

Configuration de l'intégration ISE 2.4 et FMC

6.2.3 pxGrid

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configuration d'ISE](#)

[Étape 1. Activer les services pxGrid](#)

[Étape 2. Configurer ISE pour approuver tous les comptes basés sur des certificats pxGrid](#)

[Étape 3. Exporter les certificats d'administration ISE MNT et pxGrid CA](#)

[Configurer FMC](#)

[Étape 4. Ajouter un nouveau domaine à FMC](#)

[Étape 5. Générer un certificat CA FMC](#)

[Étape 6. Extraire le certificat et la clé privée du certificat généré à l'aide d'OpenSSL](#)

[Étape 7. Installer le certificat dans FMC](#)

[Étape 8. Importer le certificat FMC dans ISE](#)

[Étape 9. Configurer la connexion pxGrid sur FMC](#)

[Vérifier](#)

[Vérification dans ISE](#)

[Vérification dans FMC](#)

[Dépannage](#)

Introduction

Ce document décrit le processus de configuration pour l'intégration de l'ISE pxGrid version 2.4 et de FMC version 6.2.3.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- ISE 2.4
- FMC 6.2.3
- LDAP (Active Directory/Lightweight Directory Access Protocol)

Composants utilisés

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

logiciel suivantes :

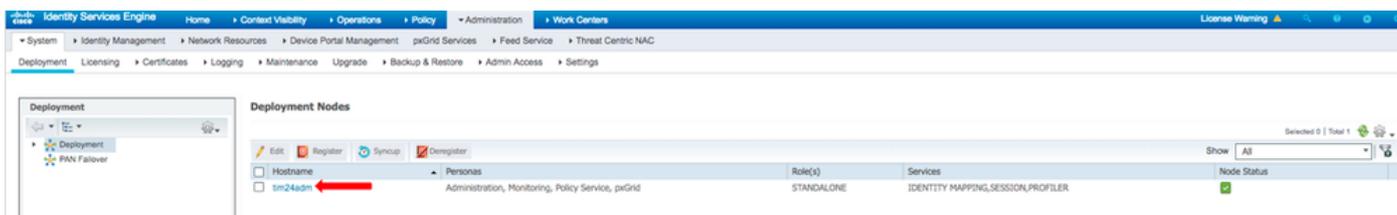
- ISE autonome 2.4
- FMCv 6.2.3
- Active Directory 2012R2
- Identity Services Engine (ISE) pxGrid version 2.4
- Firepower Management Center (FMC) version 6.2.3

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.

Configuration d'ISE

Étape 1. Activer les services pxGrid

1. Connectez-vous à l'interface utilisateur graphique d'administration ISE, accédez à **Administration > Deployment**.
2. Sélectionnez le noeud ISE à utiliser pour le profil pxGrid.



3. Activez le service pxGrid et cliquez sur **Save** comme indiqué dans l'image.

Deployment Nodes List > tim24adm

Edit Node

General Settings Profiling Configuration

Hostname
FQDN
IP Address
Node Type Identity Services Engine (ISE)

Role **STANDALONE** **Make Primary**

Administration

Monitoring

Role PRIMARY

Other Monitoring Node

Policy Service

Enable Session Services ⓘ

Include Node in Node Group None ⓘ

Enable Profiling Service ⓘ

Enable Threat Centric NAC Service ⓘ

Enable SXP Service ⓘ

Enable Device Admin Service ⓘ

Enable Passive Identity Service ⓘ

pxGrid ⓘ

Save Reset

4. Vérifiez que les services pxGrid s'exécutent à partir de l'interface de ligne de commande.

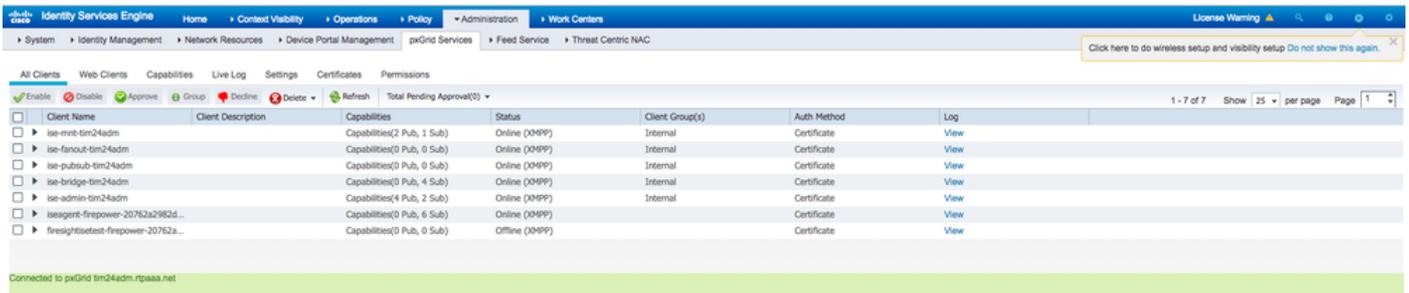
Remarque : le processus nécessite jusqu'à 5 minutes pour que les services pxGrid démarrent et déterminent l'état de haute disponibilité (HA) si plus d'un noeud pxGrid est utilisé.

5. Connectez SSH à l'interface de ligne de commande du noeud ISE pxGrid et vérifiez l'état de l'application.

```
# show application status ise | in pxGrid
pxGrid Infrastructure Service running 24062
pxGrid Publisher Subscriber Service running 24366
pxGrid Connection Manager running 24323
pxGrid Controller running 24404
#
```

6. Accédez à l'interface utilisateur graphique de l'administrateur ISE et vérifiez que les services sont en ligne et fonctionnent. Accédez à **Administration > pxGrid Services**.

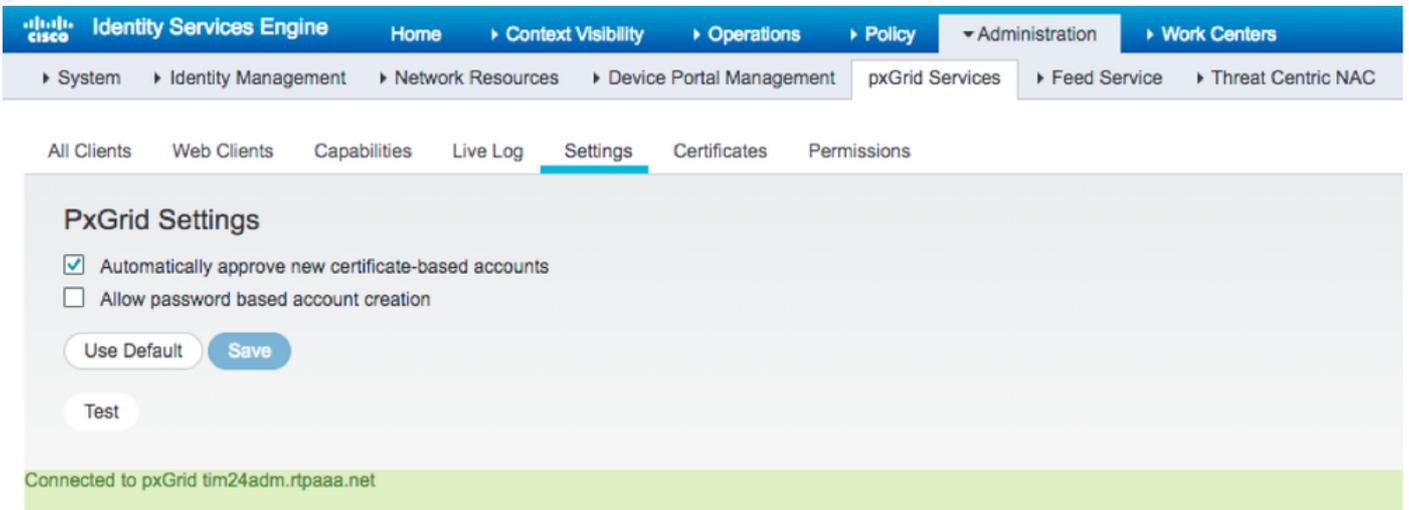
7. En bas de la page, ISE affiche **Connected to pxGrid <pxGrid node FQDN>**.



Étape 2. Configurer ISE pour approuver tous les comptes basés sur des certificats pxGrid

1. Accédez à **Administration > pxGrid Services > Settings**.

2. Cochez la case « Approuver automatiquement les nouveaux comptes basés sur un certificat » et cliquez sur **Enregistrer**.



Remarque : si cette option n'est pas activée, l'administrateur doit approuver manuellement la connexion FMC à ISE.

Étape 3. Exporter les certificats d'administration ISE MNT et pxGrid CA

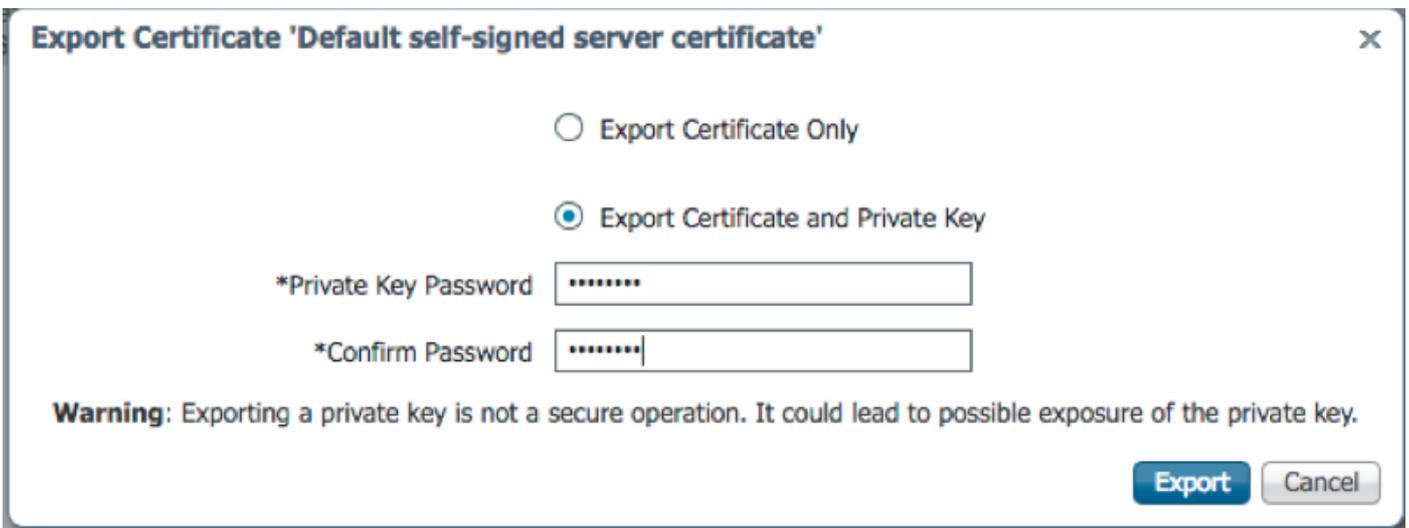
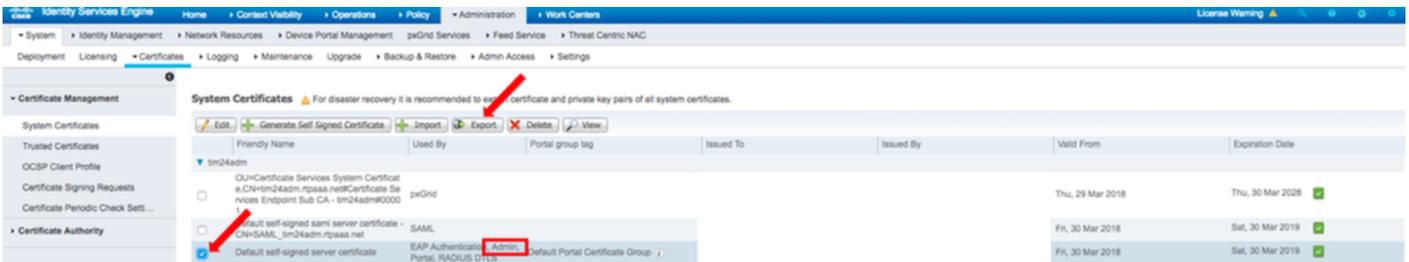
1. Accédez à **Administration > Certificats > Certificats système**.

2. Développez le noeud Surveillance principale (MNT) s'il n'est pas activé sur le noeud Administration principale.

3. Sélectionnez le certificat avec le champ « Utilisé par l'administrateur ».

Remarque : ce guide utilise le certificat auto-signé ISE par défaut pour l'administration. Si vous utilisez un certificat d'administration signé par une autorité de certification, exportez l'autorité de certification racine qui a signé le certificat d'administration sur le noeud MNT ISE.

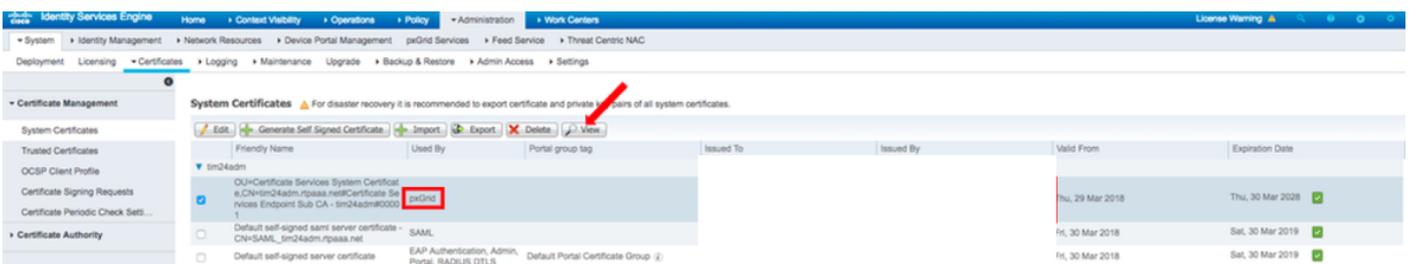
4. Cliquez sur **Exporter**.
5. Choisissez l'option Exporter le certificat et la clé privée.
6. Définissez une clé de chiffrement.
7. **Exportez et enregistrez** le fichier comme indiqué dans l'image.



9. Revenez à l'écran ISE System Certificates (Certificats système ISE).
10. Déterminez le champ Émis par sur le certificat avec l'utilisation « pxGrid » dans la colonne Utilisé par.

Remarque : dans les versions antérieures d'ISE, il s'agissait d'un certificat auto-signé, mais à partir de la version 2.2, ce certificat est émis par la chaîne d'autorité de certification ISE interne par défaut.

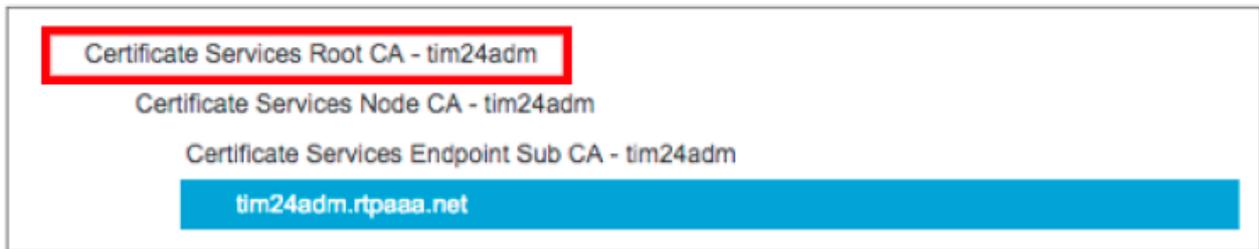
11. Sélectionnez le certificat et cliquez sur **Afficher** comme indiqué dans l'image.



12. Déterminez le certificat de niveau supérieur (racine). Dans ce cas, il s'agit de **"Certificate Services Root CA - tim24adm"**.

13. Fermez la fenêtre d'affichage des certificats comme indiqué dans l'image.

Certificate Hierarchy



tim24adm.rtpaaa.net
Issued By : Certificate Services Endpoint Sub CA - tim24adm
Expires : Thu, 30 Mar 2028 14:17:12 EDT

Certificate status is good

Details

Issued To

Common Name (CN)

Organization Unit (OU) **Certificate Services System Certificate**

Organization (O)

City (L)

State (ST)

Country (C)

Serial Number **58:2A:91:45:E8:23:42:74:98:53:06:94:33:9E:AD:83**

Close

14. Développez le menu ISE Certificate Authority.

15. Sélectionnez **Certificats d'autorité de certification**.

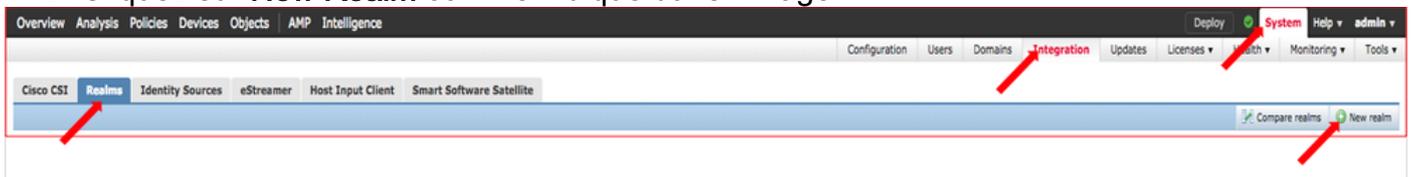
16. Sélectionnez le certificat racine identifié et cliquez sur **Exporter**. Enregistrez ensuite le certificat d'autorité de certification racine pxGrid comme indiqué dans l'image.

Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Expiration Status
Certificate Services Endpoint Sub CA - sm24adm#00003	Enabled	Infrastructure.Endpoints	32 D2 72 55 A9 7D 40 13 8F 2A EF CF 0D 1C 41 AB	Certificate Services Endpoint Sub CA - sm24adm	Certificate Services Node CA - sm24adm	Thu, 29 Mar 2018	Thu, 30 Mar 2028	✓
Certificate Services Root CA - sm24adm#00001	Enabled	Infrastructure.Endpoints	36 67 74 15 A6 AB 4F EB B7 46 87 37 1A A6 56	Certificate Services Root CA - sm24adm	Certificate Services Root CA - sm24adm	Thu, 29 Mar 2018	Thu, 30 Mar 2028	✓
Certificate Services Node CA - sm24adm#00002	Enabled	Infrastructure.Endpoints	30 1A 22 E7 AA E5 45 35 8C 65 7B EE 53 09 34 3E	sm24adm	sm24adm	Thu, 29 Mar 2018	Thu, 30 Mar 2028	✓
Certificate Services OCSP Responder - sm24adm#00004	Enabled	Infrastructure.Endpoints	74 C2 35 B8 32 6A 40 0F AC C8 D9 BB 91 DC 07 D7	Certificate Services OCSP Responder - sm24adm	Certificate Services Node CA - sm24adm	Thu, 29 Mar 2018	Thu, 30 Mar 2023	✓

Configurer FMC

Étape 4. Ajouter un nouveau domaine à FMC

1. Accédez à l'interface utilisateur graphique de FMC et accédez à **System > Integration > Realms**.
2. Cliquez sur **New Realm** comme indiqué dans l'image.



3. Remplissez le formulaire et cliquez sur le bouton Tester la connexion à Active Directory (AD).

Remarque : le nom d'utilisateur de la jointure Active Directory doit être au format UPN (User Principal Name), sinon le test échoue.

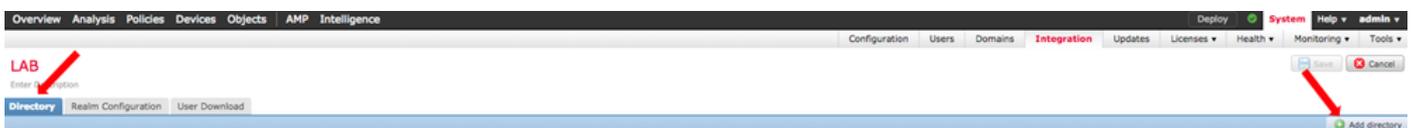
4. Si le test de la jointure Active Directory réussit, cliquez sur **OK**.

Add New Realm

Name *	ISEpxGrid	
Description	Realm for use with pxGrid	
Type *	AD	
AD Primary Domain *		ex: domain.com
AD Join Username		ex: user@domain
AD Join Password	<input type="button" value="Test AD Join"/>
Directory Username *	admin	ex: user@domain
Directory Password *	
Base DN *	CN=Users,DN=rtpaaa,DN=net	ex: ou=user,dc=cisco,dc=com
Group DN *	DN=rtpaaa,DN=net	ex: ou=group,dc=cisco,dc=com
Group Attribute	Member	

* Required Field

5. Cliquez sur l'onglet **Répertoire**, puis cliquez sur **Ajouter un répertoire** comme indiqué dans l'image.



6. Configurez IP/Hostname et testez la connexion.

Remarque : si le test échoue, vérifiez les informations d'identification dans l'onglet Configuration du domaine.

7. Cliquez sur **OK**.

Edit directory

Hostname / IP Address

Port

Encryption STARTTLS LDAPS None

SSL Certificate

Status

 Test connection succeeded

8. Cliquez sur l'onglet **Téléchargement utilisateur**.



9. Si cette option n'est pas déjà sélectionnée, activez le téléchargement des utilisateurs et des groupes

10. Cliquez sur Télécharger maintenant

LAB

Enter Description

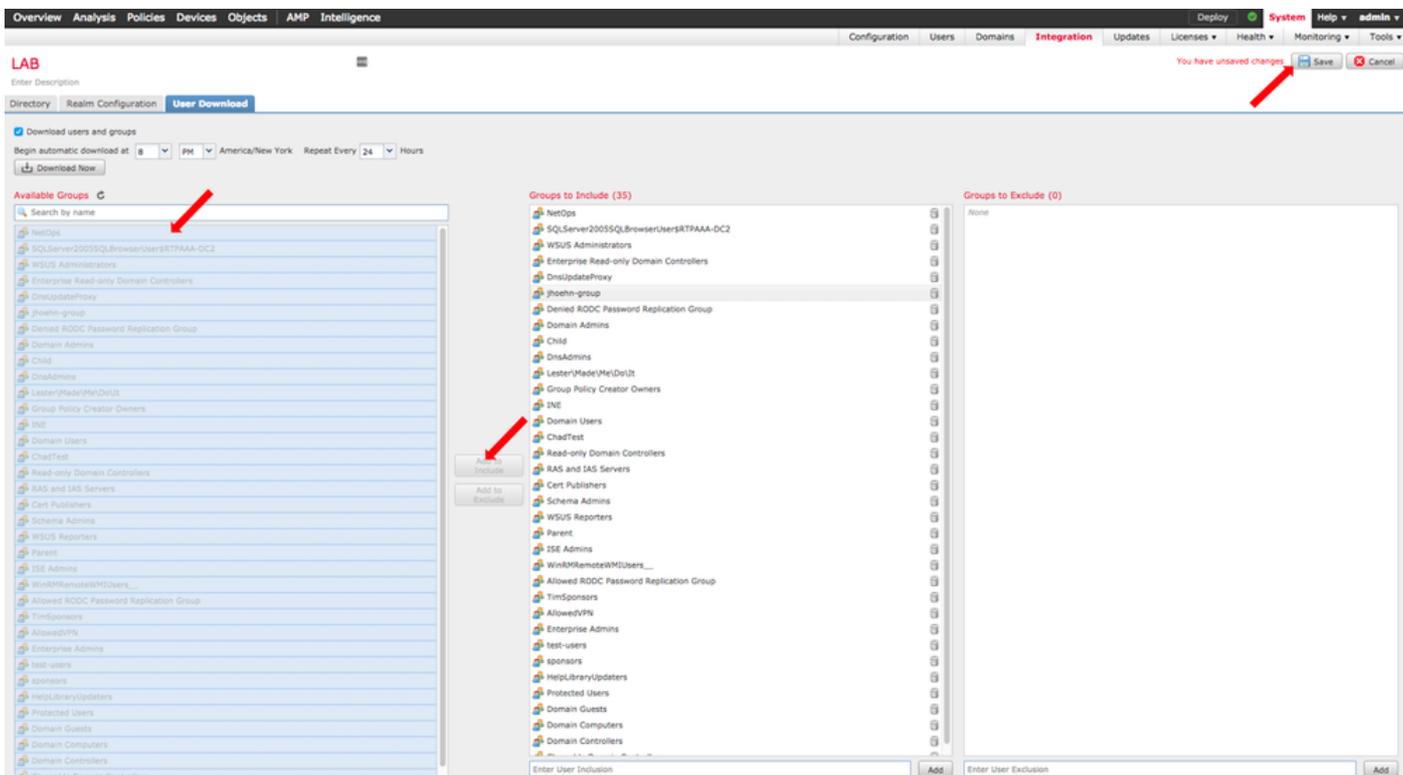
Directory Realm Configuration **User Download**

Download users and groups

Begin automatic download at America/New York Repeat Every Hours

11. Une fois la liste renseignée, ajoutez les groupes souhaités et sélectionnez **Ajouter à inclure**.

12. Enregistrez la **configuration du domaine**.

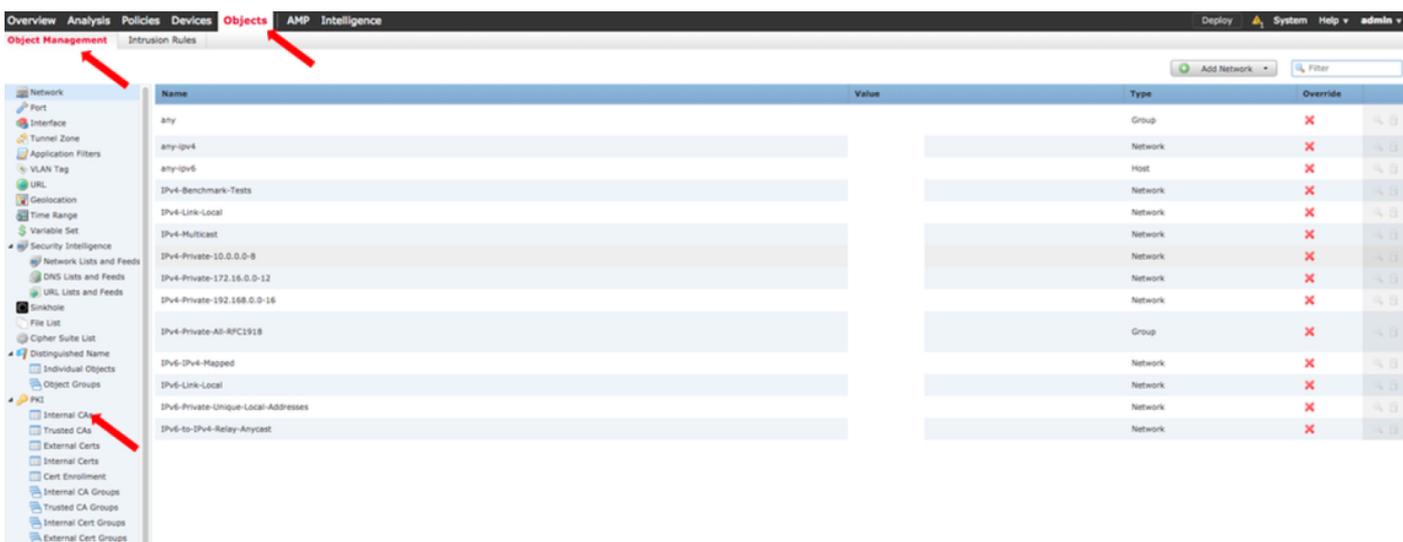


13. Activez l'état du domaine.



Étape 5. Générer un certificat CA FMC

1. Accédez à **Objets > Gestion des objets > Autorités de certification internes** comme indiqué dans l'image.



2. Cliquez sur **Generate CA**.

3. Remplissez le formulaire et cliquez sur **Generate self-signed CA**.



Generate Internal Certificate Authority

Name:

Country Name (two-letter code):

State or Province:

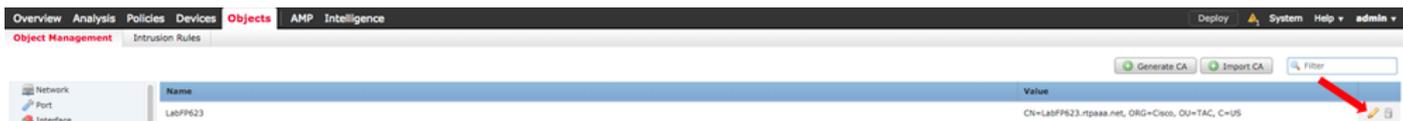
Locality or City:

Organization:

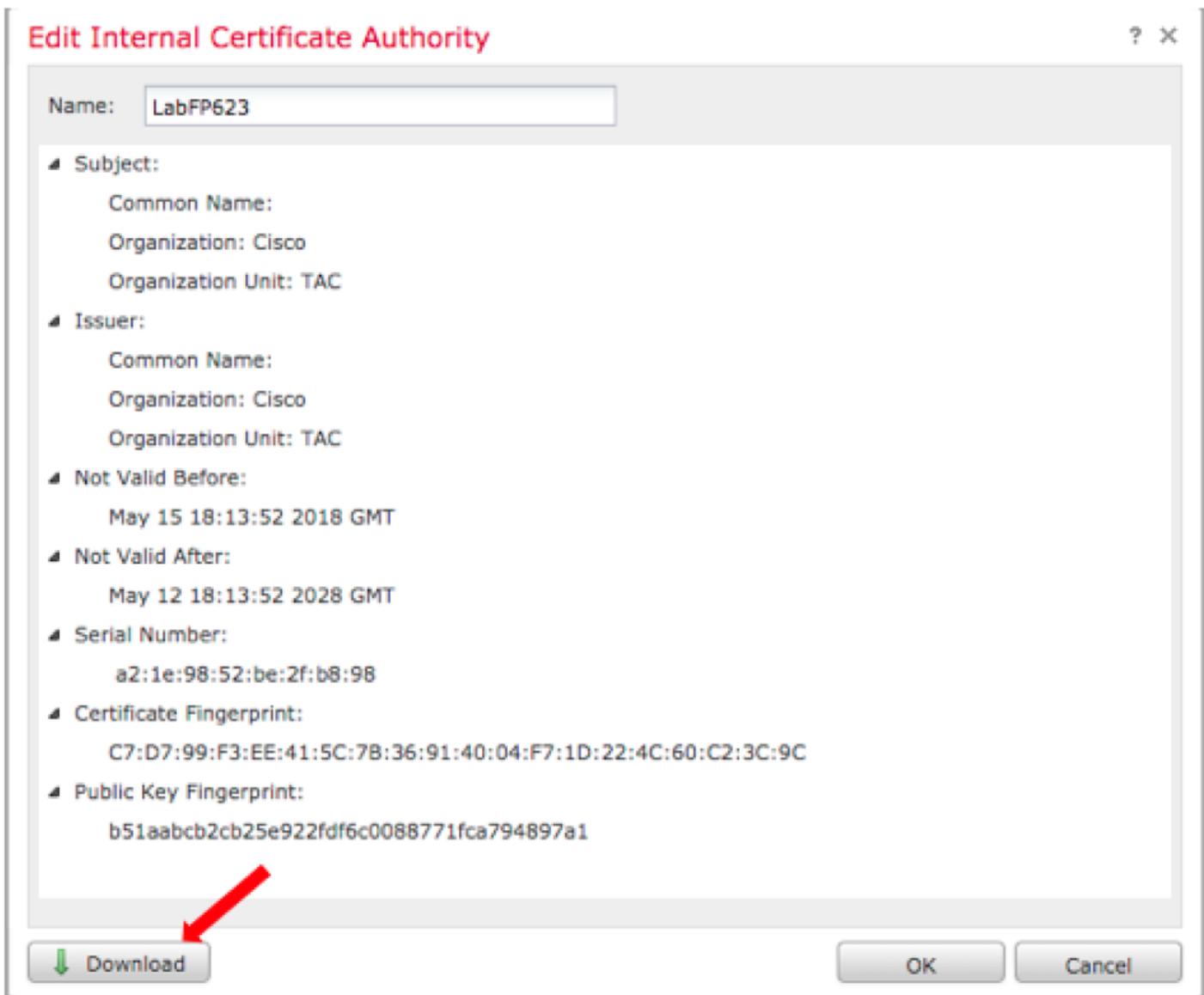
Organizational Unit (Department):

Common Name:

4. Une fois la génération terminée, cliquez sur le crayon à droite du certificat CA généré, comme illustré dans l'image.



5. Cliquez sur **Télécharger**.



6. Configurez et confirmez le mot de passe de cryptage, puis cliquez sur **OK**.

7. Enregistrez le fichier PKCS (Public-Key Cryptography Standards) p12 dans votre système de fichiers local.

Étape 6. Extraire le certificat et la clé privée du certificat généré à l'aide d'OpenSSL

Ceci est fait soit sur la racine du FMC, soit sur n'importe quel client capable de commandes OpenSSL. Cet exemple utilise un shell Linux standard.

1. Utilisez **openssl** afin d'extraire le certificat (CER) et la clé privée (PVK) du fichier p12.

2. Extrayez le fichier CER, puis configurez la clé d'exportation de certificat à partir de la génération de certificat sur FMC.

```
~$ openssl pkcs12 -nokeys -clcerts -in <filename.p12> -out <filename.cer>
Password:
Last login: Tue May 15 18:46:41 UTC 2018
Enter Import Password:
MAC verified OK
```

3. Extrayez le fichier PVK, configurez la clé d'exportation de certificat, puis définissez une

nouvelle phrase de passe PEM et confirmez.

```
~$ openssl pkcs12 -nocerts -in <filename.p12> -out <filename.pvk>
```

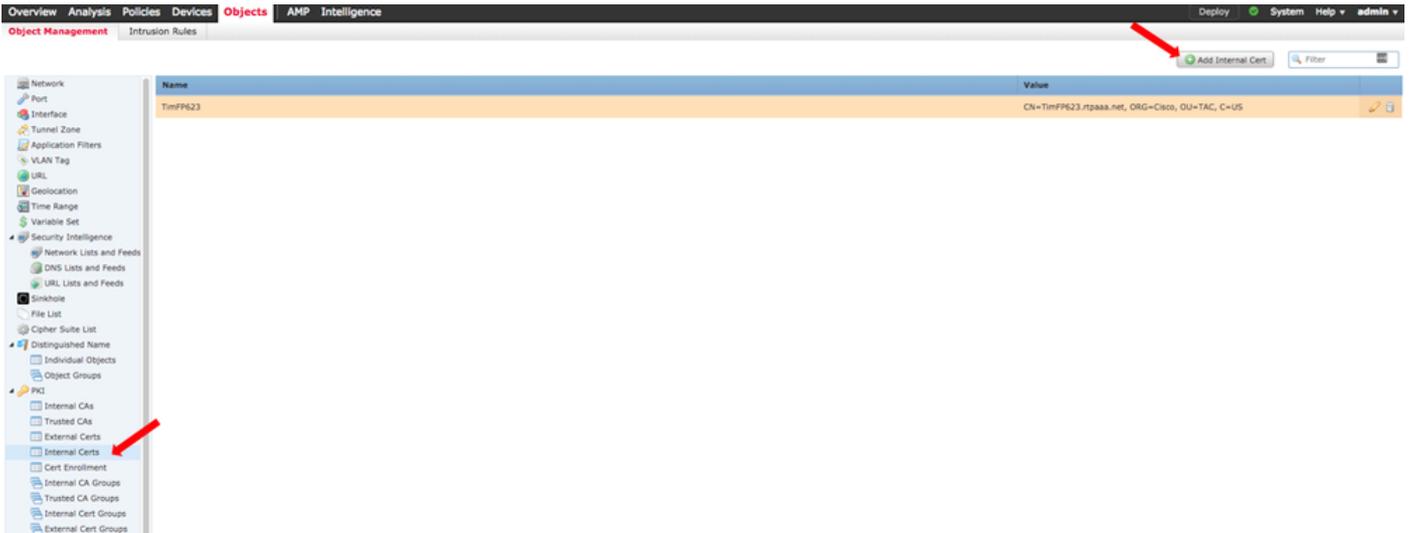
Password: Last login: Tue May 15 18:46:41 UTC 2018 Enter Import Password: MAC verified OK

4. Cette phrase PEM est nécessaire à l'étape suivante.

Étape 7. Installer le certificat dans FMC

1. Accédez à **Objets > Gestion des objets > PKI > Certs internes**.

2. Cliquez sur **Add Internal Cert** comme indiqué dans l'image.



3. Configurez un nom pour le certificat interne.

4. Accédez à l'emplacement du fichier CER et sélectionnez-le. Une fois que les données de certificat sont renseignées, sélectionnez la seconde.

5. Parcourez **Option** et sélectionnez le fichier PVK.

6. Supprimez tous les "attributs de sac" et toutes les valeurs de fin de la section PVK. Le PVK commence par **-----BEGIN ENCRYPTED PRIVATE KEY-----** et se termine par **-----END ENCRYPTED PRIVATE KEY-----**.

Remarque : vous ne pouvez pas cliquer sur **OK** si le texte PVK comporte des caractères en dehors des traits d'union de début et de fin.

7. Cochez la case **Chiffré** et configurez le mot de passe créé lors de l'exportation du PVK à l'étape 6.

8. Cliquez sur **OK**.

Add Known Internal Certificate



Name:

Certificate Data or, choose a file:

```
-----BEGIN CERTIFICATE-----
MIIDFTCCAmWgAwIBAgIJAKIemFK+L7iYMA0GCSqGSIb3DQEBCwUAMGQxCzAJBgNV
BAYTAIVTMQswCQYDVQQIDAJOQzEMMAoGA1UEBwwDUIRQM4wDAYDVQQKDAVDAxNj
bzEMMAoGA1UECwwDVEFDMRwwGgYDVQQDDDBNMYWJGUDYyMy5ydHBhYWEubmV0MB4X
DTE4MDUxNTE4MTM1MlloXDTI4MDUxMjE4MTM1MlowZDELMAkGA1UEBhMCVVMx
BgNVBAGMAK5DMQwwCgYDVQQHDANSVFAXDjAMBgNVBAoMBUNpc2NmMQwwCgYDVQQL
DANUQUxHDAaBgNVBAMME0xhYkZQNjIzLnJ0cGFhYS5uZXQwgwEIMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQMjtS5UIFIZkZK/TSGtkOCmuivTK5kk1WzAy6
D7Gm/c69cXw/VfIPWnSBzhEkiRTyspmTMdyf/4TJvUmUH60h1O8/8dZeqJOzbjon
-----
```

Key or, choose a file:

Bag Attributes
localKeyID: C7 D7 99 F3 EE 41 5C 7B 36 91 40 04 F7 1D 22 4C 60 C2 3C 9C ← DELETE
Key Attributes: <no attributes="">

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFDjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQI5uV3MsiHZsICAggA
MBQGCCqGSIb3DQMHBAAhgGVm1+xHLIASCBMjjJxkffXUNUcdB22smybvWotwbcRrt
xL0qjEStmwuyExVp+TWC3AyIJN1DE7/rRssjRAqsnSOxIvDGmg0dVsvnbqZwjFP
74POu/O2Vy99iFoVgW2q9DyXyL/h64TH9CZtwLKIOGOeEunNKpamDnpfyN8QC4DC
fXvNZ8yNG4HrEcFmnnij0EwJ0QT8Jn5gAUj+AIPMe32zPqwocCRNYrRXMVM9+Jwp
-----
```

Encrypted, and the password is:

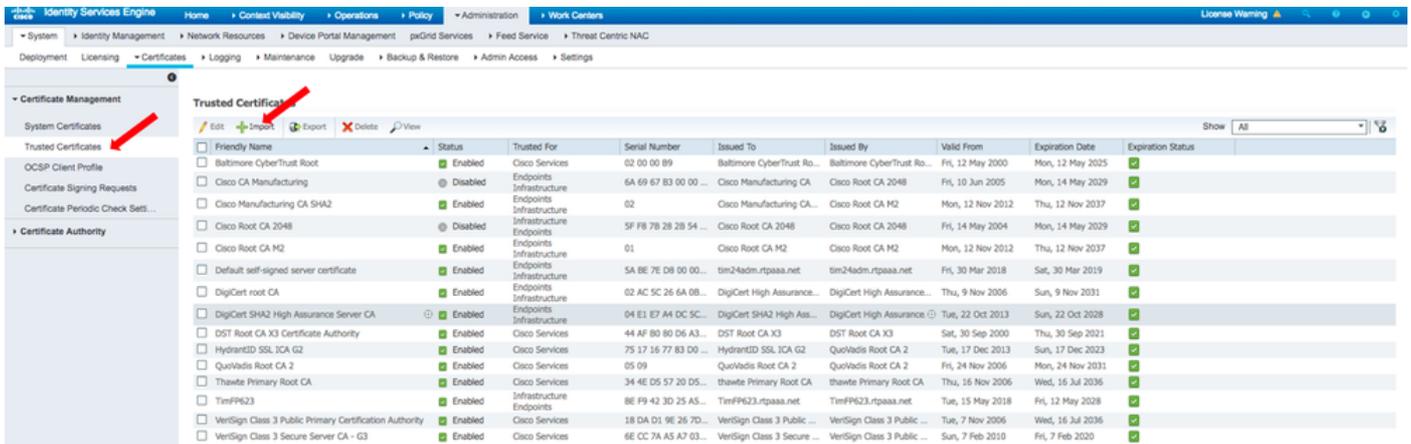
```
cfCJU2QGI4jT0SorN4u2Lk+S+Qd1s7Ii2wIQMWKPI2R9UGv1tyM6HTPCGoCo6VDI
acCICUasecVrYY081GKTVVJ3bWgWfPtR3OH12YCA2whcCKcG50MByB4tjhHN036q
O/g=
-----END ENCRYPTED PRIVATE KEY-----
</no> ← DELETE
```

Encrypted, and the password is:

Étape 8. Importer le certificat FMC dans ISE

1. Accédez à l'interface utilisateur graphique d'ISE et sélectionnez Administration > System > Certificates > Trusted Certificates.

2. Cliquez sur Importer.



3. Cliquez sur **Choose File** et sélectionnez le fichier FMC CER sur votre système local.

Facultatif : configurez un nom convivial.

4. Vérifiez **Trust** pour l'authentification au sein d'ISE.

Facultatif : configurez une description.

5. Cliquez sur **Submit** comme indiqué dans l'image.

Import a new Certificate into the Certificate Store

* Certificate File TZfpcert.cer

Friendly Name

Trusted For:

Trust for authentication within ISE

Trust for client authentication and Syslog

Trust for authentication of Cisco Services

Validate Certificate Extensions

Description

Étape 9. Configurer la connexion pxGrid sur FMC

1. Accédez à **System > Integration > Identity Sources** comme indiqué dans l'image.



2. Cliquez sur **ISE**.

3. Configurez l'adresse IP ou le nom d'hôte du noeud ISE pxGrid.

4. Sélectionnez le signe + à droite de l'autorité de certification pxGrid Server.

5. Nommez le fichier d'autorité de certification du serveur, puis accédez à l'autorité de certification de signature racine pxGrid collectée à l'étape 3. et cliquez sur **Enregistrer**.

6. Sélectionnez le signe + à droite de l'autorité de certification du serveur MNT.

7. Nommez le fichier d'autorité de certification du serveur, puis accédez au certificat Admin collecté à l'étape 3. et cliquez sur **Enregistrer**.

8. Sélectionnez le fichier **FMC CER** dans la liste déroulante.

Identity Sources

Service Type: None Identity Services Engine User Agent

Primary Host Name/IP Address *

Secondary Host Name/IP Address

pxGrid Server CA * +

MNT Server CA * +

FMC Server Certificate * +

ISE Network Filter ex. 10.89.31.0/24, 192.168.8.0/24, ...

* Required Field

9. Cliquez sur **Test**.

10. Si le test réussit, cliquez sur **OK**, puis sur **Save** en haut à droite de l'écran.

Status

 ISE connection status:
Primary host: Success

[Additional Logs](#)

Remarque : lorsque vous exécutez deux noeuds ISE pxGrid, il est normal qu'un hôte affiche Success et un autre Failure, car pxGrid ne s'exécute activement que sur un noeud ISE à la fois. Cela dépend de la configuration si l'hôte principal peut afficher Échec et l'hôte secondaire, Succès. Tout dépend du noeud dans ISE qui est le noeud pxGrid actif.

Vérifier

Vérification dans ISE

1. Ouvrez l'interface utilisateur graphique d'ISE et accédez à Administration > pxGrid Services.

En cas de réussite, deux connexions firepower sont répertoriées dans la liste des clients. Un pour le FMC réel (iseagent-hostname-33bytes) et un pour le périphérique de test (firesightisetest-hostname-33bytes).

Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method	Log
		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate	View
		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View
		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View
		Capabilities(0 Pub, 4 Sub)	Online (XMPP)	Internal	Certificate	View
		Capabilities(4 Pub, 7 Sub)	Online (XMPP)	Internal	Certificate	View
		Capabilities(0 Pub, 6 Sub)	Online (XMPP)		Certificate	View
		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)		Certificate	View

La connexion iseagent-firepower affiche six (6) sous-réseaux et apparaît en ligne.

La connexion firesightisetest-firepower affiche zéro (0) sous-réseau et apparaît hors ligne.

La vue étendue du client iseagent-firepower affiche les six abonnements.

Capability Name	Capability Version	Messaging Role	Message Filter
<input type="radio"/> AdaptiveNetworkControl	1.0	Sub	
<input type="radio"/> Core	1.0	Sub	
<input type="radio"/> EndpointProfileMetaData	1.0	Sub	
<input type="radio"/> EndpointProtectionService	1.0	Sub	
<input type="radio"/> SessionDirectory	1.0	Sub	
<input type="radio"/> TrustSecMetaData	1.0	Sub	

Remarque : en raison du bogue Cisco [IDCSCvo75376](#) il existe une limitation de nom d'hôte et le téléchargement en masse échoue. Le bouton de test du FMC affiche un échec de connectivité. Cela concerne 2.3p6, 2.4p6 et 2.6. La recommandation actuelle est d'exécuter 2.3 patch 5 ou 2.4 patch 5 jusqu'à ce qu'un patch officiel soit publié.

Vérification dans FMC

1. Ouvrez l'interface utilisateur graphique de FMC et accédez à Analysis > Users > Active Sessions.

Toutes les sessions actives publiées via la fonctionnalité d'annuaire de sessions dans ISE sont affichées dans le tableau Sessions actives sur FMC.

Login Time	Last Seen	User	Authentication Type	Current IP	Realm	Username	First Name	Last Name	E-Mail	Department	Phone	Discoverx Application	Device
2018-05-15 13:28:21	2018-05-15 13:27:36	xiao.yao (LAB\yao@lab.LDAP)	Passive Authentication		LAB					users (doaaa)		<input type="checkbox"/> LDAP	firepower
2018-05-15 12:35:54	2018-05-15 12:35:54	admin.admin (LAB\admin.LDAP)	Passive Authentication		LAB					users (doaaa)		<input type="checkbox"/> LDAP	firepower
2018-05-15 11:27:14	2018-05-15 11:27:14	tom (LAB\tom.LDAP)	Passive Authentication		LAB					users (doaaa)		<input type="checkbox"/> LDAP	firepower
2018-05-15 11:20:30	2018-05-15 11:20:30	clark.kent (LAB\jwoerman.LDAP)	Passive Authentication		LAB					users (doaaa)		<input type="checkbox"/> LDAP	firepower

En mode sudo de l'interface de ligne de commande FMC, la session `adi_cli` affiche les

informations de session utilisateur envoyées par ISE à FMC.

```
ssh admin@<FMC IP ADDRESS>
Password:
Last login: Tue May 15 19:03:01 UTC 2018 from dhcp-172-18-250-115.cisco.com on ssh
Last login: Wed May 16 16:28:50 2018 from dhcp-172-18-250-115.cisco.com
```

Copyright 2004-2018, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

```
Cisco Fire Linux OS v6.2.3 (build 13)
Cisco Firepower Management Center for VMWare v6.2.3 (build 83)
```

```
admin@firepower:~$ sudo -i
Password:
Last login: Wed May 16 16:01:01 UTC 2018 on cron
root@firepower:~# adi_cli session
```

```
received user session: username tom, ip ::ffff:172.18.250.148, location_ip ::ffff:10.36.150.11,
realm_id 2, domain rtpaaa.net, type Add, identity Passive.
received user session: username xiayao, ip ::ffff:10.36.148.98, location_ip ::, realm_id 2,
domain rtpaaa.net, type Add, identity Passive.
received user session: username admin, ip ::ffff:10.36.150.24, location_ip ::, realm_id 2,
domain rtpaaa.net, type Add, identity Passive.
received user session: username administrator, ip ::ffff:172.18.124.200, location_ip ::,
realm_id 2, domain rtpaaa.net, type Add, identity Passive.
```

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

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.