

Configuration et dépannage d'ISE 3.2 avec intégration FMC 7.2.4

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Composants utilisés](#)

[Informations générales.](#)

[Configurer](#)

[Préparez l'ISE pour l'intégration.](#)

[Préparez le FMC pour l'intégration.](#)

[Configuration de la connexion pxGrid entre ISE et FMC.](#)

[Vérifier.](#)

[Validation sur FMC.](#)

[Validation sur ISE.](#)

[Dépannage](#)

[Dépannage sur FMC.](#)

[Dépannage sur ISE.](#)

[Problèmes courants.](#)

[Le client abonné PxGrid n'est pas approuvé sur ISE.](#)

[Chaîne de certificats ISE PxGrid incomplète.](#)

[Référence.](#)

Introduction

Ce document décrit les procédures d'intégration d'Identity Services Engine avec Firewall Management Center à l'aide des connexions Platform Exchange Grid.

Conditions préalables

Cisco recommande des connaissances sur les sujets suivants :

- Moteur du service de vérification des identités (ISE)
- Plateforme Exchange Grid
- Centre de gestion des pare-feu (FMC)
- Certificats TLS/SSL.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Identity Services Engine (ISE) version 3.2 correctif 3
- Firewall Management Center version 7.2.4

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales.

Cette documentation fournit une solution pour intégrer FMC et ISE à l'aide de pxGrid version 2.

Cisco Firepower Management Center (FMC) est une plate-forme centralisée pour les pare-feu de nouvelle génération et les systèmes de prévention des intrusions. Elle permet la gestion des politiques, la détection des menaces et la gestion des incidents.

Cisco Identity Services Engine est une solution complète qui fournit un accès sécurisé aux terminaux en fournissant des services d'authentification, d'autorisation et de responsabilité (AAA) et d'application des politiques.

Platform Exchange Grid (pxGrid) vous permet d'échanger des informations entre des réseaux multifournisseurs et multiplates-formes.

Cette intégration vous permet d'obtenir une surveillance sécurisée, la détection des menaces et l'ensemble des stratégies réseau basées sur les informations partagées.

Le framework PxGrid a 2 versions. La version à utiliser dépend de la version ISE et du correctif que vous devez vérifier.

À partir de la version ISE 3.1, tous les pxGLes connexions rid d'ISE sont basées sur la version de pxgrid 2.

PxGrid version 1.

La première version de ce cadre (pxGrid v1) est caractérisée en raison de la facilité de maintenance qui a été vue à travers la commande show application status ise tel qu'il est affiché dans le résultat suivant.

Lorsque la fonction pxGrid est activée dans le noeud, vous voyez la fonction pxGrid caractéristiques en cours d'exécution.

```
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	

Facilité de maintenance de PxGrid version 1

Dans cette version de cette plate-forme, il est connu d'avoir un seul noeud pxGrid avec les processus pxGrid en état d'exécution alors que les autres noeuds pxGrid sont en état de veille.

Ces noeuds surveillent en permanence l'état du noeud pxGrid avec les services associés en cours d'exécution.

Dans ce cas, le noeud pxGrid principal a bénéficié d'une promotion et l'autre noeud pxGrid a activé ses services pxGrid.

Cependant, cela représentait un temps d'arrêt lorsque ce basculement s'est produit.

La première version de pxgrid était basée sur la communication dans le protocole XMPP (Extensible Messaging and Presence Protocol) qui est un ensemble de technologies utilisées dans les infrastructures de collaboration et de voix.

Les rubriques partagées dans une connexion pxGrid v1 sont les suivantes :

- Répertoire de session
- Métadonnées de profil de terminal
- Métadonnées Trustsec
- Fonctionnalité Endpoint Protection
- Contrôle adaptatif du réseau
- Sujet MDM_Offline
- Identité
- SXP

PxGrid version 2.

Ce document couvre l'utilisation de PxGrid version 2. Cette plate-forme fonctionne en utilisant les

opérations REST sur les protocoles ISE et WebSocket, ce qui apporte des améliorations, une évolutivité, des performances et une flexibilité améliorées dans les modèles de données.

Dans cette version, vous ne voyez pas les fonctionnalités pxgrid s'exécutant comme dans la version précédente avec la commande `show application status ise`.

Reportez-vous à la section relative à la validation d'ISE dans ce document pour connaître les mécanismes à vérifier pour examiner la fonctionnalité pxGrid.

Avec cette version, vous avez tous les noeuds pxGrid que vous configurez en tant que noeuds pxGrid actifs. Ils sont prêts à participer à tout moment à l'échange d'informations.

Dans la version 1, un seul noeud présentait la facilité de maintenance de pxGrid comme étant en cours d'exécution.

Les rubriques partagées dans une connexion pxGrid v2 sont les suivantes :

- Répertoire de session
- Défaillance De Rayon
- Configuration du profileur
- État du système
- MDM
- État ANC
- TrustSec
- Configuration TrustSec
- TrustSec SXP
- Ressource de terminal.

Composants de pxGrid comme plate-forme.

Contrôleur PxGrid (ISE) : Doit faire confiance à chacun des participants qui utilisent pxGrid.

Client : Peut être abonné et éditeur de différents sujets.

Éditeur : Client qui partage des informations avec le contrôleur.

Abonné : Client qui consomme les informations d'une rubrique.

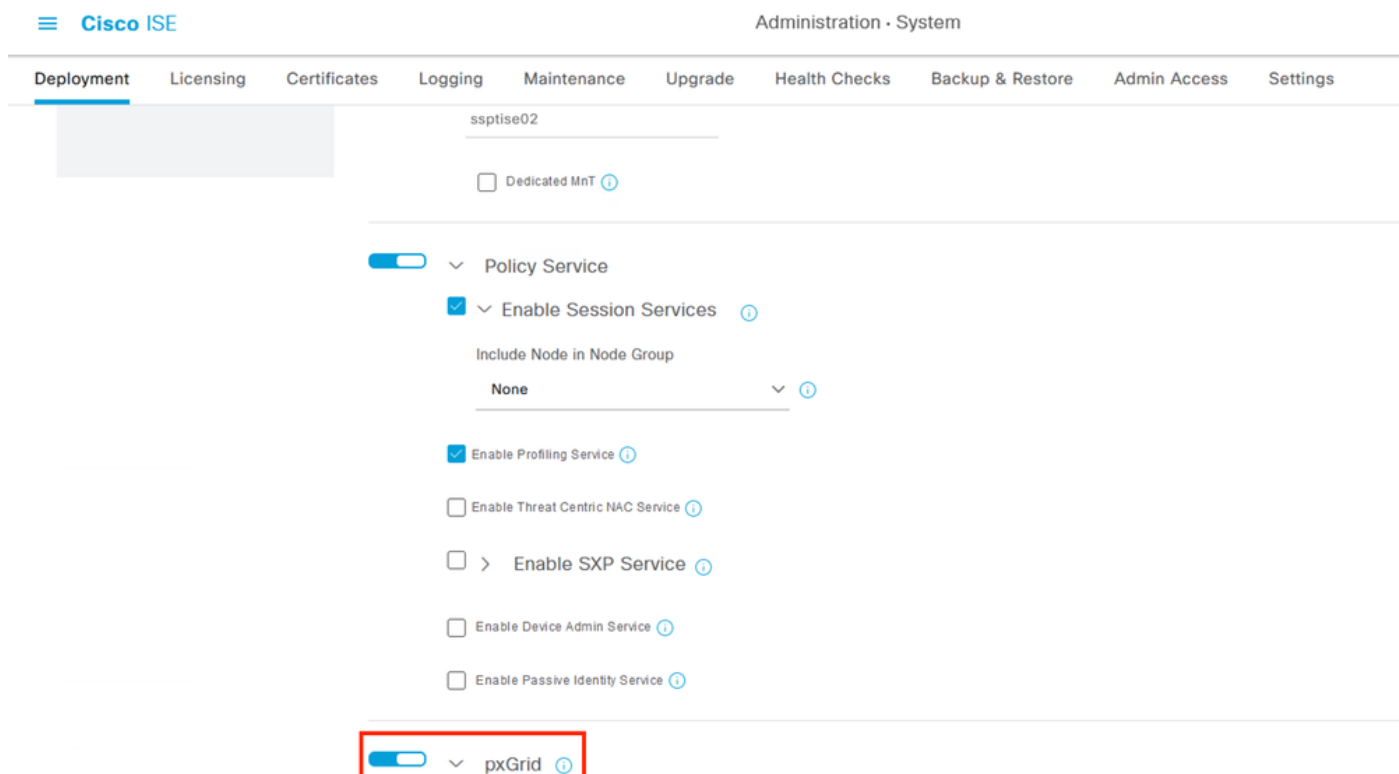
Cette intégration vous permet de créer des stratégies de contenu sur FMC en fonction des informations partagées par ISE et de leurs rubriques publiées (liées à l'activité des terminaux).

Configurer

Préparez l'ISE pour l'intégration.

Étape 1. Configurez le noeud ISE pour exécuter le personnage pxGrid sur celui-ci dans le menu Administration > System > Deployment.

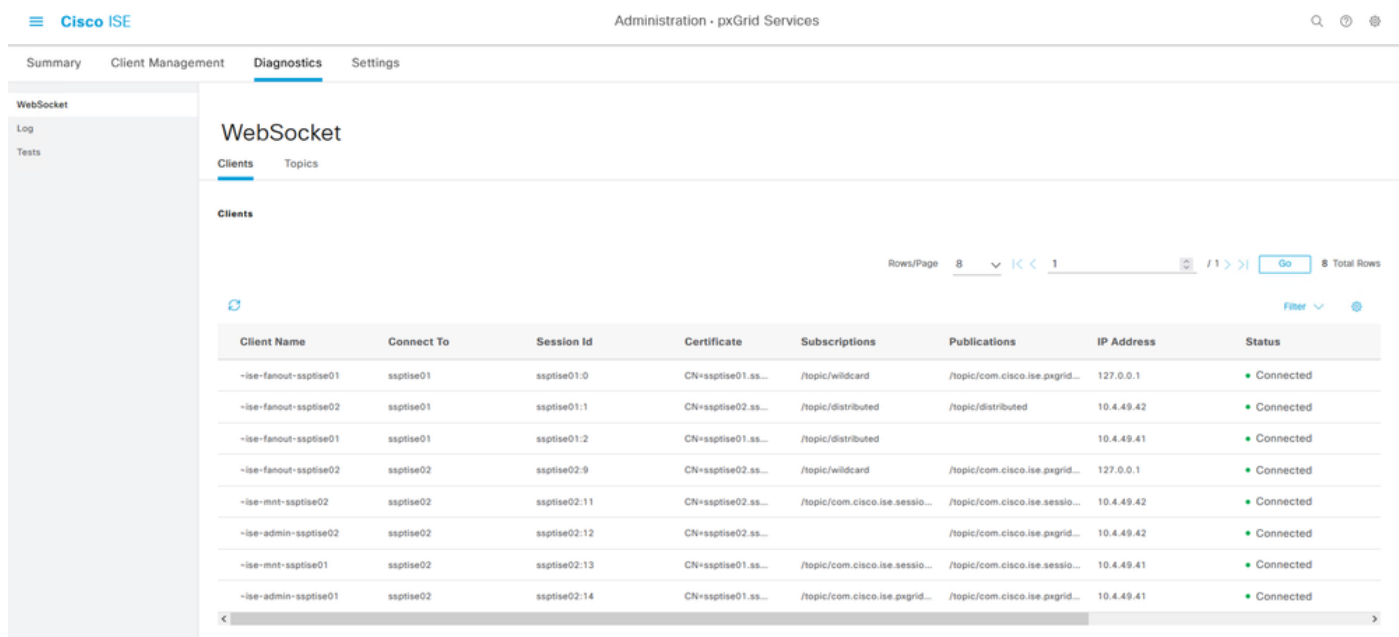
Sélectionnez les noeuds et activez la fonctionnalité pxGrid.



Activation des services ISE pxGrid dans un noeud.

Étape 2. Après avoir activé les noeuds avec la fonctionnalité pxGrid, vérifiez l'état des Websockets associées aux clients internes connectés.

Accédez à Administration > pxGrid Services > Websocket. Notez que les clients pointent vers les services ISE directement via l'adresse IP 127.0.0.1.

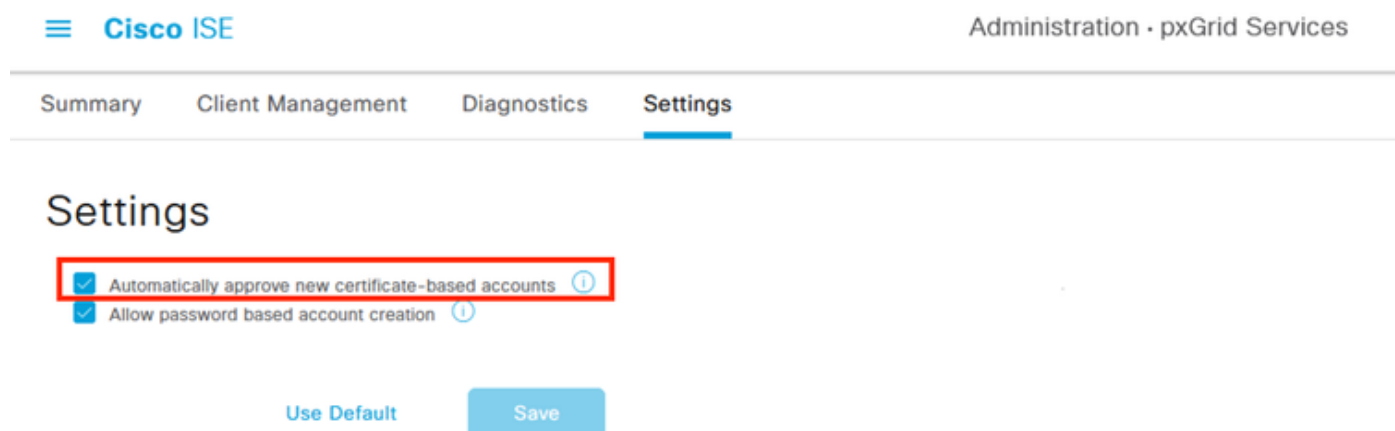


WebSockets internes d'ISE.

Étape 3. Naviguez dans le menu Administration > pxGrid Services > Settings et sélectionnez l'option pour approuver automatiquement les nouveaux comptes basés sur des certificats,

Cette étape est facultative à ce stade, cependant, pour la connexion pxGrid, il est recommandé d'activer cette case à cocher.

Vous pouvez ensuite accepter le FMC en tant qu'abonné manuellement.



Activation de l'approbation automatique pour les comptes basés sur un certificat pxGrid.

Étape 4. Vérifiez les certificats liés à la fonctionnalité pxGrid de votre environnement dans Administration > System > System Certificates,

Il est recommandé que vous ayez des certificats pxGrid homogènes dans tous les noeuds de votre déploiement signés par la même autorité de certification racine

Dans ce scénario, nous utilisons les certificats ISE internes générés. Pour cette version d'ISE, où dans cet exemple, l'autorité de certification racine correspond au noeud PAN.

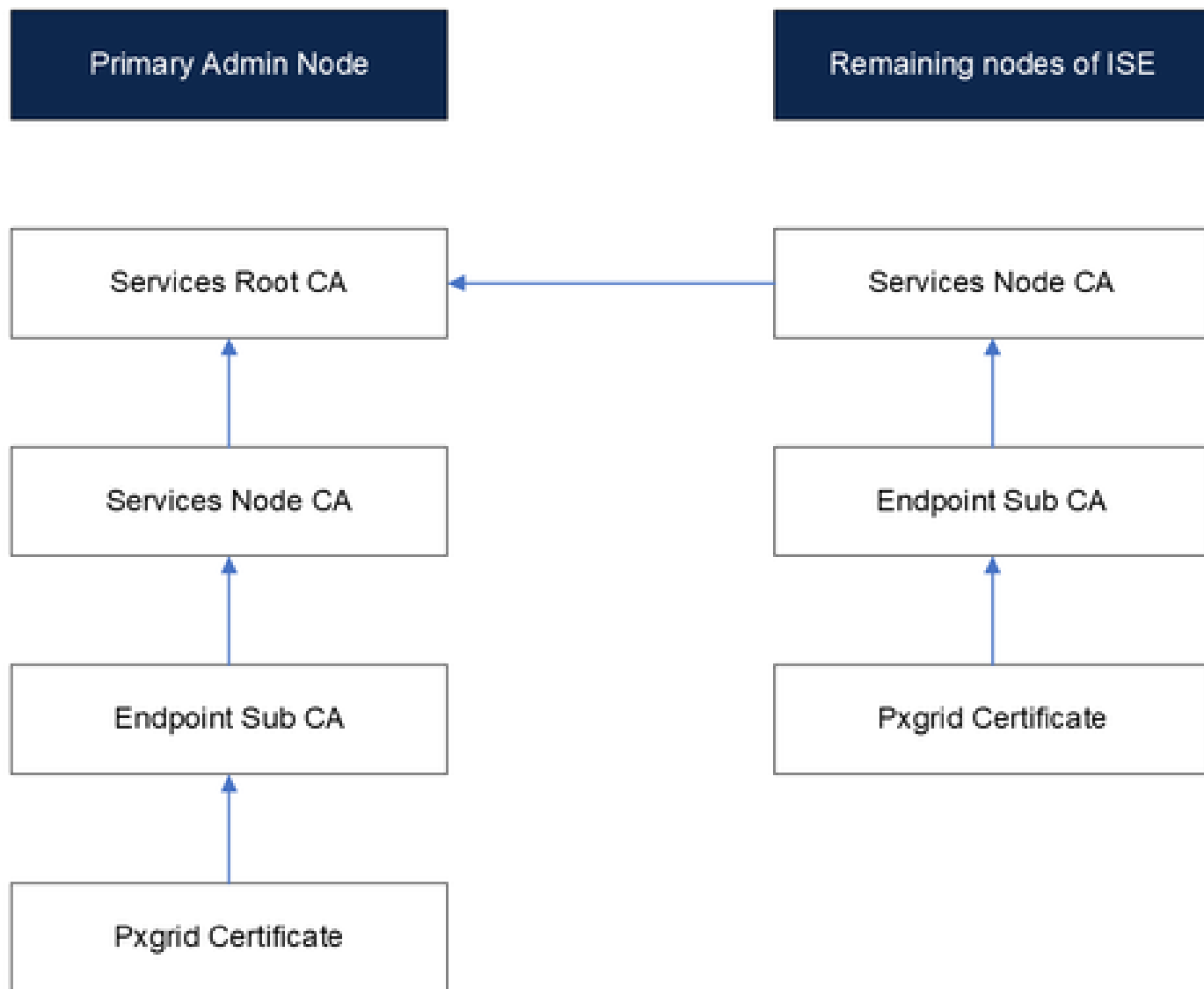


Schéma des certificats internes sur ISE.



Remarque : Pour plus d'informations sur la structure interne des certificats générés sur ISE, veuillez vous reporter à [Comprendre les services d'autorité de certification interne ISE.](#)

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 - ssptseu1000001								
☐ CN=ssptse01.ssptsec.mex, O=U=Certificate Services System Certificate#Certificate Services Endpoint Sub CA - ssptse01#00002	pxGrid		ssptse01.ssptsec.mex	Certificate Services Endpoint Sub CA - ssptse01	Fri, 30 Jun 2023	Sat, 1 Jul 2028	Active	
☐ ise01_External_CA	Admin, EAP Authentication, RADIUS DTLS, Portal	Default Portal Certificate Group ①	ssptse01.ssptsec.mex	ssptsec-CXLABS-WIN2K22D-CA-2	Mon, 3 Jul 2023	Wed, 2 Jul 2025	Active	
ssptse02								
☐ Default self-signed saml server certificate - CN=SAML_ssptse01.ssptsec.mex	SAML		SAML_ssptse01.ssptsec.mex	SAML_ssptse01.ssptsec.mex	Sat, 1 Jul 2023	Thu, 29 Jun 2028	Active	
☐ ise02_External_CA	Admin, EAP Authentication, RADIUS DTLS, Portal	Default Portal Certificate Group ①	ssptse01.ssptsec.mex	ssptsec-CXLABS-WIN2K22D-CA-2	Mon, 3 Jul 2023	Wed, 2 Jul 2025	Active	
☐ CN=ssptse02.ssptsec.mex, O=U=ISE Messaging Service#Certificate Services Endpoint Sub CA - ssptse02#00004	ISE Messaging Service		ssptse02.ssptsec.mex	Certificate Services Endpoint Sub CA - ssptse02	Sat, 1 Jul 2023	Sun, 2 Jul 2028	Active	
☐ CN=ssptse02.ssptsec.mex, O=U=Certificate Services System Certificate#Certificate Services Endpoint Sub CA - ssptse02#00003	pxGrid		ssptse02.ssptsec.mex	Certificate Services Endpoint Sub CA - ssptse02	Sat, 1 Jul 2023	Sun, 2 Jul 2028	Active	

Certificats PxGrid dans un déploiement distribué.

Étape 5. Vérifiez l'état des certificats pxGrid.

Dans le menu précédent, sélectionnez une case à cocher dans un certificat pxGrid de noeud, puis sélectionnez l'option Afficher.

Le résultat ressemble à celui affiché ici dans les certificats pxGrid.

The screenshot displays the Cisco ISE Administration interface. The left sidebar shows the navigation menu with 'Certificate Management' expanded. The main content area is titled 'System Certificates' and lists various certificates. A modal window titled 'Certificate Hierarchy' is open, showing the hierarchy of certificates. The 'Details' section for the 'sspitsec02.sspitsec.mex' certificate is highlighted, showing its status as 'good' and its expiration date as 'Sun, 2 Jul 2028 11:45:44 MDT'.

Certificate Hierarchy

- Certificate Services Root CA - sspitsec01
 - Certificate Services Node CA - sspitsec02
 - Certificate Services Endpoint Sub CA - sspitsec02
 - sspitsec02.sspitsec.mex**

Details

Issued To: sspitsec02.sspitsec.mex

Common Name (CN): sspitsec02.sspitsec.mex

Organization Unit (OU): Certificate Services System Certificate

Organization (O):

City (L):

State (ST):

Country (C):

Certificate status is good

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

Vérification du certificat pxGrid.

Préparez le FMC pour l'intégration.

Étape 1.Vérifiez que l'heure interne FMC est à jour.

Naviguez jusqu'à Système > Configuration > Heure et vérifiez que l'heure configurée sur le FMC est le plus récent.

The screenshot shows the FMC interface with the 'System / Configuration' menu selected. The 'Time Synchronization' page is displayed, showing the current setting as 'Via NTP (based on System Configuration Time Synchronization)'. The current time is 2023-08-26 19:08. A table lists the NTP servers and their status:

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)

Vérification de la mise à jour du FMC.

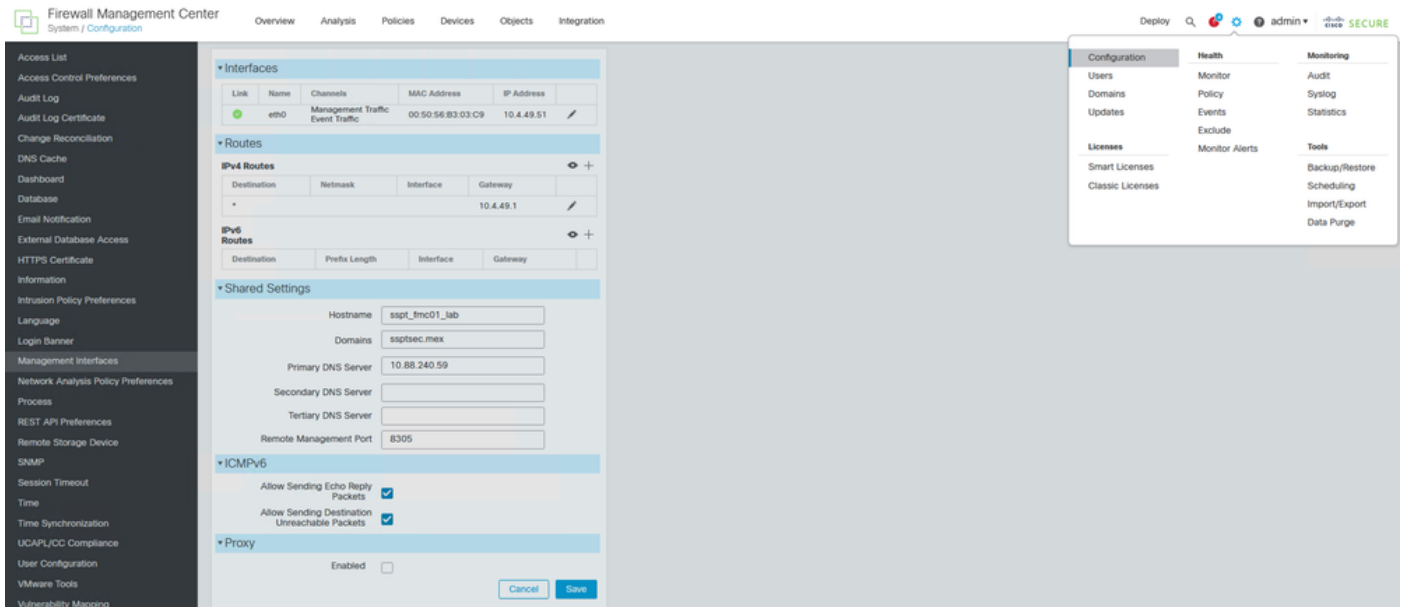
Si l'heure FMC n'est pas mise à jour, assurez-vous que NTP est correctement configuré et en Synchronisation. NTP peut être configuré sous Système > Configuration > Heure > + Ajouter.

The screenshot shows the FMC interface with the 'System / Configuration' menu selected. The 'Time Synchronization' page is displayed, showing the 'Serve Time via NTP' dropdown set to 'Enabled'. The 'Set My Clock' section shows 'Manually in Local Configuration' selected. Below, there is a table of NTP servers:

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

Synchronisation temporelle sur FMC.

Étape 2. Naviguez jusqu'à Système > Configuration > Interface de gestion > Paramètres partagés et vérifiez qu'au moins Serveur DNS principal champ contient une valide IP du serveur DNS.



Configuration DNS sur FMC.

Étape 3 : vérifiez que le nom d'hôte FMC est configuré.

Naviguez jusqu'à Système > Configuration > Interface de gestion > Paramètres partagés et vérifiez que Nom de l'hôte contient le nom d'hôte FMC.

Vous pouvez vérifier cette étape lors de la révision de l'étape précédente de cette section .

Configuration de la connexion pxGrid entre ISE et FMC.

Étape 1. Accédez au menu Administration > pxGrid Services > Client Management > Certificates.

Dans la première option, sélectionnez Je veux générer un certificat unique (sans demande de signature de certificat).

Dans la section Common Name (CN), entrez le FQDN du FMC indiquant que l'ISE doit émettre un certificat.

Fournissez une description.

Dans la section de Subject Alternative Name (SAN), saisissez le nom de domaine complet et l'adresse IP du FMC à connecter.

Au bas de la page Certificate Download Format, sélectionnez l'option Certificate in Privacy Enhanced Electronic Mail (PEM) format dans le menu déroulant.

Entrez le format PEM PKCSS (y compris la chaîne de certificats).

Entrez et stockez un mot de passe dans Certificate Password lorsque vous utiliserez ce mot de passe ultérieurement dans FMC.

Confirmez le mot de passe, puis sélectionnez Créer.

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...v

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...v ⓘ

Certificate Password*
***** ⓘ

Confirm Password*

Reset Create

Exemple de génération de certificat pxGrid.

Étape 2. Un fichier zip est téléchargé sur votre ordinateur. Décompressez le fichier et vérifiez que vous disposez des fichiers suivants dans votre environnement :

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

Certificats PxGrid générés par ISE.

Étape 3. Dans FMC, accédez au menu Objets > Gestion des objets > PKI > Certs internes.

Sélectionnez l'option Ajouter un certificat interne.

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-PIX connection and captive portal configuration.

Name	Value
No records to display	

PKI

- Cert Enrollment
- External Cert Groups
- External Certs
- Internal CA Groups
- Internal CAs
- Internal Cert Groups
- Internal Certs
- Trusted CA Groups
- Trusted CAs

Ajout du certificat FMC comme certificat interne.

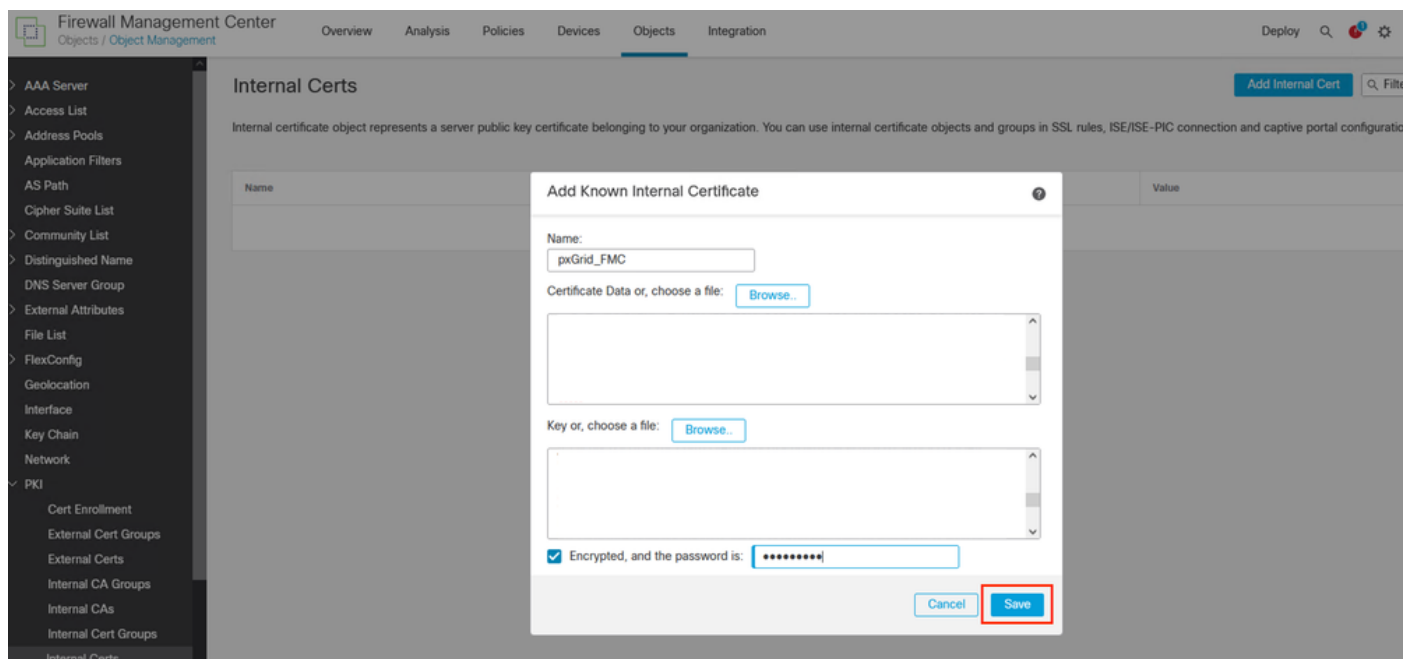
Étape 4. Attribuez un nom au certificat alloué sur FMC.

Parcourez le certificat que vous avez créé pour le FMC à partir d'ISE dans la section Certificate Data.

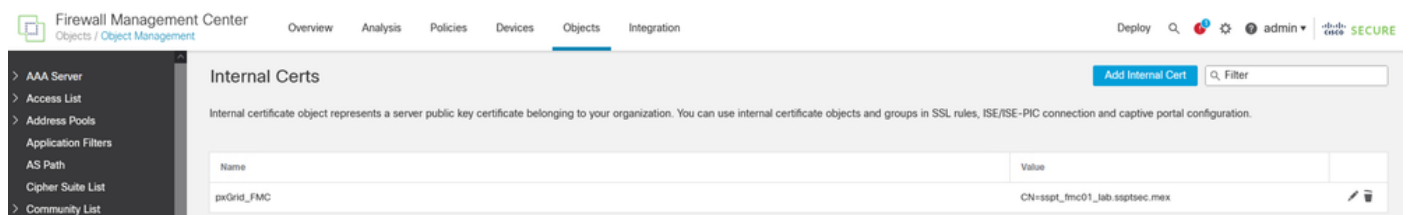
Parcourez le fichier avec l'extension .key pour remplir le champ suivant.

Sélectionnez l'option Encrypted, et entrez le mot de passe que vous avez utilisé lorsque vous avez créé le certificat sur ISE.

Enregistrez la configuration.



Exportation du certificat FMC généré par ISE.



Certificat FMC.

Étape 5. Accédez au menu Objets > Gestion des objets > ICP > Autorités de certification approuvées,

Sélectionnez Ajouter des autorités de certification approuvées.

Trusted CAs

Trusted certificate authority (CA) object represents a CA public key certificate belonging to a trusted CA. You can use external CA objects in SSL policy, realm configurations and ISE/ISE-PIC connection.

Name	Value	
AAA-Certificate-Services	CN=AAA Certificate Services, ORG=Comodo CA Limited, C=GB	
ACCVRAZ1	CN=ACCVRAZ1, ORG=ACCV, OU=PKIAACCV, C=ES	
Actalis-Authentication-Root-CA	CN=Actalis Authentication Root CA, ORG=Actalis S.p.A./03358520967, C=IT	
AffirmTrust-Commercial	CN=AffirmTrust Commercial, ORG=AffirmTrust, C=US	
AffirmTrust-Networking	CN=AffirmTrust Networking, ORG=AffirmTrust, C=US	
AffirmTrust-Premium	CN=AffirmTrust Premium, ORG=AffirmTrust, C=US	
AffirmTrust-Premium-ECC	CN=AffirmTrust Premium ECC, ORG=AffirmTrust, C=US	
Amazon-Root-CA-1	CN=Amazon Root CA 1, ORG=Amazon, C=US	
Amazon-Root-CA-2	CN=Amazon Root CA 2, ORG=Amazon, C=US	
Amazon-Root-CA-3	CN=Amazon Root CA 3, ORG=Amazon, C=US	
Amazon-Root-CA-4	CN=Amazon Root CA 4, ORG=Amazon, C=US	
Atos-TrustedRoot-2011	CN=Atos TrustedRoot 2011, ORG=Atos, C=DE	
Autoridad-de-Certificacion-Firmaprofesional-CIF-A62634068	CN=Autoridad de Certificacion Firmaprofesional CIF A62634068, C=ES	
Baltimore-CyberTrust-Root	CN=Baltimore CyberTrust Root, ORG=Baltimore, OU=CyberTrust, C=IE	
Buypass-Class-2-Root-CA	CN=Buypass Class 2 Root CA, ORG=Buypass AS-983163327, C=NO	

Ajout de l'ISE rootCA en tant que certificat sécurisé.

Étape 6. Nommez l'autorité de certification.

Recherchez et sélectionnez l'autorité de certification racine ISE téléchargée à partir du fichier ISE.

Enregistrez votre configuration.

Import Trusted Certificate Authority

Name: ISE_rootCA

Certificate Data or, choose a file: [Browse...](#)

-----BEGIN CERTIFICATE-----
 [Certificate Data]
 -----END CERTIFICATE-----

☐ Encrypted, and the password is: [Password Field]

[Cancel](#) [Save](#)

Exportation de l'autorité de certification racine ISE.

Étape 7. Accédez au menu Integration > Other Integrations > Identity Sources.

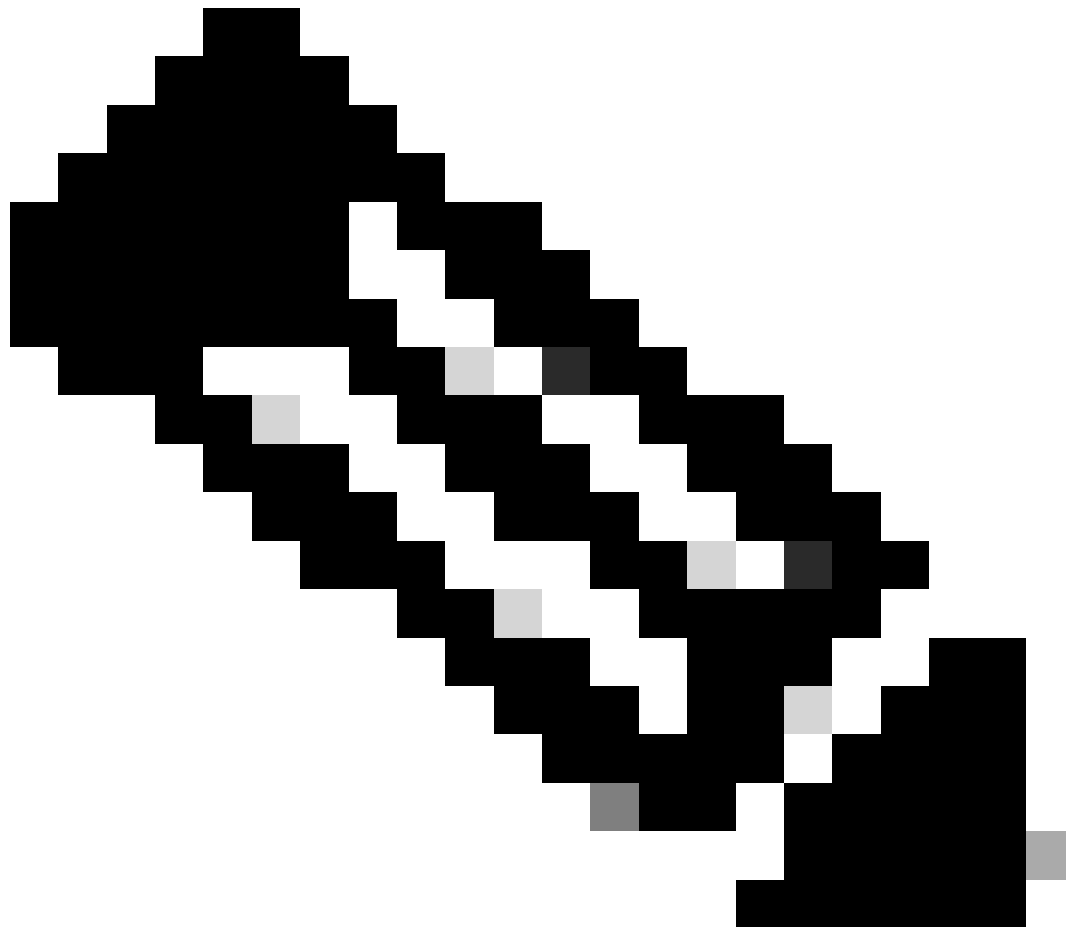
Sélectionner dans le type de service : Identity Services Engine,

Saisissez l'adresse IP ou le nom de domaine complet du noeud pxGrid qui devient le noeud principal.

Répétez la procédure pour le noeud Secondary pxGrid.

Sélectionnez dans le menu déroulant le certificat pxGrid généré par ISE pour la section certificat client pxGrid,

Dans la section MNT Server CA et pxGrid Server CA, sélectionnez l'autorité de certification racine ISE que vous avez exportée à la dernière étape.



Remarque : L'autorité de certification du serveur pxGrid correspond à l'autorité de certification racine du certificat utilisé par pxGrid sur les noeuds pxGrid.

L'autorité de certification du serveur MNT correspond à l'autorité de certification du certificat utilisé par pxGrid sur les noeuds MNT.

(Facultatif) Vous pouvez vous abonner au répertoire de session et à la rubrique SXP à partir d'ISE.

Enregistrez la configuration.

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

Configuration d'ISE comme source d'identité dans FMC.

Vérifier.

Validation sur FMC.

Dans le menu, naviguez vers Integration > Other Integrations > Identity Sources > Identity Services Engine, avant d'enregistrer votre configuration. Vous pouvez tester les paramètres du lien pxGrid.

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

Communication PxGrid réussie.

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.

Validation sur ISE.

Lorsque le client FMC pxGrid a été correctement intégré sur ISE, vous pouvez voir (dans le Administration > pxGrid Services > Gestion des clients > menu Clients) les clients portant le nom fmc sont inclus et activés.

Cisco ISE

Administration - pxGrid Services

SummaryClient ManagementDiagnosticsSettings

Clients

Policy

Groups

Certificates

pxGrid Cloud Connection

pxGrid Cloud Policy

Clients

Clients must register and receive account approval to use pxGrid services in Cisco ISE. Clients use the pxGrid Client Library through the pxGrid SDK to register as clients. Cisco ISE supports both auto and manual registrations.

pxGrid Clients

Rows/Page4<<1>>

Trash

Edit

Enable

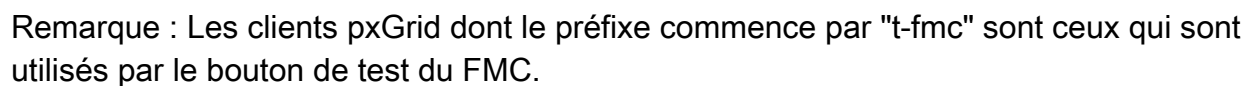
Disable

Approve

Decline

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

Clients PxGrid disponibles et activés.



Dans le scénario dans lequel vous avez le FMC dans Haute disponibilité, vous voyez ensuite les unités principale et secondaire telles qu'elles sont affichées dans cet exemple :

WebSockets disponible sur ISE.

Dans l'onglet suivant de ce menu dénommé Toptique, vous pouvez vérifiez que les abonnés FMC ont été ajoutés aux rubriques pxGrid publiées par ISE.

Par exemple, il y a la rubrique relative au groupe de sécurité de where vous Vous pouvez voir que FMC sont souscrits et reçoivent des informations relatives par SGT publié par ISE.

Administration - pxGrid Services

Summary Client Management **Diagnostics** Settings

WebSocket

Log Tests

Topics

Rows/Page 10 << 1 1 >> Go 10 Total Rows

Name	Publisher Count	Subscriber Count
/topic/wildcard	0	2
/topic/cisco-ise-config-trustsec-security-group	0	2

Rows/Page 10 << 1 1 >> Go 2 Total Rows

Client Name	Messaging Role
fmc-6c85c3d160511eeb4b1395...	Sub
fmc-6c85c3d160511eeb4b1395...	Sub

Rubriques par abonné pxGrid.

IDans le menu Administration > pxGrid Services > Diagnostics > Log, événements importants associés à dans la communication pxGrid (pour les noeuds avec la fonctionnalité activée activée) s'affichent.

Elles présentent les informations relatives à l'intégration.

Administration - pxGrid Services

Summary Client Management **Diagnostics** Settings

WebSocket

Log Tests

Live Log

Rows/Page 25 << 1 1 >> Go 131 Total Rows

Timestamp	Client	Server	Host	Event Type	Description
2023-08-21 06:31 -05:00	fmc-6c85c3d160511eeb4b1395...	ws://10.4.49.41/pxgrid/ise/pubsub	sxptise01	PUBLISH_SERVER_SUBSCRIBE	Pubsub subscribe, subscription=[d=880ba640-97d8-4c17-81c1-d591e0ca...
2023-08-21 06:31 -05:00	fmc-6c85c3d160511eeb4b1395...	ws://10.4.49.41/pxgrid/ise/pubsub	sxptise01	PUBLISH_SERVER_SUBSCRIBE	Pubsub subscribe, subscription=[d=6523e2d0-91e6-4199-be54-ed186e09...
2023-08-21 06:31 -05:00	fmc-6c85c3d160511eeb4b1395...	ws://10.4.49.41/pxgrid/ise/pubsub	sxptise01	PUBLISH_SERVER_SUBSCRIBE	Pubsub subscribe, subscription=[d=30b0cd50-9c75-4c3a-9b19-203fed12...
2023-08-21 06:31 -05:00	fmc-6c85c3d160511eeb4b1395...	ws://10.4.49.41/pxgrid/ise/pubsub	sxptise01	PUBLISH_SERVER_SUBSCRIBE	Pubsub subscribe, subscription=[d=a3d9508e-3001-475d-b6fb-3a25aaf49...
2023-08-21 06:31 -05:00	fmc-6c85c3d160511eeb4b1395...	ws://10.4.49.41/pxgrid/ise/pubsub	sxptise01	WS_SERVER_CONNECTED	WebSocket connected, session=[d=6,client=fmc-6c85c3d160511eeb4b1...

Journaux en direct PxGrid.

Dépannage

Dépannage sur FMC.

Vérifiez que FMC est en mesure de résoudre son propre nom d'hôte et les noeuds ISE par noms d'hôte.

Exemple :

<#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

Vérifiez les points suivants Le processus ADI est en cours d'exécution :

<#root>

>

expert

sudo suadmin@sspt_fmc01_lab:~\$

sudo su

root@sspt_fmc01_lab:/Volume/home/admin#

pmtool status | grep adi

adi (normal) - Running 7911

EAssurez-vous que la communication entre FMC et ISE le pauvreLe TCP 8910 est autorisé. De FMC CLI nous pouvons configurer a tcpdump capture de paquets pour confirmer la communication bidirectionnelle.

<#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

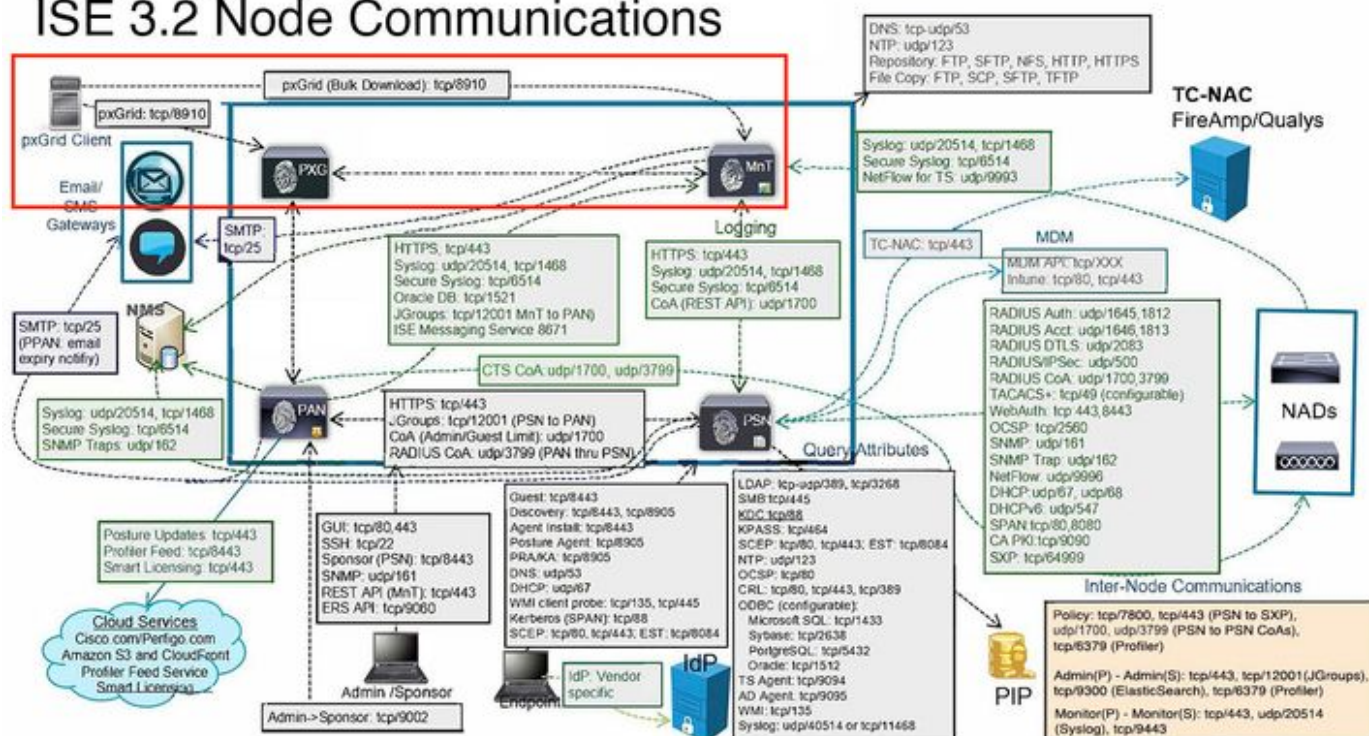
: Flags [.], ack 1, win 229, options [nop,nop,TS val 2701166400 ecr 2268665064], length 0
[...]

Dépannage sur ISE.

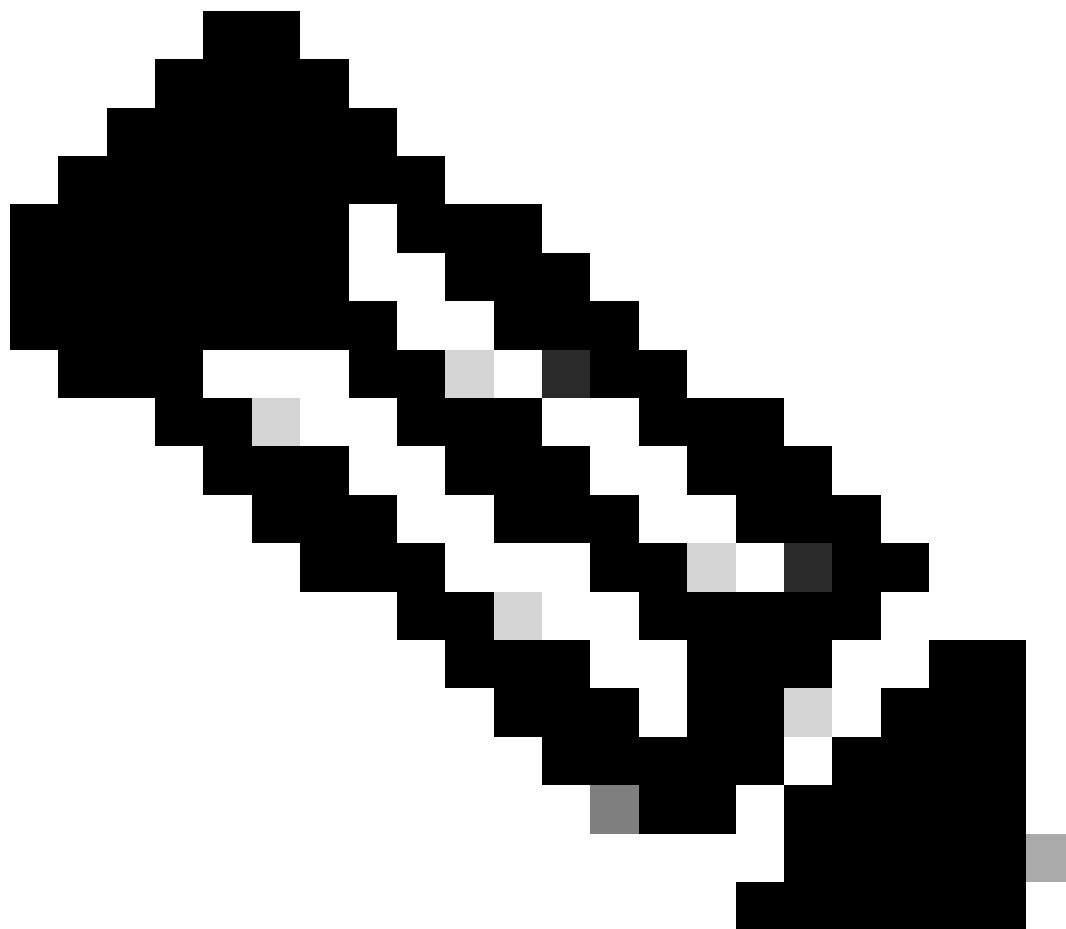
Vérifiez que les communications sur le port 8910 est opérationnel.

Il s'agit du port utilisé par le client pxGridpour communiquer avec les noeuds pxGrid et les noeuds MnT pour le téléchargement en masse des informations.

ISE 3.2 Node Communications



Interaction PxGrid dans un environnement ISE.



Remarque : Le client pxGrid, dans ce cas le FMC communique aux noeuds pxGrid et au noeud MNT secondaire (SMNT) pour obtenir (Téléchargement en masse) les informations, en cas de défaillance dans le SMNT, il recherche les informations par le MNT principal.

Idans les noeuds ISE où se trouve la communication avec le client pxGrid, vous pouvez consulter si la le port est ouvert ou si des sockets sont connectés à ce port.

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

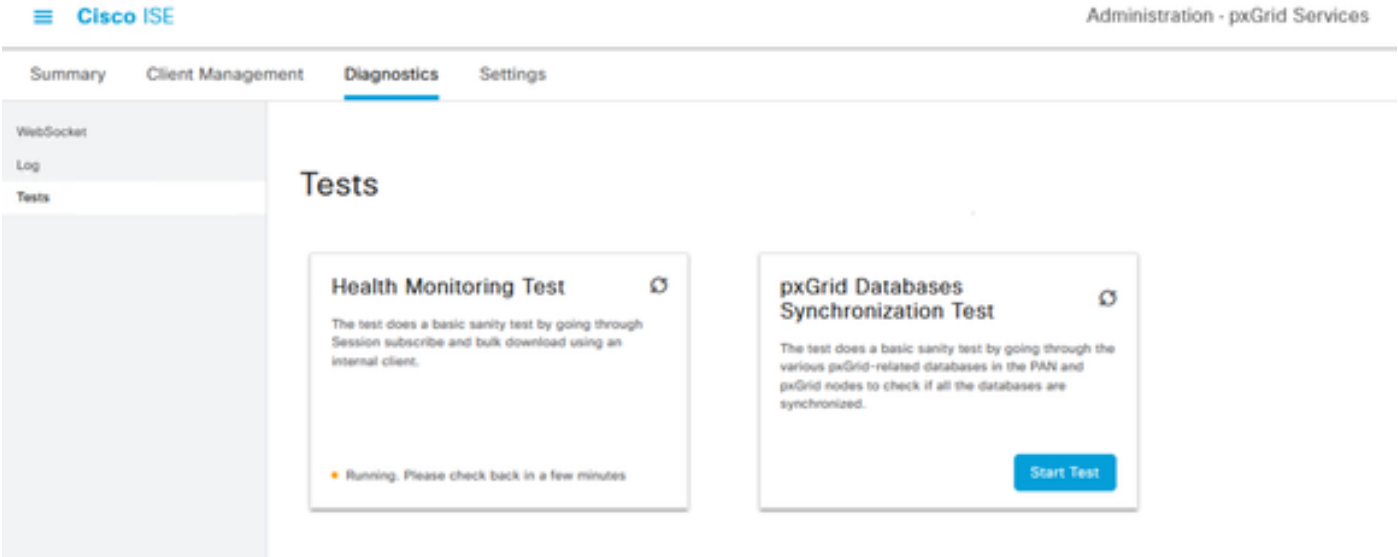
Deux tests sont disponibles sur ISE pour diagnostiquer l'état global des implémentations pxGrid.

Celles-ci se trouvent dans le menu Administration > pxGrid Services > Diagnostics > Test.

Les tests affichés dans cette section sont effectués en interne sur ISE.

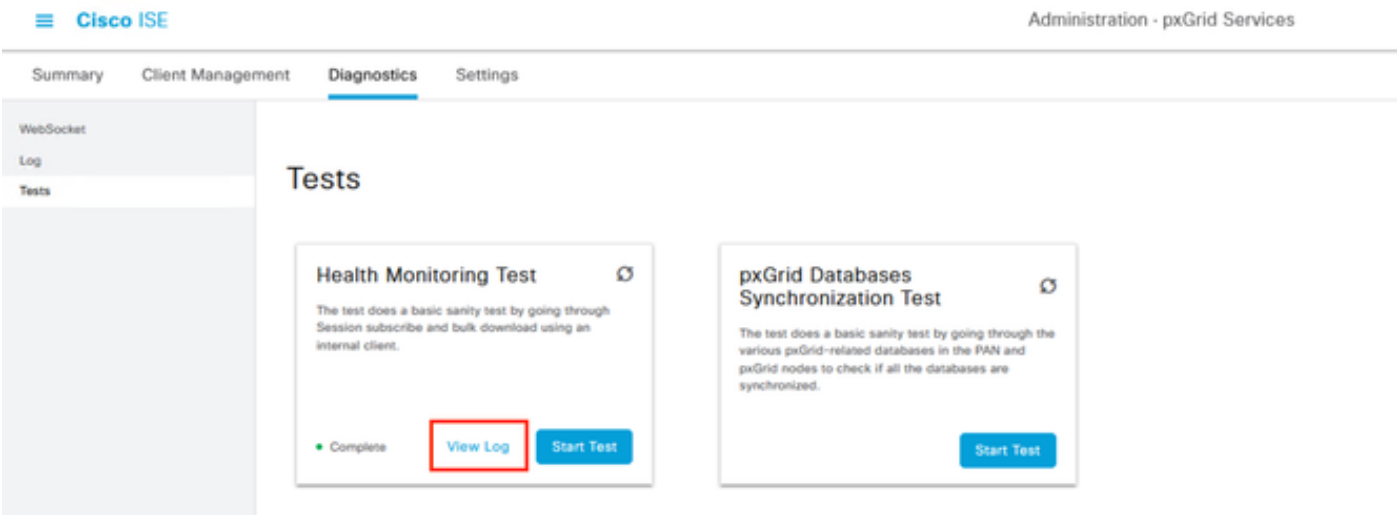
Test de contrôle de santé examine l'aspect du service pxGridascendant, qui évalue si un client peut accéder au répertoire de session, au service et aux rubriques publiés par le contrôleur pxGrid.

Sélectionnez le option Début Essai et attendez que les journaux soient collectés.



Test de contrôle d'intégrité PxGrid.

Une fois le test terminé, sélectionnez le option Afficher le journal. Pour cet exemple, le contenu du journal est:



Examen du test de contrôle d'intégrité.

```
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
```

```

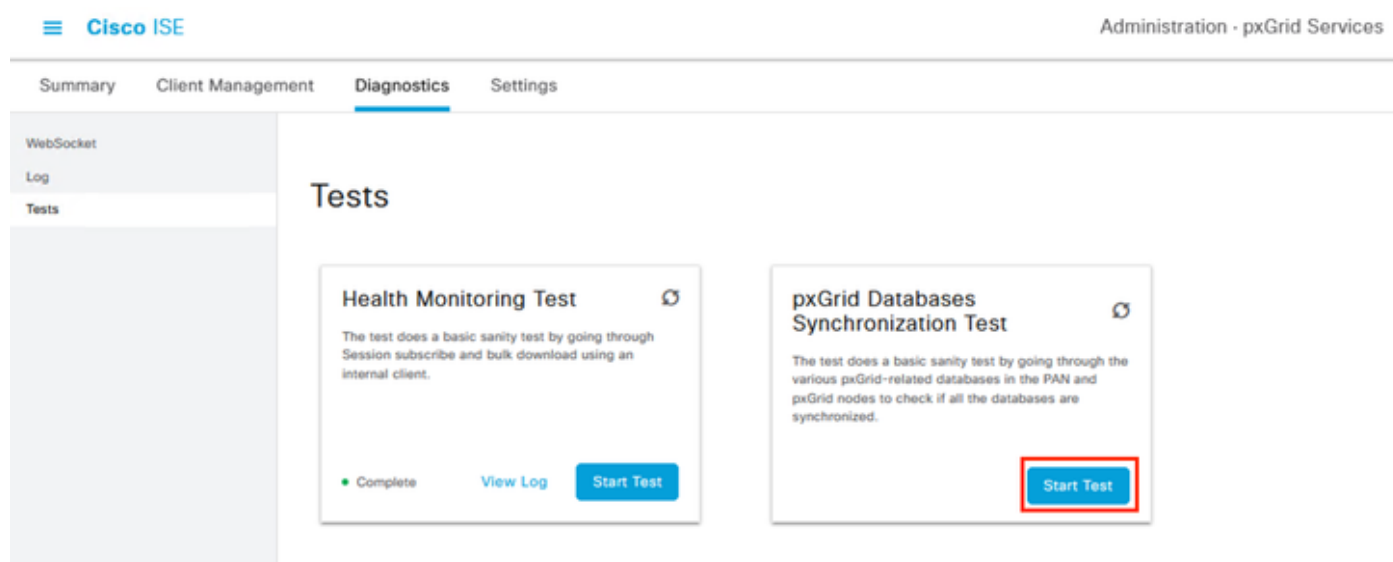
22-Aug-2023 17:03:15 [INFO] ----- Connection Test Completed -----
22-Aug-2023 17:03:15 [INFO] ----- Starting Download Test -----
22-Aug-2023 17:03:15 [INFO] Downloading sessions since 2023-08-21T17:03:15.273-06:00
22-Aug-2023 17:03:15 [INFO] Response status=200
22-Aug-2023 17:03:15 [INFO] Number of sessions 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 *****

```

Test de synchronisation de base de données PxGrid vérifie si les informations dans les bases de données est correct entre les noeuds PAN et pxGrid et synchronisé.

Par conséquent, les informations envoyées aux abonnés pxGrid précis.

Sélectionnez le option Démarrer le test et attendre que les résultats viennent à être évalués.



Test de synchronisation des bases de données PxGrid.

Ce résultat a été obtenu à partir des journaux générés.

```

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

```

```

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

```

Collecter une capture sur à partir des noeuds pxGrid pointant vers le noeud FMC principal.

Accédez au menu Opérations > Dépannage > Outils de diagnostic > Dépôt TCP,

Sélectionnez le option par Add une nouvelle capture.

The screenshot shows the Cisco ISE interface with the 'Operations - Troubleshoot' header. The left sidebar contains 'Diagnostic Tools', 'Download Logs', and 'Debug Wizard'. Under 'Diagnostic Tools', 'General Tools' is expanded, showing 'TCP Dump' as the selected option. The main area is titled 'TCP Dump' and contains a table with columns: Host Name, Network Interface, Filter, File Name, Repository, File Size, Number of Files, Time Limit, Promiscuous Mode, and Status. The 'Add' button is highlighted with a red box.

Génération d'une capture de paquets sur ISE.

Configurez les paramètres de la capture.

Dans Nom de l'hôte , sélectionnez le noeud pxGrid principal sélectionné dans le FMC.

Filtre le trafic avec cette syntaxe ip host <IP FMC>

Nommer la capture et ensuite procéder par Enregistrer et Exécuter.

The screenshot shows the Cisco ISE interface with the 'Operations - Troubleshoot' header. The left sidebar contains 'Diagnostic Tools', 'Download Logs', and 'Debug Wizard'. Under 'Diagnostic Tools', 'General Tools' is expanded, showing 'TCP Dump' as the selected option. The main area is titled 'Edit TCP Dump' and contains a form with the following fields: Host Name (ssptise01), Network Interface (GigabitEthernet 0 [Up, Running]), Filter (ip host 10.4.49.51), File Name (taccap), Repository (None), File Size (10 Mb), Limit to (1 File(s)), Time Limit (5 Minute(s)), and Promiscuous Mode (unchecked). The 'Save and Run' button is highlighted with a red box.

Exemple de configuration de capture de paquets.

Dans une autre fenêtre, dans le menu FMC Intégration > Autres intégrations > Identité Sources, Testez la connexion avec l'ISE via le canal pxGrid.

WLorsque vous obtenez le résultat du test, procéder par Speigné la capture sur ISE.

Cisco ISE

Operations - Troubleshoot

Diagnostics Tools

Download Logs

Debug Wizard

General Tools

RADIUS Authentication Troub...

Execute Network Device Com...

Evaluate Configuration Validat...

Posture Troubleshooting

Agentless Posture Troublesho...

EndPoint Debug

TCP Dump

Session Trace Tests

TrustSec Tools

TCP Dump

The TCP Dump utility page is to monitor the contents of packets on a network interface and troubleshoot problems on the network as they appear

Rows/Page 1 1 1 Go 1 Total Rows

Add

Edit

Trash

Start

Stop

Download

Host Name

Network Interface

Filter

File Name

Repository

File S...

Number of ...

Time Limit

Promiscuous M...

Status

ssptise01.sptsec.mex

GigabitEthernet 0 [Up, Run...

ip host 10.4.49.51

taccap

10

1

5

false

RUNNING

Arrêt d'une capture de paquets sur ISE.

Télécharger la capture et démarrez l'analyse. Ce scénario affiche une capture d'une connexion opérationnelle qui peut servir de référence.

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
10.4.49.41	10.4.49.51	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

Communication PxGrid entre ISE et FMC.

En outre, sur ISE, vous pouvez collecter des débogages liés à pxTraitement de grille.

Naviguer dans le menu Opérations > Dépannage > Assistant de débogage > Débogage Configuration du journal,

Sélectionnez le noeud ISE correspondant à analyser, puis Modifier.

Cisco ISE

Operations - Troubleshoot

Diagnostics Tools

Download Logs

Debug Wizard

Debug Profile Configuration

Debug Log Configuration

Node List

Edit

Reset to Default

Node Name

Replication Role

ssptise01

PRIMARY

ssptise02

SECONDARY

Sélection d'un noeud à déboguer sur ISE.

Filtrez les composants affichés et modifiez la Niveau de journalisation sur DEBUG the pxgrid composante par procéder avec une analyse.

Enregistrer la configuration.

Cisco ISE

Operations - Troubleshoot

Diagnostic ToolsDownload LogsDebug Wizard

Debug Profile Configuration

Debug Log Configuration

Node List > ssptise01.ssptsec.mex

Debug Level Configuration

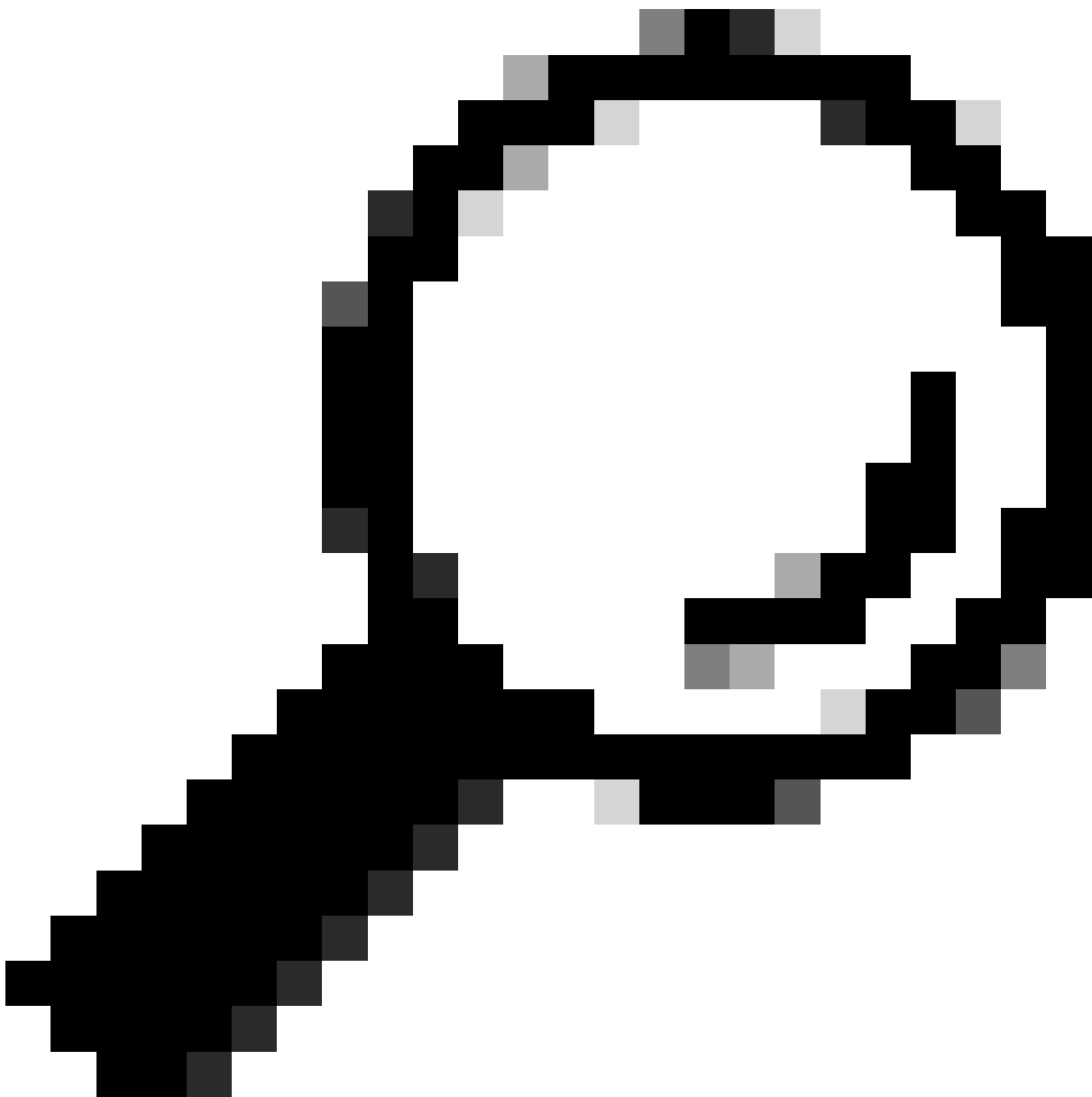
EditReset to Default

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

Modification du composant pxGrid au niveau de débogage.

Reproduisez le comportement à analyser, puis procéder pour analyser les journaux collectés dans le fichier pxgrid-server.log. Autres journaux que vous pouvez examiner sur le noeud ISE pour le dépannage sont les suivants :

```
#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
```

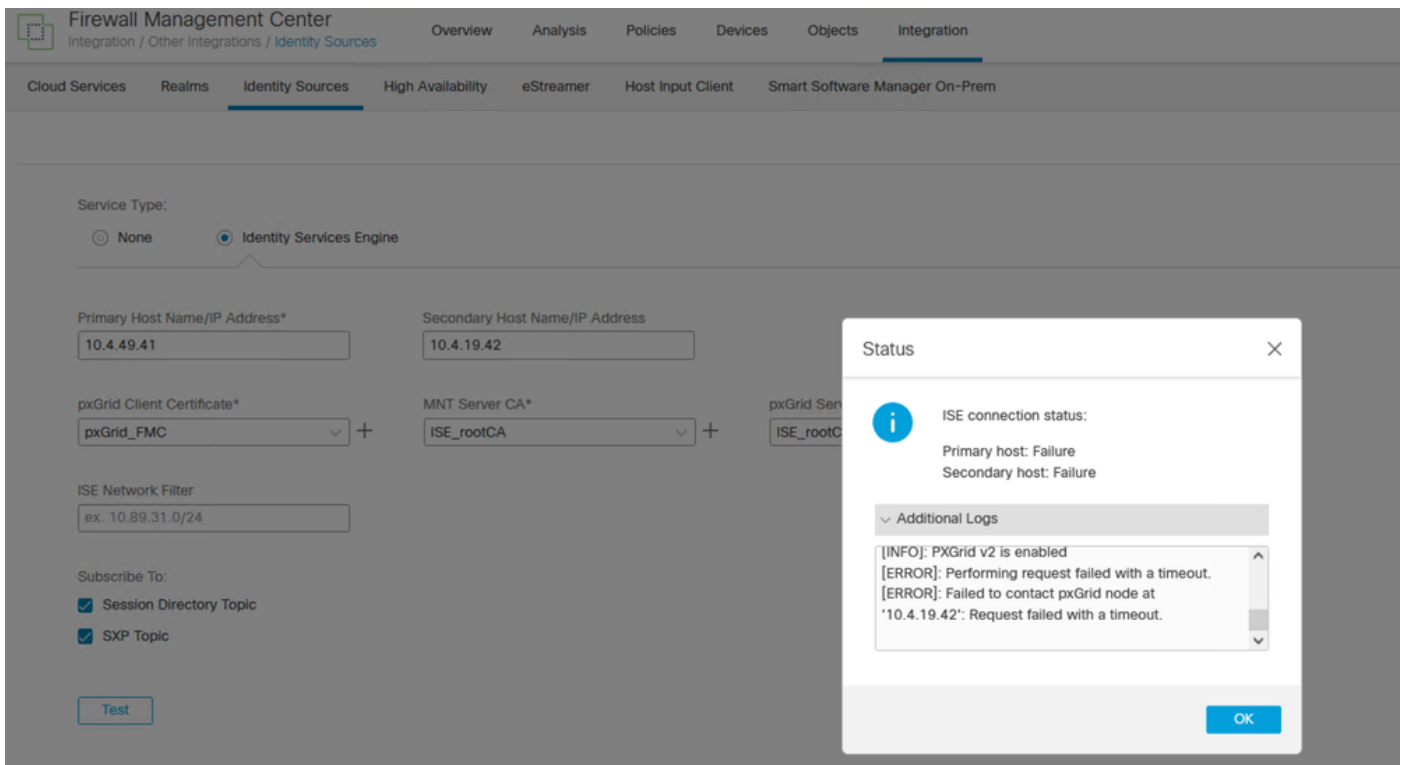


Conseil : Pour d'autres recommandations de collecte de journaux, consultez la vidéo [How to Enable Debugs on ISE 3.x Versions.](#)

Problèmes courants.

Le client abonné PxGrid n'est pas approuvé sur ISE.

Pour ce cas d'utilisation, le résultat associé au bouton pxGrid du test FMC montre ce comportement :



Échec de la connexion FMC pxGrid.

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
```

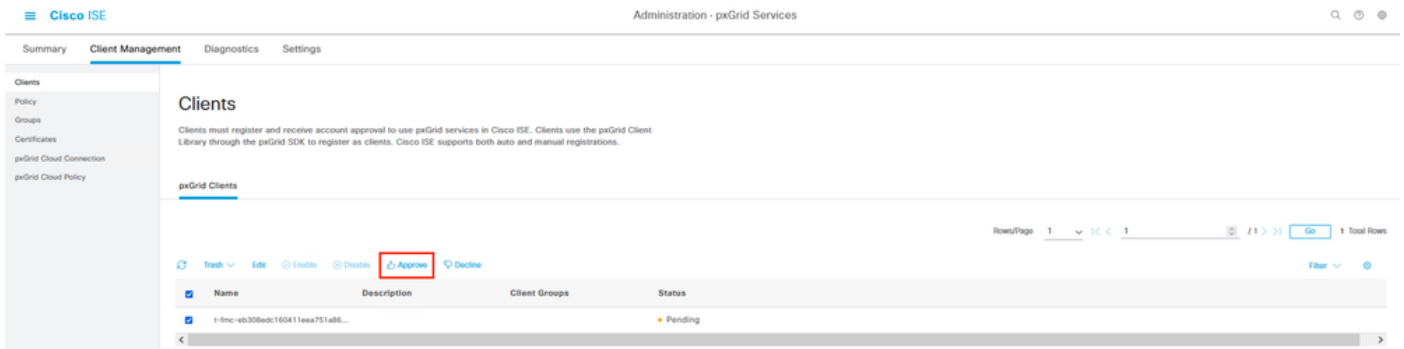
Secondary host:

```
[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.
```

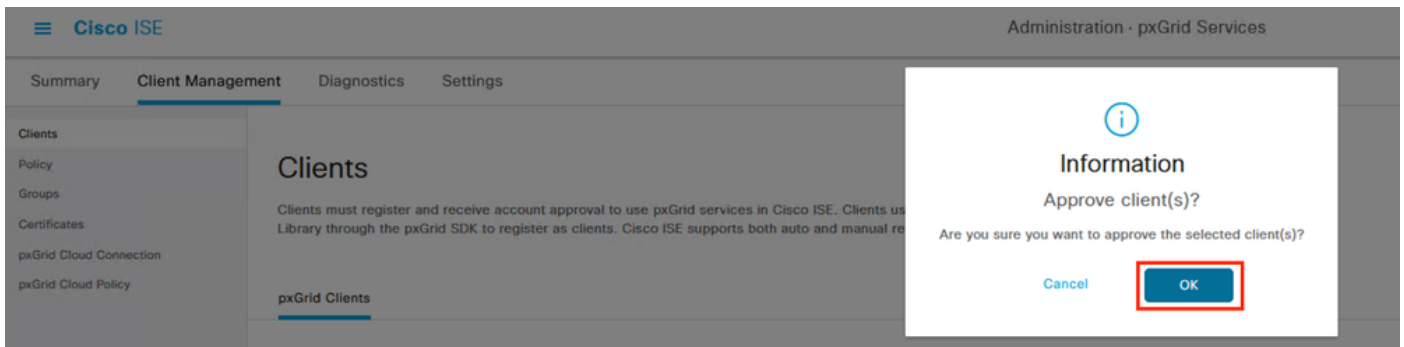
Sur ISE, notez le comportement dans le menu Administration > PxGrid Services > Client Management > Clients indiquant que le client pxGrid (FMC) est en attente d'approbation.

Cliquez sur le bouton Approuver, confirmez la sélection dans la fenêtre suivante et tentez à nouveau l'intégration.

Cette fois, l'intégration est réussie.



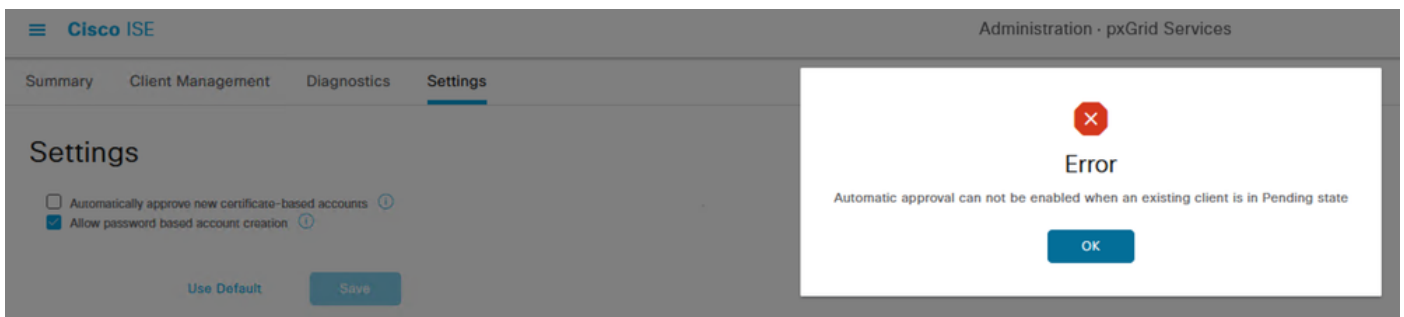
Le client FMC est en attente.



Confirmation de l'approbation du client pxGrid.

Notez si vous souhaitez activer l'approbation automatique des clients pxGrid basés sur un certificat.

Approuvez/refusez les clients de la page précédente car cette alarme peut apparaître.



Erreur liée à l'approbation des clients pxGrid.

Certificat ISE PxGrid chaîne incomplet.

Dans ce scénario, si vous naviguez vers le menu Administration > System > Certificate, sélectionnez le certificat pxgrid et sélectionnez l'option View,

En cas de problème avec le certificat, ces erreurs associées sont possibles.

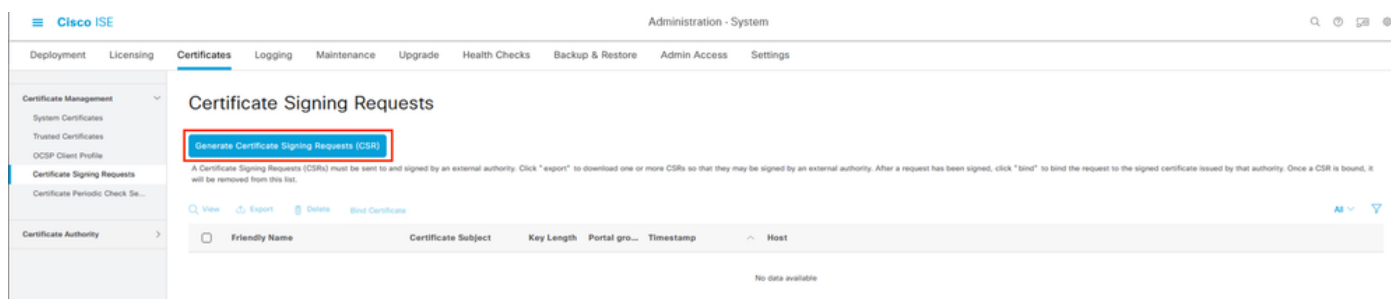
Certificate trust chain is incomplete

Erreur liée à la chaîne de certificats incomplète.

La première étape consiste à vérifier si l'autorité de certification racine ISE est terminée dans l'option Affichage.

En cas de certificat manquant dans la hiérarchie, vous pouvez émettre l'ensemble de l'autorité de certification racine de déploiement ISE.

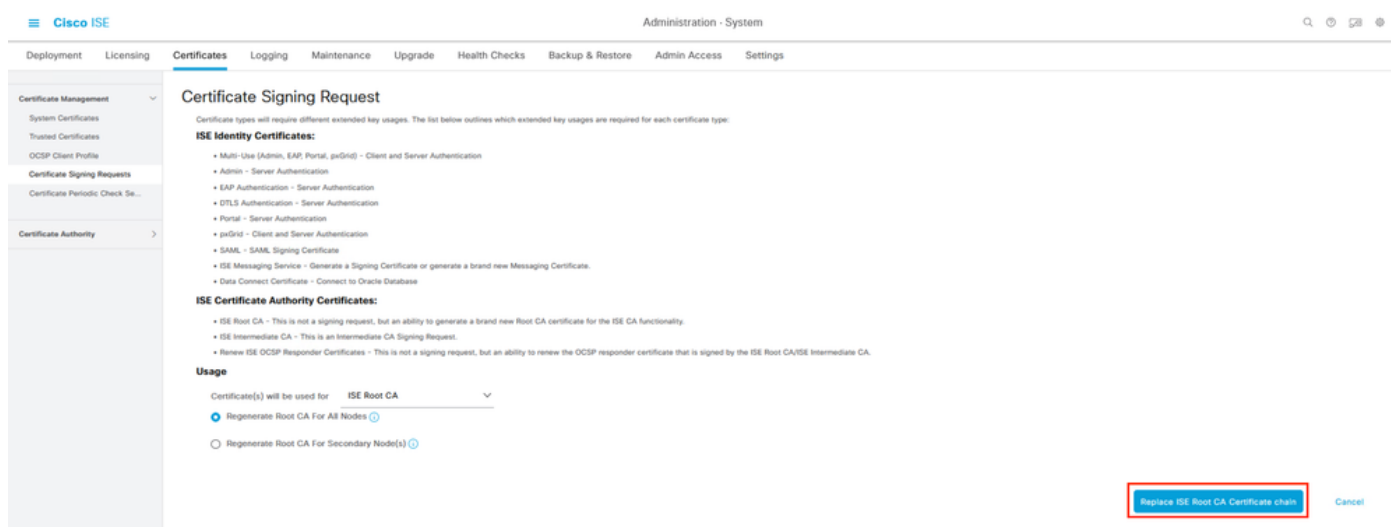
Accédez au menu Administration > System > Certificates > Certificate Management > Certificate Signing Request (RSE) et sélectionnez ce bouton.



Génération d'un CSR sur ISE.

Dans ce menu, sélectionnez dans Utilisation d'ISE Root CA et régénérez l'autorité de certification racine ISE pour tous les nœuds.

Continuer avec le bouton Remplacer la chaîne de certificats CA racine ISE.



Configuration de la demande de signature de certificat.

Attendez que les certificats soient générés dans tous les nœuds de l'impasse en œuvre

Une fois l'opération terminée, l'ISE affiche la notification suivante.

The screenshot shows the Cisco ISE Administration interface. The 'Certificates' tab is selected. The 'CA Certificates' section displays a table with the following data:

Friendly Name	Status	Trusted For	Serial Number	Issued To
Certificate Services Root CA - n1se32w00021	Enabled	Infrastructure,Endpoints	56 1C BA C5 B6 69 43 FF 9F E1 7B B4 02 91 F5 52	Certificate Services Root CA - n1se32
Certificate Services Node CA - n1se32w00022	Enabled	Infrastructure,Endpoints	2F 9D AC 27 FF 20 43 71 8D 3E FB 2A 85 1D 5D B7	Certificate Services Node CA - n1se32
Certificate Services Endpoint Sub CA - n1se32w00023	Enabled	Infrastructure,Endpoints	13 A5 F8 63 5F 5E 4C 24 AE 7A 0A 98 2D 9E 01 BC	Certificate Services Endpoint Sub CA - n1se32
Certificate Services OCSP Responder - n1se32w00024	Enabled	Infrastructure,Endpoints		

A modal message is displayed over the table:

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

OK

Confirmation de la génération de certificats.

Vérifiez si le pxGla chaîne de confiance du certificat rid est terminée en sélectionnant l'option Visualiser dans Certificats système.

Référence.

[Page des développeurs Cisco PxGrid.](#)

[Guide de l'administrateur de Cisco Identity Services Engine, version 3.2, chapitre : Cisco pxGrid.](#)

[Guide d'installation de Cisco Identity Services Engine, version 3.2, chapitre : Référence des ports Cisco ISE](#)

[Guide de référence CLI de Cisco Identity Services Engine, version 2.4](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.