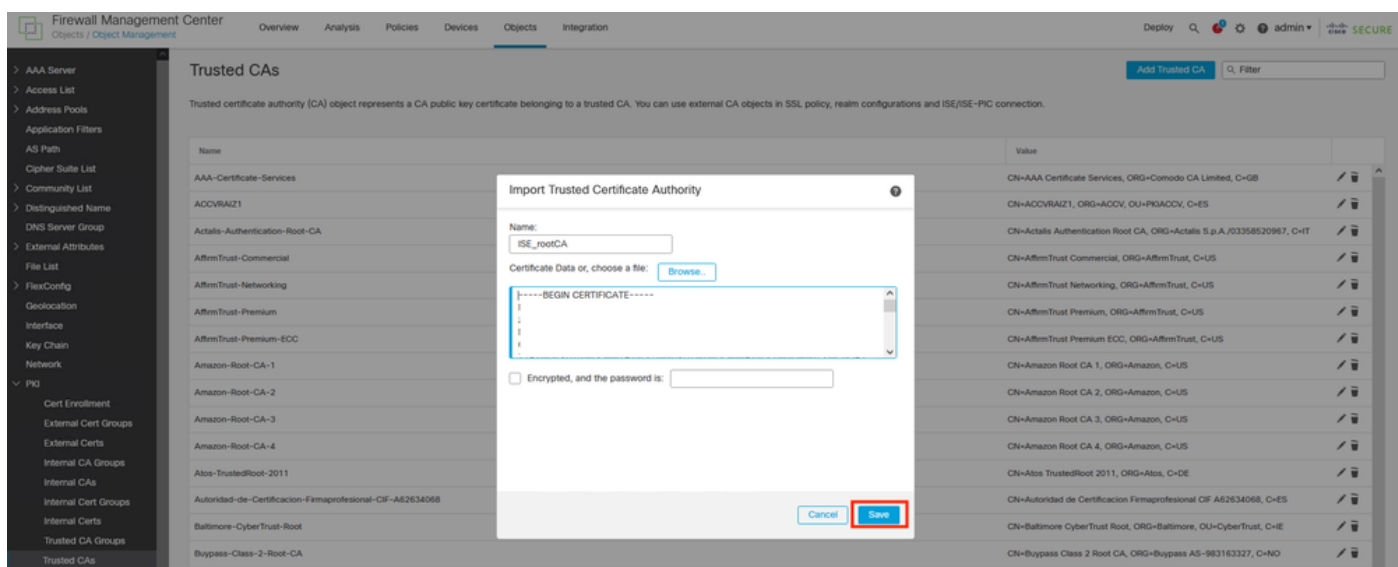


將ISE rootCA新增為受信任證書。

步驟6.命名證書頒發機構。

瀏覽並選擇從ISE檔案下載的ISE根CA。

儲存您的組態。



匯出ISE rootCA。

步驟7.導航至選單Integration > Other Integrations > Identity Sources。

在服務型別中選擇：身份服務引擎，

輸入成為主節點的pxGrid節點的IP地址或FQDN。

對輔助pxGrid節點重複此過程。

從下拉選單中選擇ISE為pxGrid Client Certificate部分生成的pxGrid證書

在MNT伺服器CA和pxGrid伺服器CA部分，選擇您在上一步中匯出的ISE根CA。



附註：pxGrid伺服器CA對應於pxGrid節點上pxGrid正在使用的證書的根證書頒發機構。

MNT伺服器CA對應於MNT節點上pxGrid正在使用的證書的證書頒發機構。

(可選) 您可以從ISE訂閱會話目錄和SXP主題。

儲存組態。

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中將ISE設定為身份源。

驗證.

驗證FMC。

在儲存配置之前，在選單中導航到Integration > Other Integrations > Identity Source > Identity Services Engine。可以測試pxGrid連結的設定。

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通訊成功。

Primary host:

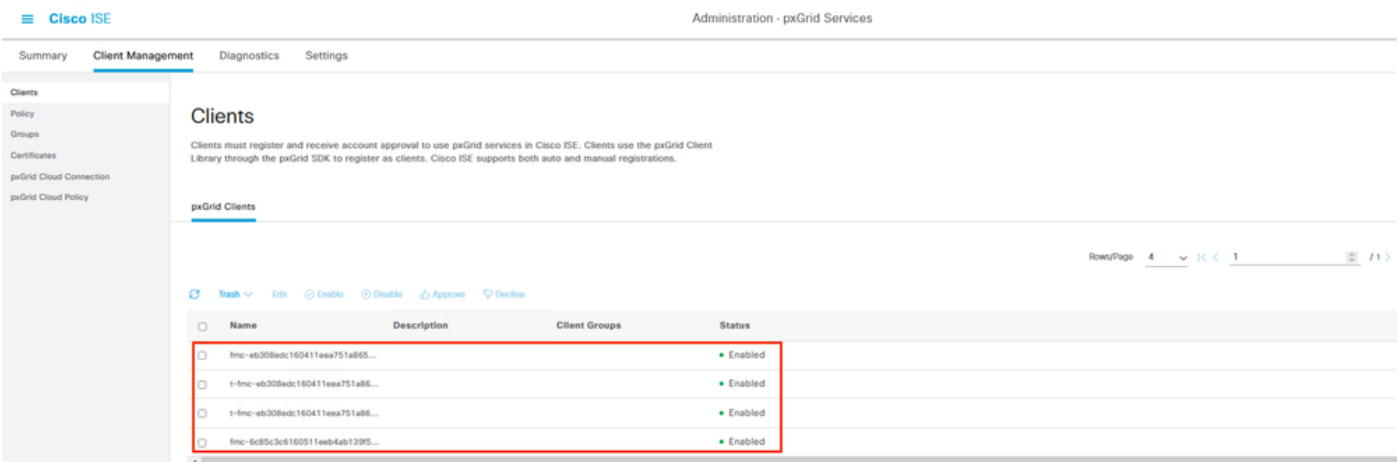
```
[INFO]: PXGrid v2 is enabled
[INFO]: pxgrid 2.0: account activate succeeded
[INFO]: Successful connection to ssptise02.ssptsec.mex:8910
[INFO]: Successful connection to ssptise01.ssptsec.mex:8910
[INFO]: These ISE Services are up: SessionDirectory, SXP, EndpointProfile, SecurityGroups, AdaptiveNetwork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

Secondary host:

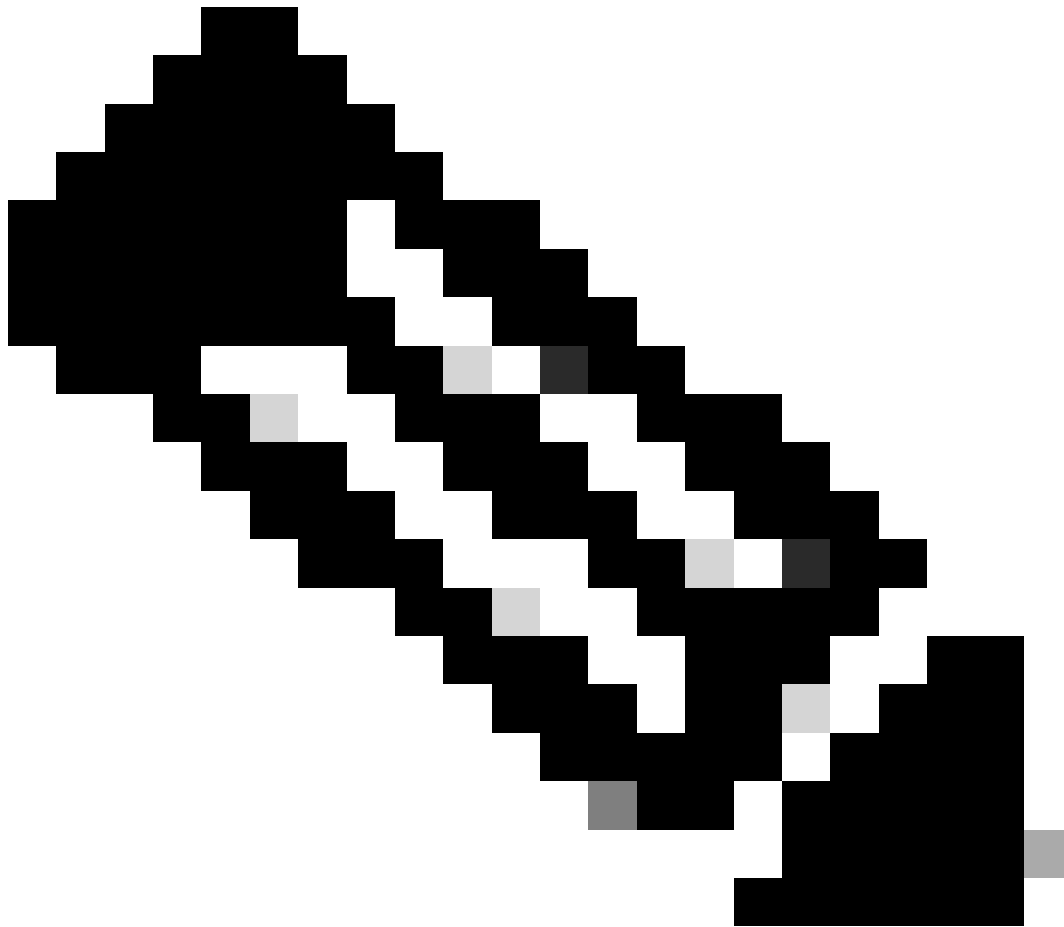
```
[INFO]: PXGrid v2 is enabled
[INFO]: pxgrid 2.0: account activate succeeded
[INFO]: Successful connection to ssptise02.ssptsec.mex:8910
[INFO]: Successful connection to ssptise01.ssptsec.mex:8910
[INFO]: These ISE Services are up: SessionDirectory, SXP, EndpointProfile, SecurityGroups, AdaptiveNetwork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

在ISE上驗證。

當FMC pxGrid客戶端成功整合到ISE上時，您 然後請參閱(在 管理> pxGrid服務>客戶端管理 > 客戶端選單) 包含名為fmc的客戶端，且已啟用。



PxGrid客戶端可用並啟用。



還有，如果導航到選單Administration > pxGrid Services > Diagnostics > WebSocket，然後您會看到連線s 到 FMC。

Cisco ISE Administration - pxGrid Services

Summary Client Management **Diagnostics** Settings

WebSocket

Clients Topics

Clients

Row/Page 2 < 1 Go 2 Total Rows

Client Name	Connect To	Session Id	Certificate	Subscriptions	Publications	IP Address	Status	Start time	Duration (dd:h:mm:ss)
fmc-es308edc160411eeab7...	expired01	expired01.5	Ctrl-signt_fmc01_...	/topic/com.cisco.ise.sessio...		10.4.49.51	Connected	2023-08-21 05:30:18 MDT	01:10:19:42
fmc-fd85c3e6160511eeab4...	expired01	expired01.6	Ctrl-signt_fmc01_...	/topic/com.cisco.ise.sessio...		10.4.49.52	Connected	2023-08-21 05:31:56 MDT	01:10:18:03

在下一個頁籤中 從此選單 已命名 Topics中，您可以 驗證是否已將FMC訂閱者新增到ISE發佈的 pxGrid主題中。

例如，有一個主題與中的安全組相關 其中 您可以看到兩個FMC 訂閱和接收相關的資訊 成長至 SGT 由ISE發佈。

Cisco ISEAdministration - pxGrid Services

SummaryClient ManagementDiagnosticsSettings

WebSocket

ClientsTopics

Topics

Rows/Page101 < 1Go10 Total Rows

Name	Publisher Count	Subscriber Count
/topic/wellcard	0	2
/topic/com.cisco.ise.config.trustsec.security.group	0	2

Rows/Page101 < 1Go2 Total Rows

Client Name	Messaging Role
fmc-eb308dc160411ee7...	Sub
fmc-6c85c3cd160511eeb4...	Sub

每個pxGrid使用者的主題。

I在選單Administration > pxGrid Services > Diagnostics > Log中，重要事件 顯示在pxGrid通訊中相關的（對於已啟用功能的節點）。

這些描述與整合相關的資訊。

Cisco ISEAdministration - pxGrid Services

SummaryClient ManagementDiagnosticsSettings

WebSocket

Log

Tests

Live Log

Rows/Page251 < 1Go131 Total Rows

Timestamp	Client	Server	Host	Event Type	Description
2023-08-21 06:31 -05:00	fmc-6c85c3cd160511eeb4ab1395...	wsa://10.4.49.41/pxgrid/ise/pubsub	sxptise01	PUBSUB_SERVER_SUBSCRIBE	Pubsub subscribe: subscription-[d=880ba640-97d8-4c17-81c1-d59fbdca...
2023-08-21 06:31 -05:00	fmc-6c85c3cd160511eeb4ab1395...	wsa://10.4.49.41/pxgrid/ise/pubsub	sxptise01	PUBSUB_SERVER_SUBSCRIBE	Pubsub subscribe: subscription-[d=6523e2d0-91e6-4199-be54-ed186d09...
2023-08-21 06:31 -05:00	fmc-6c85c3cd160511eeb4ab1395...	wsa://10.4.49.41/pxgrid/ise/pubsub	sxptise01	PUBSUB_SERVER_SUBSCRIBE	Pubsub subscribe: subscription-[d=308ccdfb-9c75-4c3a-9619-203faed12...
2023-08-21 06:31 -05:00	fmc-6c85c3cd160511eeb4ab1395...	wsa://10.4.49.41/pxgrid/ise/pubsub	sxptise01	PUBSUB_SERVER_SUBSCRIBE	Pubsub subscribe: subscription-[d=63d9508e-3001-475d-b6fb-3a25aaf49...
2023-08-21 06:31 -05:00	fmc-6c85c3cd160511eeb4ab1395...	wsa://10.4.49.41/pxgrid/ise/pubsub	sxptise01	WS_SERVER_CONNECTED	Websocket connected: session-[d=6,client=fmc-6c85c3cd160511eeb4ab1...

PxGrid即時日誌。

疑難排解

FMC故障排除。

確認FMC能夠按主機名解析自己的主機名和ISE節點。

舉例來說：

```
<#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

```

確保 ADI進程已啟動並正在運行：

```
<#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確保從FMC到ISE的通訊 port TCP 8910被允許。來自FMC CLI 我們可以 設定 答 tcpdump 資料包捕獲，用於確認雙向通訊。

```
<#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
```

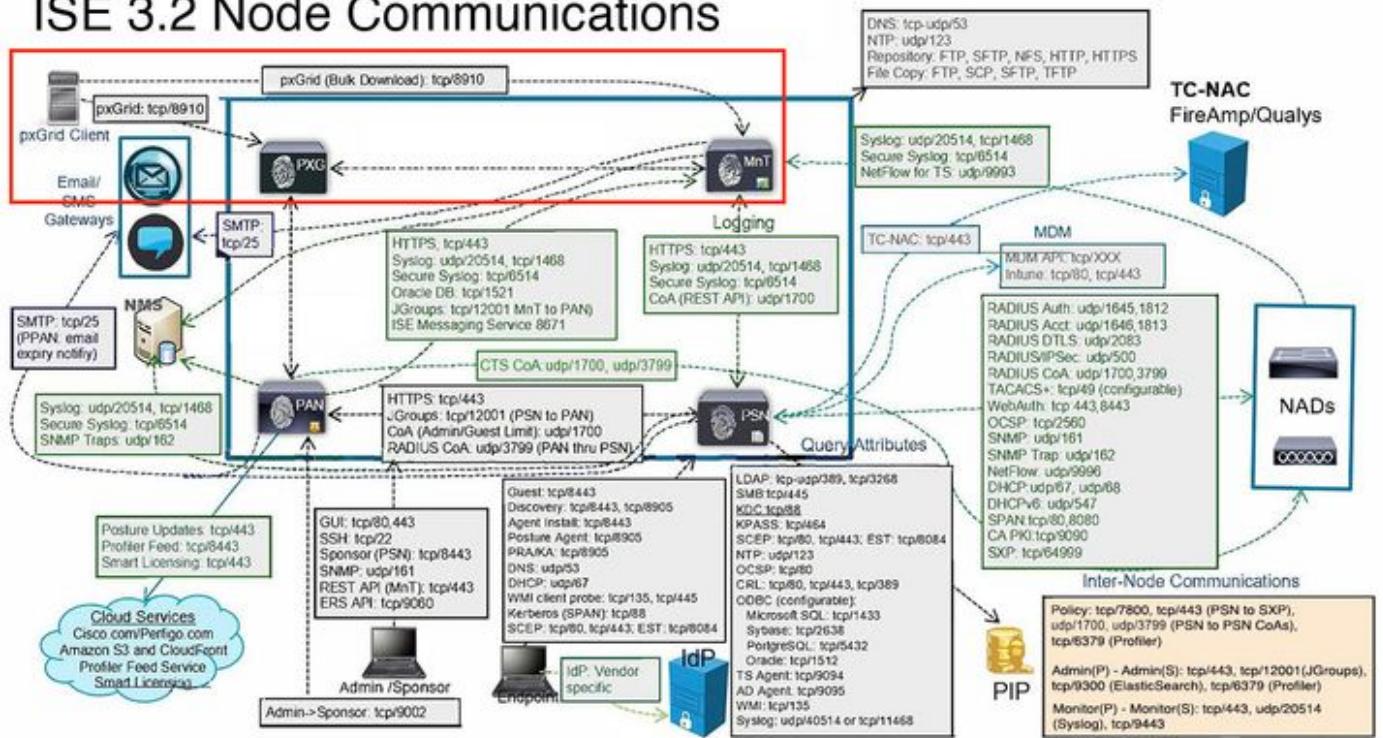
```
: Flags [.], ack 1, win 229, options [nop,nop,TS val 2701166400 ecr 2268665064], length 0  
[...]
```

ISE故障排除。

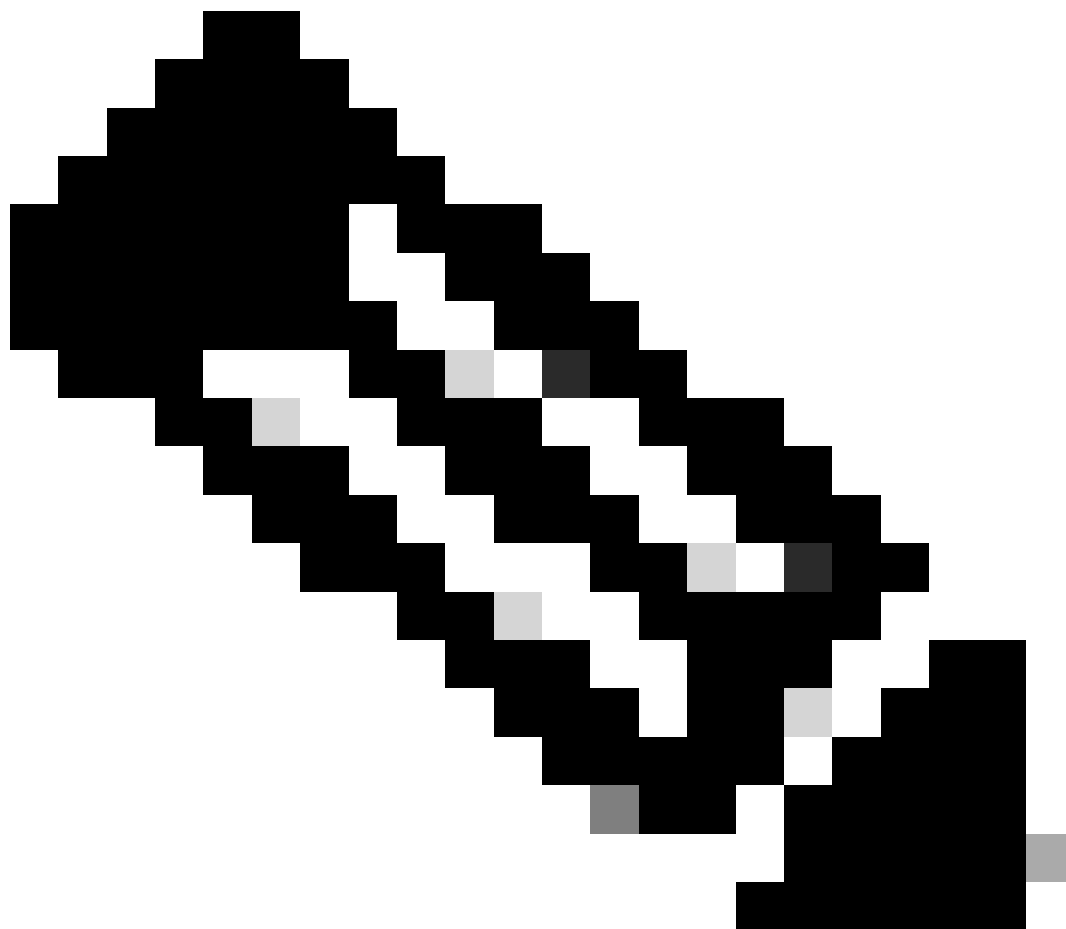
驗證埠8910上的通訊 已運行。

這是pxGrid客戶端使用的埠用於與pxGrid節點和MnT節點通訊以進行資訊批次下載。

ISE 3.2 Node Communications



ISE環境中のPxGrid互動。



附註：pxGrid客戶端（本例中為FMC）與pxGrid節點和輔助MNT(SMNT)節點通訊以獲取資訊（批次下載），如果SMNT發生故障，則通過主要MNT查詢資訊。

在與pxGrid客戶端進行通訊的ISE節點上，您可以檢視 如果 埠是 開啟或 如果有套接字連線到 那個埠。

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

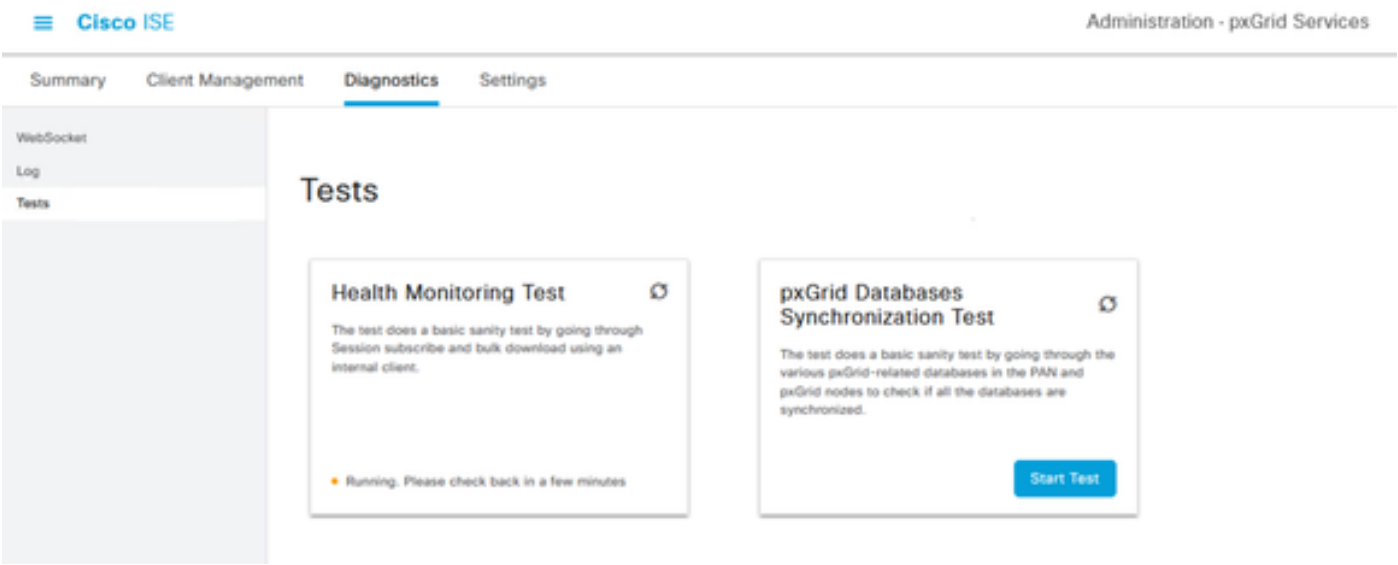
在ISE上有2項測試可用於診斷pxGrid實施的總體狀態。

這些可在選單上找到 管理> pxGrid服務>診斷>測試。

本節顯示的測試在ISE內部執行。

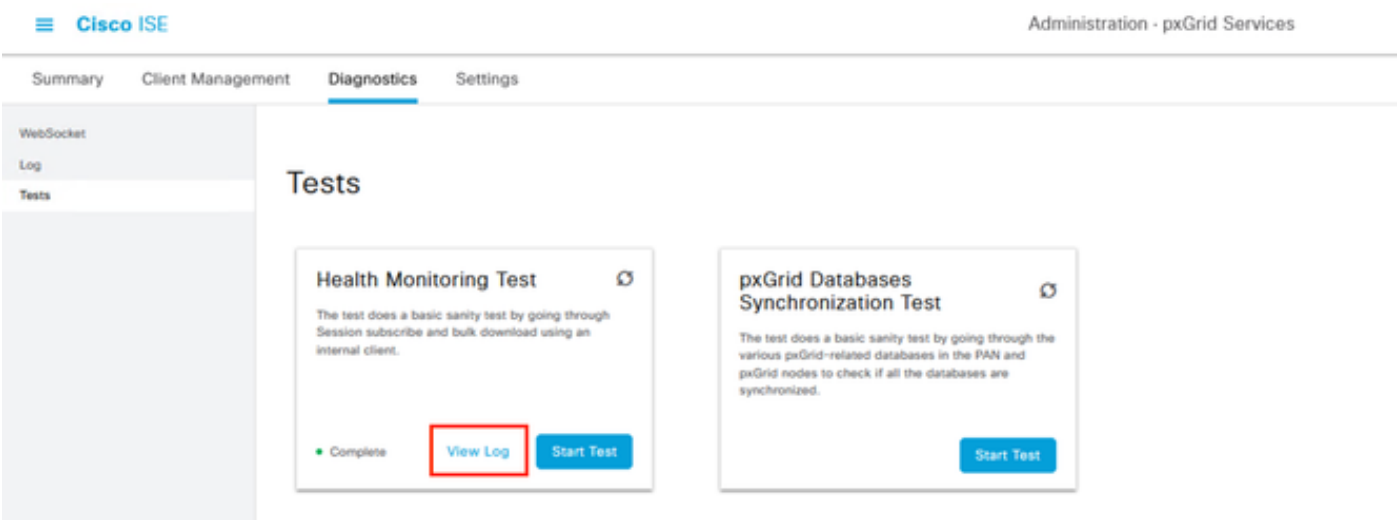
運行狀況監控測試 檢視pxGrid服務外觀up、 該選項評估客戶端是否可以訪問pxGrid控制器發佈的會話目錄、服務和主題。

選擇 選項 開始 測試 然後等待日誌的收集。



PxGrid運行狀況監控測試。

測試完成後，選擇 選項 檢視日誌。 在本示例中，日誌的內容 是：



檢視運行狀況監控測試。

```
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
```

```

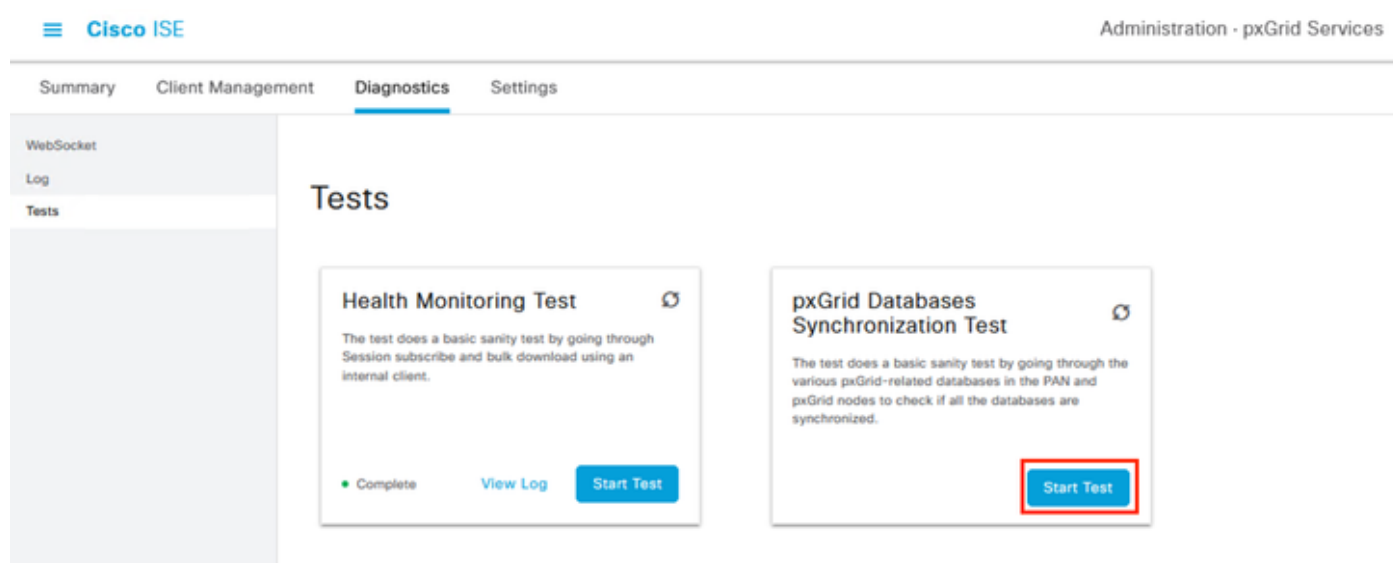
22-Aug-2023 17:03:15 [INFO] ----- Download Test Completed -----
22-Aug-2023 17:03:15 [INFO] ----- Starting Subscribe Test -----
22-Aug-2023 17:03:16 [INFO] STOMP CONNECT host=ssptise02.ssptsec.mex
22-Aug-2023 17:03:16 [INFO] STOMP SUBSCRIBE topic=/topic/com.cisco.ise.session
22-Aug-2023 17:03:16 [INFO] 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資料庫同步測試檢查是否 資訊 資料庫中的PAN和pxGrid節點之間正確且已同步。

因此，傳送到pxGrid使用者的資訊是 準確。

選擇 選項 啟動測試 等待評估結果。



PxGrid資料庫同步測試。

從生成的日誌中獲得此輸出。

```

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

```

```

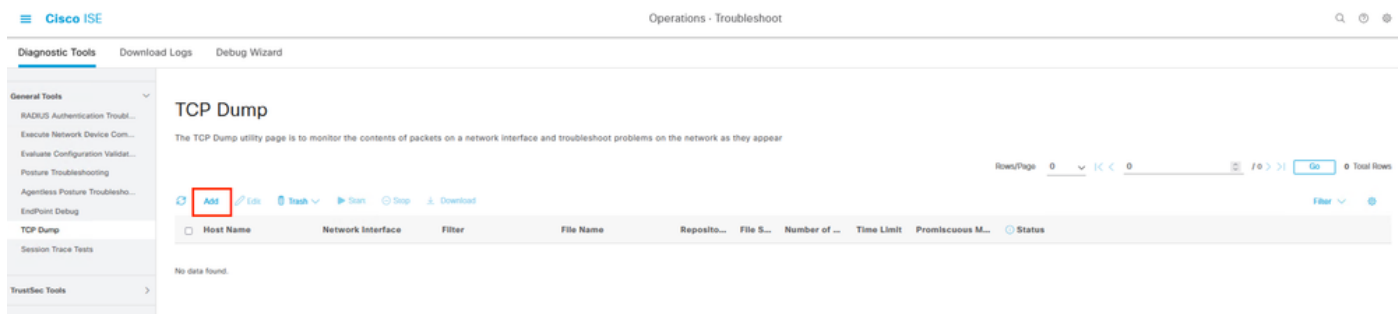
Primary PAN : ssptise01.ssptsec.mex
pxGrid Nodes : ssptise01.ssptsec.mex ssptise02.ssptsec.mex

```

收集捕獲 從指向主FMC節點的pxGrid節點。

導航至選單 Operations > Troubleshoot > Diagnostic Tools > TCP Dump,

選擇 選項 成長至 新增 新捕捉。



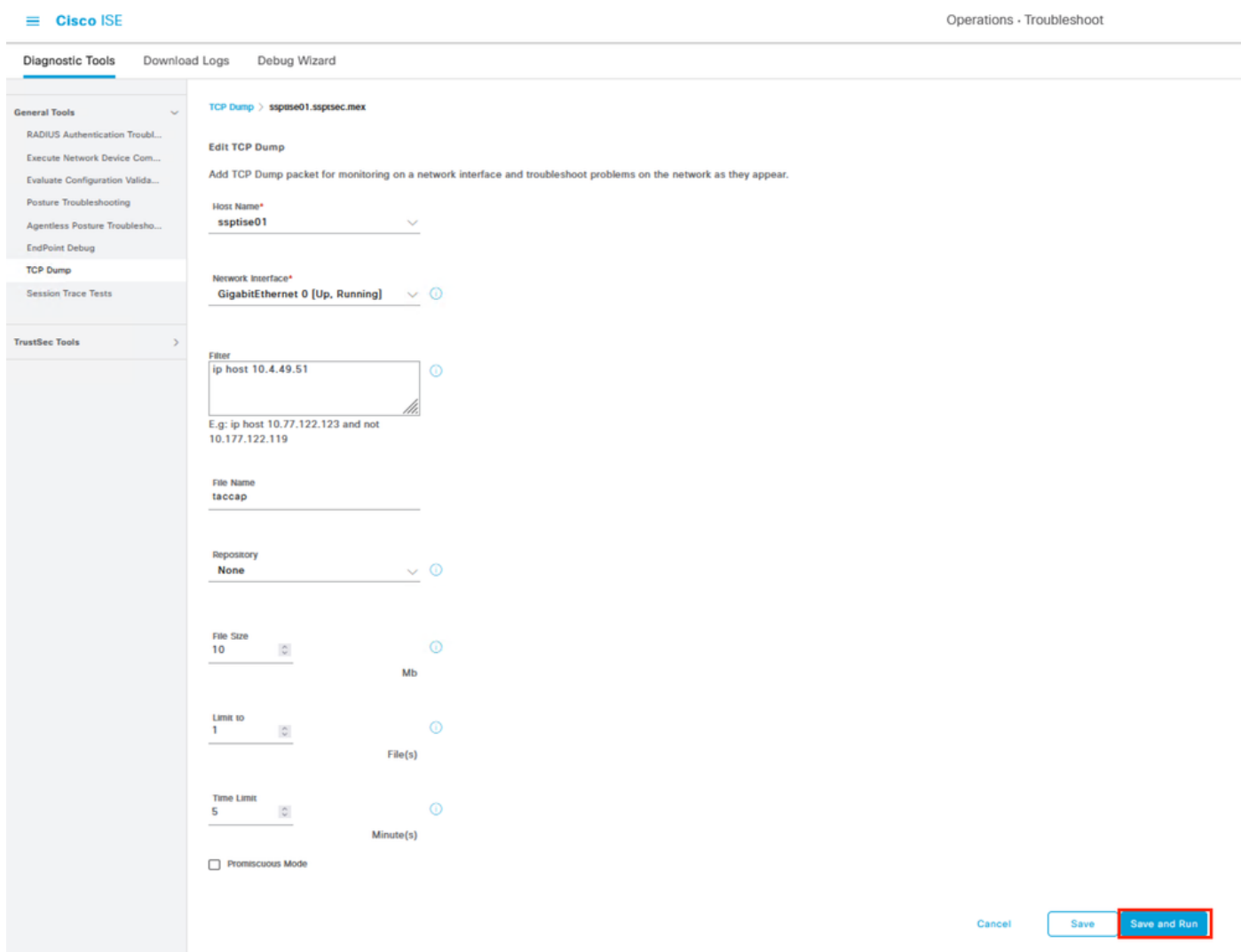
在ISE上生成資料包捕獲。

配置捕獲的引數。

在 主機名、 選擇在FMC中選擇的主pxGrid節點。

篩選條件 與此 語法 ip host <FMC IP>

為捕獲命名 然後 繼續 成長至 儲存 和運行。

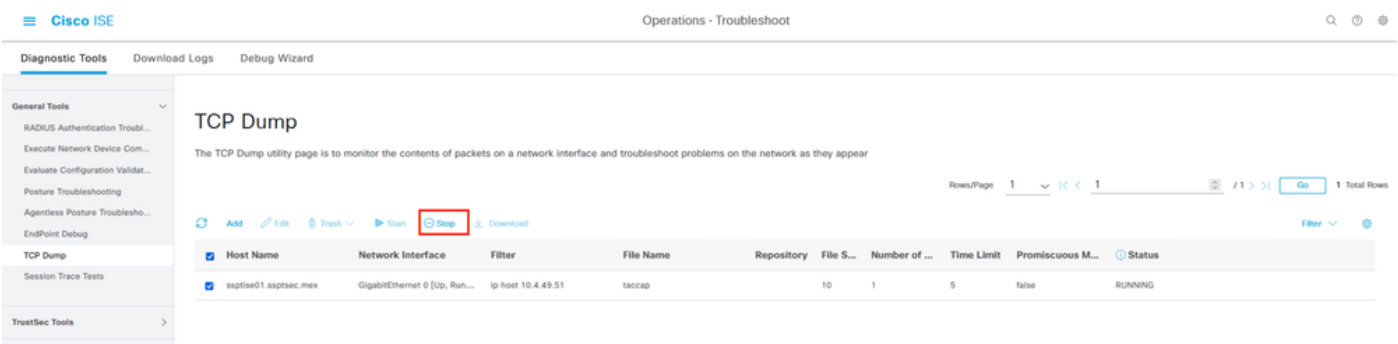


資料包捕獲配置示例。

在另一個視窗中，在FMC選單中 整合>其他整合>身份 來源中， 測試通過pxGrid通道與ISE的連線

。

W當你拿到測試結果時，繼續 成長至 S頂端 在ISE上捕獲。



停止ISE上的資料包捕獲。

下載 捕獲並開始分析。此方案顯示可以用作參考的工作連線的捕獲。

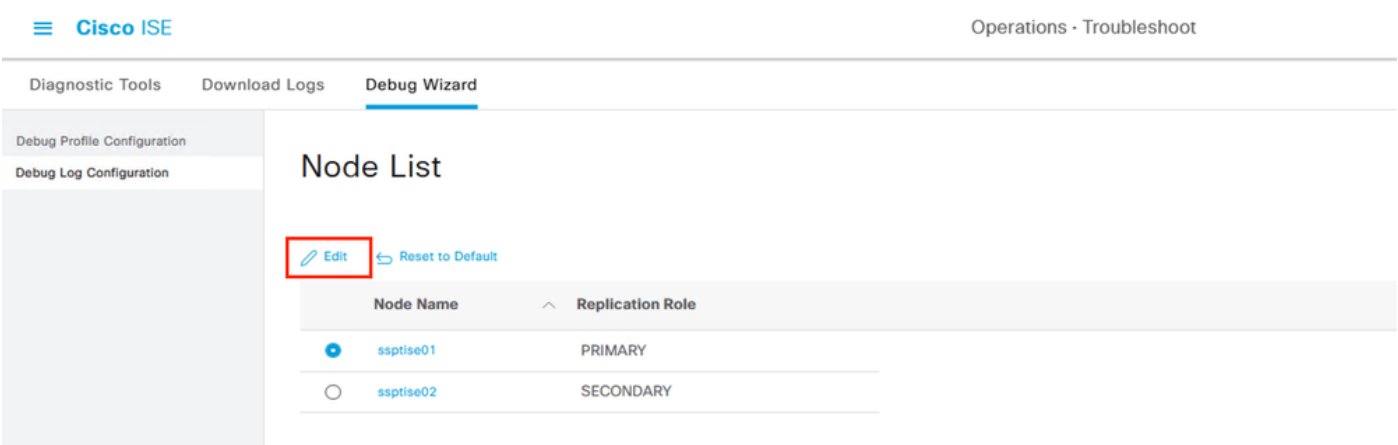
10.4.49.51	10.4.49.41	TCP	74	47508 → 8910 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=2738457626 TSecr=0 WS=128
10.4.49.41	10.4.49.51	TCP	74	8910 → 47508 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=2305956319 TSecr=2738457626 WS=128
10.4.49.51	10.4.49.41	TCP	66	47508 → 8910 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=2738457627 TSecr=2305956319
10.4.49.51	10.4.49.41	TLsv1.2	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	TLsv1.2	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	TLsv1.2	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	TLsv1.2	72	Change Cipher Spec
10.4.49.41	10.4.49.51	TLsv1.2	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	TLsv1.2	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	TLsv1.2	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	TLsv1.2	515	Application Data
10.4.49.41	10.4.49.51	TLsv1.2	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	TLsv1.2	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之間的PxGrid通訊。

此外，在ISE上，您可以收集與px相關的調試網格處理。

瀏覽選單 操作>故障排除>調試嚮導>調試 日誌配置中，

選擇要分析的對應ISE節點，然後 編輯。



選擇要在ISE上調試的節點。

篩選顯示的元件並更改 日誌級別到 偵錯pxgrid 元件 成長至 繼續 分析一下。

儲存 組態。

Debug Level Configuration

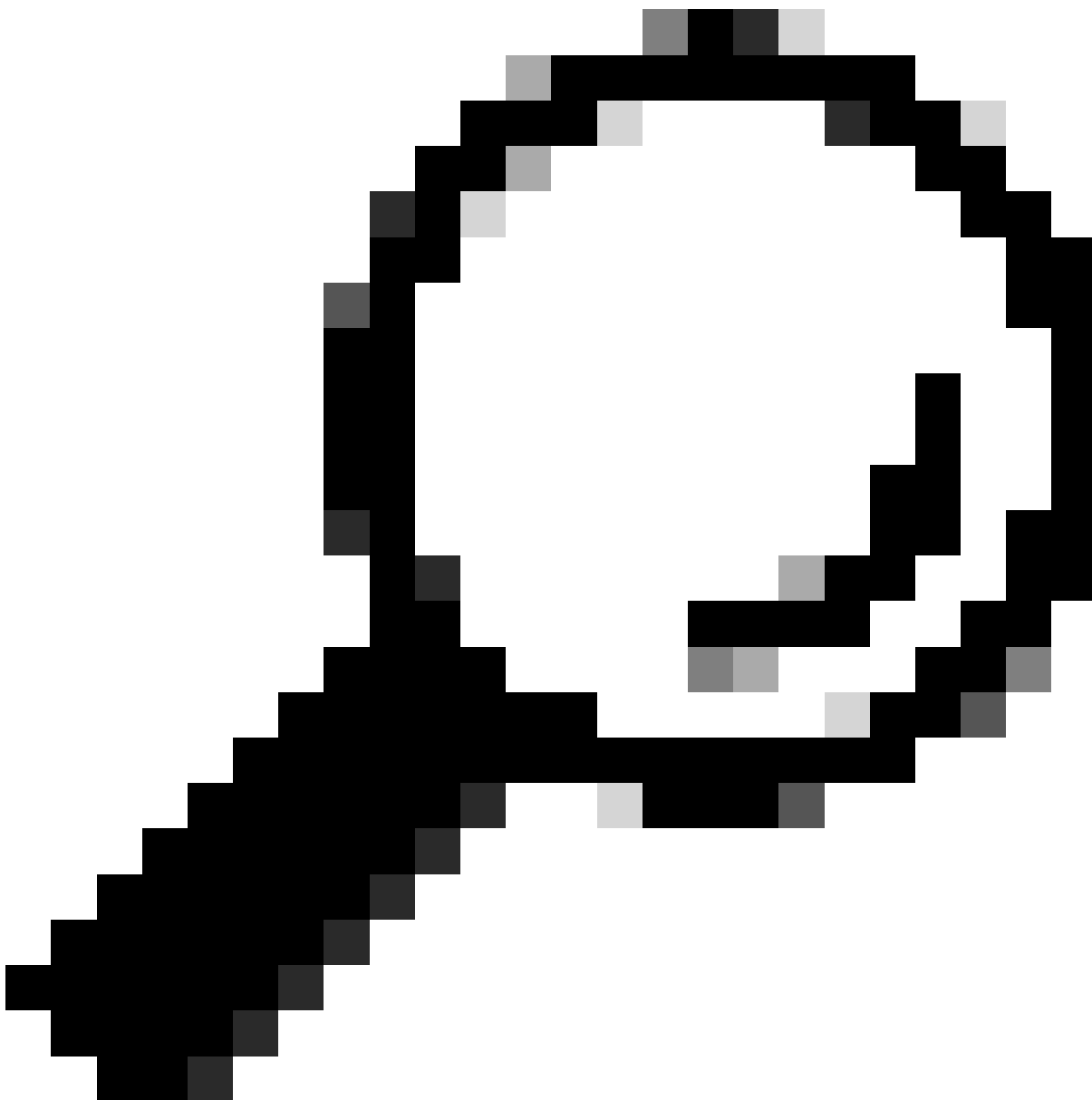
[Edit](#) [Reset to Default](#)

	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

將pxGrid元件更改為調試級別。

重現要分析的行為，然後繼續分析在pxgrid-server.log檔案中收集的日誌。其他日誌您可以在ISE節點上檢視以下內容進行故障排除：

```
#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
```

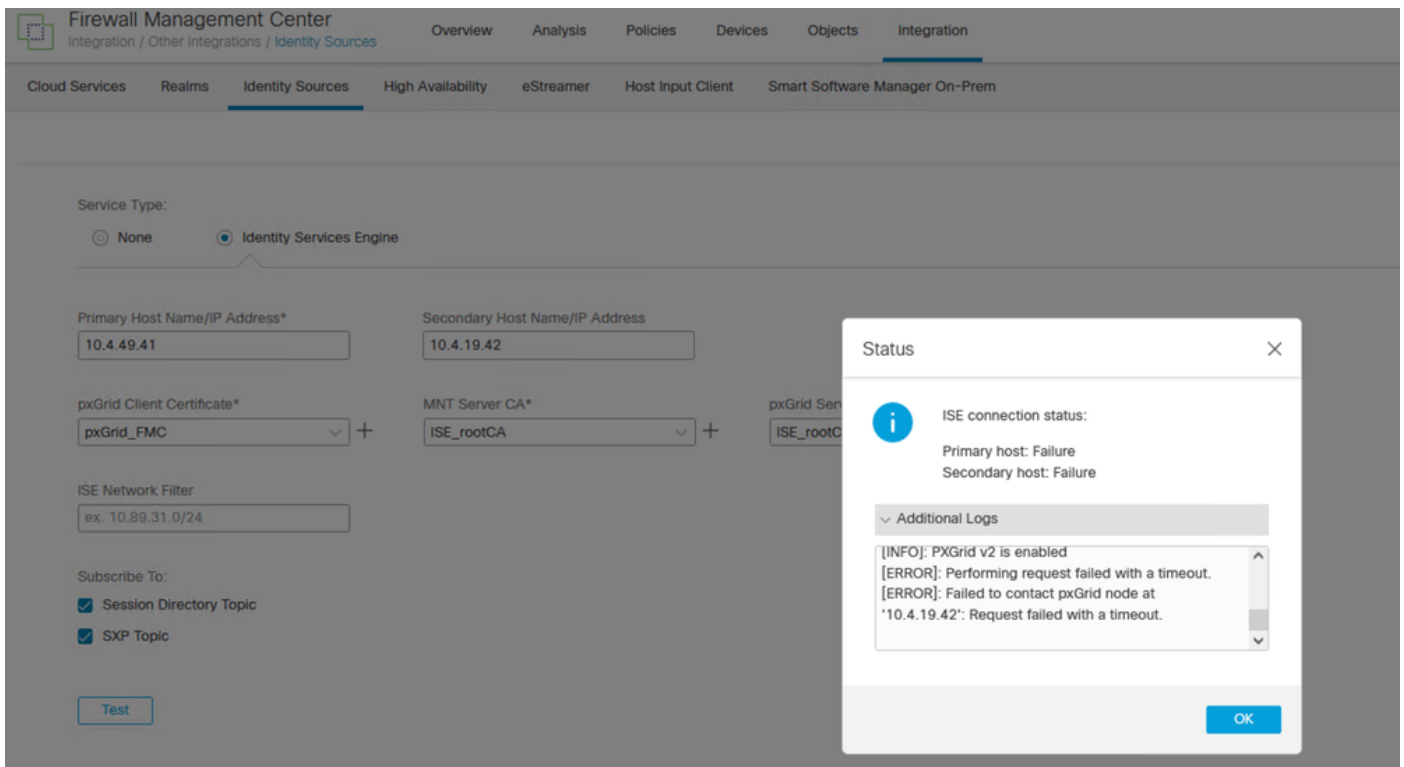


提示：有關進一步的日誌收集建議，請檢視[如何在ISE 3.x版本上啟用調試](#)影片。

常見問題。

PxGrid使用者客戶端未在ISE上獲得批准。

對於此使用情形，FMC測試pxGrid按鈕的相關輸出會顯示以下行為：



FMC pxGrid連線失敗。

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
```

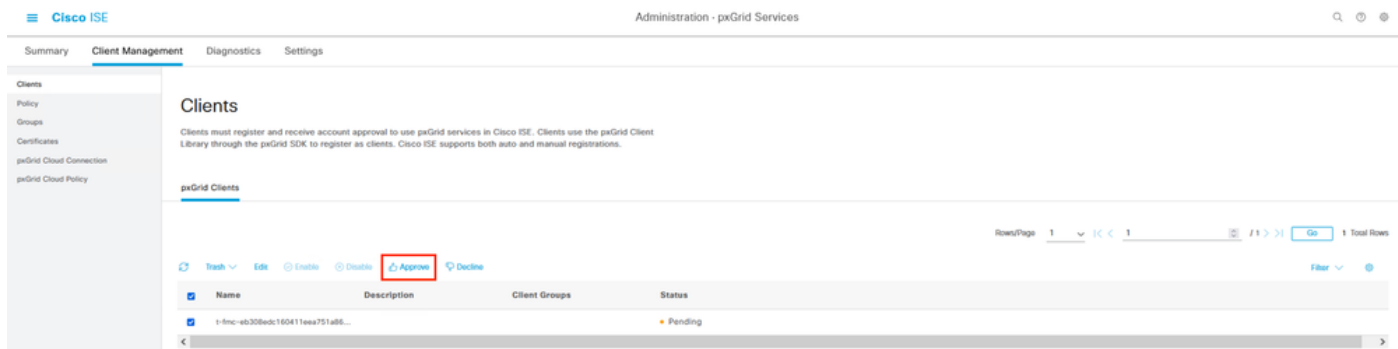
Secondary host:

```
[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.
```

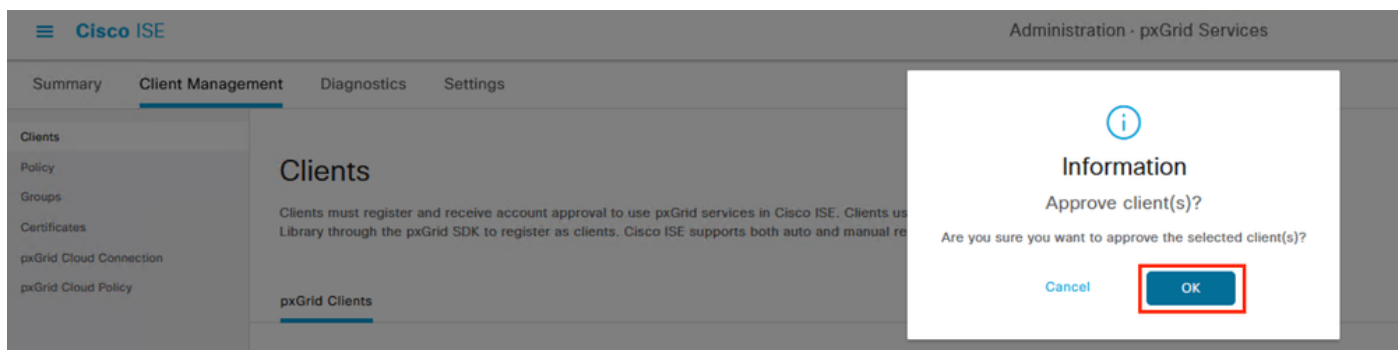
在ISE上，請注意選單Administration > PxGrid Services > Client Management > Clients中的行為，指示pxGrid客戶端(FMC)正在等待批准。

選擇Approve按鈕，確認下一個視窗中的選擇，然後再次嘗試整合。

這次整合成功。



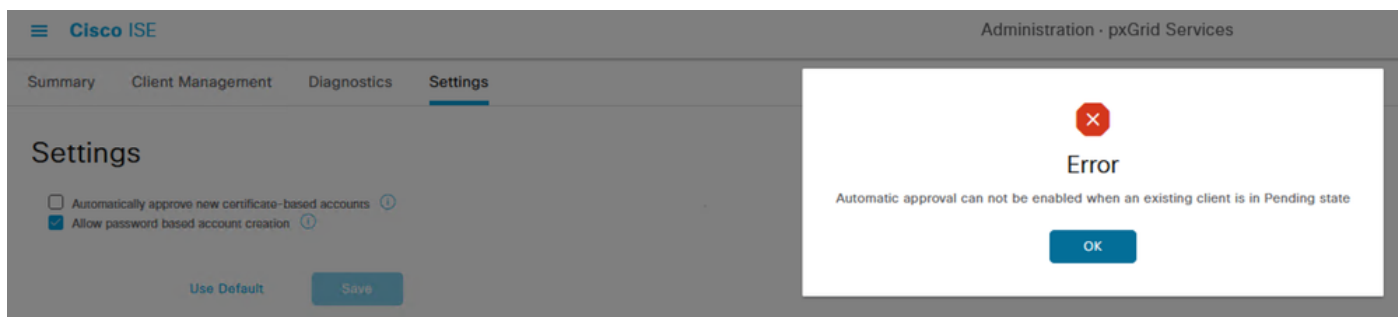
FMC客戶端處於掛起狀態。



確認pxGrid客戶端的批准。

請注意，如果要啟用基於證書的pxGrid客戶端的自動審批。

批准/拒絕上一頁的客戶端，因為可能會出現此警報。



與批准pxGrid客戶端相關的錯誤。

PxGrid ISE證書 鏈 不完整.

在此場景中，如果導航到選單Administration > System > Certificate，請選擇pxgrid證書並選擇View選項，

如果憑證有問題，可能會出現這些相關的錯誤。

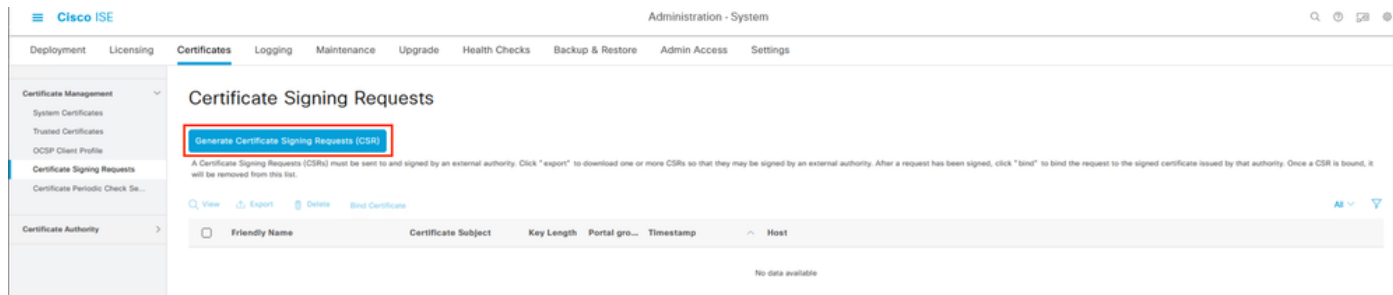
 Certificate trust chain is incomplete

與證書鏈不完整相關的錯誤。

T要檢查的第一步是是否已完成ISE根CA在「檢視」選項中關閉。

如果層次結構中缺少證書，您可以頒發整個ISE部署根CA。

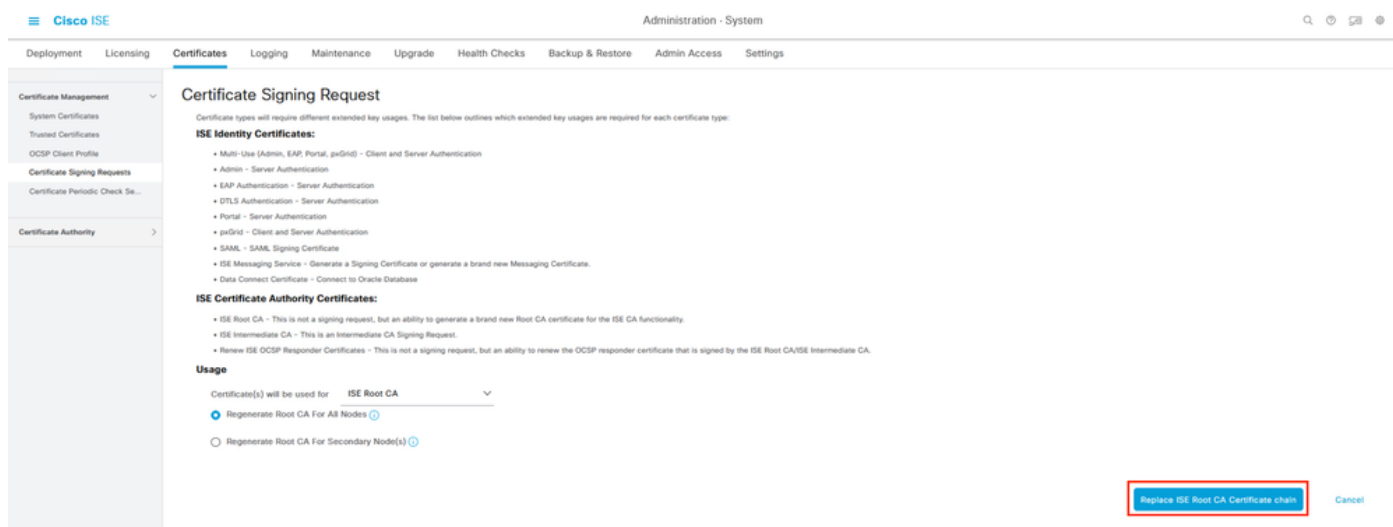
B瀏覽至選單Administration > System > Certificates > Certificate Management > Certificate Signing Request(CSR)和 選擇該按鈕。



在ISE上生成CSR。

在此選單中，選擇 使用ISE根CA 並再生所有節點的ISE根CA。

繼續按鈕操作 替換ISE根CA證書鏈。



正在配置證書簽名請求。

等待IMP的所有節點中生成證書病理。

完成後，ISE顯示下一個通知。

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

Overview

Issued Certificates

Certificate Authority Certifica...

Internal CA Settings

Certificate Templates

External CA Settings

CA Certificates

Edit

+ Import

Export

Delete

View

Refresh

	Friendly Name	Status	Trusted For	Serial Number	Issued To
▼ n1ise32					
☐	Certificate Services Root CA - n1ise32W00021	Enabled	Infrastructure,Endpoints	56 1C BA C5 B6 69 43 FF 9F E1 7B 84 02 91 F5 52	Certificate Services Root CA - n1ise32
☐	Certificate Services Node CA - n1ise32W00022	Enabled	Infrastructure,Endpoints	2F 9D AC 27 FF 20 43 71 8D 3E FB 2A 85 1D 5D B7	Certificate Services Node CA - n1ise32
☐	Certificate Services Endpoint Sub CA - n1ise32W00023	Enabled	Infrastructure,Endpoints	13 A5 F8 63 5F 5E 4C 24 AE 7A 0A 98 2D 9E 01 BC	Certificate Services Endpoint Sub CA - n1ise32
☐	Certificate Services OCSP Responder - n1ise32W00024	Enabled	Infrastructure,Endpoints		
> n2ise32					
> n3ise32					

×

There will be some delay in generating and showing certificates. Please refresh the table if certificates do not show up

OK

確認證書生成。

確認pxGrid證書信任鏈已完成 通過選擇選項 檢視 在系統證書中。

參考。

[PxGrid思科開發人員頁面。](#)

[思科身份服務引擎管理員指南3.2版，章節：Cisco pxGrid。](#)

[思科身份服務引擎安裝指南3.2版，章節：思科ISE埠參考](#)

[思科身份服務引擎CLI參考指南2.4版](#)

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）。