Configurez la PIC ISE 2.2 avec le fournisseur du Répertoire actif WMI

Contenu

Introduction

Ce document décrit comment configurer et dépanner le déploiement passif du connecteur d'identité de Cisco Identity Services Engine (PIC ISE) avec le fournisseur de Windows Management Instrumentation de Répertoire actif (AD WMI). La PIC ISE est une version légère ISE qui se concentre sur les caractéristiques passives d'ID.

La PIC ISE est une solution simple d'ID pour tout le dossier de sécurité Cisco qui utilise l'identité

passive seulement. Il signifie que l'autorisation ou les stratégies ne peut pas être configurée sur la PIC ISE. Il prend en charge différents fournisseurs (agents, WMI, Syslog, API) et peut être intégré par l'intermédiaire du REPOS API. Il a des capacités de questionner des points finaux (est-il l'utilisateur ouvert une session ? Est le point final toujours connecté ?)

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Engine de gestion d'identité de Cisco
- Microsoft Active Directory
- Microsoft WMI

Composants utilisés

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

- Version 2.2.0.470 passive de connecteur d'identité d'engine de gestion d'identité de Cisco
- Microsoft Windows 7 Service Pack 1
- Microsoft Windows Server 2012 r2

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

La quantité maximale de Noeuds dans le déploiement PIC ISE est 2. Cet exemple affiche comment configurer le déploiement PIC ISE pour la Haute disponibilité, les virtual machine de SO2 (VMs) sont utilisés. Dans un déploiement PIC ISE, les Noeuds peuvent avoir des rôles : Primaire et secondaire. Dans ce seulement un noeud peut être primaire à la fois et des rôles peuvent seulement être changés manuellement par le GUI. En cas de panne primaire toutes les caractéristiques fonctionnent toujours sur secondaire excepté UI. Seulement la promotion manuelle à primaire active l'UI.

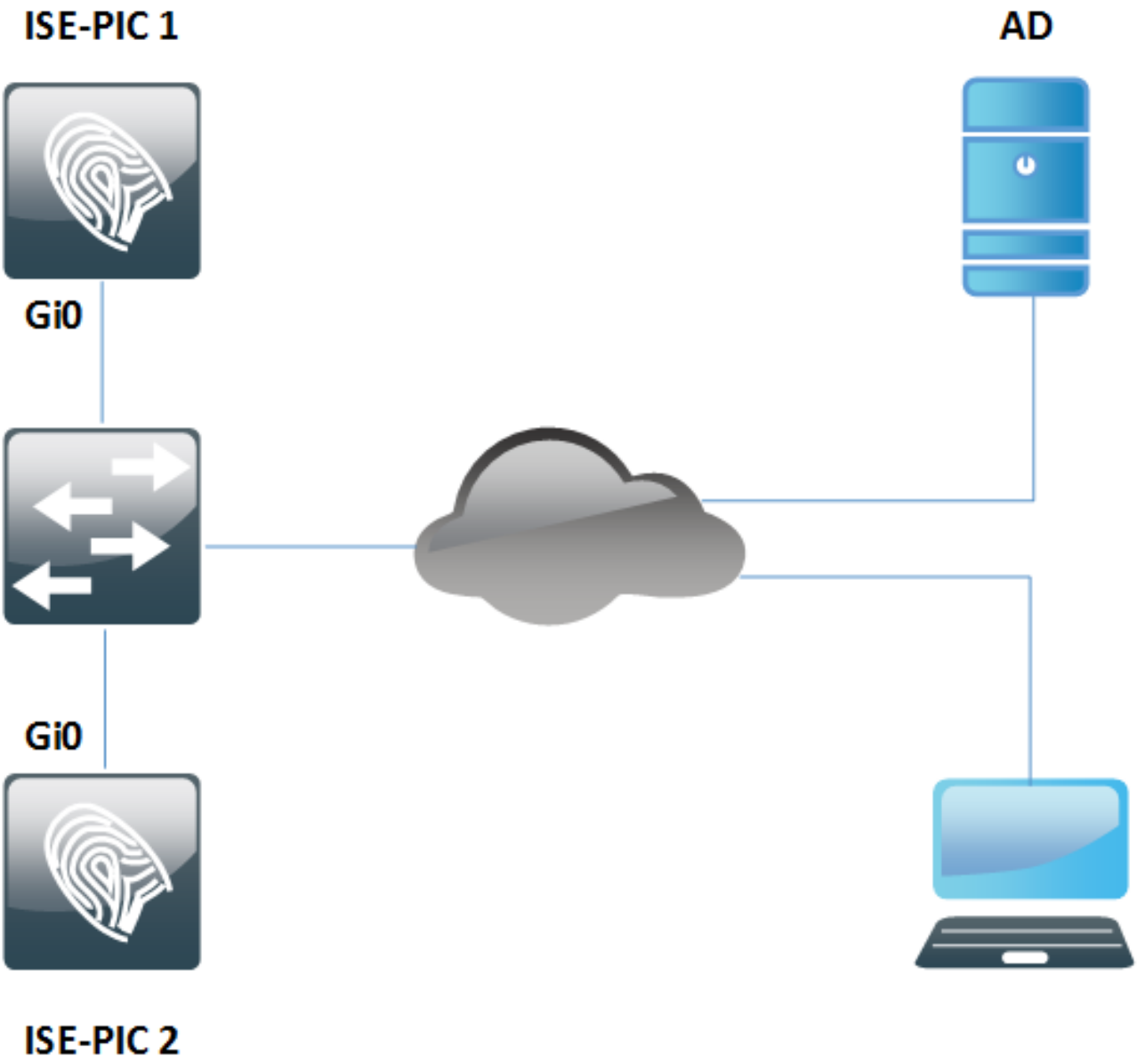
Cet exemple affiche comment configurer le fournisseur WMI pour le Répertoire actif. WMI se compose d'un ensemble d'extensions aux Windows Driver Model qui fournissent une interface du système d'exploitation par laquelle a équipé des composants donnent les informations et notification. WMI est l'implémentation de Microsoft de la Gestion d'entreprise basée sur le WEB (WBEM) et des normes communes du modèle de l'information (CIM) du Task Force distribué de Gestion (DMTF).

Note: Plus d'informations sur WMI peuvent être trouvées sur le site de Microsoft de

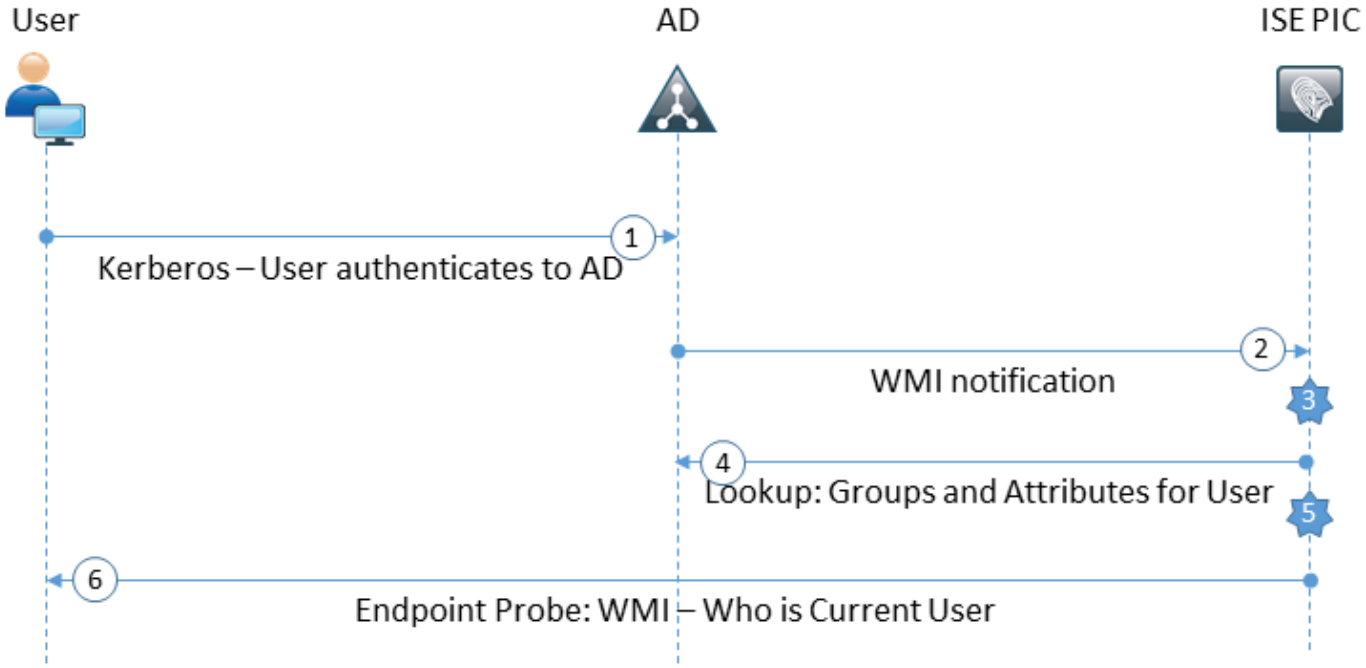
fonctionnaire : Au sujet de WMI

Diagramme du réseau

Les informations dans le document utilisent la configuration réseau affichée dans l'image :



Flux des tâches



1. Ouvrez une session au PC et obtenez authentifié sur l'AD.

2. WMI informe la PIC ISE au sujet de cette authentification.

3. ISE ajoute le nom d'utilisateur obligatoire : IP_Address à son répertoire de session.

4. ISE récupère les Groupes d'utilisateurs et les attributs de l'AD.

5. ISE enregistre ces informations dans son répertoire de session.

6. Toutes les 4 heures (non configurables) ISE PIC de passages de sonde de point final : D'abord il essaye WMI au point final.Si WMI échoue alors la PIC ISE exécute ISEExec. Il questionne le point final pour l'utilisateur et l'enable WMI pendant la fois prochaine.Également la PIC ISE récupère l'adresse MAC du point final et du type de SYSTÈME D'EXPLOITATION.

   Sur la PIC ISE il est possible d'activer/seulement des sondes de point final. Le noeud primaire questionne tous les points finaux, noeud secondaire est pour la Haute disponibilité seulement.

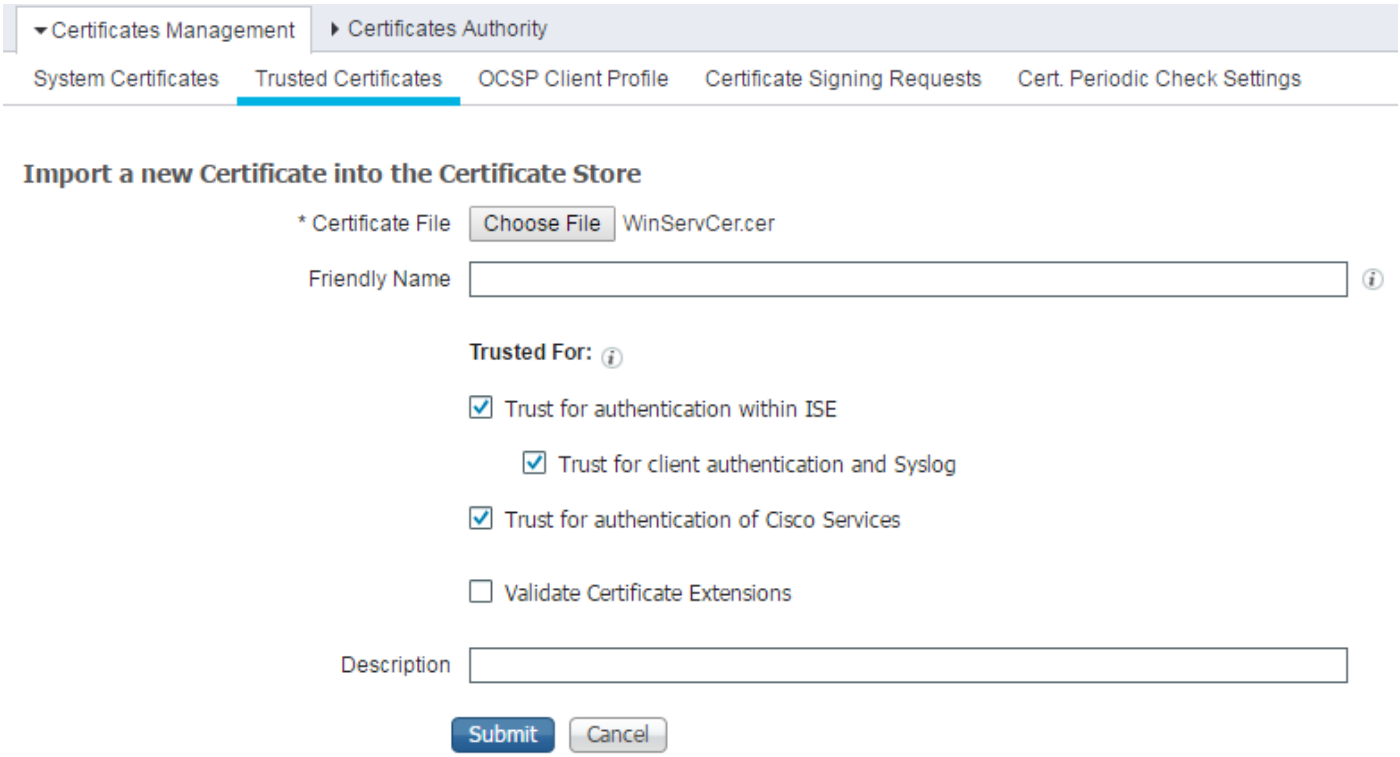
Configurez

Configurez le déploiement PIC ISE

Étape 1 (facultative). Installez les Certificats de confiance.

La pleine chaîne des Certificats de votre Autorité de certification (CA) devrait être installée sur la mémoire de confiance par ISE. Ouvrez une session au GUI PIC ISE et naviguez vers les **Certificats > la Gestion de Certificats > les Certificats de confiance**. Cliquez sur l'**importation** et sélectionnez votre certificat de Ca de votre PC.

Suivant les indications de l'image, cliquez sur Submit pour sauvegarder des modifications. Répétez cette étape pour tous les Certificats de la chaîne. Répétez les étapes sur le noeud secondaire aussi bien.

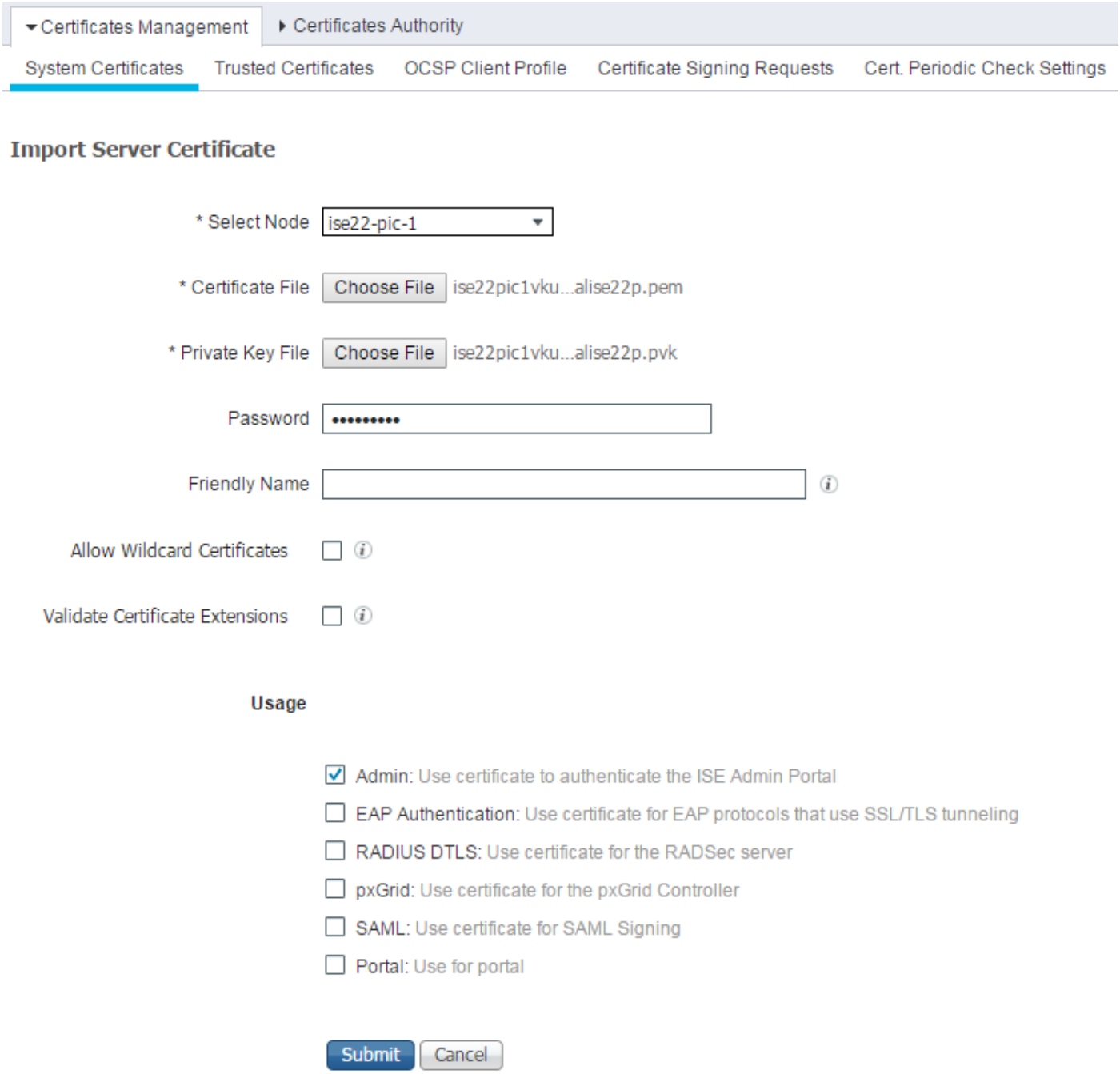


Étape 2 (facultative). Installez les Certificats de système.

L'option 1. délivre un certificat déjà généré par CA avec la clé privée.

Naviguez vers des **Certificats de Certificats > de Gestion > de système de Certificats** et cliquez sur l'**importation**. Sélectionnez le **fichier du certificat** et le **fichier principal privé**, entrent dans le champ de *mot de passe* si la clé privée est chiffrée.

Suivant les indications des options d'**utilisation de** contrôle d'image :



Note: Puisque la PIC ISE est basée sur le code ISE et peut facilement être convertie en ISE complet avec les permis appropriés, toutes les options d'utilisation sont disponibles. Des rôles tels que l'**authentification EAP**, **RADIUS DTLS**, **SAML** et **portail** ne sont pas utilisés par la PIC ISE.

Cliquez sur Submit pour installer le certificat. Répétez cette procédure sur un noeud secondaire aussi bien.

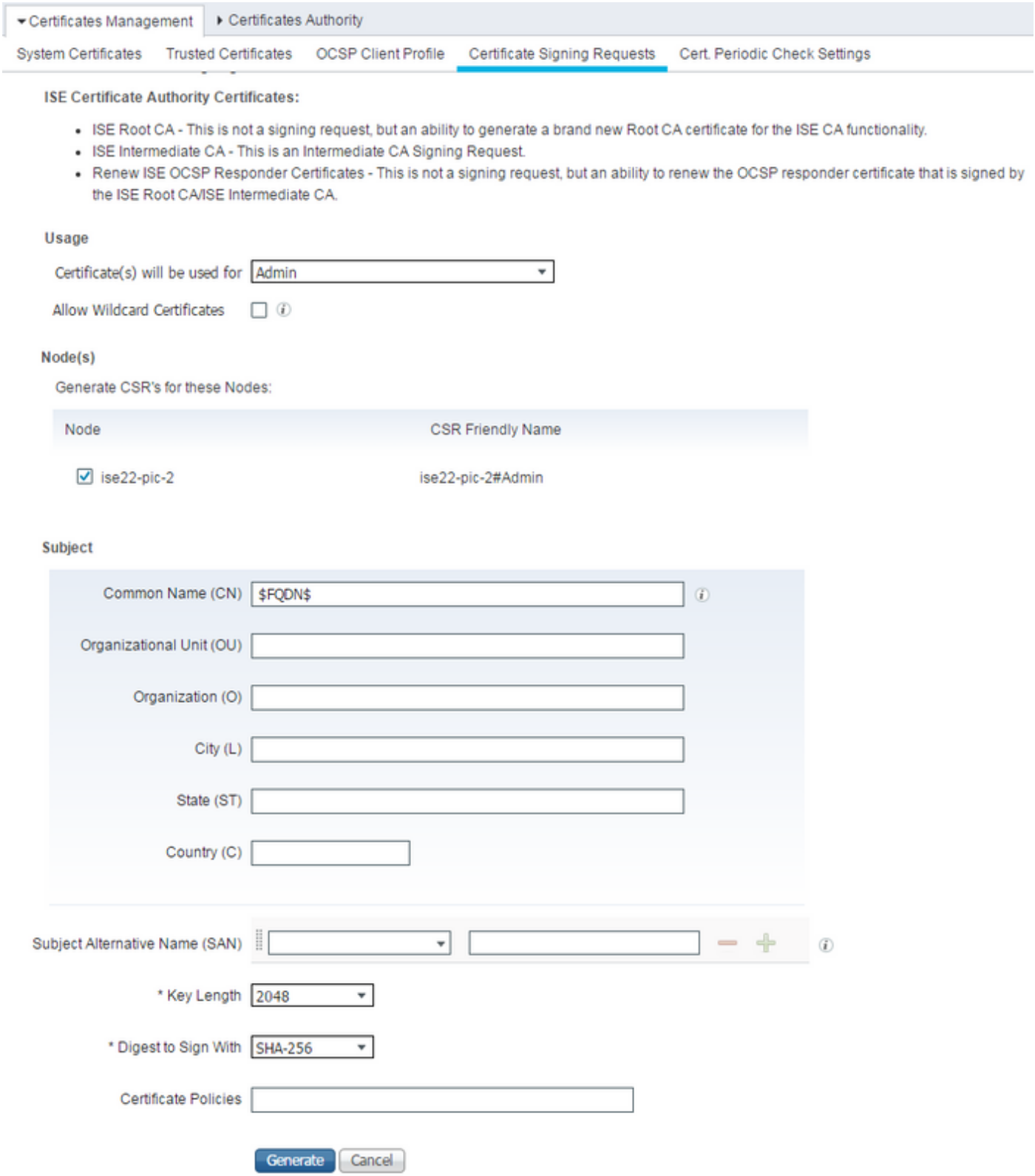
Note: Tous les services sur les reprises de noeud PIC ISE après importation de certificat de serveur.

L'option 2. génèrent la demande de signature de certificat (CSR), la signent avec le CA et lient sur ISE.

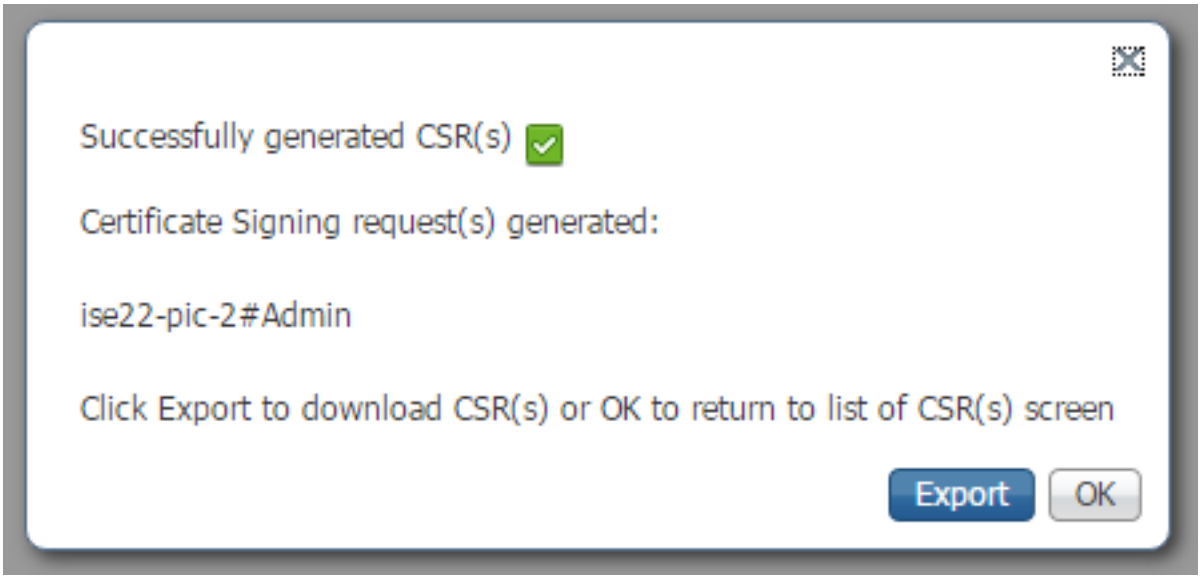
Naviguez vers la page de **demandes de signature de Certificats > de Gestion > de certificat de**

Certificats et le clic **génèrent les demandes de signature de certificat (CSR)**.

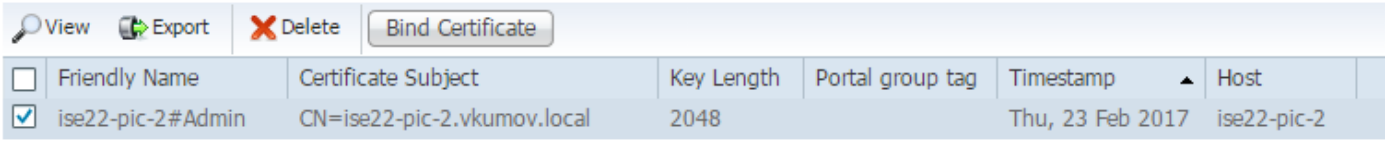
Sélectionnez le noeud et l'utilisation, entrent dans les autres champs s'il y a lieu :



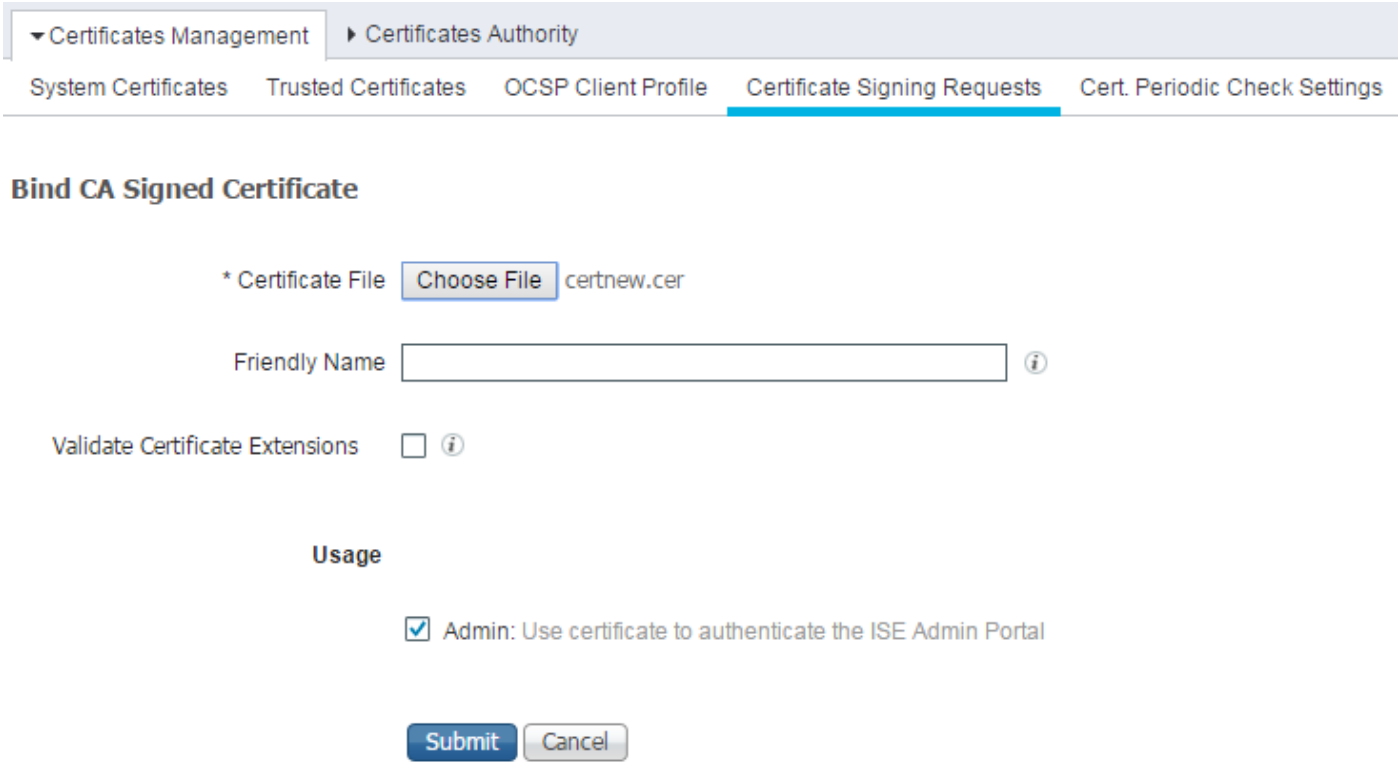
Le clic **se produisent.** La nouvelle fenêtre s'affiche avec une option **d'exporter le** CSR généré :



Cliquez sur l'**exportation,** sauvegardez le fichier généré ***.pem** et signez-le avec le CA. Une fois que le CSR est signé naviguent de nouveau à la page de **demandes de signature de Certificats > de Gestion > de certificat de Certificats**, sélectionnent votre CSR et cliquez sur le **certificat de grippage** :



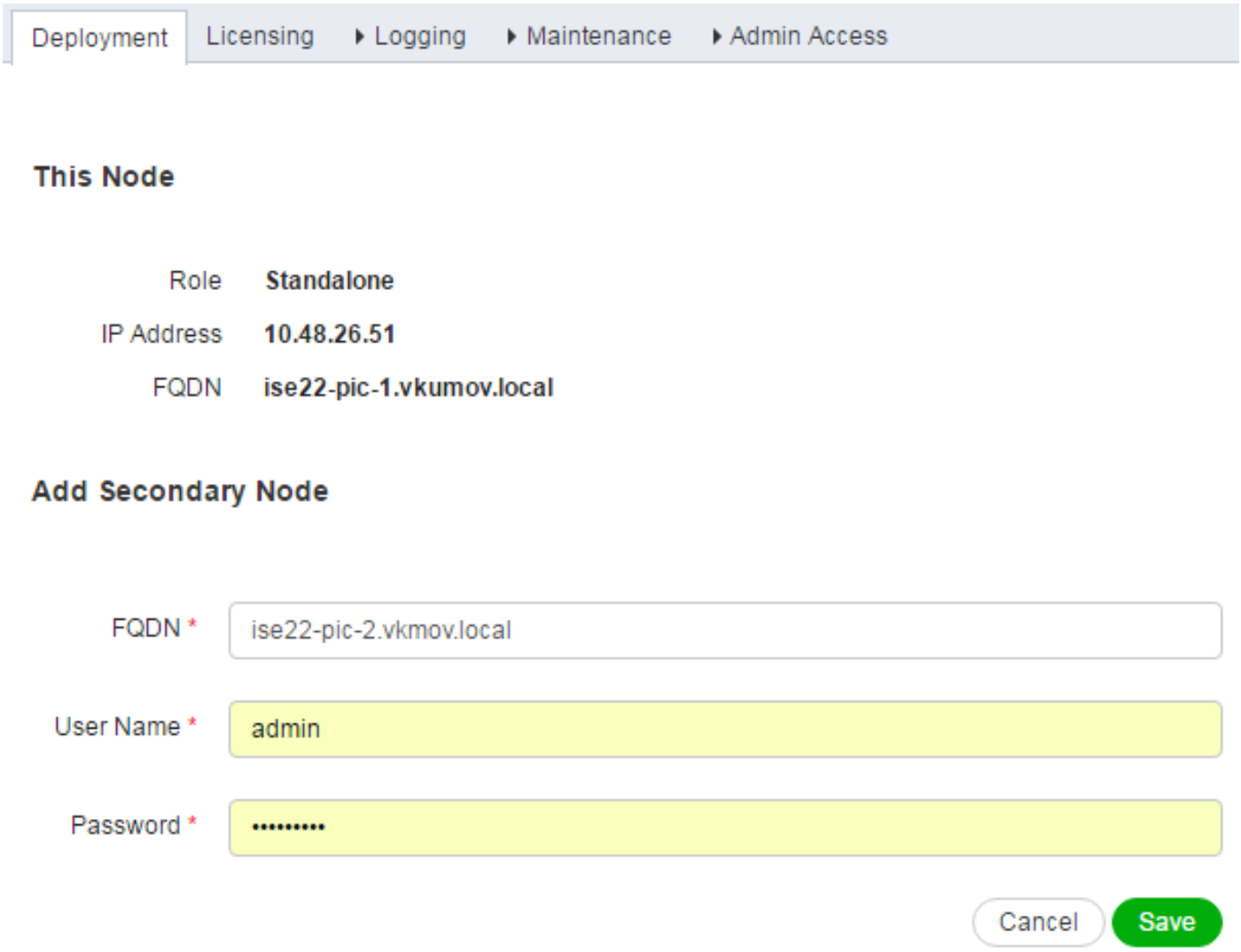
Sélectionnez le certificat qui a été signé avec votre CA et cliquez sur Submit pour appliquer des modifications :



Tous les services sur la reprise de noeud PIC ISE après que vous cliquiez sur Submit pour installer le certificat.

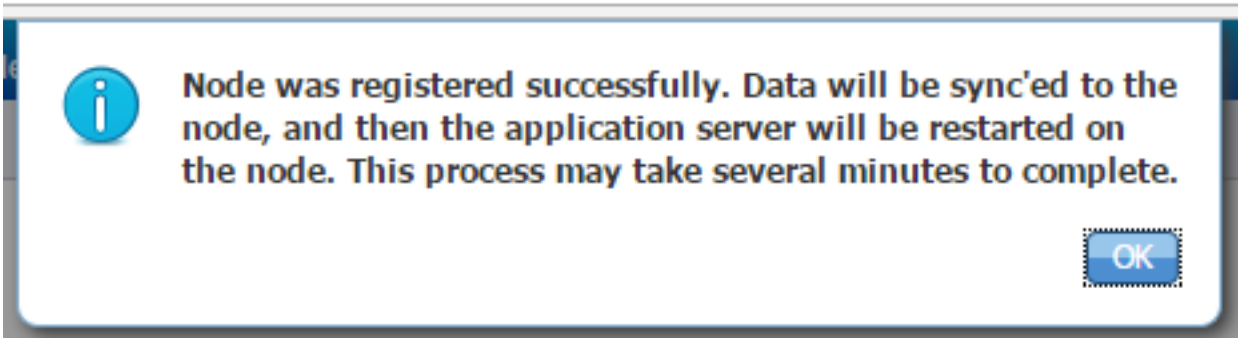
Étape 3. Ajoutez le noeud secondaire au déploiement.

La PIC ISE laisse avoir 2 Noeuds dans un déploiement pour la Haute disponibilité. Il n'exige pas d'avoir une confiance bi-directionnelle des Certificats (comparant au déploiement habituel ISE). Afin d'ajouter un noeud secondaire au déploiement, naviguez vers la **page de gestion > de déploiement** sur votre noeud primaire PIC ISE, suivant les indications de l'image :

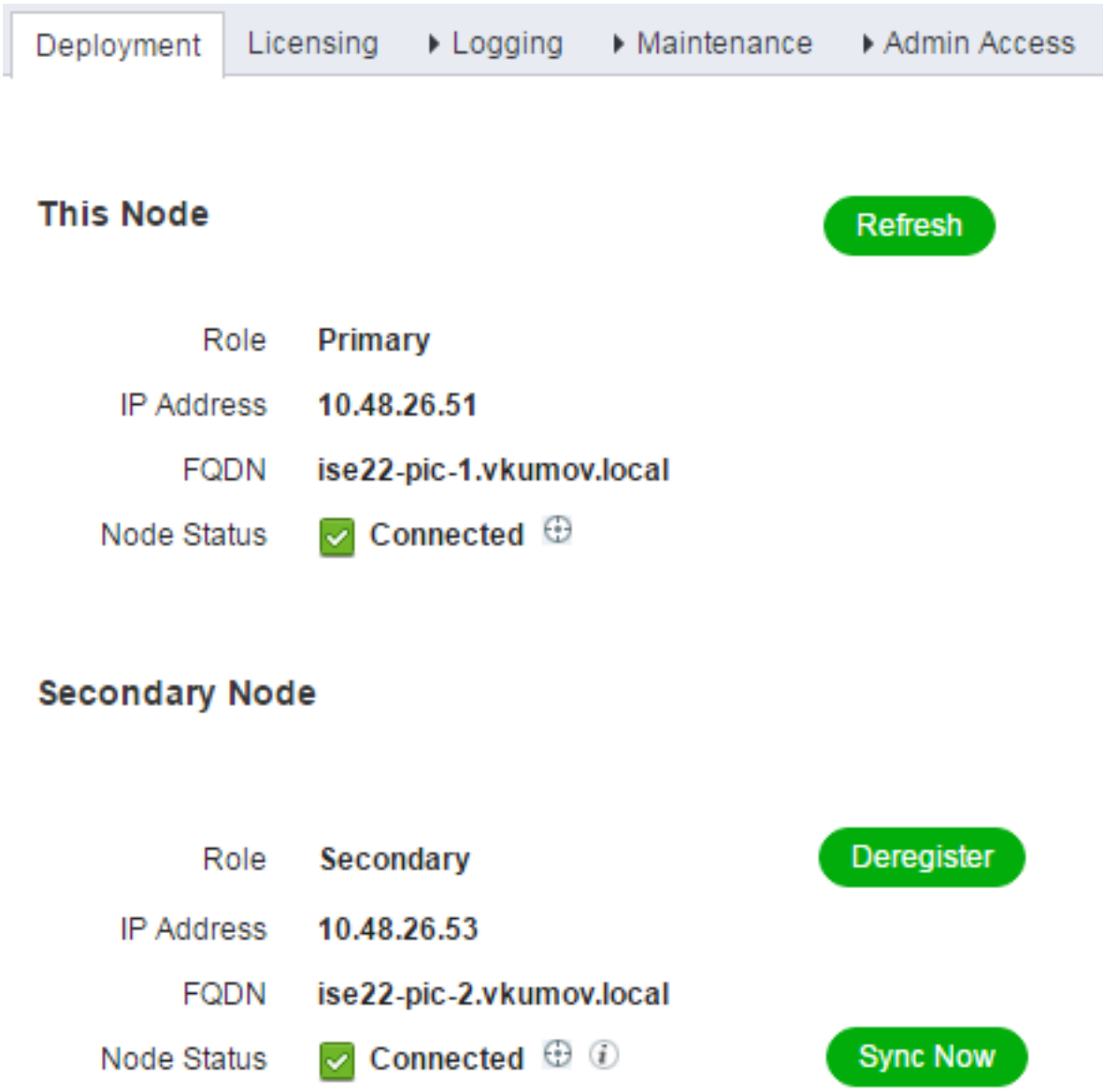


Écrivez le nom de domaine complet (FQDN) du noeud secondaire, des qualifications d'administrateur de cette **sauvegarde de** noeud et de clic. Au cas où le noeud primaire PIC ISE ne pourrait pas vérifier le certificat d'admin du deuxième noeud il demande la confirmation avant qu'il installe ce certificat dans la mémoire de confiance.

Dans un tel **certificat d'importation de** clic de cas **et poursuivez** afin de joindre le noeud au déploiement. Vous devriez obtenir une notification que le noeud est ajouté avec succès. Tous les services sur les reprises secondaires de noeud.



Dans un délai de 10-20 minutes des Noeuds devraient être synchronisés et le statut du noeud devrait changer d'**en cours** à connecté :



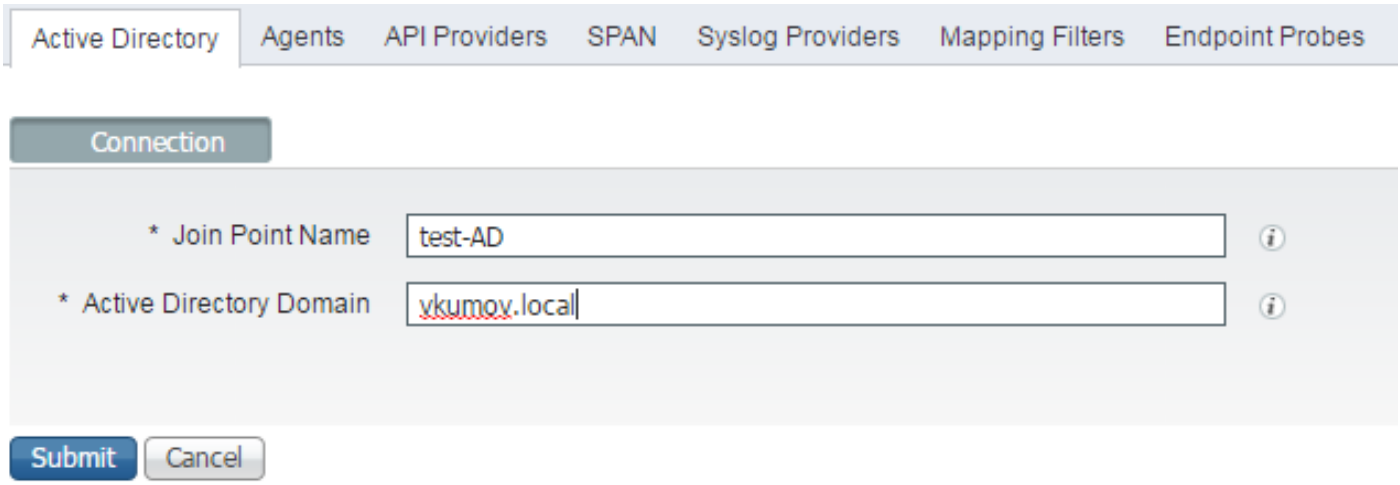
Configurez les fournisseurs de Répertoire actif

La PIC ISE emploie les Windows Management Instrumentation (WMI) pour collecter des informations au sujet des sessions d'AD et des actes comme un communitation de bar/sous-titre, qui signifie :

- La PIC ISE s'abonne à certains événements
- WMI alerte la PIC ISE quand ces événements se produisent : 4768 (ticket Kerberos accordant) et 4770 (renouvellement de ticket Kerberos)Les entrées dans le répertoire de session expirent (la purge)

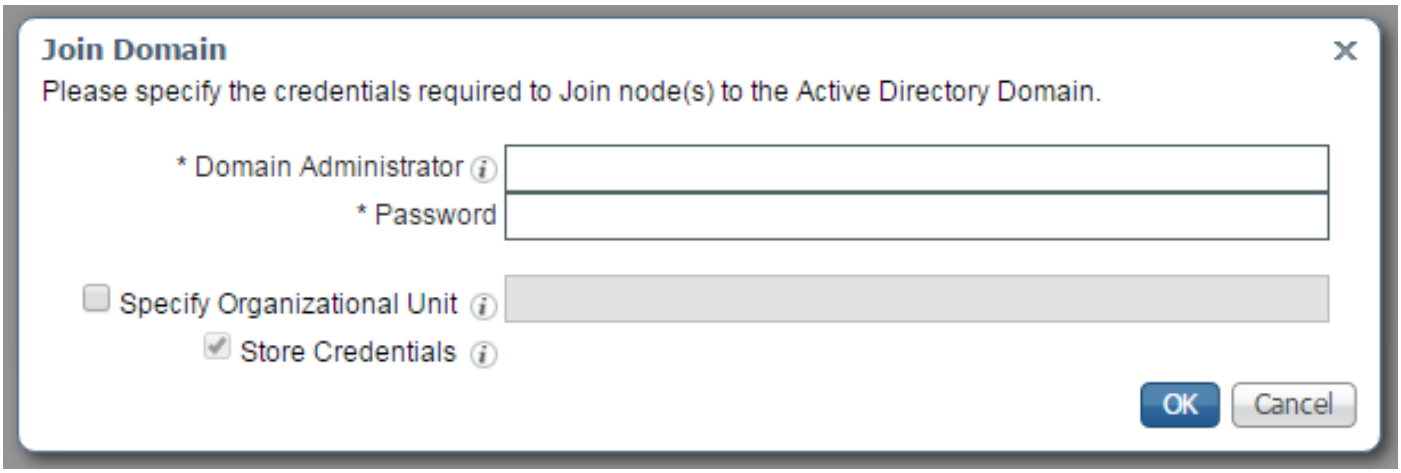
Étape 1. Joignez la PIC ISE au domaine.

Afin de joindre la PIC ISE au domaine, naviguez vers les **fournisseurs > le Répertoire actif** et cliquez sur Add :



Le remplissage **joignent des champs Domain de nom** et de **Répertoire actif de point** et cliquent sur Submit pour sauvegarder des modifications. **Joignez le nom de point** est un nom qui est utilisé à la PIC ISE seulement. **Le domaine de Répertoire actif** est le nom du domaine où la PIC ISE devrait être jointe et elle devrait être résoluble avec le serveur DNS configuré sur la PIC ISE.

Après la création de la PIC du point ISE Join devrait te demander si vous voudriez joindre des Noeuds au domaine. Cliquez sur **Yes**. Une fenêtre devrait s'afficher pour que vous fournissiez des qualifications pour joindre le domaine :



Remplissez champs d'**administrateur** et de **mot de passe de domaine** et cliquez sur OK**.**

Quoique le champ s'appelle **Domain Administrator** il n'est pas nécessaire d'utiliser l'utilisateur d'administrateur **pour joindre la** PIC ISE au domaine. Cet utilisateur devrait avoir des privilèges suffisants de créer et retirer des comptes d'ordinateur dans le domaine, ou modifiez les mots de passe pour des comptes d'ordinateur précédemment créés. Des autorisations de compte de Répertoire actif exigées pour exécuter de diverses exécutions peuvent être trouvées dans ce document.

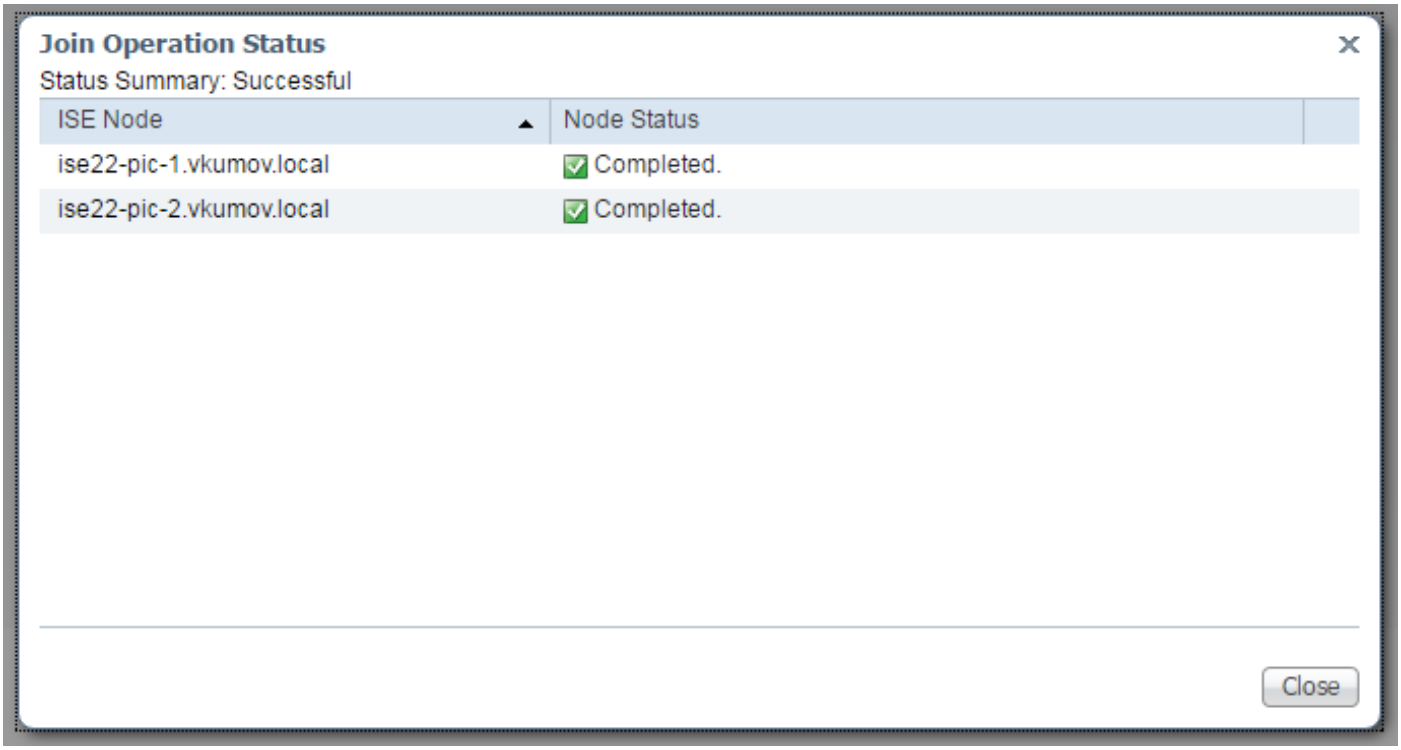
Cependant c'est administrateur de domaine d'utilisation de requiredto que les qualifications pendant se joignent si vous voudriez utiliser WMI. L'option du **config WMI** exige :

- Changements dans le registre
- Autorisations d'utiliser DCOM

- Autorisations d'utiliser WMI à distance
- Access pour lire le journal d'événements de Sécurité du domaine Controlle d'AD
- Le pare-feu Windows doit permettre le trafic de/à la PIC ISE (des stratégies correspondantes de pare-feu Windows seront créées pendant le **config WMI**)

  Note: **Les qualifications de mémoire** est toujours soient activées sur la PIC ISE puisqu'on l'exige pour des sondes de point final et la configuration WMI. ISE les enregistre a chiffré intérieurement.

Suivant les indications de l'image, la PIC ISE donne le résultat de l'exécution dans une nouvelle fenêtre :



Étape 2. Autorisations d'optimisation sur l'AD.

Vérifiez et accordez les autorisations pour l'utilisateur sur l'AD par document : [Installation et guide de l'administrateur passifs du connecteur d'identité de Cisco Identity Services Engine (ISE-PIC) :]

Placez les autorisations quand utilisateur d'AD dans le groupe d'admin de domaine

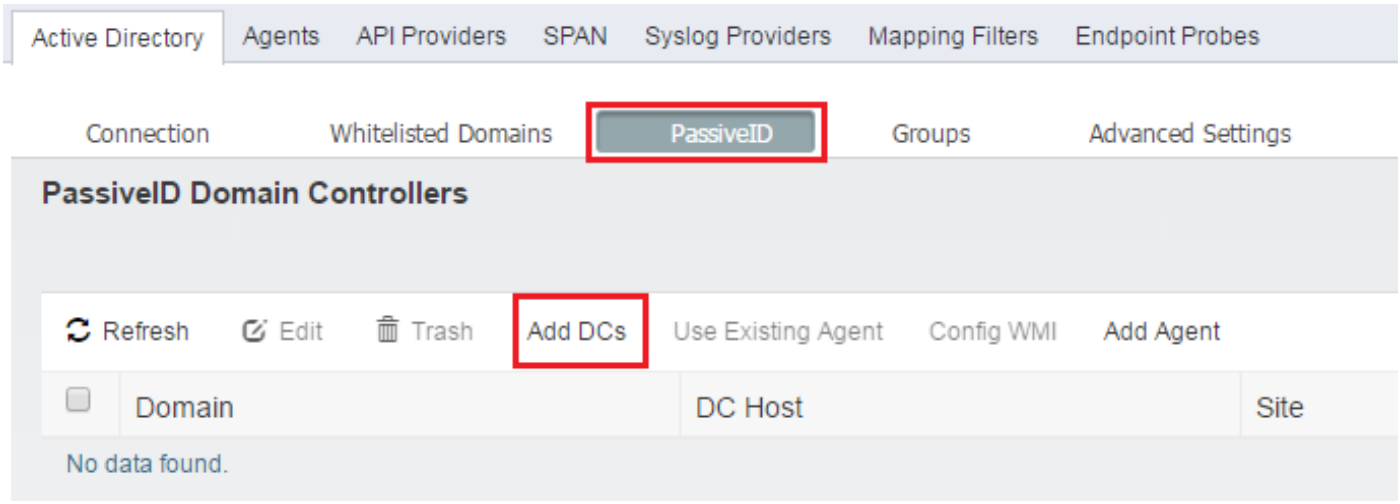
Pour Windows 2008 R2,Windows 2012, et Windows 2012 R2, le groupe d'admin de domaine n'ont pas le plein contrôle sur certaines clés de registre dans le système d'exploitation Windows par défaut. L'admin de Répertoire actif doit donner à l'utilisateur de Répertoire actif des autorisations de plein contrôle sur la clé de registre suivante

- `HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`
- `HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-`

00600806D9B6}

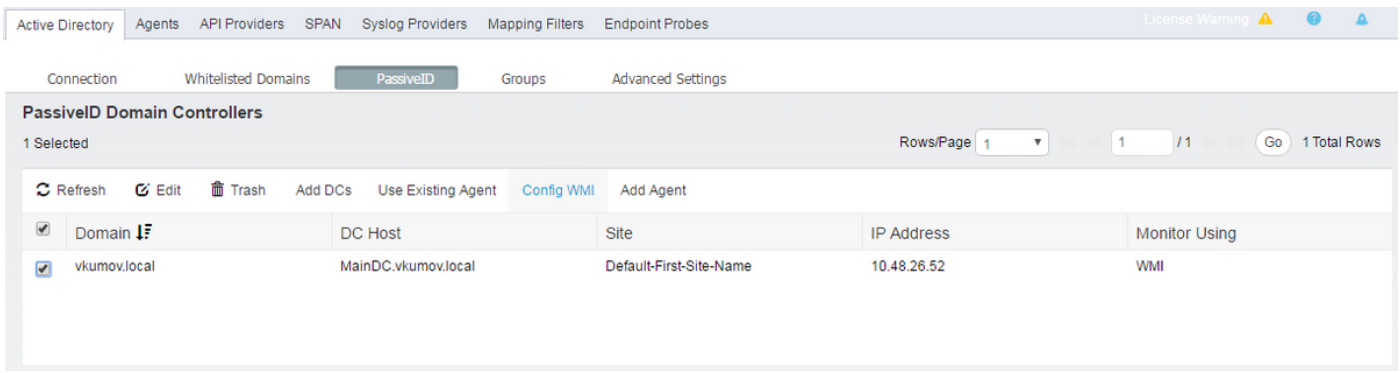
Étape 3. Ajoutez les agents de PassiveID.

Àla page de domaine d'AD naviguez vers l'onglet de PassiveID et cliquez sur Add **DCS**, suivant les indications de l'image :

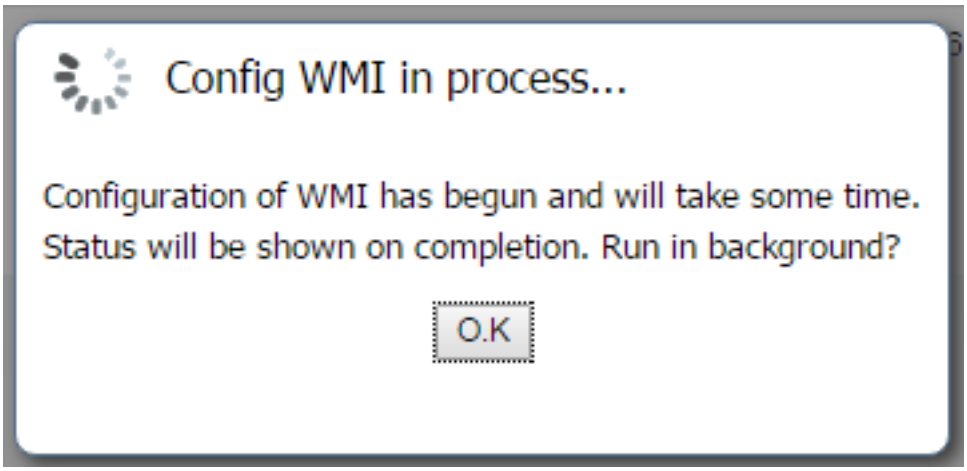


Une nouvelle fenêtre s'affiche et ISE charge une liste de tous les contrôleurs de domaine disponibles. Sélectionnez DCS où vous voudriez configurer WMI et cliquer sur OK pour sauvegarder des modifications, suivant les indications de l'image :

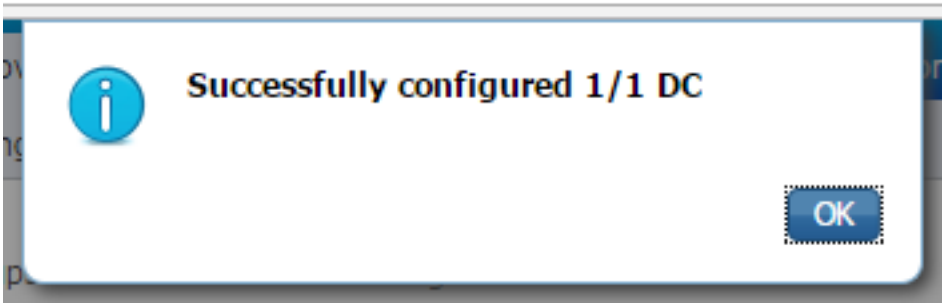
DCS sélectionné sont ajoutés à la liste de **contrôleurs de domaine de PassiveID.** Sélectionnez votre DCS et cliquez sur le bouton du **config WMI** :



La PIC ISE prouve à un message que le processus de configuration est en cours :



Après que le couple des minutes il t'affiche un message que WMI est avec succès configuré sur DCS sélectionné :



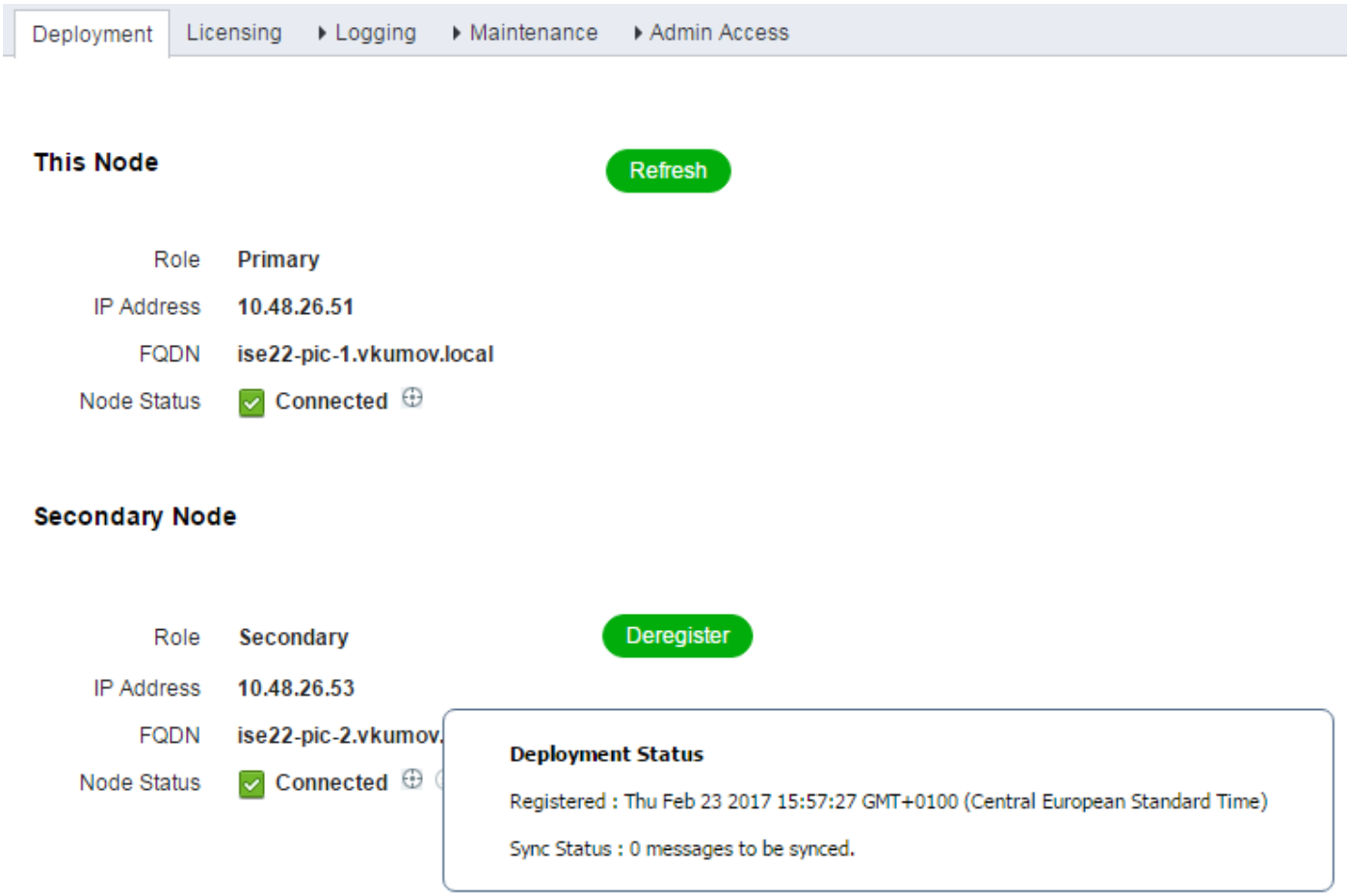
Vérifiez

Déploiement

Le statut du déploiement peut être signé quelques unes de manières :

Page de déploiement

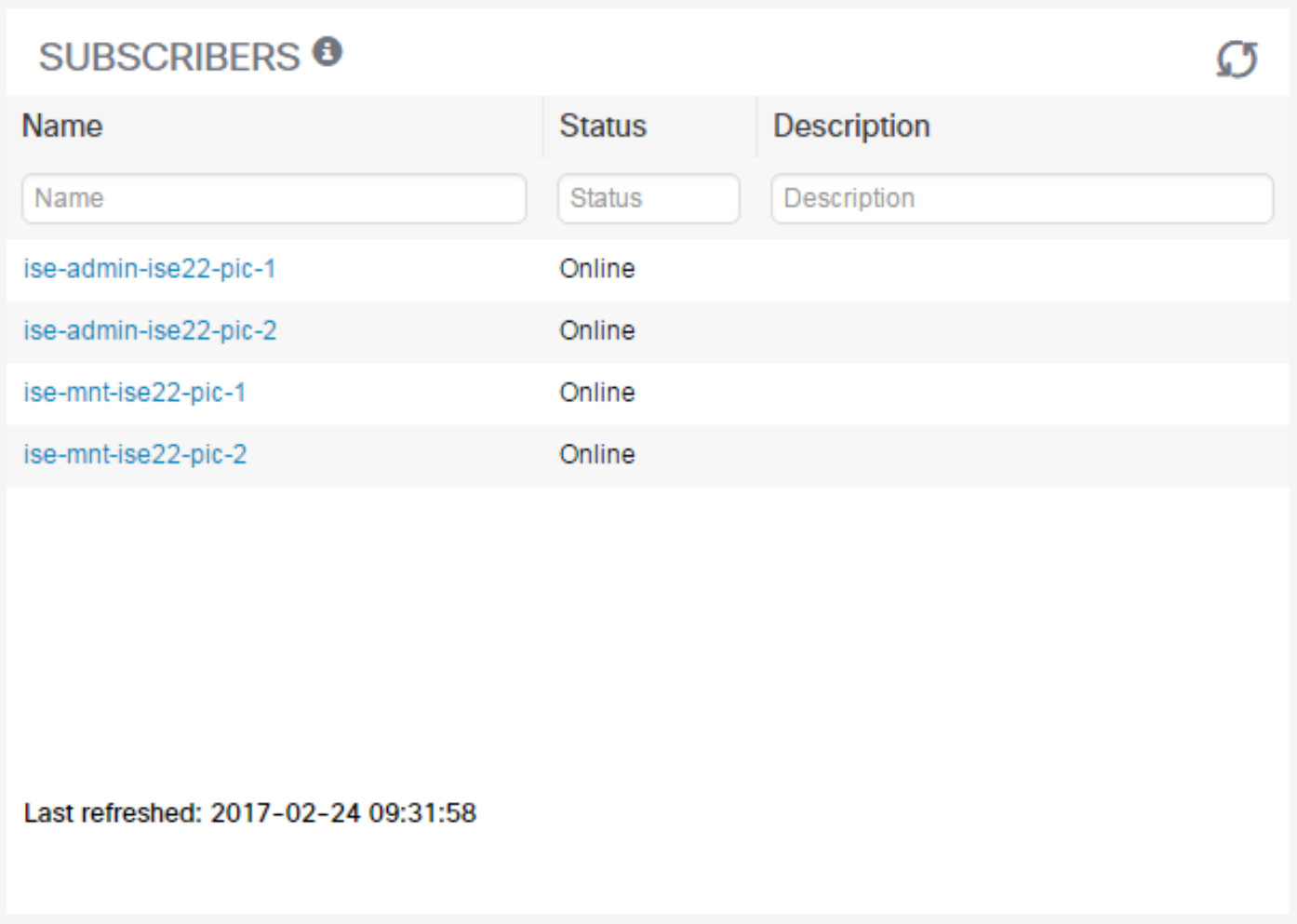
Naviguez vers la **page de gestion > de déploiement que l'**état actuel du déploiement peut être vérifié :



De cette page le noeud secondaire peut De radié de l'immatriculation si nécessaire. La synchronisation manuelle peut être commencée et l'**état de sync** peut être vérifié.

Page de tableau de bord

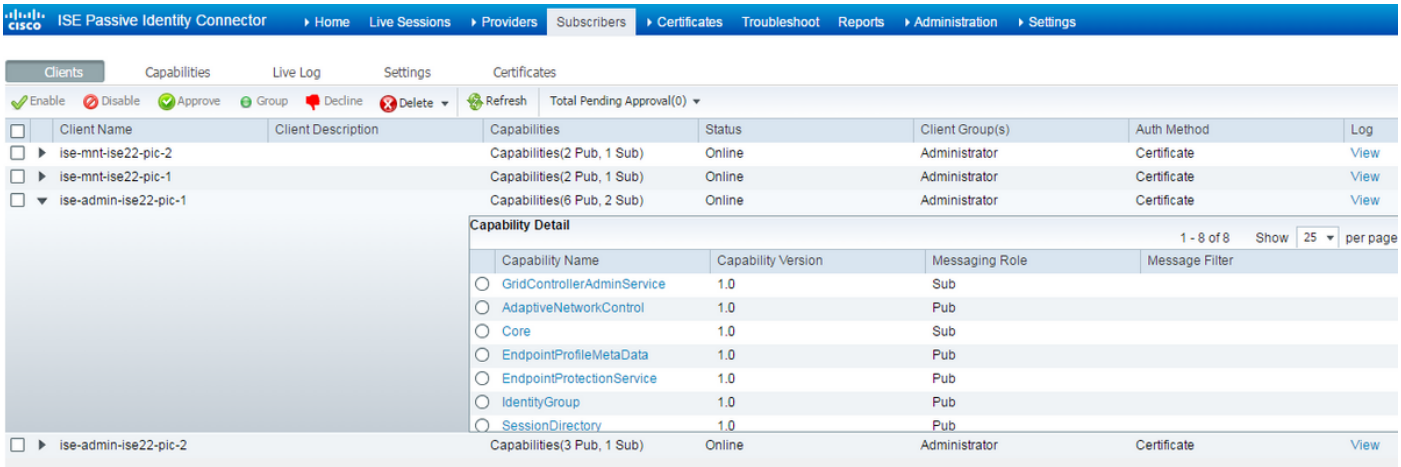
Àune page principale PIC ISE il y a un dashlet appelé **Subscribers**. Avec ce dashlet vous pouvez vérifier l'état actuel de vos Noeuds PIC ISE, suivant les indications de l'image :



La PIC ISE crée 2 abonnés pour chaque noeud - **admin** et **MNT.** Tous devraient être dans l'**état en ligne** qui signifie que les Noeuds sont reacheable et opérationnels.

Abonnés

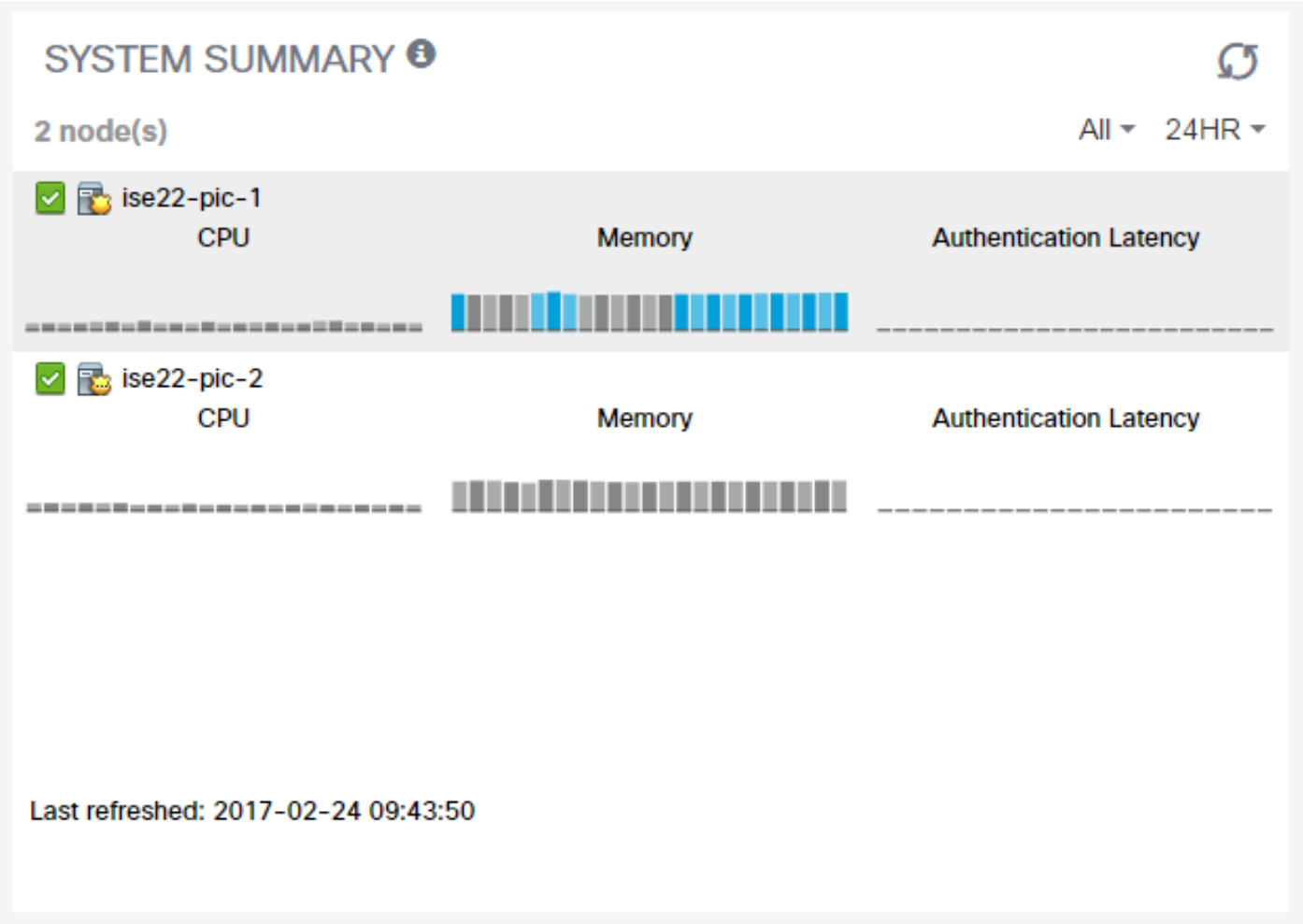
Les abonnés paginent est une version étendue de dashlet d'abonnés de page d'accueil de PIC ISE. Cette page affiche tout le pxGrid associé, toutefois le statut de Noeuds PIC ISE peut être vérifié ici aussi bien :



Résumé de système

La PIC ISE laisse surveiller le résumé de santés des Noeuds aussi bien. Ce dashlet peut être

trouvé à la maison **> tableau de bord > supplémentaire** :

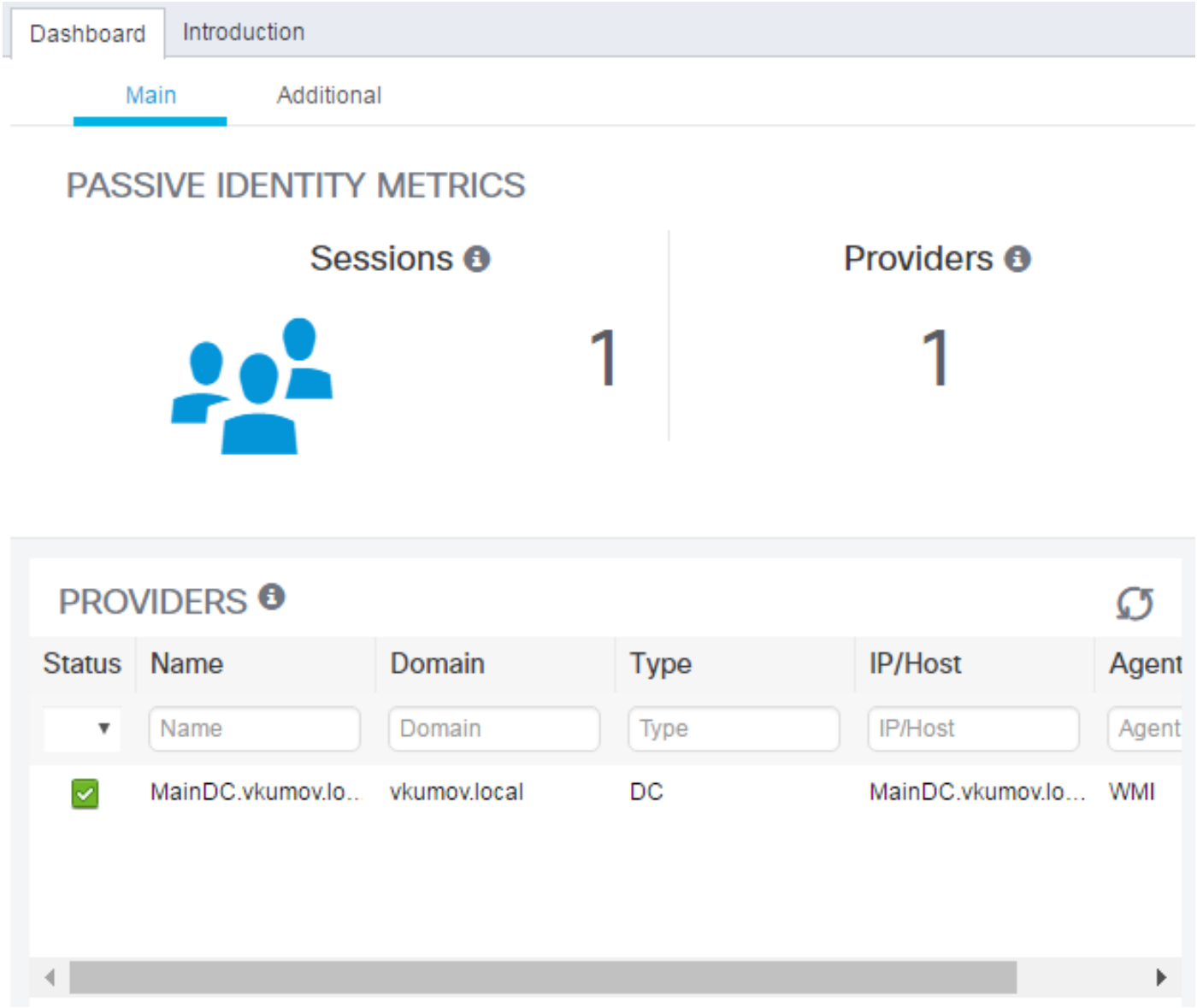


La latence d'authentification est toujours 0ms puisque la PIC ISE n'exécute aucunes authentifications/autorisation.

Fournisseurs et sessions

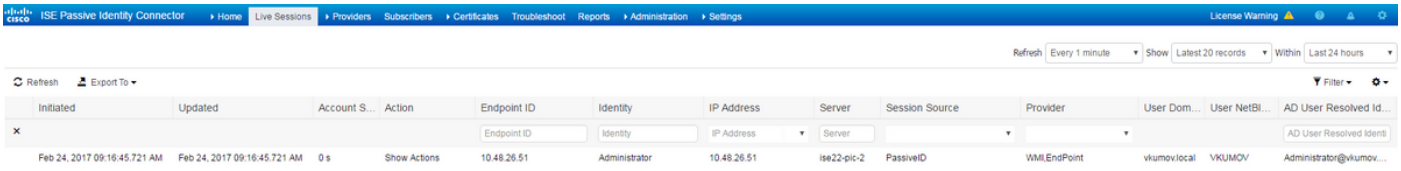
Page d'accueil

Des statuts de fournisseurs, leur quantité et la quantité de sessions trouvées peuvent être vérifiés tandis que vous naviguez **pour autoguider > page de tableau de bord** :



Sessions vivantes

Les informations détaillées au sujet de toutes les sessions d'utilisateurs trouvées peuvent être trouvées à la page de **sessions Live** :



Il contient une telle informations en tant que :

- Fournisseur - quels fournisseurs ont été utilisés pour identifier cette session
- Initié et mis à jour - horodateurs où la session est initiée et mise à jour en conséquence
- Adresse IP - l'adresse du point final
- L'action - les actions qu'ISE peut exécuter (par exemple, état de point final de contrôle, ou si

la PIC ISE est intégrée avec le pxGrid alors envoie une demande d'effacer la session)

Dépannez

Déploiement

Pour dépanner des questions de déploiement et de repliaction, examinez ces fichiers journal :

- replication.log
- deployment.log
- ise-psc.log

Afin d'activer met au point, navigue vers la **gestion > se connectant > configuration de log de debug** :

Node List > **ise22-pic-1.vkumov.local**

Debug Level Configuration

Edit | Reset to Default

Component Name	Log Level	Description
portal-web-action	INFO	Base Portal debug messages
posture	INFO	Posture debug messages
previewportal	INFO	Preview Portal debug messages
profiler	INFO	profiler debug messages
provisioning	INFO	Client Provisioning client debug messages
prrt-JNI	INFO	prrt policy decision request processing layer related messages
pxgrid	INFO	pxGrid messages
Replication-Deployment	DEBUG	Logger related to Deployment Registeration,Deregistration,Sync and ...
Replication-JGroup	WARN	Logger related to JGroup Node State
ReplicationTracker	INFO	PSC replication related debug messages
report	INFO	Debug reports on M&T nodes
RuleEngine-Attributes	INFO	Additional rule evaluation attributes in audit logging at DEBUG
RuleEngine-Policy-IDGroups	INFO	Additional policy vs id group audit logging at DEBUG

Ceux-ci met au point sont écrits au fichier de **replication.log**. Voici un exemple d'un processus de réplication normal :

```
2017-02-24 10:11:06,893 INFO [pool-215-thread-1][]
cisco.cpm.deployment.replication.PublisherImpl -::::- Calling the publisher job from
clusterstate processor
2017-02-24 10:11:06,893 DEBUG [pool-214-thread-1][]
cisco.cpm.deployment.replication.PublisherImpl -::::- Started executing publisher job
2017-02-24 10:11:06,894 DEBUG [pool-214-thread-1][]
cisco.cpm.deployment.replication.PublisherImpl -::::- Number of messages with no sequence number
is 0
2017-02-24 10:11:06,894 DEBUG [pool-214-thread-1][]
cisco.cpm.deployment.replication.PublisherImpl -::::- Finished executing publisher job
2017-02-24 10:11:06,895 DEBUG [pool-214-thread-1][]
api.services.persistance.dao.ChangeDataDaoImpl -::::- Data returned in getMinMaxBySequence
method=[id=[63ce2fe0-f8cd-11e6-b0ad-005056991a2e],startTime=[0],endTime=[0],applied=[false],data
length=[794],sequenceNumber=[502]2017-02-22 08:06:10.782]
2017-02-24 10:11:06,895 DEBUG [pool-214-thread-1][]
api.services.persistance.dao.ChangeDataDaoImpl -::::- Data returned in getMinMaxBySequence
```

```
method=[id=[3ded93c0-fa70-11e6-b684-005056990fbb],startTime=[0],endTime=[0],applied=[false],data
length=[794],sequenceNumber=[1600]2017-02-24 10:04:26.364]
2017-02-24 10:11:06,895 DEBUG [pool-214-thread-1][]
cisco.cpm.deployment.replication.ClientNodeProxy -:::::- Calling setClusterState(name: ise22-pic-
1, minSequence: 502, sequence: 1600, active: {ise22-pic-1-5015})
2017-02-24 10:11:06,896 INFO [pool-214-thread-1][]
cisco.cpm.deployment.replication.PublisherImpl -:::::- Finished sending the clusterState !!!
2017-02-24 10:11:06,899 DEBUG [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- MonitorJob starting
2017-02-24 10:11:06,901 DEBUG [pool-216-thread-1][]
cisco.cpm.deployment.replication.ClientNodeProxy -:::NodeStateMonitor:- Calling getNodeStates()
2017-02-24 10:11:06,904 INFO [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- Nodes in
distrubution: {ise22-pic-2=nodeName: ise22-pic-2, status: SYNC COMPLETED, transientStatus: ,
lastStatusTime: 1487927436906, seqNumber: 1600, createTime: 2017-02-24 10:04:26.364} --- Nodes
in cluster: [name: ise22-pic-2, Address: ise22-pic-2-38077, sequence: 1600, createtime: 2017-02-
24 10:04:26.364]
2017-02-24 10:11:06,904 DEBUG [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- Adding [ nodeName:
ise22-pic-2, status: SYNC COMPLETED, transientStatus: , lastStatusTime: 1487927436906,
seqNumber: 1600, createTime: 2017-02-24 10:04:26.364 ] to liveDeploymentMembers
2017-02-24 10:11:06,905 DEBUG [pool-216-thread-1][]
api.services.persistance.dao.ChangeDataDaoImpl -:::NodeStateMonitor:- Data returned in
getMinMaxBySequence method=[id=[63ce2fe0-f8cd-11e6-b0ad-
005056991a2e],startTime=[0],endTime=[0],applied=[false],data
length=[794],sequenceNumber=[502]2017-02-22 08:06:10.782]
2017-02-24 10:11:06,905 DEBUG [pool-216-thread-1][]
api.services.persistance.dao.ChangeDataDaoImpl -:::NodeStateMonitor:- Data returned in
getMinMaxBySequence method=[id=[3ded93c0-fa70-11e6-b684-
005056990fbb],startTime=[0],endTime=[0],applied=[false],data
length=[794],sequenceNumber=[1600]2017-02-24 10:04:26.364]
2017-02-24 10:11:06,905 INFO [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- Primary node
current status minmum sequence[ 1600 ], cluster state: [ name: ise22-pic-1, minSequence: 502,
sequence: 1600, active: {ise22-pic-1-5015} ]
2017-02-24 10:11:06,905 DEBUG [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- Processing node
state [ name: ise22-pic-2, Address: ise22-pic-2-38077, sequence: 1600, createtime:2017-02-24
10:04:26.364 ]
2017-02-24 10:11:06,905 DEBUG [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- ise22-pic-2 - [
nodeName: ise22-pic-2, status: SYNC COMPLETED, transientStatus: , lastStatusTime: 1487927436906,
seqNumber: 1600, createTime: 2017-02-24 10:04:26.364 ]
2017-02-24 10:11:06,905 DEBUG [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- Adding nodeName:
ise22-pic-2, status: SYNC COMPLETED, transientStatus: , lastStatusTime: 1487927436906,
seqNumber: 1600, createTime: 2017-02-24 10:04:26.364 to liveJGroupMembers
2017-02-24 10:11:06,905 INFO [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- No Of
deployedNodes: [ 1 ], No Of liveJGroupNodes: [ 1 ], deadOrSyncInPrgMembersExist: [ false ],
latestMinSequence: [ 502 ]
2017-02-24 10:11:06,905 DEBUG [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:-
deadOrSyncInPrgMembersExist =[false], minSequence=[1598],clusterState=[502]
```

Un message d'**ise-psc.log** :

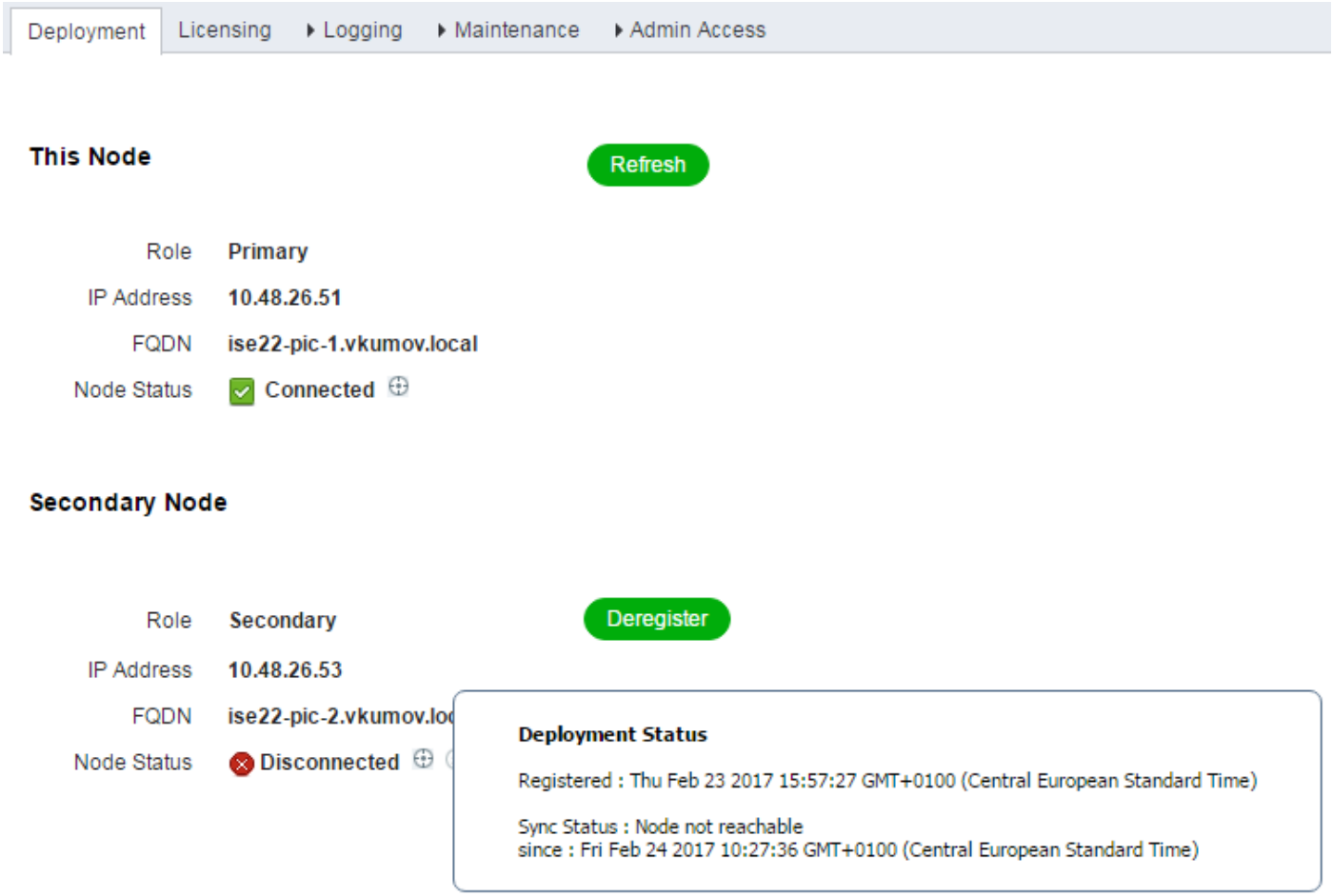
```
2017-02-24 10:11:06,893 INFO [pool-215-thread-1][]
cisco.cpm.deployment.replication.PublisherImpl -:::::- Calling the publisher job from
clusterstate processor
2017-02-24 10:11:06,893 DEBUG [pool-214-thread-1][]
cisco.cpm.deployment.replication.PublisherImpl -:::::- Started executing publisher job
```

2017-02-24 10:11:06,894 DEBUG [pool-214-thread-1][]
cisco.cpm.deployment.replication.PublisherImpl -::::- Number of messages with no sequence number is 0
2017-02-24 10:11:06,894 DEBUG [pool-214-thread-1][]
cisco.cpm.deployment.replication.PublisherImpl -::::- Finished executing publisher job
2017-02-24 10:11:06,895 DEBUG [pool-214-thread-1][]
api.services.persistance.dao.ChangeDataDaoImpl -::::- Data returned in getMinMaxBySequence method=[id=[63ce2fe0-f8cd-11e6-b0ad-005056991a2e],startTime=[0],endTime=[0],applied=[false],data length=[794],sequenceNumber=[502]2017-02-22 08:06:10.782]
2017-02-24 10:11:06,895 DEBUG [pool-214-thread-1][]
api.services.persistance.dao.ChangeDataDaoImpl -::::- Data returned in getMinMaxBySequence method=[id=[3ded93c0-fa70-11e6-b684-005056990fbb],startTime=[0],endTime=[0],applied=[false],data length=[794],sequenceNumber=[1600]2017-02-24 10:04:26.364]
2017-02-24 10:11:06,895 DEBUG [pool-214-thread-1][]
cisco.cpm.deployment.replication.ClientNodeProxy -::::- Calling setClusterState(name: ise22-pic-1, minSequence: 502, sequence: 1600, active: {ise22-pic-1-5015})
2017-02-24 10:11:06,896 INFO [pool-214-thread-1][]
cisco.cpm.deployment.replication.PublisherImpl -::::- Finished sending the clusterState !!!
2017-02-24 10:11:06,899 DEBUG [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- MonitorJob starting
2017-02-24 10:11:06,901 DEBUG [pool-216-thread-1][]
cisco.cpm.deployment.replication.ClientNodeProxy -:::NodeStateMonitor:- Calling getNodeStates()
2017-02-24 10:11:06,904 INFO [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- Nodes in distrubution: {ise22-pic-2=nodeName: ise22-pic-2, **status: SYNC COMPLETED**, transientStatus: , lastStatusTime: 1487927436906, seqNumber: 1600, createTime: 2017-02-24 10:04:26.364} --- Nodes in cluster: [name: ise22-pic-2, Address: ise22-pic-2-38077, sequence: 1600, createtime: 2017-02-24 10:04:26.364]
2017-02-24 10:11:06,904 DEBUG [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- Adding [nodeName: ise22-pic-2, **status: SYNC COMPLETED**, transientStatus: , lastStatusTime: 1487927436906, seqNumber: 1600, createTime: 2017-02-24 10:04:26.364] to liveDeploymentMembers
2017-02-24 10:11:06,905 DEBUG [pool-216-thread-1][]
api.services.persistance.dao.ChangeDataDaoImpl -:::NodeStateMonitor:- Data returned in getMinMaxBySequence method=[id=[63ce2fe0-f8cd-11e6-b0ad-005056991a2e],startTime=[0],endTime=[0],applied=[false],data length=[794],sequenceNumber=[502]2017-02-22 08:06:10.782]
2017-02-24 10:11:06,905 DEBUG [pool-216-thread-1][]
api.services.persistance.dao.ChangeDataDaoImpl -:::NodeStateMonitor:- Data returned in getMinMaxBySequence method=[id=[3ded93c0-fa70-11e6-b684-005056990fbb],startTime=[0],endTime=[0],applied=[false],data length=[794],sequenceNumber=[1600]2017-02-24 10:04:26.364]
2017-02-24 10:11:06,905 INFO [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- Primary node current status minmum sequence[1600], cluster state: [name: ise22-pic-1, minSequence: 502, sequence: 1600, active: {ise22-pic-1-5015}]
2017-02-24 10:11:06,905 DEBUG [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- Processing node state [name: ise22-pic-2, Address: ise22-pic-2-38077, sequence: 1600, createtime:2017-02-24 10:04:26.364]
2017-02-24 10:11:06,905 DEBUG [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- ise22-pic-2 - [nodeName: ise22-pic-2, status: SYNC COMPLETED, transientStatus: , lastStatusTime: 1487927436906, seqNumber: 1600, createTime: 2017-02-24 10:04:26.364]
2017-02-24 10:11:06,905 DEBUG [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- Adding nodeName: ise22-pic-2, status: SYNC COMPLETED, transientStatus: , lastStatusTime: 1487927436906, seqNumber: 1600, createTime: 2017-02-24 10:04:26.364 to liveJGroupMembers
2017-02-24 10:11:06,905 INFO [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- No Of deployedNodes: [1], No Of liveJGroupNodes: [1], deadOrSyncInPrgMembersExist: [false], latestMinSequence: [502]
2017-02-24 10:11:06,905 DEBUG [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:-

```
deadOrSyncInPrgMembersExist =[false], minSequence=[1598],clusterState=[502]
```

Problème courant : le noeud secondaire n'est pas reacheable

Si le noeud secondaire devient unreacheable il serait affiché à la **page de gestion > de déploiement** :



ise-psc.log contient le ce message :

```
2017-02-24 10:43:21,587 INFO   [admin-http-pool155][]
admin.restui.features.deployment.DeploymentIDCUIApi -::::- Replication status for node ise22-
pic-2 = NODE NOT REACHABLE
```

Ce message explique ce qui n'est pas reacheable, par exemple le noeud ne répond pas pour cingler :

```
2017-02-24 11:03:53,359 INFO   [counterscheduler-call-1][]
cisco.cpm.infrastructure.utils.GenericUtil -::::- Received pingNode response : Node is reachable
```

Actions de prendre : vérifiez si FQDN du noeud socandary est résoluble, connexion réseau de base de contrôle entre les Noeuds.

Au cas où les applications ne seraient pas dans l'état courant sur le noeud secondaire ou il y a un Pare-feu entre les Noeuds, **ise-psc.log** peut afficher ces messages :

```
2017-02-24 11:08:14,656 INFO   [Thread-10][] com.cisco.epm.util.NodeCheck -:::- Now checking
against secondary pap ise22-pic-2
2017-02-24 11:08:14,656 INFO   [Thread-10][] com.cisco.epm.util.NodeCheckHelper -:::-  inside
getHostConfigRemoteServer
2017-02-24 11:08:14,766 WARN   [Thread-10][]
deployment.client.cert.validator.HttpsCertPathValidatorImpl -:::- Error while connecting to
host: ise22-pic-2.vkumov.local. java.net.ConnectException: Connection refused
2017-02-24 11:08:14,871 WARN   [Thread-10][] com.cisco.epm.util.NodeCheckHelper -:::- Unable to
retrieve the host config from standby pap java.net.ConnectException: Connection refused
2017-02-24 11:08:14,871 WARN   [Thread-10][] com.cisco.epm.util.NodeCheckHelper -:::- returning
null from getHostConfigRemoteServer
2017-02-24 11:08:14,871 INFO   [Thread-10][] com.cisco.epm.util.NodeCheck -:::-
remotePrimaryConfig.getNodeRoleStatus() NULL
2017-02-24 11:08:14,871 INFO   [Thread-10][] com.cisco.epm.util.NodeCheck -:::-
remoteClusterInfo.getDeploymentName NULL
```

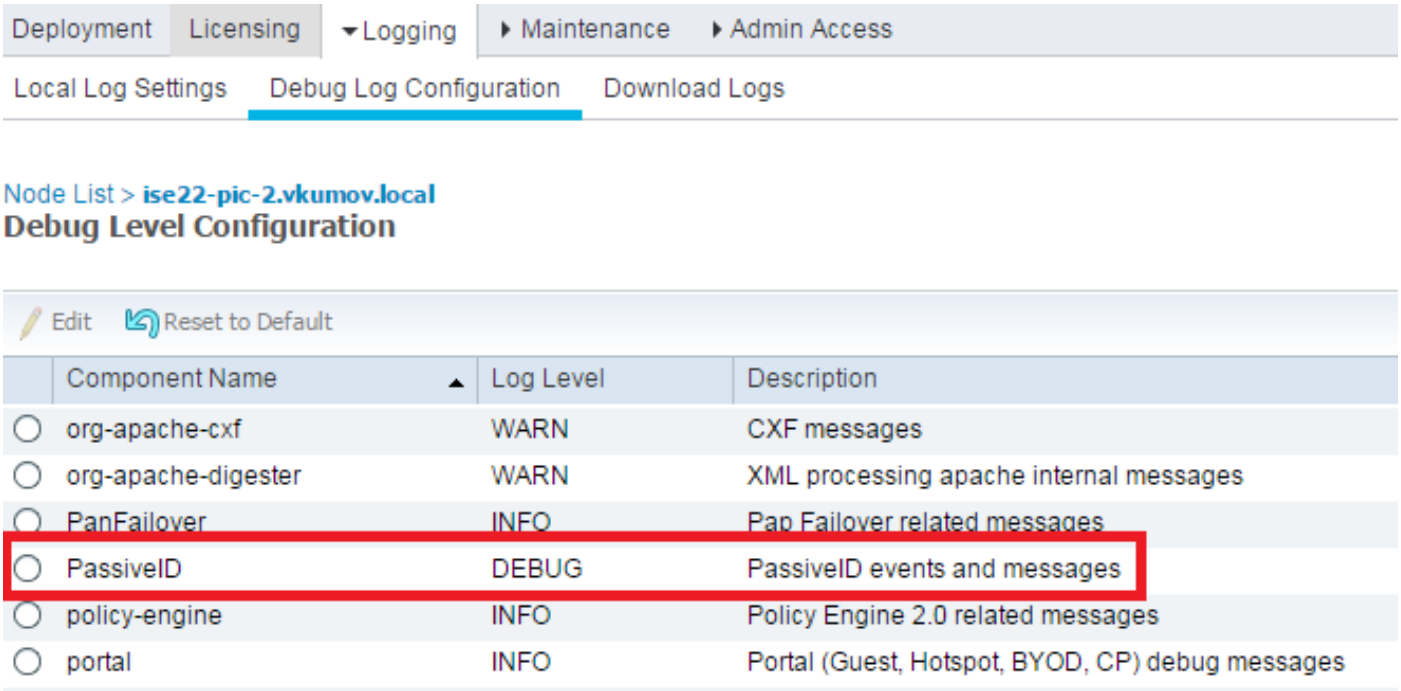
Actions de prendre : vérifiez l'état d'application sur le noeud secondaire, connexion réseau de contrôle si on permet toutes les connexions entre les Noeuds.

Répertoire actif et WMI

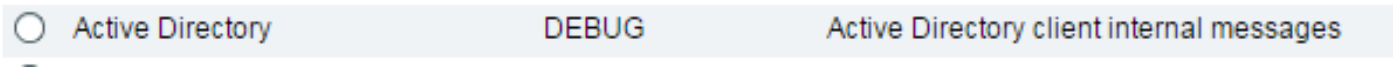
Pour dépanner le Répertoire actif WMI examinez ces fichiers :

- passive-wmi.log
- passive-endpoint.log
- ise-psc.log
- ad_agent.log

Et l'utile met au point peut activé à la **gestion > se connectant > configuration de log de debug** :



Et :



Voici un exemple d'une nouvelle session instruite de **passive-wmi.log** avec met au point activé :

2017-02-24 11:36:22,584 DEBUG [Thread-11][] com.cisco.idc.dc-probe- **New login event retrieved from Domain Controller**. Identity Mapping.ticket =
instance of **__InstanceCreationEvent**
{
SECURITY_DESCRIPTOR = {1, 0, 20, 128, 96, 0, 0, 0, 112, 0, 0, 0, 0, 0, 0, 0, 20, 0, 0, 0, 2, 0, 76, 0, 3, 0, 0, 0, 0, 0, 20, 0, 69, 0, 15, 0, 1, 1, 0, 0, 0, 0, 0, 5, 18, 0, 0, 0, 0, 0, 24, 0, 69, 0, 0, 0, 1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0, 0, 0, 24, 0, 65, 0, 0, 0, 1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 61, 2, 0, 0, 1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0, 1, 1, 0, 0, 0, 0, 0, 5, 18, 0, 0, 0};
TargetInstance =
instance of Win32_NTLogEvent
{
Category = 14339;
CategoryString = "Kerberos Authentication Service";
ComputerName = "MainDC.vkumov.local";
EventCode = 4768;
EventIdentifier = 4768;
EventType = 4;
InsertionStrings = {"Administrator", "vkumov.local", "S-1-5-21-2952046201-2792970045-1866348404-500", "krbtgt", "S-1-5-21-2952046201-2792970045-1866348404-502", "0x40810010", "0x0", "0x12", "2", "::1", "0", "", "", ""};
Logfile = "Security";
Message = "A Kerberos authentication ticket (TGT) was requested.
\n
\nAccount Information:
\n\tAccount Name:\t\tAdministrator
\n\tSupplied Realm Name:\tvkumov.local
\n\tUser ID:\t\t\tS-1-5-21-2952046201-2792970045-1866348404-500
\n
\nService Information:
\n\tService Name:\t\tkrbtgt
\n\tService ID:\t\tS-1-5-21-2952046201-2792970045-1866348404-502
\n
\nNetwork Information:
\n\tClient Address:\t\t::1
\n\tClient Port:\t\t0
\n
\nAdditional Information:
\n\tTicket Options:\t\t0x40810010
\n\tResult Code:\t\t0x0
\n\tTicket Encryption Type:\t0x12
\n\tPre-Authentication Type:\t2
\n
\nCertificate Information:
\n\tCertificate Issuer Name:\t\t
\n\tCertificate Serial Number:\t
\n\tCertificate Thumbprint:\t\t
\n
\nCertificate information is only provided if a certificate was used for pre-authentication.
\n
\nPre-authentication types, ticket options, encryption types and result codes are defined in RFC 4120.";
RecordNumber = 918032;
SourceName = "Microsoft-Windows-Security-Auditing";
TimeGenerated = "20170224103621.575178-000";
TimeWritten = "20170224103621.575178-000";
Type = "Audit Success";
};
TIME_CREATED = "131324061825752057";
};
 , Identity Mapping.dc-domainname = vkumov.local , Identity Mapping.dc-connection-type = Current events , Identity Mapping.dc-name = MainDC.vkumov.local , Identity Mapping.dc-host =

MainDC.vkumov.local/10.48.26.52 ,
2017-02-24 11:36:22,587 DEBUG [Thread-11][] com.cisco.idc.dc-probe- Replaced local IP. Identity Mapping.ticket =
instance of __InstanceCreationEvent
{
SECURITY_DESCRIPTOR = {1, 0, 20, 128, 96, 0, 0, 0, 112, 0, 0, 0, 0, 0, 0, 0, 20, 0, 0, 0, 2, 0, 76, 0, 3, 0, 0, 0, 0, 0, 20, 0, 69, 0, 15, 0, 1, 1, 0, 0, 0, 0, 0, 5, 18, 0, 0, 0, 0, 0, 24, 0, 69, 0, 0, 0, 1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0, 0, 0, 24, 0, 65, 0, 0, 0, 1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 61, 2, 0, 0, 1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0, 1, 1, 0, 0, 0, 0, 0, 5, 18, 0, 0, 0};
TargetInstance =
instance of Win32_NTLogEvent
{
Category = 14339;
CategoryString = "Kerberos Authentication Service";
ComputerName = "MainDC.vkumov.local";
EventCode = 4768;
EventIdentifier = 4768;
EventType = 4;
InsertionStrings = {"Administrator", "vkumov.local", "S-1-5-21-2952046201-2792970045-1866348404-500", "krbtgt", "S-1-5-21-2952046201-2792970045-1866348404-502", "0x40810010", "0x0", "0x12", "2", "::1", "0", "", "", ""};
Logfile = "Security";
Message = "A Kerberos authentication ticket (TGT) was requested.
\n
\nAccount Information:
\n\tAccount Name:\t\tAdministrator
\n\tSupplied Realm Name:\tvkumov.local
\n\tUser ID:\t\t\tS-1-5-21-2952046201-2792970045-1866348404-500
\n
\nService Information:
\n\tService Name:\t\tkrbtgt
\n\tService ID:\t\tS-1-5-21-2952046201-2792970045-1866348404-502
\n
\nNetwork Information:
\n\tClient Address:\t\t::1
\n\tClient Port:\t\t0
\n
\nAdditional Information:
\n\tTicket Options:\t\t0x40810010
\n\tResult Code:\t\t0x0
\n\tTicket Encryption Type:\t0x12
\n\tPre-Authentication Type:\t2
\n
\nCertificate Information:
\n\tCertificate Issuer Name:\t\t
\n\tCertificate Serial Number:\t
\n\tCertificate Thumbprint:\t\t
\n
\nCertificate information is only provided if a certificate was used for pre-authentication.
\n
\nPre-authentication types, ticket options, encryption types and result codes are defined in RFC 4120.";
RecordNumber = 918032;
SourceName = "Microsoft-Windows-Security-Auditing";
TimeGenerated = "20170224103621.575178-000";
TimeWritten = "20170224103621.575178-000";
Type = "Audit Success";
};
TIME_CREATED = "131324061825752057";
};
 , Identity Mapping.dc-domainname = vkumov.local , Identity Mapping.dc-connection-type = Current events , Identity Mapping.probe = WMI , Identity Mapping.event-local-ip-address = ::1 , Identity Mapping.dc-name = MainDC.vkumov.local , Identity Mapping.dc-host =

MainDC.vkumov.local/10.48.26.52 , Identity Mapping.server = ise22-pic-2 , Identity Mapping.event-ip-address = 10.48.26.52 ,
2017-02-24 11:36:22,589 DEBUG [Thread-11][] com.cisco.idc.dc-probe- Received login event. Identity Mapping.ticket =
instance of __InstanceCreationEvent
{
SECURITY_DESCRIPTOR = {1, 0, 20, 128, 96, 0, 0, 0, 112, 0, 0, 0, 0, 0, 0, 0, 20, 0, 0, 0, 2, 0, 76, 0, 3, 0, 0, 0, 0, 0, 20, 0, 69, 0, 15, 0, 1, 1, 0, 0, 0, 0, 0, 5, 18, 0, 0, 0, 0, 0, 24, 0, 69, 0, 0, 0, 1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0, 0, 0, 24, 0, 65, 0, 0, 0, 1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 61, 2, 0, 0, 1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0, 1, 1, 0, 0, 0, 0, 0, 5, 18, 0, 0, 0};
TargetInstance =
instance of Win32_NTLogEvent
{
Category = 14339;
CategoryString = "Kerberos Authentication Service";
ComputerName = "MainDC.vkumov.local";
EventCode = 4768;
EventIdentifier = 4768;
EventType = 4;
InsertionStrings = {"Administrator", "vkumov.local", "S-1-5-21-2952046201-2792970045-1866348404-500", "krbtgt", "S-1-5-21-2952046201-2792970045-1866348404-502", "0x40810010", "0x0", "0x12", "2", "::1", "0", "", "", ""};
Logfile = "Security";
Message = "A Kerberos authentication ticket (TGT) was requested.
\n
\nAccount Information:
\n\tAccount Name:\t\tAdministrator
\n\tSupplied Realm Name:\tvkumov.local
\n\tUser ID:\t\t\tS-1-5-21-2952046201-2792970045-1866348404-500
\n
\nService Information:
\n\tService Name:\t\tkrbtgt
\n\tService ID:\t\tS-1-5-21-2952046201-2792970045-1866348404-502
\n
\nNetwork Information:
\n\tClient Address:\t\t::1
\n\tClient Port:\t\t0
\n
\nAdditional Information:
\n\tTicket Options:\t\t0x40810010
\n\tResult Code:\t\t0x0
\n\tTicket Encryption Type:\t0x12
\n\tPre-Authentication Type:\t2
\n
\nCertificate Information:
\n\tCertificate Issuer Name:\t\t
\n\tCertificate Serial Number:\t
\n\tCertificate Thumbprint:\t\t
\n
\nCertificate information is only provided if a certificate was used for pre-authentication.
\n
\nPre-authentication types, ticket options, encryption types and result codes are defined in RFC 4120.";
RecordNumber = 918032;
SourceName = "Microsoft-Windows-Security-Auditing";
TimeGenerated = "20170224103621.575178-000";
TimeWritten = "20170224103621.575178-000";
Type = "Audit Success";
};
TIME_CREATED = "131324061825752057";
};
 , Identity Mapping.dc-domainname = vkumov.local , Identity Mapping.dc-connection-type = Current events , Identity Mapping.probe = WMI , Identity Mapping.event-local-ip-address = ::1 , Identity

```
Mapping.dc-name = MainDC.vkumov.local , Identity Mapping.event-user-name = Administrator ,
Identity Mapping.dc-host = MainDC.vkumov.local/10.48.26.52 , Identity Mapping.server = ise22-
pic-2 , Identity Mapping.event-ip-address = 10.48.26.52 ,
```

Exemple de contrôle de point final de **passive-endpoint.log** (dans ce cas le point final était unreacheable d'ISE) :

```
2017-02-24 11:36:22,584 DEBUG  [Thread-11][] com.cisco.idc.dc-probe- New login event retrieved
from Domain Controller. Identity Mapping.ticket =
instance of __InstanceCreationEvent
{
SECURITY_DESCRIPTOR = {1, 0, 20, 128, 96, 0, 0, 0, 112, 0, 0, 0, 0, 0, 0, 0, 20, 0, 0, 0, 2, 0,
76, 0, 3, 0, 0, 0, 0, 0, 20, 0, 69, 0, 15, 0, 1, 1, 0, 0, 0, 0, 0, 5, 18, 0, 0, 0, 0, 0, 24, 0,
69, 0, 0, 0, 1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0, 0, 0, 24, 0, 65, 0, 0, 0, 1, 2,
0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 61, 2, 0, 0, 1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0, 1,
1, 0, 0, 0, 0, 0, 5, 18, 0, 0, 0};
TargetInstance =
instance of Win32_NTLogEvent
{
Category = 14339;
CategoryString = "Kerberos Authentication Service";
ComputerName = "MainDC.vkumov.local";
EventCode = 4768;
EventIdentifier = 4768;
EventType = 4;
InsertionStrings = {"Administrator", "vkumov.local", "S-1-5-21-2952046201-2792970045-1866348404-
500", "krbtgt", "S-1-5-21-2952046201-2792970045-1866348404-502", "0x40810010", "0x0", "0x12",
"2", "::1", "0", "", "", ""};
Logfile = "Security";
Message = "A Kerberos authentication ticket (TGT) was requested.
\n
\nAccount Information:
\n\tAccount Name:\t\tAdministrator
\n\tSupplied Realm Name:\tvkumov.local
\n\tUser ID:\t\t\tS-1-5-21-2952046201-2792970045-1866348404-500
\n
\nService Information:
\n\tService Name:\t\tkrbtgt
\n\tService ID:\t\tS-1-5-21-2952046201-2792970045-1866348404-502
\n
\nNetwork Information:
\n\tClient Address:\t\t::1
\n\tClient Port:\t\t0
\n
\nAdditional Information:
\n\tTicket Options:\t\t0x40810010
\n\tResult Code:\t\t0x0
\n\tTicket Encryption Type:\t0x12
\n\tPre-Authentication Type:\t2
\n
\nCertificate Information:
\n\tCertificate Issuer Name:\t\t
\n\tCertificate Serial Number:\t
\n\tCertificate Thumbprint:\t\t
\n
\nCertificate information is only provided if a certificate was used for pre-authentication.
\n
\nPre-authentication types, ticket options, encryption types and result codes are defined in RFC
4120.";
RecordNumber = 918032;
SourceName = "Microsoft-Windows-Security-Auditing";
```

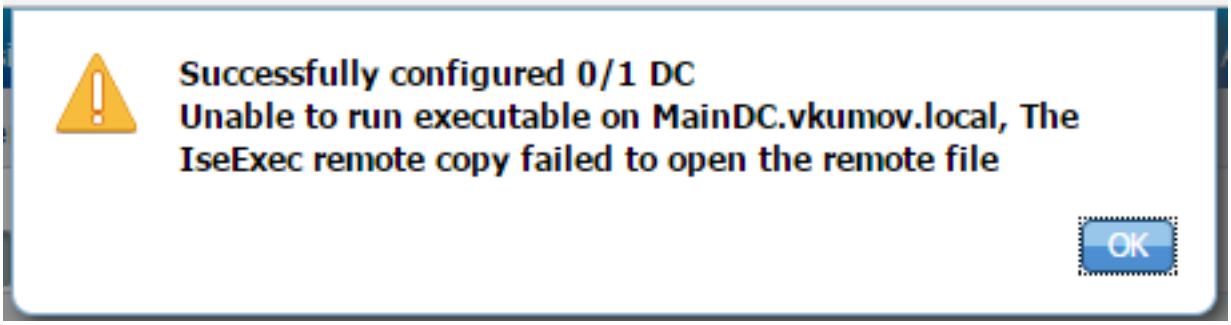
TimeGenerated = "20170224103621.575178-000";
TimeWritten = "20170224103621.575178-000";
Type = "Audit Success";
};
TIME_CREATED = "131324061825752057";
};
 , Identity Mapping.dc-domainname = vkumov.local , Identity Mapping.dc-connection-type = Current events , Identity Mapping.dc-name = MainDC.vkumov.local , Identity Mapping.dc-host = MainDC.vkumov.local/10.48.26.52 ,
2017-02-24 11:36:22,587 DEBUG [Thread-11][] com.cisco.idc.dc-probe- Replaced local IP. Identity Mapping.ticket =
instance of __InstanceCreationEvent
{
SECURITY_DESCRIPTOR = {1, 0, 20, 128, 96, 0, 0, 0, 112, 0, 0, 0, 0, 0, 0, 0, 20, 0, 0, 0, 2, 0, 76, 0, 3, 0, 0, 0, 0, 0, 20, 0, 69, 0, 15, 0, 1, 1, 0, 0, 0, 0, 0, 5, 18, 0, 0, 0, 0, 0, 24, 0, 69, 0, 0, 0, 1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0, 0, 0, 24, 0, 65, 0, 0, 0, 1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 61, 2, 0, 0, 1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0, 1, 1, 0, 0, 0, 0, 0, 5, 18, 0, 0, 0};
TargetInstance =
instance of Win32_NTLogEvent
{
Category = 14339;
CategoryString = "Kerberos Authentication Service";
ComputerName = "MainDC.vkumov.local";
EventCode = 4768;
EventIdentifier = 4768;
EventType = 4;
InsertionStrings = {"Administrator", "vkumov.local", "S-1-5-21-2952046201-2792970045-1866348404-500", "krbtgt", "S-1-5-21-2952046201-2792970045-1866348404-502", "0x40810010", "0x0", "0x12", "2", "::1", "0", "", "", ""};
Logfile = "Security";
Message = "A Kerberos authentication ticket (TGT) was requested.
\n
\nAccount Information:
\n\tAccount Name:\t\tAdministrator
\n\tSupplied Realm Name:\tvkumov.local
\n\tUser ID:\t\t\tS-1-5-21-2952046201-2792970045-1866348404-500
\n
\nService Information:
\n\tService Name:\t\tkrbtgt
\n\tService ID:\t\tS-1-5-21-2952046201-2792970045-1866348404-502
\n
\nNetwork Information:
\n\tClient Address:\t\t::1
\n\tClient Port:\t\t0
\n
\nAdditional Information:
\n\tTicket Options:\t\t0x40810010
\n\tResult Code:\t\t0x0
\n\tTicket Encryption Type:\t0x12
\n\tPre-Authentication Type:\t2
\n
\nCertificate Information:
\n\tCertificate Issuer Name:\t\t
\n\tCertificate Serial Number:\t
\n\tCertificate Thumbprint:\t\t
\n
\nCertificate information is only provided if a certificate was used for pre-authentication.
\n
\nPre-authentication types, ticket options, encryption types and result codes are defined in RFC 4120.";
RecordNumber = 918032;
SourceName = "Microsoft-Windows-Security-Auditing";
TimeGenerated = "20170224103621.575178-000";

TimeWritten = "20170224103621.575178-000";
Type = "Audit Success";
};
TIME_CREATED = "131324061825752057";
};
 , Identity Mapping.dc-domainname = vkumov.local , Identity Mapping.dc-connection-type = Current events , Identity Mapping.probe = WMI , Identity Mapping.event-local-ip-address = ::1 , Identity Mapping.dc-name = MainDC.vkumov.local , Identity Mapping.dc-host = MainDC.vkumov.local/10.48.26.52 , Identity Mapping.server = ise22-pic-2 , Identity Mapping.event-ip-address = 10.48.26.52 ,
2017-02-24 11:36:22,589 DEBUG [Thread-11][] com.cisco.idc.dc-probe- Received login event.
Identity Mapping.ticket =
instance of __InstanceCreationEvent
{
SECURITY_DESCRIPTOR = {1, 0, 20, 128, 96, 0, 0, 0, 112, 0, 0, 0, 0, 0, 0, 0, 20, 0, 0, 0, 2, 0, 76, 0, 3, 0, 0, 0, 0, 0, 20, 0, 69, 0, 15, 0, 1, 1, 0, 0, 0, 0, 0, 5, 18, 0, 0, 0, 0, 0, 24, 0, 69, 0, 0, 0, 1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0, 0, 0, 24, 0, 65, 0, 0, 0, 1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 61, 2, 0, 0, 1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0, 1, 1, 0, 0, 0, 0, 0, 5, 18, 0, 0, 0};
TargetInstance =
instance of Win32_NTLogEvent
{
Category = 14339;
CategoryString = "Kerberos Authentication Service";
ComputerName = "MainDC.vkumov.local";
EventCode = 4768;
EventIdentifier = 4768;
EventType = 4;
InsertionStrings = {"Administrator", "vkumov.local", "S-1-5-21-2952046201-2792970045-1866348404-500", "krbtgt", "S-1-5-21-2952046201-2792970045-1866348404-502", "0x40810010", "0x0", "0x12", "2", "::1", "0", "", "", ""};
Logfile = "Security";
Message = "A Kerberos authentication ticket (TGT) was requested.
\n
\nAccount Information:
\n\tAccount Name:\t\tAdministrator
\n\tSupplied Realm Name:\tvkumov.local
\n\tUser ID:\t\t\tS-1-5-21-2952046201-2792970045-1866348404-500
\n
\nService Information:
\n\tService Name:\t\tkrbtgt
\n\tService ID:\t\tS-1-5-21-2952046201-2792970045-1866348404-502
\n
\nNetwork Information:
\n\tClient Address:\t\t::1
\n\tClient Port:\t\t0
\n
\nAdditional Information:
\n\tTicket Options:\t\t0x40810010
\n\tResult Code:\t\t0x0
\n\tTicket Encryption Type:\t0x12
\n\tPre-Authentication Type:\t2
\n
\nCertificate Information:
\n\tCertificate Issuer Name:\t\t
\n\tCertificate Serial Number:\t
\n\tCertificate Thumbprint:\t\t
\n
\nCertificate information is only provided if a certificate was used for pre-authentication.
\n
\nPre-authentication types, ticket options, encryption types and result codes are defined in RFC 4120.";
RecordNumber = 918032;
SourceName = "Microsoft-Windows-Security-Auditing";

```
TimeGenerated = "20170224103621.575178-000";
TimeWritten = "20170224103621.575178-000";
Type = "Audit Success";
};
TIME_CREATED = "131324061825752057";
};
 , Identity Mapping.dc-domainname = vkumov.local , Identity Mapping.dc-connection-type = Current
events , Identity Mapping.probe = WMI , Identity Mapping.event-local-ip-address = ::1 , Identity
Mapping.dc-name = MainDC.vkumov.local , Identity Mapping.event-user-name = Administrator ,
Identity Mapping.dc-host = MainDC.vkumov.local/10.48.26.52 , Identity Mapping.server = ise22-
pic-2 , Identity Mapping.event-ip-address = 10.48.26.52 ,
```

Problème courant : La PIC ISE jette « incapable d'exécuter exécutable sur le name> <DC… » erreur

Si l'utilisateur qui est utilisé pour joindre la PIC ISE au domaine n'a pas assez d'autorisations, la PIC ISE jette une erreur pendant la configuration WMI :



Approprié met au point peut être trouvé au fichier d'**ad_agent.log** (le niveau de log de Répertoire actif devrait être placé POUR DÉBUGGER) :

```
26/02/2017 19:15:45,VERBOSE,139954093012736,SMBGSSContextNegotiate: state =
1,lwio/server/smbcommon/smbkrb5.c:460
26/02/2017 19:15:45,VERBOSE,139956055955200,Session 0x7f49bc001430 is eligible for
reaping,lwio/server/rdr/session2.c:290
26/02/2017 19:15:45,VERBOSE,139954101405440,Error at ../../lsass/server/auth-providers/ad-open-
provider/provider-main.c:7503 [code: C0000022],lsass/server/auth-providers/ad-open-
provider/provider-main.c:7503
26/02/2017 19:15:45,VERBOSE,139954101405440,Extended Error code: 60190 (symbol:
LW_ERROR_ISEEXEC_CP_OPEN_REMOTE_FILE),lsass/server/auth-providers/ad-open-provider/provider-
main.c:7627
26/02/2017 19:15:45,VERBOSE,139954101405440,Error at ../../lsass/server/auth-providers/ad-open-
provider/provider-main.c:7628 [code: C0000022],lsass/server/auth-providers/ad-open-
provider/provider-main.c:7628
26/02/2017 19:15:45,VERBOSE,139954101405440,Error code: 5 (symbol:
ERROR_ACCESS_DENIED),lsass/server/auth-providers/ad-open-provider/provider-main.c:7782
26/02/2017 19:15:45,VERBOSE,139954101405440,Error code: 5 (symbol:
ERROR_ACCESS_DENIED),lsass/server/auth-providers/ad-open-provider/provider-main.c:7855
26/02/2017 19:15:45,VERBOSE,139954101405440,Error code: 5 (symbol:
ERROR_ACCESS_DENIED),lsass/server/api/api2.c:2713
26/02/2017 19:15:45,VERBOSE,139956064347904,(session:ee880a4e15e682f4-08401b84f371a140)
Dropping: LWMSG_STATUS_PEER_CLOSE,lwmsg/src/peer-task.c:625
26/02/2017 19:15:50,VERBOSE,139956055955200,RdrSocketRelease(0x7f496800b6e0, 38): socket is
eligible for reaping,lwio/server/rdr/socket.c:2239
```

Actions de prendre : Re-joignez les Noeuds PIC ISE au domaine avec des qualifications d'administrateur de domaine ou ajoutez l'utilisateur pour lequel est utilisé joignent l'exécution au groupe d'*admins de domaine* dans l'AD.