

FMC 7.2.4統合でのISE 3.2の設定およびトラブルシューティング

内容

[はじめに](#)

[前提条件](#)

[使用するコンポーネント](#)

[バックグラウンド情報](#)

[設定](#)

[統合のためにISEを準備します。](#)

[統合のためにFMCを準備します。](#)

[ISEとFMC間のpxGrid接続の設定](#)

[検証を行います。](#)

[FMCで検証します。](#)

[ISEでの検証。](#)

[トラブルシュート](#)

[FMCでのトラブルシューティング。](#)

[ISEでのトラブルシューティング](#)

[一般的な問題](#)

[PxGridサブスクライバクライアントがISEで承認されていません。](#)

[PxGrid ISE証明書チェーンが不完全です。](#)

[参照](#)

はじめに

このドキュメントでは、Platform Exchange Grid接続を使用して、Identity Services Engine(ISE)をファイアウォール管理センター(FMC)と統合する手順について説明します。

前提条件

次の項目に関する知識があることが推奨されます。

- Identity Services Engine (ISE)
- Platform Exchangeグリッド
- ファイアウォール管理センター(FMC)
- TLS/SSL証明書。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Identity Services Engine(ISE)バージョン3.2パッチ3
- Firewall Management Center(FMC)バージョン7.2.4

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

バックグラウンド情報.

このドキュメントでは、pxGridバージョン2を使用してFMCとISEを統合するソリューションについて説明します。

Cisco Firepower Management Center(FMC)は、次世代ファイアウォールおよび侵入防御システムのための中央集中型プラットフォームで、ポリシー管理、脅威検出、インシデント対応を提供します。

Cisco Identity Services Engine(ISE)は、認証、許可、アカウントビリティ(AAA)のサービスとポリシー適用を提供することで、エンドポイントへのセキュアなアクセスを実現する包括的なソリューションです。

Platform Exchange Grid(pxGrid)を使用すると、マルチベンダーのクロスプラットフォームネットワーク間で情報を交換できます。

この統合により、セキュアなモニタリング、脅威の検出、および共有される情報に基づくネットワークポリシーの設定が可能になります。

PxGridフレームワークには2つのバージョンがあります。どちらを使用するかは、確認する必要があるISEのバージョンとパッチによって異なります。

バージョンISE 3.1以降、すべてのpxGiseからのRID接続は、pxgridバージョンに基づいています
2.

PxGridバージョン1。

Tこのフレームワークの最初のバージョン (pxGrid v1) show application status iseコマンドで確認したサービサビリティによって特徴付けられます。次の出力に表示されているとおりです。

ノードでpxGrid機能を有効にすると、pxGrid 機能 実行中のステータス.

```
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バージョン1サービスアビリティ。

このプラットフォームのこのバージョンでは、他のpxGridノードがスタンバイ状態にある間、実行中の状態にあるpxGridプロセスを持つpxGridノードは1つだけであることが知られています。

これらのノードは、関連するサービスが実行されているpxGridノードのステータスを常に監視しています。

その中で、プライマリpxGridノードはプロモーションがあり、他のpxGridノードはpxGridサービスを有効にしました。

ただし、これは、このフェールオーバーが発生した際のダウンタイムを表していました。

pxgridの最初のバージョンは、コラボレーションおよび音声インフラストラクチャで使用するテクノロジーセットであるExtensible Messaging and Presence Protocol(XMPP)での通信に基づいています。

pxGrid v1接続で共有されるトピックは次のとおりです。

- セッションディレクトリ
- エンドポイントプロファイルメタデータ
- Trustsecメタデータ
- エンドポイント保護機能
- 適応型ネットワーク制御
- MDM_Offlineトピック
- Identity
- SXP

PxGridバージョン2。

このドキュメントでは、PxGridバージョン2の使用について説明します。このプラットフォーム

は、ISEおよびWebSocketプロトコル上でREST操作を使用して動作し、データモデルの拡張機能、改善されたスケーラビリティ、パフォーマンス、および柔軟性をもたらします。

このバージョンでは、show application status iseコマンドを使用して、以前のバージョンのようにpxgrid機能を実行することはできません。

pxGrid機能を確認するために確認するメカニズムについては、このドキュメントのISEの検証セクションを参照してください。

このバージョンでは、アクティブpxGridノードとして設定するすべてのpxGridノードがあります。これらはいつでも情報交換に参加する準備ができています。

バージョン1では、1つのノードのみがpxGridのサービスビリティを実行中として保持していました。

pxGrid v2接続で共有されるトピックは次のとおりです。

- セッションディレクトリ
- Radiusの障害
- プロファイラの設定
- システムヘルス
- MDM
- ANCステータス
- TrustSecの
- TrustSecの設定
- TrustSec SXP
- エンドポイント資産。

プラットフォームとしてのpxGridのコンポーネント

PxGridコントローラ(ISE):pxGridを使用する各参加者を信頼する必要があります。

クライアント：さまざまなトピックのサブスクライバとパブリッシャを指定できます。

パブリッシャ：コントローラと情報を共有するクライアント。

サブスクライバ：トピックの情報を消費するクライアント。

この統合により、ISEによって共有される情報および公開されたトピック (エンドポイントアクティビティに関連) に基づいて、FMCでコンテンツポリシーを作成できます。

設定

統合のためにISEを準備します。

ステップ 1：メニューAdministration > System > Deploymentで、ISEノード上でpxGridペルソナを実行するようにISEノードを設定します。

ノードを選択し、pxGrid機能を有効にします。

 Dedicated MnT 

None

☐ Enable Passive Identity Service ⓘ

pxGrid ⓘ

Q ?

Test

Clients Topics

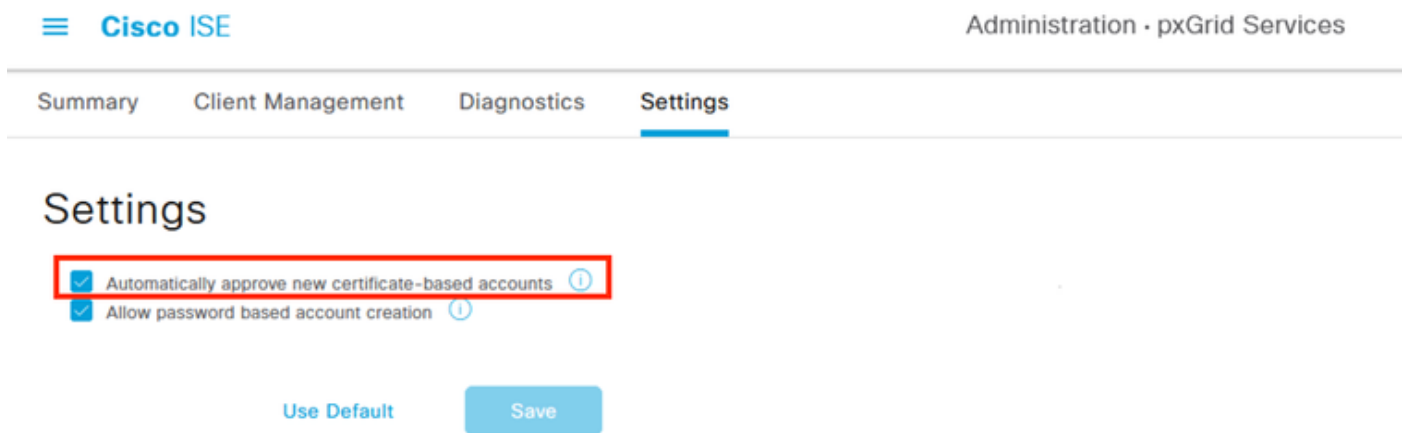
Clients

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

ステップ3: メニューAdministration > pxGrid Services > Settingsの順に移動し、Automatically approve new certificate-base accountsのオプションを選択します。

この手順は現時点ではオプションですが、pxGrid接続の場合は、このチェックボックスをオンにすることをお勧めします。

その後、FMCをサブスクライバとして手動で受け入れることができます。

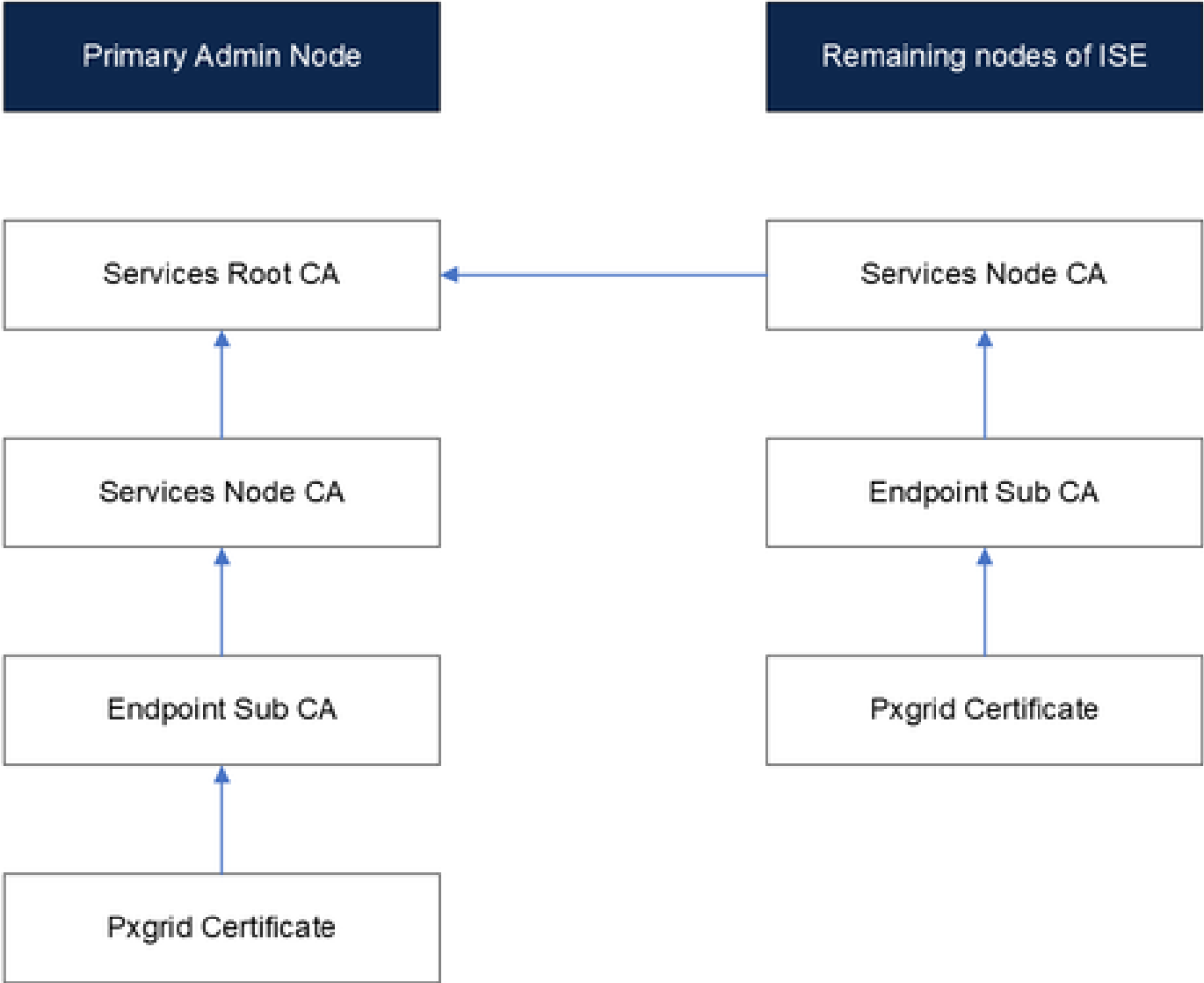


pxGrid証明書ベースのアカウントの自動承認を有効にしています。

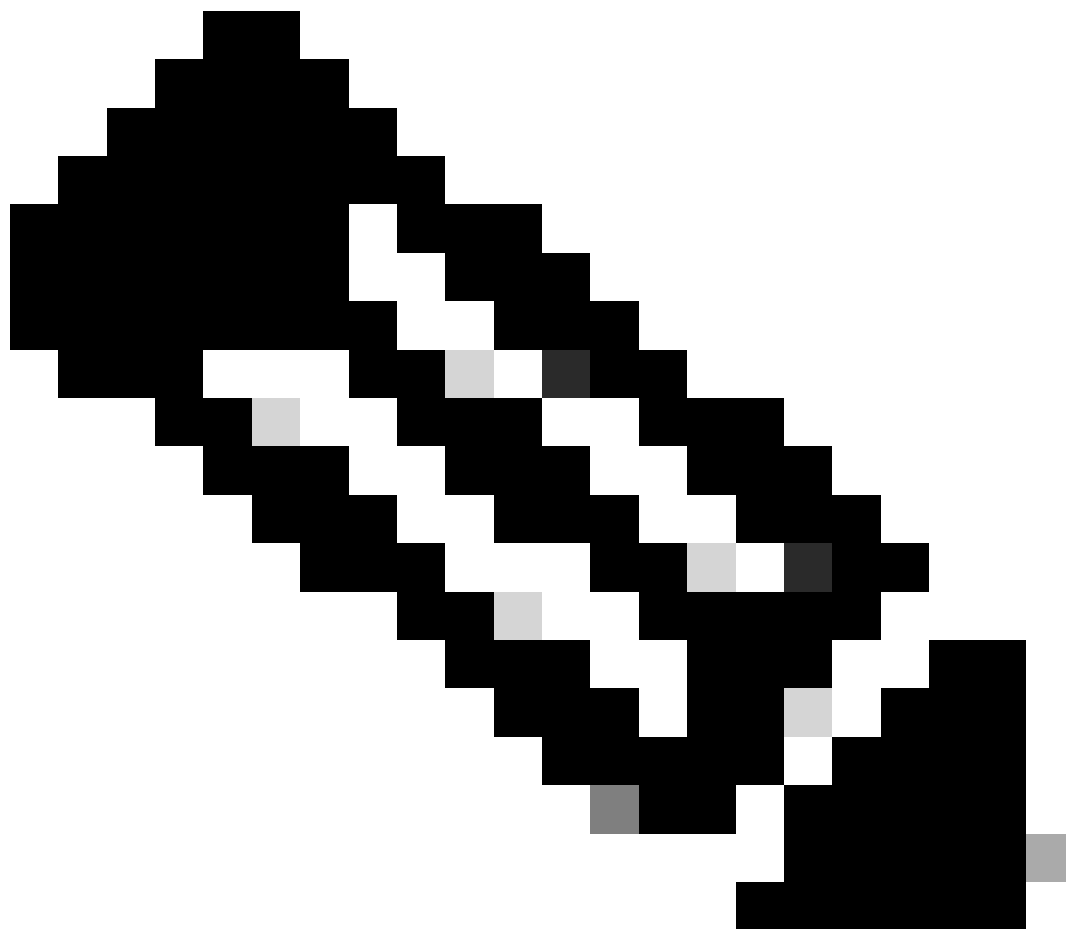
ステップ4:環境のpxGrid機能に関連する証明書をAdministration > System > System Certificatesで確認します。

同じルート認証局(CA)によって署名された展開のすべてのノードに、均一なpxGrid証明書をインストールすることをお勧めします

このシナリオでは、生成された内部ISE証明書を使用します。このバージョンのISEでは、この例ではルートCAがPANノードに対応します。



ISEの内部証明書のダイアグラムを作成します。



注:ISEで生成される証明書の内部構造の詳細については、「[ISEの内部認証局サービスについて](#)」を参照してください。

System Certificates ⚠ For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.								
Edit + Generate Self Signed Certificate + Import Export Delete View								
Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status	
CA - sspstse01sspstse01								
☐ CN=sspstse01.sspstsec.mex, O=U=Certificate Services System Certificate#Certificate Services Endpoint Sub CA - sspstse01#00002	pxGrid		sspstse01.sspstsec.mex	Certificate Services Endpoint Sub CA - sspstse01	Fri, 30 Jun 2023	Sat, 1 Jul 2028	☒	Active
☐ ise01_External_CA	Admin, EAP Authentication, RADIUS DTLS, Portal	Default Portal Certificate Group ⓘ	sspstse01.sspstsec.mex	sspstsec-CXLABS-WIN2K22D-CA-2	Mon, 3 Jul 2023	Wed, 2 Jul 2025	☒	Active
sspstse02								
☐ Default self-signed saml server certificate - CN=SAML.sspstse01.sspstsec.mex	SAML		SAML.sspstse01.sspstsec.mex	SAML.sspstse01.sspstsec.mex	Sat, 1 Jul 2023	Thu, 29 Jun 2028	☒	Active
☐ ise02_External_CA	Admin, EAP Authentication, RADIUS DTLS, Portal	Default Portal Certificate Group ⓘ	sspstse01.sspstsec.mex	sspstsec-CXLABS-WIN2K22D-CA-2	Mon, 3 Jul 2023	Wed, 2 Jul 2025	☒	Active
☐ CN=sspstse02.sspstsec.mex, O=U=ISE Messaging Service#Certificate Services Endpoint Sub CA - sspstse02#00004	ISE Messaging Service		sspstse02.sspstsec.mex	Certificate Services Endpoint Sub CA - sspstse02	Sat, 1 Jul 2023	Sun, 2 Jul 2028	☒	Active
☐ CN=sspstse02.sspstsec.mex, O=U=Certificate Services System Certificate#Certificate Services Endpoint Sub CA - sspstse02#00003	pxGrid		sspstse02.sspstsec.mex	Certificate Services Endpoint Sub CA - sspstse02	Sat, 1 Jul 2023	Sun, 2 Jul 2028	☒	Active

分散配置でのPxGrid証明書。

ステップ 5: pxGrid証明書のステータスを確認します。

前のメニューから、ノードpxGrid証明書のチェックボックスを選択し、オプションビューを選択します。

出力は、pxGrid証明書の中に次のように表示されます。

The screenshot displays the Cisco ISE Administration console. The left sidebar shows the navigation menu with 'Certificate Management' expanded. The main content area is titled 'System Certificates' and includes a table of certificates. A modal window titled 'Certificate Hierarchy' is open, showing the hierarchy of certificates and the details of a selected certificate.

System Certificates Table:

Friendly Name	Used By	Portal group tag
CA - ssp0501100001		
CH-sps0501 sspsec.mex, O U-Certificate Services System Certificate/Certificate Services Endpoint Sub CA - ssp0501000002	gaGrid	
ise01_External_CA	Admin, EAP Authentication, RADIUS DTLS, Portal	Default Portal Certificate S
▼ ssp0502		
Default self-signed saml server SAML certificate - CN=SAML_sps0501.sspsec.mex		
ise02_External_CA	Admin, EAP Authentication, RADIUS DTLS, Portal	Default Portal Certificate S

Certificate Hierarchy:

- Certificate Services Root CA - ssp0501
- Certificate Services Node CA - ssp0502
- Certificate Services Endpoint Sub CA - ssp0502
- ssp0502 sspsec.mex**

Certificate Details:

- Issued By:** Certificate Services Endpoint Sub CA - ssp0502
- Expires:** Sun, 2 Jul 2028 11:45:44 MDT
- Certificate status is good**

Details:

- Issued To:**
- Common Name (CN):** ssp0502.sspsec.mex
- Organization Unit (OU):** Certificate Services System Certificate
- Organization (O):**
- City (L):**
- State (ST):**
- Country (C):**

pxGrid証明書の検証。

統合のためにFMCを準備します。

ステップ 1 : FMC内部時刻が 最新.

移動先： システム>構成 時間 FMCに設定されている時刻が 最新.

The screenshot shows the FMC System Configuration page. The left sidebar lists various configuration options, with 'Time' selected at the bottom. The main content area displays the 'Current Setting' for 'Via NTP (based on System Configuration Time Synchronization)' as of 2023-08-26 19:08. Below this, a table lists NTP servers:

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

The right sidebar shows the 'Configuration' tab selected, with sub-tabs for Users, Domains, Updates, Licenses, Smart Licenses, and Classic Licenses. The 'Monitoring' tab is also visible, showing Monitor, Policy, Events, Exclude, Monitor Alerts, and Tools.

FMCが最新であることを確認します。

FMC時刻が更新されていない場合は、NTPが正しく設定されていることを確認します と イン sync.NTPは システム>設定>時間> +追加.

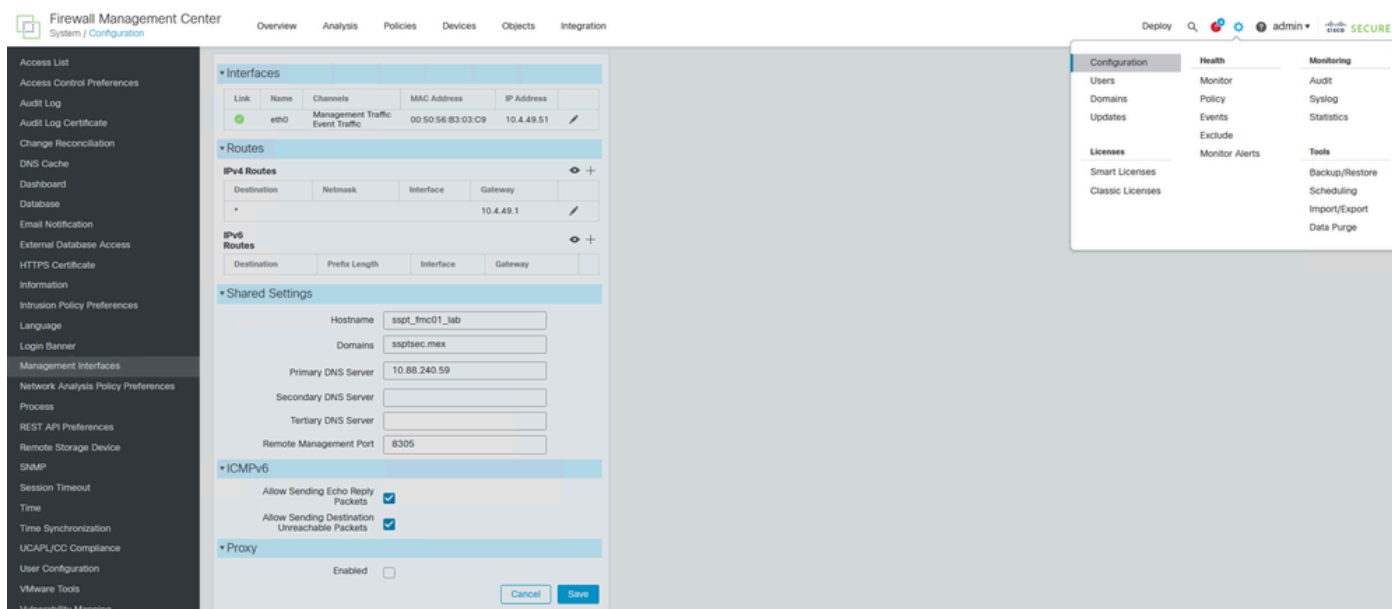
The screenshot shows the FMC System Configuration page, specifically the 'Time Synchronization' section. The left sidebar lists various configuration options, with 'Time Synchronization' selected at the bottom. The main content area displays the 'Set My Clock' section, where 'Serve Time via NTP' is set to 'Enabled'. Below this, there are options to 'Manually in Local Configuration' or 'Via NTP'. The 'Via NTP' option is selected, and a table lists NTP servers:

NTP Server	Authentication	Action
0.sourcefire.pool.ntp.org	N/A	Q / [icon]
1.sourcefire.pool.ntp.org	N/A	Q / [icon]

The right sidebar shows the 'Configuration' tab selected, with sub-tabs for Users, Domains, Updates, Licenses, Smart Licenses, and Classic Licenses. The 'Monitoring' tab is also visible, showing Monitor, Policy, Events, Exclude, Monitor Alerts, and Tools.

FMCでの時刻同期

ステップ 2： 移動先： システム>構成 Management Interface >共有設定 少なくとも – プライマリDNSサーバ フィールド 含む 有効な DNSサーバのIP。



FMCでのDNS設定。

ステップ 3 : FMCホスト名が設定されていることを確認します。

移動先 : システム>設定>管理インターフェイス>共有設定 確認してください ホスト名 フィールドにはFMCホスト名が含まれます。

このセクションの前の手順を確認する際に、この手順を確認できます (一部の出力は省略) 。

ISEとFMC間のpxGrid接続の設定

ステップ 1 : メニューAdministration > pxGrid Services > Client Management > Certificatesに移動します。

最初のオプションで、I want to Generate a single certificate (without a certificate signing request).を選択します。

Common Name(CN)セクションで、ISEが証明書を発行するFMCのFQDNを入力します。

説明を入力します。

Subject Alternative Name (SAN)のセクションで、接続するFMCのFQDNとIPアドレスを入力します。

Certificate Download Formatの下部で、ドロップダウンメニューからCertificate in Privacy Enhanced Electronic Mail (PEM)形式のオプションを選択します。

入力PKCSS PEM形式 (証明書チェーンを含む) 。

後でFMCでパスワードを使用するときに、パスワードをCertificate Passwordに入力して保存します。

パスワードを確認し、Createを選択します。

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 (withou...▼

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証明書の生成例。

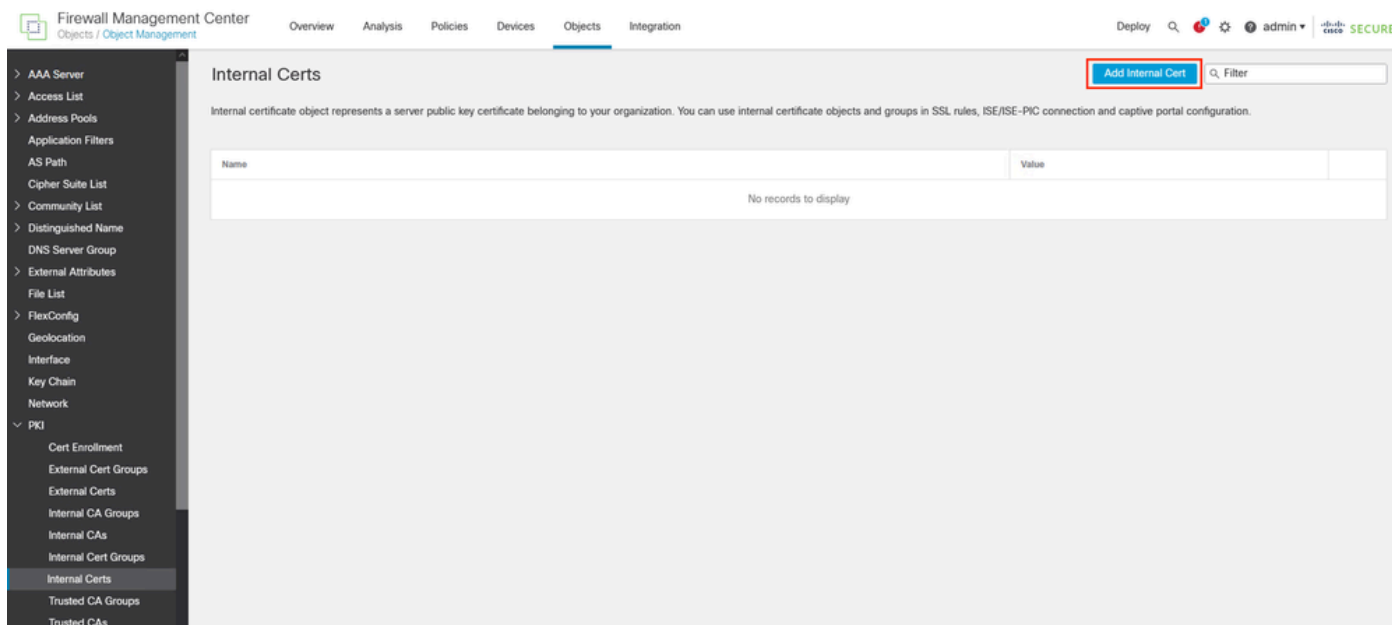
ステップ 2 : zipファイルがコンピュータにダウンロードされます。ファイルを圧縮解除し、環境に次のファイルがあることを確認します。

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

ISEによって生成されたPxGrid証明書。

ステップ 3 : FMCで、メニューObjects > Objects Management > PKI > Internal Certsに移動します。

Add Internal Certオプションを選択します。



内部証明書としてのFMC証明書の追加

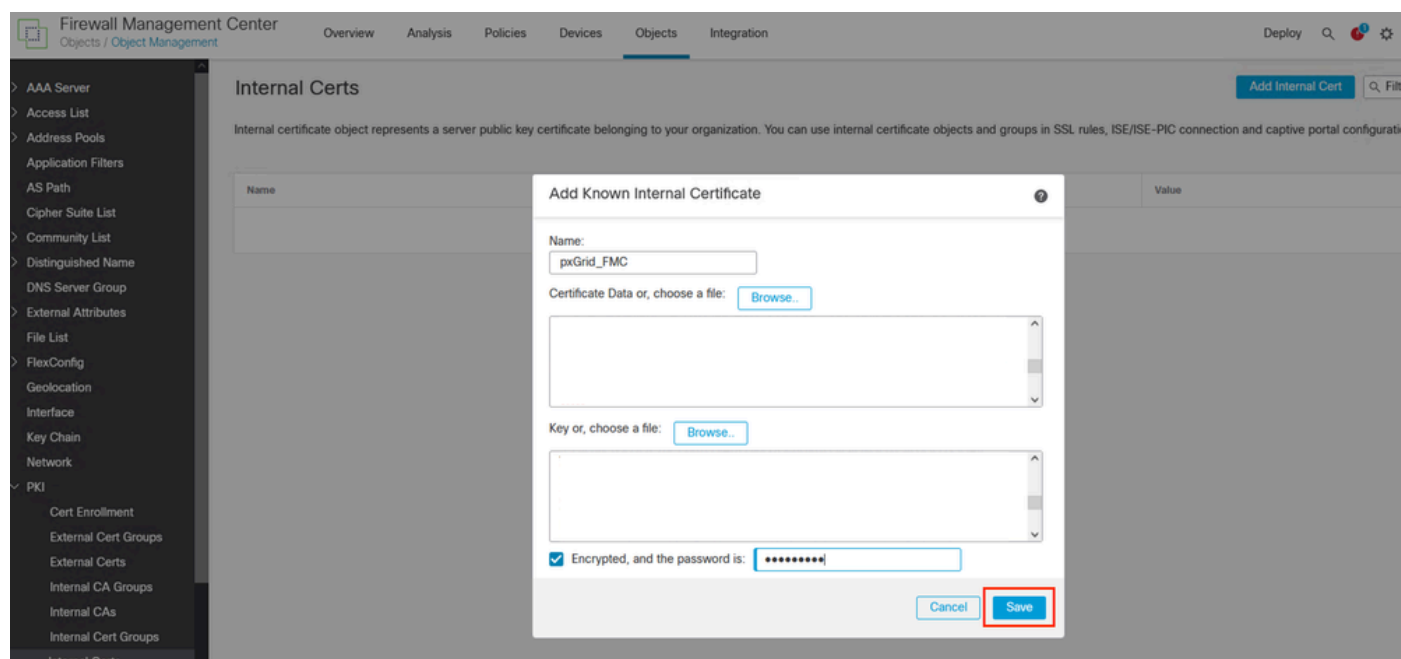
ステップ 4 : FMCで割り当てられる証明書に名前を付けます。

ISEの証明書データセクションで、FMC用に作成した証明書を参照します。

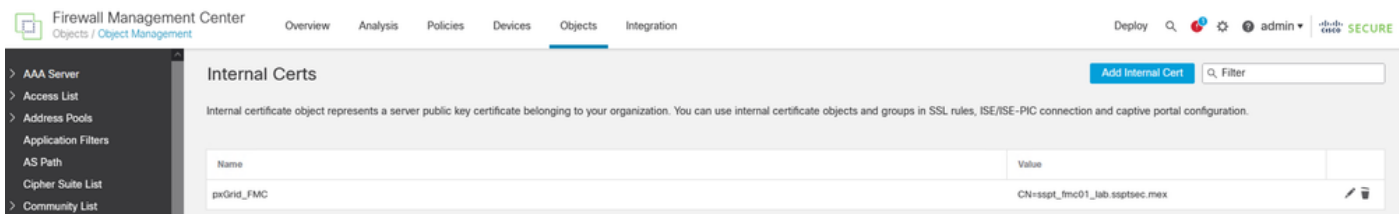
.keyという拡張子を持つファイルを参照し、次のフィールドに入力します。

Encryptedオプションを選択し、ISEで証明書を作成したときに使用したパスワードを入力します。

設定を保存します。



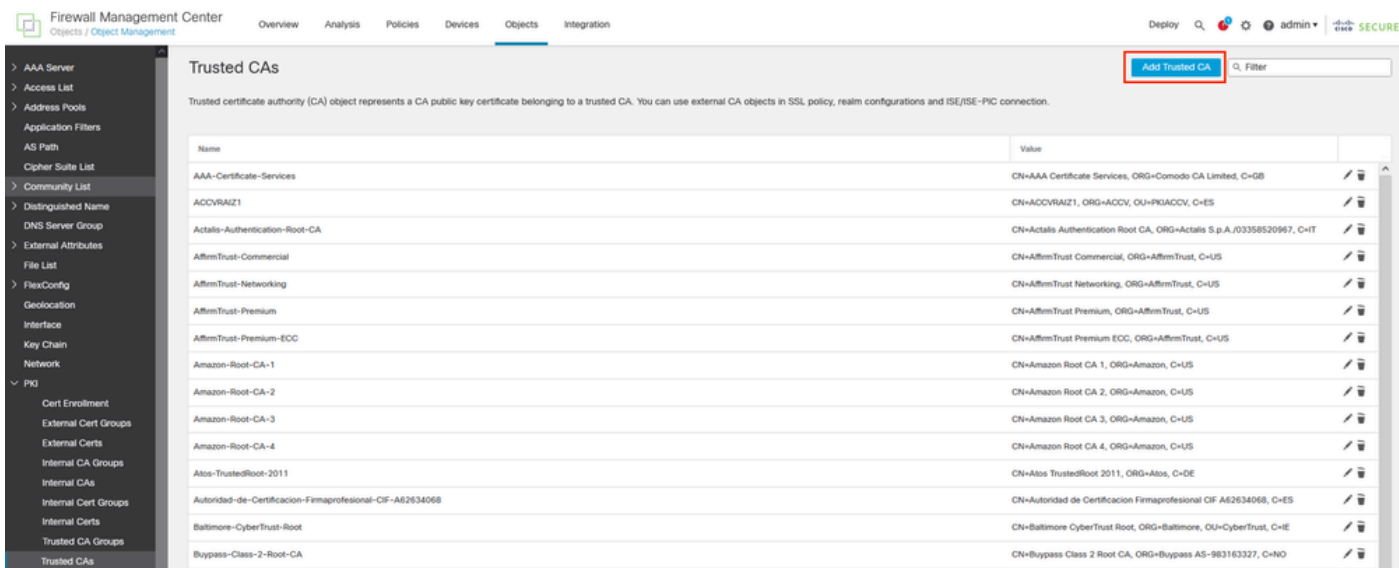
ISEによって生成されたFMC証明書をエクスポートします。



FMC証明書。

ステップ 5：メニューObjects > Objects Management > PKI > Trusted CAsに移動します。

Add Trusted CAsを選択します。

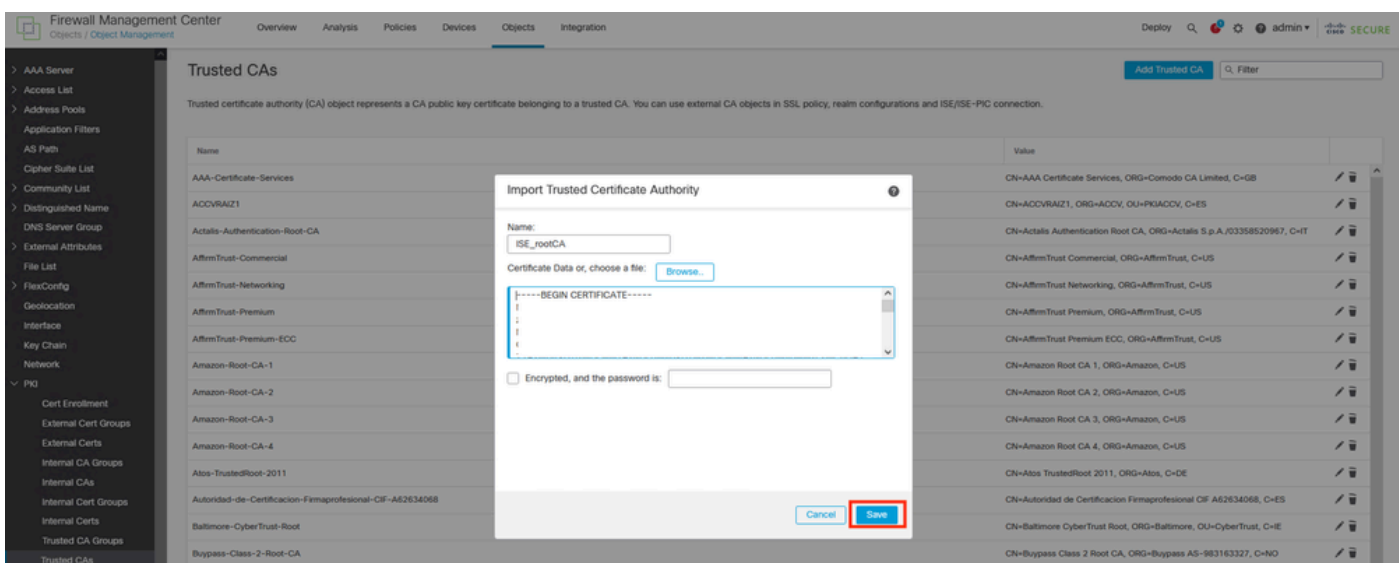


ISEルートCAを信頼できる証明書として追加します。

手順 6：認証局に名前を付けます。

ISEファイルからダウンロードしたISE rootCAを参照して選択します。

設定を保存します。



ISE rootCAをエクスポートします。

手順 7 : [統合] > [その他の統合] > [アイデンティティソース]メニューに移動します。

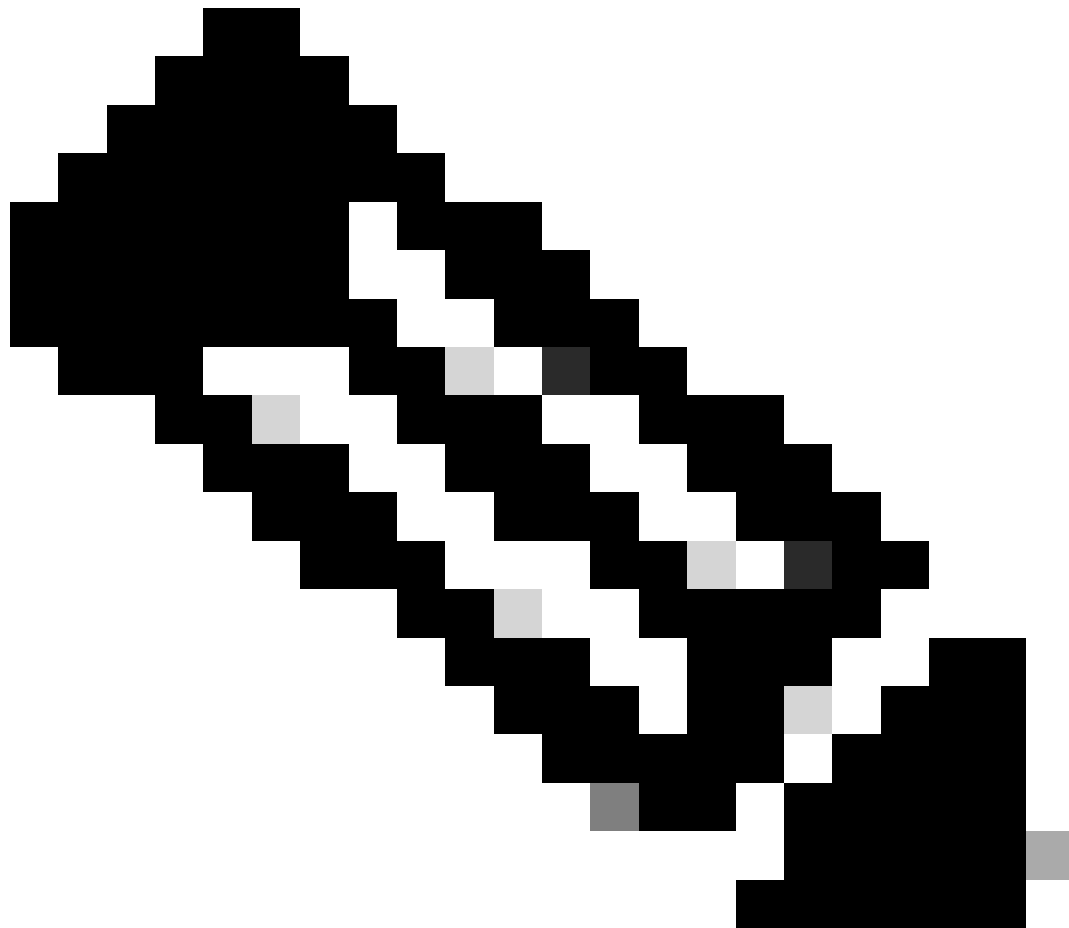
サービスタイプ : Identity Services Engineで選択します。

プライマリノードになるpxGridノードのIPアドレスまたはFQDNを入力します。

Secondary pxGridノードに対してこの手順を繰り返します。

ドロップダウンメニューから、セクション「pxGridクライアント証明書」のISEによって生成されたpxGrid証明書を選択します。

セクションMNT Server CAおよびpxGrid Server CAで、最後の手順でエクスポートしたISEルートCAを選択します。



注:pxGridサーバCAは、pxGridノード上のpxGridによって使用されている証明書のルート認証局(CA)に対応します。

MNTサーバCAは、MNTノード上のpxGridで使用されている証明書の認証局(CA)に対応します。

(オプション) ISEからセッションディレクトリとSXPトピックを登録できます。

設定を保存します。

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

You have unsaved changes Cancel Save

FMCでISEをアイデンティティソースとして設定します。

検証を行います。

FMCで検証します。

メニューで、設定を保存する前に、統合>その他の統合>アイデンティティソース> Identity Services Engineに移動します。pxGridリンクの設定をテストできます。

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が正常に通信しました。

Primary host:

[INFO]: PXGrid v2 is enabled

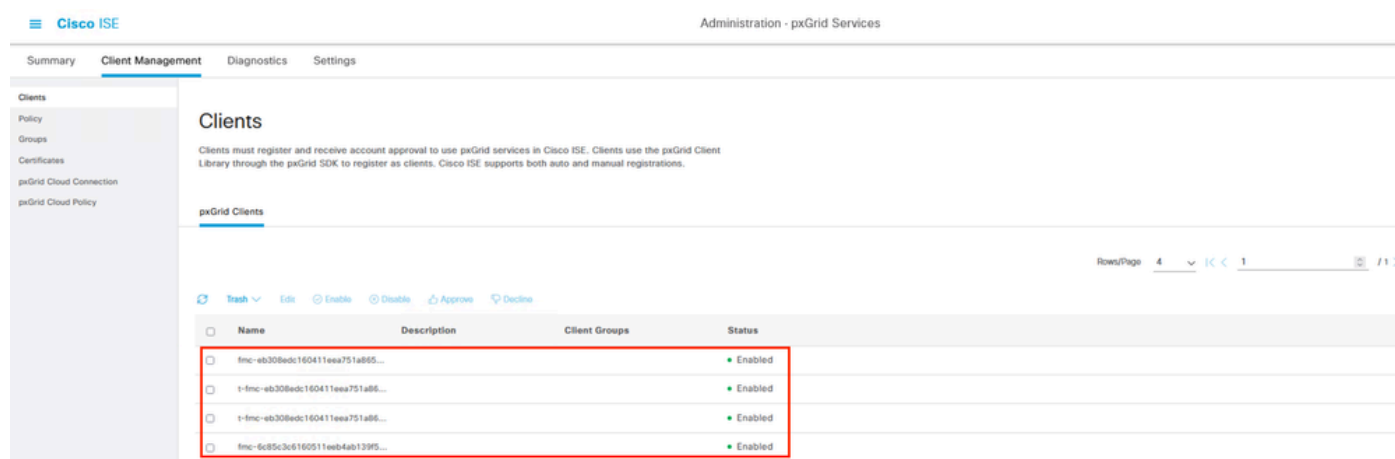

```
[INFO]: pxgrid 2.0: account activate succeeded
[INFO]: Successful connection to ssptise02.ssptsec.mex:8910
[INFO]: Successful connection to ssptise01.ssptsec.mex:8910
[INFO]: These ISE Services are up: SessionDirectory, SXP, EndpointProfile, SecurityGroups, AdaptiveNetwork
[INFO]: All requested ISE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

ISEでの検証。

FMC pxGridクライアントがISEに正常に統合されると、ユーザは、[こちら](#)を参照してください(の Administration > pxGrid Services > Client Management > Clientsメニュー) fmcという名前のクライアントが含まれ、enabled.



The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Cisco ISE' and 'Administration - pxGrid Services'. The left sidebar shows a menu with 'Clients' selected. The main content area is titled 'Clients' and contains a table of pxGrid clients. The table has columns for 'Name', 'Description', 'Client Groups', and 'Status'. There are four rows of clients, all with a status of 'Enabled'. A red box highlights the first four rows of the table.

Name	Description	Client Groups	Status
fmc-eb308edc160411eea751a865...			Enabled
t-fmc-eb308edc160411eea751a86...			Enabled
t-fmc-eb308edc160411eea751a86...			Enabled
fmc-6c85c3c6160511eeb4ab139f5...			Enabled

PxGridクライアントが使用可能で有効になっていること。



FMCがインストールされているシナリオでは、ハイ アベイラビリティ、次の例に示すように、プライマリユニットとセカンダリユニットが表示されます。

Cisco ISE

Administration - pxGrid Services

Summary Client Management **Diagnostics** Settings

WebSocket

Clients Topics

Clients

Rows/Page 2 < 1 Go 2 Total Rows

Client Name	Connect To	Session Id	Certificate	Subscriptions	Publications	IP Address	Status	Start time	Duration (dd:mm:ss)
fmc-e6308edc160411eeab7...	x asprise01	sasprise01.5	CR=rspr_fmcd1...	/api/com.cisco.ise.sesio...		10.4.49.51	Connected	2023-08-21 05:30:18 MDT	01:10:42
fmc-6d8fc3d6160511eeab4...	sasprise01	sasprise01.6	CR=rspr_fmcd1...	/api/com.cisco.ise.sesio...		10.4.49.52	Connected	2023-08-21 05:31:56 MDT	01:10:03

WebSocketはISEで使用できます。

次のタブ このメニューから 名前付き T光学、 次のことができます fmcサブスクライバがISEによって公開されたpxGridトピックに追加されていることを確認します。

たとえば、セキュリティグループに関連するトピックがあります。 値は次のとおりです。 ユーザは、 両方のFMCが サブスクライブされ、関連する情報を受信している から SGT ISEによって公開されます。

Cisco ISEAdministration - pxGrid Services

SummaryClient ManagementDiagnosticsSettings

WebSocketLogTests

WebSocketClientsTopics

Topics

Row/Page 101 < 1Go 10 Total Rows

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

Row/Page 101 < 1Go 2 Total Rows

Client Name	Messaging Role
fmc-eb308dc160411ea7...	Sub
fmc-6d85c3d160511eb4...	Sub

pxGridサブスクライバごとのトピック。

InメニューAdministration > pxGrid Services > Diagnostics > Log、 重要イベント 関連： in pxGrid通信 (有効な機能を持つノードの場合) が表示されます。

統合に関連する情報を示します。

Cisco ISEAdministration - pxGrid Services

SummaryClient ManagementDiagnosticsSettings

WebSocketLogTests

Live Log

Row/Page 251 < 1Go 131 Total Rows

Timestamp	Client	Server	Host	Event Type	Description
2023-08-21 06:31 -05:00	fmc-6d85c3d160511eb4b1395...	wsa://10.4.49.41/pxgrid/ise/pubsub	sxptise01	PUBSUB_SERVER_SUBSCRIBE	Pubsub subscribe, subscription=[d=880ba640-97d8-4c17-81c1-d591edca...
2023-08-21 06:31 -05:00	fmc-6d85c3d160511eb4b1395...	wsa://10.4.49.41/pxgrid/ise/pubsub	sxptise01	PUBSUB_SERVER_SUBSCRIBE	Pubsub subscribe, subscription=[d=b523e2d0-91e6-4199-be54-ed186cd9...
2023-08-21 06:31 -05:00	fmc-6d85c3d160511eb4b1395...	wsa://10.4.49.41/pxgrid/ise/pubsub	sxptise01	PUBSUB_SERVER_SUBSCRIBE	Pubsub subscribe, subscription=[d=30bccd50-9c75-4c3e-9b19-203fed12...
2023-08-21 06:31 -05:00	fmc-6d85c3d160511eb4b1395...	wsa://10.4.49.41/pxgrid/ise/pubsub	sxptise01	PUBSUB_SERVER_SUBSCRIBE	Pubsub subscribe, subscription=[d=a3d9508e-3001-4750-b6fb-3a25aaf49...
2023-08-21 06:31 -05:00	fmc-6d85c3d160511eb4b1395...	wsa://10.4.49.41/pxgrid/ise/pubsub	sxptise01	WS_SERVER_CONNECTED	WebSocket connected, session=[d=6,client=fmc-6d85c3d160511eb4b1...

PxGridライブログ。

トラブルシュート

FMCでのトラブルシューティング。

FMCが自身のホスト名とISEノードをホスト名で解決できることを確認します。

例：

<#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

```

以下を確認します。ADIプロセスが起動し、実行中です。

```
<#root>
```

```
>
```

```
expert
```

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

```
sudo su
```

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

```
pmtool status | grep adi
```

adi (normal) - Running 7911

EFMCからISEへの通信が ポートt TCP 8910が許可されます。FMCから CLI を使う場合： 私たちは 設定 a tcpdump 双方向通信を確認するためのパケットキャプチャ。

<#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

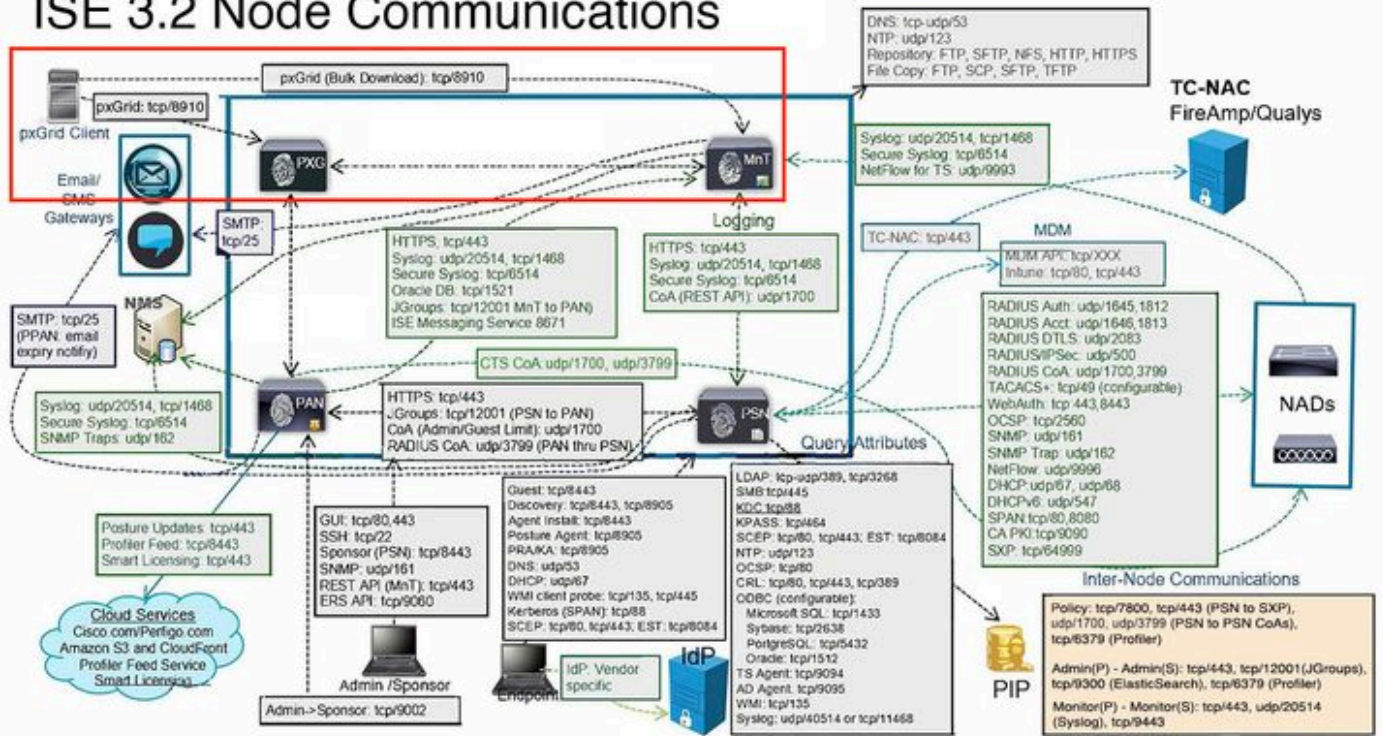
: Flags [.], ack 1, win 229, options [nop,nop,TS val 2701166400 ecr 2268665064], length 0
[...]

ISEでのトラブルシューティング

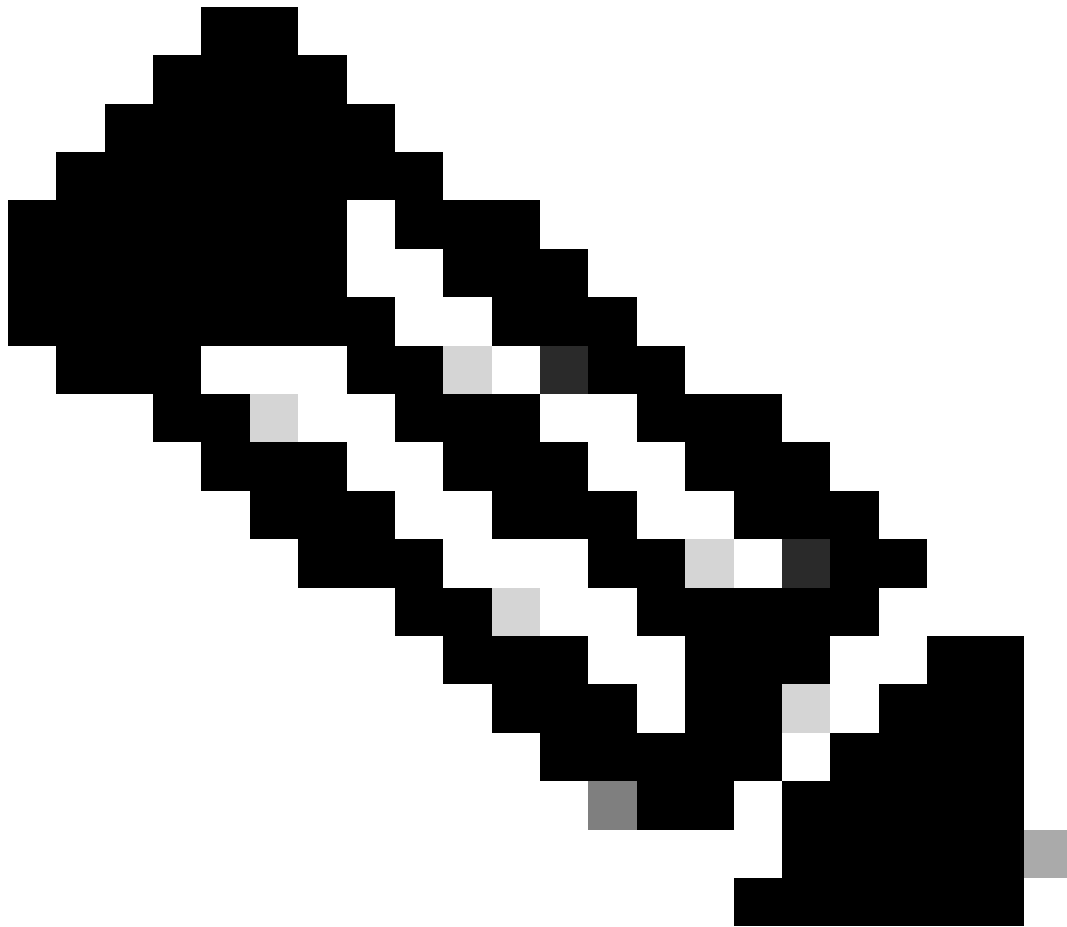
ポート8910の通信を確認します。動作しています。

これは、pxGridクライアントによって使用されるポートですを使用して、pxGridノードおよび MnTノードと通信し、情報を一括ダウンロードできます。

ISE 3.2 Node Communications



ISE環境でのPxGridインタラクション



注:pxGridクライアントは、この場合FMCがpxGridノード (クライアントID) およびセカンダリMNT(SMNT)ノードと通信して情報の (一括ダウンロード) を取得し、SMNTで障害が発生した場合はプライマリMNT経由で情報を検索します。

lpxGridクライアントとの通信が行われるISEノードでは、if the ポートは openまたは 接続されているソケットがある場合 ポートを指定します。

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

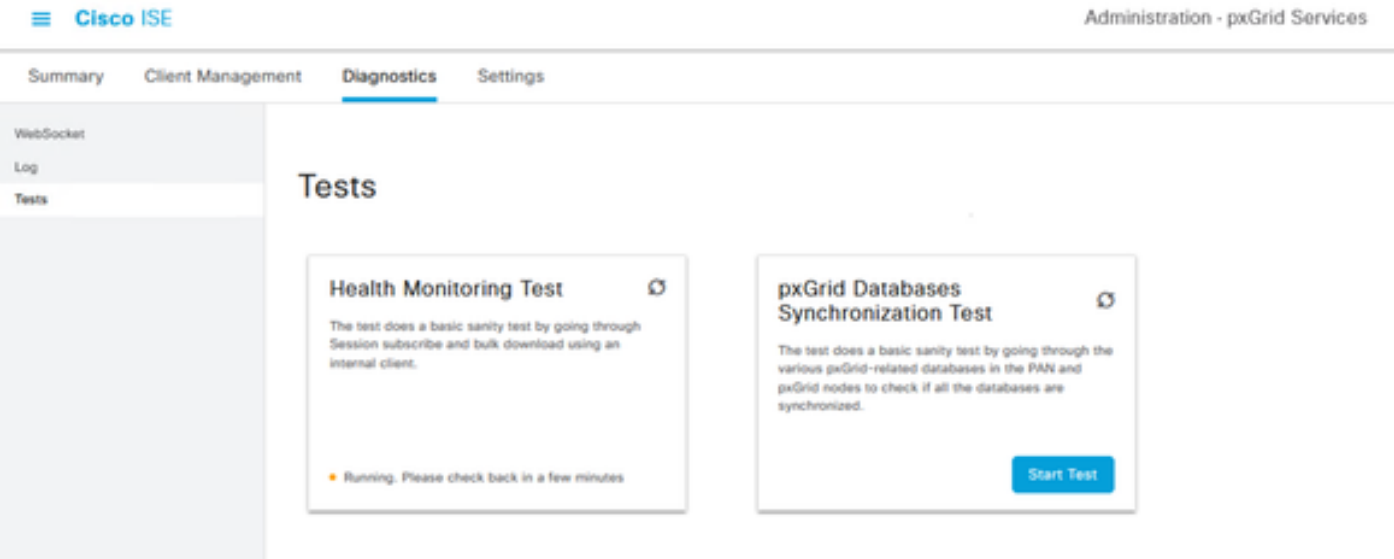
ISEでは、pxGrid実装の全体的なステータスを診断する2つのテストを利用できます。

それらはメニューにあります Administration > pxGrid Services > Diagnostics > Testの順に選択します。

このセクションに示すテストは、ISEの内部で実行されます。

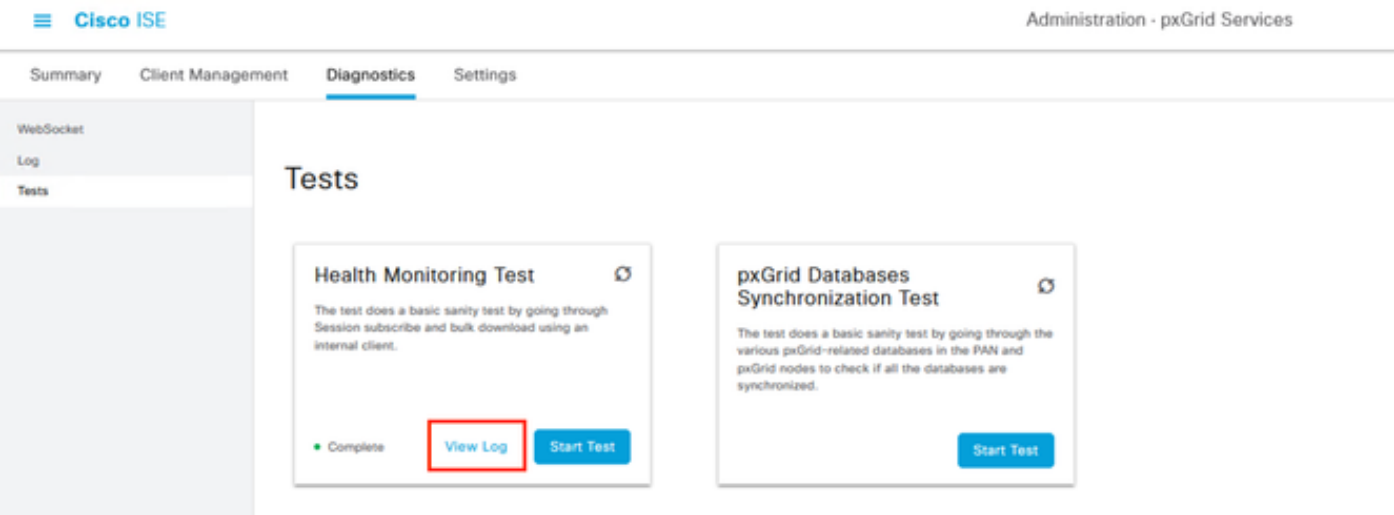
ヘルスマモニタリングテスト pxGridサービスの外観を確認します。up, クライアントがpxGridコントロールラによって公開されたセッションディレクトリ、サービス、およびトピックにアクセスできるかどうかを評価します。

を選択します。 オプション 開始 テスト ログが収集されるまで待ちます。



PxGridヘルスマモニタリングテスト。

テストが完了したら、 オプション View Logを選択します。 この例では、ログの内容は が:



ヘルスマモニタリングテストのレビュー。

```
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 -----
```



```

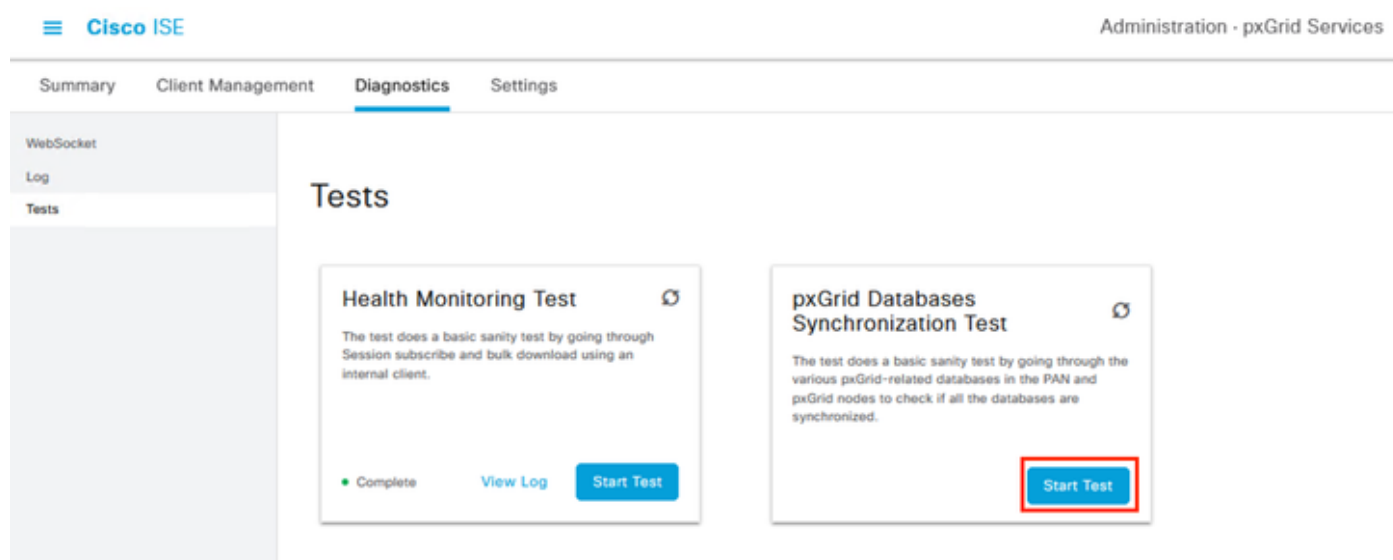
22-Aug-2023 17:03:15 [INFO] ----- Starting Download Test -----
22-Aug-2023 17:03:15 [INFO] Downloading sessions since 2023-08-21T17:03:15.273-06:00
22-Aug-2023 17:03:15 [INFO] Response status=200
22-Aug-2023 17:03:15 [INFO] Number of sessions read: 0
22-Aug-2023 17:03:15 [INFO] ----- Download Test Completed -----
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データベース同期テストで 情報 データベース内では、PANノードとpxGridノードの間が正しく、同期されます。

したがって、pxGridサブスクライバに送信される情報は 正確。

を選択します。 オプション テストの開始 結果が評価されるまで待ちます



PxGridデータベース同期テスト。

生成されたログから、次の出力を取得しました。

```

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

```

```

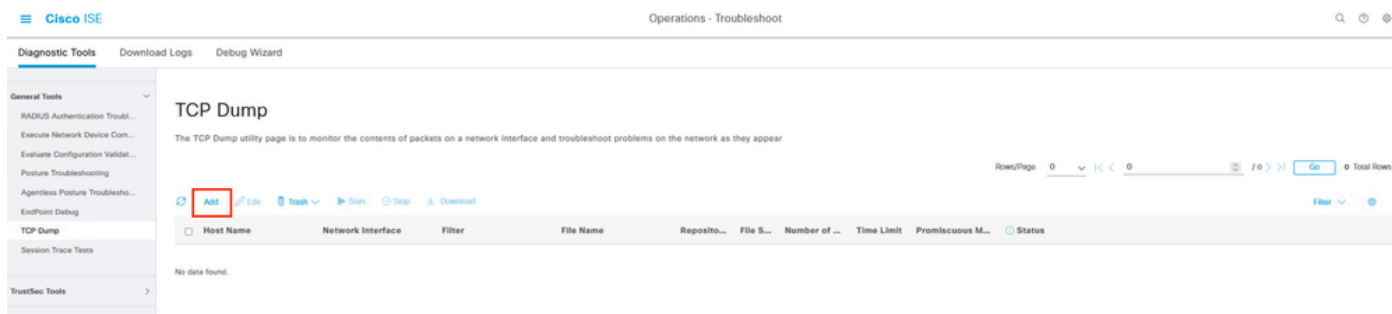
Primary PAN : ssptise01.ssptsec.mex
pxGrid Nodes : ssptise01.ssptsec.mex ssptise02.ssptsec.mex

```

キャプチャを収集する pxGridノードからプライマリFMCノードに向かって描画されます。

メニューに移動します Operations > Troubleshoot > Diagnostic Tools > TCP Dump、

を選択します。 オプション から 追加 新しいキャプチャ.



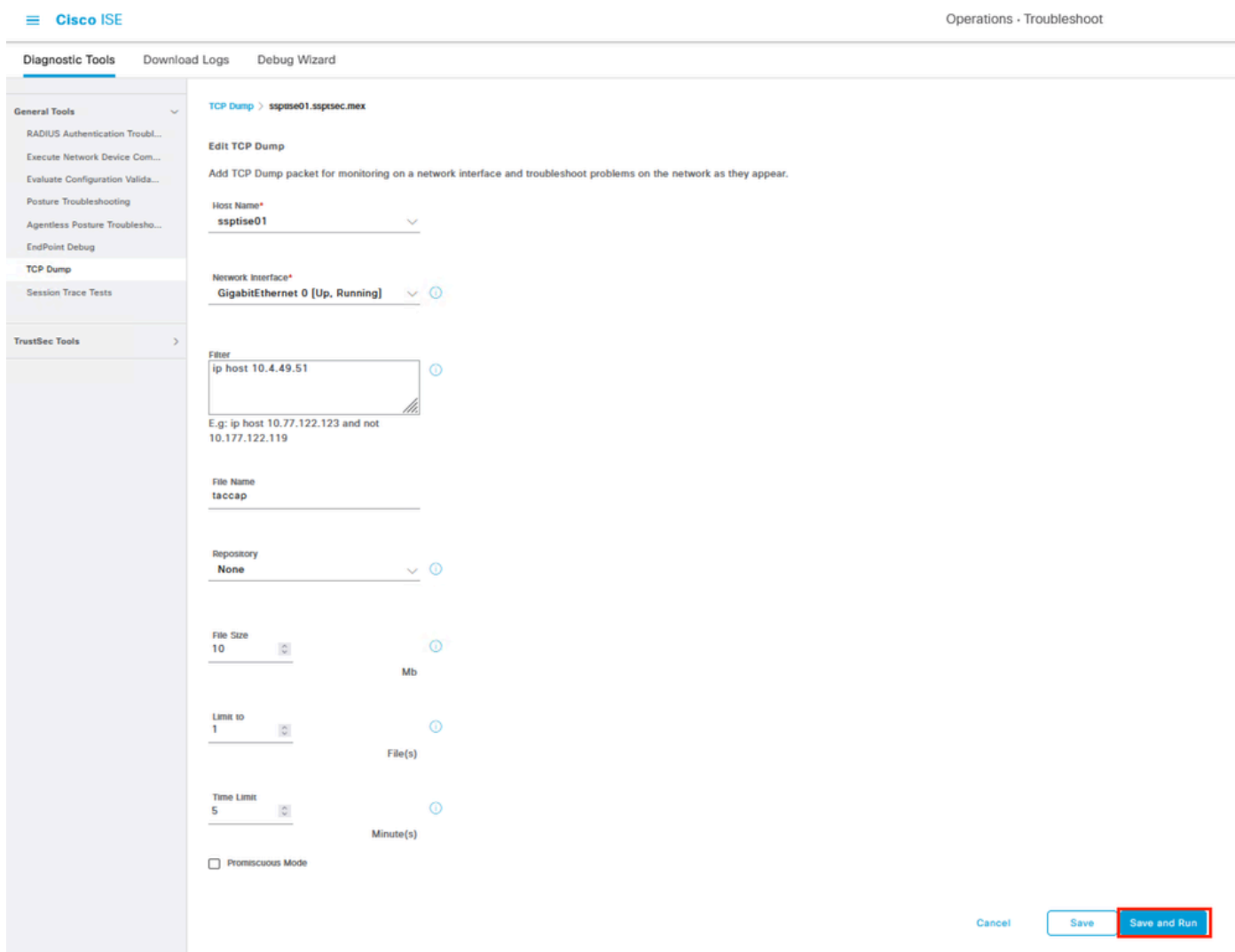
ISEでのパケットキャプチャの生成

キャプチャのパラメータを設定します。

イン ホスト名, fmcで選択したプライマリpxGridノードを選択します。

フィルタ トラフィックを 構文 ip host <FMCのIP>

キャプチャに名前を付けます そして – 進む から 保存します。 および実行.



パケットキャプチャの設定例。

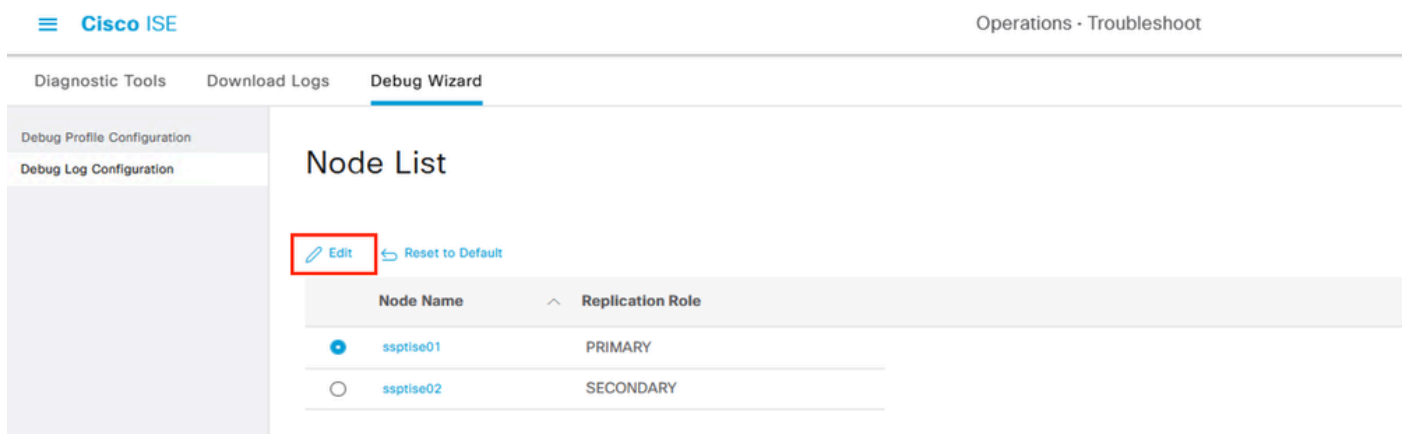
Wテストの結果が得られたら - 進む から Stop ISE上のキャプチャ。



10.4.49.51	10.4.49.41	TCP	74	* → 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	TLShv1.2	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	TLShv1.2	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	TLShv1.2	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	TLShv1.2	72	Change Cipher Spec
10.4.49.41	10.4.49.51	TLShv1.2	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	TLShv1.2	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
10.4.49.41	10.4.49.51	TLShv1.2	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
10.4.49.41	10.4.49.51	TLShv1.2	515	Application Data
10.4.49.41	10.4.49.51	TLShv1.2	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	TLShv1.2	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

さらに、ISEで、pxに関連するデバッグを収集できますグリッド処理。

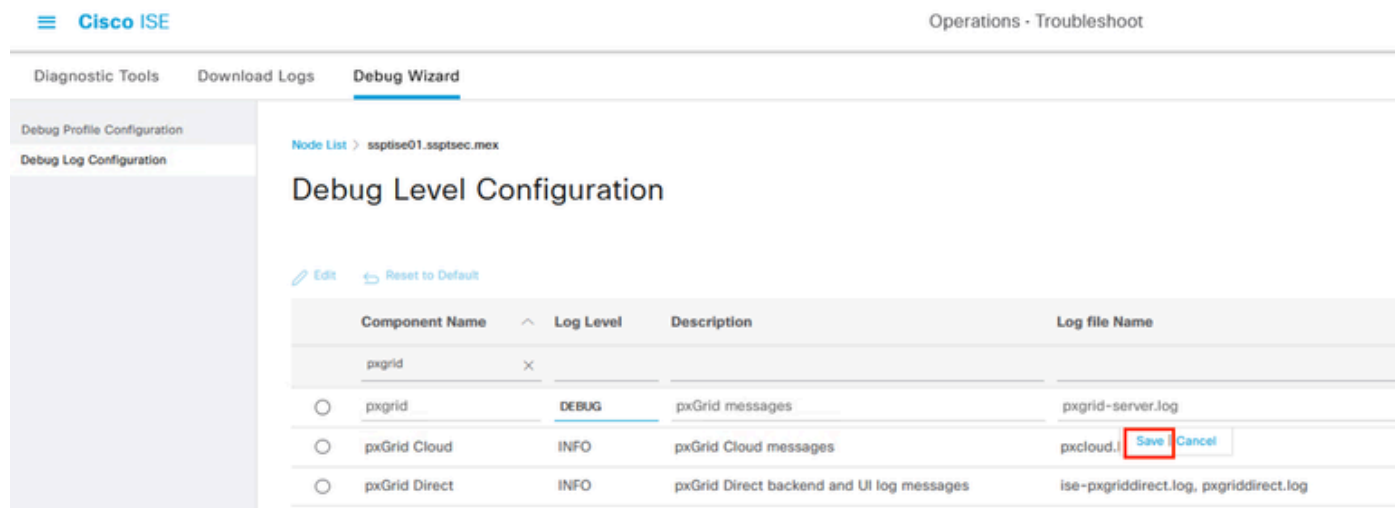
分析する対応するISEノードを選択し、編集。



ISEでデバッグするノードの選択

表示されるコンポーネントをフィルタし、 ログレベル: pxgridのデバッグ コンポーネント から 進む 分析を行います

保存します。 設定です。



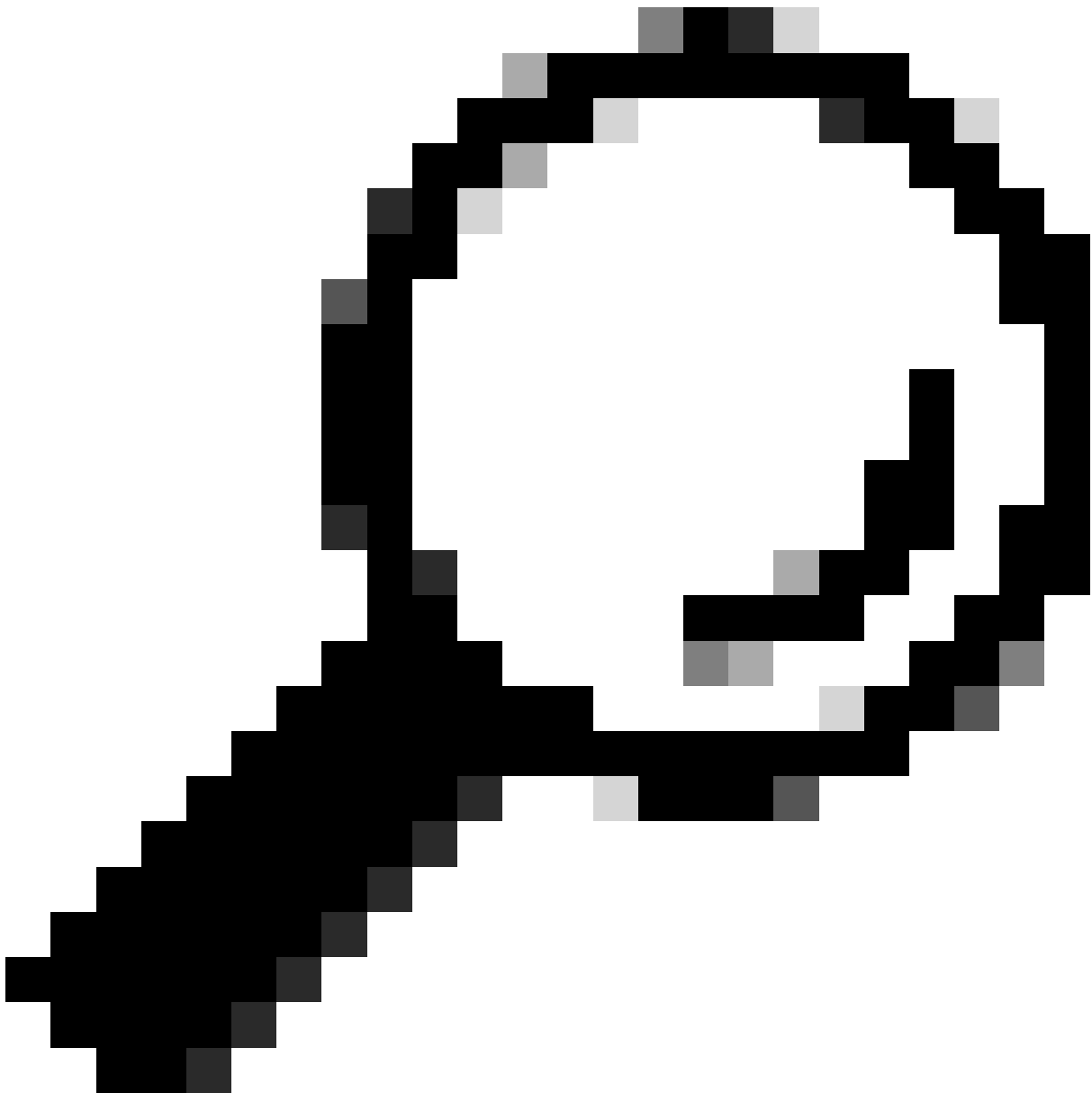
The screenshot shows the Cisco ISE interface with the 'Debug Wizard' tab selected. The 'Debug Log Configuration' section is active, displaying a table for 'Debug Level Configuration'. The table has columns for Component Name, Log Level, Description, and Log file Name. The 'pxgrid' component is selected, and its log level is set to 'DEBUG'. The 'pxGrid Cloud' component is set to 'INFO', and the 'pxGrid Direct' component is set to 'INFO'. The 'Save' button is highlighted with a red box.

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

pxGridコンポーネントをデバッグレベルに変更します。

分析する動作を再現し、進む pxgrid-server.logファイルで収集されたログを分析します。その他のログトラブルシューティングするISEノードで確認できる項目は次のとおりです。

```
#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
```

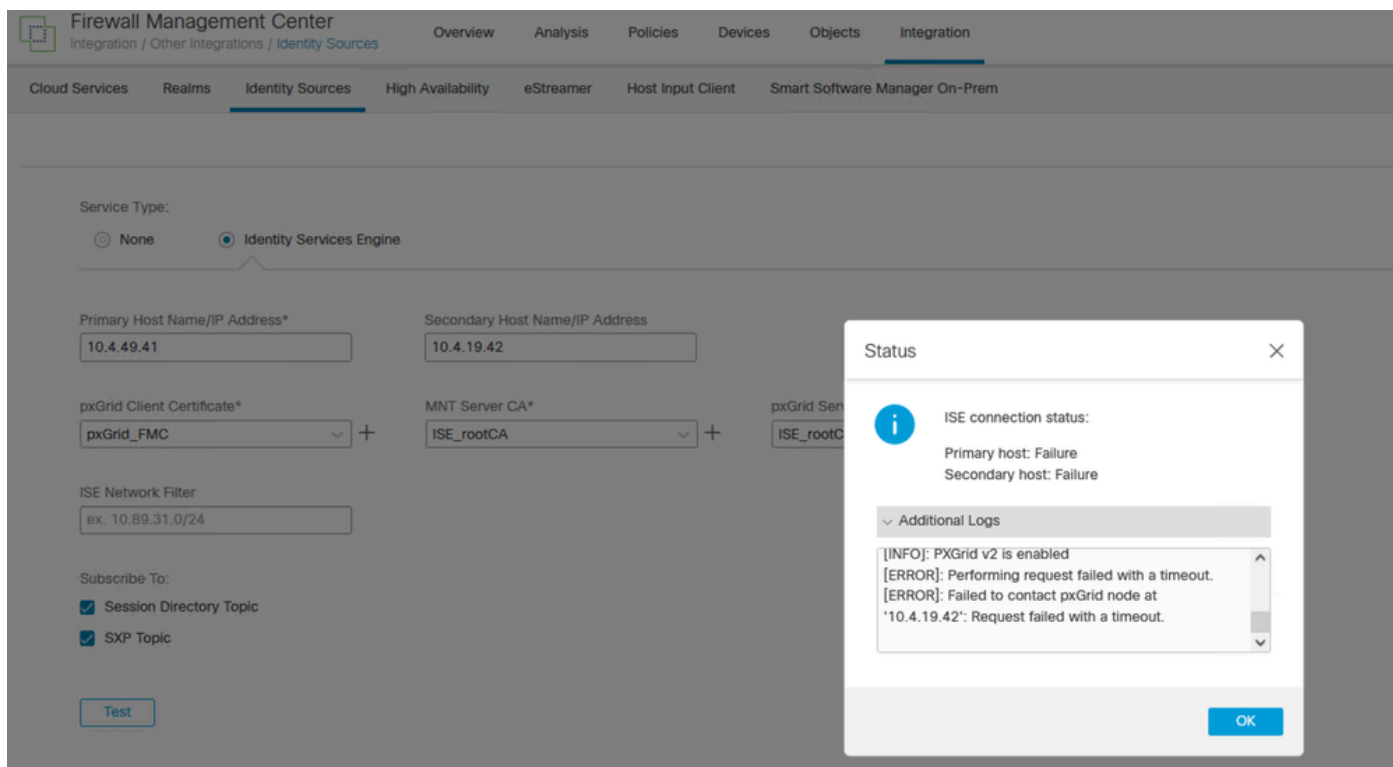


ヒント：さらにログ収集の推奨事項については、ビデオ「[ISE 3.xバージョンでデバッグを有効にする方法](#)」を確認してください。

一般的な問題.

PxGridサブスクライバクライアントがISEで承認されていません。

この使用例では、FMCのtest pxGridボタンに関連する出力が次の動作を示しています。



FMC pxGrid接続に失敗しました。

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
```

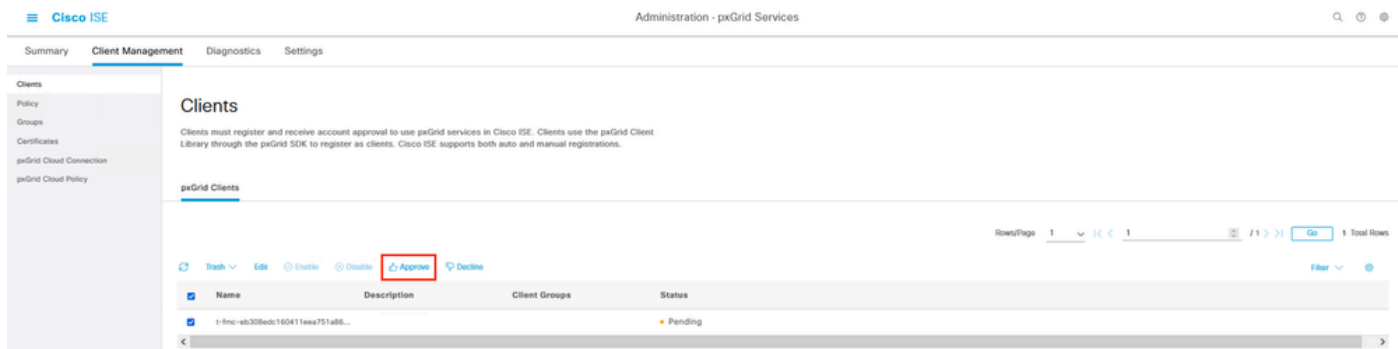
Secondary host:

```
[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.
```

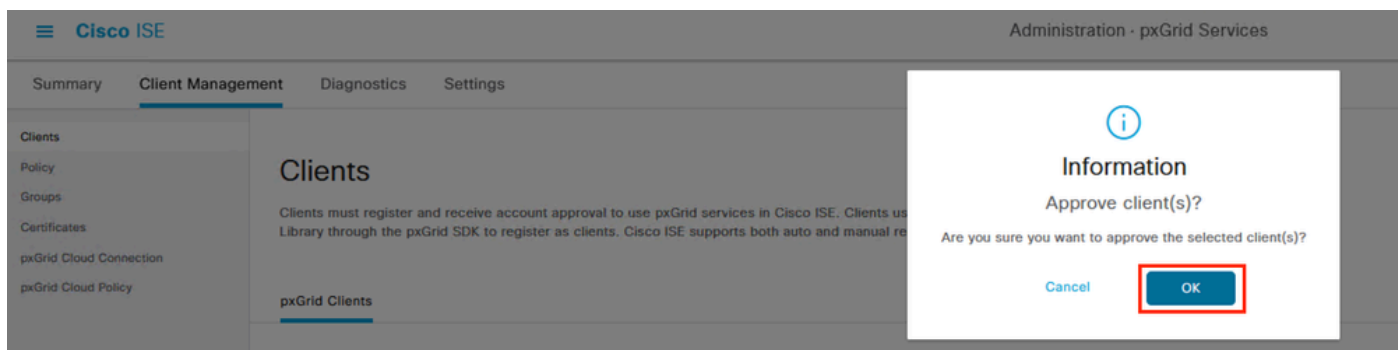
ISEで、Administration > PxGrid Services > Client Management > Clientsの順に選択したメニュー内の動作に注目してください。これは、pxGridクライアント(FMC)が承認を保留していることを示しています。

Approveボタンを選択し、次のウィンドウで選択を確認して、統合を再試行します。

今度は統合が成功します。



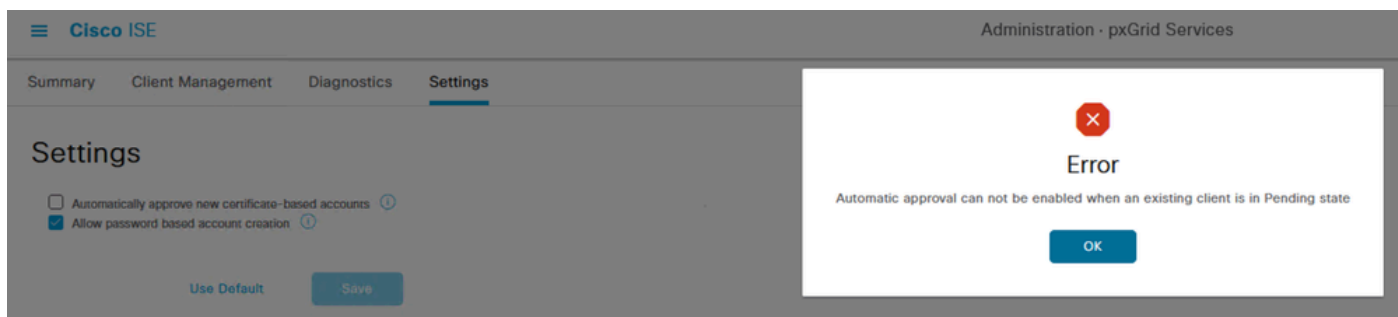
FMCクライアントがpendingステータスになっている。



pxGridクライアントの承認の確認。

証明書ベースのpxGridクライアントの自動承認を有効にする場合に注意してください。

このアラームが表示される可能性があるため、前のページのクライアントを承認/拒否します。



pxGridクライアントの承認に関連するエラーです。

PxGrid ISE証明書 チェーン incomplete.

このシナリオでは、メニューAdministration > System > Certificateに移動した場合、pxgrid証明書を選択し、オプションViewを選択します。

証明書に問題がある場合は、次の関連エラーが発生する可能性があります。

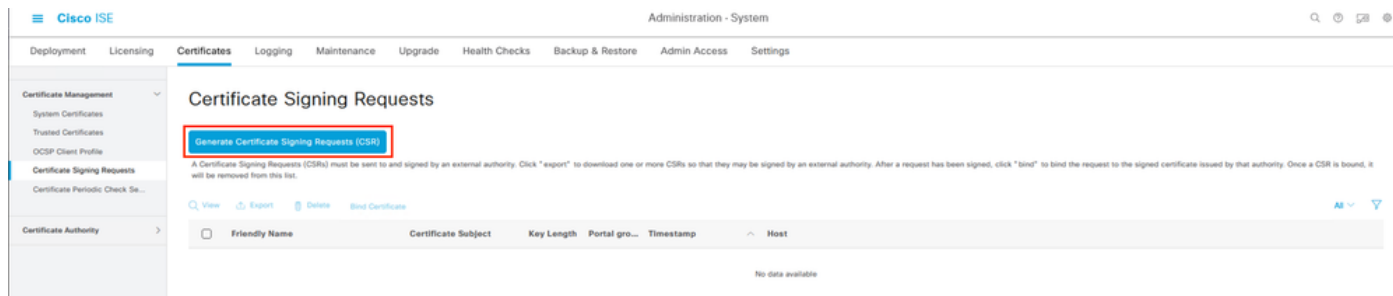
 Certificate trust chain is incomplete

証明書チェーンの未完了に関連するエラーです。

最初に確認するステップは、ISEルートCAが完全であるかどうかを確認することですViewオプションのEd

階層に証明書がない場合は、ISE導入ルートCA全体を発行できます。

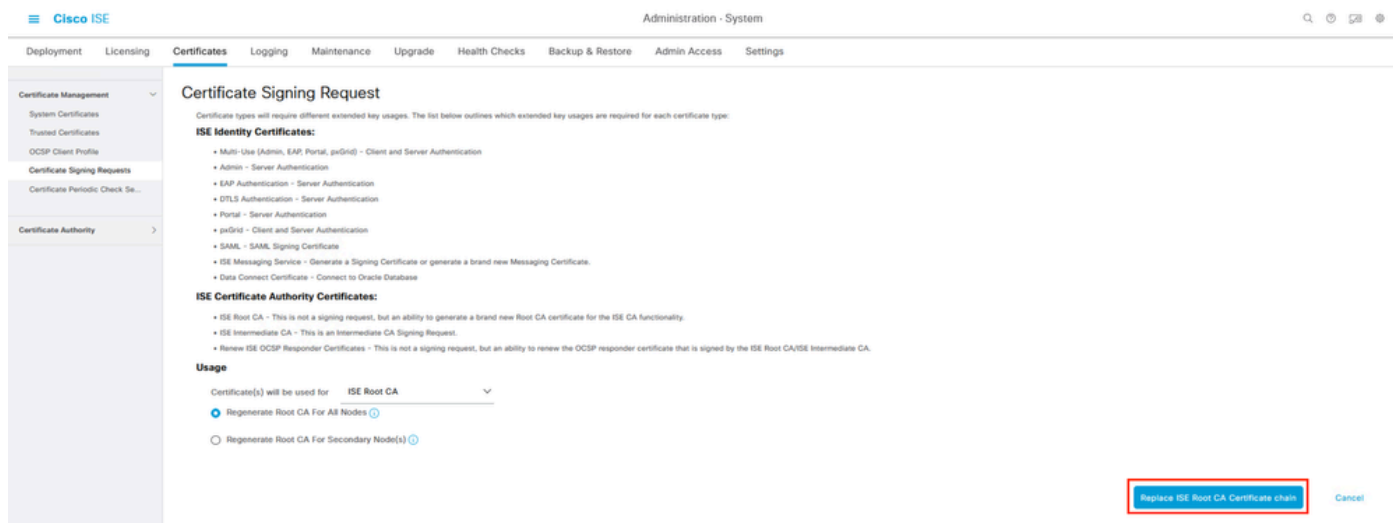
BメニューAdministration > System > Certificates > Certificate Management > Certificate Signing Request (CSR)および そのボタンを選択します。



ISEでのCSRの生成

このメニューで、 使用ISEルートCA すべてのノードのISEルートCAを再生成します。

ボタンを押して進みます ISEルートCA証明書チェーンの交換.



証明書署名要求の設定

証明書がimpのすべてのノードで生成されるまで待ちます説明。

完了すると、ISEは次の通知を表示します.

Cisco ISEAdministration - System

DeploymentLicensingCertificatesLoggingMaintenanceUpgradeHealth ChecksBackup & RestoreAdmin AccessSettings

Certificate ManagementSystem CertificatesTrusted CertificatesOCSP Client ProfileCertificate Signing RequestsCertificate Periodic Check Se...

Certificate AuthorityOverviewIssued CertificatesCertificate Authority Certifica...Internal CA SettingsCertificate TemplatesExternal CA Settings

CA Certificates

Edit+ ImportExportDeleteViewRefresh

	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 upOK

証明書の生成の確認。

pxGrid証明書信頼チェーンが完了しました オプションを選択する [View] 証明書に含まれます。

参照.

[PxGrid Cisco開発者ページ](#)

[Cisco Identity Services Engine管理者ガイド、リリース3.2、章：Cisco pxGrid](#)

[Cisco Identity Services Engineインストールガイド、リリース3.2、章：Cisco ISEポートリファレンス](#)

[Cisco Identity Services Engine CLIリファレンスガイド、リリース2.4](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。