Configuration et dépannage d'ISE 3.2 avec intégration FMC 7.2.4

Table des matières

- Introduction
- Conditions préalables
  - Composants utilisés
- Informations générales
  - pxGrid Version 1
  - PxGrid Version 2
  - Composants de pxGrid en tant que plate-forme
- Configurer
  - Préparation de l'ISE pour l'intégration
  - Préparer 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 le processus d'intégration d'Identity Services Engine avec Firewall Management Center à l'aide de connexions Platform Exchange Grid.

Conditions préalables

Cisco recommande des connaissances sur les sujets suivants :

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

Composants utilisés

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

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

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 permettant d'intégrer FMC et ISE à l'aide de pxGrid Version 2. Cisco Firepower Management Center (FMC) est une plate-forme centralisée pour le pare-feu de nouvelle génération et le système de prévention des intrusions, qui offre des fonctions de gestion des politiques, de détection des menaces et de réponse aux 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 plusieurs fournisseurs et le réseau multiplate-forme. Cette intégration assure la surveillance sécurisée, la détection des menaces et la définition de politiques réseau basées sur les informations partagées. Le framework PxGrid a deux versions ; une à utiliser (dépend de la version ISE) et un correctif ; vous devez réviser.

À partir de la version ISE 3.1, toutes les connexions pxGrid d'ISE sont basées sur pxGrid Version 2.

---

pxGrid Version 1

La première version de ce framework (pxGrid v1) est caractérisée sur la facilité de maintenance vue à travers la commande show application status ise telle qu'affichée dans le résultat. Lorsque la fonctionnalité pxGrid est activée dans le noeud, vous pouvez voir les fonctionnalités pxGrid dans un état 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 la plate-forme, il n'y a qu'un seul noeud pxGrid avec le statut d'exécution du processus pxGrid tandis que les autres noeuds pxGrid sont en veille. Ces noeuds surveillent continuellement le noeud pxGrid et ses services associés pour s'assurer qu'ils fonctionnent correctement. Le noeud pxGrid secondaire a été promu principal et l'autre noeud a activé ses services pxGrid. Cependant, cela représentait un temps d'arrêt lorsque le basculement s'est produit.

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

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

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

PxGrid Version 2

Ce document couvre l'utilisation de pxGrid v2. 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 les versions précédentes avec la commande show application status ise.

Reportez-vous à la section relative à la validation d'ISE dans ce document pour comprendre les mécanismes à examiner avec les fonctionnalités de pxGrid.

Dans cette version, vous avez des noeuds pxGrid à configurer en tant que noeuds pxGrid actifs. Ils sont prêts à participer à tout moment à l'échange d'informations. Avec v1, un seul noeud conservait la facilité de maintenance de pxGrid comme étant en cours d'exécution.

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

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

Composants de pxGrid en tant que plate-forme

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

Client : Peut être un abonné et un 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 le FMC en fonction des informations partagées par ISE et de leurs rubriques publiées (liées à l'activité des terminaux).

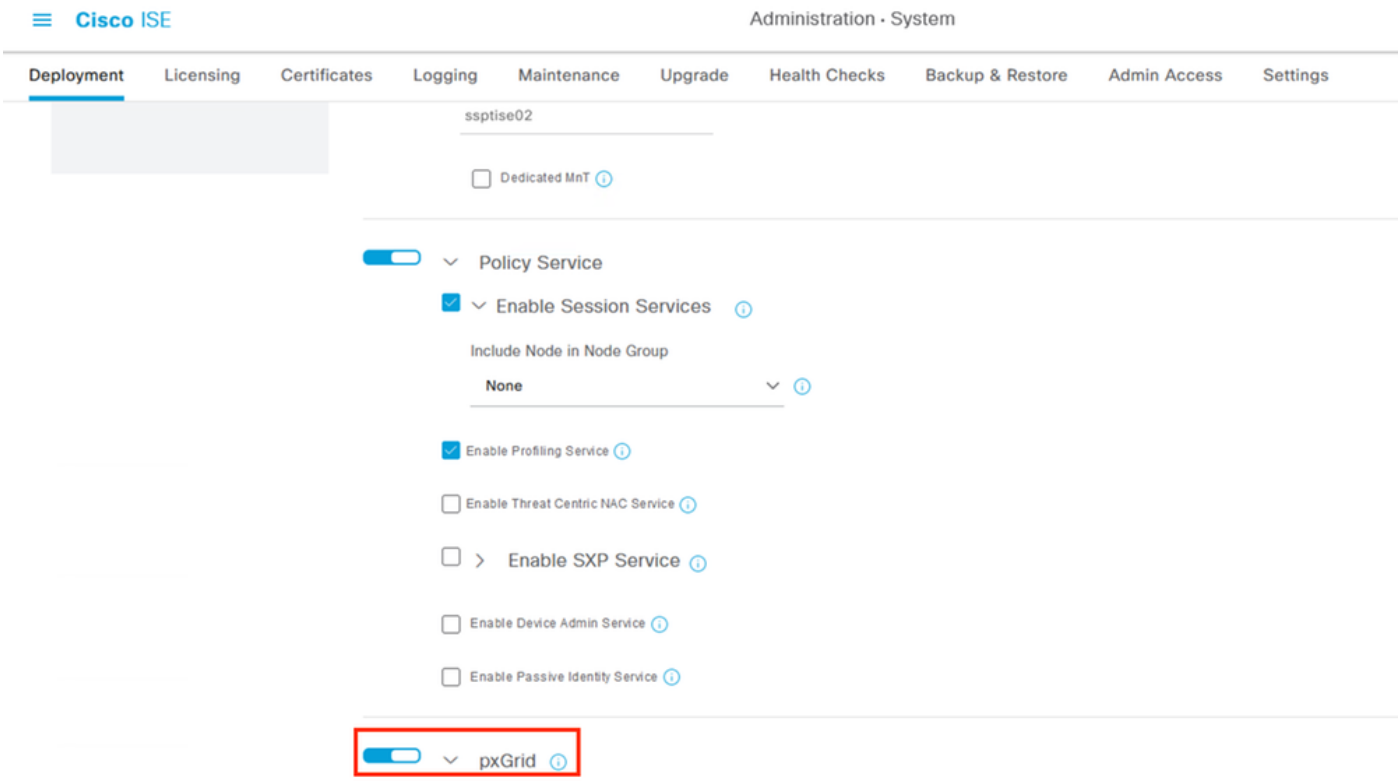
Configurer

Préparation de l'ISE pour l'intégration

Étape 1 : configuration du noeud ISE pour exécuter le profil pxGrid à partir du menu Administration > System > Deployment

---

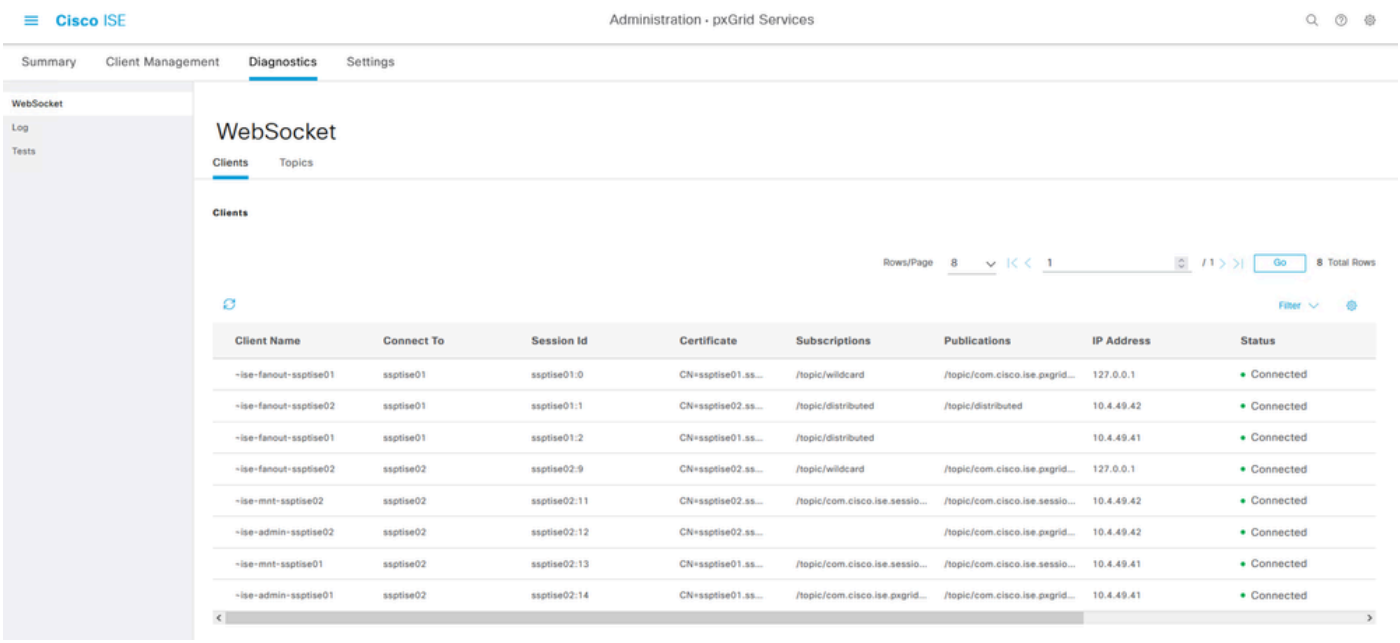
Étape 2. Sélectionnez les noeuds et activez la fonctionnalité pxGrid.



Activation des services ISE pxGrid dans un noeud.

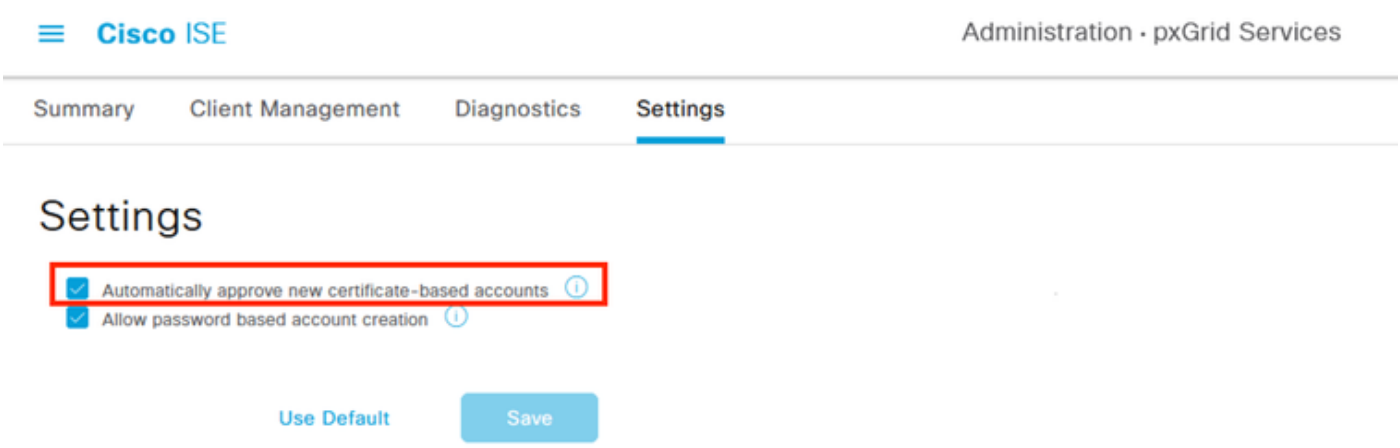
Étape 3. Après avoir activé les noeuds avec la fonctionnalité pxGrid, vérifiez l'état des Websockets associées aux clients internes connectés.

Étape 4. 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 5. Naviguez à travers le menu, Administration > pxGrid Services > Settings et sélectionnez l'option pour approuver automatiquement les nouveaux comptes de base de certificat, Cette étape est facultative, cependant, pour la connexion pxGrid, il est recommandé d'activer cette case à cocher. Vous pouvez accepter le FMC en tant qu'abonné manuellement après.



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

Étape 6. 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 cet exemple, les certificats ISE internes sont générés et l'autorité de certification racine correspond au noeud PAN.

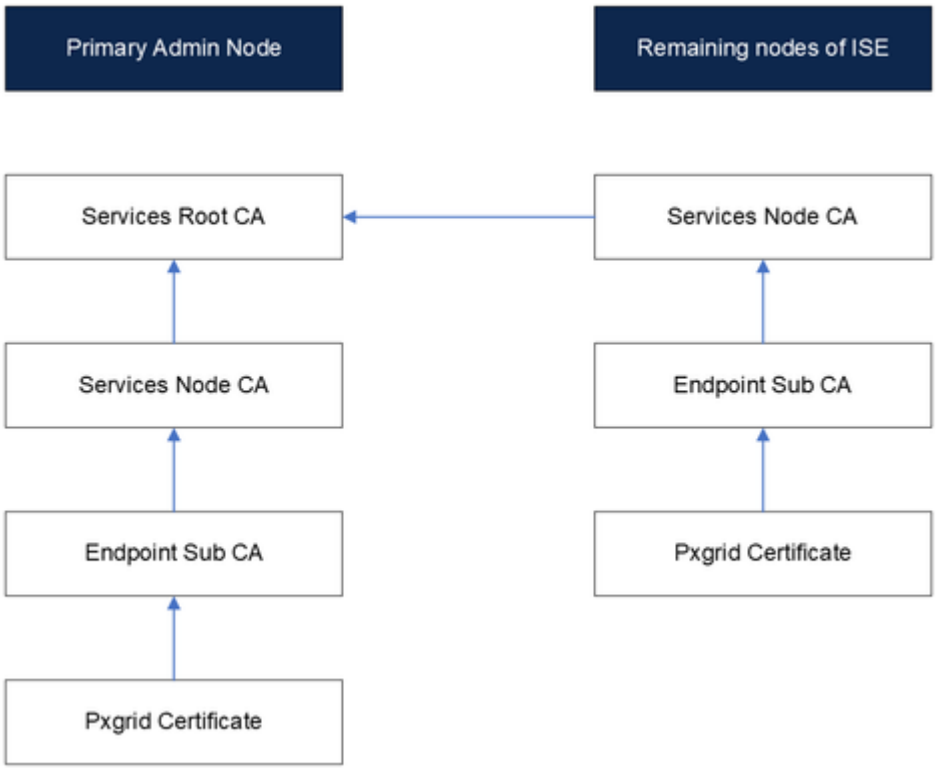
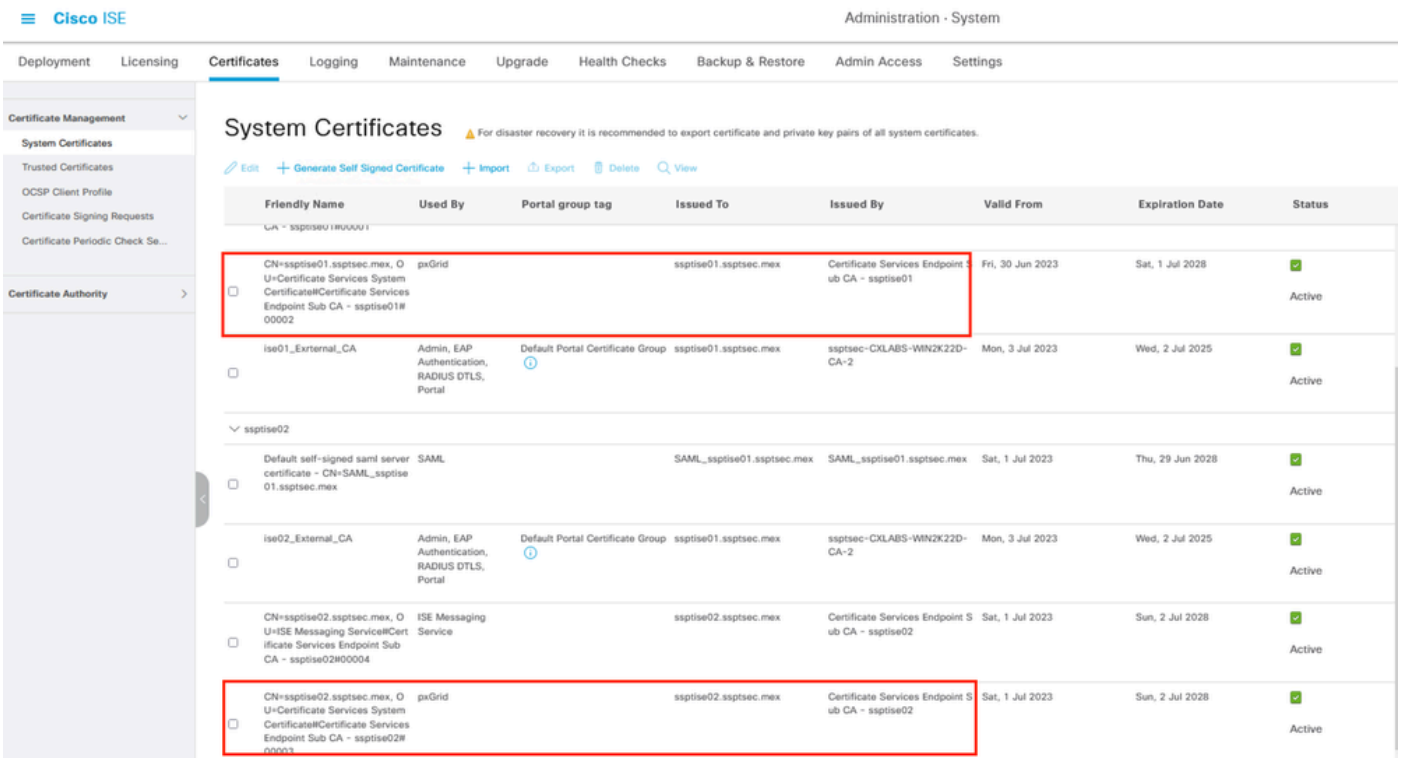


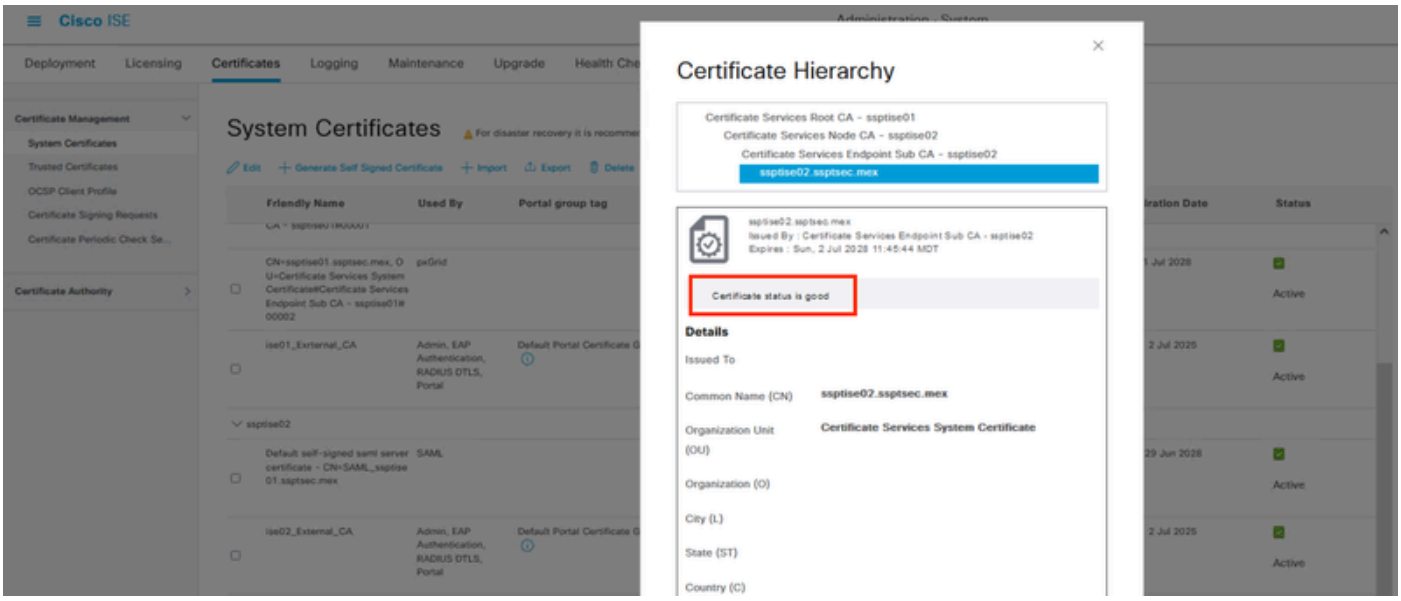
Schéma des certificats internes sur ISE.

Remarque : Pour plus d'informations sur la structure interne des certificats générés sur ISE, consultez Comprendre les services d'autorité de certification interne ISE.



Certificats PxGrid dans un déploiement distribué.

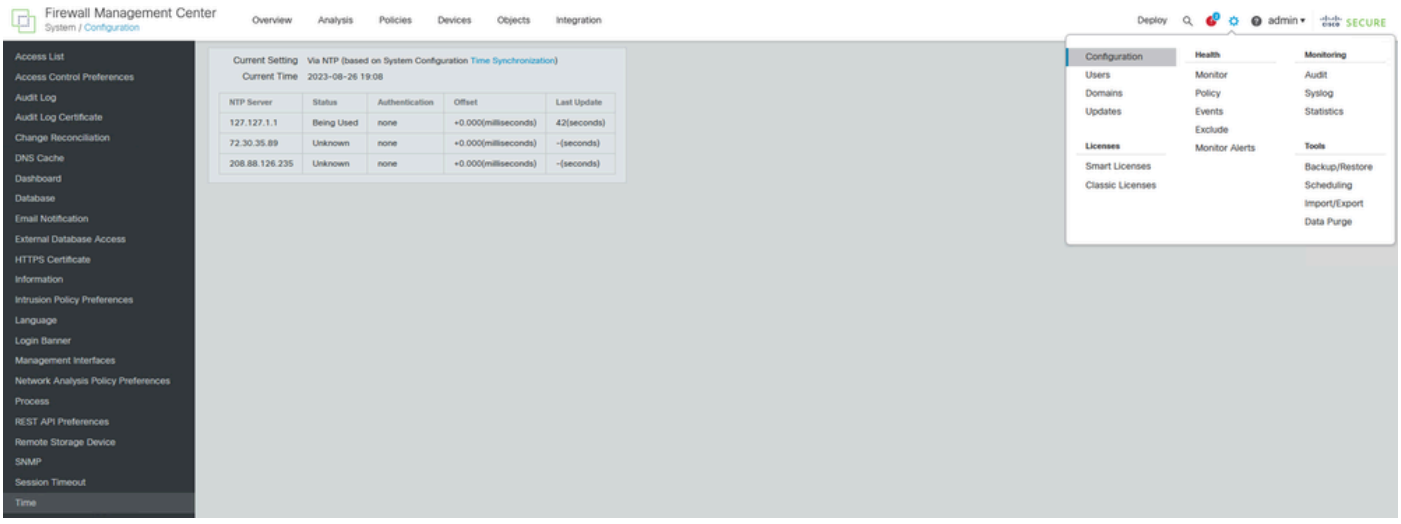
Étape 7. Vérifiez l’état des certificats pxGrid. Dans le menu précédent, cochez la case du certificat pxGrid du noeud, puis sélectionnez l'option View. Le résultat ressemble à celui affiché dans les certificats pxGrid.



Vérification du certificat pxGrid.

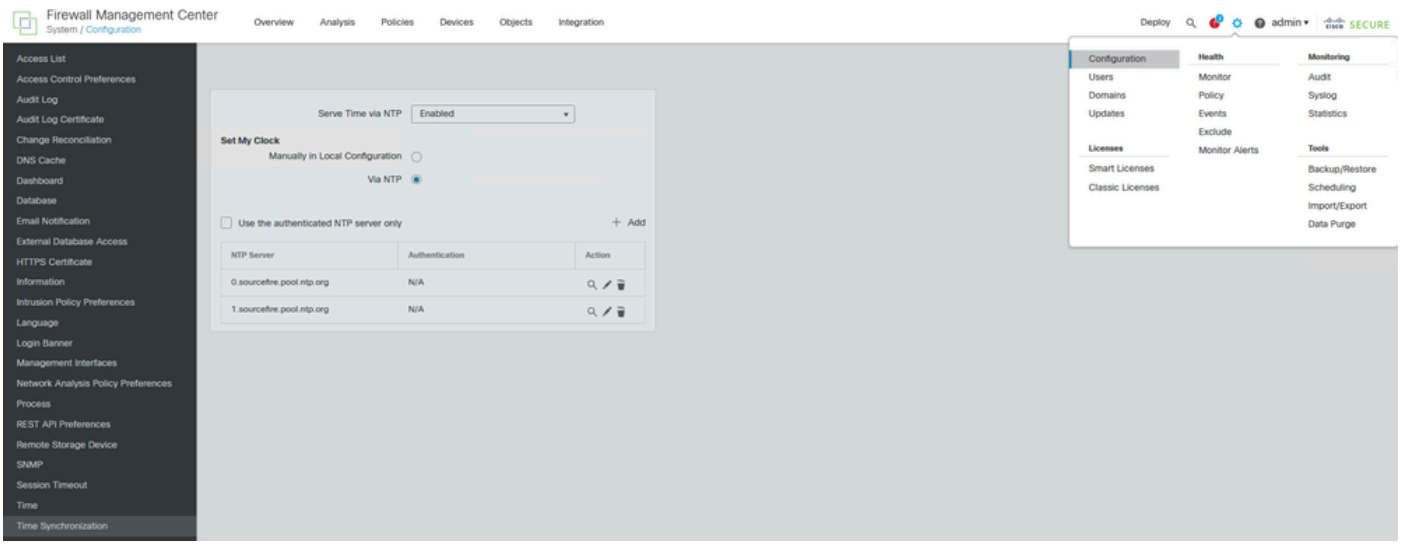
Préparer le FMC pour l'intégration

Étape 1. Confirmez que l’heure interne FMC est à jour de nNaviguez jusqu'à System > Configuration > Time.



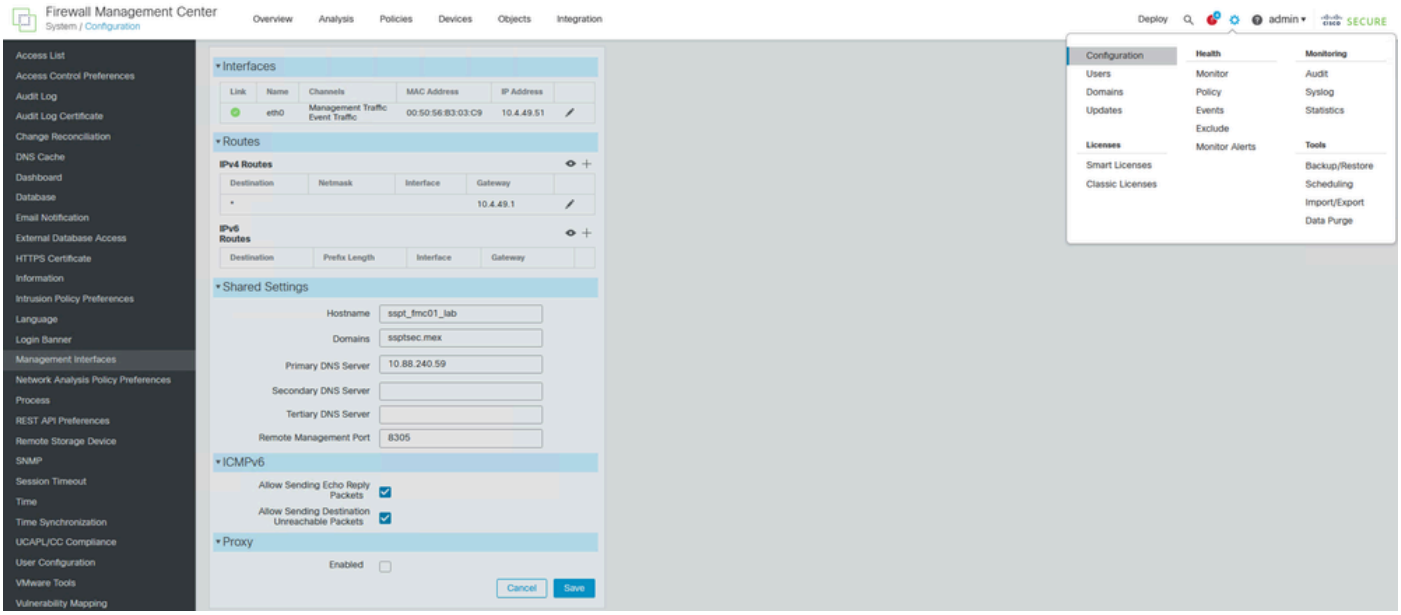
Vérification de la mise à jour du FMC.

Si l'heure FMC n'est pas mise à jour, assurez-vous que le protocole NTP est correctement configuré et en synchronisation. NTP peut être configuré sous System > Configuration > Time > + Add.



Synchronisation temporelle sur FMC.

Étape 2. Accédez à System > Configuration > Management Interface > Shared Settings et vérifiez que le champ Primary DNS Server contient une adresse IP valide de serveur DNS.



Configuration DNS sur FMC.

Étape 3. Confirmez que le nom d'hôte FMC est configuré. Accédez à Système > Configuration > Interface de gestion > Paramètres partagés et vérifiez que le champ Nom d'hôte contient le nom d'hôte FMC. Vérifiez cette étape lors de la révision de l'étape précédente de cette section.

Configuration de la connexion pxGrid entre ISE et FMC

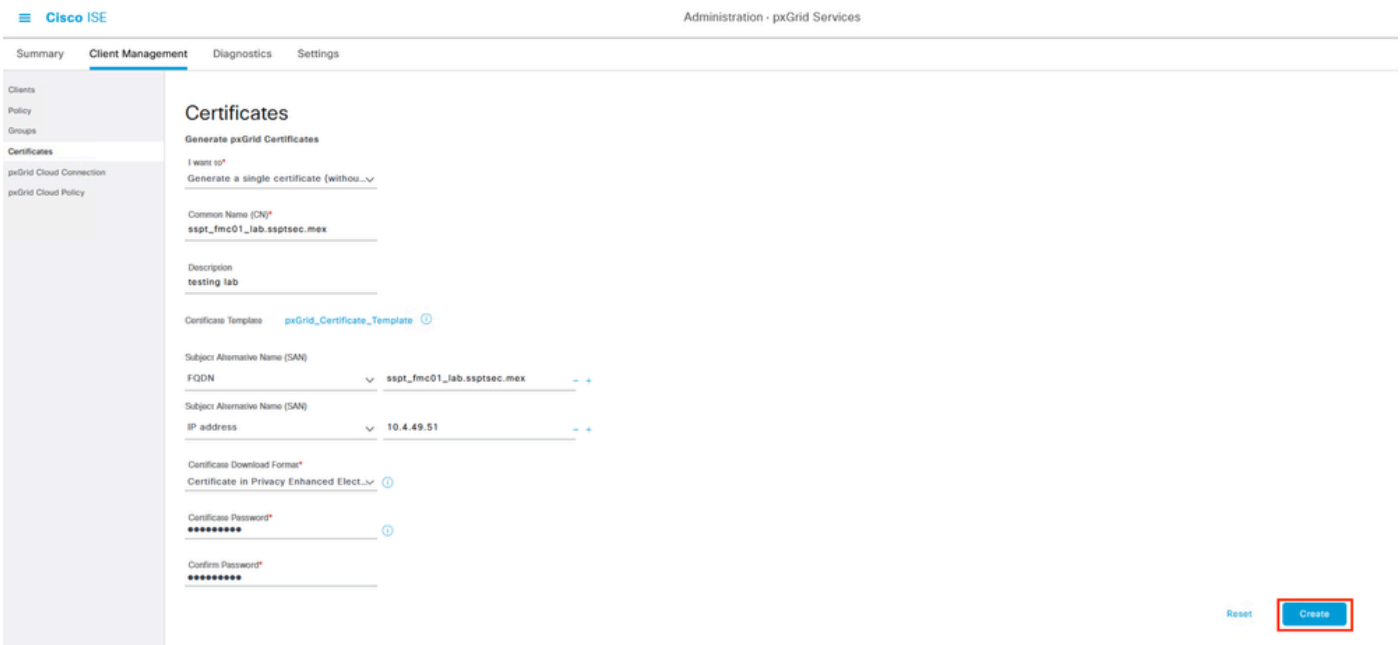
Étape 1. Accédez au menu Administration > pxGrid Services > Client Management > Certificates. Dans la première option, sélectionnez I want to Generate a single certificate (without a certificate sign request).

Étape 2. Dans la section Common Name (CN), entrez le nom de domaine complet du FMC où l'ISE émet un certificat et fournissez une description.

Étape 3. Dans la section Subject Alternative Name (SAN), entrez le nom de domaine complet et l'adresse IP du FMC à connecter.

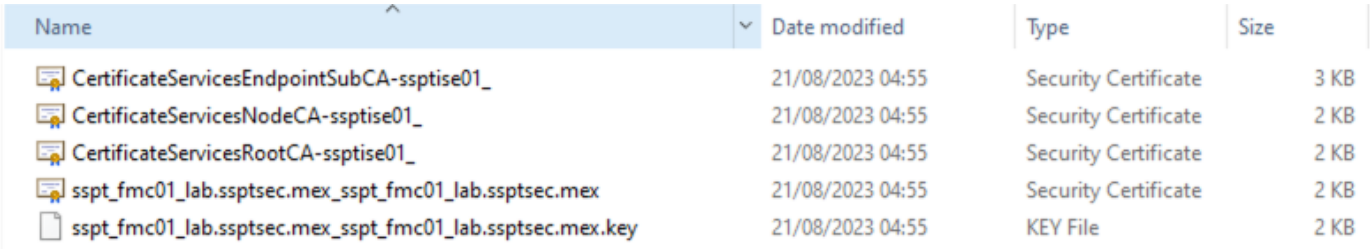
Étape 4. Au bas du Format de téléchargement de certificat, sélectionnez le menu déroulant et choisissez Certificate in Privacy Enhanced Electronic Mail (PEM) format. Entrez le format PEM PKCSS (y compris la chaîne de certificats).

Étape 5. Entrez et stockez un mot de passe dans Certificate Password (ce mot de passe est utilisé ultérieurement dans FMC). Confirmez le mot de passe et sélectionnez Créer.



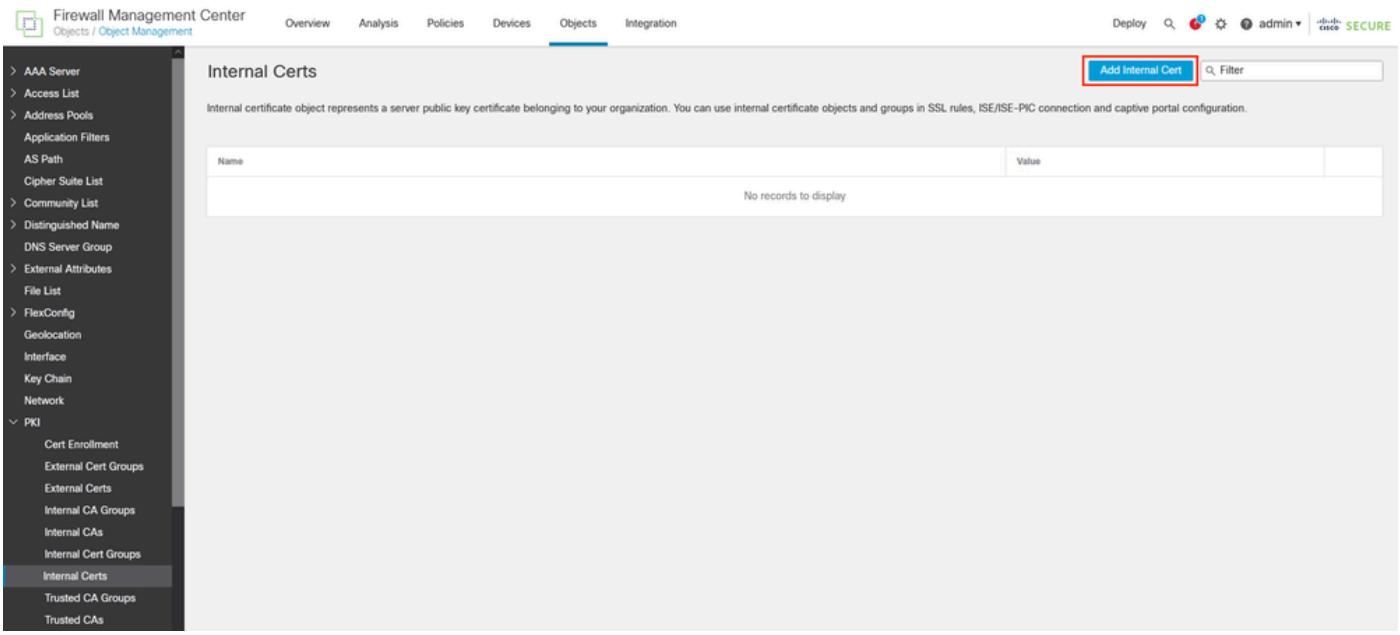
Exemple de génération de certificat pxGrid.

Étape 6. Un fichier zip est téléchargé sur votre ordinateur. Décompressez le fichier et vérifiez que vous disposez des fichiers suivants dans votre environnement :



Certificats PxGrid générés par ISE.

Étape 7. Dans FMC, accédez au menu Objets > Gestion des objets > PKI > Certs internes. Sélectionnez l'option Ajouter un certificat interne.

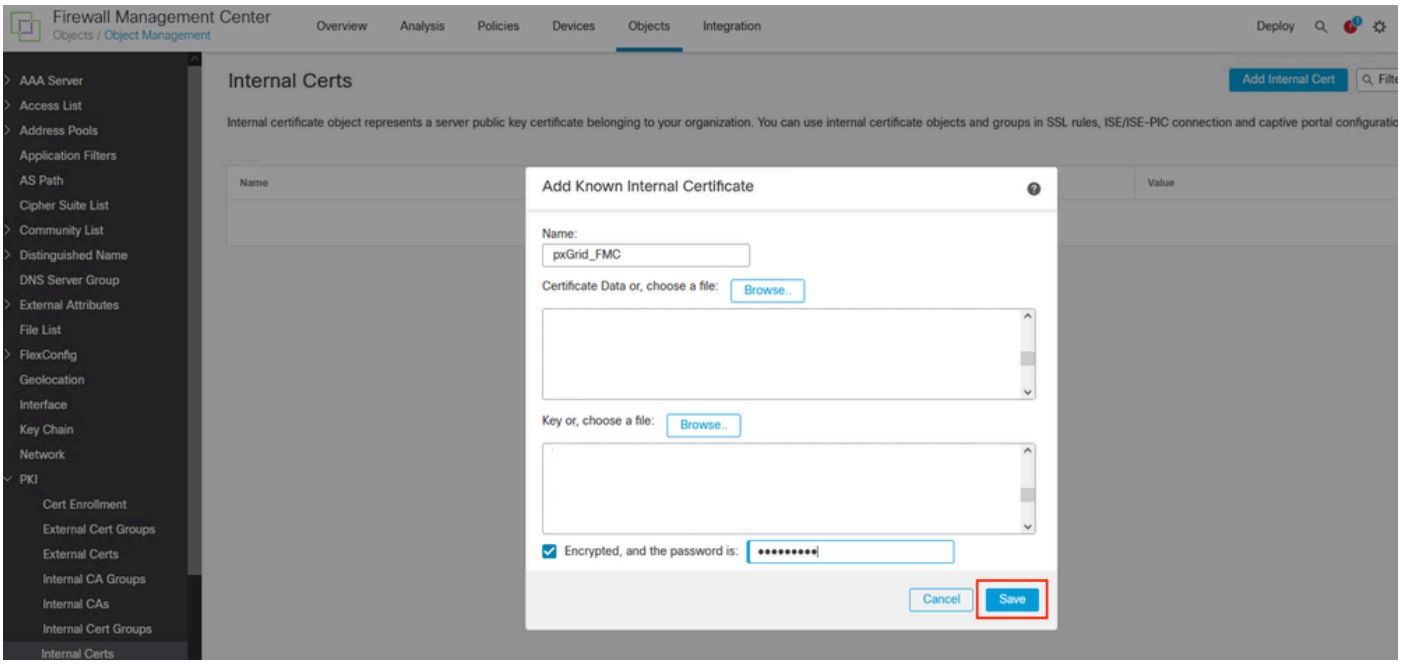


Ajout du certificat FMC comme certificat interne.

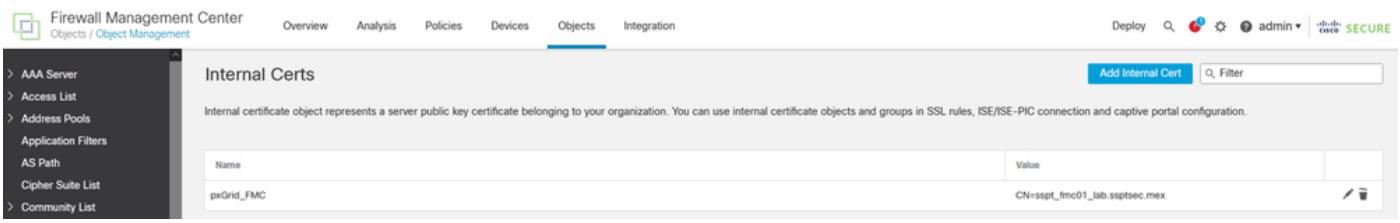
Étape 8. Attribuez un nom au certificat alloué sur FMC. Parcourez le certificat que vous avez créé pour FMC depuis ISE dans la section Certificate Data.

Étape 9. Parcourez le fichier avec l'extension .key pour remplir le champ suivant.

Étape 10. Sélectionnez l'option Chiffré et entrez le mot de passe que vous avez utilisé lors de la création du certificat sur ISE. Enregistrez la configuration.

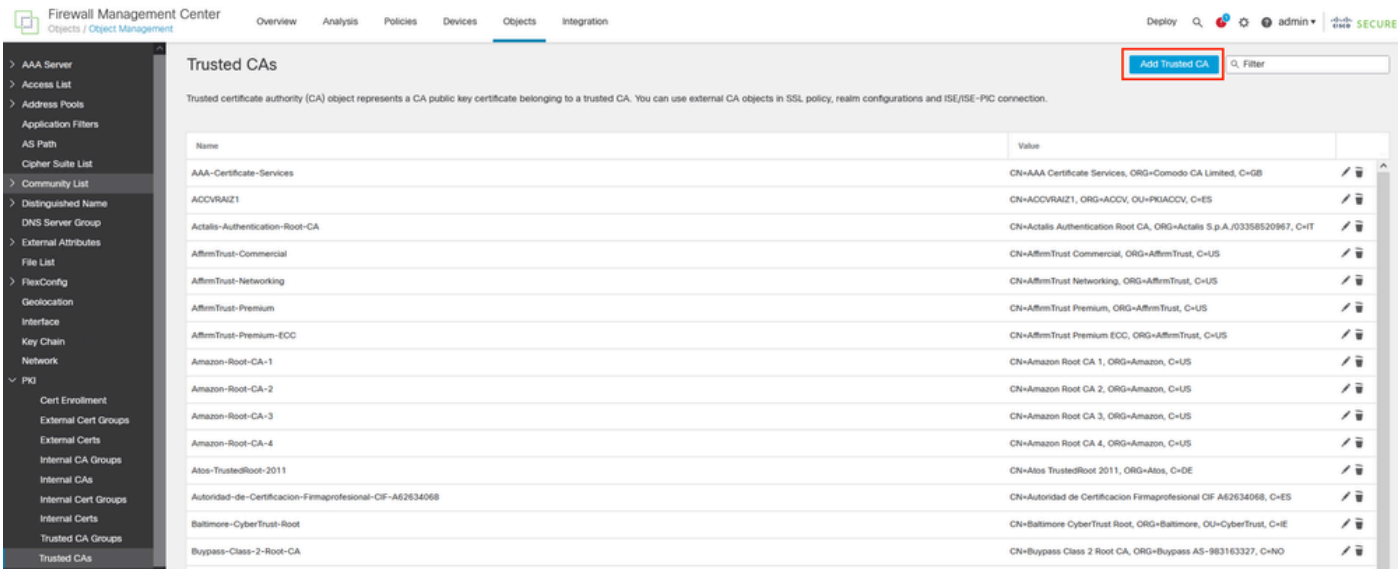


Exportation du certificat FMC généré par ISE.



Certificat FMC.

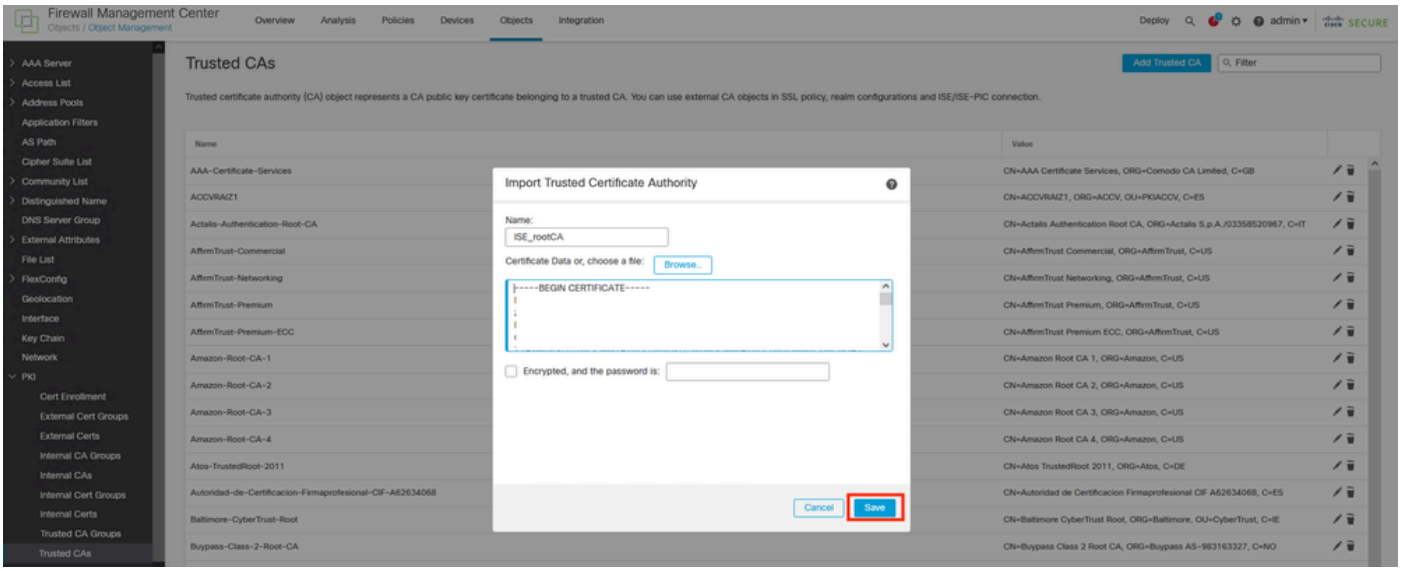
Étape 5. Accédez au menu Objets > Gestion des objets > ICP > Autorités de certification de confiance, sélectionnez Ajouter des autorités de certification de confiance.



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

Étape 11. Nommez l’autorité de certification.

Étape 12. Parcourez et sélectionnez l'autorité de certification racine ISE téléchargée à partir du fichier ISE. Enregistrez votre configuration.



Exportation de l'autorité de certification racine ISE.

Étape 13. Accédez au menu Integration > Other Integrations > Identity Sources. Sélectionnez le type de service : Identity Services Engine,

---

Étape 14. Entrez 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.

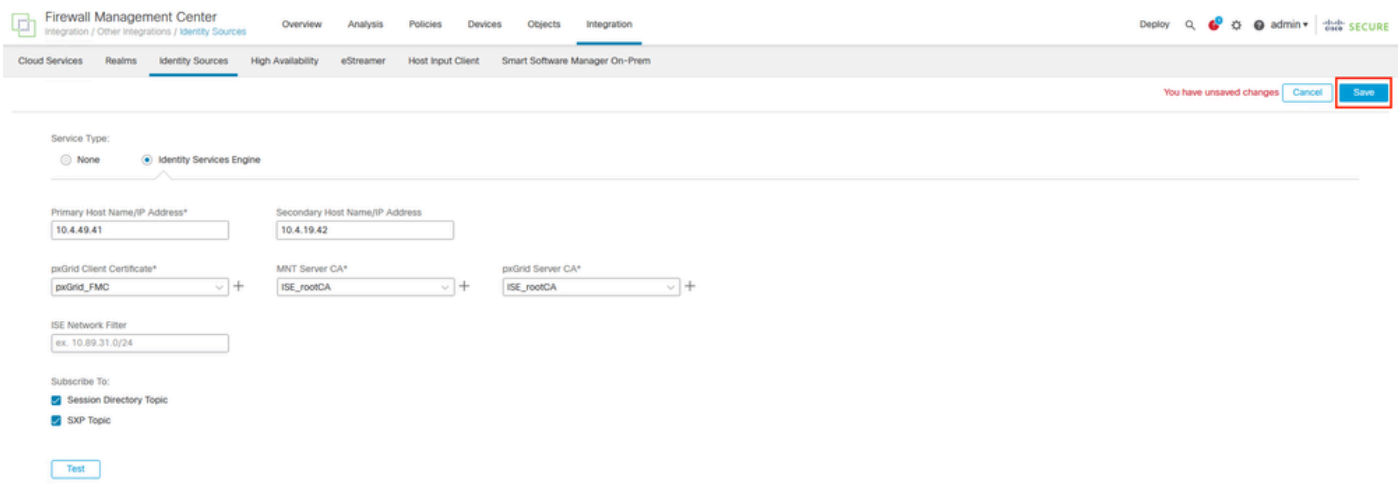
Étape 15. Sélectionnez dans le menu déroulant le certificat pxGrid généré par ISE pour la section certificat client pxGrid.

Étape 16. Dans la section CA du serveur MNT et CA du serveur pxGrid, sélectionnez la CA 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.

Étape 17. Facultatif : vous pouvez vous abonner au répertoire de session et à la rubrique SXP à partir d'ISE. Enregistrez la configuration.

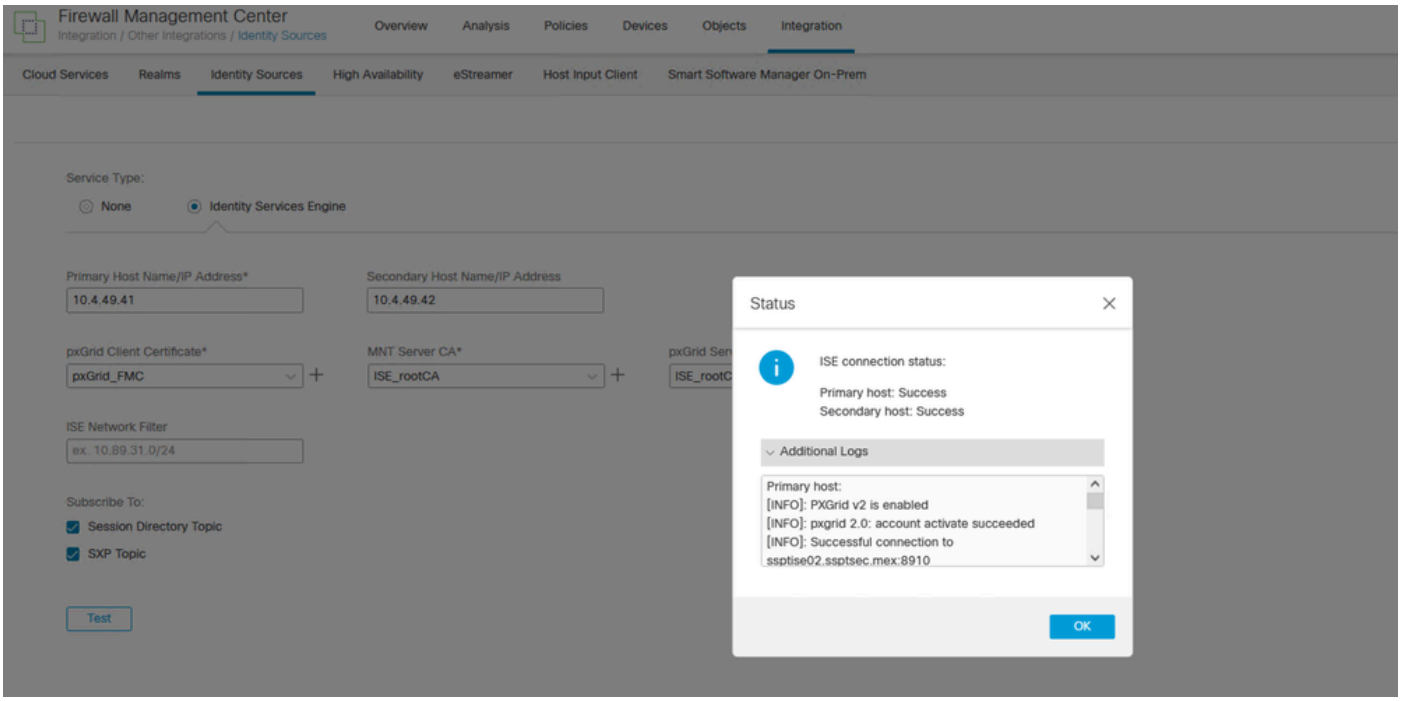


Configuration d'ISE comme source d'identité dans FMC.

Vérifier

Validation sur FMC

Étape 1. Dans le menu, accédez à Integration > Other Integrations > Identity Sources > Identity Services Engine. Avant d'enregistrer votre configuration, vous pouvez tester les paramètres du lien pxGrid.



Communication PxGrid réussie.

```
Primary host:

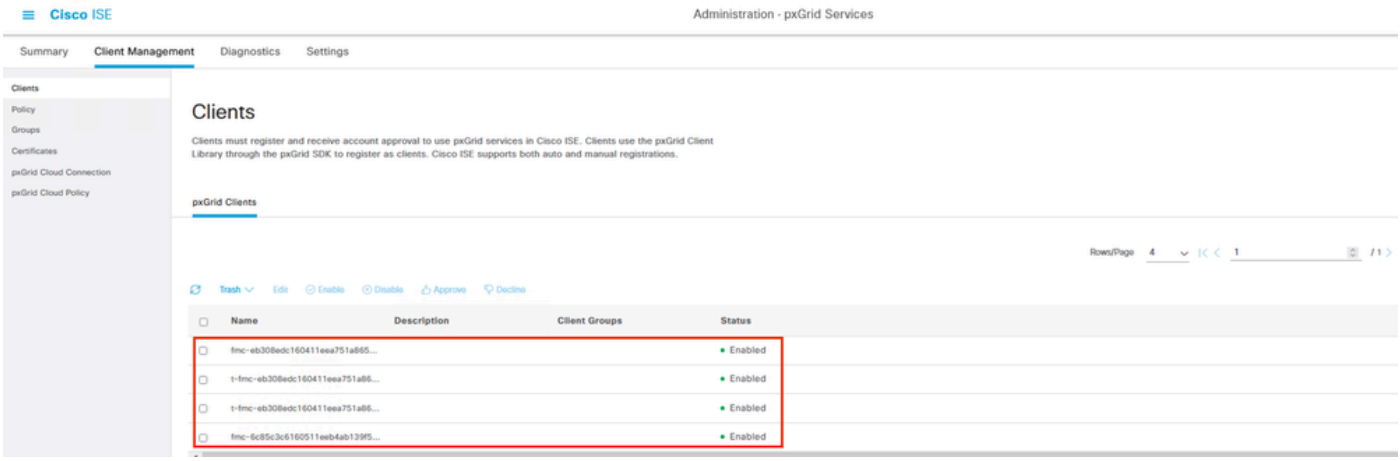
[INFO]: PXGrid v2 is enabled
[INFO]: pxgrid 2.0: account activate succeeded
[INFO]: Successful connection to ssptise02.ssptsec.mex:8910
[INFO]: Successful connection to ssptise01.ssptsec.mex:8910
[INFO]: These ISE Services are up: SessionDirectory, SXP, EndpointProfile, SecurityGroups, AdaptiveNetw
[INFO]: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

Validation sur ISE

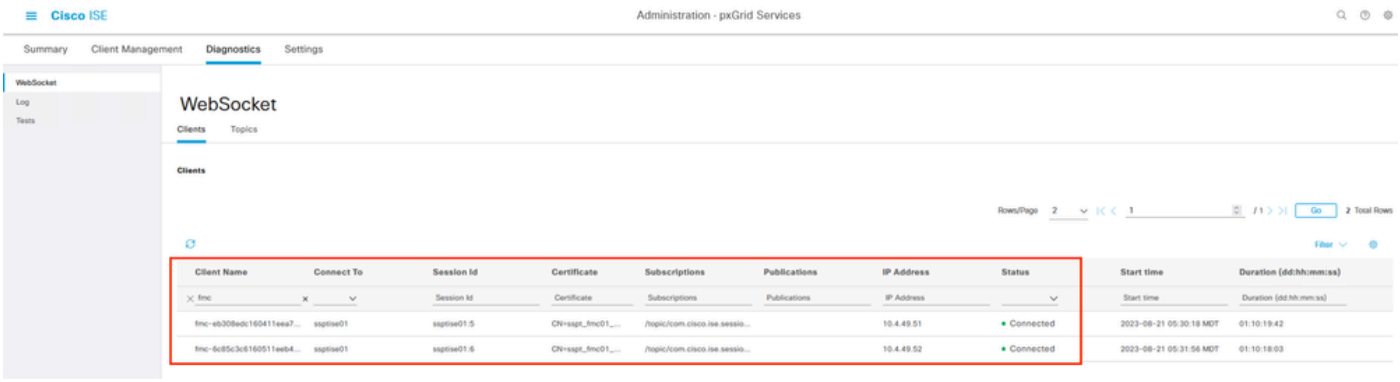
Étape 1. Lorsque le client FMC pxGrid a été correctement intégré sur ISE, vous pouvez voir dans le menu Administration > pxGrid Services > Client Management > Clients, les clients portant le nom fmc sont inclus et activés.



Clients PxGrid disponibles et activés.

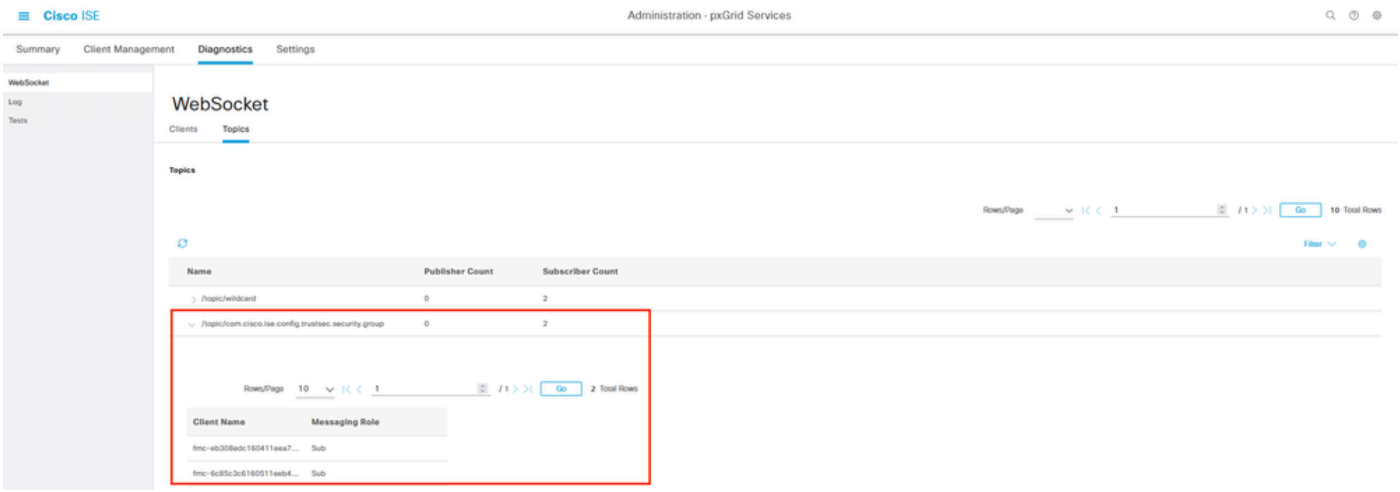
Remarque : Les clients pxGrid avec le préfixe « t-fmc » sont utilisés par le bouton de test FMC.

Étape 2. Si vous accédez au menu Administration > pxGrid Services > Diagnostics > WebSocket, vous voyez les connexions vers le FMC. Dans ce scénario, vous disposez de FMC en haute disponibilité (HA). Les unités principale et secondaire sont affichées comme dans cet exemple :



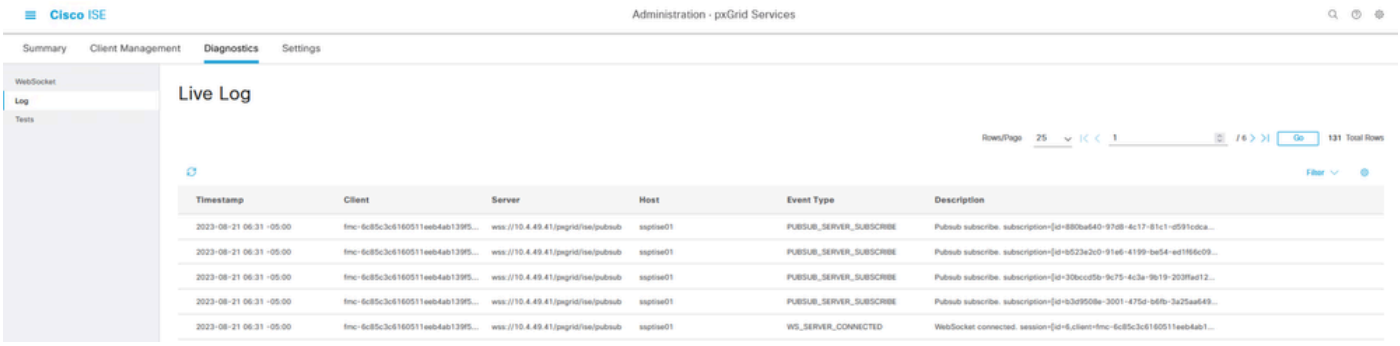
WebSockets disponible sur ISE.

Étape 3. Dans l'onglet suivant, sous Rubriques, vérifiez que les abonnés FMC sont ajoutés aux rubriques pxGrid publiées par ISE.Par exemple, la rubrique relative au groupe de sécurité où vous voyez les deux FMC sont abonnés et reçoivent des informations relatives aux balises de groupe de sécurité publiées par ISE.



Rubriques par abonné pxGrid.

Étape 4. Dans le menu Administration > pxGrid Services > Diagnostics > Log, les événements importants liés à la communication pxGrid (pour les noeuds avec la fonctionnalité activée) sont affichés. Elles présentent les informations relatives à l'intégration.



Journaux en direct PxGrid.

Dépannage

Dépannage sur FMC

Vérifiez que FMC peut résoudre son propre nom d'hôte et ses 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
```

Assurez-vous que le processus ADI est opérationnel :

<#root>

>

expert

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

sudo su

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

```
  pmtool status | grep adi
```

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

Assurez-vous que la communication entre FMC et ISE sur le port TCP 8910 est autorisée. À partir de l'interface de ligne de commande FMC, vous pouvez configurer une capture de paquets tcpudump 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
```

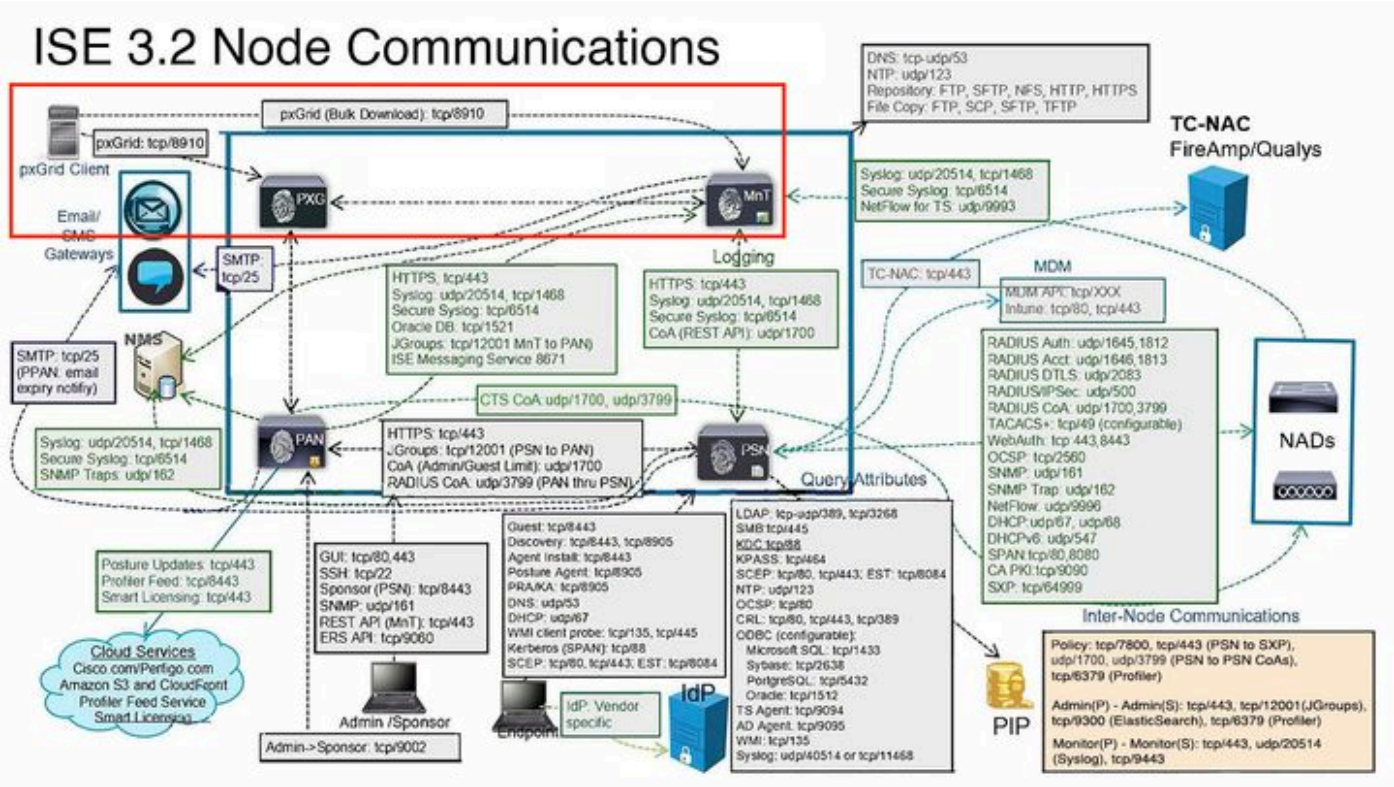
```
: Flags [S.], seq 3024877968, ack 3033526172, win 28960, options [mss 1460,sackOK,TS val 2268665064 ecr
22:34:08.415894 IP
```

```
 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

Étape 1. Vérifiez que la communication sur le port 8910 est opérationnelle. Il s'agit du port utilisé par les clients pxGrid pour communiquer avec les noeuds pxGrid et les noeuds MnT pour le téléchargement en masse des informations.



Interaction PxGrid dans un environnement ISE.

Remarque : Le client pxGrid, (dans ce cas) le FMC communique aux noeuds pxGrid et le noeud MNT secondaire (SMNT) reçoit le téléchargement en masse des informations. Si une défaillance se produit dans le SMNT, il recherche les informations via le MNT principal.

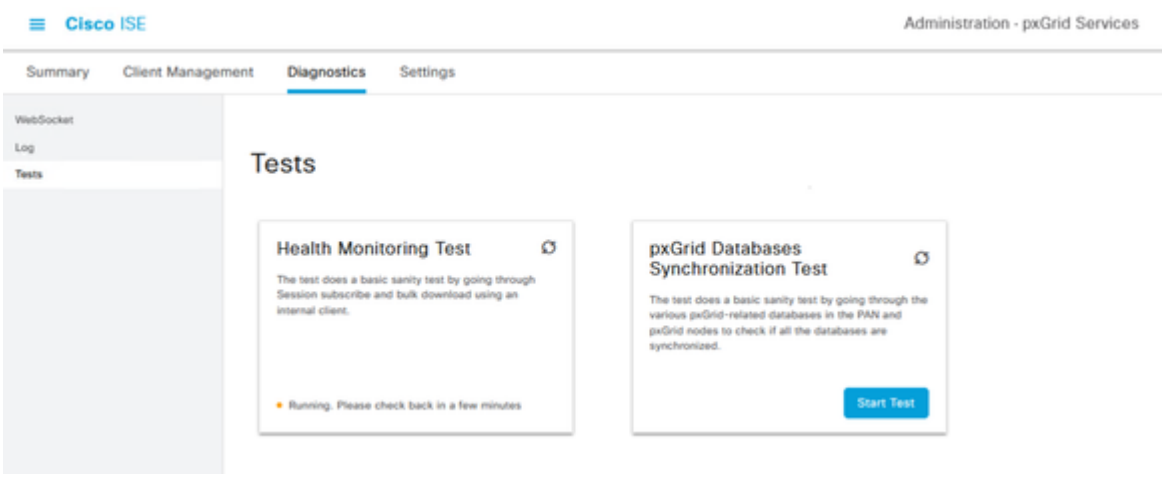
Dans les noeuds ISE où la communication avec le client pxGrid est conservée, vous pouvez vérifier si le port est ouvert ou si des sockets sont connectés à ce port.

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

Étape 2. 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.

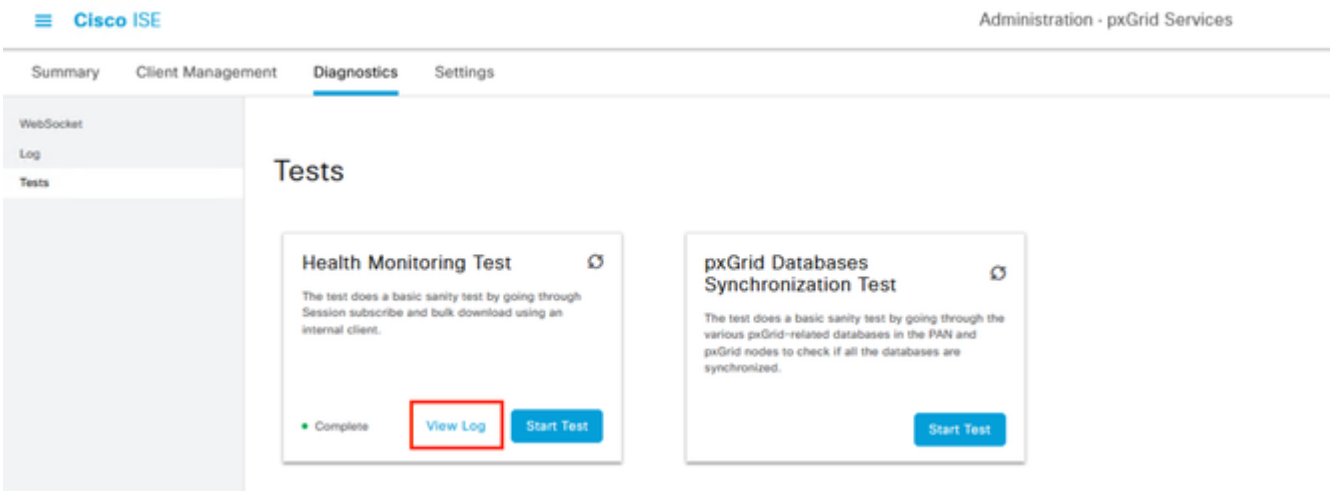
Étape 3. Le Test de contrôle de santé examine la recherche de service pxGrid, qui évalue si un client peut accéder au répertoire de session, au service et aux rubriques publiés par le contrôleur pxGrid.

Étape 4. Sélectionnez l'option Start Test et attendez que les journaux soient rassemblés.



Test de contrôle d'intégrité PxGrid.

Étape 5. Une fois le test terminé, sélectionnez l'option Afficher le journal. Dans cet exemple, le contenu du journal est :

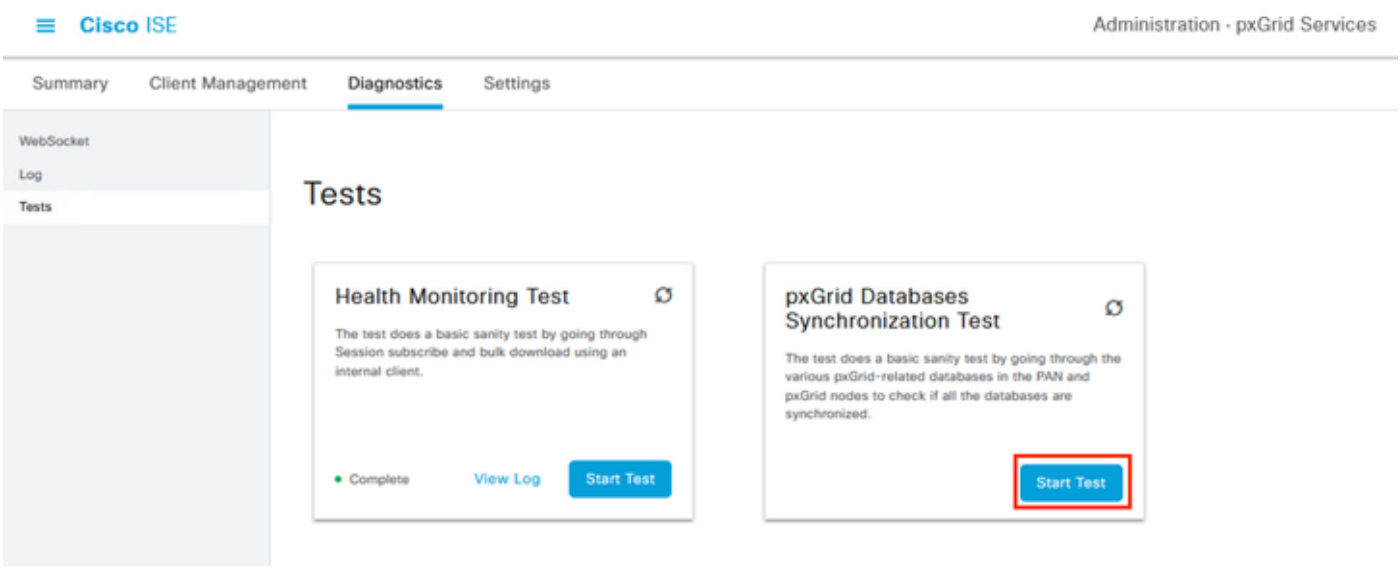


Examen du test de contrôle d'intégrité.

```
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 **********
```

Le test de synchronisation de base de données PxGrid vérifie si les informations dans les bases de données sont correctes entre les noeuds PAN et pxGrid et si elles sont synchronisées.Par conséquent, les informations envoyées aux abonnés pxGrid sont exactes.

Étape 6. Sélectionnez l’option Start Test et attendre que les résultats soient évalués.



Test de synchronisation des bases de données PxGrid.

Étape 7. À partir des journaux générés, ce résultat a été obtenu.

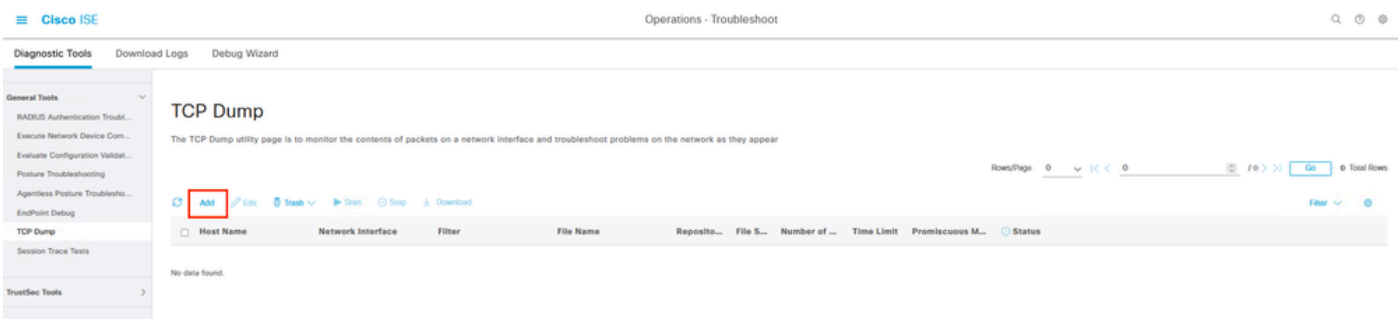
```
ssptise01.ssptsec.mex : In Sync
ssptise02.ssptsec.mex : In Sync

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

Étape 8. Obtenez une capture des noeuds pxGrid pointant vers le noeud FMC principal.

Étape 9. Accédez au menu Operations > Troubleshoot > Diagnostic Tools > TCP Dump.

Étape 10. Sélectionnez l'option permettant d'ajouter une nouvelle capture.



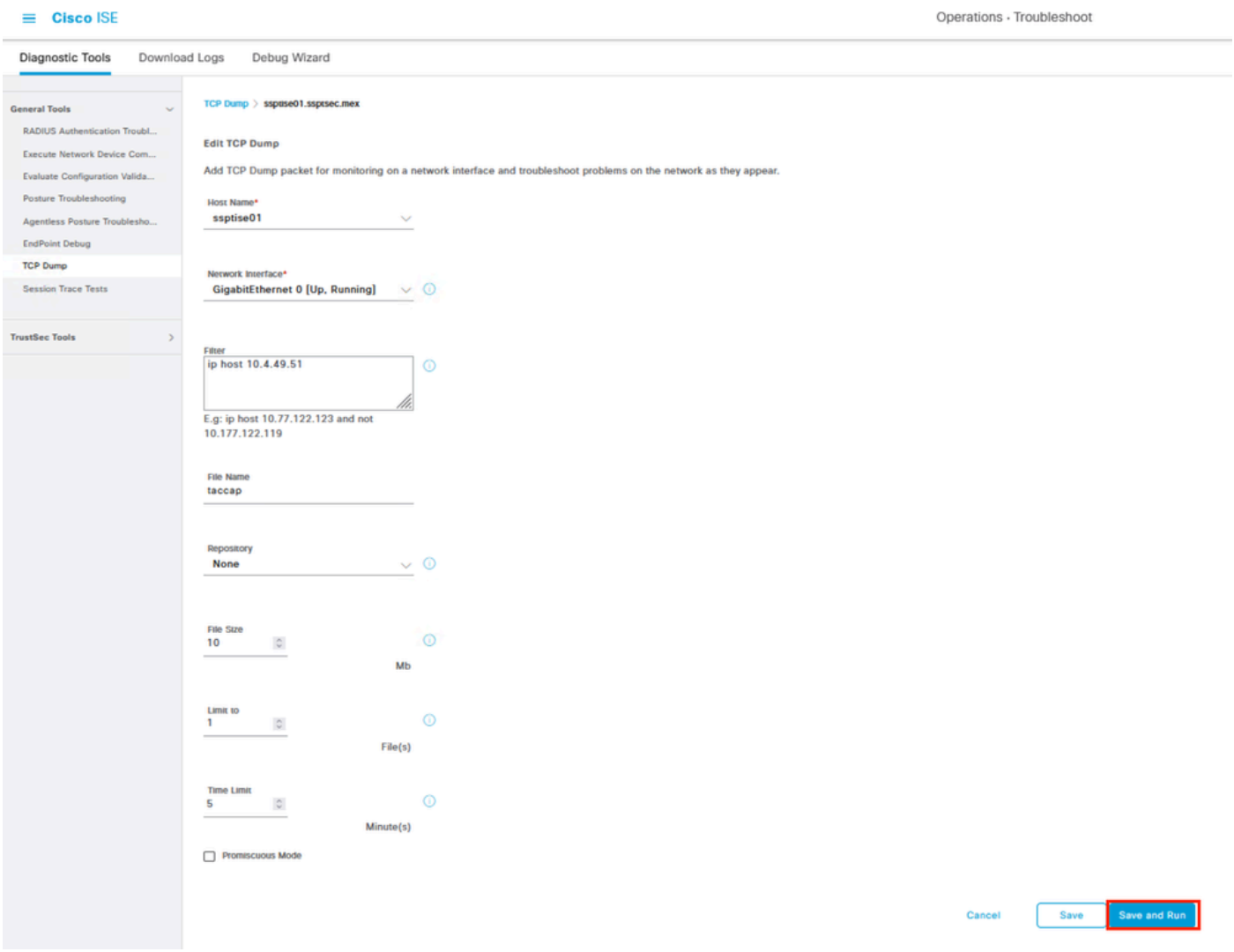
Génération d'une capture de paquets sur ISE.

Étape 11 : configuration des paramètres de capture

Étape 12. Dans HostName, sélectionnez le noeud pxGrid principal sélectionné dans FMC.

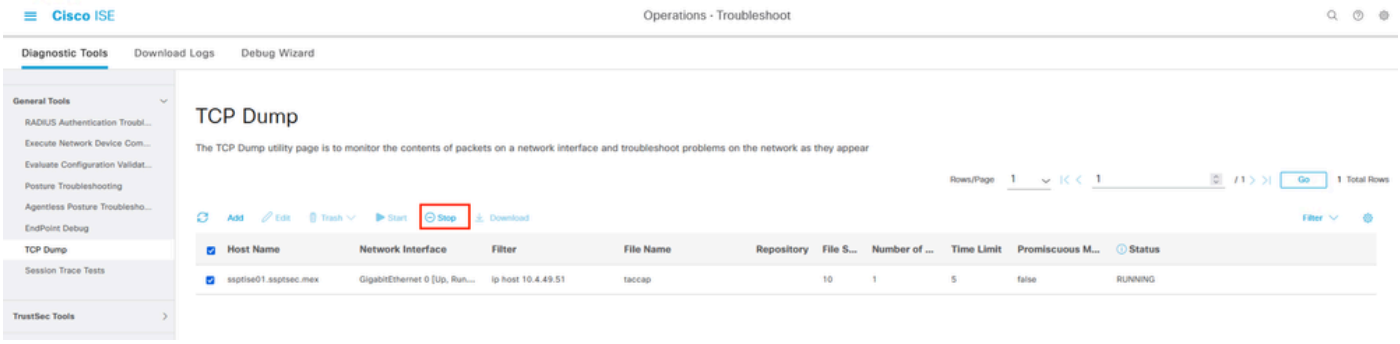
Étape 13. Filtrer le trafic avec cette syntaxe ip host <FMC IP>

Étape 14. Nommez la capture, puis passez à Enregistrer et exécuter.



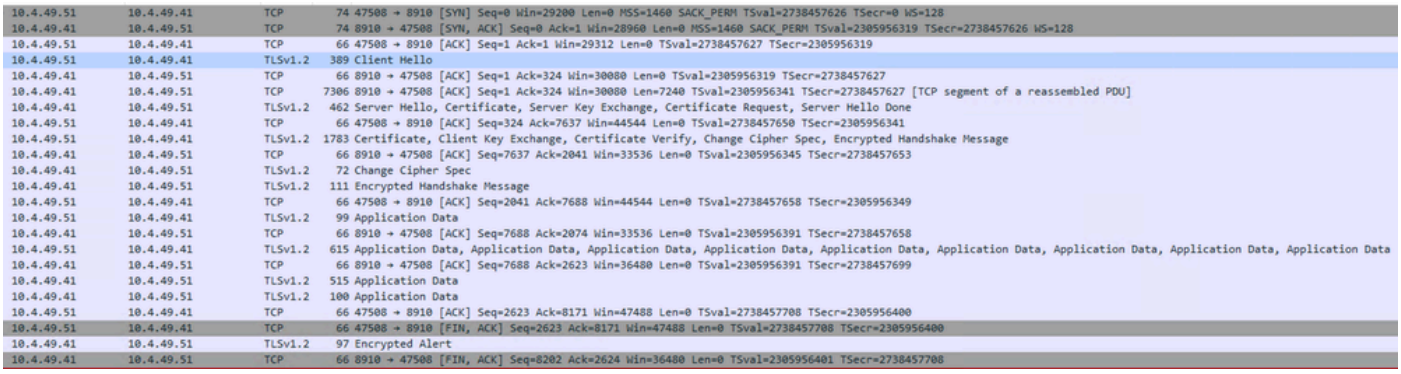
Exemple de configuration de capture de paquets.

Étape 15. Dans une autre fenêtre, dans le menu FMC, sélectionnez Integration > Other Integrations > Identity Sources. Et testez la connexion avec l'ISE via le canal pxGrid. Lorsque vous recevez le résultat du test, passez à Arrêter la capture sur l'ISE.



Arrêt d'une capture de paquets sur ISE.

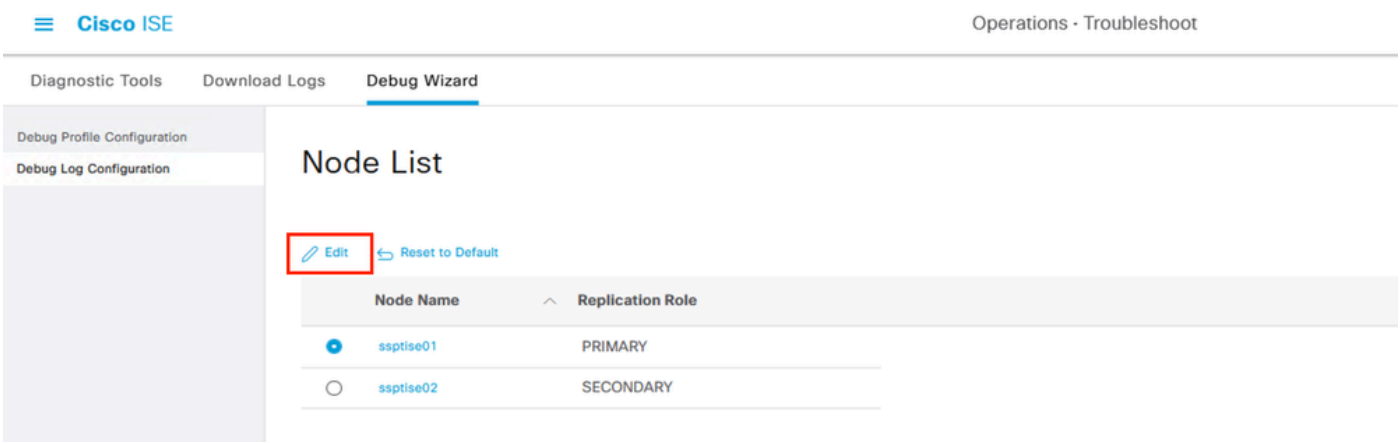
Étape 16. Téléchargez la capture et lancez l'analyse. Ce scénario affiche une capture d'une connexion opérationnelle qui peut servir de référence.



```
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, 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
```

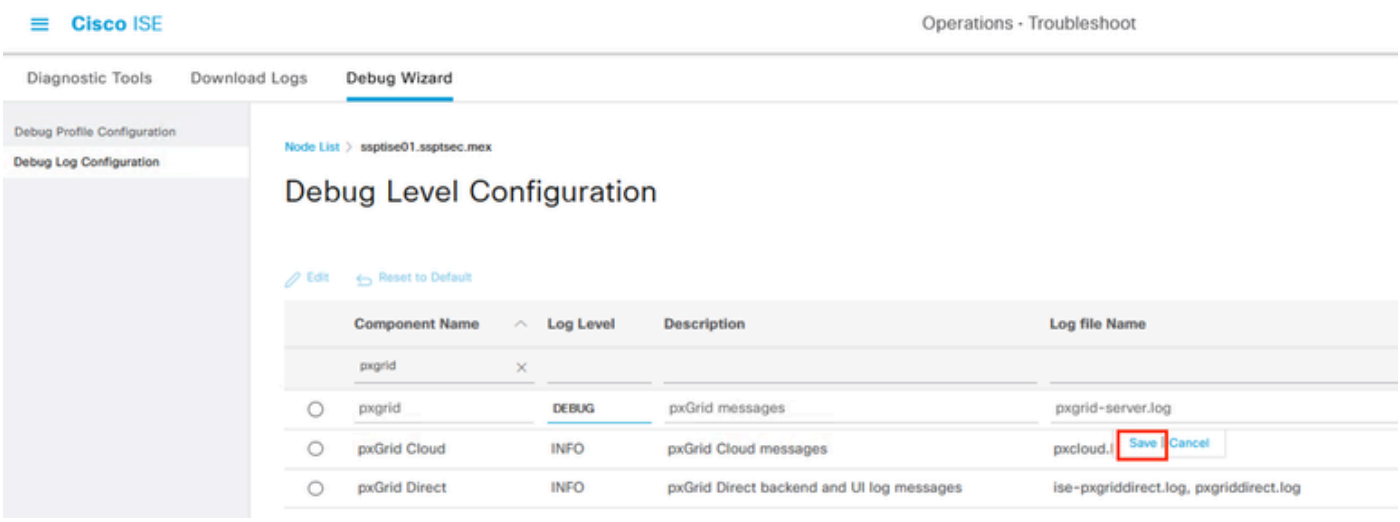
Communication PxGrid entre ISE et FMC.

Étape 17. Sur ISE, vous pouvez collecter des débogages liés au traitement de pxGrid. Naviguez dans le menu Operations > Troubleshoot > Debug Wizard > Debug Log Configuration. Sélectionnez le noeud ISE correspondant à analyser, puis Modifier.



Sélection d'un noeud à déboguer sur ISE.

Étape 18. Filtrez les composants affichés et définissez le niveau de consignation sur DEBUG. Cela débogue le composant pxGrid pour poursuivre l'analyse.Enregistrez la configuration.



Modification du composant pxGrid au niveau de débogage.

Reproduisez le comportement à analyser, puis continuez à analyser les journaux collectés sur le fichier pxgrid-server.log. Les autres journaux que vous pouvez consulter sur le noeud ISE pour le dépannage sont les suivants :

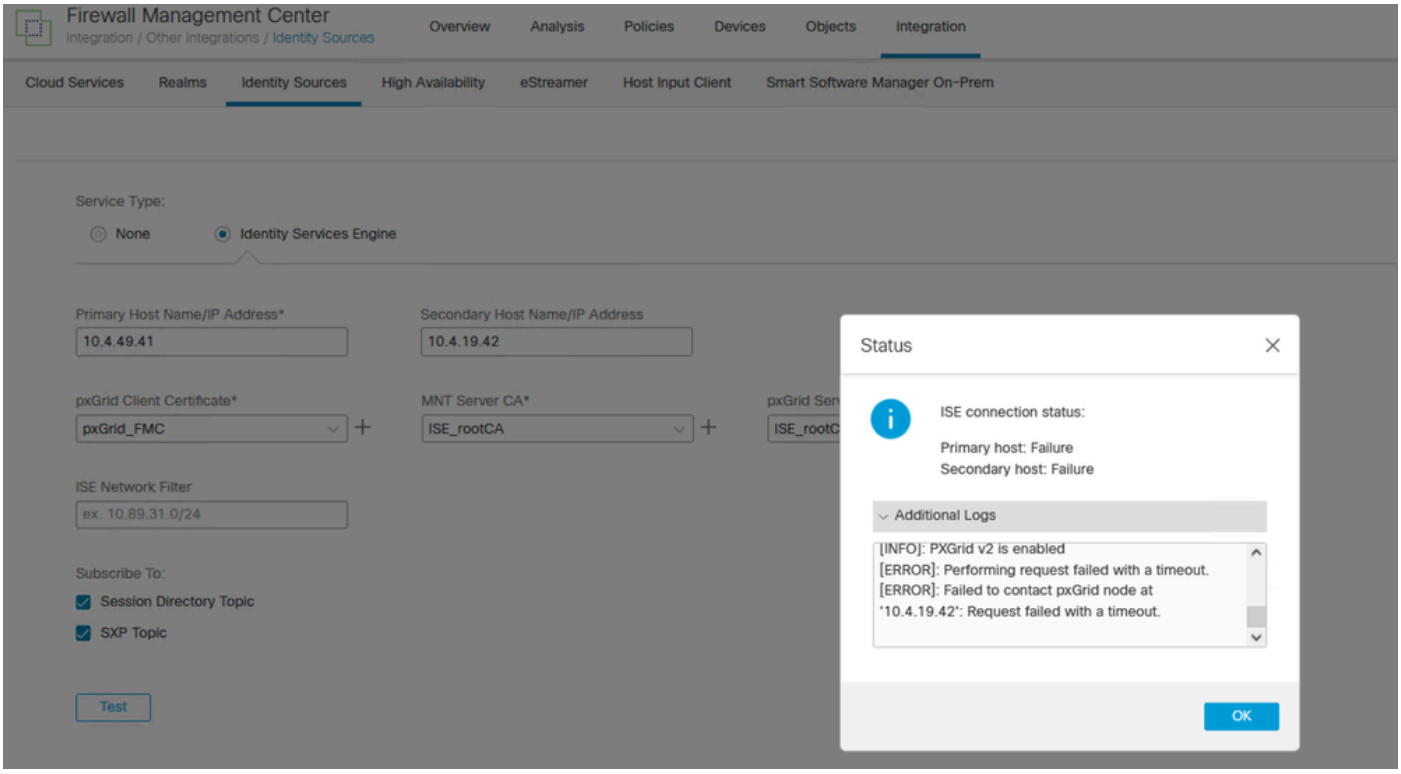
```
#show logging application | include pxgrid
ise-pxgriddirect.log
pxgrid/pxgrid-server.log
pxgrid/pxgrid-test.log
pxgrid/pxgrid_dbsync_summary.log
pxgrid/pxgrid_internal_dbsync_summary.log
pxgriddirect.log
```

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

Dans ce cas d'utilisation, le résultat associé au bouton FMC test pxGrid affiche le comportement suivant :



Échec de la connexion FMC pxGrid.

```
Primary host:

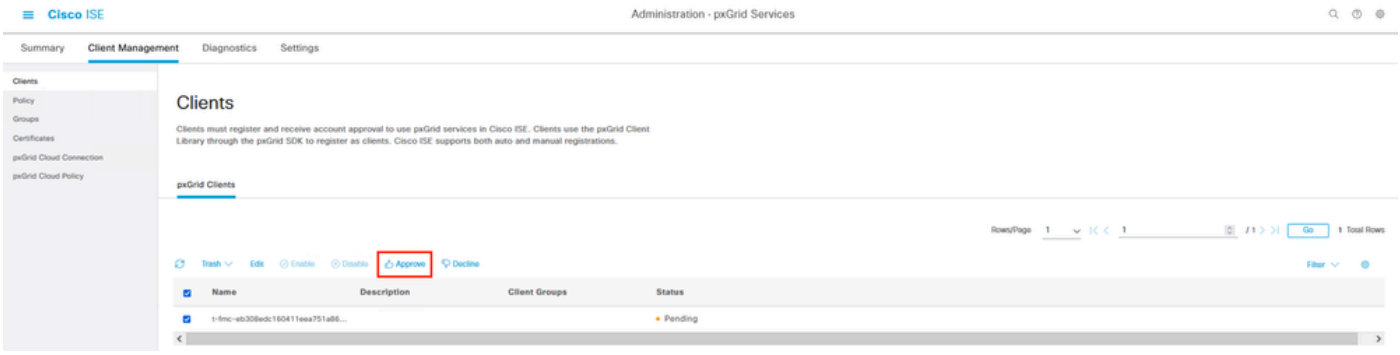
[INFO]: PXGrid v2 is enabled
[ERROR]: pxgrid 2.0: failed account activation. accountState=PENDING
[ERROR]: Failed to contact pxGrid node at '10.4.49.41': pxgrid2.0: Could not activate account

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, qui indique que le client pxGrid (FMC) est en attente d'approbation.

Étape 1. Cliquez sur le bouton Approuver et confirmez la sélection dans la fenêtre suivante et réessayez l'intégration. Cette fois, l'intégration est réussie.

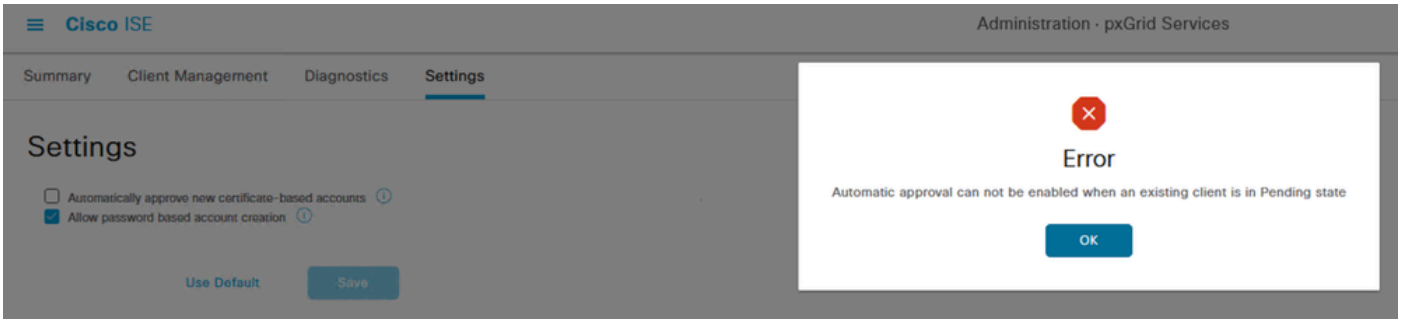


Le client FMC est en attente.



Confirmation de l'approbation du client pxGrid.

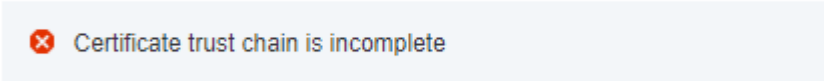
Si vous souhaitez activer l'approbation automatique des clients pxGrid basés sur un certificat, vous pouvez approuver/refuser les clients de la page précédente, car cette alarme peut s'afficher.



Erreur liée à l'approbation des clients pxGrid.

Chaîne de certificats ISE PxGrid incomplète

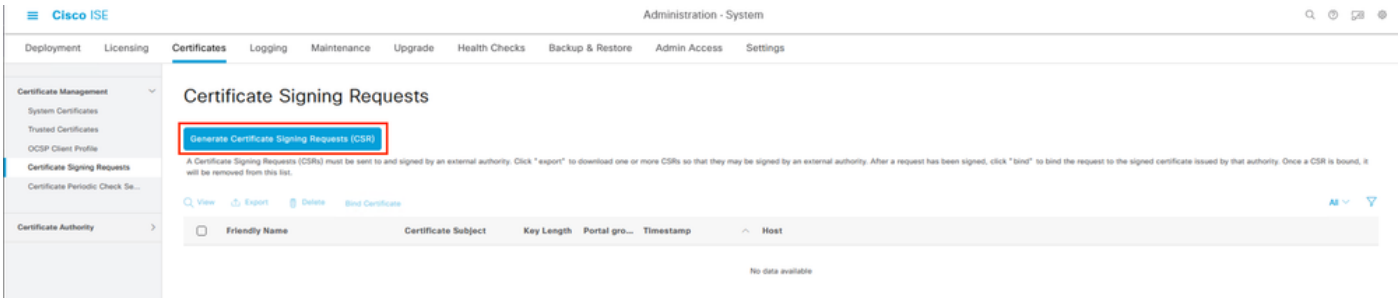
Étape 1. Dans ce scénario, si vous accédez au menu Administration > System > Certificate, sélectionnez le certificat pxGrid et sélectionnez l'option View. Si vous rencontrez un problème avec le certificat, ces erreurs peuvent se produire :



Erreur liée à la chaîne de certificats incomplète.

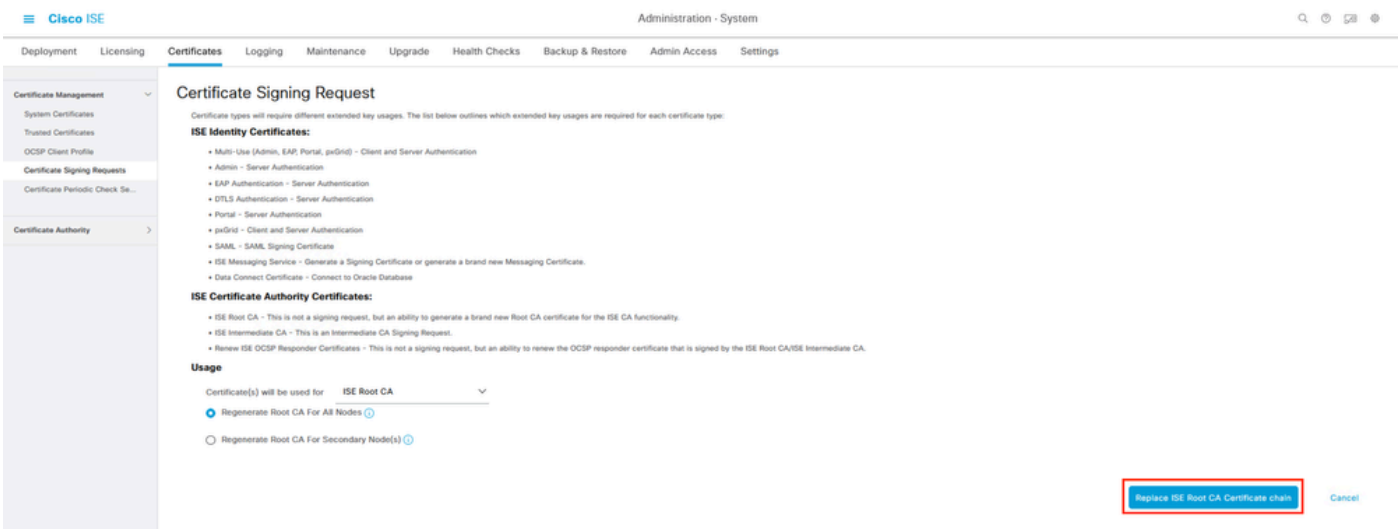
Étape 2. Vérifiez d'abord si l'autorité de certification racine ISE est terminée dans l'option View. Si un certificat est manquant dans la hiérarchie, vous pouvez émettre l'ensemble de l'autorité de certification racine de déploiement ISE.

Étape 3. Accédez au menu Administration > System > Certificates > Certificate Management > Certificate Signing Request (CSR) et sélectionnez le même bouton dans l'image suivante.



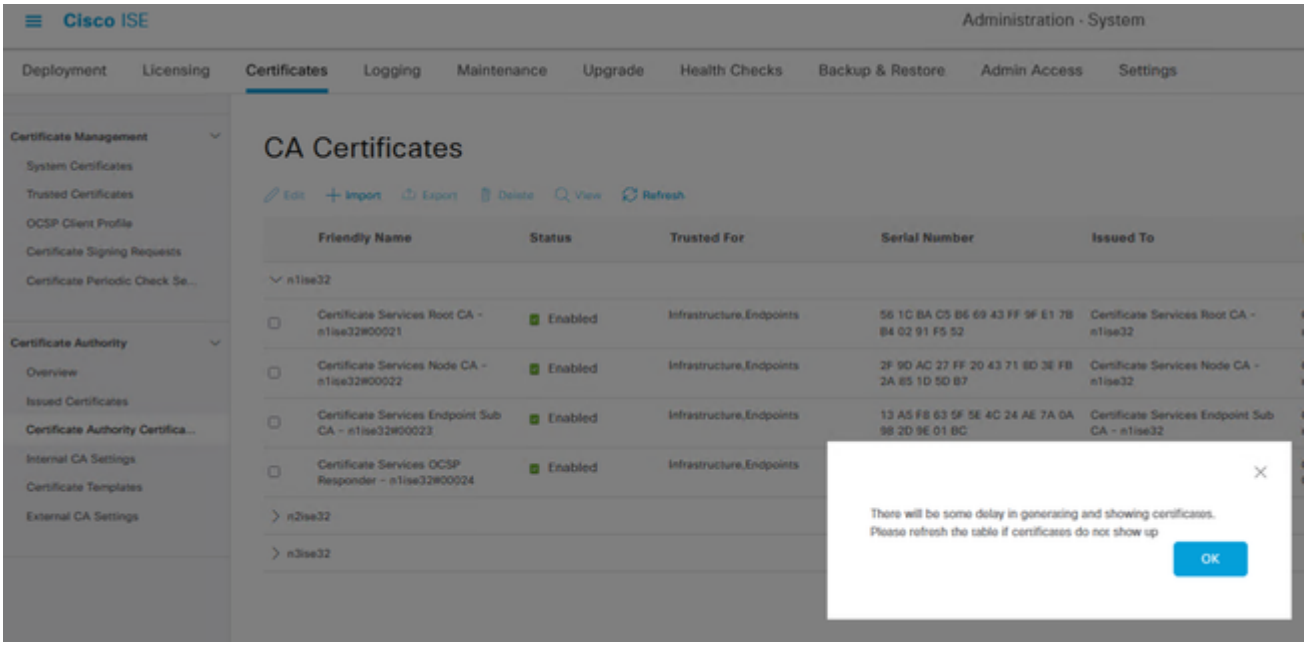
Génération d'un CSR sur ISE.

Étape 4. Dans ce menu, sélectionnez Usage ISE Root CA et régénérez l'autorité de certification racine ISE pour tous les noeuds. Continuez avec le bouton Remplacer la chaîne de certificats de CA racine ISE.



Configuration de la demande de signature de certificat.

Étape 5. Attendez que les certificats soient générés dans tous les noeuds de l’implémentation.Une fois l'opération terminée, l'ISE affiche la notification suivante.



Confirmation de la génération de certificats.

Étape 6. Confirmez si la chaîne de confiance de certificats pxGrid est terminée en sélectionnant l'option View de la page System Certificates.

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.