تكوين ISE 2.2 PIC مع موفر WMI ل Active Directory

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
معلومات أساسية
الرسم التخطيطي للشبكة
سير العمل
التكوين
تكوين نشر ISE PIC
الخطوة 1 (اختيارية). تثبيت الشهادات الموثوق بها.
الخطوة 2 (اختيارية). تثبيت شهادات النظام.
الخطوة 3. قم بإضافة عقدة ثانوية إلى النشر.
تكوين موفر خدمة Active Directory
الخطوة 1. انضم إلى ISE PIC إلى المجال.
الخطوة 2. ضبط الأذونات على AD.
الخطوة 3. إضافة وكلاء PassiveID.
التحقق من الصحة
النشر
صفحة النشر
صفحة حول المعلومات
مكتبة
ملخص النظام
المورفون والجلسات
الصفحة الرئيسية
جلسات عمل مباشرة
استكشاف الأخطاء وإصلاحها
النشر
المشكلة المشتركة: العقدة الثانوية غير قابلة للوغ
Active Directory و WMI
المشكلة الشائعة: ISE PIC Throws "يتعذر تشغيل الملف التنفيذي على

المقدمة

يوضح هذا المستند كيفية تكوين نشر موصل الهوية الخامل (ISE PIC) لمحرك خدمات الهوية واستكشاف أخطاء هذا النشر وإصلاحها باستخدام موفر Active Directory Windows Management Instrumentation (AD WMI). ISE PIC هو إصدار ISE خفيف الوزن يركز على ميزات معرف الخامل.

ISE PIC هو حل معرف واحد لجميع حزم أمان Cisco التي تستخدم الهوية السلبية فقط. وهذا يعني أنه ال يمكن تكوين التخويل أو السياسات على ISE PIC. وهو يدعم موفرين مختلفين

(الوكلاء و WMI و Syslog و API) ويمكن دمجهم عبر واجهة برمجة تطبيقات REST. لديه قدرات للاستعلام عن نقاط النهاية (هل قام المستخدم بتسجيل الدخول؟ هل لا تزال نقطة النهاية متصلة؟)

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة أساسية بالمواضيع التالية:

- محرك خدمة الهوية من Cisco
- Microsoft Active Directory
- Microsoft WMI

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Cisco Identity Service Engine Passive Identity Connector، الإصدار 2.2.0.470
- Microsoft Windows 7 Service Pack 1
- نظام التشغيل Microsoft Windows Server 2012 R2

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

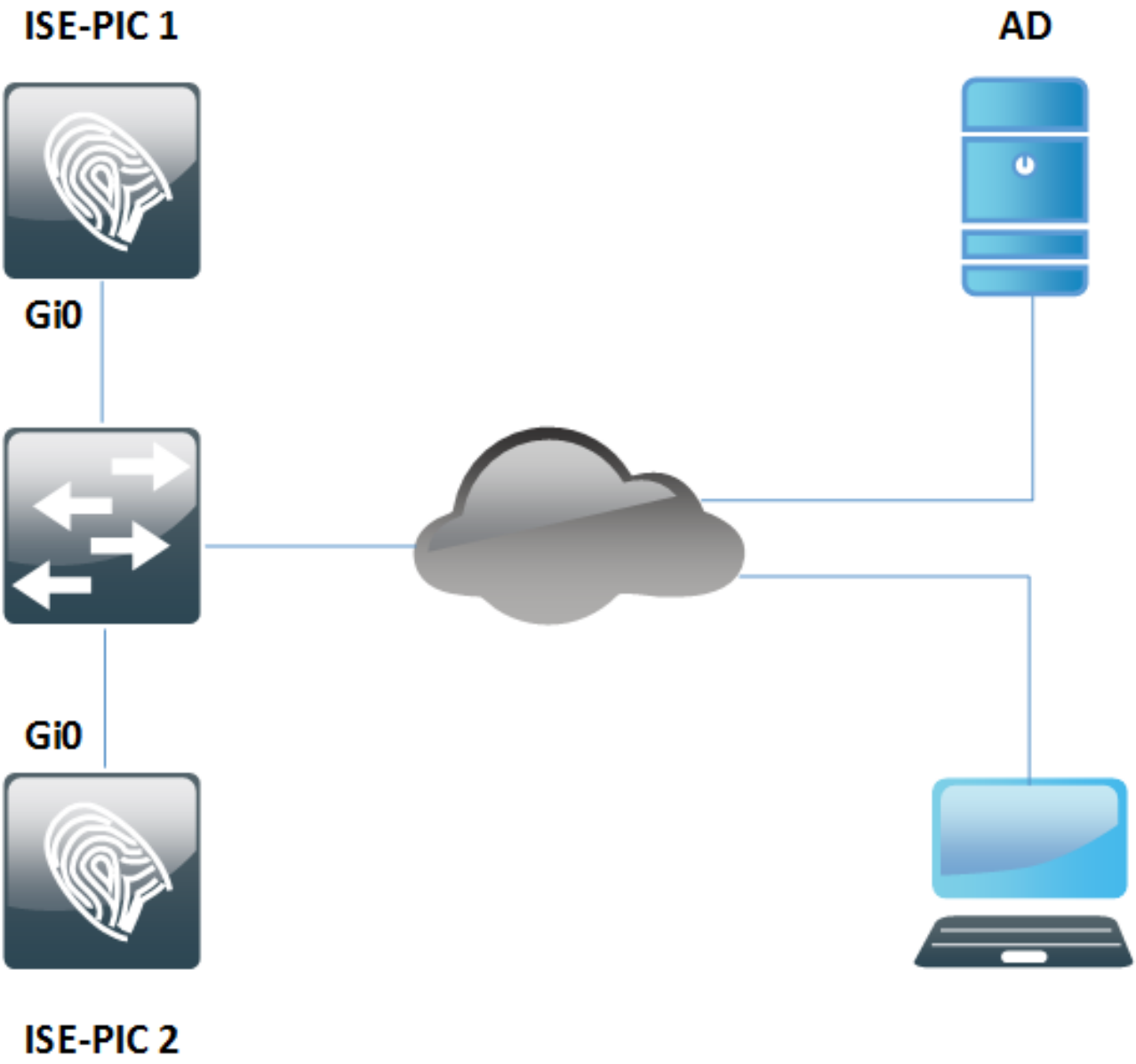
الحد الأقصى لعدد العقد في نشر طاقة ISE PIC هو 2. يوضح هذا المثال كيفية تكوين نشر طاقة ISE PIC للحصول على توفر عال، وبالتالي يتم إستخدام جهازين افتراضيين (VM). في نشر طاقة ISE PIC، يمكن أن يكون للعقد أدوار: أساسي وثانوي. في هذه العقدة الوحيدة يمكن أن تكون أساسية في المرة الواحدة ويمكن تغيير الأدوار يدويا فقط من خلال واجهة المستخدم الرسومية (GUI). في حالة الفشل الأساسي، لا تزال جميع المميزات قيد التشغيل على الثانوية باستثناء واجهة المستخدم. لا يمكن واجهة المستخدم سوى الترقية اليدوية إلى الأساسي.

يوضح هذا المثال كيفية تكوين موفر WMI ل Active Directory. يتكون WMI من مجموعة من الملحقات لنموذج برنامج تشغيل Windows توفر واجهة نظام تشغيل توفر من خلالها المكونات المزودة بالأدوات المعلومات والإشعارات. WMI هي تطبيق Microsoft لمعايير إدارة المؤسسات القائمة على الويب (WBEM) ونموذج المعلومات المشتركة (CIM) من فريق عمل الإدارة الموزعة (DMTF).

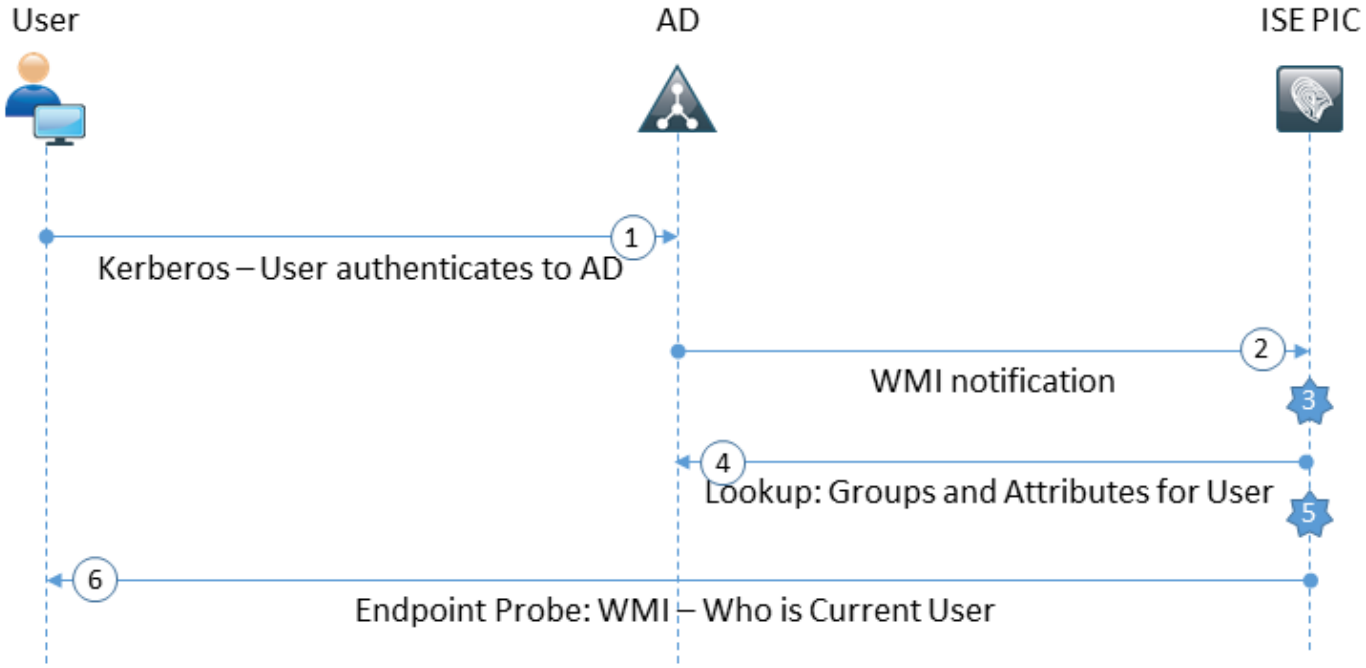
> **ملاحظة:** يمكن العثور على مزيد من المعلومات حول WMI في موقع Microsoft الرسمي: حول WMI

الرسم التخطيطي للشبكة

تستخدم المعلومات الواردة في المستند إعداد الشبكة الموضح في الصورة:



سير العمل



1. قم بتسجيل الدخول إلى الكمبيوتر وتتم المصادقة عليه على AD.

2. تقوم WMI بإعلام ISE PIC حول هذه المصادقة.

3. يضيف ISE اسم مستخدم الربط:IP_ADDRESS إلى دليل جلسة العمل الخاص به.

4. يسترجع ISE مجموعات وسمات المستخدم من AD.

5. يقوم ISE بحفظ هذه المعلومات في دليل جلسة العمل الخاص به.

6. تقوم بطاقة ISE PIC كل 4 ساعات (غير قابلة للتكوين) بتشغيل Endpoint Probe: أولا، يحاول WMI إلى نقطة النهاية.في حالة فشل WMI، يقوم ISE PIC بتشغيل ISEExec. يقوم باستعلام نقطة النهاية للمستخدم وتمكين WMI في المرة القادمة.كما أن ISE PIC يستعيد عنوان MAC الخاص بنقطة النهاية ونوع نظام التشغيل.

   في ISE PIC، من الممكن فقط تمكين/تعطيل إختبارات نقطة النهاية. تقوم العقدة الأساسية باستعلام كافة نقاط النهاية، بينما تستخدم العقدة الثانوية في حالة التوفر العالي فقط.

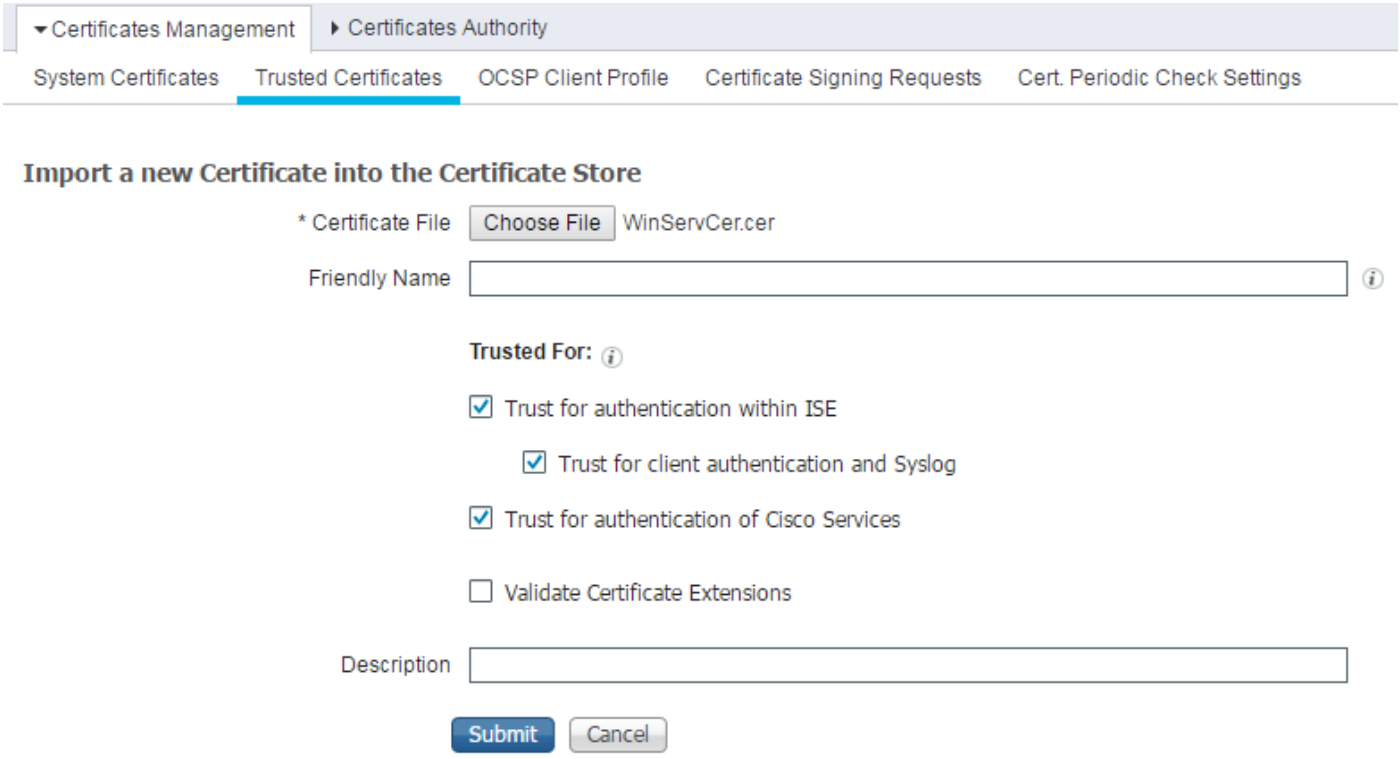
التكوين

تكوين نشر ISE PIC

الخطوة 1 (اختيارية). تثبيت الشهادات الموثوق بها.

يجب تثبيت سلسلة الشهادات الكاملة الخاصة ب "المرجع المصدق" (CA) على مخزن ISE الموثوق. قم بتسجيل الدخول إلى واجهة المستخدم الرسومية ISE PIC وانتقل إلى **الشهادات > إدارة الشهادات > الشهادات الموثوق بها**. انقر على **إستيراد** وحدد شهادة المرجع المصدق من الكمبيوتر.

كما هو موضح في الصورة، انقر فوق **إرسال** لحفظ التغييرات. كرر هذه الخطوة لجميع شهادات السلسلة. كرر الخطوات على العقدة الثانوية أيضا.

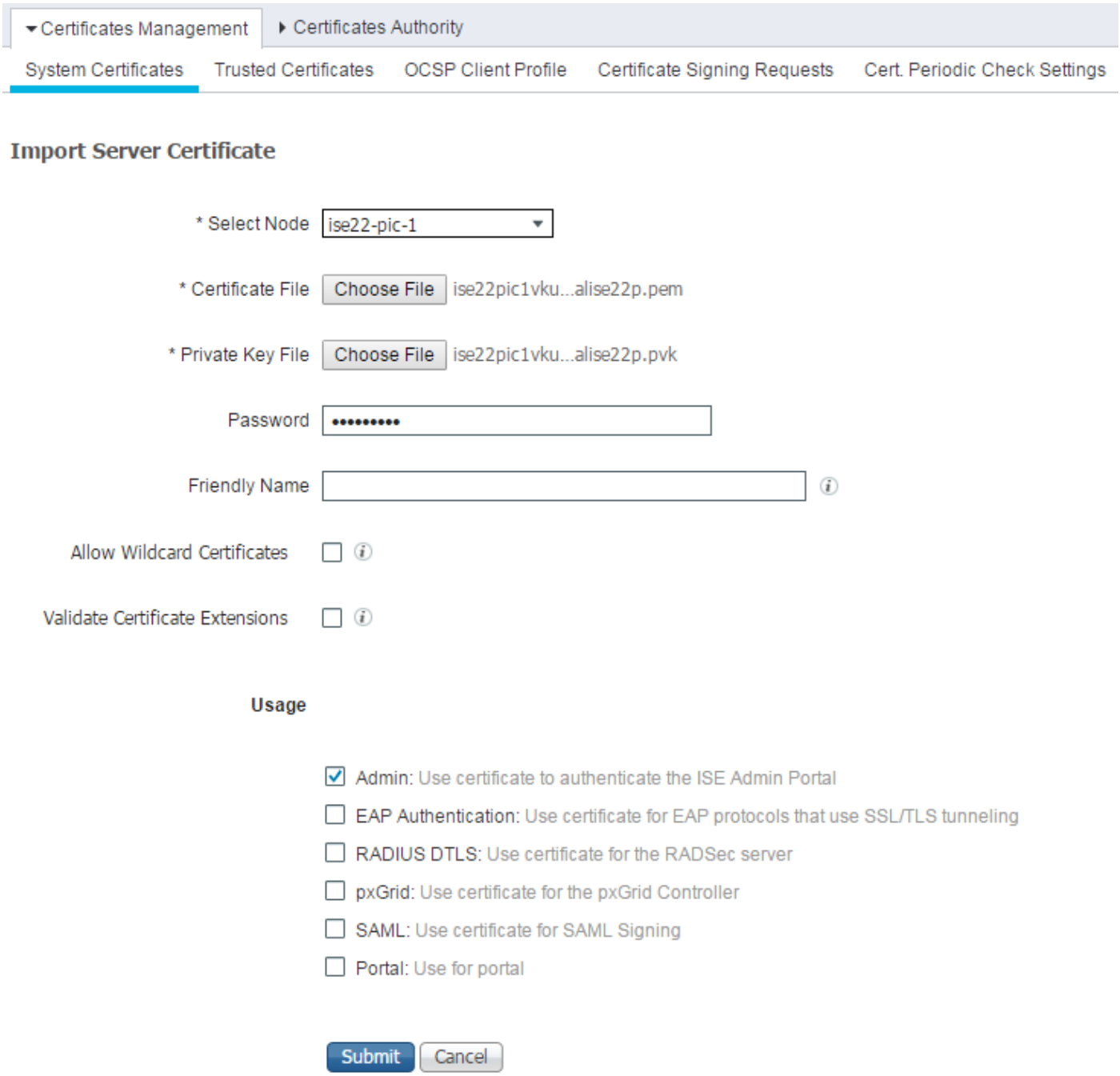


الخطوة 2 (اختيارية). تثبيت شهادات النظام.

خيار 1. الشهادات التي تم إنشاؤها بالفعل بواسطة CA بالإضافة إلى المفتاح الخاص.

انتقل إلى **الشهادات > إدارة الشهادات > شهادات النظام** وانقر **إستيراد**. حدد **ملف الشهادة** و**ملف المفتاح الخاص**، أدخل حقل *كلمة المرور* إذا تم تشفير المفتاح الخاص.

كما هو موضح في خيارات التحقق من **الاستخدام** بالصورة:



ملاحظة: نظرا لأن بطاقة ISE PIC تستند إلى رمز ISE ويمكن تحويلها بسهولة إلى نظام ISE كامل المميزات مع الترخيص المناسب، فإن جميع خيارات الاستخدام متوفرة. لا تستخدم الأدوار مثل **مصادقة EAP** و**RADIUS DTLS** و**SAML** و**Portal** بواسطة ISE PIC.

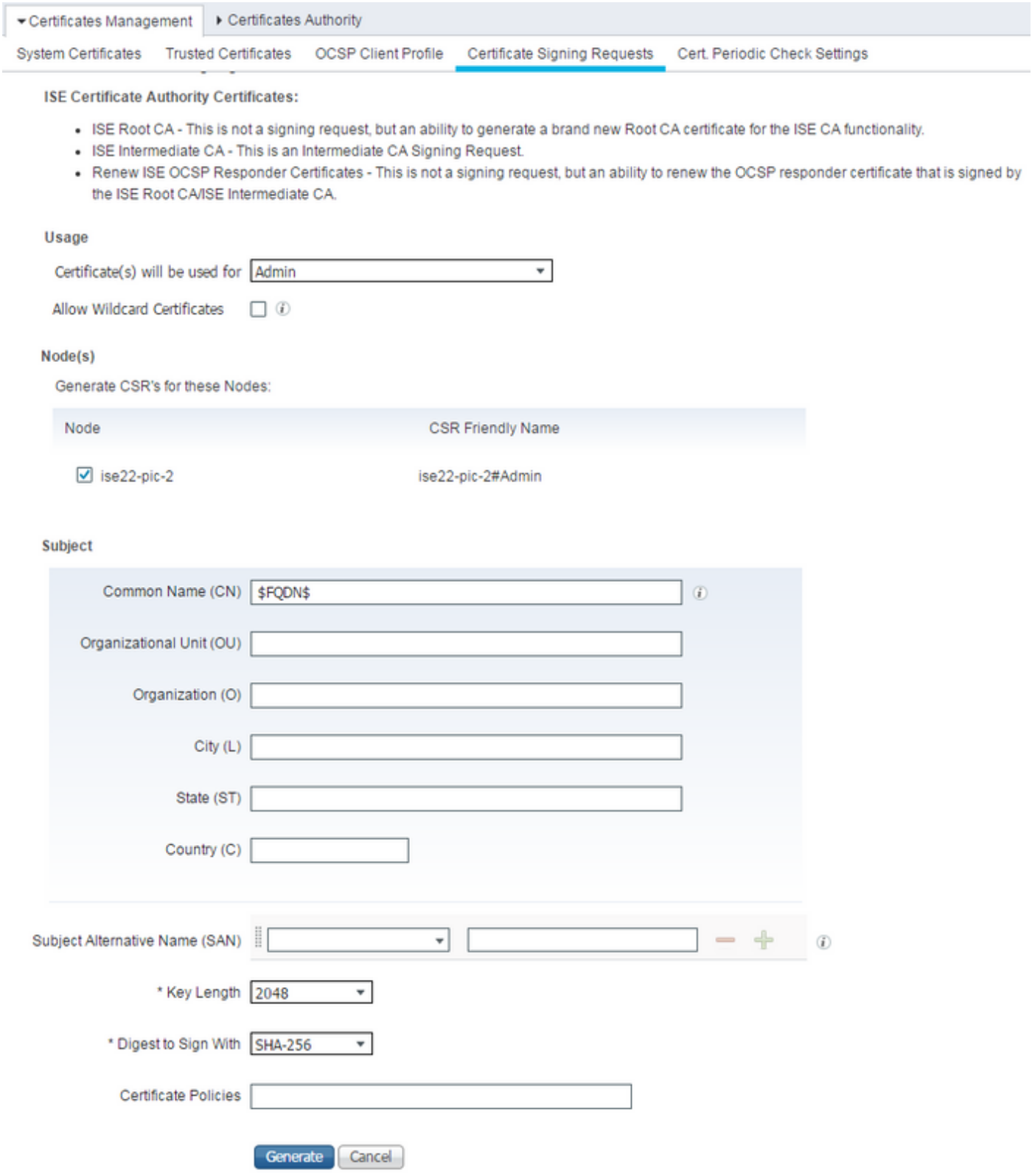
انقر على **إرسال** لتثبيت الشهادة. كرر هذا الإجراء على عقدة ثانوية أيضا.

ملاحظة: تتم إعادة تشغيل جميع الخدمات الموجودة على عقدة ISE PIC بعد استيراد شهادة الخادم.

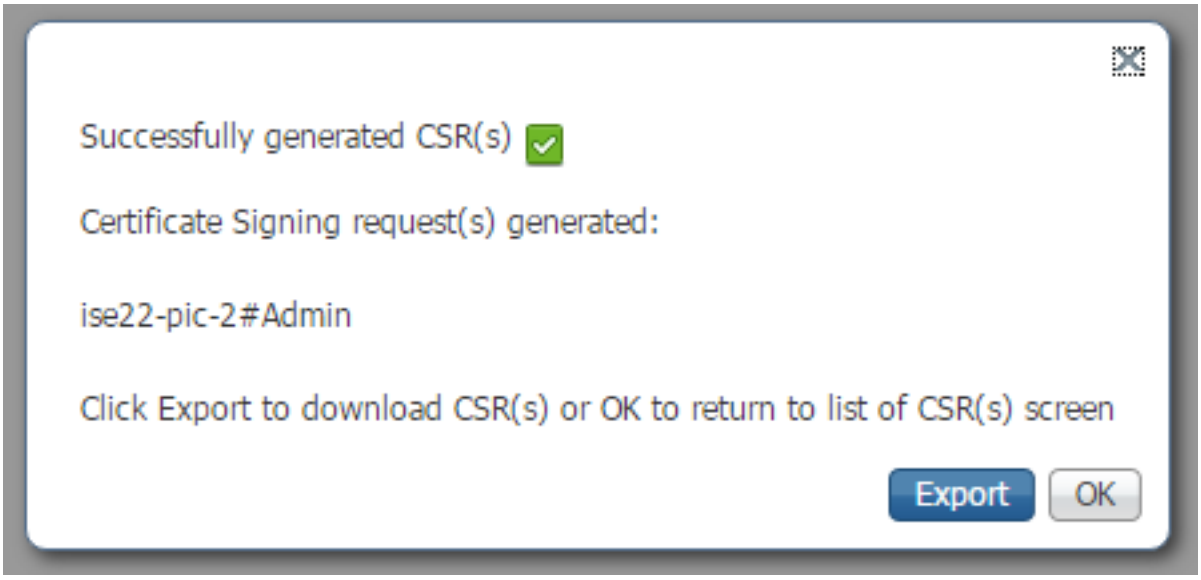
الخيار 2. إنشاء طلب توقيع الشهادة (CSR)، وتوقيعه باستخدام CA والربط على ISE.

انتقل إلى **الشهادات > إدارة الشهادات >** صفحة **طلبات توقيع الشهادات** وانقر **إنشاء طلبات توقيع الشهادات (CSR)**.

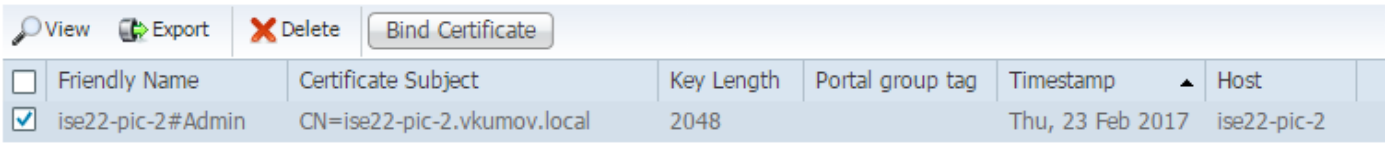
حدد العقدة والاستخدام وأدخل الحقول الأخرى إذا لزم الأمر:



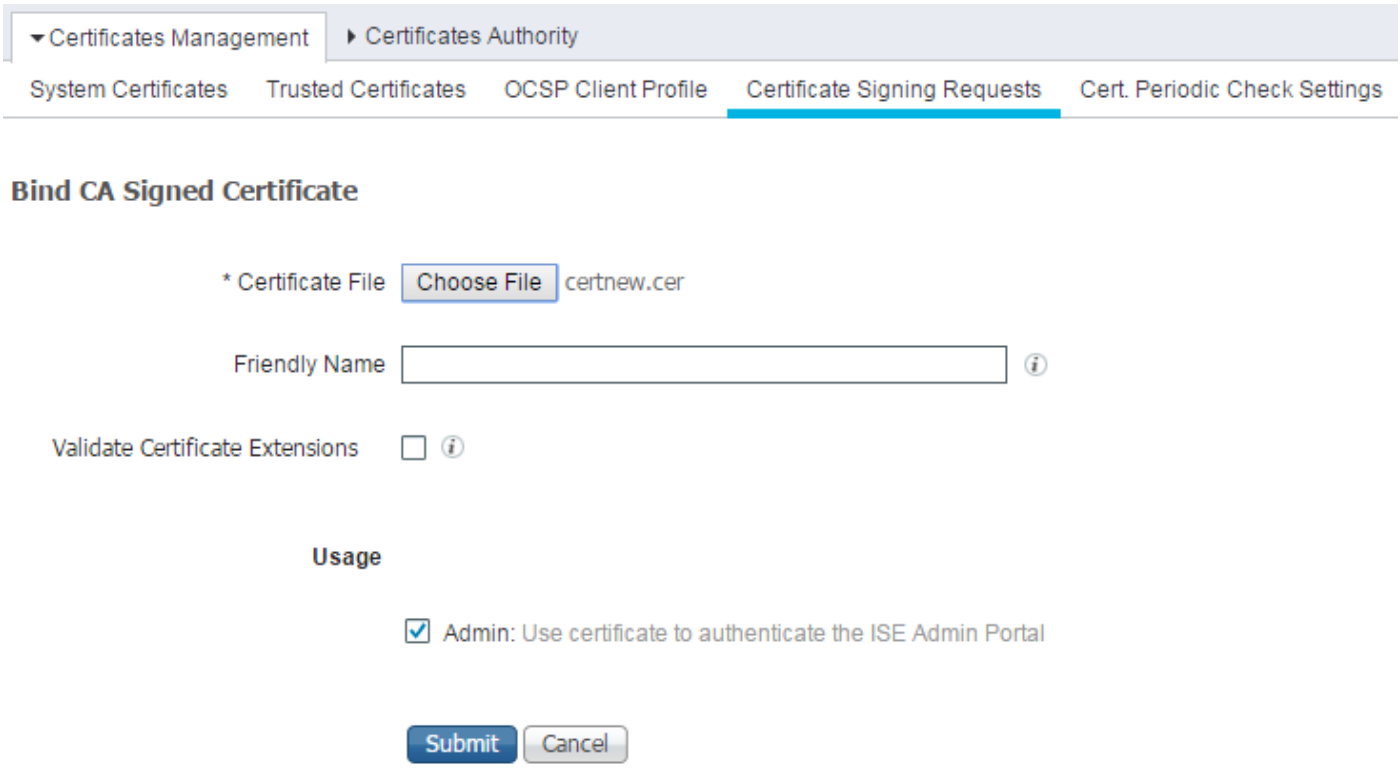
انقر على **إنشاء.** تظهر نافذة جديدة مع خيار **تصدير** CSR **الذي** تم إنشاؤه:



انقر على **تصدير**، احفظ ملف **PEM** الذي تم إنشاؤه وتوقيعه باستخدام CA. عندما يتم توقيع CSR، انتقل إلى **الإدارة > الشهادات > طلبات توقيع الشهادات**، حدد CSR الخاص بك وانقر **ربط الشهادة**:



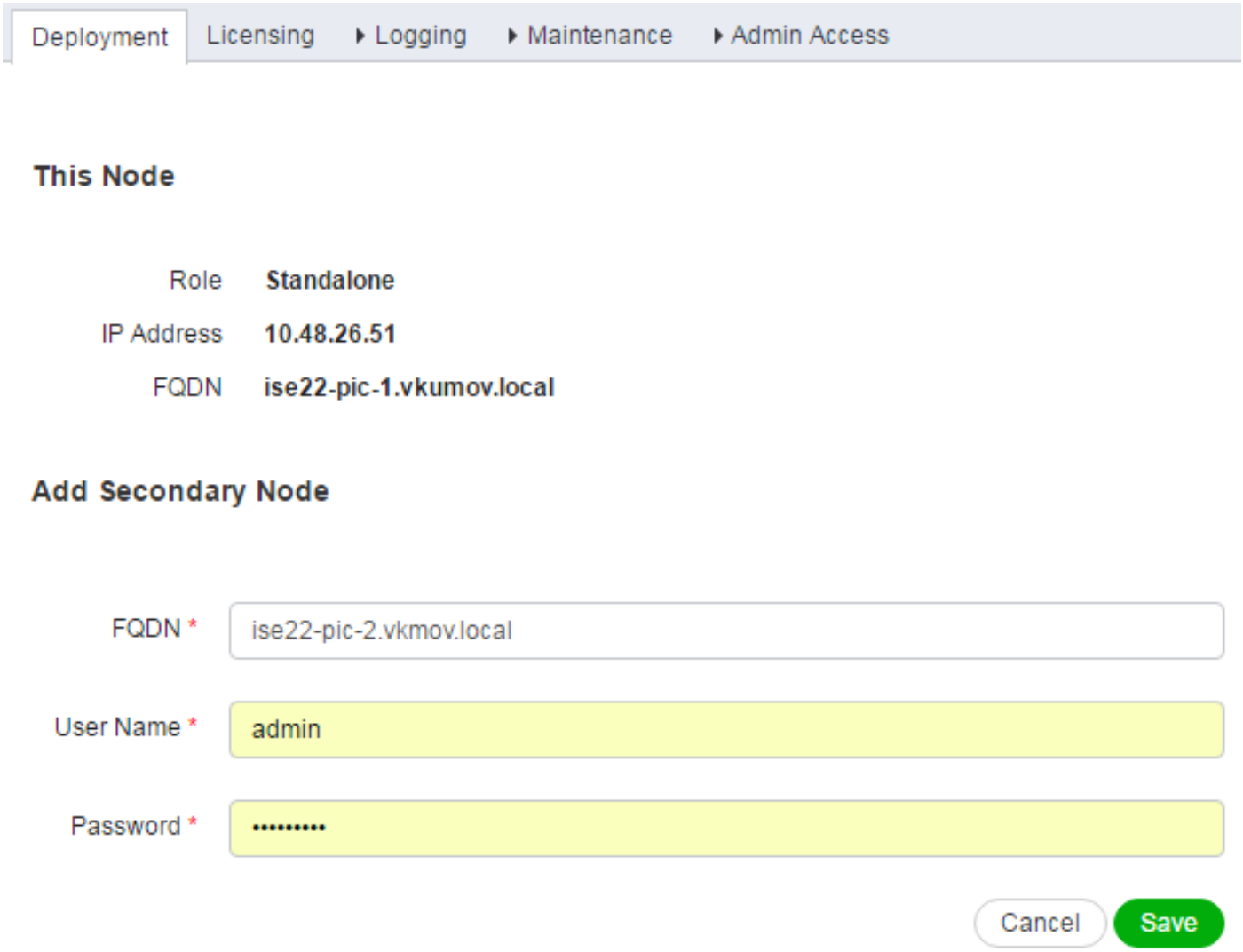
حدد الشهادة الموقعة مع المرجع المصدق وانقر على **إرسال** لتطبيق التغييرات:



تتم إعادة تشغيل جميع الخدمات الموجودة على عقدة ISE PIC بعد النقر فوق **إرسال** لتثبيت الشهادة.

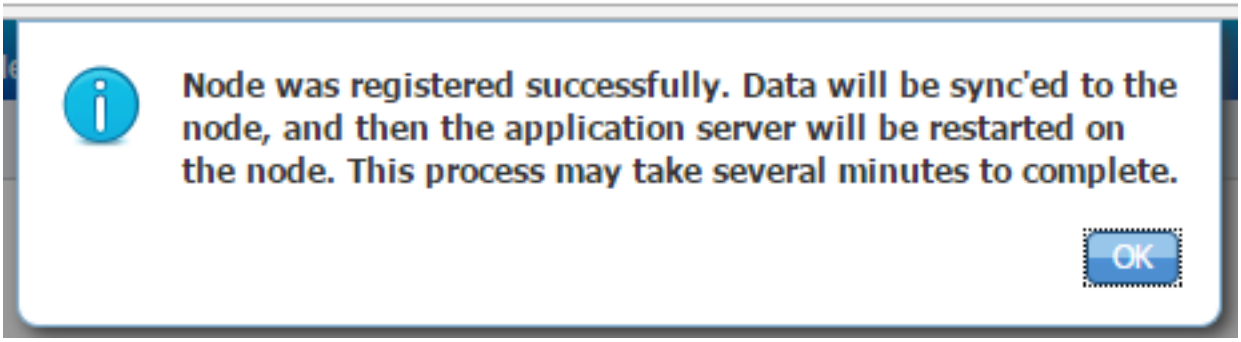
الخطوة 3. قم بإضافة عقدة ثانوية إلى النشر.

يسمح ISE PIC بوجود عقدتين في عملية نشر للحصول على توفر فائق. الا يتطلب الأمر أن يكون لديك ثقة ثنائية الإتجاه بالشهادات (مقارنة بنشر ISE المعتاد). لإضافة عقدة ثانوية إلى النشر، انتقل إلى **إدارة > صفحة نشر** على عقدة ISE PIC الأساسية، كما هو موضح في الصورة:

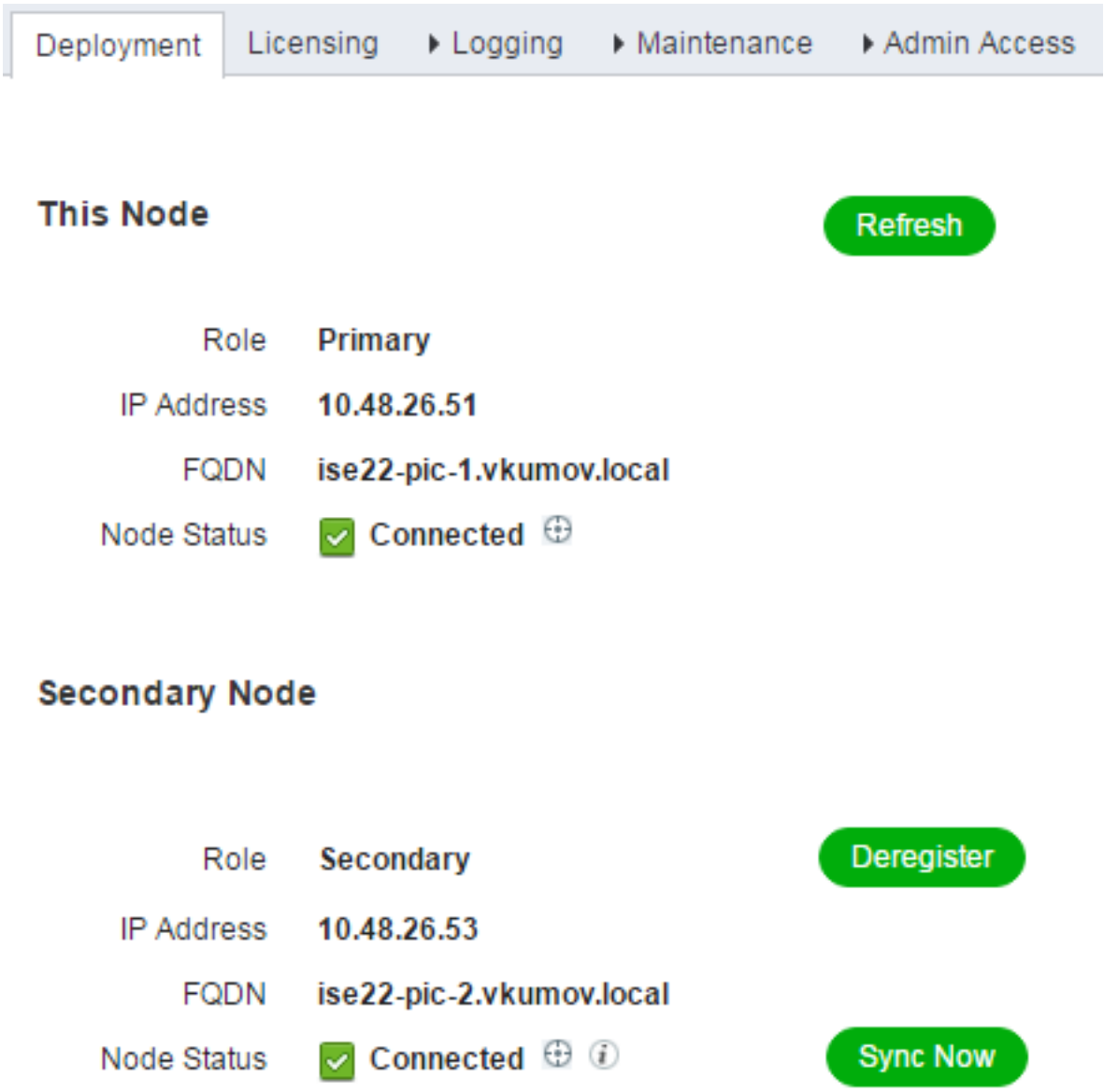


أدخل اسم المجال المؤهل بالكامل (FQDN) للعقدة الثانوية، وبيانات اعتماد المسؤول لتلك العقدة وانقر فوق **حفظ**. في حالة عدم قدرة عقدة ISE الأساسية على التحقق من شهادة مسؤول العقدة الثانية، تطلب تأكيدا قبل تثبيت تلك الشهادة في المخزن الموثوق به.

في هذه الحالة انقر فوق **إستيراد الشهادة وتابع** للانضمام إلى العقدة إلى النشر. يجب أن تحصل على إعلام بأن العقدة قد تمت إضافتها بنجاح. تتم إعادة تشغيل جميع الخدمات على العقدة الثانوية.



يجب مزامنة العقد في غضون 10 إلى 20 دقيقة ويجب تغيير حالة العقدة من **قيد التقدم** إلى **متصل**:



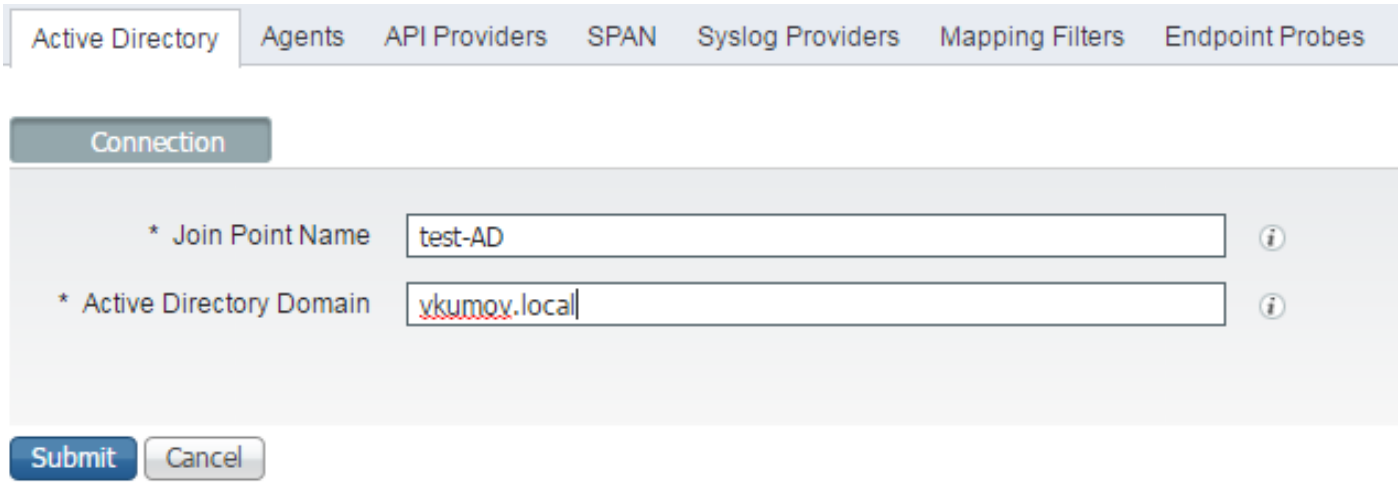
تكوين موفري خدمة Active Directory

يستخدم ISE PIC Windows Management Instrumentation (WMI) لجمع المعلومات عن جلسات العمل من AD ويعمل مثل اتصال Pub/Sub، مما يعني:

- يشترك ISE PIC في أحداث معينة
- تنبه WMI ISE PIC عند حدوث هذه الأحداث: 4768 (منح البطاقات ل Kerberos) و 4770 (تجديد البطاقات ل Kerberos)انتهاء صلاحية الإدخالات في دليل جلسة العمل (الإزالة)

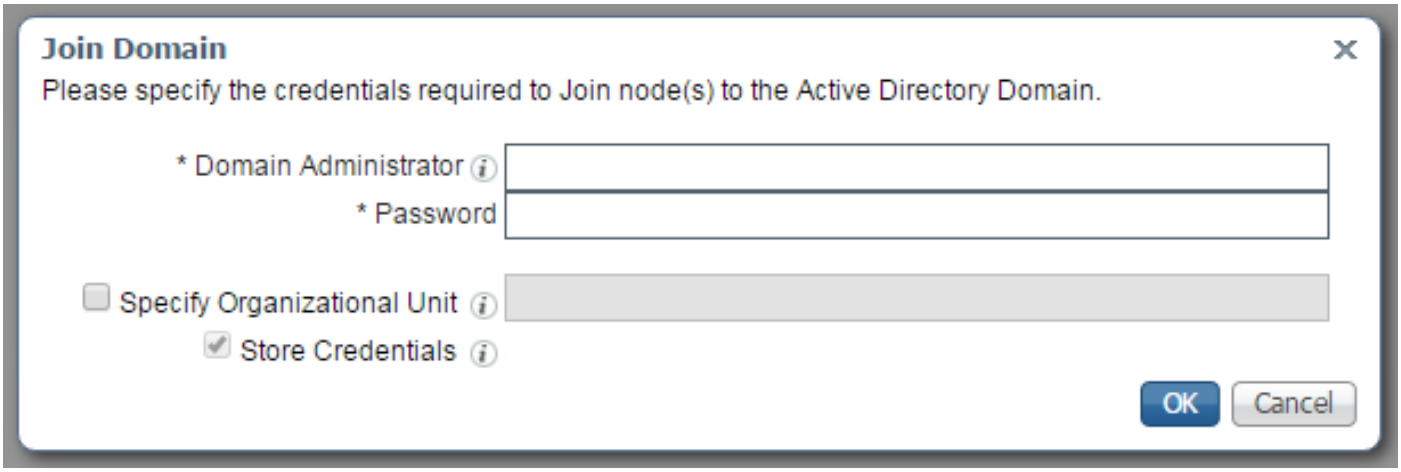
الخطوة 1. انضم إلى ISE PIC إلى المجال.

من أجل ضم ISE PIC إلى المجال، انتقل إلى **موفري > Active Directory** وانقر فوق **إضافة**:



قم بتعبئة حقلي **اسم نقطة الاتصال** و**مجال Active Directory** وانقر فوق **إرسال** لحفظ التغييرات. **اسم نقطة الربط** هو اسم يتم إستخدامه في ISE PIC فقط. **مجال Active Directory** هو اسم المجال الذي يجب فيه ضم ISE PIC ويجب أن يكون قابلا للحل مع خادم DNS الذي تم تكوينه على ISE PIC.

بعد إنشاء Join Point ISE PIC يجب أن يسألك إذا كنت ترغب في ضم العقد إلى المجال. طقطقة **نعم**. يجب أن يظهر إطار لكي توفر بيانات اعتماد للانضمام إلى المجال:



ألم **مدير المجال** وحقول **كلمة المرور** وانقر على **موافق**.

على الرغم من أن الحقل يسمى **Domain Administrator**، إلا أنه ليس من الضروري إستخدام مستخدم المسؤول **للانضمام إلى** ISE PIC إلى المجال. يجب أن يتمتع هذا المستخدم بامتيازات كافية لإنشاء حسابات أجهزة في المجال وإزالتها، أو تغيير كلمات المرور لحسابات الأجهزة التي تم إنشاؤها مسبقا. يمكن العثور على أذونات حساب Active Directory المطلوبة لتنفيذ عمليات مختلفة في هذا المستند.

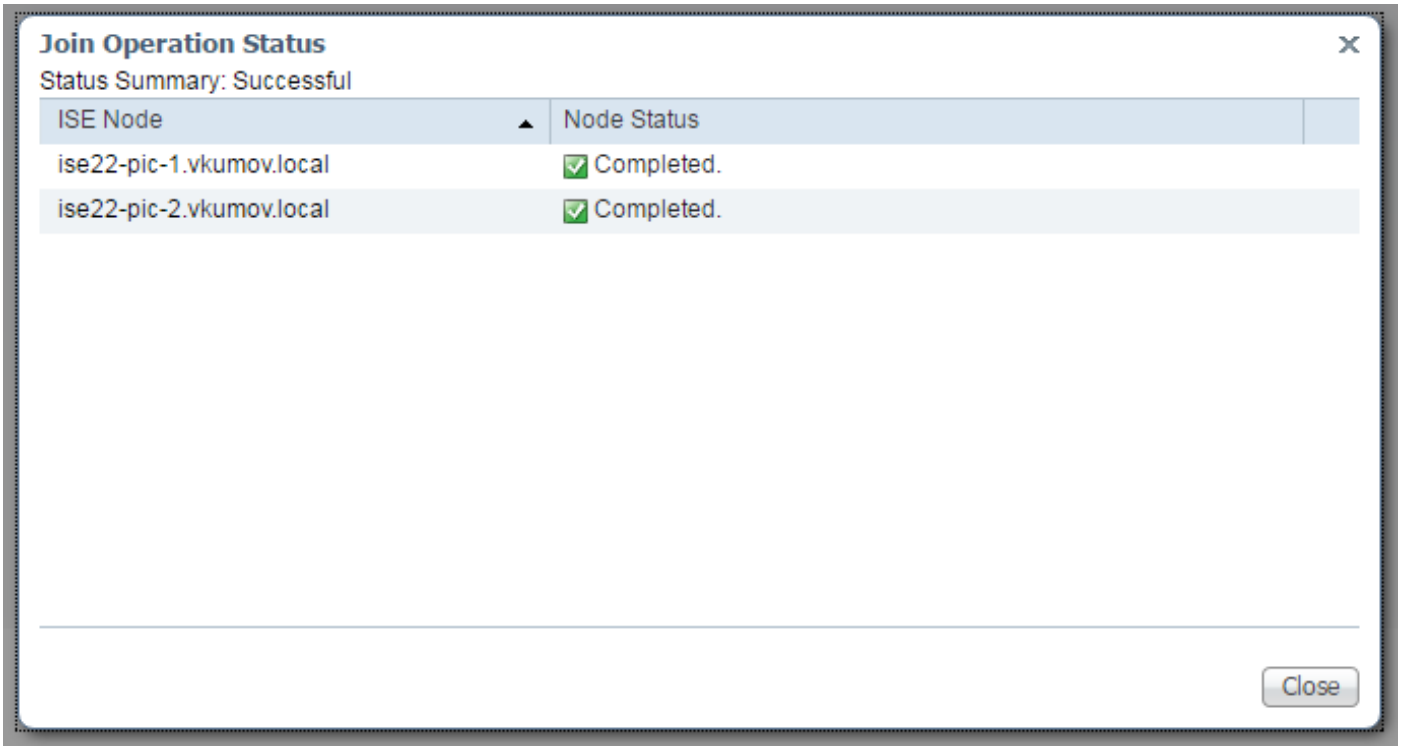
ومع ذلك، يجب إستخدام بيانات اعتماد مسؤول المجال أثناء الانضمام إذا كنت ترغب في إستخدام WMI. يتطلب خيار **تكوين WMI**:

- تغييرات السجل
- أذونات الاستخدام DCOM
- أذونات الاستخدام WMI عن بعد

- الوصول لقراءة سجل أحداث الأمان الخاص بوحدة التحكم بمجال AD
- يجب أن يسمح جدار حماية Windows لحركة مرور البيانات من/إلى ISE PIC (سيتم إنشاء سياسات جدار حماية Windows المطابقة أثناء **تكوين WMI**)

  ملاحظة: يتم دائما تمكين **بيانات اعتماد التخزين** على بطاقة ISE PIC نظرا لأنها مطلوبة لاستكشافات نقاط النهاية وتكوين WMI. يقوم قسم خدمات الهوية (ISE) بتخزين هذه المنتجات مشفرة داخليا.

كما هو موضح في الصورة، تعرض ISE PIC نتيجة العملية في نافذة جديدة:



الخطوة 2. ضبط الأذونات على AD.

التحقق من أذونات المستخدم في AD وفقا للمستند: تثبيت Identity Engine Passive Identity Connector (ISE-PIC) دليل المسؤول:

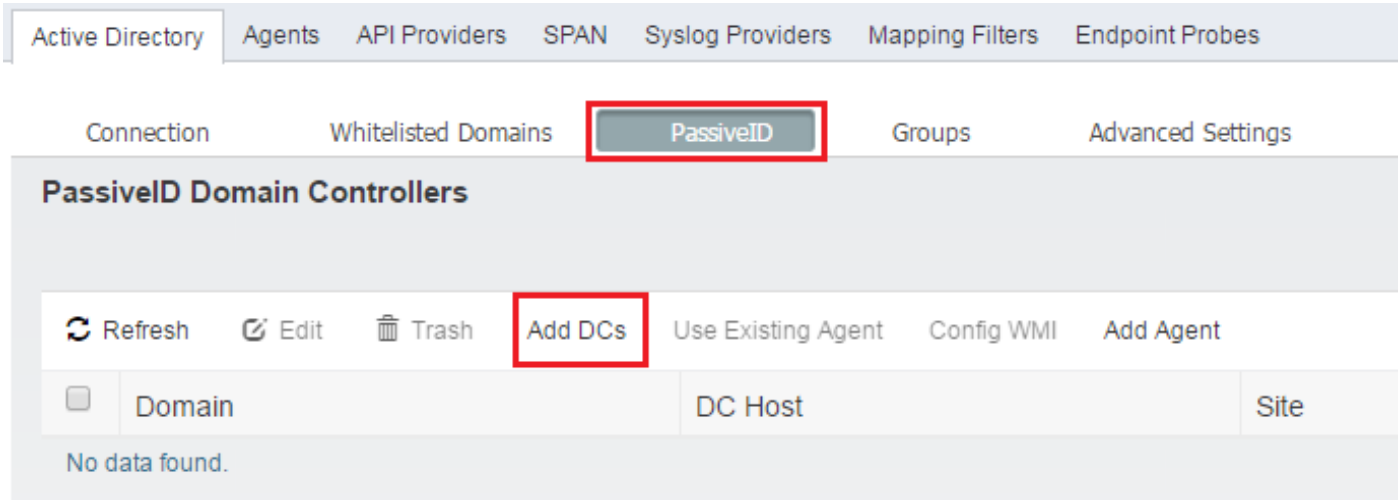
تعيين الأذونات عند مستخدم AD في مجموعة مسؤول المجال

بالنسبة لنظام التشغيل Windows 2008 R2 و Windows 2012 و Windows 2012 R2، لا تملك مجموعة إدارة المجال بشكل افتراضي التحكم الكامل في مفاتيح تسجيل معينة في نظام تشغيل Windows. يجب أن يمنح مسؤول Active Directory أذونات التحكم الكامل لمستخدم Active Directory على مفاتيح التسجيل التالية

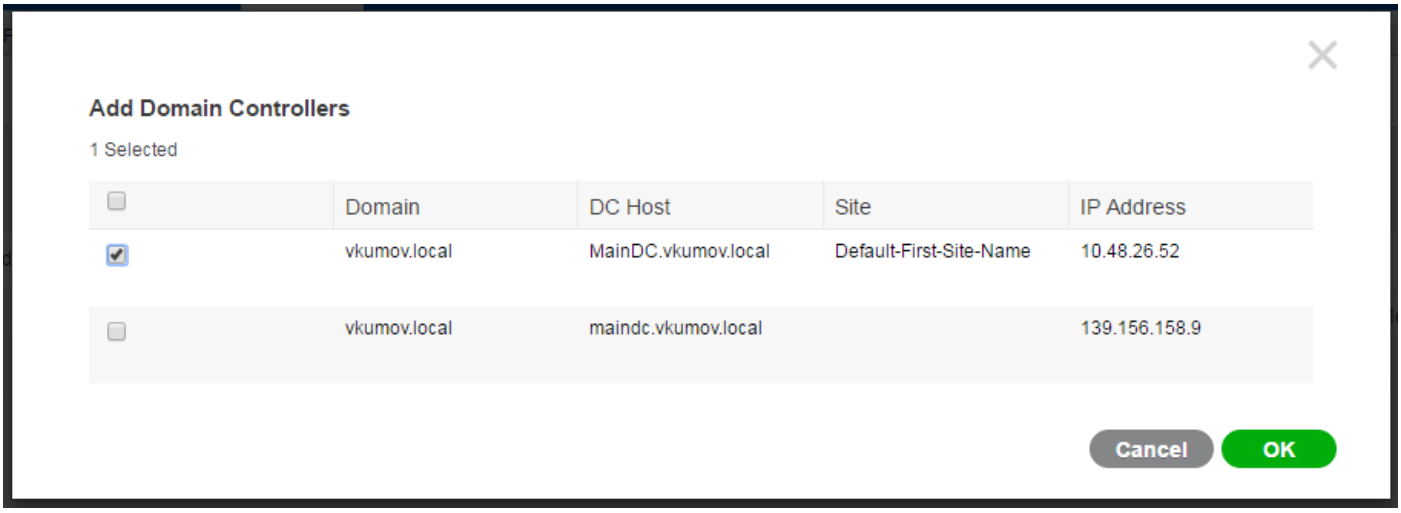
- `HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`
- `HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`

الخطوة 3. إضافة وكلاء PassiveID.

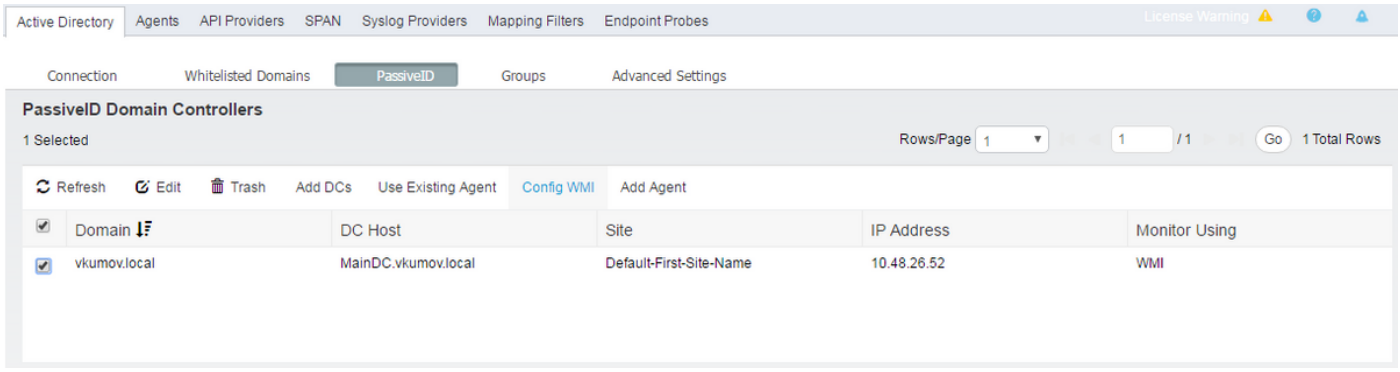
في صفحة مجال AD، انتقل إلى علامة التبويب PassiveID وانقر فوق **إضافة ملفات DC**، كما هو موضح في الصورة:



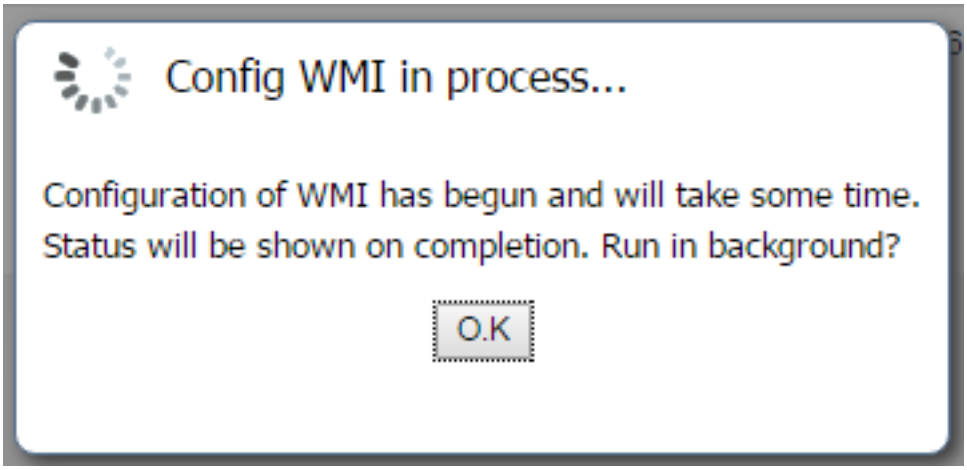
يظهر إطار جديد وتقوم ISE بتحميل قائمة بجميع وحدات التحكم بالمجال المتوفرة. حدد وحدات التحكم في الوصول (DC) التي ترغب في تكوين WMI فيها وانقر فوق **موافق** لحفظ التغييرات، كما هو موضح في الصورة:



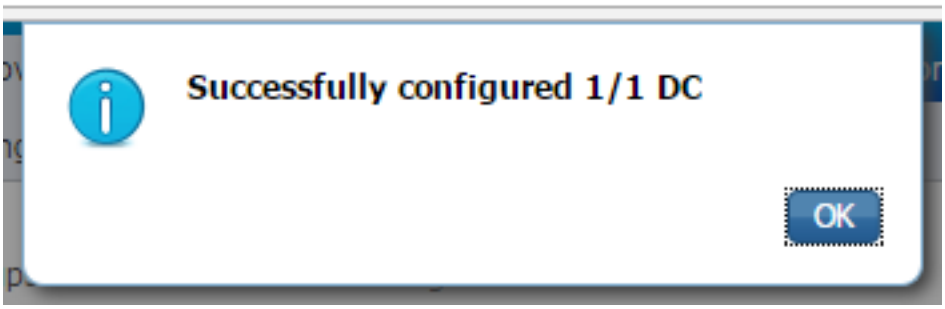
تتم إضافة وحدات التحكم بالمجال DC المحددة إلى قائمة وحدات التحكم **بالمجال PassiveID.** **حدد وحدات التحكم في الوصول (DC) وانقر فوق الزر تكوين WMI**:



تعرض ISE PIC رسالة تشير إلى أن عملية التكوين قيد التقدم:



بعد مرور دقيقتين، تظهر لك رسالة مفادها أنه تم تكوين WMI بنجاح على وحدات التحكم بالمجال DC المحددة:



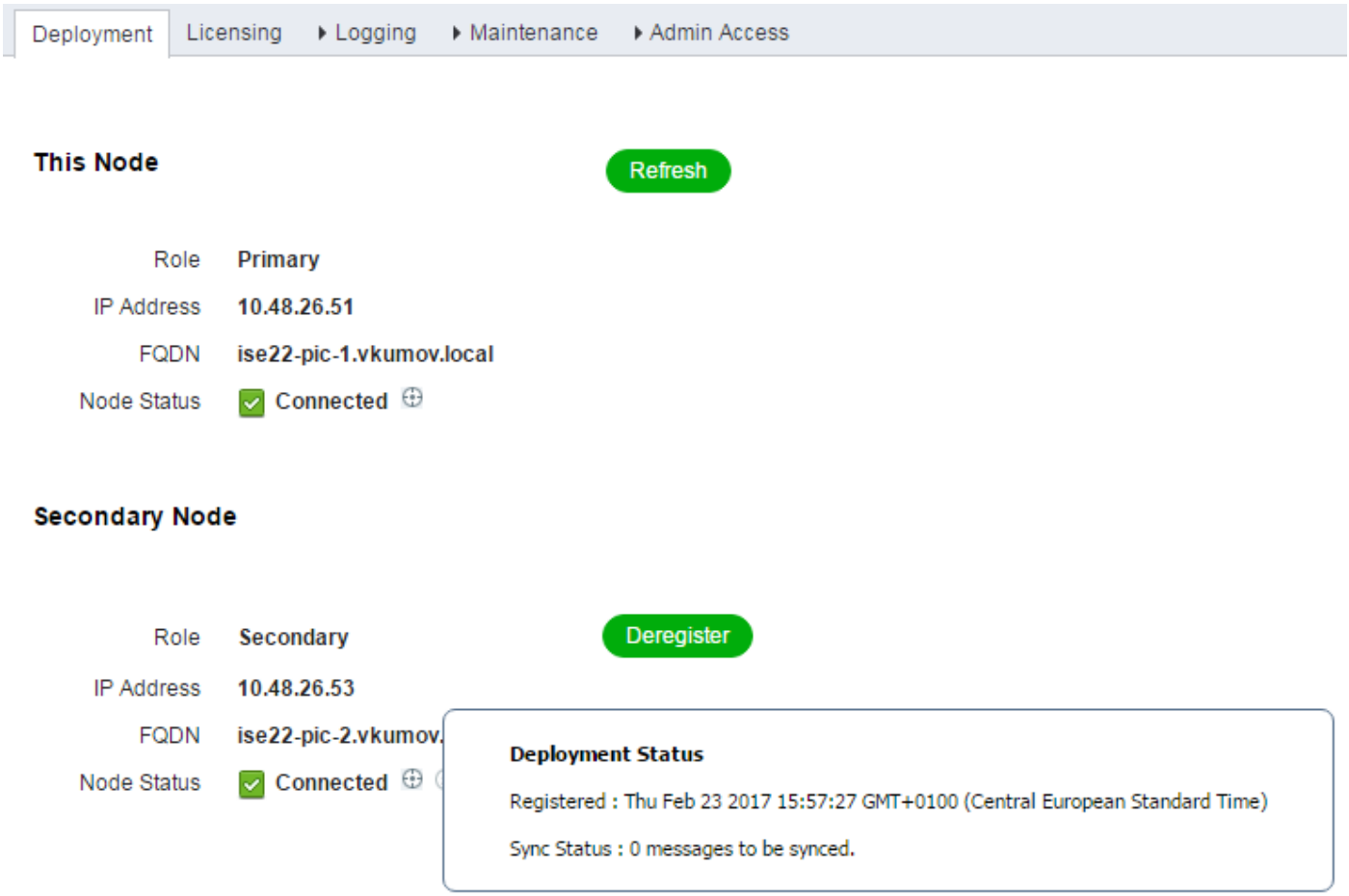
التحقق من الصحة

النشر

يمكن التحقق من حالة النشر بعدة طرق:

صفحة النشر

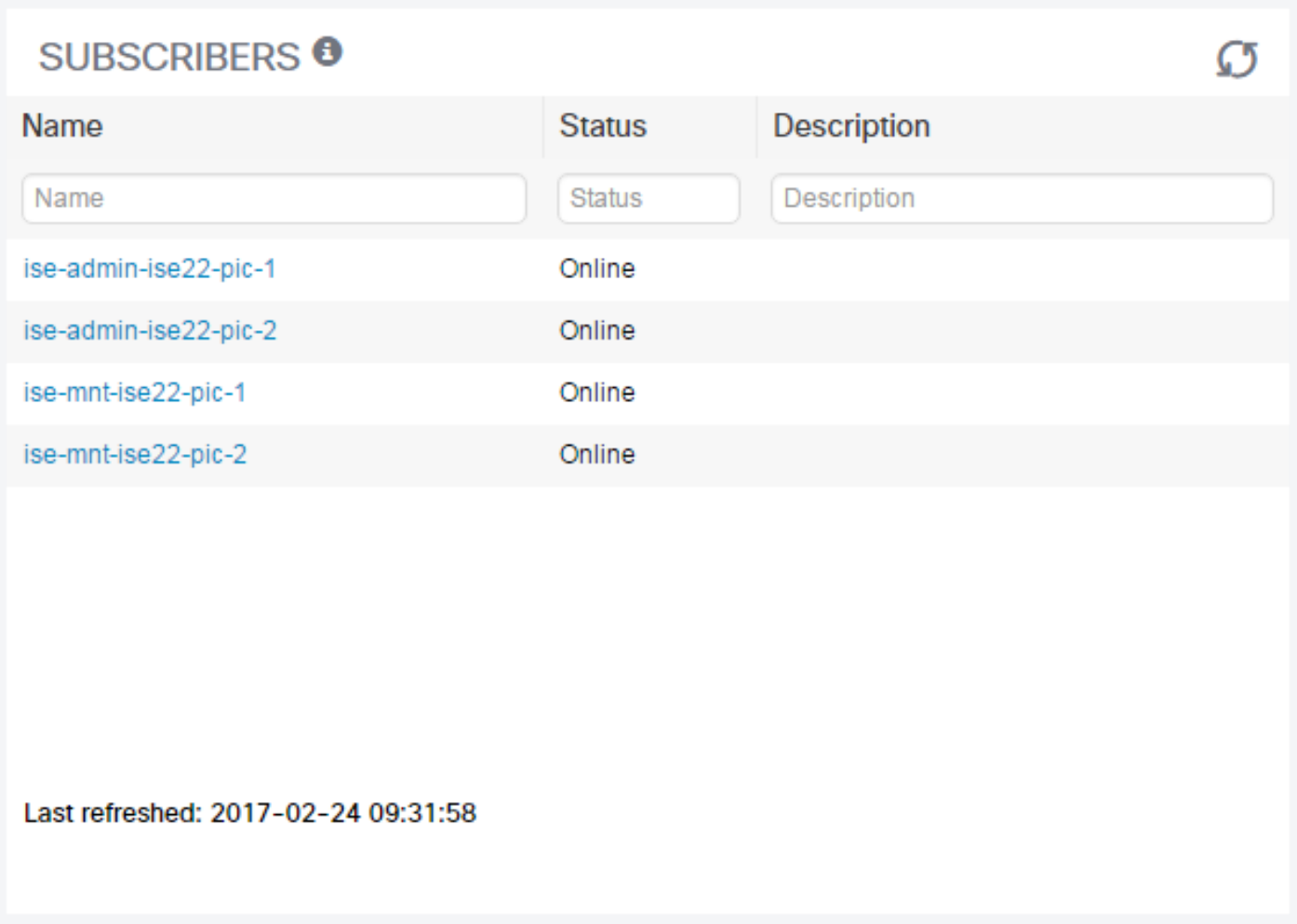
انتقل إلى **إدارة > صفحة النشر** يمكن التحقق من الحالة الحالية للنشر:



من هذه الصفحة يمكن إلغاء تسجيل العقدة الثانوية إذا لزم الأمر. يمكن بدء المزامنة اليدوية ويمكن التحقق من **حالة المزامنة**.

صفحة لوحة المعلومات

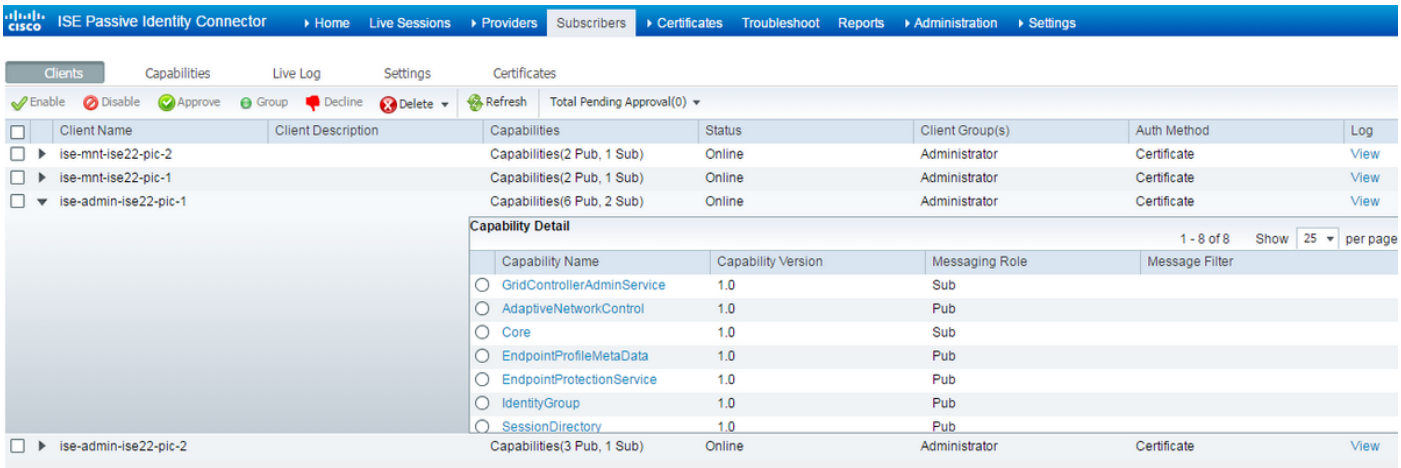
في صفحة ISE PIC الرئيسية هناك dashlet يسمى **مشتركين**. باستخدام dashlet هذا، يمكنك التحقق من الحالة الحالية لعقد ISE PIC، كما هو موضح في الصورة:



يقوم ISE PIC بإنشاء مشتركين لكل عقدة - admin وmnt. **يجب أن تكون جميعها في وضع متصل** مما يعني أن العقد قابلة للتنشيط وتشغيلها.

مكتتبون

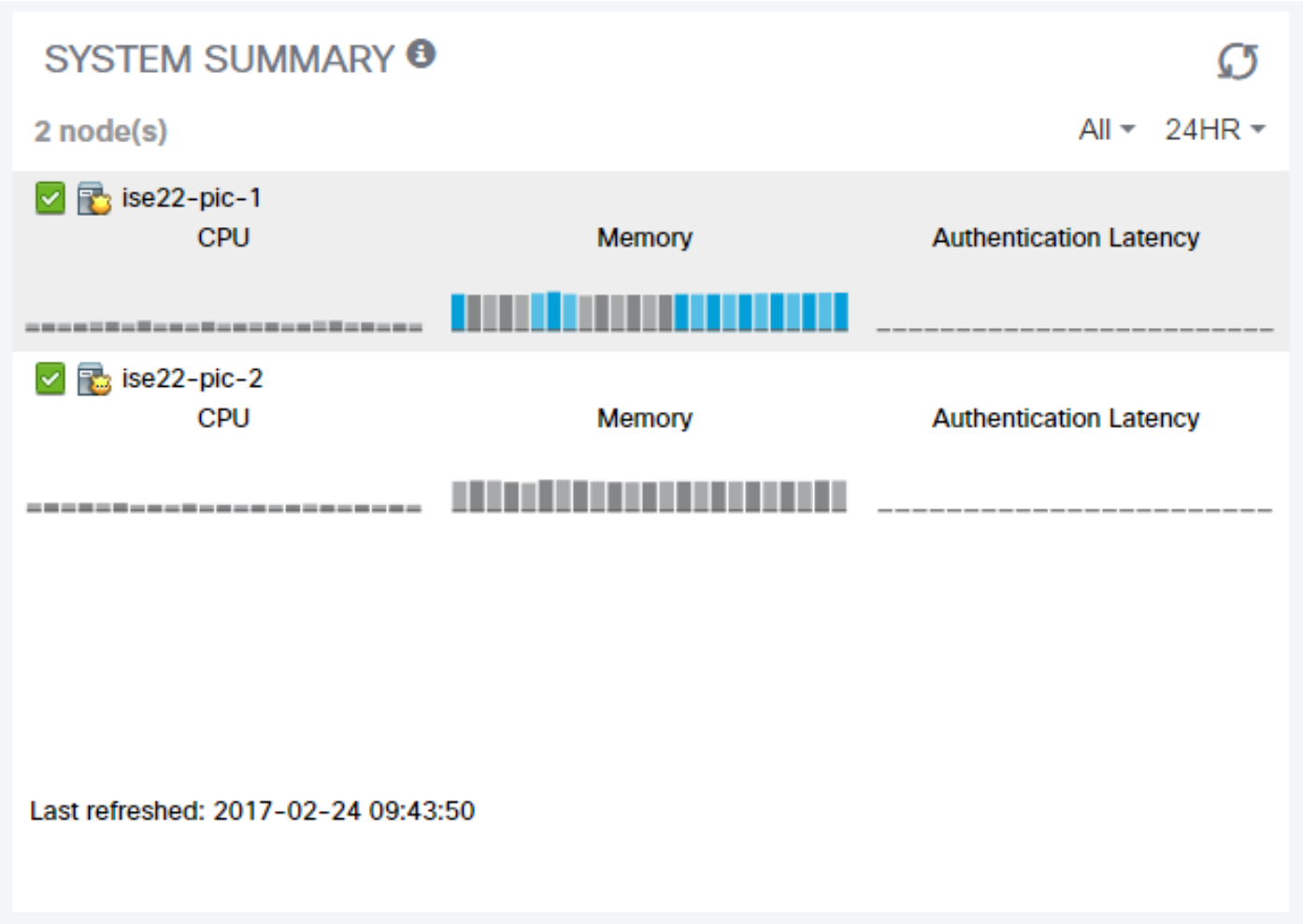
صفحة **المشتركين** هي إصدار موسع من dashlet للمشتركين من الصفحة الرئيسية ل ISE PIC. تظهر هذه الصفحة جميع PxGrid ذات الصلة، ومع ذلك يمكن التحقق من حالة عقد ISE PIC هنا أيضا:



ملخص النظام

يسمح ISE PIC بمراقبة ملخص الحماية للعقد كذلك. يمكن العثور على dashlet هذا في

المنزل > لوحة المعلومات > إضافي:

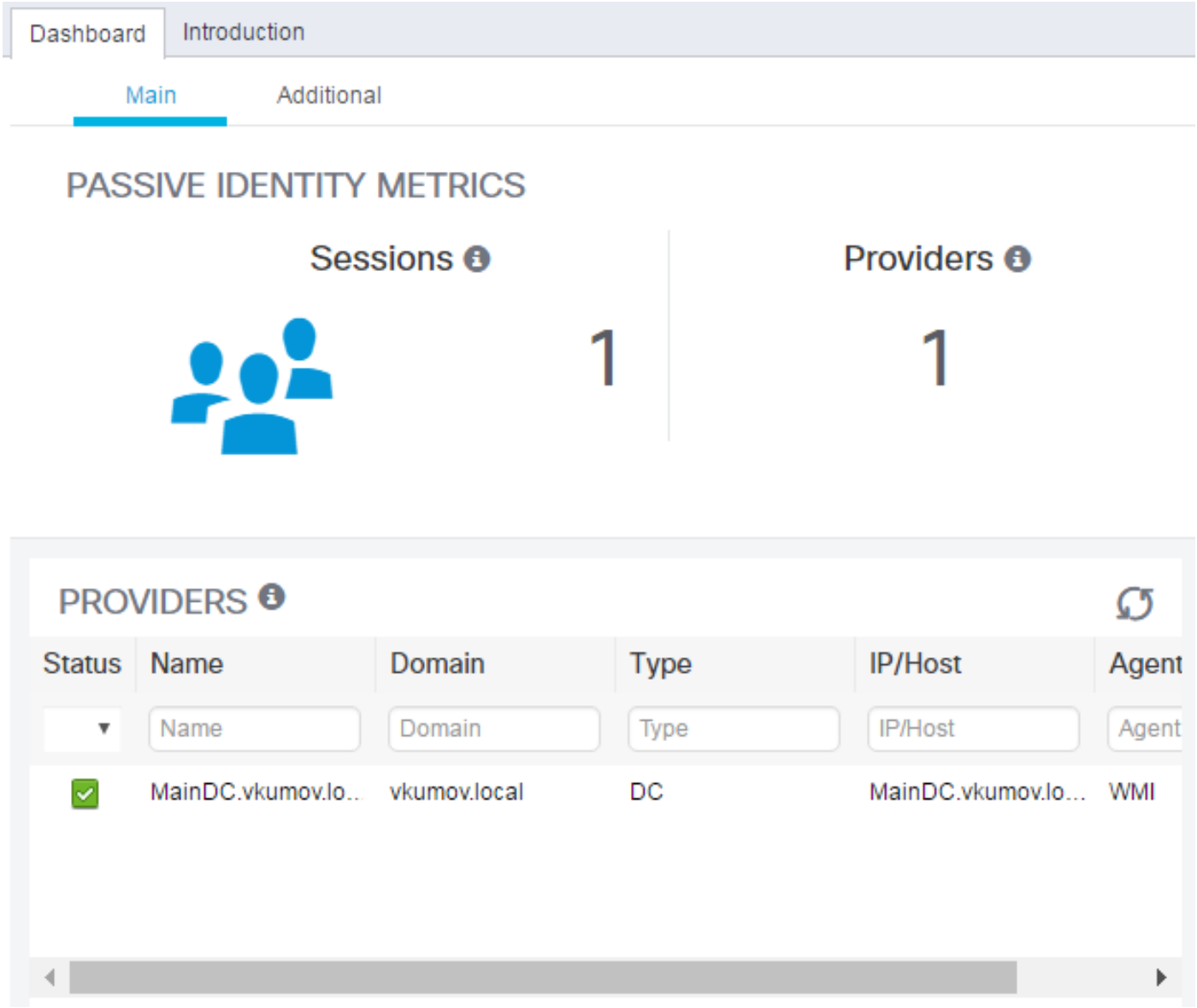


دائما ما يكون **زمن الوصول للمصادقة** 0ms حيث أن ISE PIC لا يقوم بأي مصادقة/تخويل.

الموفرون والجلسات

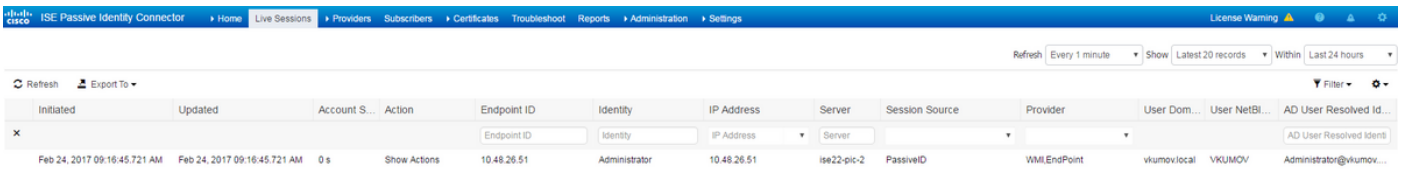
الصفحة الرئيسية

يمكن التحقق من حالات الموفرين وكمالتهم ومقدار جلسات العمل التي تم العثور عليها أثناء التنقل إلى **الصفحة الرئيسية > صفحة لوحة المعلومات**:



جلسات عمل مباشرة

يمكن العثور على معلومات تفصيلية حول جميع جلسات عمل المستخدمين التي تم العثور عليها في صفحة **جلسات عمل Live**:



وهو يحتوي على معلومات مثل:

- الموفر - ما هو الموفرون الذين تم إستخدامهم لتعريف جلسة العمل هذه
- بدء الجلسة وتحديثها - الطوابع الزمنية عند بدء الجلسة وتحديثها وفقا لذلك
- عنوان IP - عنوان نقطة النهاية
- الإجراء - الإجراءات التي يمكن ل ISE تنفيذها (على سبيل المثال، التحقق من حالة

نقطة النهاية، أو إذا تم دمج ISE PIC مع pxGrid ثم إرسال طلب لمسح الجلسة)

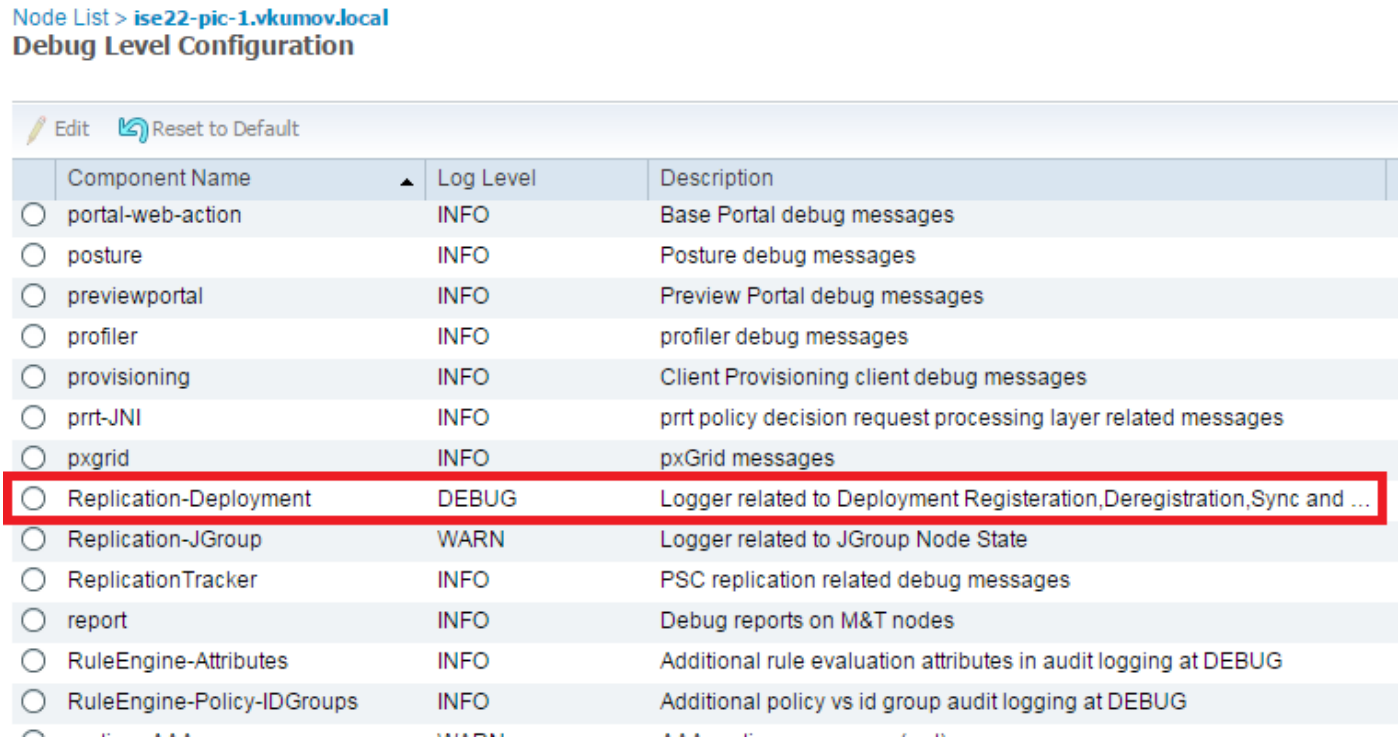
استكشاف الأخطاء وإصلاحها

النشر

لاستكشاف أخطاء النشر والنسخ المتماثل وإصلاحها، ابحث في ملفات السجل هذه:

- ملف النسخ
- deployment.log
- ise-psc.log

لتمكين تصحيح الأخطاء، انتقل إلى **الإدارة > تسجيل الدخول > تكوين سجل تصحيح الأخطاء**:



تتم كتابة هذه الأخطاء إلى ملف **replication.log**. فيما يلي مثال على عملية نسخ مماثل عادية:

```
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
```

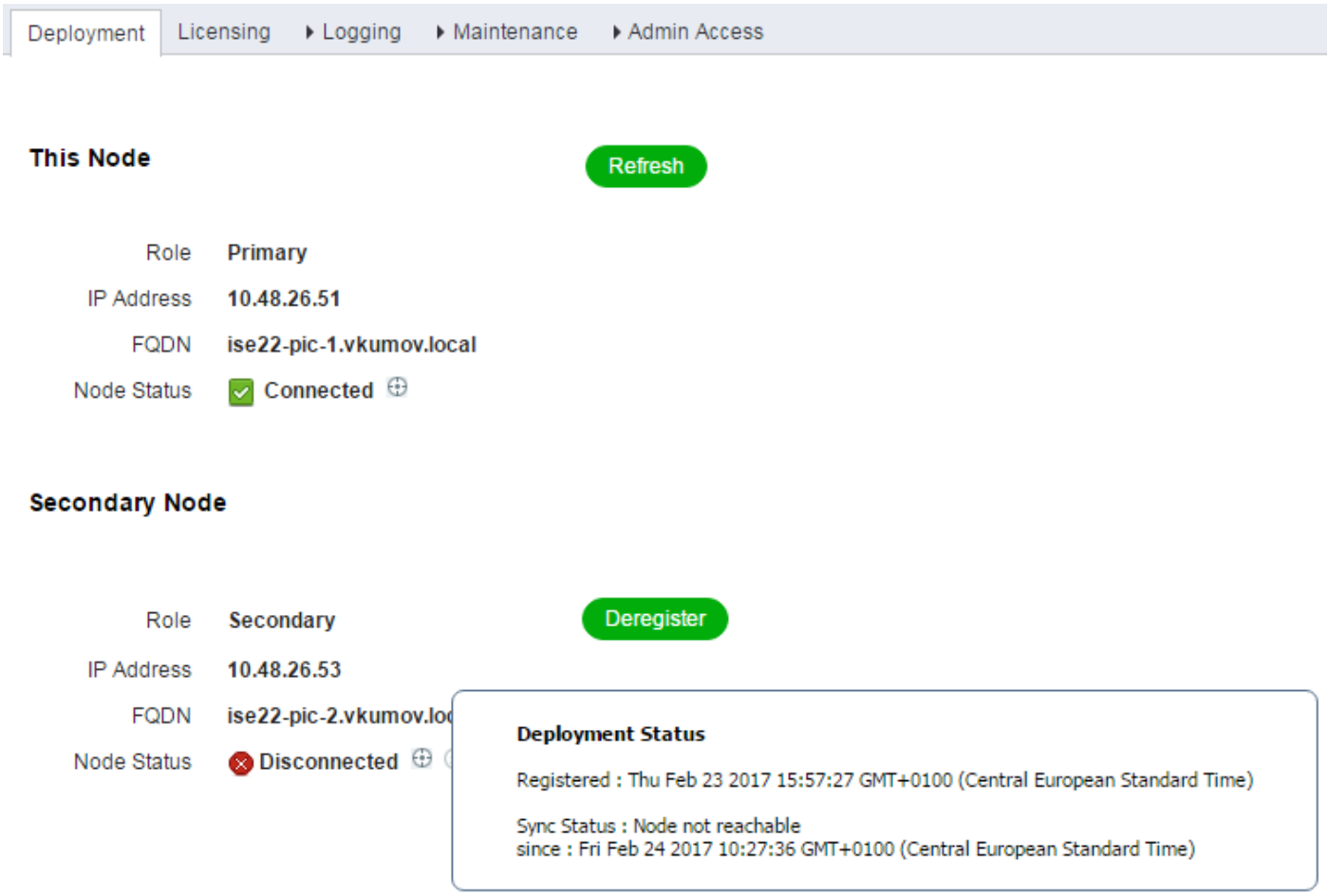
```
method=[id=[3ded93c0-fa70-11e6-b684-005056990fbb],startTime=[0],endTime=[0],applied=[false],data
length=[794],sequenceNumber=[1600]2017-02-24 10:04:26.364]
2017-02-24 10:11:06,895 DEBUG [pool-214-thread-1][]
cisco.cpm.deployment.replication.ClientNodeProxy -:::::- Calling setClusterState(name: ise22-pic-
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]
```

رسالة من **ise-psc.log**:

```
2017-02-24 10:19:36,902 INFO   [pool-216-thread-1][]
api.services.persistance.dao.DistributionDAO -:::NodeStateMonitor:- Host Name: ise22-pic-2, DB
'SEC_REPLICATIONSTATUS' = SYNC COMPLETED, Node Persona: SECONDARY, ReplicationStatus obj status:
SYNC_COMPLETED
```

المشكلة المشتركة: العقدة الثانوية غير قابلة للبلوغ

إذا أصبحت العقدة الثانوية غير قابلة للإصلاح، فسيتم عرضها في **صفحة الإدارة > النشر**:



يحتوي **ISE-psc.log** على هذه الرسالة:

```
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
```

توضح هذه الرسالة ما لا يمكن الوصول إليه، على سبيل المثال لا تستجيب العقدة إلى ping:

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

الإجراءات التي يجب اتخاذها: التحقق من إمكانية حل FQDN للعقدة الثانوية، تحقق من اتصال الشبكة الأساسي بين العقد.

في حالة عدم تشغيل التطبيقات في العقدة الثانوية أو في حالة وجود جدار حماية بين العقد، **قد يعرض ise-psc.log** الرسائل التالية:

```
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
```

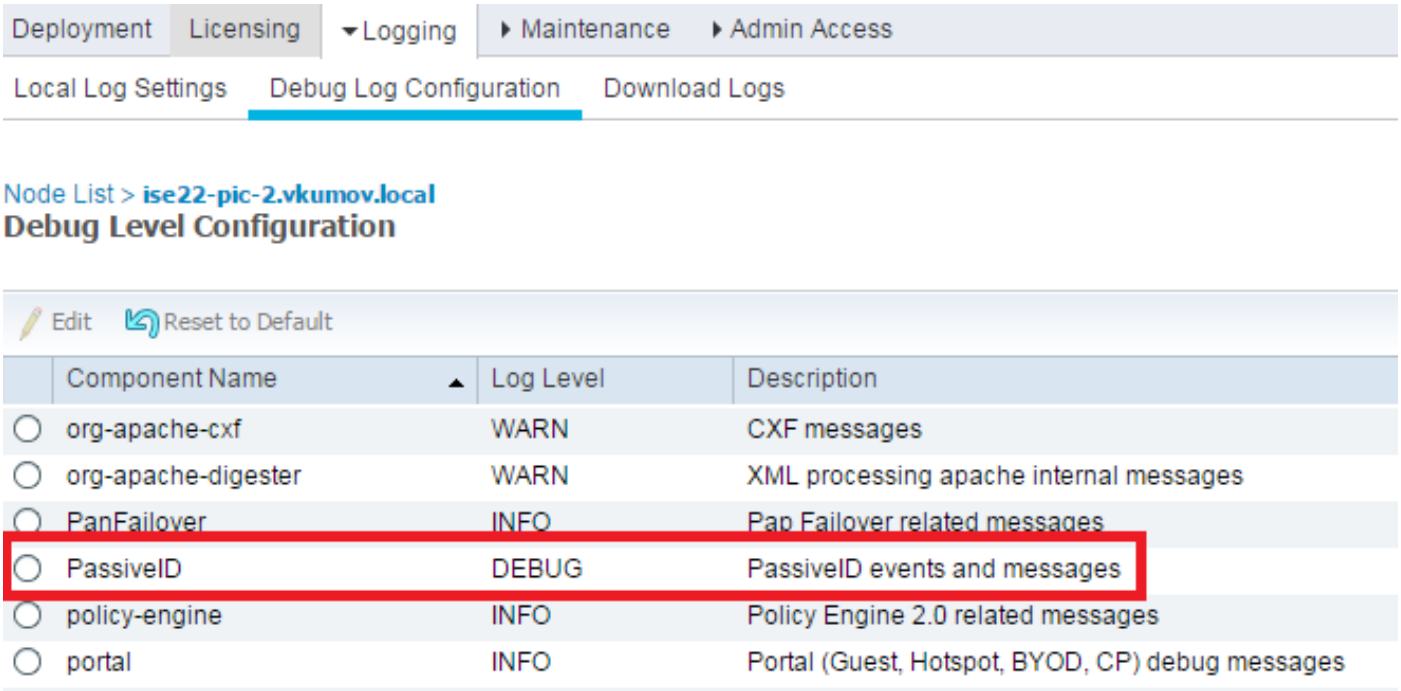
الإجراءات التي يجب إتخاذها: تحقق من حالة التطبيق على العقدة الثانوية، تحقق من اتصال الشبكة إذا كان يسمح بجميع الاتصالات بين العقد.

Active Directory و WMI

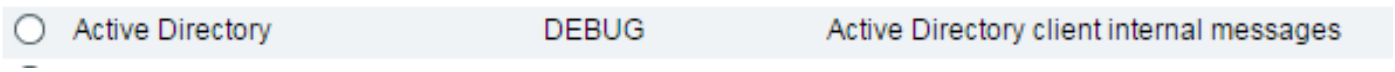
لاستكشاف أخطاء Active Directory WMI وإصلاحها، ابحث في هذه الملفات:

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

ويمكن تمكين تصحيح الأخطاء المفيد في **الإدارة > تسجيل الدخول > تكوين سجل الأخطاء**:



و:



هنا مثال من جديد يعلم جلسة من **passive-wmi.log** مع تمكين تصحيح الأخطاء:

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

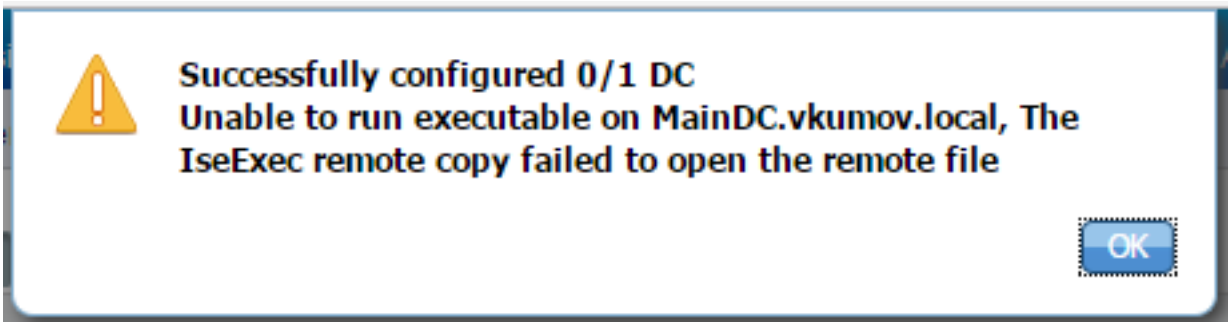
```
Mapping.dc-name = MainDC.vkumov.local , Identity Mapping.event-user-name = Administrator ,
Identity Mapping.dc-host = MainDC.vkumov.local/10.48.26.52 , Identity Mapping.server = ise22-
pic-2 , Identity Mapping.event-ip-address = 10.48.26.52 ,
```

مثال على التحقق من نقطة النهاية من **passive-endpoint.log** (في هذه الحالة كانت نقطة النهاية ال يمكن الوصول إليها من ISE):

```
2017-02-23 13:48:29,298 INFO   [EndPointProbe-Workers-Check-2][] com.cisco.idc.endpoint-probe-
[PsExec-10.48.26.51]  is User=vkumov.local/Administrator Still There ? ...
2017-02-23 13:48:32,335 INFO   [EndPointProbe-Workers-Check-2][] com.cisco.idc.endpoint-probe-
[PsExec-10.48.26.51]  Identity check result is - > Endpoint UNREACHABLE
```

مشكلة شائعة: ISE PIC ترمي خطأ "يتعذر تشغيل الملف التنفيذي على <DC name>..."

إذا لم يكن لدى المستخدم المستخدم المستخدم للانضمام إلى بطاقة ISE PIC للمجال الأذونات الكافية، فإن بطاقة ISE PIC تلقي خطأ أثناء تكوين WMI:



يمكن العثور على تصحيح الأخطاء المناسب في ملف **ad_agent.log** (**يجب تعيين مستوى سجل Active Directory على تصحيح الأخطاء**):

```
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
```

الإجراءات التي يجب إتخاذها: إعادة الانضمام إلى عقد ISE PIC إلى المجال باستخدام بيانات اعتماد مسؤول المجال أو إضافة المستخدم المستخدم المستخدم لعملية الانضمام إلى مجموعة *مسؤولي المجال* في AD.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).